TAG Cyber
Security Annual
3RD QUARTER 2023

CYBERSECURITY IN OUTER SPACE UNPREPARED?

ARTICLES / OPINIONS / INTERVIEWS

INTRODUCTION

WHY YOU SHOULD CARE ABOUT SPACE

DAVID HECHLER, EDITOR

If you asked a variety of people—some with tech backgrounds, some without—if they fear they will be harmed by a catastrophic cyberattack, I suspect the answers would be mixed. If you probed deeper and explored what those who answered yes worry about, I bet you would get lots of explanations. Some might talk about ransomware. Others might mention deepfakes or another form of deception linked to artificial intelligence (all the rage these days). But I would be surprised if anyone brought up outer space.

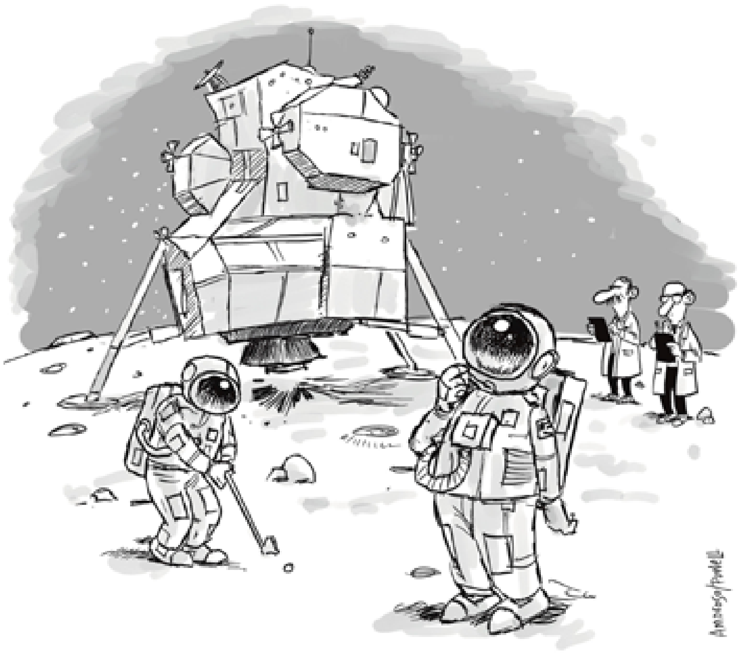
I'm not saying that they should. But I will say they could.

So much of the world's cyber infrastructure is up there. And it's getting more and more crowded. And dangerous. There have been near-collisions. There's an increasing sense of competition in space among nation-states that are adversaries. And that makes us all a lot more vulnerable than we may think.

I hasten to add that the six feature articles we have in this issue are not designed to scare you. They cover a broad range of subjects. There are cautionary tales, but there are also articles that dwell on the ways satellites have opened the world to places that had been isolated and neglected. Most of the articles offer advice that companies can learn from.

There are useful history lessons and articles that look forward. One points out the ways nation-states are unprepared to communicate, should there be a disaster. Another discusses the 1967 law that is supposed to keep the peace up there. A third one suggests there will be missions to Mars during this decade.

The message we hope you take away is this: Outer space hasn't gotten its due. Doesn't it say something that a Chinese spy balloon on the loose overshadowed any other news you can quickly think of on this subject? It's time we paid attention.



The first Deepfake.

TAG Cyber Security Annual
2ND QUARTER 2023

Lester Goodman, Director of Content

David Hechler, Editor

Contibutors

Dr, Edward Amoroso
Moriah Hara
David Hechler
John J. Masserini
David Neuman
Christopher R. Wilder

Editorial & Creative

Lester Goodman
David Hechler
Jaimie Kanwar
Julius Williams
Miles McDonald
Rich Powell

Research & Development

Matt Amoroso
Shawn Hopkins

Sales & Customer Relations

Rick Friedel
Trish Vatis
Michael McKenna
Laurie Mushinsky
Julia Almazova
Jane Mangiamele

Administration

Liam Baglivo

Dr. Edward Amoroso, Founder & CEO

TAG Cyber Security Annual
3RD QUARTER 2023
CYBERSECURITY IN OUTER SPACE
UNPREPARED?
ARTICLES | OPINIONS | INTERVIEWS

Volume 9 No. 3

Publisher: TAG Cyber, a division of TAG Infosphere, Inc.,
45 Broadway, Suite 1250, New York, NY 10006.

Security experts and practitioners must recognize that best practices, technologies, and information about the cyber security industry and its participants will always be changing. Such experts and practitioners must therefore rely on their experience, expertise, and knowledge with respect to interpretation and application of the opinions, information, advice, and recommendations contained and described herein.

Neither the authors of this document nor TAG Infosphere, Inc. assume any liability for any injury and/or damage to persons or organizations as a matter of products liability, negligence or otherwise, or from any use or operation of any products, vendors, methods, instructions, recommendations, or ideas contained in any aspect of the 2023 TAG Cyber Security Annual volumes.

The opinions, information, advice, and recommendations expressed in this publication are not representations of fact, and are subject to change without notice. TAG Infosphere, Inc. reserves the right to change its policies or explanations of its policies at any time without notice.

The opinions expressed in this document are those of the TAG Cyber Analysts, and in no way reflect those of its Distinguished Vendors.

July 26, 2023

CONTENTS

IN FOCUS:

WE IGNORE OUTER SPACE SECURITY AT OUR PERIL

CYBERSECURITY IN THE SPACE DOMAIN: SAFEGUARDING OUR FUTURE

SPACE CENTER HOUSTON

International Space Center Mission Control

DAVID NEUMAN

In the quiet and bustling offices of the International Space Station's control center in Houston, Texas, a tension-filled silence suddenly hung in the air. The screens in front of the control team flickered, shifting from the usual display of telemetry data to an ominous black. Only a single line of text remained: "Access granted. Control transferred."

A thousand kilometers above, the International Space Station (ISS) began slowly veering off its usual orbital track, unbeknownst to the astronauts living and working inside. Meanwhile, thousands of kilometers below, another significant event was taking place.

Simultaneously, the global positioning system (GPS) ground stations, a constellation of 24 satellites traveling 12,000 miles above the Earth to provide positioning data to billions of users around the globe, started reporting unexpected anomalies. This wasn't an isolated error; all 24 satellites were rapidly rendered non-operational. The lifeblood of navigation and timestamping systems worldwide was effectively silenced.

Down on Earth, the impacts of this double-edged attack were almost immediate. Air traffic controllers stared at their screens in bewilderment as the positional data of thousands of planes disappeared.

Contemplating the chaos of a major cyberattack on space technology may be easier than trying to imagine a coordinated response.

Ships at sea lost their bearings, and self-driving vehicles on the streets came to a bewildered halt, unable to pinpoint their location. Stock markets experienced extreme turbulence as high-frequency trading systems faltered.

In the backrooms of power grids, engineers watched in horror as synchronization of the grid, which relied on GPS timestamps, started to fail, causing blackouts in cities worldwide. At the same time, billions of smartphone users were suddenly unable to access location-based services, severely disrupting daily life and business operations. The world had been rendered blind and lost in space and time.

At the ISS control center, the staff desperately tried to regain command of the space station. Their concern was not just for astronaut safety but also for the dozens of crucial scientific experiments onboard, many of which had implications for climate research and future space exploration. As the ISS continued its unintended and risky orbital maneuver, the specter of the uncontrollable descent of the 420,000 kg station towards Earth loomed, with potentially catastrophic consequences for those on board and those in the projected impact zone on Earth.

Suppose this hypothetical scenario had actually happened. What would come next?

Chaos would have erupted in the civilian world and within the corridors of power, both domestic and international. A flurry of activity would have begun within various government agencies in the United States. The Department of Homeland Security would have quickly mobilized to protect and coordinate a response to cyberattacks against terrestrial components of the space systems.

And so it went. As they worked tirelessly to manage the impact on civilian infrastructure, the Federal Bureau of Investigation launched a parallel investigation, seeking to identify the perpetrators of the cybercrime. Simultaneously, the Department of Defense, in coordination with the U.S. Space Force and U.S. Cyber Command, focused on the defense of national space systems. Their immediate goal was to restore control of the International Space Station and the GPS satellites while securing other space-based assets against potential follow-up attacks.

The National Reconnaissance Office, tasked with operating intelligence satellites, was also in high gear, scanning through petabytes of data to ascertain if the attack originated from a foreign power. Meanwhile, the National Aeronautics and Space Administration (NASA) provided technical support, applying its extensive expertise on the ISS to help regain control of the wayward space station.

Despite this flurry of activity, there was a palpable sense of confusion and tension due to overlapping jurisdictions and the need for defined responsibilities. It needed to be made clear who should be taking the lead, causing delays in the response and creating friction between agencies. With its responsibility for commercial spaceflight, the Federal Aviation Administration felt sidelined despite the significant impact on commercial aviation and navigation systems.

Internationally, the response was even more fragmented. Nations dependent on GPS scrambled to mitigate the impacts. Discussions started at the United Nations about the need for an international framework for space cybersecurity. The spacefaring nations, each with its own stake in space assets, urgently convened to discuss a joint response. But the absence of an international body with clear responsibility and authority to respond to space-based cyberattacks added another layer of complexity and delay.

This hypothetical is indeed the stuff of science fiction. And yet, it represents a plausible threat in our increasingly interconnected and space-reliant world. The repercussions such an event could have on society and businesses worldwide, from disrupting air travel and telecommunications to causing catastrophic power failures and affecting financial markets, are alarming.

Our future on Earth and in space is irrevocably tied to our ability to safeguard these crucial systems from cyber threats. Hence, the need for technological solutions and international cooperation, for norms and defined responsibilities in this rapidly growing field. This is not merely about preserving the status quo; it's about securing a future where space continues to be a resource that unites nations, propels economic growth, and catalyzes scientific discovery.

WE ARE INTERTWINED WITH THE SPACE DOMAIN

Our entanglement with these space systems stretches far wider and deeper into our everyday lives and societies than one might initially realize. A look at satellite communications, weather forecasting, climate monitoring, and other dependencies throws this into stark relief.

An attack on satellite communications, the backbone of global connectivity, would go beyond merely obstructing GPS navigation. It would cripple services like TV broadcasts, internet connectivity, and long-distance telephony. This would be particularly detrimental to remote and rural areas, where traditional infrastructure may not reach, potentially isolating entire communities.

Simultaneously, our ability to predict and prepare for severe weather conditions could be dramatically hampered if the satellites that monitor weather patterns and climate trends were compromised. Such an event would not only impair our ability to provide life-saving early warnings for hurricanes or monsoons, it could also compromise our long-term understanding of climate change, with far-reaching implications for the planet.

Similarly, an attack on space-based systems that support precision agriculture, global financial systems, emergency services, and scientific research would prove devastating. Farmers could face massive agricultural losses without the weather data they rely on. Disruptions in the precise timestamping provided by GPS satellites could send shockwaves through global stock exchanges and banking transactions, potentially triggering widespread economic instability. Additionally, we rely on emergency services for safety and security, such as fire, police, and ambulance services, which could significantly increase response times without reliable navigation systems. Finally, pursuing knowledge could be stalled, as researchers across various fields—from wildlife migration to astronomy—rely heavily on satellite technology for data gathering and observation.

THE COMPOSITION OF SPACE SYSTEMS AND OPERATIONS

This extensive network of dependencies highlights the need for robust and proactive measures to safeguard space-based assets from the looming threat of cyberattacks. Protecting space systems requires cyber defenders to fully grasp intricate operations and interconnections. Like an enterprise, these systems contain many connected components, each potentially a vulnerability that adversaries could exploit. Comprehending how they fit together, function, and interact is key. It empowers defenders to anticipate threats, implement protections, and maintain resilience.

Securing assets from cyber threats isn't just about guarding individual components. It's about protecting an entire ecosystem, which demands a holistic understanding of the system's architecture and operations. In the intricate ballet of global communication, space-based assets such as satellites, space telescopes, and space stations perform their dance high above the Earth. Each celestial body houses its onboard systems.

Think of these as the asset's brain—containing computer processors, storage, sensors, and communication antennas. Some even have thrusters for maneuvering. This array of onboard systems receives commands from Earth and manages the assets' daily operations, ensuring the harmony of their orbital dance.

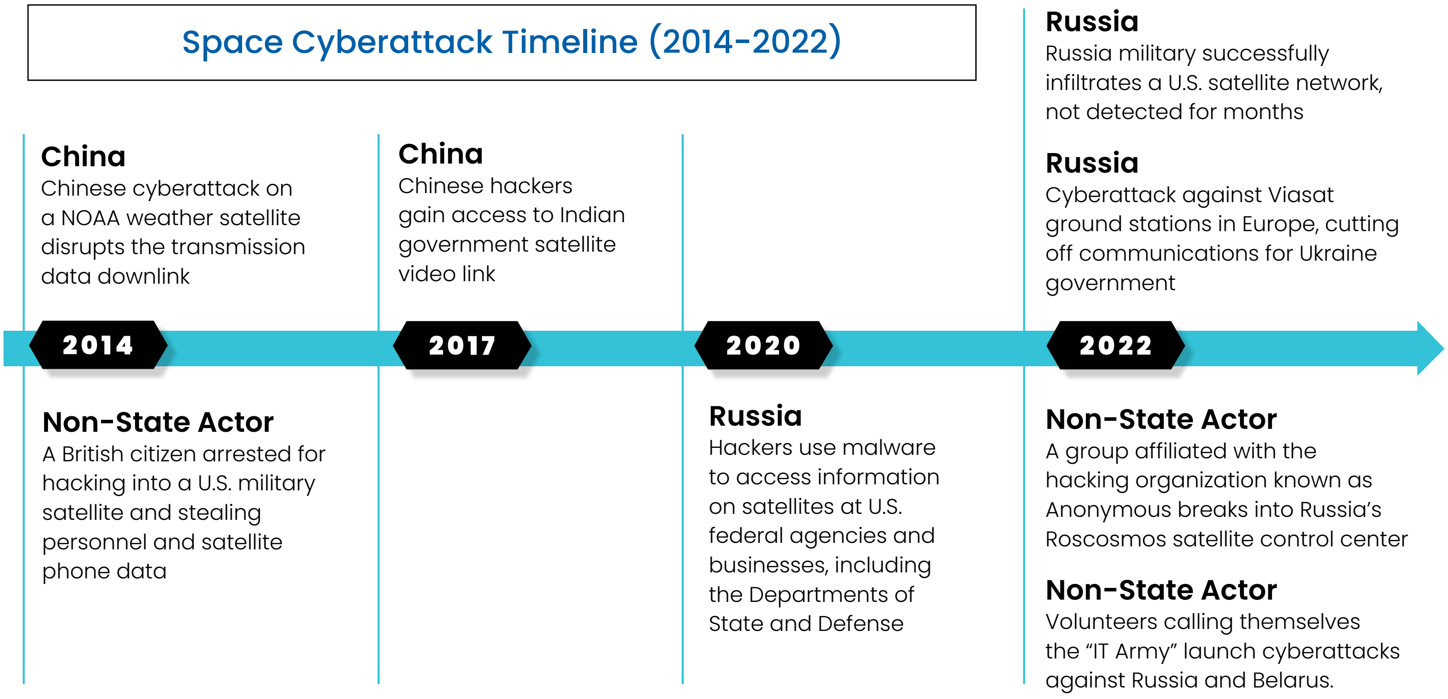
On the Earth's surface, the dance partners of these space assets are the ground stations, each equipped with large antennas. Positioned strategically around the world, they maintain a constant pas de deux with the satellites, undeterred by the Earth's rotation. Here is where the conversation happens—ground stations dispatch commands to the satellites and, in return, receive a cascade of data. They function as the essential terrestrial connection points in this vast space communication network, transmitting and receiving signals like the ebb and flow of an electromagnetic tide.

But the dance does not end there. The data, once received, embarks on a new journey, coursing through terrestrial networks toward data centers scattered across various locations. The frequencies and technologies forming these communication links vary, fine-tuned for the type of satellite and its distance from Earth. The information is processed, stored, and analyzed in these data centers, converting the raw data into a comprehensible format for further use.

Finally, these data centers also take on the pivotal role of a command hub, from which operators send instructions to the space-based assets. This intricate network, stretching from the silent void of space to the bustling data centers on Earth, forms a complicated choreography far more elaborate and interconnected than traditional technology systems. Understanding this network is vital to appreciating the sophistication of our modern space infrastructure, and the vulnerabilities that must be secured to protect it.

THREATS TO SPACE OPERATIONS

While specific details about cyberattacks on space systems are often classified or undisclosed due to national security concerns, several recent incidents shed light on the types and severity of such threats. These real-world attacks illustrate the diversity of the space ecosystem's cyber threats, ranging from service disruption to espionage. The threats can come from various sources, including nation-states, non-nation threat actors, and individual hackers. (I have created below a timeline of recent space-related attacks, including published attributions of the attackers.)



Space Cyberattack Timeline (2014-2022)

2014

China
Chinese cyberattack on a NOAA weather satellite disrupts the transmission data downlink

Non-State Actor
A British citizen arrested for hacking into a U.S. military satellite and stealing personnel and satellite phone data

2017

China
Chinese hackers gain access to Indian government satellite video link

2020

Russia
Hackers use malware to access information on satellites at U.S. federal agencies and businesses, including the Departments of State and Defense

2022

Russia
Russia military successfully infiltrates a U.S. satellite network, not detected for months

Russia
Cyberattack against Viasat ground stations in Europe, cutting off communications for Ukraine government

Non-State Actor
A group affiliated with the hacking organization known as Anonymous breaks into Russia's Roscosmos satellite control center

Non-State Actor
Volunteers calling themselves the "IT Army" launch cyberattacks against Russia and Belarus.

Why is space particularly susceptible to cyber threats? While space assets share similarities with those affecting terrestrial systems, several factors make them uniquely vulnerable. Assets such as satellites are designed to operate for many years, sometimes even decades. This longevity means their onboard security can quickly become outdated, making them more vulnerable to evolving threats. Once a satellite is in orbit, it's virtually impossible to physically access it for repairs or upgrades. Therefore, any security vulnerabilities present at launch, or those that arise due to changing threat landscapes, can't be rectified.

Due to the inherent latency in communication with space assets, and the limited processing capabilities of many satellites, sophisticated real-time intrusion detection and response measures take time to implement. The radio signals used for satellite communication can be relatively easy to intercept, jam, or spoof, especially those of lower-frequency bands, unless protected by strong encryption and authentication measures. Components for space assets often come from a global supply chain, increasing the risk of compromised hardware or software being included in the final product.

Given these challenges, cybersecurity in the space domain requires specialized strategies and solutions that go beyond the measures employed in traditional IT systems. It calls for secure design and manufacturing advances, robust encryption and authentication protocols, secure and reliable command-and-control systems, and international cooperation to establish space-specific cybersecurity norms and practices.

SECURING SPACE AGAINST CYBERATTACKS

As we extend our reach into the cosmos, security becomes paramount. This reality is rendered more pressing as the scope of our space economy continues to expand. The 5,400 satellites currently in orbit will be dwarfed by the anticipated launch of more than 24,500 satellites over the next decade. Commercial ventures will account for over 70% of these new celestial bodies.

The escalating significance of these assets to the global infrastructure, and the mounting sophistication of cyber threats, underline the urgency for innovative solutions. However, the unique hurdles presented necessitate a different approach than we typically employ to tackle traditional cybersecurity issues.

Several solutions are emerging, each addressing the specific cybersecurity demands of the space domain. Quantum encryption, for instance, is leading the way in communication protection between space assets and ground stations, as traditional encryption methods risk obsolescence in the face of advancing quantum computing. AI and machine learning are emerging as invaluable tools for real-time threat identification, sifting through massive data sets to improve response times and system resilience.

As our space assets multiply, secure space traffic management is becoming increasingly vital for identifying potential cyberattacks and ensuring safe operation. A commitment to cyber resilience in space systems design is essential. Building these systems with cybersecurity as a cornerstone from inception will help ensure they can withstand future threats.

In an increasingly interconnected world, establishing international cybersecurity standards for space could unify and enhance the security of all spacefaring nations and companies. And leveraging blockchain technology could help secure the integrity of hardware and software used in space systems, mitigating a significant source of the threats.

Finally, strengthening the security of land-based components, such as ground stations and data centers, is crucial to a holistic space strategy. By integrating these innovative technologies and approaches, we can fortify the cybersecurity of the space domain, securing the critical services we rely on now and will continue to rely on in the future.

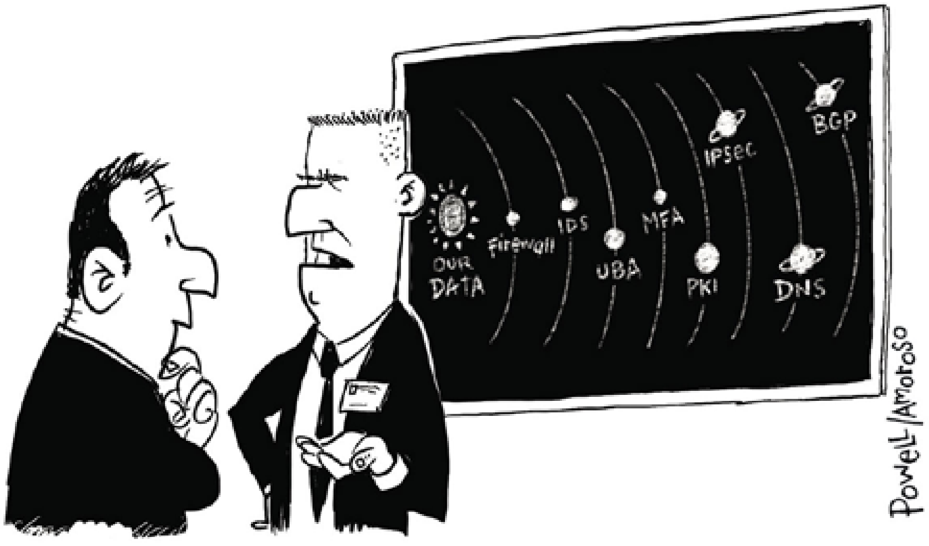
THE TAKEAWAY

My hypothetical cyberattack was designed to serve as a sobering reminder of the potential vulnerabilities and profound consequences of such an attack on our space-based systems. I hope it underscored thought-provoking questions about our preparedness, the interconnectedness of our world, and the urgent need for action.

Moreover, the response portrayed in our scenario highlights the challenges of coordinating a timely and effective counter to space-based cyber threats. Overlapping jurisdictions, a lack of defined responsibilities, and the absence of international protocols create confusion and delays, leaving us vulnerable. It emphasizes the critical need for collaboration and clear lines of authority to ensure a swift and coordinated response.

I hope the scenario also underscored the unique nature of space as a domain for cyber threats. The longevity of space assets, the difficulty of access for upgrades, and the global supply chains make them particularly susceptible to evolving risks. We must recognize the distinctive characteristics of space systems and develop tailored strategies to protect them from threats that transcend traditional cybersecurity approaches.

Our future, on Earth and beyond, is inseparable from the space domain. It is time for governments, organizations, and individuals to prioritize the protection of our space-based systems and preserve the benefits they bring. Will we unite to strengthen resilience, foster international collaboration, and establish robust frameworks to defend against space-based cyber threats? The answer will shape the future of our interconnected world and determine whether space remains a beacon of unity, innovation, and exploration.



"Uh, yes – I will admit some NASA influence in the new security architecture."

EIGHT SPACE HACKS WE SHOULD EXPECT TO SEE

DR. EDWARD AMOROSO

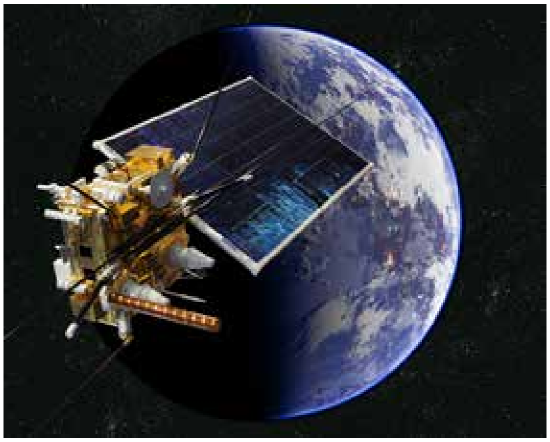
Maybe you remember the New York Times **report** a few years ago that suggested that the U.S. military had secretly hacked an attempted missile launch by North Korea. In my opinion, it is probably wrong. Pyongyang seems sufficiently inept to not need the assistance of foreign hackers to cause their launches to fail.

That said, I believe that the technical and operational capabilities are 100% present and available to target space systems. This includes ground-based launch and control, space-to-ground communications, space-born satellites, vehicles, and stations, and other space-based resources, including sensitive data collection.

I am not talking here about garden-variety hacking by newbies, but rather professional targeting of space-based assets by the world's most capable offensive actors. In the most obvious cases, this means nation-states targeting other nation-states because they have usually been the most motivated. But it can include other use-cases.

Consider, for instance, Elon Musk and the controversies he has stirred up in recent years. My 40 years of experience in cybersecurity tells me that when someone acts the way he has, some group will decide to target him. And hacking campaigns are the perfect medium. They are easy to pull off and feasible to do anonymously and with impunity. I expect to see more of them.

Below I imagine eight scenarios that target space. And I'll also suggest potential solutions. I am not making predictions here. I am only describing attacks that seem the most feasible to me. Also, don't expect a complex analysis of weaknesses in a synthetic aperture radar scheme. My purpose is to explain in simple terms what I would expect to begin happening in a more regular manner as we increase our activity in space.



Nation-states are likely the most motivated to attack space technology, but they are not alone.

HACK 1 THEFT OF SATELLITE SURVEILLANCE DATA

This is an obvious cyber risk. We should expect to see this happening frequently as nations such as the United States extend their global footprints into space. And this is not some theoretical prediction. Back in 2014, a Russian hacking group called **Turla** managed to hijack satellite data that was being sent to users in Africa and the Middle East. A couple of years later, the infamous **Shadow Brokers** hacking group released offensive satellite data intercept tools they'd stolen from the National Security Agency, which had developed them. To deal with this type of theft, satellite communications will require transition to fully zero trust-based secure sessions using contextual, adaptive authentication and post-quantum encryption of data.

HACK 2 ATTACKS ON THE SPACE SOFTWARE SUPPLY CHAIN

This seems a more likely attack path given the complexity of space-based systems and their growing dependence on third-party and open source code. The well-known SolarWinds attack in 2019 could just as easily have targeted code developed for space applications as IT management systems. Expect to see AI-generated code also finding its way into space system reuse—a trend accelerated by the commercialization of space by for-profit companies. To address this threat, the space supply chain will require the software bill of materials (SBOM) and the software compositional analysis (SCA) to address supply chain risks in mission-critical components.

HACK 3 SATELLITE SERVICE JAMMING

Jamming is a well-known denial of service attack, and space systems have always been vulnerable. In 2014, a Russian company called KRET made available a sophisticated GPS and military **satellite jamming system.** Two years earlier, South Korea reported that its military and civilian satellites appeared to have been jammed intentionally by the North Koreans. Technology-based solutions to this problem will have to become more prominent. Methods for improving the defense against denial-of-service attacks will become a higher technical and operational priority in robust satellite communications for both commercial and military applications.

HACK 4 GPS SPOOFING

GPS spoofing involves tricking receivers by sending fake or manipulated signals intended to confuse the calculation of position, velocity, or time information. The U.S. GPS system consists of a group of satellites, referred to collectively as Navstar, that broadcast codes for transmission. The military encrypts these codes, but civilian use is clear text, which invites the spoofing problem. As a result, civilian GPS security infrastructure and protocol improvements will be required to harden signal acquisition, signal manipulation avoidance, proper timing, and secure transmission.

HACK 5 KINETIC ATTACKS ON SATELLITES (ASAT)

This is the Hollywood version of space attacks, where nation-states spectacularly blow up or otherwise severely damage each other's satellites. In 2019, India destroyed one of its own satellites called Microsat-R as part of an operational test. The result was considerable debate about **space debris,** which can create real danger because it doesn't go anywhere, and how this method might be extended to space warfare. (The **United States, Russia, and China** have also destroyed satellites to demonstrate their capabilities.) Solutions here will require a combination of technical hardening of satellites against kinetic attacks as well as diplomatic and international norms on what is considered acceptable behavior in this dangerous new area of testing and warfare.

HACK 6 ATTACKS ON THE SPACE SOFTWARE SUPPLY CHAIN

Software-defined satellites support the ability to program the hardware more flexibly—an obvious advantage for a flying object. Functions such as redirecting or splitting capacity and changing beam characteristics are good examples of modern advances in this new technology. One can only imagine the types of software hacks that will come with such technological capability for virtualized operations. Solutions will emerge from the security virtualization community that will ensure that satellite software is modular, segmented, and properly distributed to avoid cascading threats within and between satellite infrastructure.

HACK 7 REMOTE ACCESS TO SATELLITES

It should be obvious that satellites require administration and even updates at times. To date, this has required astronauts (my first boss at Bell Labs was Terry Hart, a specialist astronaut who flew on Shuttle mission STS-41-C, which basically fixed a satellite). As this process matures and includes a more modern software patch and update infrastructure, we should expect to see hackers targeting this capability. Solutions will be required that can ensure properly authenticated, validated, secured, and monitored updates to the software on a future software-defined satellite.

HACK 8 HACKS TO U.S. SPACE FORCE

In December 2016, U.S. Department of Homeland Security officials confirmed that a Russian cyberwarfare group known as APT28 had been **targeting U.S. satellites**. Presumably, this falls into the responsibility of the new **U.S. Space Force** (USSF), established in 2019 as a branch of the armed forces. Its goal is to organize, train, and equip space forces to protect U.S. interests in space. Since its inception, USSF has been building out infrastructure to deal with vulnerabilities. As such, one must expect this to be a massive target of foreign nation-states. One can only hope this brand new agency is up to the task.

I could go on, but you get the idea. The risks and the opportunities for nation-states to exploit these vulnerabilities are plentiful.

For those of you in the vendor community, it is worth mentioning that in a commercial cybersecurity market where there are too many solutions using the same technical and operational approaches (e.g., EDR, SIEM, EPP, and on and on), our TAG Cyber analysts see basically zero proposals from startups to address the threats listed above. *Hint, hint.*

LESSONS FROM SPACE: SECURING THE ENTERPRISE SUPPLY CHAIN

JOHN J. MASSERINI

As I write this, the team over at Virgin Galactic is celebrating its first commercial space flight, joining SpaceX as the only two private companies taking humans to space. Unsurprisingly, both companies have announced plans to leverage the technology they are developing for trips to Mars by the end of the decade.

When we consider the complexity of a roundtrip mission to Mars, it quickly becomes apparent that any such effort would heavily rely upon numerous partners, third parties, and a host of supply chain dependencies. Everything from nutritional supplies and clothing to various operating systems and processor boards will all be designed and produced by third parties. What lessons can terrestrial corporate enterprises learn from studying how space missions manage supply chain risk? And how can we take advantage of that learning?

Over the past several years, supply chain security has become the rallying cry for both the enterprise and the vendor communities. While understanding the risk within our collective supply chains is critical, and obviously fraught with various challenges that will take us years to unwind, understanding the scope and breadth of supply chain risks in space is an entirely new level of complexity. From ensuring a safe food supply to having a high level of confidence in the accuracy and logic of critical processing units, there is no limit to the ways a secure supply chain is essential if we are to achieve our interplanetary objectives.

So, when we look at the supply chain for space missions, having clarity on precisely what software will be executed during which parts of the mission is of critical importance. Historically, government-funded and executed space missions maintained a high degree of control around the components used during the building of mission vehicles and control systems. There was generally a high level of inherent trust within the supply chain, given the extreme level of secrecy surrounding early NASA missions.

Crisis management takes on a whole new meaning when it applies to space travel, but some of the basic tenets can also apply to businesses.

Today, however, with the almost feverish push to move space exploration to the commercial sector, supply chain risks are significantly higher than ever before. In the early days of manned space exploration, NASA had complete control over every design activity that went into the vehicle. Now these commercial ventures are buying parts, processors, and services from a host of third parties, all of which could wreak havoc on the mission. We have all read the substantiated reports of backdoors built into widely used firmware, but what are the potential implications of a similar incident impacting a space mission?

Consider the projected trip to Mars that will likely occur in the average reader's lifetime. The entire vehicle must be a completely self-contained domicile for the astronauts for years. Air, food, water—all of the necessities of life must be fully actualized on board the vessel. What would happen if, a couple of months into the flight, a piece of ransomware woke up and took control of the air purification or guidance system? Who would pay the ransom? What if the demand wasn't for money but rather for geopolitical action that put the lives of the astronauts up for barter? What are the ultimate supply chain risks that are deemed "acceptable" when evaluating the costs of supplies and vendors versus the risk introduced into the mission? And more importantly, who will be accountable if those accepted risks end up causing mission failure?

WHAT CAN BUSINESSES LEARN FROM SPACE MISSIONS?

Securing the supply chain of a space mission is far more complicated than managing third parties here on Earth. Unlike our typical enterprise infrastructures, there is no backup to restore, a system restart is potentially a life-or-death decision, and "cleaning up the mess" is simply not viable. We cannot drop in a new piece of hardware or patch away the problem, or even roll back to a known-good point in time. No, supply chain risk must be addressed head-on, long before the ignition switch is proverbially thrown.

Obviously, crisis management takes on an entirely new meaning when dealing with space travel, but some of the same basic tenets that would protect those brave souls who board that ship can be applied as part of every enterprise architecture design here on terra firma. These are principles to which all companies can and should subscribe.

1. **Segment, segment, segment:** With the explosion of cloud services over the past decade, along with the ever-increasing adoption of virtualization internally, segregating third-party critical services from each other with segmentation drastically minimizes the overall risk to the mission—whether the mission is going to Mars or just making this year's numbers. If the environmental support functions on

a spacecraft do not need to have access to the propulsion systems, they shouldn't. If there is no need for an outsourced customer support function to be on the same network as your internal finance team, then why allow it to be?

2. **Strip it down:** According to NASA, the Space Shuttle had a whopping 2k of memory that contained 154 executable instructions. Stop and consider that for just a moment. Every single byte of memory was accounted for, every instruction was the absolute minimum it took to perform the job, which resulted in the most successful space operation for decades. So why does a vendor doing data analytics need hundreds of open source libraries maintained by unknown resources from who knows where?

   Isn't it time we start holding these software providers—including Apple, Microsoft, and Red Hat—responsible for providing us with the absolute minimal operating system that we need to get the devices functional, and allowing us to control what else gets loaded? This is arguably the biggest challenge most vendors have. Requiring suppliers to submit a software bill of materials (SBOM) won't fix all the problems, but it would at least tie some accountability to the vendors and facilitate the removal of anything unnecessary. Force your supply chain vendors to be transparent, hold them accountable, and be prepared to walk away from a tool if they balk at providing a secure and functional solution.

3. **Mission Control is mandatory:** The mere idea of a space mission without Mission Control is incomprehensible. Even with our highly segmented environments aboard the ship, and the absolute minimum amount of code in use to execute the trip, there is still enough room for telemetry gathering and communication sharing with Mission Control. So why, then, do so many third parties and supply chain vendors scoff at the idea of providing you visibility into what their systems are doing? They seem to be suggesting that doing so would be giving up control.

   The argument, however ridiculous, is that there is "proprietary information" within their systems or "stability and availability concerns" that preclude them from providing access to their environment for monitoring. It's time to demand that your third parties provide you with the same level of insight as you have throughout the rest of your environment. They should understand that providing their telemetry to your Mission Control platform is no longer optional.

By implementing these three basic principles, an enterprise can make significant progress toward mitigating the supply chain risks it faces. Consider segmenting your networks from your third parties, or at a minimum, limiting the traffic that can cross the partner/enterprise boundary. Much like the mission vehicle, a failure in one system (or network) should not impact the adjacent one. Also, minimizing the attack surface, or "stripping it down," is crucial to understanding the inherent risk a third party can introduce. Knowing exactly what your third party is installing, building, or configuring is a fundamental practice in supply chain management. Finally, you should demand to have as much visibility into their environment as you have in yours. Make them integrate that capability into your Security Operations Center (a.k.a. your "Mission Control"). Observability is critical in managing risk, and your Mission Control should see everything.

THE REAL MEANING OF "MISSION CRITICAL"

In many organizations, the term "mission critical" has a very distinct meaning. Yet, it is a term often tossed around the enterprise to indicate an application or technology that is of utmost importance to the revenue stream. Sadly, in many organizations that mission critical mentality ends when it comes to investments in resiliency and security—both of which are absolutely required during a space mission.

When you evaluate your supply chain, do you feel comfortable that you have resiliency and security from your third-party providers? Do they contribute to your mission of protecting your business, your customers, and your brand? Do they support your "Mission Control" in a way that is beneficial and empowering? If not, it may be time to jettison them and find a company that will.

HARNESSING SATELLITE TECHNOLOGY FOR ECONOMIC TRANSFORMATION: AN INSIDER'S PERSPECTIVE

CHRISTOPHER R. WILDER

During three decades of forging a path in security and communications, my fascination with satellite technology's explosive, game-changing potential has only intensified. I was first exposed to it in the U.S. Navy and then in the intelligence community. My interest has been particularly piqued by its efficacy in creating and securing critical infrastructure, especially in remote regions and emerging economies, where traditional communication and surveillance often fall short.

CHRISTOPHER R. WILDER

I advise multiple private and public sector projects worldwide that leverage satellites to open economies, provide access to commerce and education, and improve internet connectivity. Our work is focused on 20 African countries, several Asian countries, the Middle East, and South America, where each is rich in opportunity but challenged by an infrastructure gap.

Satellite technology is a linchpin of reliable and secure communication networks in remote regions such as these. It's especially effective for monitoring critical infrastructures like power grids, transportation networks, and water systems. I've seen how satellite technology and ground control facilities manage crucial infrastructure operations and enhance physical security by offering surveillance and early warning against threats and bad actors.

In many parts of the world, conventional terrestrial communication networks are either scarce or nonexistent. This is due to geographical and socioeconomic challenges that make establishing physical infrastructure difficult. It is here that satellite communication shines. It allows these regions to stay connected, profoundly impacting public safety, emergency response efforts, and economic development.

While the costs are going down, satellite communications are still expensive. But companies like **Starlink** and **Viasat** are bringing down prices and providing access to a broader population. Further, satellite technology enables essential services like telemedicine, distance learning, and e-commerce. I've seen firsthand how these services spur economic development and enhance the quality of life for populations in regions lacking conventional infrastructure.

Satellite networks are generally secure. Their primary vulnerability often lies in the ground systems.

For example, I was recently involved in a project in the Middle East, assisting a life support camp for oil and gas workers. After the camp was acquired from its previous owners, as a result of our security and geopolitical intelligence assessment, we decided to provide free internet connectivity via satellite and other means to the local communities and residents in and around the camp.

The local community valued access to commerce, education, and social media. These opportunities were perceived as a benefit rather than a threat. Access to the internet and the world represent opportunity and hope for underserved communities. As a result, local support helped reduce the threat that bad actors would harm the camp and our people, who had delivered the main access to the online world in the region.

IT'S NOT JUST THE EYE IN THE SKY

Ground controls are indispensable in satellite operations. They help identify and resolve problems. They play a vital role in safeguarding critical infrastructure by monitoring potential threats, such as space debris or solar flares, which could compromise satellite operations.

Satellite technology plays a significant role in increasing physical security through remote monitoring systems. I've witnessed how these systems enable real-time tracking and surveillance of key infrastructures, like power plants and transportation networks. They can detect and alert security personnel to threats like unauthorized entry or equipment tampering. They can track bad actors and build a body of evidence to help prove criminal activity. These abilities are particularly valuable in emerging economies and countries with limited infrastructure.

Satellite technology bridges infrastructure gaps and enhances economic development in remote regions with inadequate traditional infrastructure. Through reliable communication and remote monitoring, the technology allows businesses to operate more efficiently, fostering the creation of new industries. I've found it invaluable in providing improved physical security measures, particularly in regions vulnerable to political instability or conflict such as what we see today in Eastern Europe and many nations in Africa.

ADVICE FROM THE FIELD

Austin Gadient

While satellite networks are generally secure, their primary vulnerability often lies in the ground systems, which may house vulnerable workstations, outdated IoT devices, and individuals susceptible to phishing attacks or social engineering campaigns. **Austin Gadient,** co-founder and chief technology officer of Linux Security company **Vali Cyber**, recently told me about hacking groups that successfully exploited vulnerabilities on Russian and Indian satellites.

Considering these risks, Gadient, who previously served in the U.S. Air Force and worked for the Department of Defense in its satellite technology advancement program, emphasized the need for robust network security and segmentation. The keys, he said, are efficient patch management processes, comprehensive asset inventory systems, and encryption. He suggested adding endpoint detection response (EDR) and network intrusion detection software to identify and respond to threats.

Gadient also talked about the importance of adopting a systematic approach. He underscored the importance of adhering to a risk management framework like NIST, ISO, or SOC/2 to ensure comprehensive coverage. Companies should question the vendors they use about their own security practices when procuring software. Gadient recommended that vendors use static application security testing (SAST) and dynamic application security testing (DAST) to check for vulnerabilities.

Physical security measures like badge systems, fences, bollards, cameras, and motion sensors are critical to protecting ground control systems. Ongoing monitoring by trained experts is vital to ensure that the security of these systems is maintained. I agree with Gadient that satellite cameras and motion sensors should be deployed, and trained experts should consistently monitor them.

BRIDGING THE GAP BETWEEN IT AND OT SYSTEMS

Finally, satellite network security is a complex issue spanning the information technology (IT) and operational technology (OT) domains. Gadient told me that he's seen a dichotomy in the approach companies take. Many maintain a clear segmentation between their OT and IT environments, a practice adhered to in the Department of Defense. This segmentation is crucial in the face of cyber threats that are often initiated via phishing emails and other IT-centric attack vectors. He added that It's imperative to ensure that robust firewalls and network segmentation will prevent a compromise in the IT environment from traversing into the OT environment.

However, maintaining strict network segmentation has its downsides. An IT environment, by its nature, allows for faster updates and the adoption of cutting-edge technologies. Balancing this need for innovation while maintaining a robust security posture is tricky. Any new technology introduced must be put through rigorous security compliance certification from trusted and certified vendors. Failing to do so can be dangerous.

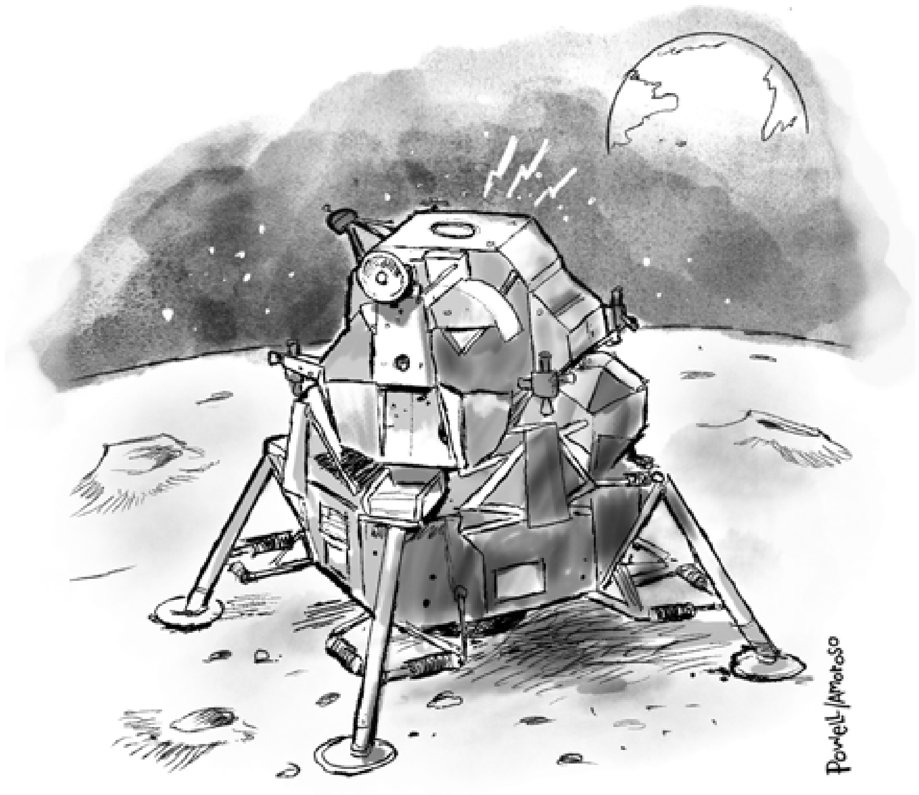
For instance, there have been cases where knock-off versions of satellite ground control products from China were sold as genuine Cisco products. The companies that bought them later learned that they were loaded with backdoors and worms that led to severe security compromises. Therefore, purchasing from trusted vendors should be seen as an essential aspect of network security. Even if local regulations don't require adherence to strict rules, leveraging international risk management and compliance frameworks can provide a sound structure for building secure satellite architectures. Compliance may not equate to security, but it does provide a blueprint for best practices in the field.

THE TAKEAWAY

The importance of a robust security posture for satellite networks cannot be overstated. Ground system vulnerabilities pose real threats, and if they get exploited, the damage is just as real.

Striking a balance between innovation and security is difficult but not impossible. New technology adoption must be accompanied by rigorous security compliance checks and ongoing security assessments. And working with trustworthy vendors is pivotal.

International risk management and compliance frameworks provide a key structure for building secure architectures, regardless of your operational environment. The future demands a proactive approach to security. By investing in strong network security, responsibly integrating advanced technologies, and adhering to risk management protocols, we can ensure the continued security of our satellite networks while driving technological progress forward.



Uh, Houston - we'd like to start up our engines,
so please confirm payment of ransomware."

WHY RESILIENCE IN SPACE IS RELEVANT TO YOUR BUSINESS

MORIAH HARA

If you are concerned about attacks on the cloud providers that power your business, you may also need to worry about attacks on satellites that increasingly power these providers. In the last two decades, whether we've realized it or not, we've grown ever more dependent on space-based technology. Space-based services support critical infrastructure such as utilities, aviation, and emergency communications. If U.S. satellites went down today, within hours most of the planet's traffic would grind to a halt. The world economy would shut down. Most countries would declare a state of emergency. This is because cell towers use satellites to route phone calls, ATMs, and cash registers. Electrical grids use them to send power to your house, and stock exchanges use them to regulate the trades that go into stock portfolios and investment funds.

We've come a long way from what started as a competition between the U.S. and Russia with the launch of Sputnik in 1957. The last 20 years in particular have seen a massive economic investment in space. The global space economy's value reached $350 billion in 2020 and is projected to grow to $1 trillion by 2040. As an increasing number of satellites are launched—Amazon, OneWeb, Boeing, Telesat, and SpaceX are planning vast new groups—these so-called mega constellations will increasingly provide network and communication services to enterprises.

Space is getting ever more crowded. Already 80 countries have a presence there, and major companies plan to launch another 50,000 satellites.

Consider that cloud service providers (CSPs) are utilizing medium Earth orbit satellites to improve data transfer, especially between physically challenging locations. For example, some CSPs are using satellites to transfer data to and from aircraft and cruise ships. Europe is expected to witness a notable adoption of satellites for internet of things (IoT) solutions as enterprises across various verticals are looking to reach users in remote regions.

The expansion of edge computing beyond traditional terrestrial network connections is driving direct connections between data centers and satellite broadband ground stations to reduce latency and increase application speeds. As the need for big data and large language models for AI application processing increases, the demand for increased bandwidth will rise along with it.

GROWING BENEFITS AND GEOPOLITICAL CONFLICTS

So much started with the global positioning system. GPS was developed and launched by the U.S. military in the 1980s and became fully operational in 1993. When other countries, such as Russia, added their own satellite positioning systems, the global navigation satellite system (GNSS) was born. GNSS provides the global financial system event synchronization and timestamping for all financial transactions. It also allows for the exact synchronization of computer, telecommunications, and financial networks, and it plays a significant role in coordinating the elaborate choreography of orbiting satellites.

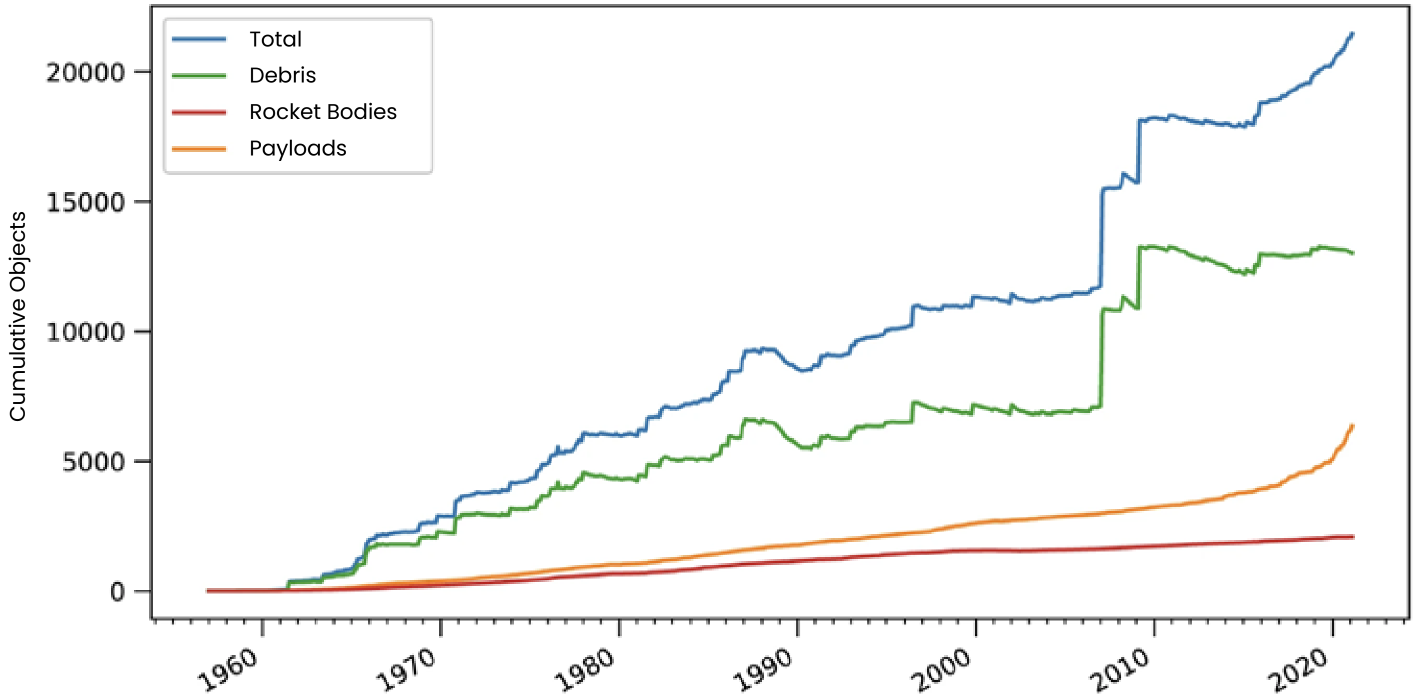
Satellites provide information about Earth's clouds, oceans, land, and air. They can also observe wildfires, volcanoes, and smoke and provide early warning to save lives. All this information helps scientists predict weather and climate. They can provide internet access to remote locations and rural areas that otherwise do not have broadband coverage. Elon Musk's Starlink, for example, has more than 4,000 small satellites in low Earth orbit for this purpose.

Though satellites have brought nations closer together, they have also exacerbated conflict between them. Space is not just a race to see who can be first. There have been findings of deposits of metal oxides in some of the large craters of the Moon, which is believed to contain reserves of silicon, titanium, aluminum, and rare earth metals. These metals are used in our critical daily technologies: the screens of smartphones, computers, and flat panel televisions; motors of computer drives; batteries of hybrid and electric cars; and new-generation light bulbs. Many countries have the incentive to go after them, especially those that don't want to rely on China, which currently holds a third of Earth's known reserves.

There's another form of conflict that is a regular irritant. As countries expanded their space-based networks, they gained insights into events around the globe. Satellite data opened up global transparency and gave spying and surveillance a big boost. The net result is that tensions continue to rise.

THE RISKS GROW AS WELL

The dangers are not limited to advanced espionage. The United States, China, and Russia, the three nations competing most fiercely for preeminence, seem to be jostling for advantages if and when weapons are used in space during a war. Each country has not only created anti-satellite (ASAT) weapons systems, they've each tested their systems on one of their own satellites. In the process, they created another danger: space debris.



SOURCE: SCIENTIFIC REPORTS

Figure 1 The Rise of Space Traffic from Tests, Collisions, and New Satellites

Cumulative on-orbit distribution functions (all orbits). Deorbited objects are not included. The 2007 and 2009 spikes are a Chinese anti-satellite test and the Iridium 33-Kosmos 2251 collision, respectively. The recent, rapid rise of the orange curve represents NewSpace.

Blowing up a satellite adds thousands of pieces of debris in orbit (see Figure 1 above), increasing the risk of collisions. And things are getting complicated. More than half of the 8,000 satellites revolving around Earth are inactive. International agreements such as NASA's (nonbinding) **Artemis Accords** are trying to address this. But space is getting ever more crowded. More than 80 countries now have a presence there. On top of that, the major companies mentioned earlier are planning to launch an additional 50,000 satellites in orbit. This means a lot more collision avoidance maneuvers will be needed to avert disaster.

There's another risk that companies would do well to consider. According to the U.S. Department of Defense, China represents one of the top threats to the U.S. presence in space—not because it has the capability of shooting down satellites, but because it can inflict damage through cyberattacks. A paper published in 2020 called **"China's Space and Counterspace Capabilities and Activities"** examines China's space program and the competitive threat it represents to its counterpart in the United States.

Not surprisingly, China's land-based offensive and deterrent strategies for cyberwarfare are similar to its goals in space: specifically, to reduce U.S. and allied military effectiveness in the event of a future military confrontation. The People's Liberation Army, the principal military force of the People's Republic of China, views cyberspace, space, and electronic warfare as inherently intertwined. Its goals include degrading and denying a potential enemy's use of space, and having the most advanced technological capabilities that will provide economic and societal benefits as well as more advanced surveillance capacity.

In response to this threat, President Donald Trump issued a memorandum on space policy in September 2020. **Policy Directive-5—Cybersecurity Principles for Space Systems** offers the government and the commercial space industry guidance on how to protect space assets and their supporting infrastructure from cyber threats, and how to ensure continuity of operations in the wake of attacks.

If businesses needed a reminder about the stakes, Russia delivered it in 2022. As Russian troops invaded Ukraine in February, Russian military hackers targeted the Viasat satellite system, deploying destructive "wiper" malware called AcidRain against Viasat terminals, permanently disabling them. Thousands of terminals for businesses, individuals, and the military were effectively destroyed in this way. About 5,800 Enercon wind turbines in Germany were also impacted and 30,000 internet connections across Europe were affected. The operation resulted in an immediate and significant loss of communication in the earliest days of the war.

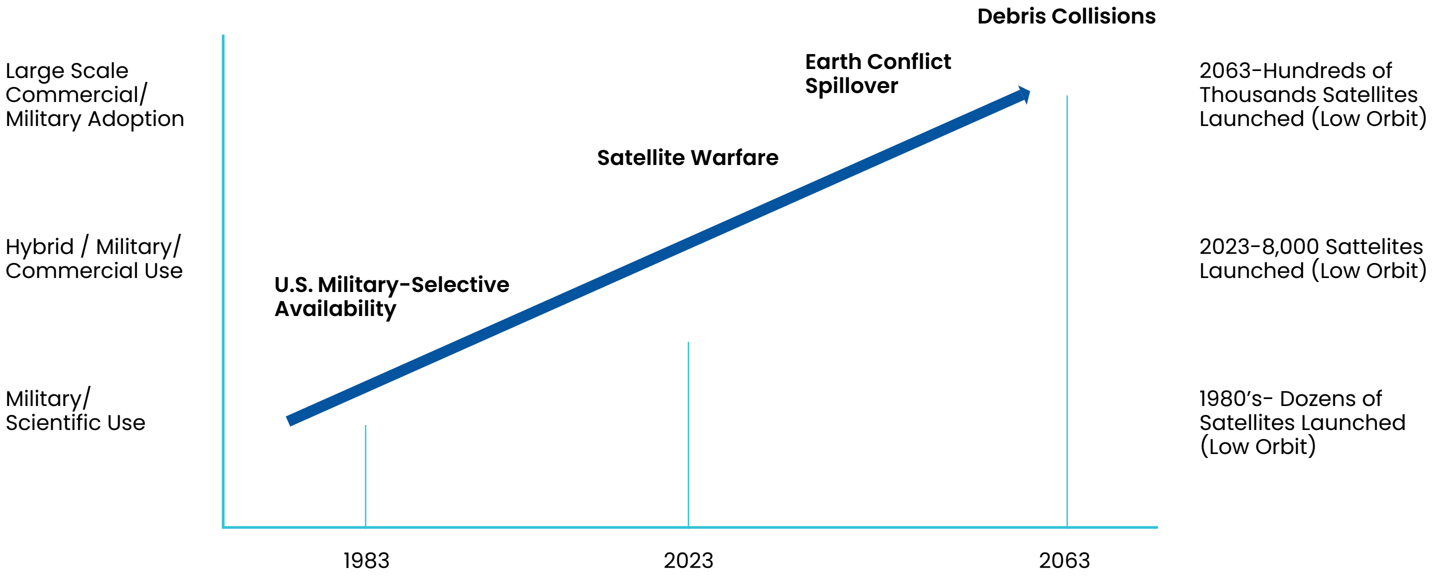

Debris Collisions
Earth Conflict Spillover
Satellite Warfare
U.S. Military-Selective Availability
Large Scale Commercial/ Military Adoption
Hybrid / Military/ Commercial Use
Military/ Scientific Use
2063-Hundreds of Thousands Satellites Launched (Low Orbit)
2023-8,000 Sattelites Launched (Low Orbit)
1980's- Dozens of Satellites Launched (Low Orbit)
1983
2023
2063

Figure 2 Author's Prediction of Increased Availability Risk from Satellite Adoption

RISK MITIGATION

To minimize satellite communication disruptions, businesses using cloud and telecommunication providers that use satellites as part of their delivery must require transparency from providers and associated product vendors, and ensure that they are operating with built-in and continuous protective, detective, and resilience mechanisms. Third-party questionnaires should be updated to assess the maturity of these providers against relevant frameworks, and check on their ability to recover control of space vehicles under attack.

Businesses should also require transparency as to how providers are managing the supply chain risks that affect the cybersecurity of space systems. This can be done by tracking manufactured products; requiring sourcing from trusted suppliers; identifying counterfeit, fraudulent, and malicious equipment; and assessing other available risk-mitigation measures.

Commercial intelligence firms can provide companies situational awareness on potential attacks to their sector. Or the companies themselves can make sure they are monitoring the threats associated with the growing importance of satellite services for critical infrastructure such as communications and banking. Satellite components on the ground and in orbit could increasingly be ideal targets for sleeper malware implants used as threat leverage between nations in conflict. If these threats are acted upon, significant impact to business communications and banking transactions will occur.

For firms that work directly in space and/or satellite operations, performing continuous risk assessments and alignment to the relevant frameworks should be required. Foundational controls such as preventing unauthorized logical access to critical space vehicles and links, and protecting core command, control, and telemetry receiver systems are table stakes. Frameworks such as the aforementioned Policy Directive-5 provide a good macro foundation for securing and monitoring core components. And NIST's **NISTIR 8270-Introduction to Cybersecurity for Commercial Satellite Operations** has more descriptive details on threats, risks, and controls that operators need to consider. Joining a collaborative group of private and public organizations such as the **Space-ISAC (Information Sharing and Analysis Center)** to share intelligence on threats within the space sector can be a proactive means of mitigating respective risks.

THE BOTTOM LINE

A few years ago, the prospect of a cyberattack against a satellite that would have an impact on the ground might have seemed farfetched. But Russia's attack on the Viasat satellite system last year not only wiped out data on terminals, it changed that very concept.

As our terrestrial and extraterrestrial internet backbones become fused, the threat surface will continue to grow. Commercial overexpansion, geopolitical tensions, and wars on earth will lead to increased risk that satellite infrastructure will be targeted. If we want to have a chance to defend it, that infrastructure will need to become part of our resilience architecture planning. And there isn't much time to waste.

"Actually, Senator - this is rocket science."

A LAWYER'S TREK TO LAW'S LAST FRONTIER

DAVID HECHLER

Jack Beard navigated a very unusual path to becoming a law school professor. It's not one that he recommends. Usually, academics don't wait long to start their careers, but Beard took a detour that lasted decades. And then, when he established himself, there was another surprise. His field of scholarship is outer space.

Jack Beard

If it all sounds a little "out there," the man himself is very much grounded. When he explains how it happened, it all makes perfect sense. And the results will soon be available for the world to see. Beard is the editor-in-chief of a much-anticipated book on the laws of space.

"The Woomera Manual on the International Law of Military Space Activities and Operations" will be published by Oxford University Press in spring 2024. The international and multidisciplinary cast of contributors has covered a lot of ground. A review volume is not yet available, but Beard said the book covers military space activities during peacetime, during times of tension and crisis, and during armed conflict. And in contrast to the way other publications of this type have analyzed sometimes amorphous rules in a new field—like cyberwar, for example—the authors sought to reach conclusions based on the words and actions of nation-states rather than the opinions of experts, Beard added. He believes this is the correct approach, since "it's states that ultimately make international law, not academics or other commentators."

TWO WORLDS BECKON

It didn't start with "Star Wars" or a childhood fascination with sci-fi. It began with the Reserve Officers' Training Corps. He needed an R.O.T.C. scholarship to pay for his college education, and he was also attracted to the military. His father and uncle had served in World War II. "So I had military in my background," he explained, "and I was also interested in military intelligence."

It was time to expand his world. He did not yet aim for the stars, but he left his hometown of Wichita, Kansas, and enrolled in Georgetown University's School of Foreign Service, where he majored in international relations. He was particularly inspired by his international law courses, he said during two long Zoom interviews. The classes sparked his interest in the law, which soon replaced military intelligence as his projected career.

> **The Pentagon seemed to celebrate technological innovations as their new invincible weapons that no one else would acquire.**

But that wasn't all he did as an undergrad. His second major was Russian, and his studies weren't limited to the language. He took in the history, government, and culture. And during his junior year, he spent a semester as an exchange student at Leningrad State University in what was then the Soviet Union. He called his time in Leningrad "life-changing."

He'd always been fascinated by Russians. "I grew up in the Cold War," Beard explained. "And they were, of course, the 'great adversary.'" There was a time, he recalled, when all you had to do if you wanted to have a conversation in Russian was pay a visit to the Pentagon. "That was where Russian speakers were."

Over time, both majors would stand him in good stead. But his first move after graduation proved a smart one. He secured an educational deferral from his obligation to the Army in order to get his J.D. from the University of Michigan Law School. This allowed him to meet his four-year obligation to the Army as a government lawyer, some of it in the **Judge Advocate General's** (JAG) Corps.

After he completed his four years of active duty, his government work did not end there. He worked for the Office of the Assistant Secretary of the Army. His interest in international law made him a good fit wherever he found himself. And over the years, his work took him around the country and then around the world. There were projects in China, Pakistan, Germany, Canada, Brazil, and, yes, even Russia.

Eventually Beard worked his way up to a job at the Office of the Secretary of Defense—associate deputy general counsel for international affairs in the Office of the General Counsel. He stayed from 1990 to 2004, often working closely with the secretary of defense. One of his biggest assignments was helping to dismantle weapons of mass destruction in the former Soviet Union under the **"Nunn-Lugar" assistance program**. He was one of the international lawyers who negotiated matters related to the removal of Ukraine's WMDs and dismantlement of its nuclear infrastructure. "I became the principal lawyer in the Defense Department for the negotiation of the implementing agreements and the overall umbrella agreement with the Russians, the Kazakhs, the Ukrainians, and the Belarusians," he said. It was a heady time. And a great spot for a Russian major.

BACK TO THE ACADEMY

It wasn't all whirlwind travel and international diplomacy. Beard's government work included long stints in Washington, where he earned an LL.M. (master of laws degree) in International and Comparative Law at Georgetown in 1989. And during those times he had an opportunity to try teaching as an adjunct lecturer in law. He started at his alma mater, Georgetown, then at George Washington, Johns Hopkins, American, and in 2002, he taught as a full-time visiting political science professor at the U.S. Naval Academy.

He liked it. He especially enjoyed the interaction with students. And he was apparently good at it. He won a teaching award at Georgetown and another at Johns Hopkins. Was it too late to change careers? "Most adjuncts don't go that way," he said. "You usually don't start an academic career more than a couple of years out of law school." In 2005, it had been 22 years since he'd graduated. That was the year that the UCLA School of Law hired him as a full-time professorial lecturer.

Returning to law school as a career move was comfortable in some ways. The teaching he knew he could handle. But there was another facet that posed a challenge. "It was the writing part of it," he said. It was the scholarship and duties of a full-time professor. "That I wasn't familiar with."

As he thought about the topics that interested him, inevitably, he returned to his years at DoD. He'd had a lot of time to think about weapons—old ones he'd been working to dismantle, and new ones that the Pentagon was deploying.

THE NEW FRONTIER

He'd been struck by the exuberance with which the Pentagon greeted new technology. They weren't just weapons, they were going to be "invincible weapons," he said. The attitude was: "This is going to be the weapon that makes competing weapons obsolete." That was the first great fallacy he witnessed again and again. The second, he said, was: "No one else will ever have it."

In the late 1990s, computers were going to completely remake the military. A few years later came the drones. And hovering above them: satellites. "Space is like the ultimate technology frontier," Beard continued. "It's all about high technology, and all these wonderful, enormous, expensive satellites parked out there 22,000 miles from Earth. Protected. Safe." The idea that anyone would be able to threaten them, Beard said, "wasn't part of the package."

> **"If none of you countries invoke the provisions that the Outer Space Treaty provides, it would appear that more and more bad behavior seems to be getting legitimized."**

That was how he came to write on this subject. "A lot of my writing has been about the unintended consequences of employing a lot of these technologies," he said. "Every new weapons technology does create new capabilities," he continued, "but at the same time creates new vulnerabilities." The onslaught of cyberattacks underscored the point. Not even satellites were safe. "Space is particularly vulnerable to cyber action, because of all the information being relayed back and forth to the satellites," Beard noted. "So it was writing in this area that was particularly attractive to me."

It didn't take long for this foray to bear fruit. In 2011, Jack Beard was hired as an assistant professor at the University of Nebraska College of Law. Three years earlier the school had launched an LL.M. degree program in **Space, Cyber, and Telecommunications Law**. With help from a NASA grant, the initiative expanded into a special concentration that J.D. students could elect as well.

By 2020, Beard was associate professor and co-director of the program. Two years later he was director. And somewhere along the line, the program had gained international recognition.

Through articles and lectures, Beard has been clear about what he's been trying to do. He'd like to see the law bring rigor to the way nations behave in space—and the way they respond to each other on the ground. Unlike cyberwar, which is another new area that provokes international disputes, there is a treaty that covers behavior in space. The Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies is its unwieldy name. It was negotiated and drafted under the auspices of the United Nations. It went into force in October 1967 and all major spacefaring nations are parties to it.

The **Outer Space Treaty**, as it's commonly called, is the foundational document designed to establish rules and keep the peace. No nations are allowed to place WMDs in orbit around Earth, or station them in space, or install them on celestial bodies. More generally, the law is designed to encourage cooperation and avoid or minimize conflicts and dangerous activities. But Beard sees flaws in the way it's used—or isn't. When nation-states complain that a satellite or space vehicle created a dangerous situation, Beard said, they rarely file an official complaint that characterizes the alleged offense as a violation of international law, perhaps fearing that the same allegation could later be aimed at them.

There are numerous examples of this phenomenon, Beard said. For example, in 2018, France complained about the maneuvering of a Russian satellite, saying it was **"unfriendly."** Two years later, the United States rebuked Russia for a separate incident, **calling Russia's action "irresponsible."** In each instance, a Russian satellite allegedly ventured too close to French and American satellites, but neither country alleged a violation of international law or even used the word "illegal." "Commentators may weigh in, but that's not going to achieve much progress in actually advancing the development or application of the Outer Space Treaty," Beard said. "As a lawyer," he continued, "I'm less interested in what experts say the law should be, and intensely more interested in what states that make international law are actually saying and doing."

THE PURPOSE OF THE BOOK

The Woomera Manual on the International Law
of Military Space Activities and Operations
Draft Manuscript (Substantive Parts)
3 March 2022
The Woomera Manual
on the International Law
of Military Space Operations
State Consultations
The Hague, June

"The Woomera Manual" manuscript that was distributed for the consultations at The Hague

"The Woomera Manual" aims to contribute to that effort. Four schools are collaborating on and funding work on the book: the University of Exeter in the United Kingdom, the Nebraska University College of Law, the University of Adelaide, and the University of New South Wales—Canberra, the last two in Australia. (Woomera itself is a village in South Australia from which the country launched its first satellite.)

Asked what he hopes will emerge from the project, Beard considered for a moment. "Well," he began, "we're looking for a reliable, practical guide, a collection focusing on state practice to help practitioners." He paused again. "You could argue to better extend the rule of law to space," he said, "but also to provide more predictability in space, to help prevent miscalculations and to promote a safer environment."

The hardest part was the research. It required examining the Outer Space Treaty in great detail to try to clarify or navigate ambiguities by ferreting out the negotiation history, which wasn't easy given the age of the agreement. And they needed to dig into statements by states, and policies inscribed in documents that were sometimes buried in old files. "A lot of academics are not interested in these things," Beard observed. They are more interested in propounding their own theories. “They want to be groundbreaking.” When there’s boring research: “Leave that to the law clerks.” But Beard and his Woomera project colleagues, who are employed primarily by universities, governments, and military services, hunkered down with their research assistants, he said.

What was often most important in this work was learning what the states decided to do and why. The work was bolstered by four workshops of the legal and technical experts, organized and funded by the universities. After the workshops concluded, the editorial board prepared the draft manuscript and submitted it to the Dutch Ministry of Foreign Affairs to circulate to states around the world, along with an invitation to review the draft and meet at The Hague to discuss it. The editorial board met with representatives from 24 nation-states, ranging from Australia to Zimbabwe, on June 1-3, 2022, to receive their comments and engage in conversation.

Beard remembered it well and seemed to relish the back and forth. They were operating under so-called Chatham House Rules, so no comments were attributed to specific individuals or nations. That made for lively discussion, and some of the “most robust” exchanges centered on Beard’s observation that states were not willing to call out bad behavior. “Look,” Beard recalled telling them, “if none of you countries invoke any of these provisions that the Outer Space Treaty provides, it would appear that more and more bad behavior seems to be getting legitimized. Any layman would look at that and say, ‘Well, if you’re not invoking it, the threshold must be really increasing.’”

Jack Beard, front row center, with fellow Woomera editorial board members Prof. Dale Stephens (on his left) and Prof. David Koplow (right), posing with representatives of states participating in the consultations at The Hague

“Oh the backlash!” Beard recalled with a smile. There was a flurry of rejoinders: “No, no, no, you don’t understand! There are many factors that may influence a diplomat to not publicly say those things. A diplomat may be protecting classified information, a diplomat may want to raise it in another context, or a diplomat may have other policy concerns.”

Finally: “We don’t want to set a precedent.” Beard smiled again. “Of course, by not responding, you’re setting a precedent. It’s a funny thing, the silence of states.” Beard expressed his gratitude for the contributions of all the representatives. The not-so-silent consultations resulted in a revised draft, as the editors incorporated the views of these states into the manuscript.

NORMS AND SOFT LAW

Why should this treaty be so important when it was drafted well before it was clear what the reality of spacefaring would be—and adopted just a decade after Russia launched that first **Sputnik** satellite in 1957? The short answer is that nothing has replaced it. It has been modestly enhanced by only four minor treaties, the last of which (the “Moon Treaty”) was adopted in 1979 and only 18 parties ratified it.

Which is not to say that no one has tried since. But the efforts have met with enough resistance that a new approach has been adopted. Beard described it in a 2017 **law review article:** “In place of legally binding agreements, a wide variety of non-binding 'soft law' instruments have been developed for space activities, variously described as 'non-binding principles, norms, standards or other statements of expected behavior in the form of recommendations, charters, terms of reference, guidelines, codes of conduct, etc.'" A prime example is what is now called the **International Code of Conduct for Outer Space Activities** (it was once known as the European Code).

If Beard sounded pained by the states' flaccid use of the Outer Space Treaty, those comments were pleasantries compared to what he had to say about negotiators' use of norms and soft law. "I hate the word *norm,*" he said. "Because *norm* is sometimes used by jurists to mean a legally binding obligation." But in his view, the word is often used by advocates and commentators in a confusing way to describe concepts or rules that are not law—any more than soft laws are laws. They're not articulating what a law is, but "what the law *should be*," he said. "For a lawyer, it's a treacherous ground where you mistake objectives, goals, and responsible behavior for law. When codes of conduct are signed by nations, they can become the worst kind of 'gentlemen's agreements'. They give the appearance of being legal and binding, when in fact they are neither," he added.

There is one soft model that is not a binding arrangement that Beard heartily endorses. In 2022, the United States declared a moratorium on destructive anti-satellite (ASAT) weapons tests, which leave in their wake dangerous space debris. This wasn't an agreement negotiated with anyone else. It was an announcement, Beard said. A commitment to responsible behavior. It was: "We're just not going to do it, and we invite others not to do it."

A funny thing happened. The initiative caught on. Other countries joined the United States in imposing a moratorium on such destructive tests. And a resolution sponsored by the U.S. and other states was brought to the U.N. General Assembly. The vote wasn't binding. A few countries didn't support it, including Russia and China. But it passed overwhelmingly and demonstrated strong support for the idea that such ASAT tests do not show due regard for the interests of other states. It may also clarify terms in the Outer Space Treaty and lay a foundation for future legal agreements. And to Beard, it was infinitely preferable to confusing multilateral soft law arrangements, which often pose as something they are not.

LOOKING AHEAD

Beard believes the book will make a meaningful contribution and will be well received when it comes out next year. The sessions in The Hague left him hopeful. "It was very clear that countries had studied the manuscript carefully and were thus able to contribute extensive oral and written comments," he said. Countries also had different views on some issues, and those opinions are reflected in the Manual. "There was great disagreement on some issues," he remembered, "for example, on what exactly the term 'free use of outer space' means in Article I of the treaty. And whether or not that includes exploitation of space resources." He paused. "You can make good arguments either way." We'll have to wait to see how it comes out.

The book may be months away, but the buzz has already begun. Eric Jensen, a law professor at Brigham Young University, who has known Beard since his days in the JAG Corps, and has established his own expertise in international law, particularly on cyberwar, had this to say: "Jack's work as the editor-in-chief of the "Woomera Manual" is indicative of his expertise in this area. I have no doubt that the Manual will quickly become THE resource on space law."

INTERVIEWS

AN INTERVIEW WITH TERRY INGOLDSBY
PRESIDENT AND OWNER, AMENAZA TECHNOLOGIES

COMPREHENSIVE THREAT ANALYSIS AND RISK ASSESSMENT SOLUTIONS

In a world where cyber threats are perpetually evolving, the ability to anticipate and strategize for potential attacks is becoming indispensable. The task of preemptive planning and detailed vulnerability analysis is complex, which is where trailblazing cybersecurity analyst Amenaza Technologies steps in, providing innovative tools to manage this challenging landscape. In a recent interview with **Amenaza**, we explored the concept of attack trees and the crucial role decision trees play in contemporary information security. We also discussed how their flagship product, *SecurITree®*, streamlines and enhances attack tree analysis, making identifying potential threats and their associated risk factors more manageable and insightful.

TAG Cyber: What are attack trees, and why do they apply to information security?

AMENAZA: Attack trees are a type of decision tree—a visual representation of an adversary's possible decisions in attacking a given target. Formally, they are a graphical, hierarchical tree structure comprised of Boolean AND, OR, and leaf nodes. Paths from the tree's bottom (leaf nodes) to the tree's top (root) node satisfy the tree's AND/OR logic and depict potential attack scenarios. Each path varies in resources required by adversaries, goals achieved, and damages victims suffer.

Amenaza understood the potential of attack tree analysis but realized it was impractical without sophisticated and purpose-built analytic software. The hierarchical nature of attack trees makes it easy and natural to divide the model into different subtrees. Experts in various areas can contribute their knowledge and assemble it into one comprehensive model.

Additionally, many components of a particular system in an organization will be similar to those used in other systems. Analysts can create component libraries and quickly and easily introduce them into new models, which substantially reduces the effort required to generate attack trees.

TAG Cyber: Why are attack trees needed in information security?

AMENAZA: With each passing year, organizations spend ever-increasing resources on cybersecurity tools. And yet, the number and magnitude of cyberattacks continue to increase.

Attack trees are a formal, objective method for assessing potential attacks against a system and predicting the adversary’s attack preference. Thorough analysis enables accurate attack frequency predictions, enabling defenders to prioritize attack scenarios based on rational decision-making.

While conventional tools (i.e., firewalls, intrusion detection systems, VPNs, and encryption) are necessary, a scattergun approach to deployment is neither practical nor efficient. To prevent or minimize attacks, viewing our systems from the perspective of our adversaries is crucial.

Attack trees are a formal, objective method for assessing potential attacks against a system and predicting the adversary’s attack preference. Thorough analysis enables accurate predictions of the frequency of each type of attack, enabling defenders to prioritize attack scenarios based on rational decision-making.

After identifying the highest-risk scenarios, the model can incorporate the best control choices (before implementation) and then repeat the analysis to gauge their effectiveness.

TAG Cyber: How does Amenaza’s SecurITree® software leverage attack tree analysis?

AMENAZA: A national intelligence agency developed attack trees in the 1990s, but limited awareness and understanding among practitioners have hindered their widespread adoption. Amenaza provides a comprehensive three-day onsite training course on attack tree theory and practice to address this issue.

Some individuals attempt to create attack trees using manual methods or generic drawing tools like Visio or CorelDraw, only to quickly realize their unsuitability. Consequently, many of these individuals become enthusiastic supporters of Amenaza’s SecurITree software, which we specifically designed to conduct attack tree analysis. The software also significantly reduces the effort required to construct and modify attack trees.

Over twenty years of research and development went into creating the SecurITree threat modeling software tool. SecurITree makes it easy to develop attack trees and provides powerful analytic functions to extract understanding from the models. Analyzing attack trees presents a challenge due to the vast number of combinatoric paths they can contain. Typical trees representing IT systems in an organization can have hundreds of thousands of potential attack paths.

One real-world example developed by Amenaza for an existing control system involved billions of scenarios! Without practical tools, the sheer volume of information can be overwhelming.

TAG Cyber: Can you provide insights into how your SecurITree tool helps organizations assess supply chain risks?

AMENAZA: Secur*IT*ree's attack tree models are remarkable due to their holistic nature, encompassing various hostile threats against a system, including cyber, physical, and transitive threats from other organizations.

Unlike conventional tools, SecurITree models recognize the significance of considering threats from interfaces with business partners and suppliers. These threat vectors often pose more significant risks than direct attacks on the organization's systems.

Ideally, the expandable attack model can incorporate the potential compromise of a supplier's system, thereby creating an additional attack vector. However, a common challenge is the lack of knowledge and means to verify a business partner's security practices. This knowledge gap becomes apparent when creating an attack tree, prompting the organization to seek information for accurate threat modeling. In cases where obtaining such information is not feasible, the attack tree model suggests an alternative approach.

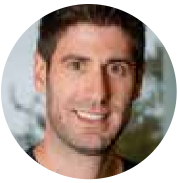
When information about a portion of the system, such as the supply chain or other technologies, is unattainable, it is prudent to model the unknown as highly deficient and establish compensating controls to mitigate the risk. This proactive strategy may result in implementing some unnecessary controls at worst, but at best, it can prevent a catastrophic event!

TAG Cyber: Can you briefly outline the benefits of the new machine learning feature introduced in SecurITree v5.4?

AMENAZA: With each new release, Amenaza strives to enhance automation for analysts. Prior to v5.4, analysts had to manually inspect individual attack scenarios and identify similarities in their characteristics.

For example, certain scenarios may have required a significant financial investment from the attacker while demanding low technical expertise and being difficult for the defender to detect. Recognizing these similarities and grouping them appropriately required considerable effort from the analyst.

However, SecurITree v5.4 introduced a machine-learning feature that automates this process. Within seconds, the software can automatically sort and group similar scenarios based on the criteria defined by the analyst, which streamlines the workflow significantly. Moreover, SecurITree v5.5 will further enhance this capability in the upcoming release, offering even more advanced functionality.



AN INTERVIEW WITH DAN AMIGA CO-FOUNDER AND CTO, ISLAND.IO

THE SECURE AND FLUID ENTERPRISE BROWSER

As our digital ecosystem becomes more interconnected, innovative solutions like Island.io's Enterprise Browser are gaining prominence. Marrying enterprise necessities with core cybersecurity tenets, Island. io delivers a product that propels businesses' digital transformation journey. Their unique approach is lauded by global corporations, bolstering cybersecurity measures while simultaneously enhancing productivity and streamlining business operations. In a fascinating recent conversation with Island, we dug deeper into the evolution of the Enterprise Browser market, delving into emerging trends and their implications for businesses. The discussion also touched on how **Island.io** integrates innovative technologies, such as generative AI, into a secure framework, allowing companies to reap the benefits without sacrificing security.

Tag Cyber: It's been almost a year since our interview with Mike Fey. How has the Enterprise Browser market evolved since then?

ISLAND: Mike Fey, Island Co-Founder and CEO, and I collaborated at Symantec after the acquisition of Fireglass, my previous company. At Fireglass, we invented remote browser isolation (RBI), which inspired me to bring a true Enterprise Browser to the market. Advisors, investors, and customers responded positively, but we knew the challenges of launching a new category. After all, none of our potential customers had a budget line item for an Enterprise Browser.

Three years in, and over a year since we emerged from stealth, our customers—primarily large enterprises with experience in every possible security and IT product category—remain incredibly positive. They all have an existing browser footprint, but they respond with enthusiasm when we show them what Island can do for cybersecurity, their digital transformation initiatives, and employee productivity. We're now deploying Island in some of the largest companies in the world, with six-figure employee counts spanning every geographic region. We took a unique approach with Island, where we hired and staffed our teams for scale and enterprise maturity from the very beginning. We intentionally deviated from the standard startup playbook, and now that we're running at the scale and speed that we knew was coming, it's absolutely paying off.

When we created the Enterprise Browser, we actively designed, built, and continue to support it as a dedicated enterprise application. Our customers can manage the browser, control application access, enforce security policies, and streamline productivity workflows.

Tag Cyber: What has surprised you about the Enterprise Browser market?

ISLAND: Two things. First, when we started pitching the Enterprise Browser, we focused on cybersecurity use cases, which remain a key driver. However, what's surprising is how often we work directly with executives other than the CISO, like the CIO, CHRO, SVP of Infrastructure, or an EVP responsible for the business. Our customers use the Enterprise Browser to drive business transformation and don't consider it a typical cybersecurity product. We anticipated this shift but were pleasantly surprised at how quickly it happened. Helping our customers deliver better products and services for their customers is incredibly motivating for all of us at Island.

Secondly, the growth rate of this category is remarkable. We initiated our efforts in 2020 and unveiled the Enterprise Browser in early 2022. Since we launched Island, other companies have entered the field, fostering a robust competitive environment and confirming the legitimacy of the category. The analyst community, including TAG Cyber, is also optimistic. It's safe to say that the Enterprise Browser category is here, and it's growing faster than our initial targets.

Tag Cyber: What macro trends are you seeing in your customer base?

ISLAND: A few years ago, people embraced the big trend of transitioning from in-office to remote work, forcing every organization to rethink how they deliver core IT and cybersecurity services without control over the daily network employees use. Now we're seeing a shift towards returning to the office, with some research showing that in-person work still has a significant advantage, especially for collaboration and building an organization's essential social networking layer.

At the same time, customers are growing their usage of business process outsourcers (BPOs) and contractors for the functions where that makes sense. These deployments are usually challenging for IT and Security teams since contractors typically use endpoints managed by the BPO rather than the customer. Island is in a unique spot where we can support all user groups equally to drive overall business efficiency and productivity.

Tag Cyber: What drives this rapid adoption of the Enterprise Browser category?

ISLAND: Over the past 20 years, we migrated enterprise applications from desktops and private data centers to the cloud and browser. However, despite becoming a crucial tool for enterprise work, enterprise needs were not the focus of original browser design. It's important to note that I don't mean to criticize major browsers. Chrome, Edge, and Safari are excellent products billions of people use daily. Indeed, the Island Enterprise Browser utilizes the same Chromium engine found in Chrome and Edge, among others. However, these browsers prioritize consumer design rather than enterprise requirements.

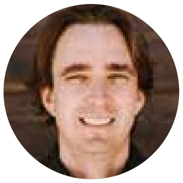
When we created the Enterprise Browser, we actively designed, built, and continue to support it as a dedicated enterprise application. Our customers can manage the browser, control application access, enforce security policies, and streamline productivity workflows using Island. We identified this missing piece during the transition to SaaS, and it explains the high demand we are experiencing.

Another factor driving adoption is the growing complexity of data sovereignty and privacy regulations. As we support increased global deployments, our customers seek ways to manage this evolving landscape. It's overly complex to send traffic to different global presence points, then break open SSL traffic to inspect contents across a distributed organization in different jurisdictions. This process makes Island's model of pushing intelligence and policy enforcement out to the browser appealing. Organizations can apply the right set of policies based on where an employee lives, and they can collect and store analytics data by region to respect data sovereignty.

Tag Cyber: We're hearing customers ask about introducing generative AI in the workplace. Is this something that Island is working on?

ISLAND: Absolutely, yes. Legacy security architectures shouldn't force organizations to miss out on the massive potential for generative AI. Balancing innovation and security is essential. To encourage this, we launched the Island AI Assistant in January 2023 to give customers immediate access to a large language model with a familiar chat-based interaction. ChatGPT caught everyone's attention with the potential for generative AI, and we're offering an enterprise-grade AI assistant natively integrated into the Island browser.

Second, many customers tell us there's a reasonable concern about sharing sensitive or proprietary data with AI tools. Using Island, organizations can implement policies to protect sensitive data and audit usage. This approach balances data security and innovation, ensuring that organizations can benefit from AI without risking their data. This is just one use case, but it's a perfect example of why organizations adopt the Enterprise Browser.



AN INTERVIEW WITH RUSSELL SPITLER
CEO AND CO-FOUNDER, NUDGE SECURITY

SAAS SECURITY AND GOVERNANCE FOR DISTRIBUTED ORGANIZATIONS

Navigating the vast and intricate SaaS attack surface can often be a daunting task for organizations. However, Nudge Security has risen to the challenge by developing a pioneering solution that comprehensively defines and manages this multifaceted threat landscape. Harnessing the power of AI and inventive methodologies, their platform meticulously uncovers all SaaS assets, enriches this inventory to facilitate a better understanding, and tirelessly monitors potential attack vectors. In our recent in-depth conversation with Nudge Security, we gained a deeper appreciation of their patented approach to SaaS discovery, their emphasis on human-centric security design, and their proactive strategies for constant monitoring. We also delved into how they're aiding organizations to bolster their SaaS supply chains.

TAG Cyber: How does Nudge Security enable organizations to discover their complete SaaS attack surface quickly and easily?

NUDGE SECURITY: First and foremost, we help *define* the SaaS attack surface, a relatively new and amorphous attack surface for most organizations. As we see it, the SaaS attack surface spans all SaaS accounts and identities used in an organization, managed and unmanaged, SaaS-to-SaaS integrations, APIs, and even the SaaS supply chain. It's a large surface area, but these assets represent the points where an attacker may access corporate data stored in SaaS environments.

Nudge Security discovers all these SaaS assets regardless of location, network, or device. We then enrich and organize this inventory to help security teams monitor publicly exposed SaaS apps, high-value SaaS targets, data breaches within their SaaS supply chain, high-risk OAuth grants, and more. Because this attack surface shifts constantly, it is crucial to discover SaaS assets historically and continuously, a process that Nudge Security automates.

TAG Cyber: What are the key advantages of Nudge Security's SaaS identity governance and administration solution?

NUDGE SECURITY: One key advantage of Nudge Security is our patented approach to SaaS discovery, which offers a fast, cost-effective way to view an organization's entire cloud and SaaS estate—without browser plugins, agents, network proxies, or changes to employee behavior.

One key advantage of Nudge Security is our patented approach to SaaS discovery, which offers a fast, cost-effective way to view an organization's cloud and SaaS estate without browser plugins, agents, network proxies, or changes to employee behavior.

Instead, our solution uses read-only API access to Microsoft 365 or Google Workspace to search for and analyze machine-generated email messages from SaaS providers (think no-reply@box.com).

The advantages of this discovery method include long-term email retention to analyze historical and current SaaS footprints, machine learning algorithms to detect consistent email patterns, and enabling the discovery of new, unknown SaaS apps without needing an extensive SaaS database. Furthermore, it offers unparalleled SaaS context, including insights into SaaS-to-SaaS OAuth integrations, authentication methods, and even the spread of a SaaS app within an organization.

Another crucial advantage of Nudge Security is our human-centered security design. For the past 20 years, perimeter-based security technologies like firewalls, proxies, and CASBs have tried to block the "bad internet," including unsanctioned cloud and SaaS. And yet, we have more of it than ever before. Clearly, something isn't working.

Even with full visibility of unsanctioned cloud and SaaS use, we can no longer realistically re-centralize the responsibility for administering, governing, and securing SaaS and cloud technologies within IT. Most organizations deal with thousands of different apps, each requiring an understanding of configuration, interconnection, and access levels.

The only way to address this problem at scale is by enlisting the same people creating it—employees. Our approach is to work *with* employees by automating employee engagement and collaboration with timely, helpful "security nudges," enabling IT to distribute administrative tasks to SaaS business owners while maintaining centralized oversight. Additionally, compared to traditional "lock and block" security controls, nudging is a smarter way to drive quick and meaningful security behavior changes.

TAG Cyber: How does Nudge Security proactively monitor MFA and SSO enrollment?

NUDGE SECURITY: A fundamental challenge of SaaS identity governance is knowing what SaaS identities exist and which meet the organization's identity security policies and goals—information usually managed with spreadsheets and considerable effort. Nudge Security makes this information available on day one, with an inventory of all SaaS accounts and identities and the identity providers and authentication methods used for each account (e.g., SSO or username and password).

With automated security nudges, IAM leaders can programmatically engage employees in identifying best practices, enabling MFA on new SaaS accounts, or initiating an SSO onboarding process. By connecting Nudge Security to Okta, our customers can further streamline and automate SaaS identity governance, including one-click de-provisioning across Okta-managed and unmanaged SaaS accounts.

TAG Cyber: In what ways does Nudge Security's built-in SaaS classification streamline SaaS vendor security assessments and compliance audits?

NUDGE SECURITY: A unique feature of Nudge Security is our ability to automatically classify and describe each SaaS application we discover. For context, we've discovered more than 32,000 unique SaaS applications in our customers' environments. Alone, the ability to search and filter by category allows our customers to immediately answer questions like, "What AI tools are people experimenting with?" "How many file-sharing services do we use?" and "Where are opportunities to consolidate SaaS to help reduce sprawl, costs, and risk?"

In addition to SaaS classification, Nudge Security gathers copious information about each discovered SaaS provider's security, risk, and compliance program. This enables governance teams to perform just-in-time vendor security assessments as SaaS applications are introduced rather than holding up the business for due diligence, encouraging employees to circumvent the IT procurement process altogether. Our customers tell us they save hours on third-party risk management with Nudge Security.

TAG Cyber: How does Nudge Security's automatic mapping of the SaaS supply chain protect against supply chain attacks?

NUDGE SECURITY: By our estimate, organizations experience an average of six data breaches in their SaaS supply chains every year. Emerging threat actors like the LAPSUS$ group exploit the complexity and lack of oversight of organizations' sprawling SaaS estates, moving laterally through the SaaS supply chain to high-value targets like Okta and CircleCI.

Nudge Security combats this trend by populating customized SaaS supply chain insights, including supply chain breach notifications. This gives our customers a unique vantage point to identify risky third- and fourth-party security incidents. Combined with the SaaS identity data Nudge Security discovers, our customers can act quickly and proactively to engage potentially affected SaaS accounts and employees rather than having to broadcast notifications organization-wide.

AN INTERVIEW WITH OREN HAREL
CO-FOUNDER AND CEO, PLAINID

SIMPLIFIED AUTHORIZATION MANAGEMENT AND ENHANCED DATA SECURITY

In this digital age, securing and controlling access to data is a critical concern for all organizations. At the forefront of this challenge, PlainID leverages Policy-Based Access Control to offer a holistic framework for enterprise-wide access control. By shifting away from traditional Role-Based Access Control, their Authorization platform transforms the ordinarily fragmented policy management process, enabling centralized oversight within a distributed environment. Our recent discussion with PlainID delved deeper into their groundbreaking platform. We explored how it aligns with various compliance requirements like GDPR and HIPAA and provides more fine-grained control over data access, strengthening security and privacy while enhancing user experience. The platform is a game changer, offering a seamless and secure way to manage authorization while promoting business growth and technological integration.

TAG Cyber: What advantages does PlainID's Authorization platform offer in simplifying access control policies?

PLAIN-ID: Authorization is essential to any modern enterprise's identity and access management (IAM) solution. Acting as an organizational gatekeeper, the process determines which employees can access which company data and, crucially, where the boundaries lie.
The PlainId Authorization Platform builds upon Policy-based Access Control (PBAC), which promotes simplicity and business agility, empowering modern organizations to establish a standardized enterprise access control framework.

Our platform's heart is centralized policy management within a distributed environment, which allows businesses to define and manage access control policies in one place. This centralization eliminates the disparate policy management spread across multiple systems (or applications), simplifying the overall policy management process. Furthermore, PlainID's platform allows enforcement deployment at various points within a distributed architecture.

These enforcement points are responsible for executing the access control decisions based on the policies defined in the centralized policy management platform. By distributing enforcement, enterprises protect their digital assets with an approach that works natively with the different technologies in the stack.

PlainID's solution allows organizations full visibility and control of access policies across their technologies.

Our platform's heart is centralized policy management within a distributed environment, which allows businesses to define and manage access control policies in one place. This centralization eliminates the disparate policy management spread across multiple systems (or applications), simplifying the policy management process.

This eliminates the need for individual applications or services to handle authorization logic and promotes a unified and standardized approach to enterprise access control.

Ultimately, with PlainID, organizations can have a unified management dashboard for authorization policies across their complex computing environment, including data, APIs, microservices, and applications.

TAG Cyber: How does PlainID's "Policy-Based Access Control" differ from traditional RBAC?

PLAIN-ID: Organizations use a variety of approaches across the security ecosystem to deliver effective authorization, including Role-Based Access Control (RBAC), which permits or denies access to resources based solely on a user's job title and function. Although RBAC serves as the current industry standard access control model, it exhibits limitations with its coarse-grained approach that defines access solely based on job titles and their associated functions.

In addition to RBAC, Attribute-based access control (ABAC) is another widely adopted option. ABAC provides a fine-grained access control solution, granting access rights to users based on policies that evaluate assigned attributes. However, this approach presents its own set of challenges. For example, writing policies in plain language is impossible, which necessitates using eXtensible access control markup language (XACML).

This old standard can be extremely complicated to understand and maintain. Coding complex policies is overly burdensome and limits the agility of the business. RBAC, while historically useful, has proven limitations with scalability and flexibility. ABAC attempted to solve this but brought additional administrative overhead. Both methods lack the identity context needed to establish trust at every stage of digital interaction.

Policy-Based Access Control (PBAC) fills this gap with its advanced, agile, policy-driven approach, dynamically responding to changes and allowing the writing of policies in natural language.

TAG Cyber: How does PlainID ensure compliance with GDPR, HIPAA, and other regulations?

PLAIN-ID: We help organizations ensure compliance by providing robust features and capabilities that align with regulatory requirements and industry standards.

Data is one of an organization's most valuable assets, and authorization lies at the heart of effective data management—ensuring that the right people have appropriate access control. Risk-based real-time authorization policies allow firms to ensure they meet data privacy and compliance regulations proactively.

By leveraging PlainID's key features and capabilities, we assist organizations in achieving and maintaining compliance with various regulatory frameworks, such as GDPR, HIPAA, PCI DSS, or industry-specific guidelines. Our products enable organizations to implement strong access controls, maintain audit trails, and enforce policies that align with compliance requirements.

TAG Cyber: In what ways does PlainID's platform integrate with existing IAM solutions?

PLAIN-ID: By leveraging Identity Providers, PlainID incorporates an identity-aware context and applies dynamic conditions to bolster security at every layer. This approach allows for real-time assessment of continuously changing attributes throughout an identity's journey, enabling informed authorization decisions that determine the safety or riskiness of data access requests.

PlainID's platform offers flexible integration options with existing IAM solutions, allowing organizations to leverage their investments in IAM infrastructure while enhancing access control capabilities with PlainID's policy-based approach. The integration supports seamless identity integration, single sign-on, user lifecycle management, attribute-based access control, and auditing/reporting, building a comprehensive and cohesive authorization framework. This makes enforcement in a distributed environment easier and more achievable than ever before.

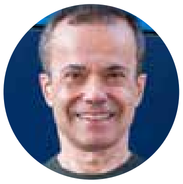
TAG Cyber: Can you outline the key features of PlainID's "authorization as a service" model?

PLAIN-ID: Our next-gen authorization platform includes flexible deployment options like cloud, hybrid, or on-premises models—without compromising performance or functionality.

With PlainID's pre-built, third-party "authorizers," we can provide access control for vital authorization enforcement patterns, including API Gateways, Microservices, and Data Lakes. Authorizers are the enablers of those controls within the organization's technology stack. The growing list of authorizers includes Istio Authorizer, Apigee Authorizer, AWS API GW Authorizer, OKTA Authorizer, Data SDK Authorizer, Google Bigquery Authorizer, and Snowflake Authorizer.

Additionally, PlainID authorizers extend access control and enterprise authorization policy management across numerous technologies in the computing infrastructure. This makes enforcement in a distributed environment a significantly more straightforward process.

With the paradigm shift to identity-first security, authorization is the new frontier in the dynamic cybersecurity landscape and is crucial for defending digital assets.



AN INTERVIEW WITH MEHRAN FARIMANI, CO-FOUNDER AND CEO, RAPIDFORT

ADVANCED SOFTWARE SECURITY AND FORTIFICATION

As digital threats become increasingly pervasive, RapidFort has emerged as a game-changer with its pioneering Software Attack Surface Management (SASM) platform, automating the creation of secure containers and drastically curtailing potential vulnerabilities. During our recent discussion with RapidFort, we explored their platform's integration with CI/CD pipelines and how its profound package analysis contributes to a robust and comprehensive vulnerability scanning and mitigation solution. We also learned more about how RapidFort efficiently mitigates risk and noise within vulnerability reports by identifying unused software components within modern cloud workloads—allowing security teams to swiftly identify and address potential threats.

TAG Cyber: How does RapidFort's Software Attack Surface Management (SASM) platform automate building secure containers?

RAPIDFORT: The construction of modern applications results in most modern cloud workloads containing vast amounts of unused software components. We recently conducted an extensive study of 1,578 unique container images and discovered that the applications did not use 68% of packages in the images. These unused packages contributed to the application's overall size and 73% of the reported vulnerabilities.

Unused software components present two classes of problems for security teams: They create a lot of noise in vulnerability reports, making it difficult to focus on vulnerabilities in the execution path and creating unnecessary patching toil. Secondly, they expose organizations to needless risk where attackers use existing software in the workloads to "live off the land" and gain deeper access to infrastructure and sensitive data.

RapidFort's platform pinpoints unused application components and their associated vulnerabilities in various parts of the software development lifecycle (SDLC) and provides security and development teams the tools to mitigate these vulnerabilities automatically.

Security teams use our run-time tools to quickly identify, prioritize, and remediate risks without burdening development teams. Using our detailed reports, security teams have the data needed to make informed decisions and ensure development teams are securing and hardening software upstream via build-time tools.

RapidFort's platform pinpoints unused application components and their associated vulnerabilities in various parts of the software development lifecycle (SDLC) and provides security and development teams the tools to mitigate these vulnerabilities automatically.

Our tools can eliminate most of the dev's patch backlog and address security issues upstream, creating a domino effect of time, effort, and cost savings. Our platform arms security and development teams with a turnkey suite of specialized tools and reporting capabilities—resulting in an advanced cybersecurity strategy.

TAG Cyber: Can you outline how RapidFort's vulnerability scanning solution seamlessly integrates with CI/CD pipelines?

RAPIDFORT: There are two parts to our solution: run-time and build-time tools. Our run-time tools don't require any CI/CD integration. Instead, they're easily deployed in Kubernetes environments within minutes, incurring less than 1% compute overhead and requiring no special privileges or permissions.

Our build-time tools easily integrate into CI/CD processes by using a few command line tools to scan, profile, and harden the container images as part of the build/release cycle.

TAG Cyber: What insights does RapidFort's scanner provide through deep package analysis?

RAPIDFORT: Our scans show exactly what's running in an execution path and if a package is required to operate an application. While a "static" scan of a container image produces a software bill of materials (SBOM) and their associated known vulnerabilities, RapidFort's run-time analysis identifies the subset of those packages the application actively uses during its operation. RapidFort refers to that subset as a "real bill of materials" or an RBOM. Uniquely, this allows us to provide insight and context for security and development teams to optimize and secure their applications.

TAG Cyber: How does RapidFort ensure accuracy in vulnerability identification?

RAPIDFORT: To accurately identify the known vulnerabilities in an application, you must first identify the list of packages used to build the application. Then, you have to query the relevant databases and advisories for vulnerability reports against those packages.

RapidFort provides comprehensive support for parsing package metadata for all popular Linux distributions and application frameworks, and it queries the widely used sources for known vulnerabilities, such as the NVD, Linux distribution advisories, and other security advisories like GitHub and GitLab.

TAG Cyber: Could you elaborate on how your Rapid Risk Score and optimization tool help prioritize vulnerability remediation?

RAPIDFORT: With the exception of a few kinds, like nation-state attacks, almost all other cybercrime is very opportunistic. Attackers target low-hanging fruit to find their path into infrastructure, and if the costs are too high or the task too difficult, they move on to weaker targets. As such, when a vulnerability has a known recipe for possible exploitation, it becomes much easier for attackers to benefit. The risk associated with a known vulnerability escalates if there's a published proof-of-concept (POC) detailing its exploitation. Such information empowers potential threat actors by providing them with the know-how to use the exploit, thereby heightening the likelihood of an attack.

RapidFort scours various data sources, like NVD, Exploit-DB, and others, to identify if a known vulnerability has a published POC. If our platform finds them, it provides references to the findings and classifies these vulnerabilities as having a greater risk. If it doesn't find a published POC, it uses a machine-learned model to estimate the likelihood that the vulnerability will have a POC published within the next 30 days.

Security teams can use this information in addition to severity data to prioritize their remediation efforts, saving time and effort. For instance, the system will flag a low or medium-severity vulnerability with a published POC for investigation in the next patching cycle. On the other hand, it will flag and prompt immediate investigation of a high-severity vulnerability within the current patching cycle.

"Ladies and gentlemen, our captain would like to know if there is a ransomware expert on board."

AN INTERVIEW WITH ALEX HARRINGTON
CO-FOUNDER AND CEO, SECURECO

STEALTH-BASED NETWORK SECURITY AND DATA PROTECTION

In the face of rising cyber threats, traditional network security measures often fall short. SecureCo, however, is redefining the rules of the game with its innovative security solutions. Using stealth, obfuscation, and encryption techniques, SecureCo protects internet connections by reducing the attack surface and emphasizing proactive security measures. This innovative approach has positioned them at the cutting edge of the cybersecurity landscape. Our recent discussion with SecureCo explored network obfuscation and how it bolsters defenses against diverse cyber threats. Furthermore, we discussed the implications of revolutionary technologies like generative AI and quantum computing on their approach to security. SecureCo's forward-thinking solutions provide robust protection in the present and lay the groundwork for navigating the future complexities of cybersecurity.

TAG Cyber: Why is SecureCo technology different from typical network security?

SECURECO: The principal difference is that we introduce stealth and obfuscation elements alongside traditional encryption security to secure internet connections. Obfuscation makes the endpoints and data-in-transit much harder to discover, target, and exploit, reducing an organization's overall attack surface. A smaller attack surface reduces vulnerability, risk, and administrative overhead, ultimately reducing financial losses from fraud, breaches, or downtime.

A second key difference is an emphasis on protecting internet data transit. As threat actors become more sophisticated, and the untrusted internet becomes increasingly dangerous, simple encryption is not enough to protect critical data against common exploits. SecureCo protects against monitoring and packet analysis threats —key elements of hacker reconnaissance—and exploits, such as man-in-the-middle, which can result in obstruction, eavesdropping, or data theft.

One more notable distinction is the emphasis on preemptive security, which is currently not in vogue. In an era of budget constraints, the return on investment (ROI) for reactive security, like detect and respond systems, is easily measured by tallying the number of flies caught in a fly trap. However, reactive solutions don't deter attackers or prevent the breach in the first place.

TAG Cyber: What cyber threats does network obfuscation protect against?

SECURECO: Network obfuscation includes a variety of tactics designed to make network assets and data less exposed to attacker discovery, Generative AI and quantum computing are seismic technology shifts that will yield unexpected results. There are some pretty clear near-term consequences to these emerging technologies, and SecureCo's technology can help companies navigate these changes.

reconnaissance, and exploitation. It works with traditional security approaches in a defense-in-depth strategy to reduce cyber risk and prevent costly incidents.

Attack surface reduction is one notable form of protection. SecureCo's method of establishing connections permits networks to operate in a connected state with no ingress ports open.

Eliminating the open ports is vital since they are a key element that attackers use to identify vulnerabilities, potentially providing an accessible exploitation pathway. Fewer open ports and reduced attack surface lower network security incidents (including initial access breaches) and avert disaster scenarios.

Network obfuscation also protects internet data transit. Nowadays, most data communications are encrypted, but this does not provide complete protection. Adversaries can still observe encrypted data flows, perform reconnaissance, and potentially monitor, intercept, redirect, or obstruct data. Obfuscation can disguise data flows and remove attribution, routing evasively to make targeting and exploitation much harder.

TAG Cyber: What are the most common enterprise use cases for network obfuscation? How widely adopted is it?

SECURECO: Military and intelligence applications have used network obfuscation for at least a decade, but only in the last few years has it been widely available for commercial adoption. Obfuscation can enhance security in common enterprise use cases, including remote access, campus networking, and cloud connectivity. SecureCo solutions can replace VPNs, supplement SASE elements (such as SD-WAN), or provide a more flexible and lower-cost alternative to dedicated telco connections. However, the use case receiving the most enterprise interest and adoption is API security, particularly for public APIs used by mobile apps.

Mobile app APIs are publicly accessible, and attackers attempt to exploit them by mimicking the API calls from the app. Brute force and credential stuffing attacks are common methods of hijacking customer accounts, resulting in financial losses, regulatory penalties, and customer dissatisfaction. Current mitigation tools like WAFs and bot detection software have not fully met these challenges. SecureCo's network obfuscation solution allows enterprises to establish a private connection between their consumer apps and the associated APIs, eliminating bot attacks from side channels.

TAG Cyber: What benefits does SecureCo's network obfuscation have relative to conventional security approaches?

SECURECO: Network obfuscation is part of a defense-in-depth security strategy. SecureCo solutions complement almost all traditional security methods, and we recommend a layered approach. When going into battle, you still want your armor and shield, but wouldn't you also want an invisibility cloak if it were available? Network obfuscation provides the closest thing you can get to internet invisibility.

Some distinctive aspects of our solutions are beneficial to the customer. First, SecureCo hosts its data delivery platform as a managed service. Our approach to attack surface reduction and data security is mainly set-and-forget. Many cybersecurity solutions are powerful tools, but organizations need a team to manage them, which inflates the cost of ownership and lowers ROI. Not so for SecureCo solutions.

Another benefit to customers is the reduction of network security incidents accompanying the deployment of our network obfuscation solution. This approach minimizes cyber risk and averts expensive breaches while significantly reducing the overhead of logging, investigating, and mitigating the overwhelming influx of incidents.

TAG Cyber: How will emerging technologies like generative AI and quantum computing drive the adoption of obfuscation security like that provided by SecureCo?

SECURECO: Generative AI and quantum computing are seismic technology shifts that will yield unexpected results. There are some pretty clear near-term consequences to these emerging technologies, and SecureCo's technology can help companies navigate these changes. Generative AI can do many things, including creating incredibly realistic human simulacra. In the same way AI can create deepfake videos or emulate a pop star's singing voice, it can also replicate human behavior and fool software designed to prevent bot attacks. This capability will make it much harder to defend authentication APIs in traditional ways. However, SecureCo's approach, which conceals the API endpoint and denies access to attackers, is not vulnerable to these AI-enhanced threats.

Quantum computing presents significant possibilities and challenges. Common encryption will be rendered useless against quantum computer decryption capabilities. It's highly probable that threat actors are stealing high-value encrypted data and storing it for the near future when quantum decryption is available. Quantum-proof algorithms are still in development, so there is no foolproof method to protect against this. However, SecureCo's network obfuscation uses de-attribution, evasive routing, and other methods to make it hard for adversaries to target and harvest customer data. The "store now, decrypt later" threat is mitigated by making customer data hard to find and identify.

AN INTERVIEW WITH MICKEY BRESMAN CEO, SEMPERIS

COMPREHENSIVE IDENTITY PROTECTION AND RESILIENCY

Identity is the new security perimeter in a world of ever-evolving digital threats, and Semperis stands at the forefront of this change with its innovative Identity Resiliency Platform. Offering comprehensive protection across Active Directory (AD) and Azure AD, the platform ensures operational resilience and robust security in the face of modern threats. Beyond threat detection, Semperis provides automated remediation and quick, malware-free recovery. In a recent chat with Mickey Bresman, CEO of Semperis, we learned more about the nuances of their platform, their proactive approach to evolving cybersecurity risks, the importance of their dedicated incident response team, and their substantial role in aiding with AD modernization—an essential, yet often underestimated facet of cyber defense.

TAG Cyber: Can you provide an overview of Semperis' Identity Resiliency Platform and its key features?

SEMPERIS: Cyberattackers persistently exploit vulnerabilities and evade security measures, necessitating a layered defense strategy. While EDR, MFA, and similar tools are essential, relying on a single tool is insufficient to protect against evolving threats.

At the same time, organizations and analysts (such as Gartner) acknowledge that identity has become the security perimeter. For example, an Active Directory (AD) is an active target, and eight or nine out of every 10 cyberattacks include AD. Considering that most organizations have AD and Azure AD (now called Microsoft Entra ID) as their core identity platform, bad actors specifically focus on those services, trying to get the "keys to the kingdom," which makes identity threat detection and response (ITDR) vital to modern cyber defense.

The Semperis Identity Resiliency Platform equips organizations with a comprehensive suite of tools and services for robust defense against cyberattacks. It offers in-depth protection for Active Directory (AD) and Azure AD—the identity backbone for 90% of organizations—ensuring operational resilience and identity security.

Organizations rely on the Semperis platform to enhance AD security by closing gaps, monitoring configurations, and analyzing attack paths. Our ITDR tools detect threats that evade traditional monitoring with change auditing and auto-remediation designed to counter fast-moving attacks. Our backup and recovery

Organizations rely on the Semperis platform to enhance AD security by closing gaps, monitoring configurations, and analyzing attack paths. Our ITDR tools detect threats that evade traditional monitoring while change auditing and auto-remediation counter fast-moving attacks.

tools reduce AD recovery time, ensuring a malware-free recovery. Strengthening identity defense, we offer post-breach forensics, breach preparedness, and response services delivered by AD cybersecurity experts. Additionally, we provide AD modernization and consolidation tools and services, valuable in M&A scenarios during the AD migration stage.

TAG Cyber: How does Semperis stay ahead of evolving cybersecurity risks targeting Active Directory?

SEMPERIS: AD and identity security experts are a significant part of our research and development teams. These teams have deep knowledge of AD and Azure AD, how cyberattackers target them, and emerging threats.

Our teams have decades of combined experience responding to cyber incidents. For example, our incident response (IR) practice allows us to see cyber criminals' techniques. We combine insights from our IR teams and security researchers to constantly enhance our solutions to deal with the latest types of attacks.

Considering our customers' industry and AD infrastructure, we customize our expertise to meet their needs. Our approach encompasses the entire life cycle of an identity-based attack, from identifying entry points to understanding post-infiltration activities and the injection of pervasive malware. Our solutions continually update IOEs, IOCs, and IOAs to monitor and counter evolving threats.

TAG Cyber: How does Semperis address the security challenges of securing AD environments?

SEMPERIS: Semperis gives defenders the advantage at every stage of an identity-based cyberattack. Our platform provides deep, comprehensive ITDR for AD and Azure AD across each stage of the identity-based attack cycle: before, during, and after an attack.

We help organizations fend off cyber threats through hybrid identity assessments that spot IOEs, IOCs, and IOAs, combined with attack-path analysis that prioritize Tier 0 assets, such as AD-privileged accounts. We also offer AD migration and consolidation support to help organizations modernize their hybrid AD environments for optimal security.

When attackers evade other defense systems, Semperis solutions can detect and remediate suspicious activity in AD and Azure AD and respond to active attacks through auto-remediation, notification, and incident response services. And in the worst-case scenarios, we enable fast AD recovery that eliminates back doors that attackers have left behind.

TAG Cyber: Can you elaborate on the role of your dedicated incident response team?

SEMPERIS: No vendor or services provider can outmatch Semperis' collective security experience in Directory Services. Our Breach Preparedness and Incident Response team comprises Microsoft MVPs, former Microsoft Premier Field Engineers, and other leading security experts. Together, they provide unrivaled experience protecting the most sensitive environments and deep expertise in on-prem AD, Azure AD, Okta, and other enterprise identity systems.

Our goal is to make hybrid AD security as efficient, comprehensive, and easy as possible. We help with fast recovery and post-breach forensics in the event of a breach and offer multiple services to help optimize identity-based security.

The AD Security Assessment is a high-level review of the environment and the considerations that led to the current design. This review evaluates important AD security boundaries and functions. The Operational Procedures Review evaluates current operational procedures.

Our Security Configuration Review uses automated tools like Purple Knight AD security assessment and manual methods to identify IOEs and IOCs in the AD environment. The Standard Active Directory Security Assessment (ADSA) targets the tactical level of the organization's AD security posture. It gathers technical information from AD and auxiliary systems, offering tactical remediation guidance.

The Attack Surface Reduction service involves an annual ADSA and quarterly sessions with Semperis experts to analyze IOCs, IOEs, and IOAs. Our team makes recommendations for reducing the attack surface and eliminating security exposures in the AD environment. We can also perform an attack path analysis to identify abnormal delegated rights and dangerous or unintended attack paths to Tier 0 assets and other critical assets.

TAG Cyber: How does Semperis help organizations modernize their AD systems?

SEMPERIS: Nine out of 10 attacks exploit AD, and many AD vulnerabilities are the result of years of configuration drift. Attackers also exploit vulnerabilities exposed during AD migration and consolidation following a merger or acquisition. Multi-forest environments face exponential risk, as the breach of one forest often leads to another, ending in a complete organization compromise.

Where AD is involved, modernization is often an urgent security priority. AD modernization is the surest way to dramatically reduce the AD attack surface. However, a full-scale AD migration and consolidation initiative requires extensive effort and planning, so many organizations delay the project.

Semperis offers a comprehensive AD modernization solution backed by industry-leading identity security tools and expert support, with a high focus on AD security throughout the migration and modernization process. We also help design the desired environment to meet modern security standards. Careful planning enables organizations to avoid security pitfalls, mitigate potential problems, and fix existing AD exposures.

As part of our approach to AD migrations, we mitigate risks during the migration process by spinning up an exact copy of the production AD to test the migration, set DSP to monitor for new vulnerabilities, and roll back unintended changes. Post-migration, Semperis monitors the destination AD to prevent configuration drift and continuously assesses the new environment for IOEs and IOCs to maintain an optimal level of AD security.

AN INTERVIEW WITH JOE SORIAL
VP PRODUCT, SHARDSECURE

REVOLUTIONARY MICROSHARDING TECHNOLOGY AND CYBERSECURITY

More organizations are moving to cloud-based storage in this digital transformation era, presenting a new frontier of data protection issues. Addressing these challenges, ShardSecure® has developed a pioneering Data Control Platform that promises enhanced security, privacy, resilience, and regulatory compliance for data in the cloud. During a recent conversation with ShardSecure, they shed light on the intricacies of their platform, discussing its key strengths in addressing the unique security challenges the cloud presents. They further illuminated how their innovative Microsharding technology not only obfuscates data but also makes it unattractive and unrewarding for potential breaches. By dispersing data across multiple clouds and rendering individual shards useless in isolation, ShardSecure has forged a game-changing path in data security, paving the way for a safer, more secure digital future.

TAG Cyber: Can you provide an overview of ShardSecure's Data Control Platform?

SHARDSECURE: At ShardSecure, we believe that all organizations can secure and protect their data wherever they want—whether on-prem, in the cloud, and in hybrid- or multi-cloud architectures. In the face of increasing cyberattacks and operational complexity, we help companies simplify data security and protection.

With strong data privacy, robust data resilience, cross-border regulatory compliance, native ransomware protection, and simple, agentless integration, the ShardSecure platform offers a multifaceted solution to complex challenges.

TAG Cyber: What specific data security challenges does ShardSecure's platform address?

SHARDSECURE: Until now, organizations had few options to secure their unstructured data and prevent third-party access in the cloud. Current solutions are resource-intensive, and new technologies like machine learning and AI require organizations to store more business-critical data in the cloud. With the challenges of complex data privacy laws and a rapidly evolving regulatory landscape, securing and protecting data in the cloud presents a major obstacle for most organizations.

Legacy solutions typically address a single aspect of data protection, privacy, or resilience, but data security needs to extend to every part of the organization. These solutions also tend to introduce significant complexity, performance drawbacks, and the need to update existing data flows and applications. Companies need new solutions fast—for privacy, compliance efforts, and security teams trying to keep data safe from exfiltration and attacks. The ShardSecure platform gives organizations the freedom and flexibility to store their data anywhere while rendering it unintelligible to unauthorized users.

With a simple, agentless implementation, the ShardSecure platform simplifies data security and privacy without legacy solutions' deployment headaches and performance drawbacks. Our "set and forget" management and policy-driven approach also helps companies maintain flexibility as data storage grows and new data privacy regulations arise.

> **With a simple, agentless implementation, the ShardSecure platform simplifies data security and privacy without legacy solutions' deployment headaches and performance drawbacks. Our "set and forget" management and policy-driven approach also helps companies maintain flexibility as data storage grows and new data privacy regulations arise.**

TAG Cyber: How do you ensure secure data handling/storage without compromising usability or performance?

SHARDSECURE: Traditional data sharding inspired ShardSecure's patented Microshard™ technology. Alongside tools like ElasticSearch and MySQL, sharding, i.e., fragmenting data into small pieces and then distributing those pieces to multiple storage locations for faster performance, is favored by storage and database companies like Oracle, Altibase, and MongoDB. ShardSecure's Microsharding techniques build upon the benefits of traditional sharding by introducing numerous data security, resilience, and compliance capabilities. We achieve high throughput and low latency by reading/writing in parallel and compressing pointers. Data security almost always brings a performance cost, but ShardSecure is a notable exception.

The ShardSecure platform also ensures data security without compromising usability. Acting as an abstraction layer, our technology operates with minimal impact on operations teams. Plus, there's no need for agents or disruption to application and data flows. ShardSecure's native multi-cloud and hybrid-cloud support also provides a single interface to manage storage locations and move data—without impacting performance.

TAG Cyber: How does the company's technology enable organizations to strengthen data security and resilience?

SHARDSECURE: ShardSecure strengthens data security by rendering data unintelligible to unauthorized users. Our innovative approach to file-level encryption works by shredding and distributing data to multiple customer-owned storage locations. By using an API-based abstraction layer between an organization's applications and its storage infrastructure, we ensure the security of that data.

ShardSecure's platform also supports robust data resilience, including multi-cloud architectures. Our technology maintains data integrity and availability during disruptions like cloud provider outages, misconfigurations, and ransomware attacks. Other solutions typically mirror data to achieve redundancy and resilience, which increases storage costs. Our algorithms, however, are based on a cost-effective architecture.

First, we maintain high availability. Each instance of ShardSecure is a virtual cluster that can be run on-prem or in the cloud, and customers can configure two or more virtual clusters for failover. Second, we maintain data integrity by performing multiple checks to detect unauthorized modifications and by self-healing data to transparently reconstruct it after malicious or unauthorized tampering or deletion. The result is accurate, available, and confidential data, regardless of storage location.

TAG Cyber: What is ShardSecure's approach to data privacy and compliance?

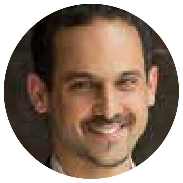
SHARDSECURE: The traditional approach to maintaining data privacy is fortifying data segmentation. ShardSecure's technology desensitizes the data, rendering PII and other sensitive material unintelligible to unauthorized users—from cloud storage admins to attackers. This approach mitigates the impact of data breaches, strengthens data privacy, and ensures compliance with cross-border regulations.

ShardSecure's platform enables organizations to address data sovereignty and residency concerns by utilizing their preferred cloud storage providers in their desired geographic locations and jurisdictions.

Organizations can distribute data across different regions of a single cloud provider, multiple cloud providers, or a hybrid mix of on-prem storage and one or more cloud providers.

ShardSecure is also validated to meet the requirements of Use Case 5 for Schrems II/European Data Protection Board (EDPB) compliance. Our split processing technology is easily deployed in a multi-party processing environment, allowing organizations to store and process data safely under Use Case 5.

With our innovative approach to data security, privacy, resilience, and compliance, ShardSecure offers a new way for companies to face modern cyber challenges and regain data control.



AN INTERVIEW WITH ERIC AVIGDOR
VP PRODUCT MANAGEMENT, VOTIRO

ZERO TRUST CONTENT SECURITY AND ANALYSIS

In the rapidly changing world of cybersecurity, a comprehensive approach to mitigating file-borne threats is indispensable. Enter Votiro, a ground-breaking company at the forefront of Zero Trust Content Security, which is making waves with its forward-thinking solutions. Operating under the assumption that all content carries potential threats, Votiro's innovative methodologies dramatically reshape how financial services and healthcare companies conduct business. Our recent conversation with them gave us profound insights into their unique approach: how they safeguard data throughout the entire file lifecycle and guarantee secure, seamless, and uninterrupted business operations. By integrating their technology, businesses can shield their sensitive information and critical systems from potential risks, effectively future-proofing their operations against evolving threats.

TAG Cyber: What makes Votiro unique in its offer to protect against file-borne threats?

VOTIRO: Our unique Zero Trust Content Security approach protects the entire file lifecycle from known and unknown (zero-day) threats and harmful data that often elude other tools, ensuring enhanced user protection. This applies to many use cases, including files uploaded to S3 buckets via web browser downloads and attached within emails, to those entering and exiting content collaboration platforms like Microsoft OneDrive, SharePoint, Teams, and Box.

Our value to the organization is simple: Unlike conventional tools dependent on known signature detection for protection, we assume that all content in and out of an organization poses a potential threat requiring disarmament. We also ensure the content remains fully functional and is delivered promptly to users, avoiding interruption to business operations.

This approach to file-borne threats is critical for those working in financial services and healthcare, as sensitive information is passed between multiple parties and necessitates zero downtime.

TAG Cyber: How does Votiro Cloud provide a lasting solution for organizations seeking to maintain long-term security?

VOTIRO: Our cloud solution only allows known-safe elements to pass through to the organization's endpoint (via email, web browser, data lake, content collaboration platform, etc.), so we're always up to date. And with the addition of AI detection for macros and other malware, Votiro is at the forefront of proactive content security.

When it comes to long-term protection within a security architecture, Chief Information Security Officers (CISOs) and other IT members can add Votiro to their stack quickly and seamlessly. As an open API solution, Votiro is ideal for organizations looking to complement their current architecture or bolster their security posture without adding unnecessary overhead.

Our cloud solution only allows known-safe elements to pass through to the organization's endpoint, so we're always up to date. And with the addition of AI detection for macros and other malware, Votiro is at the forefront of proactive content security.

TAG Cyber: What makes Votiro necessary to a security team's architecture?

VOTIRO: For starters, AV solutions rely on signatures of known threats to catch them. Yet, threat actors continue to evolve their tactics and create new ways of penetrating defense systems—creating almost 450,000 new variants daily—which means these known signatures rapidly become outdated, rendering AV-centric solutions ineffective. Votiro's answer to this constant struggle to keep up is to deconstruct all content (regardless of detecting a known threat) and then rebuilding the file from only known-safe components. This rebuilding is unlike other CDR solutions in that the end-user receives a usable file instead of a view-only PDF or Excel doc with unusable macros and other essential features.

At the same time, file-based malware targets organizations through content collaboration platforms like Dropbox, Slack, and similar tools, making it challenging to keep up with dynamic threats and an ever-changing risk surface. Votiro's proactive approach allows teams to continue working normally.

Similarly, threat actors have swiftly outsmarted the once-reliable sandboxing method. Simple Google searches can provide threat actors the information they need to ensure their malware can evade detection within the sandbox, only executing once inside the production environment or bypassing the sandbox altogether.

Consider also the negative impact on productivity and user experience. When individuals send files for sandboxing in a production environment, the time it takes can negatively affect user productivity. Again, Votiro's answer is to ensure that sandboxing never enters the equation by removing all threats before they enter any protected environment.

TAG Cyber: In what ways does Votiro's solution align with and complement solutions in highly regulated markets?

VOTIRO: Regarding financial service organizations such as banks, credit unions, and brokerage firms, security teams constantly look to remain compliant with regulations like SOX, GLBA, PCI-DSS, and GDPR to protect their customers' data from fraud or theft. However, cybercriminals are innovative and will breach endpoints with hidden threats stored within seemingly innocuous content, including images, loan applications, and tax documents.

While banks usually feel protected against these novel attacks (with signature-based security tools that rely on identifying and quarantining known threats), they remain open to unknown/zero-day attacks embedded within incoming content or data.

Irrespective of whether content is uploaded to a portal by a client or received via email, Votiro's solution keeps incoming information safe and usable, no matter where it comes from. So, even the most sensitive information (password-protected files, zip files, etc.) remains safe to open and pass between internal stakeholders.

TAG Cyber: How does Votiro's Zero Trust Content Security technology enhance overall security posture?

VOTIRO: At Votiro, we go beyond traditional detection-based protections, taking a Zero Trust approach and sanitizing all files that flow through an organization's environment. Rather than requiring a unique tech stack with complex configurations that force changes to security posture, Votiro delivers protection through APIs, which makes it a plug-and-play solution for teams with limited bandwidth and those who work within a high-risk, highly-trafficked environment.

Votiro is a Zero Trust Content Security solution, but we also leverage advanced Content Disarm and Reconstruction (CDR), initial AV detection tactics, and AI trained to identify harmful macros and other malware. This makes Votiro the enforcement and mitigation arm of Data Security Posture Management (DSPM), providing solutions for data posture gaps and those who rely on email, content collaboration tools, and data lakes to get things done.

ANALYST REPORTS

LEVERAGING OFFENSE TO IMPROVE CYBER DEFENSE USING SAFEBREACH

DR. EDWARD AMOROSO

To address modern cyberthreats to enterprises, organizations need a new paradigm of continuous security validation based on the simulation of offensive attacks to optimize cyber defensive posture. The SafeBreach platform exemplifies this breach and attack simulation approach to protect digital assets.

INTRODUCTION

Enterprise security teams today must address multiple dimensions of cyberthreats and must deal with an ever-changing and constantly expanding assortment of attack techniques. Frameworks such as MITRE ATT&CK help with this challenge, but even these models have trouble keeping up. Ongoing and active monitoring and analysis of attack methods represent good strategies for solving this problem.

In addition, security teams must deal with constant shifts in how they use enterprise technology. Most companies are experiencing a digital transformation, so how deployed security controls are configured and function will change frequently. Security teams must, therefore, continually probe and test the effectiveness of their controls to ensure that shifts in digital strategy do not undermine protection architectures.

In this article, we outline strategies for using cyberoffensive tactics to address these defensive challenges. In particular, we explain how a continuous security validation program powered by an automated breach and attack simulation (BAS) can provide increased visibility, risk reduction, remediation, and resilience for cyber defense. We use the commercial **SafeBreach** platform to illustrate this practical cybersecurity approach in enterprise environments.

HOW IS SECURITY POSTURE MEASURED?

Board members, executives and other stakeholders in an organization frequently demand information about security posture. They often assume that the CISO and enterprise security teams will have mechanisms in place to provide both a qualitative and quantitative answer to this question. The good news is that metrics can be put in place to determine whether the posture is improving or degrading.

The industry has moved toward implementing BAS methods for continuous and automated measurement of security posture. The goal is to first provide visibility into the effectiveness of security controls so that immediate mitigation can be put in place to prevent negative consequences. The simulations must be done responsibly to ensure safety and security, which is a key tenant of BAS solutions.

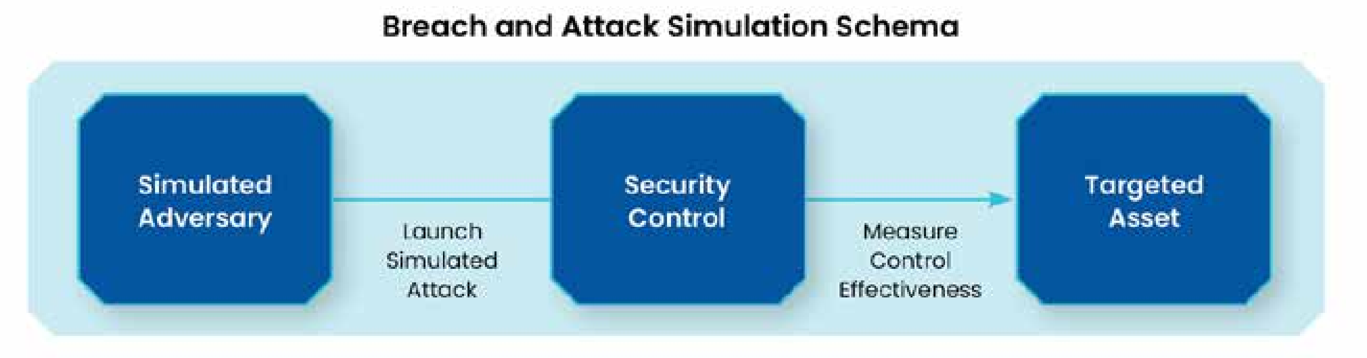


Figure 1. Breach and Attack Simulation Schema

Several advantages emerge for such BAS functionality, including continuous validation of how well certain security controls are functioning. Generally, BAS is integrated into the enterprise network infrastructure, but nothing would preclude a next-generation attack simulation from operating across organizational boundaries and perimeters in a zero-trust network environment.

HOW CAN OFFENSE BE LEVERAGED TO IMPROVE DEFENSE?

The cybersecurity community has come to recognize the necessity of continuous security validation, with the Cybersecurity and Infrastructure Security Agency (CISA) recently calling for organizations to enact a more automated, continuous approach to threat testing. This includes the ability to emulate and automate attacks based on a detailed understanding of common and emerging techniques used by malicious actors.

Such BAS-oriented visibility into enterprise security control effectiveness can be leveraged to support the following types of management initiatives:

- **Security Control Optimization:** This is one of the most powerful outcomes of an effective BAS program in an enterprise. Controls can be optimized by security teams based on outcomes observed during continuous testing and validation to close gaps or address misconfigurations to help with both security protection and framework compliance.

- **Vendor Accountability:** The use of BAS in an enterprise helps maintain accountability for commercial vendors. This not only reduces costs but also maximizes the value of deployed products and platforms, which when done properly, also minimizes the potential for “tool sprawl.”

- **Rapid Response:** The ability to respond to threats more rapidly comes with a deeper understanding of and insight into security control effectiveness. Incident response teams can focus on weak spots highlighted by the BAS platform to determine lateral movements and attack paths. Vendors like SafeBreach also provide service-level agreements to add attack coverage into the BAS platform based on new vulnerabilities.

- **Strategy Planning:** The overall security strategy and planning activities are influenced by the insights from continuous security validation with BAS. The level of visibility that BAS provides enables stakeholders to formulate long-term security plans and inform resourcing decisions. This can help justify security investments, support additional budgets for security teams, and ensure strategic alignment across the organization.

Continuously validating the effectiveness of security controls has emerged as a mandatory action in most enterprise environments. The demand for ongoing insight into threat and risk is driven both by the senior-level executives and management teams, including the board, and the working-level practitioners. In the next section, we highlight the enterprise-level SafeBreach platform, which effectively implements continuous security validation for customers using BAS.

CASE STUDY: SAFEBREACH PLATFORM

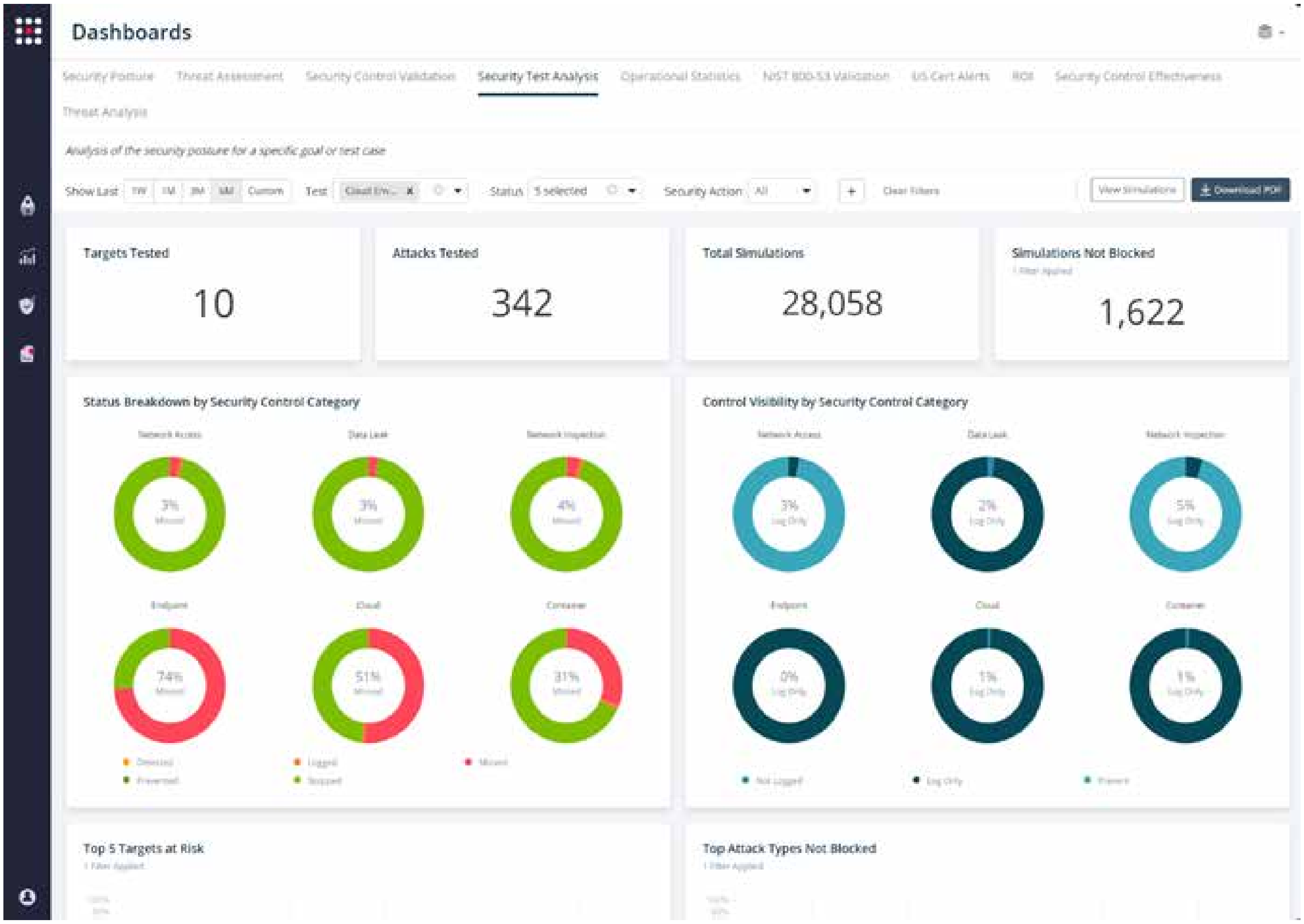
Founded in 2014, the cybersecurity company SafeBreach offers a continuous security validation BAS platform. Enterprise teams use the SafeBreach solution to safely run attack scenarios against security controls and analyze results to understand gaps, prioritize remediation efforts and inform stakeholder communications regarding the efficacy of the security architecture, business risk and future needs.

The SafeBreach BAS platform uses a set of more than 25,000 offensive attack methods that collectively comprise its patented Hacker's Playbook™. The goal is to help enterprise customers validate the efficacy of their security controls at all layers of their protection architecture—and to do so independently at each stage of the defense process. The SafeBreach offering emphasizes the following areas:

- **Real-Time Validation:** Control monitoring from SafeBreach is done in real-time through its 24-hour service level agreement on all US CERT and FBI Flash alerts. Such real-time support allows teams to test new vulnerabilities immediately, which for modern enterprise teams is superior to the offline validation exercises that have characterized the security industry for many years.

- **Identifying and Prioritizing Risk:** Detecting gaps in coverage is also an important feature of SafeBreach. These gaps might involve localized gaps in functionality or policy for a given control, or they could involve broader shortcomings in the deployment of some required control. SafeBreach also enables teams to prioritize their remediation efforts.

- **Customized Reporting:** Reporting is one of the primary drivers for enterprise security teams to procure and deploy a commercial solution such as SafeBreach. The flexibility to customize reports to the local environment is an especially useful feature in the SafeBreach reporting implementation.



Show Last: 6M
Test: Cloud Env...
Status: 5 selected
Security Action: All

Targets Tested: 10
Attacks Tested: 342
Total Simulations: 28,058
Simulations Not Blocked (1 Filter Applied): 1,622

Figure 2. Sample SafeBreach Reporting Dashboard

The industry has clearly moved from viewing BAS as optional to viewing BAS it as a mandatory tool to identify weaknesses in security controls. As a result, integration with other security solutions and platforms is an important feature. SafeBreach supports this evolution by including integrations with many major security vendors, such as Palo Alto Networks (Cortex SOAR) and Microsoft Advanced Threat Protection (ATP).

ACTION PLAN

Enterprise teams are advised to engage an action plan today to ensure they leverage this critical technology properly. While each organization will have a unique set of local management and technical approaches, every group will benefit by addressing the following list of tasks that collectively form an action plan that can lead to the effective deployment of BAS into the security architecture.

Step 1: Security Control Validation Inventory
Before BAS can be deployed, the security team must first identify how controls are currently validated, including control validation approaches such as penetration testing, enterprise security scanning and attack surface management. BAS solutions can complement or even reduce the need for these approaches, but action plans should always start with an understanding and documentation of what is presently deployed.

Step 2: BAS Solution Review
Next, the security team should select a BAS vendor. As discussed above, SafeBreach offers an effective platform for enterprise organizations that covers all major requirements, but buyers do have options. TAG Cyber's Research as a Service (RaaS) can support enterprise teams requiring detailed information on BAS vendors to ensure that the selected vendor properly integrates with their existing security infrastructure.

Step 3: Stepwise Deployment
Experience dictates that BAS deployments can be done in a stepwise manner, starting with a proof-of-concept implementation, and moving across the enterprise to cover additional portions of the network and additional controls. This is helpful because, unlike more complex platforms, BAS is relatively easy to deploy quickly and can begin deriving value immediately. TAG Cyber analysts are always available to assist enterprise teams with their planning.

TAGCYBER

ANALYST REPORT

ACCELERATING CYBERSECURITY COMPLIANCE WITH MEAN TIME TO COMPLIANCE (MTTC): AN OVERVIEW OF REGSCALE

CHRISTOPHER R. WILDER
JOHN J. MASSERINI

INTRODUCTION

As organizations increasingly migrate to cloud computing solutions to streamline IT operations and reduce costs, ensuring the security and integrity of sensitive data becomes paramount. The Federal Risk and Authorization Management Program (FedRAMP) has become a critical consideration for many companies, especially those that sell cloud-based services to the U.S. federal government. However, achieving compliance can be complex and challenging. RegScale, the world's first real-time governance, risk, and compliance (GRC) platform, specializes in helping organizations achieve compliance with multiple cybersecurity frameworks, such as the Cybersecurity Maturity Model Certification (CMMC), the Service Organization Controls 2 (SOC2), and FedRAMP. This e-book provides an in-depth overview of RegScale's GRC platform; outlines the key stages of the FedRAMP compliance process; and highlights how RegScale's expertise can help organizations achieve compliance faster and more efficiently, using the mean time to compliance (MTTC) metric.

WHAT IS MEAN TIME TO COMPLIANCE (MTTC)?

Mean time to compliance, or MTTC, is a performance metric measuring the average time that it takes for an organization to achieve compliance with a specific cybersecurity framework. This metric is valuable for organizations because it helps identify areas where improvements can be made to expedite the compliance process, ultimately leading to better security posture, reduced risk, and increased operational efficiency. By focusing on MTTC, organizations can prioritize resources, streamline processes, and make informed decisions that lead to faster and more cost-effective compliance.

WHY MTTC MATTERS

Compliance with cybersecurity frameworks such as FedRAMP, CMMC, SOC2, and others is essential for mitigating risks and maintaining the trust of clients and partners. However, achieving and maintaining compliance can be a resource-intensive process that diverts time and attention from other critical business functions. Every cybersecurity executive overseeing compliance will tell you that the journey is frustrating, labor-intensive, and requires endless hours to continuously adapt to new threats and regulatory requirements in today's rapidly evolving cybersecurity landscape. By focusing on MTTC, organizations can make data-driven decisions about where to allocate resources and how to improve processes to reduce the time and effort required to achieve compliance.

REGSCALE'S GRC PLATFORM FOR REDUCING MTTC

RegScale offers a comprehensive technology platform that streamlines and automates many aspects of the compliance process. As the world's first real-time GRC platform, it provides a centralized location for managing compliance activities and tracking progress, including documentation, policy, risk, and audit management. The platform provides real-time reporting and dashboards that give organizations visibility into their compliance status and progress toward reducing their MTTC.

RegScale's GRC platform is highly configurable, allowing organizations to tailor their compliance activities to their unique business requirements and compliance objectives. The platform is also cloud-based, enabling organizations to access compliance activities and progress from anywhere, at any time, and on any device. With RegScale's platform, organizations can manage compliance activities more efficiently, reducing the time and resources required to achieve compliance and, ultimately, reducing their overall MTTC.

Key strategies for reducing MTTC, using RegScale:

1. **Compliance Strategy and Road Map:** RegScale works with organizations to develop a tailored compliance strategy and road map that identifies the necessary steps to achieve compliance and reduce MTTC. This process begins with understanding the organization's unique business requirements, risk tolerance, and compliance objectives. From there, RegScale creates a customized plan that outlines the specific actions required to achieve compliance within the desired timeframe.

2. **Gap Analysis Support:** Once the customer performs a thorough gap analysis to identify areas where the organization's security posture falls short of the requirements of the desired compliance framework, RegScale supports the efforts to evaluate the organization's policies, procedures, and technical controls against the requirements of the relevant cybersecurity framework. The gap analysis results provide a clear picture of the areas that need improvement and a path forward, enabling organizations to prioritize their efforts and allocate resources effectively.

3. **Remediation Support:** RegScale supports implementing the necessary changes to address identified gaps, ensuring that the organization meets compliance requirements as quickly as possible. Compliance requirements may involve updating policies and procedures, implementing new technical controls, and providing employee training and awareness programs. RegScale's experienced cybersecurity professionals offer comprehensive and hands-on assistance and guidance throughout the remediation process, ensuring that organizations can achieve compliance as efficiently as possible.

   Further, RegScale's "white glove" service features a proficient customer success team providing tailored, current information to its clients. Through updated tickets and discussions, customers can access specialized training and demonstrations of new capabilities, maximizing the benefits to its customers.

4. **Continuous Monitoring and Improvement:** RegScale offers ongoing customer support to maintain compliance and continuously improve the organization's security posture, reducing MTTC for future compliance efforts, including regularly reviewing and updating policies and procedures, monitoring changes in the cybersecurity landscape, and ensuring that organizations stay current with evolving regulatory requirements. RegScale also provides periodic assessments to measure progress and identify any new gaps that may have emerged. This continuous improvement approach helps organizations maintain a strong security posture while minimizing the time and effort required for future compliance initiatives.

THE FEDRAMP COMPLIANCE PROCESS AND HOW REGSCALE HELPS ITS CUSTOMERS REDUCE THEIR MTTC

The FedRAMP framework, known for being one of the most comprehensive and cumbersome, necessitates a meticulous approach to achieving compliance, typically taking 18-24 months. RegScale, with its GRC expertise and special focus on FedRAMP, assists organizations in navigating this complex process more efficiently, ultimately speeding up their entry into the federal market. By swiftly identifying and addressing security gaps, RegScale streamlines compliance activities and empowers organizations to make data-driven decisions that optimize their efforts. This targeted approach reduces MTTC and minimizes resources expenditure, while providing a strategic advantage in a competitive landscape.

1. **Initiation and Creation of the Master Security Plan (MSP):** The FedRAMP certification process begins with organizations identifying the appropriate authorization level (Low, Moderate, or High) corresponding to the sensitivity of the data they manage. This crucial step establishes the compliance process's scope, ensuring that organizations concentrate on the most relevant controls and requirements. By aligning with the appropriate FedRAMP level, RegScale's expert guidance assists clients in developing a robust master security plan, streamlining the compliance journey, and reinforcing their commitment to protecting sensitive federal information.

2. **Assessment:** Once the MSP is in place, a thorough evaluation is conducted by a third-party assessment organization (3PAO) to evaluate the organization's security posture against the FedRAMP requirements. This process includes a review of documentation, interviews with key personnel, and technical testing of the systems and controls. The 3PAO then produces a detailed report outlining the organization's compliance status and any identified gaps.

3. **Authorization:** If the assessment demonstrates compliance, the organization receives an authorization to operate (ATO) from a federal agency, granting it the right to provide cloud services to the federal government. Obtaining an ATO is a significant milestone in the FedRAMP compliance process, as it signifies that the organization has met the stringent security requirements necessary to protect sensitive government data.

4. **Continuous Monitoring:** Organizations must monitor their security posture and report any changes to the authorizing agency, ensuring ongoing compliance. Continuous monitoring is essential for maintaining FedRAMP compliance and demonstrating a commitment to protecting sensitive government information. Continuous monitoring also includes regularly updating system security plans, conducting periodic assessments, and implementing any required remediations.

REGSCALE'S GRC EXPERTISE IN IMPROVING MTTC

RegScale has significant GRC expertise in and emphasis on FedRAMP and most other cybersecurity frameworks. The platform assists organizations of all sizes to efficiently navigate the complex cybersecurity compliance process, reducing their MTTC and accelerating their entry into the federal market. This targeted approach streamlines compliance activities, empowering organizations to make data-driven decisions that optimize their efforts while minimizing resources expenditure and providing a strategic advantage.

Initially, RegScale helps clients determine the appropriate FedRAMP authorization level (Low, Moderate, or High) according to the sensitivity of the data that they manage. This step is vital in setting the compliance process's scope, focusing on the most relevant controls and requirements. RegScale's expert guidance enables clients to develop a robust MSP, expediting the compliance journey and solidifying their commitment to protecting sensitive federal information. Once the MSP is in place, RegScale supports organizations during the third-party assessment organization (3PAO) evaluation, ensuring a thorough review of the organization's security posture against FedRAMP requirements. This support results in a comprehensive report outlining the organization's compliance status and identifying any gaps.

Upon successful assessment, organizations receive an authorization to operate (ATO) from a federal agency, granting them the right to provide cloud services to the federal government. RegScale continues to support maintaining FedRAMP compliance through continuous monitoring of security posture, regular updates to system security plans, periodic assessments, and the implementation of required remediations. This ongoing guidance helps organizations protect sensitive government information and maintain a strong security posture, minimizing the time and effort required for future compliance initiatives from FedRAMP and other cybersecurity frameworks.

EXPANDING MTTC TO OTHER CYBERSECURITY FRAMEWORKS

In addition to FedRAMP, organizations often face the challenge of maintaining compliance with other cybersecurity frameworks, such as CMMC and SOC2. RegScale's expertise extends to these frameworks, allowing it to help organizations optimize their MTTC across multiple compliance initiatives. RegScale can guide organizations through the complexities of achieving and maintaining compliance with various cybersecurity standards by applying the same principles of gap analysis, remediation support, and continuous monitoring.

WRAPPING IT UP

Mean time to compliance (MTTC) is a valuable metric for organizations seeking to improve cybersecurity compliance. By focusing on MTTC, organizations can prioritize resources, streamline processes, and make informed decisions that lead to faster and more cost-effective compliance. RegScale is the only real-time GRC platform on the market today tailored to each organization's unique needs. It helps to achieve and maintain compliance with various cybersecurity frameworks, including FedRAMP, CMMC, SOC2, and others. With its expertise in reducing MTTC, RegScale is well-positioned to guide organizations through the complex compliance landscape, leading to better security posture, reduced risk, and increased operational efficiency.

Embracing MTTC as a key performance metric is the first step toward a more proactive and streamlined approach to cybersecurity compliance, ensuring that your organization stays ahead of the curve and protects its valuable data assets. In a world where cloud computing is increasingly popular and sensitive data is constantly at risk, partnering with a cybersecurity company like RegScale can make all the difference in achieving compliance with the ever-evolving regulatory landscape. By allocating the budget to the RegScale platform, organizations can improve their mean time to compliance, leading to a more secure and efficient operation that meets the stringent requirements of federal agencies and other stakeholders.

KEY TAKEAWAYS

- MTTC is an essential performance metric that can help organizations optimize cybersecurity compliance across various frameworks, including FedRAMP, CMMC, and SOC2.
- RegScale is the world's first real-time GRC platform. It offers to guide organizations through the complexities of achieving compliance, from developing tailored strategies and road maps to providing remediation support and continuous monitoring.
- By focusing on reducing MTTC, RegScale enables organizations to prioritize resources, streamline processes, and make informed decisions that lead to faster and more cost-effective compliance.
- RegScale's expertise in reducing MTTC (and navigating the compliance landscape for multiple cybersecurity frameworks) positions it as a valuable partner for organizations looking to improve their security posture, reduce risk, and increase operational efficiency.

TAG'S TAKE

For CISOs and security teams, achieving compliance with cybersecurity frameworks can be daunting, but it is critical to ensuring the security and integrity of sensitive data. By partnering with a cybersecurity GRC software company like RegScale, organizations can improve their mean time to compliance and more effectively navigate the complex compliance landscape.

If your organization seeks assistance with FedRAMP, CMMC, SOC2, or any other cybersecurity frameworks, RegScale should be a viable solution. Its platform and expertise can help you develop a tailored GRC and compliance strategy, identify gaps in your security posture, and provide the support needed to achieve compliance as efficiently as possible. Companies in regulated environments such as health care, financial services, and the government utilize RegScale to ensure compliance with compliance requirements. RegScale's platform and commitment to helping obtain compliance framework faster through MTTC, organizations can be confident that your organization can protect their valuable data assets and maintain the trust of clients and partners in today's ever-evolving cybersecurity landscape.

TAGCYBER

ANALYST REPORT

USING BALBIX TO SECURE HIGHER EDUCATION FROM RANSOMWARE THREATS

DR. EDWARD AMOROSO
DR. GAURAV BANGA

Higher educational institutions are particularly prone to cybersecurity threats due to ransomware. We offer guidance for how schools can reduce the associated cyber risk using the commercial Balbix cybersecurity platform.

INTRODUCTION

The university campus network was once well-defined and secure behind a perimeter firewall. However, like all organizational information technology (IT) infrastructure, this setup has shifted toward a virtual architecture consistent with zero trust principles. Accordingly, university workloads have shifted from premise data centers to the cloud and software-as-a-service (SaaS).

A consistent backdrop that IT security teams at universities have always had to accept is the general culture of open access and free sharing so indicative of a learning environment. As such, it has never been easy for security teams to impose policies that restrict access—and this has remained true for modern zero trust-based university networks.

As a result, universities are now excellent targets for ransomware attacks, given the open nature of their infrastructure, their open culture of sharing, and their surprisingly significant resources. Consider that universities manage endowments that can reach billions of dollars. Donors' personally identifiable information is high-value data that must be protected. Hackers and criminals view universities as great ransomware targets.

In this report, we explain how the university network has evolved and how this specifically makes them vulnerable to the types of attacks commonly found in ransomware campaigns. We then show how attack surface management from commercial security vendor Balbix offers an effective means to reduce this cyber risk.

HIGHER EDUCATION COMPUTING ENVIRONMENTS

The modern higher educational institution faces a series of cybersecurity challenges that combine conventional enterprise risk with the unique characteristics of higher learning environments. In particular, colleges and universities must find means to address cybersecurity problems such as the following:

- **Protecting Important Research** – Protecting research and results from adversarial eyes has grown in significance with increased nation-state-sponsored cyberthreats.
- **Managing Endowment Risk** – The size of many university endowments has increased the risk of ransomware demands from an adversary.
- **Balancing Privacy and Openness** – The challenge arises that student privacy must be balanced with the competing need to maintain an open sharing environment.

These risks are complemented by the full range of common enterprise cybersecurity challenges that face any organization of non-trivial size. Accordingly, larger colleges and universities will tend to be at higher risk, if only because the value of their targeted resources (e.g., endowments) is also high.

RANSOMWARE RISKS FOR HIGHER EDUCATION

A common attack strategy against universities involves the use of ransomware to make demands of the school's leadership. In March 2021, for example, the FBI issued a warning for U.S.-based higher education regarding the growing incidence of ransomware targeting the sector.

Universities, specifically, must contend with several challenges related to the growing ransomware risk. One issue they must deal with is sub-optimal budgets as few universities have established a culture and tradition of heavy cybersecurity spending. This creates a disadvantage for most higher education settings to implement the best controls.

In addition, reporting relationships for CISOs in higher education have been poorly defined. After a major breach incident at Penn State, for example, the university reevaluated the role of its CISO and decided to elevate the position, providing that role with greater responsibility and authority to take suitable security preventive or responsive action.

Perhaps the greatest challenge is that many universities have not been aggressive enough in deploying the best possible cybersecurity platforms to their infrastructure. Oftentimes, they have used free software, open-source tools, or freemium versions of protection. This trend must shift in favor of the best available protection platforms.

HOW BALBIX CAN HELP HIGHER EDUCATION REDUCE RANSOMWARE RISK

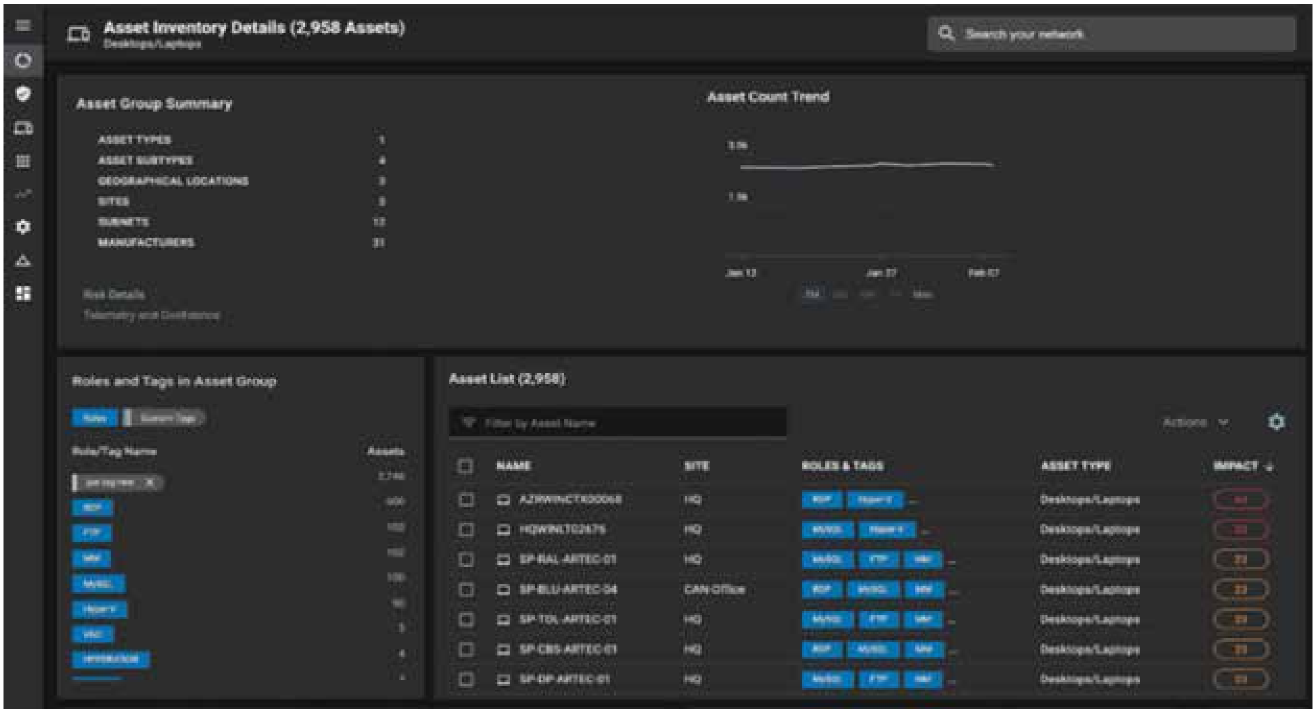
The Balbix Security Cloud offers an excellent commercial option for higher education CISOs and their security teams to effectively reduce their risk, especially for the growing ransomware campaigns targeting colleges and universities. Balbix has great experience and expertise in this sector and understands the challenges facing higher education CISOs.

The Balbix Security Cloud supports cybersecurity posture automation with consequences expressed in a way that is actionable and that connects with CISOs and their teams. The solution was created to complement existing vulnerability management and related security posture capabilities used in the enterprise, while also addressing the major challenges and shortcomings that such functions have typically exhibited for most security teams. Some higher education teams will find that Balbix can replace their existing posture tools.

Automated Asset Discovery and Inventory

The first goal of the Balbix platform is to address the ongoing challenge of inaccurate and incomplete asset inventories, which is common in colleges and universities. Without having clarity around the specific devices, apps, endpoints, and other resources in use across the campus network, as well as across the cloud and SaaS, it becomes impossible to have a complete measure of the security posture. This challenge is further driven by the consistent change that occurs for even those assets with an established inventory.

Balbix addresses this requirement through automated, continuous monitoring of the campus network posture, including traffic flows, to discover assets. The types of assets that emerge from this task include premise and cloud-based devices, applications, systems, and services—including managed and unmanaged assets. Fixed and mobile systems, including internet of things (IoT) devices, are also included in the asset discovery capability.



ASSET TYPES	1
ASSET SUBTYPES	4
GEOGRAPHICAL LOCATIONS	3
SITES	3
SUBNETS	12
MANUFACTURERS	31

Role/Tag Name	Assets
[illegible]	[illegible]
RDP	600
FTP	102
VM	102
MySQL	100
Hyper-V	90
VNC	3
[illegible]	4

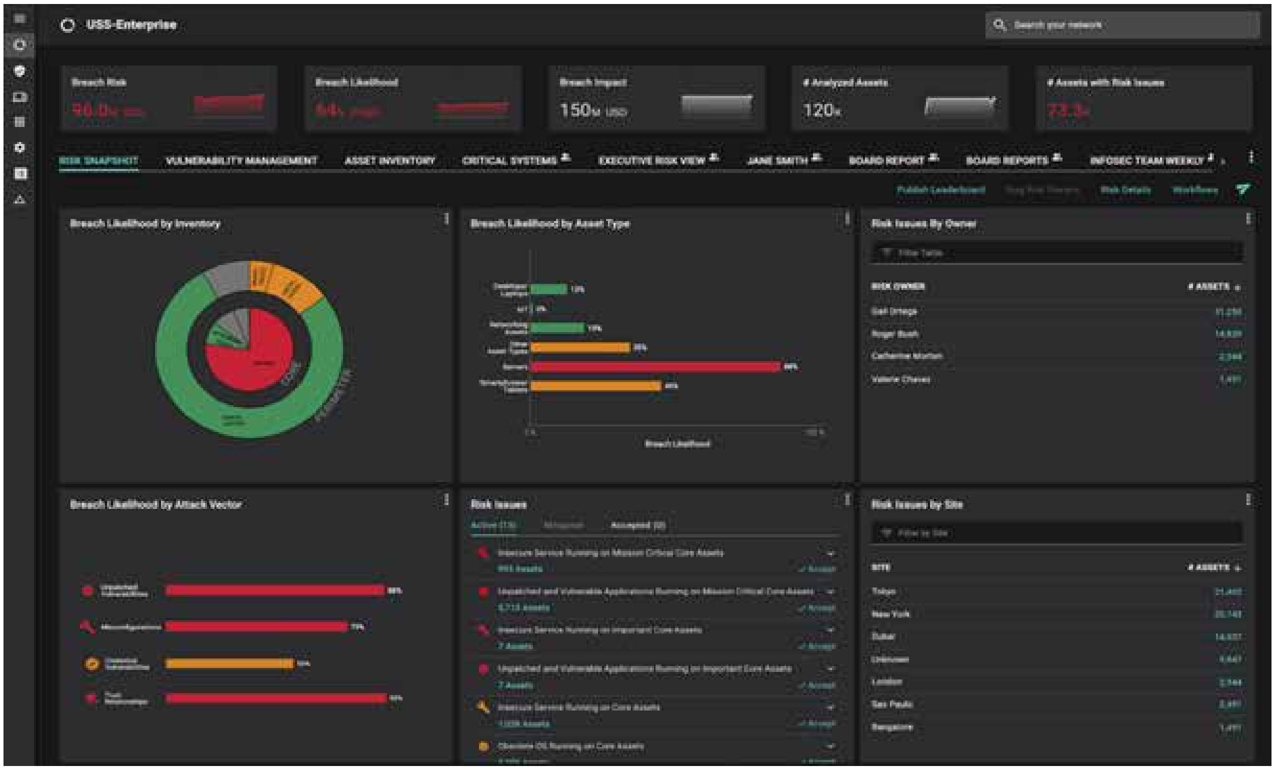
□	NAME	SITE	ROLES & TAGS	ASSET TYPE	IMPACT ↓
□	AZRWINCTX00068	HQ	RDP Hyper-V ...	Desktops/Laptops	[illegible]
□	HQWINLTO2676	HQ	MySQL Hyper-V ...	Desktops/Laptops	[illegible]
□	SP-RAL-ARTEC-01	HQ	MySQL FTP VM ...	Desktops/Laptops	[illegible]
□	SP-BLU-ARTEC-04	CAN Office	RDP MySQL VM ...	Desktops/Laptops	[illegible]
□	SP-TOL-ARTEC-01	HQ	MySQL FTP VM ...	Desktops/Laptops	[illegible]
□	SP-CBS-ARTEC-01	HQ	RDP MySQL VM ...	Desktops/Laptops	[illegible]
□	SP-DP-ARTEC-01	HQ	MySQL FTP VM ...	Desktops/Laptops	[illegible]

Figure 1. Balbix Platform. Discovered Asset Details.

The output data discovered in the Balbix platform, using its library of API-based connectors, includes identifying access to SaaS-based and on-premise tools and systems. Balbix performs the heavy lifting of unifying data from different tools, deduplicating, correlating, and performing machine-learning-based inferencing. The solution takes advantage of scheduled exports for end-to-end automation, resulting in a near real-time analysis. It also presents risk quantifications (see below) in financial terms so higher education officials and staff can better understand the consequences of exposures.

Continuous Cybersecurity Asset Management

Once a complete view of the security posture has been created for the entire attack surface, the obligation emerges to manage and maintain the asset inventory and associated context in a unified and maximally automated manner. The Balbix platform includes support for vulnerability and risk management workflows to ensure that assets are managed continuously to provide accurate security posture even as the attack surface evolves.



RISK OWNER	# ASSETS
Gail Ortega	11,250
Roger Bush	14,839
Catherine Morton	2,344
Valerie Chavez	1,491

Insecure Service Running on Mission Critical Core Assets
995 Assets ✓ Accept
Unpatched and Vulnerable Applications Running on Mission Critical Core Assets
5,713 Assets ✓ Accept
Insecure Service Running on Important Core Assets
7 Assets ✓ Accept
Unpatched and Vulnerable Applications Running on Important Core Assets
7 Assets ✓ Accept
Insecure Service Running on Core Assets
1,029 Assets ✓ Accept
Obsolete OS Running on Core Assets

SITE	# ASSETS
Tokyo	21,460
New York	20,142
Dubai	14,557
Unknown	4,647
London	2,744
Sao Paulo	2,491
Bangalore	1,491

Figure 2. Balbix Security Cloud. Risk Quantifications.

The collected data used to help categorize and manage assets based on their visible attributes includes IP addresses, DNS information, inventory data, and other signals that can be used to identify entities. Balbix uses a technique called host enumeration logic (HEL) to normalize the accurate asset inventory view to support stateful, intelligent deduplication, sanitization and other data clean-up tasks.

Such tasks must be performed at all levels of the technology stack, each of which will provide a different type of asset-related information. Layer 7 analysis, for example, extracts application-level information about assets, whereas layer 3 and 4 analysis extracts information about packet headers and protocol behaviors. The goal is to combine this collection into a unified view of the discovered asset. The Balbix unified data model extends to 450+ attributes of assets. The data model includes coverage for laptops, traditional VMs and physical servers, IoT, network equipment, and SaaS assets, plus cloud-hosted Kubernetes clusters, AWS S3 buckets, AWS EC2 instances, and their equivalents in GCP and Azure environments.

Risk-Based Vulnerability Management
A major problem reported by college and university security teams is the large volume of alerts collected by typical vulnerability management and scanning tools. It is common for the number of alerts to become so high that security teams cannot maintain proper risk categorization, handling, and mitigation. This situation is ironic because the success of vulnerability management programs is often measured based on the number of alerts generated.

The Balbix platform handles volumes that result from vulnerability management processes by ingesting and analyzing data from a large number of security, IT, and business-related data sources. These sources include vulnerability assessment tools, security scanning platforms, threat and vulnerability feeds, breach and attack simulation tools, SAST and DAST tools, penetration testing results, crowdsourced security test output, endpoint controls, CMDBs, ticketing systems, GRC tools, and more.

Enterprise Vulnerability Prioritization

Prioritizing vulnerabilities requires attention to relevant factors, most of which will vary in intensity between academic environments. The Balbix approach involves establishing several major categories of factors so that higher education teams can organize the best mitigation strategies. Such mitigation can start with those vulnerabilities that can have the greatest negative impact on critical assets. The factors address vulnerability severity and threat level, asset exposure, criticality, and security controls.

Ultimately, the goal is to perform a continuous breach likelihood calculation, which is a computed summation of the individual attack vector computations. Such analysis is complemented by probabilistic graph models, which estimate the vulnerability levels associated with the various risk scenarios. Collectively, these computations and values provide a college or university with an accurate understanding of its cybersecurity posture.

Cyber Risk Quantification

The goal of accurately establishing a quantitative measure of security posture for the organizational attack surface requires the use of a risk formula that makes sense to the local domain. To avoid multiple equations, formulas, and other metrics, the Balbix platform defines a consistent cyber risk equation that can be used across all assets and over all aspects of the school to perform continuous cyber risk assessments.

The Balbix platform automates risk quantification. While this is certainly not a new strategy in enterprise cybersecurity, the specialized artificial intelligence models integrated into the platform support the calculation of risk trending, breach likelihood, breach impact scoring, breach likelihood by inventory and more. These are presented in a visual display that is easy to share with both IT security staff and higher education officials.

In addition, Balbix higher education customers benefit from the financial impacts that can be traced back to conditions of underlying assets and vulnerabilities for easy remediation. Expressing risk in business contexts has become a common approach for enterprise security teams hoping to illustrate the consequences of cyber risk to management and executive staff while supporting operational and strategic decision-making based on business risk.

Board-level Cyber Risk Visibility and Reporting

The final goal of the Balbix platform is to ensure that campus IT security teams have the best available tools for reporting and explaining vulnerability and risk posture to the organization. This must include reports for school officials, including trustees, as well as colleagues with a more detailed understanding of security programs. Such reporting must cover the entire attack surface and must account for ongoing change.

Most college and university officials will tend to focus on the reputational impact of potential breaches because this represents the most direct consequence of cyber risks such as ransomware. Balbix supports detailed impact modeling that uses estimates based on factors such as prior information, contextual impact modeling based on business tags, usage, volumes and interactions, and impact modeling based on inferences from prior and contextual data.

ENTERPRISE ACTION PLAN

It is recommended that higher education security teams and college or university officials act immediately to review, address and improve their cybersecurity posture assessment. This is best done using an automated platform that can unify existing posture-related tools such as scanning and security testing. As suggested above, the Balbix platform provides excellent support in this regard and should be included in source selection plans.

BENEFITS OF EXTERNAL ATTACK SURFACE MANAGEMENT (EASM) ACROSS BOTH SECURITY AND IT

DR. EDWARD AMOROSO

This report explains how the commercial CyCognito External Attack Surface Management (EASM) platform supports many different team roles across both enterprise security and IT.

INTRODUCTION

Enterprise teams can no longer view the benefits of a security platform in an organizationally siloed manner. Rather, they must view benefits holistically across the various groups that will derive value. For security teams, this requires attention across many different functions including vulnerability management and penetration testing.

For information technology (IT) groups, the benefit must also be carefully considered since a major role for most IT operations teams involves keeping infrastructure up and running. Security platforms cannot just focus on risk reduction without also demonstrating clear value to these IT partner teams.

In fact, security teams typically depend on IT operations teams to enable 24/7/365 coverage for internally and externally facing protections. For example, where a security team might select and deploy an identity and access management (IAM) platform, the IT operations team will often be engaged to support and maintain the servers and applications.

In this report, we look specifically at investments in enterprise attack surface management (EASM) with a focus on the commercial solution offered by cybersecurity vendor CyCognito. The goal is to demonstrate how EASM, in general, and CyCognito, in particular, enable value across enterprise security and IT teams.

HOW DOES EASM WORK?

External Attack Surface Management (EASM) is an approach to identifying and managing the cyber risk associated with an organization's modern digital perimeter. By perimeter, we imply all the various physical and logical access points that exist in a given enterprise—and this can be quite complex.

In the early days of networking, an attack surface was relatively straightforward to identify. That is, it was delimited by the corporate firewall, usually implemented as a perimeter network, sometimes referred to as a demilitarized zone (DMZ). This concept gradually waned in usefulness as companies implemented work-from-home, outsourcing, wireless connectivity, and so on.

Thus, the discipline of EASM emerged as a requirement to create a virtual identification of what was previously a physically identified component. This is obviously necessary to identify weaknesses and exploitable vulnerabilities at the entry point to a company's networks, systems, applications, and data.

A major goal for EASM is to help identify where these problems exist and to inform a prioritization that allows enterprise teams to know exactly how to allocate resources to optimize cyber risk management tasks. This is best done via continuous monitoring of the attack surface with emphasis on showing potential attack vectors.

HOW DOES CYCOGNITO IMPLEMENT EASM?

A good way to explain and illustrate External Attack Surface Management (EASM) is in the context of its commercial implementation by cybersecurity vendor CyCognito. Their platform represents a clean and canonical implementation of the solution area, offering a convenient means for introducing the basic concepts of EASM.

The CyCognito platform supports EASM through a range of offensive-minded reconnaissance activities across a target infrastructure. The CyCognito methodology includes support for the following continuous and automated tasks:

- **Attack Surface Discovery** – Business assets and relationships are discovered, analyzed, and graphed. The result is an understanding of the external attack surface.
- **Contextualization** – Relevant factors are used to classify assets and associated data. The context informs deeper understanding of the relationships between assets and owners.
- **Testing** – A suite of tests on the external attack surface that reveal weaknesses and uncover how malicious actors could target valued assets.
- **Prioritization** – The discovered risks are prioritized based on context, inventory, ease of attacker exploitation, and difficulty of remediation.
- **Remediation Guidance** – The platform streamlines remediation through actionable guidance and exploitation intelligence geared toward reducing attack surface risk.

These tasks are presented sequentially, and certainly, there are relationships between the tasks that imply a basic ordering. The attack surface must be identified before context and testing can be established. However, it is reasonable to think of the CyCognito approach as ongoing and consisting of interleaved tasks. Remediation of known issues, for example, can be done concurrently with new elements of an attack surface being discovered.

HOW DOES CYCOGNITO SUPPORT SECURITY TEAMS?

It is relatively straightforward to see how EASM, in general, and CyCognito, in particular, support and enable the mission of enterprise security teams. Below, we list common security functional personas found in practical settings, and show how the CyCognito solution is closely aligned with the purpose and objectives for that role:

- **Vulnerability Management** – The application of EASM to vulnerability management (VM) is direct since both disciplines are focused on the visibility and posture of exploitable access points. Many teams run their EASM platform in the context of their VM infrastructure.
- **Penetration Testing** – Most penetration testing teams, whether internal or external to the organization, find EASM to be a useful resource in establishing a roadmap for testing or a validation of their identified soft spots in a target enterprise.
- **Risk Management** – The aspects of risk management focused on exploits and access are directly influenced by the posture guidance offered by an EASM platform. Without such real-time context, risk management can drift out of date quickly.
- **Security Audit** – Security auditors, whether internal or external, now use EASM posture as a means for determining where and how to review and assess the effectiveness of documented cybersecurity controls.
- **Application Testing** – The importance of software applications, whether internally or externally hosted cannot be underestimated. Testing of applications depends on EASM for both context and correlation of results.
- **IT Operations** – As will be described in the section below, operational tasks, including support for compliance and risk management, that are coordinated between the security and IT teams are directly improved by EASM platform support.

While the list just cited includes many aspects of enterprise security, one might have difficulty finding any aspect of a protection program that is not influenced directly by CyCognito EASM deployment and use. Network security, forensics, and application security, for example, will all benefit from the presence of a solid commercial EASM support infrastructure.

HOW DOES CYCOGNITO SUPPORT IT OPERATIONS TEAMS?

To demonstrate the value of CyCognito's EASM for IT operations, it is first essential that we clearly define what the objectives are for a typical IT operations team. If we can show that EASM can itself help to advance the goals for such organizations, then we will increase the return on investment (ROI) for the entire organization. IT operations goals can be grouped as follows:

- **Business Enablement** – The most obvious objective for any IT operations team is to enable the business services and functions to meet the mission goals of the company.
- **Friction Avoidance** – A complementary objective is that users, business units, partners, and other stakeholders should never see unnecessary friction—and in fact, should experience zero friction whenever possible.
- **Unit Cost Optimization** – The assumed goal for any operations team is that unit costs must be managed and optimized. This is especially true in environments that must scale across large swaths of users.
- **Service Level Agreements** – IT operations teams are tasked with ensuring that infrastructure and applications are working as per service level agreements with business unit leaders.

These objectives provide a useful framework for examination of whether IT operations teams, independent of their support for the security team, will also experience benefits from the deployment of EASM – and CyCognito in particular. Below, we review each of these three goals and show that ROI support is generally positive in each case.

BUSINESS ENABLEMENT

As suggested earlier, IT operations teams must enable a wide variety of different business services and functions to meet the mission goals of the company, including the drive for digital transformation. An understanding of the external attack surface using the CyCognito platform allows these IT operations teams to ensure three important security properties in new external applications supporting the organization:

- **Existing Vulnerability Avoidance** – The ability to monitor the attack surface helps IT operations teams avoid deployment of services that would inherit existing vulnerabilities. For example, if some region is shown to exhibit weakness, perhaps found during EASM testing, then the IT operations team could avoid new deployments into this region until the problem is fixed.
- **New Vulnerability Avoidance** – The presence of EASM capability enables IT operations teams to have rapid visibility to new services, such as cloud-hosted or SaaS applications that introduce new exploitable vulnerabilities. Such visibility is a powerful tool for any IT operations team.
- **Digital Transformation Enablement** – Digital transformation has turned your external attack surface into a constantly changing entity. The CyCognito platform specifically offers the ability to help IT operations and security teams map their legacy IT environments and monitor newly emerging environments for security vulnerabilities, including those that are the result of misconfigurations.

FRICTION AVOIDANCE

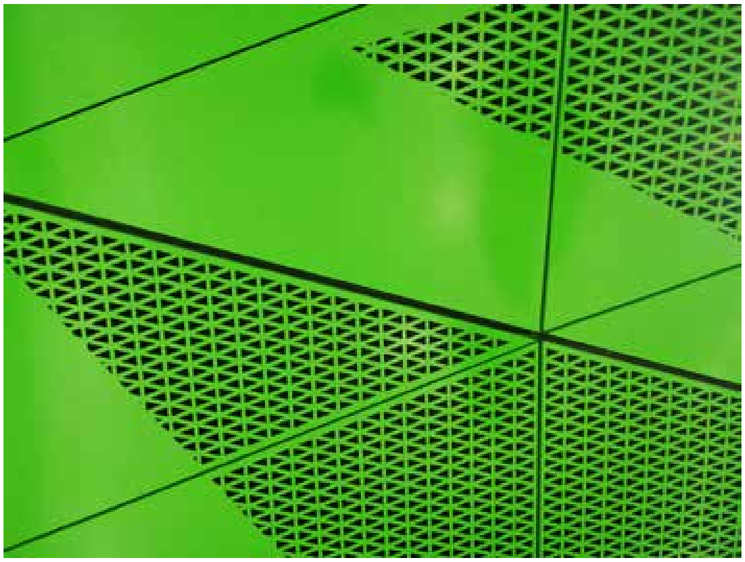
As suggested earlier, IT operations teams must ensure that users, business units, partners, and other stakeholders do not experience unnecessary friction in their use of technology and services. Correspondingly, the use of CyCognito's EASM solution is also valuable to prevent friction in many internal IT operational tasks. In this way, the security simplifies the experience for IT operations staff. This occurs as follows:

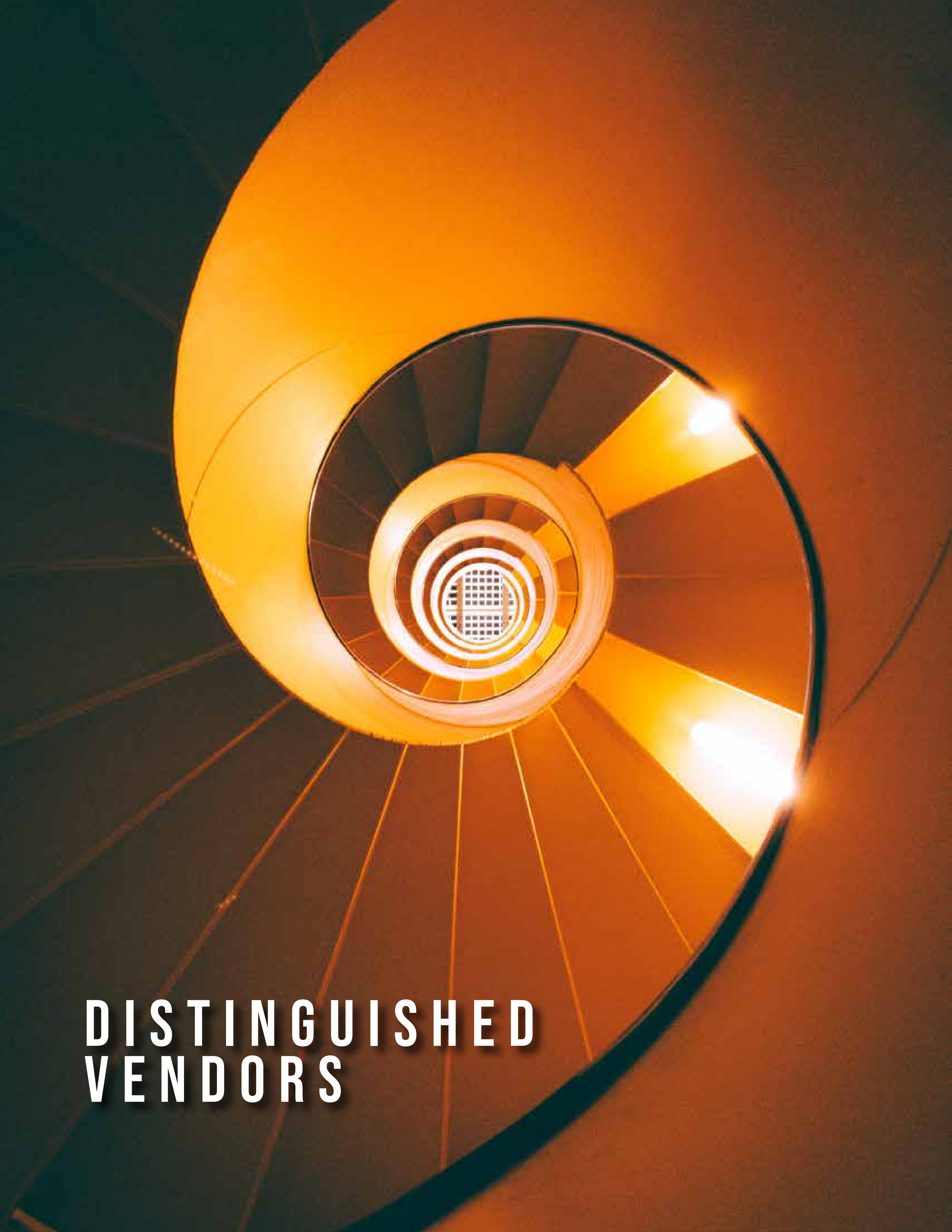
- **Continuously Monitored Surface** – The continuous manner in which monitoring is done for the external attack surface ensures that IT operations teams do not need to delay any planned operational task or job to pre-determine security posture. Rather, this is an ongoing task that supports any scheduled activity.
- **Automated Testing and Reporting** – The automation associated with tasks such as reporting helps IT operations teams avoid the friction of having to provide security documentation or justification for scheduled tasks or jobs. This simplifies operations and reduces the burden of work for IT operations teams.
- **Mergers and Acquisition Support** – An important additional use case related to the avoidance of friction involves EASM-based assessment of the externally visible infrastructure for companies being acquired or merged. Such visibility can improve planning, budgeting, and risk management.

UNIT COST OPTIMIZATION

Finally, the goal of unit cost management pervades all aspects of IT operations team activity, especially in recent years, where IT teams feel great pressure to reduce technology spend. The cost situation will be different across organizations, especially where budgets between security and IT operations might be managed separately. Nevertheless, it is common for CyCognito's platform to reduce the need for IT operational spend in the following ways:

- **Workflow Cost Reductions** – Most IT operations teams depend on workflow to schedule, monitor, and provide metrics on their various tasks and jobs. The presence of automated EASM from CyCognito is a valuable means to avoid new licensing for expensive IT service management and workflow tools.
- **Product and Technology Mapping** – EASM platforms such as CyCognito provide useful support for IT operations teams identifying blind spots such as departments or subsidiaries with licenses they might not be authorized to be using in their day-to-day business activity.
- **Monitoring Tool Cost Reductions** – The monitoring and active testing capability inherent in any attack surface management tool will reduce the need for IT operations teams to have to engage additional monitoring licenses for its own coverage. This has the effect of optimizing budgets for monitoring across both IT operations and security.





DISTINGUISHED VENDORS

DISTINGUISHED VENDORS

Q3 2023

Working with cybersecurity vendors is our passion. It's what we do every day. Following is a list of the Distinguished Vendors we've worked with this past three months. They are the cream of the crop in their area—and we can vouch for their expertise. While we never create quadrants or waves that rank and sort vendors (which is ridiculous), we are 100% eager to celebrate good technology and solutions when we find them. And the vendors below certainly have met that criteria.

Abacode is a managed cybersecurity and compliance provider (MCCP) that delivers customized, framework-based programs using leading technologies and professional services. Their unique approach achieves security and compliance results four times faster than the industry average, while increasing efficiency and streamlining processes for clients worldwide.

Amenaza Technologies Ltd. is a leading threat analysis and risk assessment solutions provider. With its flagship product, Secure*I*Tree®, the company assists organizations in identifying potential vulnerabilities, analyzing threat scenarios, and optimizing security countermeasures. Founded in 1998, Amenaza Technologies is headquartered in Calgary, Canada, serving diverse global clients.

Anvilogic's AI-powered SOC platform automates threat detection, investigation, hunting and triage across hybrid logging platforms. By leveraging AI-driven recommendations and 1000+ out-of-the-box detections, security teams can improve detection coverage to quickly identify and prioritize potential risks. Anvilogic's mission is to empower organizations so they can protect their assets and stay ahead of constantly evolving cyber threats.

Aqua Security stops cloud native attacks and is the only company with a $1M Cloud Native Protection Warranty to guarantee it. As the pioneer and largest pure-play cloud native security company, Aqua offers the industry's most unified cloud native application protection platform (CNAPP), which protects the entire development lifecycle from dev to cloud and back.

TAG CYBER DISTINGUISHED VENDORS

2023

BEYOND IDENTITY

Beyond Identity is a leading technology innovator in FIDO2-certified multi-factor authentication, delivering a passwordless, phishing-resistant and frictionless user experience that prevents credential breaches and delights users. Companies like Snowflake, Unqork, and Roblox rely on Beyond Identity's cloud-native platform to advance their Zero Trust strategies.

BREACHRX

BreachRx is the leading automated incident reporting and response platform used by security and technical leaders to overcome one of their biggest challenges—reducing cybersecurity regulatory and incident compliance risks. The BreachRx SaaS platform streamlines collaboration and frees internal bandwidth across a business while ensuring compliance with the most stringent global cybersecurity and privacy frameworks.

Cymulate

Cymulate's Extended Security Posture Management allows organizations to measure and maximize operational efficiency while minimizing risk exposure. Based on real-time data, Cymulate protects IT environments, cloud initiatives and critical data against threat evolutions. Using simulation, evaluation, and remediation, Cymulate empowers and defends organizations worldwide, including leading healthcare and financial services.

invicti

Invicti Security – which acquired and combined AppSec leaders Acunetix and Netsparker—is on a mission: application security with zero noise. An AppSec leader for more than 15 years, Invicti delivers continuous application security that is designed to be reliable for security and practical for development, as well as serve critical compliance requirements.

Island

Island is the browser designed for the enterprise that makes work fluid yet fundamentally secure. With the core needs of the enterprise embedded in the browser itself, Island enables organizations to shape how anyone, anywhere, works with their information while delivering the Chromium-based browser experience users expect: Island, The Enterprise Browser.

nudge

Nudge Security, founded in 2021 by Jaime Blasco and Russell Spitler, aids distributed organizations in effectively managing SaaS security and governance. Recognized by CSO Magazine as a "Cybersecurity startup to watch" and an SC Awards finalist for "Most promising early-stage startup," Nudge champions employee-centric security solutions. Discover more at www.nudgesecurity.com or follow them on Twitter and LinkedIn.

plainID

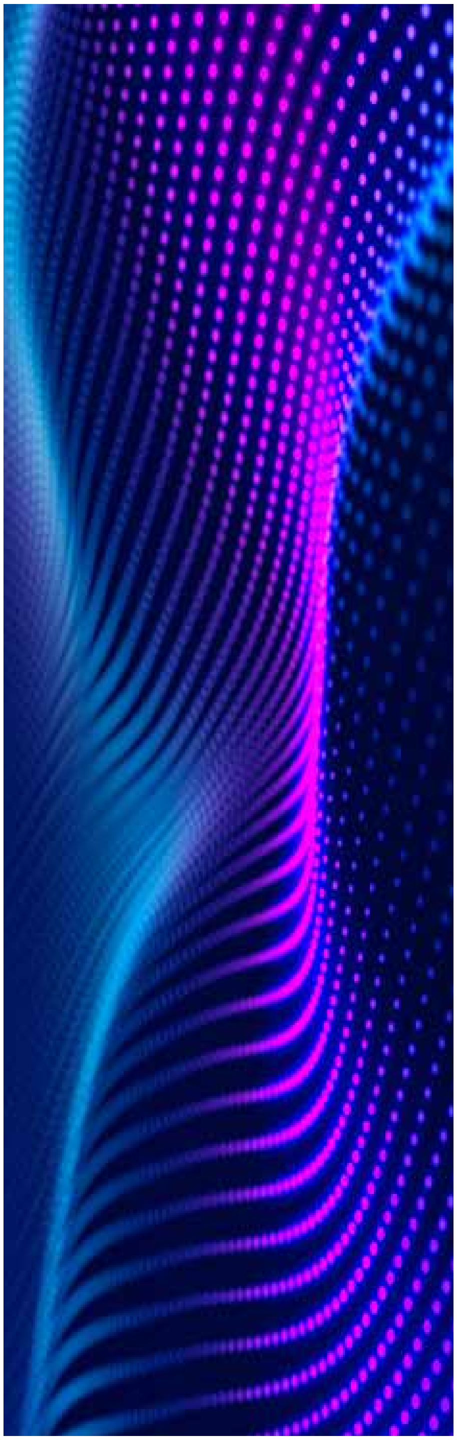
PlainID Inc., a leading Authorization-as-a-Service provider, leverages Policy Based Access Control (PBAC) to simplify authorization management, enabling organizations to create, enforce, and manage policies enterprise-wide. Firms meet user journey demands through secure identity-to-asset connections, implementing zero-trust architectures, and enhancing data security. The PlainID Authorization Platform facilitates business growth by integrating technologies with advanced authorization features.

RAPIDFORT

RapidFort.com is the pioneering Software Attack Surface Management platform (SASM), offering comprehensive runtime and build-time tool suites. Our cutting-edge solutions empower organizations to scan, analyze, and fortify modern software, ensuring enhanced security and resilience while safeguarding software from potential vulnerabilities.

secureco

SecureCo provides network security solutions protected by stealth and obfuscation. Our innovative approach shields networks, APIs, and cloud connections from reconnaissance, exploitation, and breach. Trusted for the most demanding commercial and government cybersecurity applications, we deliver high-performance, exceptionally secure endpoint and data transit protection, reducing attack surface, vulnerability, and administrative overhead.



TAG CYBER DISTINGUISHED VENDORS

2023

Semperis is a pioneering cybersecurity company providing enterprise-level identity protection solutions. Their Identity Resiliency Platform offers comprehensive protection for Active Directory (AD) and Azure AD, ensuring operational resilience against cyber threats. Semperis also provides automated remediation, swift recovery tools, and dedicated incident response services, making them a trusted cybersecurity partner.

ShardSecure is a cybersecurity company that specializes in Microsharding technology. Their revolutionary solution disassembles data, distributes the shards across multiple clouds, and renders them useless in isolation. By making data breaches unattractive and unrewarding, ShardSecure provides organizations with unparalleled security. The company, founded in 2018, has its headquarters in New York, USA.

SPHERE is an award-winning, woman-owned cybersecurity business that is redefining how organizations improve security, enhance compliance and achieve identity hygiene. SPHERE puts rigorous controls in place to secure a company's most sensitive data, while creating the right governance process for systems and assets, and keeping the company compliant with relevant industry regulations.

TXOne Networks Inc. offers cybersecurity solutions that ensure the reliability and safety of industrial control systems and operational technology environments through OT zero trust methodology. TXOne works with leading manufacturers and critical infrastructure operators to develop practical, approaches to cyberdefense.

Varonis is a pioneer in data security and analytics, specializing in software for data protection, compliance, and threat detection and response. Varonis protects enterprise data by analyzing data activity, perimeter telemetry and user behavior, while preventing disaster by locking down sensitive data and efficiently sustaining a secure state with automation.

Votiro is a Zero Trust Content Security company that detects, disarms, and analyzes billions of files between organizations, their employees, and the customers that rely on them. Votiro is an open API platform that allows teams to receive safe, fully functional files without slowing down business.

TAGCYBER