

TAG Cyber •  
**SecurityAnnual**  
2ND QUARTER 2023

**AI**  
**WILL BE**  
**THE END OF**  
**CYBERSECURITY**  
**(AS WE KNOW IT)**

IN FOCUS:

ARTIFICIAL INTELLIGENCE  
AND CYBERSECURITY

ARTICLES / OPINIONS / INTERVIEWS

# ARTIFICIAL INTELLIGENCE: THREAT, MENACE OR MIRACLE?



LESTER GOODMAN,  
DIRECTOR OF CONTENT,  
TAG CYBER

If you have experienced any of the tsunami of articles and reports about AI in recent months, the headline on this page should feel familiar. Ranging from predictions of the end of civilization to “gotcha” moments of artificially inspired snarkiness, to handwringing that the technology can’t tell whether to set your laundry cycle for whites or colors, there seems to be no end to the negativity. Even given the occasional medical miracle.

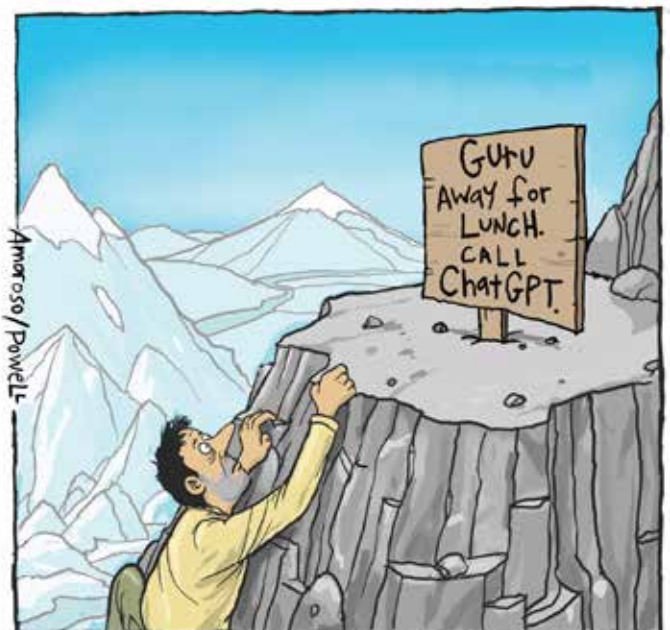
When TAG Cyber’s analysts and content team decided to try to bring some clarity to the discussion, Dr Edward Amoroso, Founder and CEO, threw down a gauntlet: **“AI will be the end of cybersecurity,”** he said. Then he added, **“And that’s a good thing.”**

As one might imagine, the reaction within an organization based in, and serving as a beacon to, the cyber industry was something akin to shock. Our initial thinking was to respond to Ed’s provocation in a free-form roundtable and hash it out. Sometimes it takes the stopping power of a strong statement to draw eyes and minds. As you will see on page 6, however, Amoroso’s explanation of his statement is reasoned and level.

Ultimately, we did not hold a Great Debate. Or even a discussion. Our writers thought about the subject and, with the guiding hand of our Editor, David Hechler, produced a series of articles, reports (and even cartoons) that begins with Ed’s throwdown, but goes on to cover the subject in a way that demonstrates how far-ranging it really is. We wrote about a new NIST framework that CISOs will want to study; the status of legislation that addresses AI dangers; the challenges of, and opportunities for, making the most of AI in smart cities and automated vehicles; and the uncertain future of humans working side by side with AI.

Our Quarterly ended up with the type of balanced coverage of a major topic that TAG Cyber specializes in. But that did not stop me from running the “end of cyber” headline on our cover. I hope and believe that it will draw readers and get them thinking. And that is the mission of this publication. Given that opportunity, I smelled blood.

So, threat? Menace? Miracle? Maybe a little of each.



Lester Goodman, Director of Content

David Hechler, Editor

Michelle Perino, Managing Editor

#### Contributors

Dr. Edward Amoroso  
Dr. Jennifer Bayuk  
David Hechler  
John J. Masserini  
Dave Neuman  
Christopher R. Wilder

#### Editorial & Creative

Lester Goodman  
David Hechler  
Michelle Perino  
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



Volume 9 No. 2

Publisher: TAG Cyber, a division of TAG Infosphere, Inc.,  
45 Broadway, Suite 1250, New York, NY 10006.  
Copyright © 2023 by TAG Infosphere. All rights reserved.

This publication may be freely reproduced, freely quoted, freely distributed, or freely transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or any information storage and retrieval system without need to request permission from the publisher, so long as the content is neither changed nor attributed to a different source.

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 Cyber LLC 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 Cyber LLC 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.**

April, 19, 2023

# C O N T E N T S

Introduction	2	Automate Incident Response and Readiness With BreachRX Andy Lunsford, BreachRX	43
<b>WILL AI CHANGE EVERYTHING, EVERYWHERE, ALL AT ONCE?</b>	<b>5</b>	Continuous Threat Exposure Management With Cymulate Carolyn Crandall, Cymulate	46
AI Will Be the End of Cybersecurity (As We Know It)	6	Scalable Security Testing for the SDLC From Invicti Sonal Shah, Invicti Security	49
Can AI Protect Humans from Humans?	8	Threat-Informed Cyber Operations Support With Purple Teaming From SnapAttack Peter Prizio, SnapAttack	52
Why AI-Based Cybersecurity Will Continue to Need the Human Touch	10	Protecting Assets Through Identity Hygiene With SPHERE Fredy Martinez-Pardo, SPHERE	55
The Intersection of AI, Transportation and Smart Cities: Charting a Secure and Ethical Future	13	Ground-Up Cybersecurity for OT Environments From TXOne Networks Dave Purdy, TXOne Networks	58
A CISO's Take on NIST's Advice for Dealing with AI	18	Securing Mission-Critical Data With Varonis Matt Radolec, Varonis	61
How Should Artificial Intelligence Be Regulated?	22		
Guidance on Security Issues Related to ChatGPT	26		
<b>INTERVIEWS</b>	<b>29</b>	<b>ANALYST REPORTS</b>	<b>64</b>
All-In-One Cybersecurity and Compliance From Abacode Anil Markose, Abacode	30	TAG Navigator: A New Approach to Commercial Cybersecurity Vendor Comparison	65
AI-Driven Threat Detection From Anvilogic Karthik Kannan, Anvilogic	33	Engineering Effective Network Detection and Response for the Enterprise	71
Cloud Native Application Protection From Aqua Security Dror Davidoff, Aqua Security	37	EDR and CDR Are Different. Here's How	77
Beyond Identity's Zero Trust Authentication Thomas "Tj" Jermoluk, Beyond Identity	40	Why Enterprise Browsers Should be Included in Compliance Frameworks	80
		<b>DISTINGUISHED VENDORS</b>	<b>83</b>



**WILL  
AI  
CHANGE  
EVERYTHING,  
EVERYWHERE,  
ALL  
AT  
ONCE?**

# AI WILL BE THE END OF CYBERSECURITY (AS WE KNOW IT)

DR. EDWARD AMOROSO

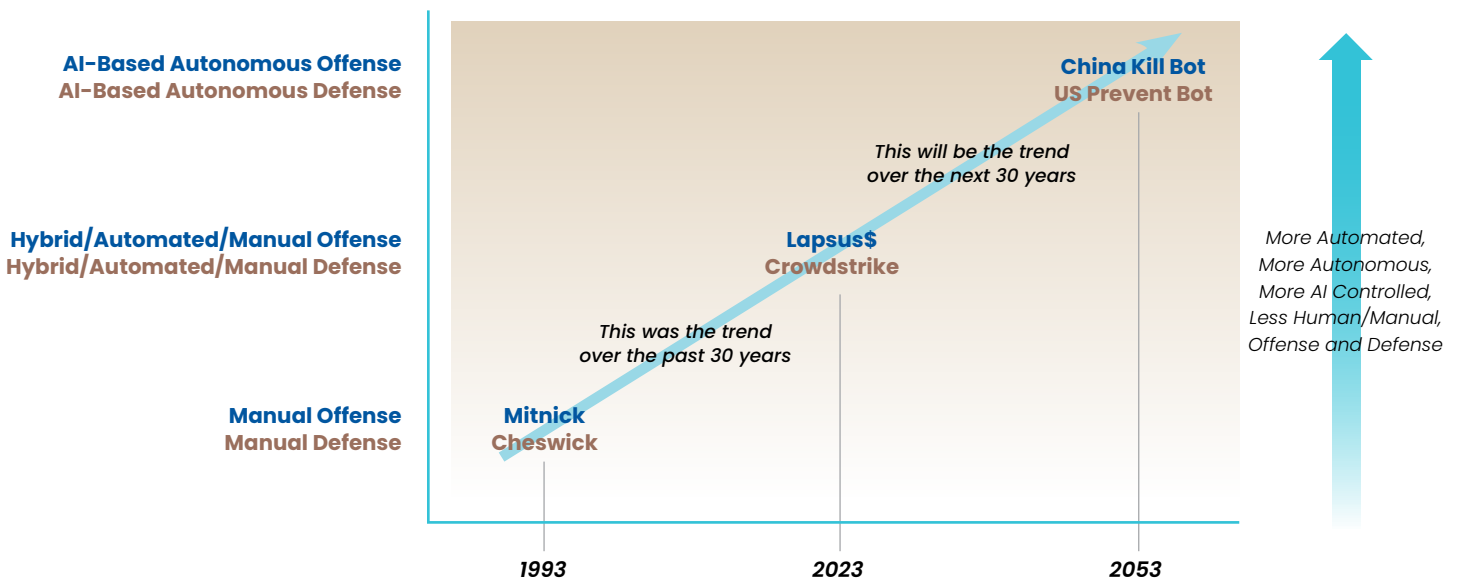


Figure 1. Author’s Prediction of AI’s Influence on the Future of Cybersecurity

I believe we can now glimpse the *end* of cybersecurity, as we know it—and it will be driven by artificial intelligence. Now, before you go and cancel your Series A term sheet or reduce your CISO’s quarterly budget, let me explain what I mean.

Almost exactly 40 years ago, David Letterman set up a wonderful **competition** between a humidifier and a dehumidifier, fighting it out in the same room, while the humans watched to see which would win the vapor contest.

This display of machine versus machine offers a crude glimpse into where cybersecurity is headed long-term. That is, in the future cyber offensive and defensive platforms will be AI-controlled and autonomous. It will be AI versus AI.





*Humidifier Vs. Dehumidifier. The Late Night Show with David Letterman, July 5, 1983*



This is a logical extrapolation of where cybersecurity has always been headed. The earliest hacks and protections in the Awesome Nineties were controlled manually. [Kevin Mitnick](#), the hacker, and [Bill Cheswick](#), the hackee, typed into keyboards.

Now—roughly 30 years later—every cyberattack and every cyber defensive platform combines human operation with strong automated controls. For example, TAG Cyber sees that botnets now run via combined human/automated control, as do protection platforms.

And so, perhaps 30 years from now, we should expect to see 100% automated offensive tools targeting 100% automated defensive platforms. And, as with the humidifier and dehumidifier conflict, the humans will watch to see who wins.

This has nice implications. First, it will be a great leveler. The asymmetry between nation-states and corporate targets

could be a thing of the past when both organizations have the same tech. Both big and small teams use the same Windows 365 today, for example.

In addition, AI will drive cybersecurity risk into the same category as, say, physical bank robberies. There will be some incidents, certainly, but the intensity and frequency will drop to a level that no longer requires the same level of attention.

However, because AI will enable creativity, we should expect to see both *malicious* creativity as well as *defensive* creativity. And this, my friends, will be the future of cybersecurity. I think that perhaps we should call this *Cybersecurity 2.0*.

Yes, perhaps in the future humans will use external AI to threaten the normal AI-to-AI combat. Or maybe fake news or outcomes from biased AI will become a new industry. Who knows? But with ongoing advances in AI, this will look nothing like what we have now.



M Y  
T A K E

## CAN AI PROTECT HUMANS FROM HUMANS?

DAVID HECHLER

Since November 2022, when ChatGPT-3.5 was first made available for the public to sample for free, a lot has been written about artificial intelligence, machine learning and that particular product. In addition to the high praise ChatGPT earned, a good deal has been written about its unpredictability, as various journalists probed the recesses of its anthropomorphized “psyche.” When the program seemed to lose its balance during some of these conversations, commentators pointed out that the flaws reflected the fact that the data it’s trained on comes from people. Its unpredictability mirrors ours.



AI has come a long way. It’s clear that programs like ChatGPT will continue to advance rapidly in coming years. It will be much more reliable. That’s a prediction that seems like a sure bet. But what about humans?

We play a pivotal role here, too. And when people write with confidence what we can expect from AI, I’m not sure they take into account our own unpredictability. When we talk about the way AI will shape the world, we have to consider how we shape AI.

The idea that AI will bring an end to cybersecurity in the coming decades seems to rest on several assumptions that may appear to be reasonable. And they may pan out. But I suggest that a review of the recent history of other technological innovations demonstrates the ways in which humans make it difficult to predict the future.

**Sometimes it’s easier to predict the progress of technology than the way humans will respond to it.**



For instance, in early 2020 scientists and governments were scrambling to create medicines that would either immunize populations against Covid19, or at least mitigate its effects on the infected. The great fear was that companies would not be able to produce vaccines in time to prevent millions of deaths worldwide. Almost miraculously multiple companies came through in record time.

Yet, there were still millions of deaths. Why? Some countries refused to accept donated medication because they would not acknowledge that vaccines produced by other countries were more effective than their own. Some countries prioritized treatment of younger citizens, leaving high-risk populations untreated. People from a wide variety of countries—rich and poor alike—posed questions about the safety and efficacy of vaccines. Others raised religious objections. Vaccines became a political football, and many people refused to be inoculated.

The technological challenge, which seemed so daunting, proved to be the easy part. The obstacles were the human responses.

There are reasons to think that our hope that AI will cure the turmoil and conflict that bedevil cybersecurity will prove just as illusory as was our faith in the healing power of vaccines. After all, AI isn't new. Nor is the belief that it will prove to be an increasingly powerful defense against cyberattacks. Part of the problem is that, time and again, **humans** prove to be the weak link in the chain. For example, companies work hard to fortify their perimeter defense. Where do the criminals find holes? **The vast majority of data breaches** are attributable to employees clicking on links in phishing emails.

And every time we think that AI will fix a problem, we find that just as often it's used by adversaries to create one. Our last Quarterly publication showcased a particularly devious variation of phishing attacks. That was the issue in which we wrote about **deepfakes**, which AI and machine learning help create. **Deepfake audios** allow hackers to mimic the voice of a company executive calling an underling with instructions to wire money to what appears to be a business partner's account.

What can make these manipulations so effective is that humans understand the vulnerabilities of their counterparts. The criminal picks out a person who is in a position to wire money and has the authority to do so. Attacks are sometimes timed to catch the victim at a moment of maximum distraction. It could be late on a Friday evening after an exhausting week. And the voice on the phone may be the boss who is out of town—and prone to angry outbursts when his instructions are questioned.

That was just one example. Clever thieves use psychology to steal in all sorts of ways. The successful ones know how to exploit their victims' vulnerabilities. When companies resist paying ransom that criminals demand before unencrypting their data, the bad guys sometimes double down. They threaten to post clients' data on the internet. Sometimes they do it without even a threat, and the clients they pick are celebrities. They used technology as a weapon, but the brains behind these attacks are all too human.

Maybe one day ChatGPT-12 will be able to design—and defend against—these kinds of capers, but they strike me as uniquely human inventions. Humans seem to be in the best position to understand human weaknesses, and to use them to their own advantage. Maybe machines will catch up sooner than I think. But every time we appear on the verge of defeating the latest fad in cyberattacks, the criminals come up with a new play. And it succeeds because it aims not at our machines, but at us.

# WHY AI-BASED CYBERSECURITY WILL CONTINUE TO NEED THE HUMAN TOUCH

DAVID HECHLER

It strikes me as almost a foregone conclusion that artificial intelligence will transform cybersecurity. But it's far less clear, at least to me, whether the result will be a standoff between enemy forces that rely almost entirely on AI defenses.

It seems inevitable that there will be an AI arms race. There already is. The United States and China are the competitors mentioned most prominently in the media. Russia, North Korea and Iran are the other nation-states active in launching cyberattacks. They'll try to match the advances of their targets. Other countries could emerge in coming decades.

It's easy to argue that AI will figure into the equation more and more prominently—on both offense and defense. But that doesn't mean that the machines will be in control. AI will not be calling all the shots. At least not in the foreseeable future. Much about the way the competition evolves will depend upon the humans who collaborate with the technology. Just as it does when AI is used by the military (as I will discuss below).

A lot of the talk right now is about the astonishing technological advances. When the conversation turns to people, they are often engineers who are building the software, and leaders of companies that are funding it—and pushing the competition. These individuals are certainly enjoying a well-deserved moment. But they aren't the only ones who are important players in this realm.

Lawyers, philosophers, journalists, researchers and all kinds of academics have expressed concern about the dangers



AI may pose not only to our country, but to humanity. Far from being seen as our protector against cyberattacks, some people view AI as a grave threat to our future.

A widely cited [survey](#) produced by AI Impacts in 2022 asked researchers who had published papers presented at two large machine-learning conferences this question: “What probability do you put on future AI advances causing human extinction or similarly permanent and severe disempowerment of the human species?” Based on 738 responses, the median respondent said the chance was 5%. But the number that many news accounts cited was double that number because 48% of respondents said the chance was 10%, and that’s the statistic almost everyone used.

“Would you work on a technology you thought had a 10% chance of wiping out humanity?” New York Times columnist Ezra Klein [wrote](#) in March 2023. Klein explained his deep concerns while acknowledging that the train has already left the station. And the challenge of slowing, much less stopping, its progress seems daunting at best. As apprehensions about ChatGPT have mounted, a chorus of voices joined his.

It’s possible that politicians may try to gain some measure of control through legislation. But even if they were convinced of the need, the likelihood of success seems highly problematic. The work is in the private sector, and the funding is from companies like Microsoft, Google and Facebook. So government doesn’t control all the purse strings. And if the government tries to create legal roadblocks, critics will almost certainly accuse it of handing China a devastating, and potentially deadly, gift.

But let’s return to cybersecurity, where the aim is to use AI to safeguard our safety. The machine learning will need to be directed by humans who study the threats and feed relevant information into the technology. In my research, the article I came across that shed the most light on this subject was [Prediction and Judgment: Why Artificial Intelligence Increases the Importance of Humans in War](#), by Avi Goldfarb and Jon R. Lindsay (this is where my earlier reference to the military comes in). Writing in the journal *International Security*, the authors did touch on cybersecurity and cyberwar, but that’s not why I found it relevant. When we’re talking about cybersecurity in the broadest sense—including battles between nation-states—then war is more than an analogy.

Goldfarb and Lindsay don’t address the cybersecurity challenges we’re addressing here, but they do talk about the ways corporations and even doctors use AI. The authors see great value in the technology. They expect it to transform the world in which we live. But they don’t see it substituting for humans. They anticipate a collaborative relationship that builds on the strengths of each. “A well-specified AI utility function has two characteristics,” they write. “First, goals are clearly defined in advance. If designers cannot formally specify payoffs and priorities for all situations, then each prediction will require a customized judgment. This is often the case in medical applications. When there are many possible situations, human judgment is often needed upon seeing the diagnosis. The judgment cannot be determined in advance because it would take too much time to specify all possible contingencies. Such dynamic or nuanced situations require, in effect, incomplete contracts that leave out complex, situation-specific details to be negotiated later.”

**“AI systems can neither design themselves nor clean their own data, which leads us to conclude that increased reliance on AI will make human skills even more important...”**

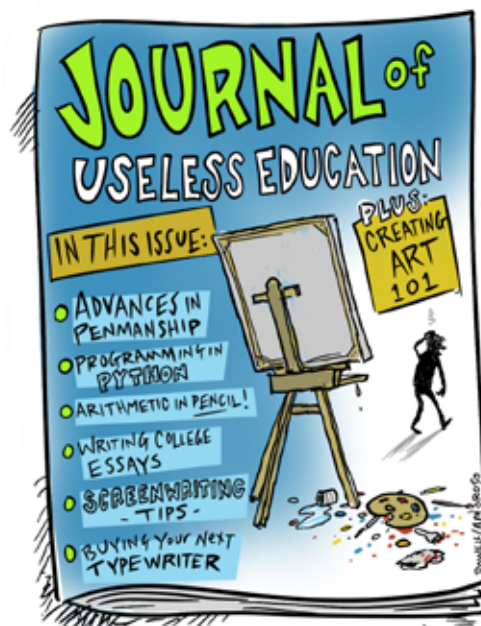


The authors go on: "AI adoption may radically change the distribution of judgment by altering who in an organization makes decisions and about what, but in all cases, humans are ultimately responsible for setting objectives, making trade-offs, and evaluating outcomes.... AI systems can neither design themselves nor clean their own data, which leads us to conclude that increased reliance on AI will make human skills even more important..."

There's another important factor concerning cybersecurity based on AI. The debate over ChatGPT may not involve the government, but the government is very much involved in the world of cybersecurity. And it will inevitably be deeply involved in budgetary and strategic decisions that involve AI. When Goldfarb and Lindsay write that "seemingly trivial procedures can become politicized when budgets and authorities are implicated," it's easy to see how this applies to cybersecurity. "Even in the absence of parochialism," they continue, "the complexity of administrative systems introduces interpretive challenges for personnel."

In the case of cybersecurity, there's plenty of personnel. The Cybersecurity and Infrastructure Security Agency, the National Security Agency and the Department of Justice all play important roles. The heads of those organizations and other appointed cybersecurity leaders don't report to AI. And their judgments affect how AI is deployed. When it comes time for lobbyists and government agencies to press representatives in the House and Senate to approve appropriations for cybersecurity tentatively slated to be included in the annual National Defense Authorization Act, they aren't likely to be glad-handed by ChatGPT.

Finally, let's not forget that the political winds in the United States have been shifting from administration to administration. There are no guarantees that new leaders will continue to support AI or a robust cybersecurity budget. A new administration's strategy could certainly change course. And the same could be true in other parts of the world. As hard as it is to predict the advances of the technology, it can be just as challenging to gauge the path that politics will take.





# THE INTERSECTION OF AI, TRANSPORTATION AND SMART CITIES: CHARTING A SECURE AND ETHICAL FUTURE



CHRISTOPHER R. WILDER

In 2017, I found myself at the epicenter of an emerging technological revolution in autonomous vehicles and smart cities. As an industry analyst, I was collaborating with industry titans like AMD, Hewlett-Packard, Intel, NVIDIA, Kontron AG, Microsoft and other organizations—including government agencies. We were working to create a roadmap for ethical AI principles. Our territory included AI-based automation and generative AI in the transportation and smart city domains. Simultaneously, we were exploring the potential of advanced storage and computing power, which could eventually enable machine and deep learning algorithms to achieve self-awareness. (I continue to advise governments and organizations on deploying next-generation solutions that advance critical infrastructure and communications to improve the lives of the people they serve.)



At this pivotal moment in AI's evolution, examining the ethical and technical challenges and opportunities that AI presents, including the often-overlooked aspect of cybersecurity, seems essential. In this article, I'll delve into these aspects, address key considerations for vendors in this industry, uncover specific ethical use cases and leave you with a few predictions.

## NAVIGATING THE ETHICAL LANDSCAPE: CHALLENGES AND OPPORTUNITIES

Let's look at some of AI's ethical challenges and opportunities in transportation and smart cities, including key concerns like data privacy, bias, job displacement and environmental sustainability.

### THE PROBLEM:

Transportation and smart cities teeter on the edge of an ethical challenge as they rely heavily on vast data from various sources. This data often includes **personal information that can identify individuals**, creating a potential minefield of privacy issues. (For more information click [here](#).)

### OPPORTUNITIES:

- Organizations must strengthen data protection measures and implement anonymization techniques to safeguard personal information.
- They must develop transparent data collection and usage policies to build trust among users.
- They should collaborate with regulators and policymakers to establish industrywide data privacy standards.

### THE PROBLEM:

AI algorithms trained on **partial or inaccurate data** can amplify these flaws, leading to skewed decision-making.

### OPPORTUNITIES:

- Identify and address biases in training data to ensure fairness and equal representation.
- Implement explainable AI (XAI) techniques to enhance transparency and accountability in AI decision-making.
- Foster access and inclusion throughout the AI development process to incorporate various perspectives.

### THE PROBLEM:

The rise of AI-based automation in transportation and smart cities will **displace numerous jobs**, particularly in public transit, trucking and traffic management sectors. (For more information click [here](#).)

### OPPORTUNITIES:

- Develop strategies for reskilling and upskilling workers to prepare them for new roles in an AI-driven economy.
- Collaborate with governments and educational institutions to create job opportunities in emerging fields related to AI and smart city technologies.
- Encourage entrepreneurship and innovation in AI and transportation to generate new employment opportunities.

### THE PROBLEM:

AI applications must be able to **scale and perform efficiently** to meet the demands of growing urban populations and increasingly complex systems. (For more information click [here](#).)



## Building and deploying ethical AI-based solutions requires a comprehensive approach that prioritizes ethics throughout.

### OPPORTUNITIES:

- Leverage advancements in hardware, such as graphical processing units (GPUs) and custom AI accelerators, to improve the performance and efficiency of AI algorithms.
- Adopt cloud and edge computing technologies to optimize resource utilization and reduce latency.
- Develop modular AI solutions that can be easily scaled and adapted to accommodate evolving requirements and technological advancements.

### THE PROBLEM:

As AI-based transportation and smart city solutions become increasingly interconnected, they become more **vulnerable to cyberthreats**. Ensuring the security of these systems is paramount to maintaining public trust and safeguarding the continued growth of AI in these sectors.

### OPPORTUNITIES:

- Implement multilayered cybersecurity strategies, including encryption, intrusion detection and threat intelligence to protect AI systems and the underlying infrastructure.
- Foster a security-focused culture within organizations, emphasizing the importance of cybersecurity at every stage of the AI development and deployment process.
- Collaborate with government agencies, industry partners and cybersecurity experts to develop and adopt standards, regulations and best practices for AI in transportation and smart cities.

## KEY CONSIDERATIONS FOR VENDORS, ENTREPRENEURS AND INNOVATORS

Building and deploying ethical AI-based solutions requires a comprehensive approach that prioritizes ethics throughout. Let's explore some of the key concerns for enterprises, vendors, entrepreneurs and innovators seeking to ensure the responsible use of AI and the promotion of social and environmental sustainability.

### THE PROBLEM:

Innovators, entrepreneurs and vendors must **navigate the rapidly evolving landscape of AI** in transportation and smart cities with their eyes wide open. Further, they must consider several factors to remain competitive, build better products and ensure ethical, unbiased and secure AI solutions.

### OPPORTUNITIES:

- Develop, join and maintain partnerships with various stakeholders, including policymakers, regulators, academics and other industry players.
- Prioritize research and development activities focused on innovative AI solutions that address real-world challenges and enhance the quality of life in urban environments.
- Ensure AI solutions adhere to ethical guidelines built with transparency, accountability and fairness.

- Invest in the education and upskilling of employees to keep pace with the fast-changing AI landscape and maintain a competitive edge in the market.
- Address critical cybersecurity issues by implementing robust security measures and fostering a culture of security awareness within the organization.

## ETHICAL USE CASES AND PREDICTIONS FOR THE FUTURE

As we reflect on the ethical considerations of AI-based solutions, it's important to consider the potential impact on the future. By examining trends and predictions we have seen in the field, we can better prepare our clients for the challenges and opportunities ahead while also focusing on responsible innovation and ethical best practices.

### THE PROBLEM:

The pace of technological innovation continues to accelerate, so it is **critical to consider the ethical implications** of its use. From AI and machine learning to virtual reality and autonomous vehicles, there are numerous areas where organizations must weigh many factors. (For more information click [here](#).)

### OPPORTUNITIES:

- AI-powered traffic management systems can optimize traffic flow and reduce congestion while prioritizing pedestrian safety and accessibility.
- Autonomous public transportation systems can provide equitable access to transport services and enhance mobility for all residents, including the elderly and people with disabilities.
- AI-driven environmental monitoring and management systems can enable more efficient use of resources, can reduce pollution and can promote sustainable urban living.
- Predictive maintenance systems that leverage AI to identify potential infrastructure issues before they escalate can minimize disruption and optimize resource allocation.

As AI technology advances, the transportation and smart city sectors will benefit from this transformative shift. By addressing ethical and technical challenges and embracing AI's opportunities, we can pave the way for our urban environments to have a more secure, efficient and sustainable future.

## EMBRACING THE HUMAN-AI SYMBIOSIS

We must recognize that AI is neither a panacea nor a replacement for human intervention and intuition. While working in the cybersecurity and cognitive computing group at HP Labs, we embarked on teaching drones how to learn and identify bad actors. The science was sound, but we could not decouple the science from the engineering because cognitive computing, much like AI, has no feedback loop. Computers can look at a puppy and a kitten side by side and not determine the difference. They both have immutable traits, such as ears, a nose and a tail, and both are super cute. However, a 2-year-old human child knows the difference immediately because they have a feedback (input/output) loop, while the AI or cognitive computing algorithm does not. We must not discount the disparity between human-AI symbiosis for augmenting common human tasks and capabilities. No amount of algorithm training can replace the human factor, nor should it.

AI will continue to play a pivotal role in shaping the transportation and smart city sectors in the coming years. This evolving landscape calls for a human-AI symbiosis, where technology augments human capabilities, creating a more efficient and harmonious human experience. Below are several areas where AI will both enhance and assist organizations to be better prepared and to respond to threats:

- 1. AI-assisted urban planning** can integrate predictive analytics, citizen input and environmental factors to design sustainable, livable and resilient cities.
- 2. AI-enhanced emergency response systems** can optimize resource allocation, streamline communication and improve overall preparedness during natural disasters or other crises.
- 3. AI-driven public health initiatives** will leverage data analytics, predictive modeling and real-time monitoring to enhance community health, track disease outbreaks and inform public health policies.
- 4. Smart energy grids** powered by AI enable dynamic energy distribution, demand forecasting and optimized utilization of renewable energy sources.
- 5. AI algorithms** automate the tedious and time-consuming tasks involved in SOC operations, such as threat detection, analysis and response. AI can quickly identify potential threats and alert security analysts for further investigation.

## THE ROAD AHEAD

The AI revolution in transportation and smart cities presents immense potential for transforming urban landscapes. It also poses significant challenges that require a proactive and collaborative approach. Stakeholders must foster a culture of continuous learning, innovation and collaboration while actively engaging with regulators, policymakers and the public to create a shared vision. Moreover, interdisciplinary collaboration and ethical AI development are crucial in addressing multifaceted urban challenges and ensuring AI-powered solutions that are secure, transparent and unbiased.

Balancing innovation with moral responsibility is essential, and addressing concerns such as data privacy, bias, job displacement and environmental sustainability is also paramount. As we move forward, embracing a human-AI symbiosis that supports inclusive innovation, prioritizes collaboration and helps build a global AI ecosystem will pave the way for a more secure, efficient and sustainable future.



# A CISO'S TAKE ON NIST'S ADVICE FOR DEALING WITH AI

DR. JENNIFER BAYUK

I speak for many, if not all, cybersecurity professionals in expressing deep appreciation for the efforts of the National Institute of Standards and Technology (NIST) in clarifying industry consensus on practices with which to address cybersecurity issues. So when I received notification from a colleague that a new NIST Artificial Intelligence Risk Management Framework (AI RMF) “may be of use” in answering tough questions about how CISOs should deal with AI, that is all I needed to hear. If Figure 1 had been a dangerous phishing email directed at CISOs, it would have had devastating consequences for our collective reputational risk. I clicked immediately.



Figure 1. Email Notification of NIST AI RMF

Although my contributions to the cybersecurity profession span three decades, my interest in artificial intelligence predates them. In college, I was amazed by the capabilities of **Eliza**, a 1960s version of generative AI whose sole function was psychological counseling. Secretaries in the office where I was an intern would spend their lunch hour discussing their personal problems with it. However, as time went on, the greatest successes in artificial intelligence were in productivity enhancements, not in human chat. My own move from AI to cybersecurity was in the context of detecting intrusions, something far easier to accomplish with AI-based pattern recognition than with humans sifting through logfiles.

## SOCIOTECHNICAL RISK MANAGEMENT

But now my attention has come full circle. Today's growing focus on AI risk has been fueled by perceived advances in generative AI rather than the relatively simple techniques of pattern recognition. While both generative and pattern-recognizing AI use historical data to identify old patterns in new data, generative AI creates new data and uses it to enhance old patterns. By contrast, pure pattern recognition technologies rely on expert feedback to verify the integrity of AI output before accepting any newly introduced data. The difference underscores a weakness in generative AI: It is harder to be intelligent if you are making it up as you go along.



Nevertheless, generative AI has recently been successful in creating the appearance of human intelligence, one of the [guideposts](#) of AI research since 1950. This is a significant shift from the application of AI to assist humans in solving hard problems (e.g. human genome maps) to the creation of autonomous programs designed to replace human activity. The NIST AI RMF appears to have been composed in full appreciation for the fact that tasks performed by AI are trending toward generative. What had once been called research has now been reframed as product development with the goal of human replacement in mind.

Zeal in the pursuit of this goal has led some people to assume that it is straightforward to replace a human with AI. While all systems have an element of such sociotechnology in that they are designed and operated by humans, AI systems lean much farther to the “socio” side of [sociotechnical risks](#) because there are more ways they can be negatively impacted by human behavior. AI RMF highlights the need for guardrails against this potential by pointing out that there are at least 10 job roles that can have an impact on AI behavior. It recommends controls to hold these roles accountable for managing AI risk, and thereby bring the risk to an acceptable residual level. It also observes that third-party providers and even end users may impact outcomes as well.

The AI RMF job roles have names that are familiar, like *design*, *development* and *deployment*. The historical responsibilities of actors working in these areas are to implement specific business requirements developed by subject matter experts. However, when NIST places “AI” in front of these areas, the behavioral aspects of the programs under development come into sharp focus. The AI roles require the job actors to interpret examples of outputs expected by the business users and, to a larger extent, use their own judgement on the margins of error they encounter in testing. Unlike historically straightforward business requirements analysis, AI actor tasks include subjective interpretation of system requirements, such as articulating and documenting the system’s underlying assumptions, interpreting models, combatting harmful bias and regularly assessing the system’s inputs and outputs.

AI RMF addresses this situation with a set of characteristics for “trustworthy” AI (see Figure 2). These include “secure and resilient” as well as “accountable and transparent” AI. As in any risk framework, it emphasizes that there cannot be accountability without transparency. Again, what is unique to AI is that it refers to newly created roles, the AI actors. These pose a new category of internal threat actor. That is, accountability and transparency for the unique activities of AI actors is linked directly to the probability and magnitude of negative consequences caused by AI.

As in any risk framework, [AI RMF] emphasizes that there cannot be accountability without transparency.

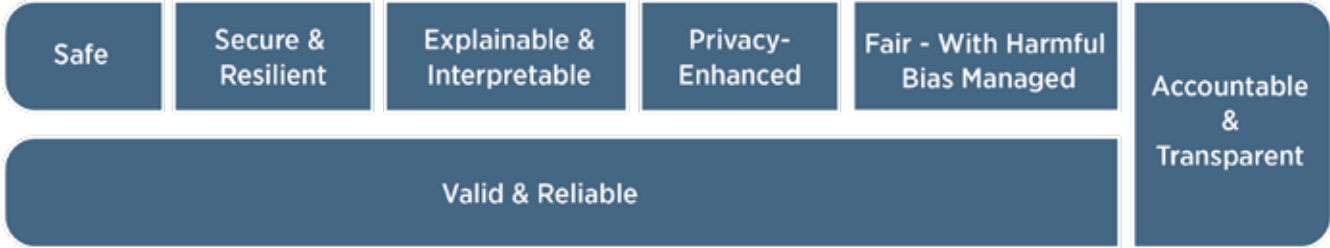


Figure 2. NIST AI RMF Trustworthy Characteristics

## THE ROLE OF CYBERSECURITY

Under the heading of “Secure and Resilient,” AI RMF lists cybersecurity concerns that include standard integrity and confidentiality issues like data poisoning and exfiltration. Data at risk includes, but is not limited to, the models upon which the AI is based, training or live data sets, and intellectual property or proprietary data sources upon which the AI system depends for expertise. AI RMF does not offer special guidance for thwarting these threats other than the [NIST Cybersecurity Framework](#) and [Risk Management Framework](#). However, it does include a supplementary playbook (currently [in draft](#)) that recommends methods to measure AI security and resiliency (see Figure 3). Key among them: “Use countermeasures (e.g, authentication, throttling, differential privacy, robust ML approaches) to increase the range of security conditions under which the system is able to return to normal function.” That is, the advice is not just to detect when the system goes haywire, but also detect if and when each AI actor deviates from its range of authorized activities.

- Establish and track AI system security tests and metrics (e.g., red-teaming activities, frequency and rate of anomalous events, system down-time, incident response times, time-to-bypass, etc.).
- Use red-team exercises to actively test the system under adversarial or stress conditions, measure system response, assess failure modes or determine if system can return to normal function after an unexpected adverse event.
- Document red-team exercise results as part of continuous improvement efforts, including the range of security test conditions and results.
- Use countermeasures (e.g, authentication, throttling, differential privacy, robust ML approaches) to increase the range of security conditions under which the system is able to return to normal function.
- Modify system security procedures and countermeasures to increase robustness and resilience to attacks in response to testing and events experienced in production.
- Verify that information about errors and attack patterns is shared with incident databases, other organizations with similar systems, and system users and stakeholders (MANAGE-4.1).
- Develop and maintain information sharing practices with AI actors from other organizations to learn from common attacks.
- Verify that third party AI resources and personnel undergo security audits and screenings. Risk indicators may include failure of third parties to provide relevant security information.

**Figure 3. NIST AI RMF Playbook of Recommended Security Metrics**

Just as NIST had organized the composition of its Cloud Security Framework (CSF), the AI RMF is a framework of functions supported by categories of actions and outcomes that are expected to facilitate function execution. Figure 4 provides an overview of the four functions (map, measure, manage, govern) that comprise the AI RMF. An enterprise is expected to adopt these functions and customize them in the service of its own risk management goals. The governance and manage functions are relatively straightforward from a cybersecurity perspective. Metrics unique to AI (i.e., the countermeasures in Figure 3) are expected to be used within the AI RMF measure function. The map function is intended to help an enterprise identify risks specific to its own AI use cases. Like the measure function, it includes several elements that are unique to addressing cybersecurity risks related to AI via a focus on AI actor behavior. For example, the map function includes this requirement: “Practices and personnel for supporting regular engagement with relevant AI actors and integrating feedback about positive, negative, and unanticipated impacts are in place and documented.”

## AI Risk Management Framework



Figure 4. NIST AI RMF Functions

Although it may be argued that close engagement with development communities on the topic of negative impact should already be routine in cybersecurity, this had not yet been extended to best practices in documenting risks unique to AI systems resulting from insider threat. Following AI RMF, a good first step for a cybersecurity approach to AI is to list types of system performance impairments, disruption or denial of service due to accidental or intentional harm that could be caused by any one of the full set of AI actors. Such a demonstration may be expected to result in business stakeholder support for technology mechanisms to minimize this risk. Control effectiveness metrics should then be established to demonstrate that it is possible to meet the key metric of detecting all the security conditions that should trigger an AI system's return to normal function. That is, the method of preserving a benign state and reinitializing the system to that state should be tested on a periodic, not just an emergency, basis.

Although these recommendations are set forth in the matter-of-fact tone that all NIST standards share, there is no assumption in AI RMF that the risk management work it endorses will be easy. In the year 2000, **Stephen Hawking was asked to comment on scientific development** going forward. His response was: "I think that the next century [21st] will be the century of complexity." With the advent of artificial intelligence on the desktops of the general public, his prediction has been fulfilled. Up until a few years ago, the management domain of the CISO had been one of the most complicated. It is rapidly becoming one of the most complex.

The difference between complicated and complex has long been a favorite **topic in systems engineering**. Complicated systems can be unfolded or separated into components. They can be understood deterministically, as building blocks. Complex system components cannot be easily unwoven because the behavior of each component depends on the behaviors of the others. A complex system can only be understood through observation of its behavior.

In generative AI, behavior analysis proceeds in multiple stages. It progresses through every AI actor's contribution to the product and then to the product itself. AI RMF calls risk management attention to this progression. True to NIST's reputation for promoting industry best practices, it reflects common **business school advice on managing complexity**. It is an approach with which every CISO is familiar: a "try, learn and adapt" strategy rather than one that assumes problems in the domain can be solved.

## PARTING ADVICE

Cybersecurity has always dealt with sociotechnical elements. As always, a CISO's best defense is a good offense. A CISO's "try, learn and adapt" cycle, developed for similar situations, should be easily adaptable to AI. As the AI RMF recommends, recognize that AI actors are the new breed of DevOps. Use the NIST CSF function to reduce the risk negative impact due to AI actor insider threat as well as AI system activity itself. And, as in any risk management endeavor, never lose focus on a cycle of continuous improvement.

# HOW SHOULD ARTIFICIAL INTELLIGENCE BE REGULATED?



DAVID NEUMAN

Artificial Intelligence has drawn much attention in early 2023, as recent advances that have been made available to sample by the general public, such as ChatGPT, have impressed many people. But the power of AI has left many, including some experts in the field, alarmed. They wonder if the technology can really be controlled by humans. And some have advocated legislation to slow and oversee its rapid advance. We surveyed the landscape and discovered that this effort has already begun.

## FIVE STATES HAVE ENACTED LAWS

Our research found that over the past two years, five states and three cities in the United States have enacted laws designed to monitor or control artificial intelligence. At least another nine states are considering similar legislation of their own. A number of the new laws address the use, and misuse, of facial recognition technology. They also create task forces and agencies to monitor the use of AI and to recommend relevant policy changes.

Since 2021, Alabama, Colorado, and Illinois have enacted laws designed to monitor the use of AI, and ensure it is not used in a manner that infringes on the rights of individuals, while fostering innovation in this rapidly evolving field. Alabama’s **law** limits facial recognition to ensure that it’s not the only basis for arrest. The law prohibits state and local law enforcement agencies from using facial recognition technology to match results, establish probable cause in a criminal investigation or make an arrest. When law enforcement seeks to establish probable cause, they are only permitted to use the technology to match results in conjunction with



**While these laws provide for the general safety and protection of citizens, they do not address all or the more complex uses of AI.**






other lawfully obtained information and evidence established by the state's AI Commission in 2021. The commission also recommends policies to mitigate negative consequences, promote public-private partnerships and advance education and workforce development in AI-related fields.

In 2022, Colorado enacted a [law](#) restricting the use of facial recognition services by state and local government agencies, and temporarily prohibiting public schools from executing new contracts for facial recognition services. State and local agencies that use or intend to use facial recognition services are required to file a notice of intent and produce an accountability report, and are also required to subject decisions that have legal effects to meaningful human review. They must periodically train individuals who use it. Agencies must maintain records to facilitate public reporting and auditing of these policies. In addition, the law restricts law enforcement's use of the technology. It prohibits police from using it to conduct ongoing surveillance, real-time identification or persistent tracking unless they obtain warrants. Agencies must disclose their use of the technology on a criminal defendant in a timely manner before trial. In addition, the law created a task force to study the use of artificial intelligence in Colorado.

In 2021, Illinois enacted two laws. [The Artificial Intelligence Video Interview Act](#) requires employers who rely on AI analysis of video interviews before selecting potential new hires for a second round of in-person interviews to collect and report demographic data about the race and ethnicity of applications not selected for the in-person interviews. The purpose is to ensure that AI has not introduced bias into the hiring process. Employers must report this data to the Department of Commerce and Economic Opportunity. The second law, the [Illinois Future of Work Act](#), created a task force to identify and assess new and emerging technologies—including AI—that impact employment.

**Understanding how AI systems make decisions and operate can be challenging, making it hard to trust them.**



Since 2021, the [law](#) in Mississippi has taken an educational approach. The Computer Science and Cyber Education Equality Act directed the State Department of Education to implement a K-12 computer science curriculum, including artificial intelligence and machine learning instruction. It includes instruction in computational thinking, cyber-related programming, cybersecurity, data science, robotics and related content. It also provides for teacher training, as needed, at all grade levels.

Finally, in 2022 Vermont passed a [law](#) that focuses on oversight of artificial intelligence in state government. It creates the Division of Artificial Intelligence within the Agency of Digital Services to review all aspects of AI developed, employed or procured by the state. The division is required to, among other things, propose a state code of ethics on the use of AI and make relevant recommendations to the General Assembly on policies, laws and regulations.

## THREE CITIES HAVE ALSO WEIGHED IN

In 2021, AI laws were passed in [Baltimore](#), Maryland; [Bellingham](#), Washington; and [New York City](#). Primarily focusing on regulating the use of facial recognition technology, each city addressed the issue in slightly different ways. All three share concerns regarding the potential threats to privacy and civil liberties posed by facial recognition technology. The laws acknowledge the need to protect citizens from potential misuse and biases inherent in the technology, and they regulate or ban the use of certain technologies, such as facial recognition, by law enforcement or government agencies.



## If a pharmaceutical company uses AI to fill a wrong prescription or make a recommendation for an alternative medicine that injures someone, who is at fault?

There are some differences among them. Baltimore implemented a one-year moratorium on using facial recognition technology in its police department and other city agencies. However, its CitiWatch surveillance program, which integrates video footage from public and private security cameras across the city, continues to use facial recognition technology for law enforcement purposes under police supervision. The primary goal of the moratorium is to provide time for the city to study the impact of facial recognition technology, evaluate its ethical implications and develop proper regulations.

Bellingham became the first city in Washington to ban facial recognition technology. The ban prohibits city departments and officials from using it—with exceptions for certain situations, such as unlocking city-owned devices like doors and computers. At around the same time, New York passed the Biometric Identifier Information Law, which requires businesses to disclose the use of

biometric data collection technologies, including facial recognition, to customers. The law also prohibits businesses from selling, leasing, trading or sharing biometric data with third parties without consent.

### WHAT THESE LAWS DO NOT ADDRESS

While these laws provide for the general safety and protection of citizens, they do not address all or the more complex uses of AI. As the technology has become more prevalent, societal and legal concerns have arisen. For example, AI systems have access to large amounts of data, and there is concern that this data could be used in ways that violate people's privacy. AI-based predictive analytics can make inferences about individuals based on their behavior, such as online activity or purchasing history. This can increase the risk of discrimination if AI ecosystems perpetuate and amplify prejudices that already exist in society, such as racial, gender and socioeconomic biases.

Understanding how AI systems make decisions and operate can be challenging, making it hard to trust them. And trust is especially important when safety is paramount—as when artificial intelligence is used in safety-critical applications, such as autonomous vehicles, industrial systems or medical devices. Errors or misinterpretations in these systems can be a matter of life or death.

Then there's the matter of liability. As AI systems become more autonomous, it can be challenging to determine who is responsible if something goes wrong. This applies when AI is used to make decisions. If a pharmaceutical company uses an AI application to fill the wrong prescription or make a recommendation for an alternative medicine that injures someone, who is at fault?

There are also questions about who owns the intellectual property rights for AI-generated works, such as music or art. For example, if AI is used to produce a work of art that becomes very valuable, who owns the rights to that art? More important, what if an AI algorithm uses music or art from multiple sources that are already copyright protected?

Since AI systems rely on large amounts of data, there are concerns about how it is collected, stored and used, who has control over it, and how it is protected. There is a risk that AI systems could be hacked or otherwise compromised, leading to data breaches. Cybersecurity is already a complex and expensive area. It should be integrated into AI systems by design, not added on later.

## POSSIBLE LAWS THAT COULD HELP MAKE AI SAFER

There will be no easy solutions to regulating AI, which is evolving rapidly and will likely continue to do so over the next decade. However, regulating AI in a sector-specific manner could help ensure that it is developed and used in ways that are appropriate and effective for each industry. Here are some examples of sector-specific AI applications that could benefit from targeted legislation.

**Healthcare:** AI is increasingly used to diagnose diseases, develop treatment plans and monitor patients. Regulations could help ensure that AI-based medical devices and software are safe, effective and reliable—and that they protect patient privacy while complying with relevant medical regulations.

**Finance:** AI improves fraud detection, risk management and investment strategies. Regulations could help ensure that AI-based financial systems are transparent, explainable, free from bias and comply with relevant financial regulations.

**Transportation:** AI is used to develop autonomous vehicles, optimize logistics and improve traffic flow. Regulations could help ensure that AI-based transportation systems are safe, reliable and meet relevant safety standards while protecting user privacy and complying with applicable transportation regulations.

**Education:** AI enhances learning, assesses student performance and develops curriculum. Regulations could help ensure that AI-based educational systems are transparent, explainable and free from bias, and that they protect student privacy and comply with relevant educational regulations.

**Manufacturing:** AI optimizes processes, reduces waste and improves quality control. Regulations could help ensure that AI-based manufacturing systems are safe, reliable and meet relevant safety standards, and that they protect worker privacy and comply with applicable manufacturing regulations.

Overall, sector-specific regulations can help ensure that AI is developed and used in ways that are appropriate and effective for each industry, while still providing adequate protection for individuals and society. By focusing on each industry's specific risks and opportunities, targeted regulations can help maximize benefits while minimizing potential harm.

These should be the goals of all future legislation in this area. We are at the early stages of adopting ways to monitor and control this powerful technology. The challenges are many, but the need is immense.

ANALYST NOTE:

# GUIDANCE ON SECURITY ISSUES RELATED TO CHATGPT

DR. EDWARD AMOROSO

---

Enterprise teams are asking frequently about the security risks associated with ChatGPT. While it remains early to provide empirical guidance, this note offers a preliminary glimpse into the types of issues likely to emerge with conversational chatbots. (Warning: This note will not include ChatGPT-generated paragraphs to mischievously demonstrate its capability.)

## INTRODUCTION TO CHATGPT

First, it should be acknowledged that ChatGPT is not synonymous with artificial intelligence (AI), nor does it represent the wide range of chat bots in general. Instead, ChatGPT is an early working prototype of a conversational system from OpenAI that provides human-like responses to questions.

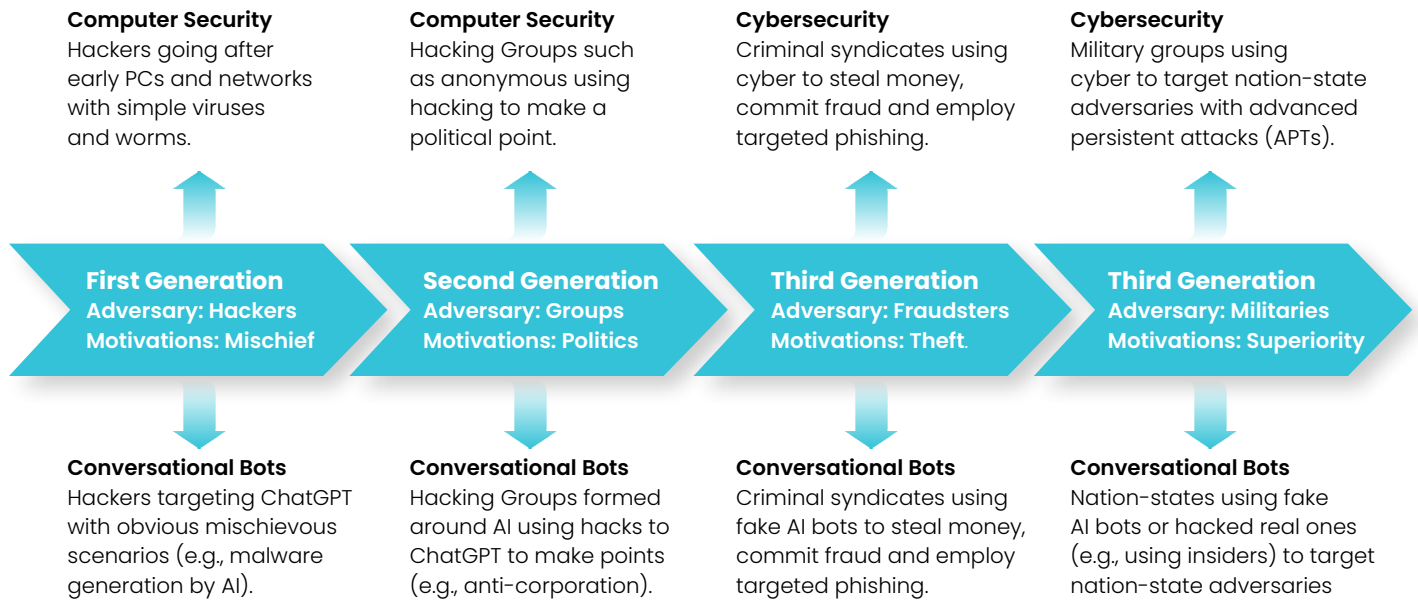
Second, it should be acknowledged that the current capabilities offered by ChatGPT, and other AI-based systems, provide just a glimpse into the future support such systems will provide to a variety of applications, including education, manufacturing, transportation, retail, health care and government.

Finally, it should be acknowledged that every new scientific or engineering advance generates early hype, followed by calm application by engineers and practitioners to integrate the new capability into the right types of usage scenarios. As security experts will attest, however, many fraudulent and criminal use cases often emerge as well.

This note is intended to give readers an early summary glimpse into the security scenarios that will emerge from intelligent AI-based conversational systems such as ChatGPT. We do not include wider applications here such as autonomous machines, robot factory automation and other non-conversational applications. We also focus on what we expect to emerge in the coming years versus the prototype functionality supported by OpenAI today.

## ADVERSARIES AND MOTIVATIONS FOR CHATBOTS

To examine security issues, we must first identify the adversaries and motivations that are likely to arise. To do so, we introduce a model that mimics the progression of adversaries and motivations that were present for computer security (now cybersecurity) during its first few decades of relevance. The model is shown below:



**Figure 1. Adversary and Motivational Model for Conversational AI Chatbots**

Two points are worth highlighting: First, it is likely that fake conversational AI bots will soon emerge that cannot be trusted. An entire infrastructure will be required to help people steer clear of fake systems so that they can stick with real ones. These fake bots will be domain specific, with answers to various useful topics (e.g., health) and questionable ones (e.g., porn).

Second, it is likely that the existing infrastructure at OpenAI is insufficient for the barrage of security issues that will emerge in the coming months. No company that goes from few users to many millions in such a short period of time can ever deal with such growth without massive security vulnerabilities.

Observers must not associate any security weaknesses in the OpenAI infrastructure as an indictment of AI or conversational bot security. Rather, this should be interpreted as the growing pains of a company evolving at an unprecedented rate. Hopefully, the OpenAI team will work quickly to establish a security infrastructure.

## SECURITY ISSUES OF CONVERSATIONAL CHATBOTS

The ten issues listed below represent an early glimpse into the types of security issues that will emerge with conversational chatbots. The summary is guided by underlying models such as the well-known CIA model of cybersecurity, and includes reference (during list development) to other models such as MITRE ATT&CK.

The descriptions here are high-level, so developers might find the discussion too abstract to put into immediate practice—although starting with high-level views is better than diving into the minutia anyway. Our hope is that this note helps to establish useful dialogue as this issue drives security initiatives, and the inevitable security attacks, to systems such as ChatGPT.

### ISSUE 1: AVAILABILITY ATTACKS

Businesses that are now beginning to depend on ChatGPT and similar services might be used to the robust search network infrastructure created over decades by Google. It seems obvious that DDOS attacks targeting OpenAI should now work, so be warned that establishing your new business operations practice around ChatGPT could result in outages.

## **ISSUE 2: FAKE CHATBOTS**

Now that ChatGPT has taken the world by storm, we should expect to see one after another competing conversational bots being produced by companies, search firms, and yes—fraudsters. We will need to begin training employees to be careful, and some sort of DMARC-like infrastructure will be needed to ensure the authenticity of any bot service.

## **ISSUE 3: OUTPUT CORRUPTION**

Business models will probably drive “intentional corruption” of output to perhaps list some firm that has paid money to be the first example in those little bullet lists that are so common in chatbot output. And we all know that what can be done intentionally can be done maliciously. Watch for hackers trying to use crafted data to train weird or biased output from bots.

## **ISSUE 4: INSIDER ATTACKS**

The sad fact is that nation-state adversaries will begin targeting successful firms such as OpenAI to integrate insiders into their working operational teams. Anyone working in critical infrastructure knows this to be true, despite any public pronouncements to the contrary. We should expect to see insider threats emerge from the most prominent firms in this area.

## **ISSUE 5: MALWARE GENERATION**

The potential to generate code implies the potential to generate bad code. And the potential to generate bad code implies the potential to generate malware. It is impossible to imagine that the technology will not move in this direction, probably with malware generators located on the Dark Web and accessible via Tor. This will happen quickly.

## **ISSUE 6: SOCIAL ENGINEERING ATTACKS**

The use of fake chatbots will provide a fertile breeding ground for misdirecting users to fake sites, fraudulent businesses and other dangerous destinations. It will soon become an art to determine how to safely use the output from a conversational chatbot to ensure that one is not being misdirected or tricked.

## **ISSUE 7: BIDIRECTIONAL CONVERSATIONS**

The current one-way “user-to-ChatGPT” conversation that exists will quickly merge into one where the conversation is much more real-time and bidirectional. This will give chatbots the ability to guide users in the direction of spilling lots of information—and the AI will know how to do this (e.g., using learned methods from the greatest interrogators who ever lived).

## **ISSUE 8: SUPPLY CHAIN SECURITY**

The usual problems associated with software supply chain will emerge quickly into the conversational chatbot space. Maybe SBOMs will help, but the truth is that we will probably not have a clue as to the software packages and interconnections that exist behind the bot we are using. The situation will be somewhat akin to the confusion that exists with TikTok.

## **ISSUE 9: MILITARY USE**

Current conversational bots like ChatGPT have limited use for military attackers, but expect to see data harvesting by nation-states as a means for informing their intelligent weapons. That conversational bot recommending good places to go skiing in Utah might actually be run by an adversary nation-state trying to learn more about your habits and whereabouts.

## **ISSUE 10: MALICIOUS TEXT**

There is a science to generating spam or phishing text, usually with intentionally introduced misspellings. This is done to weed out the intelligent recipients and highlight the true dummies who will follow the scam to completion. It is likely that chatbots will help optimize such text for email usage. So expect to see phishing attacks get better soon.





**INTERVIEWS**



AN INTERVIEW WITH ANIL MARKOSE,  
CHIEF STRATEGY OFFICER, ABACODE

## ALL-IN-ONE CYBERSECURITY AND COMPLIANCE FROM ABACODE

Companies of all sizes need to fend off an ever-increasing barrage of sophisticated cyberattacks, while also dealing with a growing number of state, federal and industry compliance regulations. This somewhat overwhelming double whammy is eating up an incredible amount of time and resources. Luckily, Abacode comes to the rescue with their Managed Cybersecurity and Compliance Provider (MCCP) Core Program, which tackles both of the above issues. We were happy to talk with the company to learn how their solution helps organizations achieve both continuous cybersecurity and compliance.

**TAG CYBER:** *How do you help companies outsource their cybersecurity and compliance programs?*

**ABACODE:** The cybersecurity industry has become overly complicated. With everything connected or as a service, the surface area keeps growing, while attacks continue to increase in complexity. Moreover, customers are pitched a seemingly endless number of tools and widgets. For most organizations, cybersecurity is a very large cost, with a low or unknown return on investment. In addition, regulated customers need to worry that a state of non-compliance could actually be revenue blocking and catastrophic. Our goal is to simplify the complex world of cyber for our clients. We work directly with members of the C-suite to understand their business goals and compliance requirements. Companies need to work their way up to a high maturity level, so we guide them through a “crawl, walk, run” journey, which ramps up based on their current state of maturity. Security is not a one-size-fits-all solution—if it were, it would be easy! We help our clients build the right program to quickly get to a state of continuous cybersecurity and compliance.

**TAG CYBER:** *What specific benefits do you provide to small businesses, mid-market companies and enterprise customers? How does your approach differ for each of these segments?*

**ABACODE:** Most of the time, the difference between a small, mid-market, or enterprise client is their access to budget and cybersecurity talent. However, we know all these companies face similar compliance bars and cyberthreats. An attacker does not discriminate; everyone is fair game. Our clients are trying to achieve a similar

**Regulators increasingly demand that organizations prove a degree of cybersecurity maturity tied to compliance with best practices. This is what we mean by the convergence of cyber and compliance.**



outcome: a continuous state of compliance and cybersecurity that is right-sized for their risk profile. However, the approach to achieve that outcome may be different, depending on size. A small company may need to outsource more to us compared to a larger enterprise client. A large enterprise may have legacy capabilities we need to integrate, while a smaller company could be a blank sheet of paper. Our MCCP Core Methodology allows customers to grow into their needs as they partner with us. As a starting point, we leverage everything they bring to us to establish a common understanding of the outcome and goals we are working towards.

***TAG CYBER: Tell us more about MCCP Core. How does it help customers?***

**ABACODE:** MCCP Core is a holistic “stack” of cybersecurity and compliance capabilities that are combined into one integrated, managed program. Regulators increasingly demand that organizations prove a degree of cybersecurity maturity tied to compliance with best practices. This is what we mean by the convergence of cyber and compliance. MCCP Core allows customers to have all the necessary components in a managed program with an underlying methodology. We use this approach to quickly ramp them up to a full state. Our clients achieve their compliance goals four-times faster when compared to many stand-alone compliance programs that lack programmatic integration, thereby reducing up to 30% of overall budget.

***TAG CYBER: How do you assist with government, risk management and compliance (GRC) readiness?***

**ABACODE:** GRC is a component of MCCP Core. We think of it as an overarching governance structure, providing the ability to prove controls are in place and working correctly in a security program. We integrate these GRC capabilities into the cybersecurity program, so it’s not an afterthought just to get through audits. A mature cybersecurity program should have the right level of governance, metrics and inspection to ensure it’s working as intended, which is core to achieving a continuous state of readiness. We help clients build a risk-based cybersecurity program for their business, but we know the program must also stand up to scrutiny and inspection. Therefore, GRC is an integral part of MCCP Core.

***TAG Cyber: We’d love to get your take on any important trends you see in enterprise cyber security, offense and defense, along with any advice you might have for practitioner readers.***

**ABACODE:** A big trend we are very concerned about is third-party risk. Many small to mid-market companies are third parties to large enterprises; there could be thousands of companies in a trusted eco-system providing sensitive data-related

services to each other. This is essentially an extension of the attack surface that most companies have no visibility over, as evidenced by an increasing number of supply chain attacks and ransomware incidents. The current approach of using point-in-time questionnaires or relying on stale attestation reports is not fit for purpose. Risk scoring services that look at companies externally and draw some conclusions are a great starting point, but they create a lot of false positives and “boy who cried wolf” type credibility issues for cybersecurity teams. We continue to advocate for the need of continuous compliance, which requires real instrumentation within an ecosystem to know if a friendly partner is now a compromised launchpad for the next attack. We expect the compliance bar to rise in this area over the next few years and the only right answer is continuous visibility into a third-party’s entire ecosystem with real-time data.



*“Next time, you’ll be more careful with that algorithmic bias.”*





AN INTERVIEW WITH KARTHIK KANNAN,  
FOUNDER AND CEO, ANVILOGIC

## AI-DRIVEN THREAT DETECTION FROM ANVILOGIC

---

Even with all the latest advances in technology, threat detection can still be a slow, manual process filled with a flow of chaotic alerts. Anvilogic's SOC platform automates threat detection, investigation and hunting, so that the time between threat and detection is reduced to mere minutes. Moreover, through the use of AI, this unified solution helps eliminate many manual tasks in the detection process. Anvilogic recently took the time to meet with us and explain the unique features of its SOC platform and how cybersecurity teams can get executives to invest more in their SOC efforts.

**TAG CYBER:** Describe to us your unique approach to the security operations center (SOC) lifecycle.

**ANVILOGIC:** Instead of taking days, our AI-driven SOC platform helps security operation teams perform automatic threat detection, investigation and hunting in minutes. Our unique approach to the SOC lifecycle combines proprietary detection and enrichment frameworks, a no-code builder, and visual hunting and triage workflows, thereby empowering teams with unmatched continuous security. Our SOC lifecycle approach also merges human expertise with artificial intelligence, streamlining the threat detection process and providing actionable insights for deliberate incident response. The platform queries data from a company's distributed environment, eliminating the need for normalization or knowing different search languages. It also centralizes data into a single repository. Moreover, it delivers detection across logging platforms and alerts in one unified platform. With over 1,000 ready-to-deploy detection rules and trending topics backed by our Purple Team, the Forge, we offer advanced threat detection capabilities that eliminate manual hours spent researching, testing, and documenting detections. Additionally, our hunting framework identifies suspicious activity, sends significant alerts for triage and investigation, and enriches data to identify and remove false positives or unwanted alerts. Machine learning trained by threat hunters identifies suspicious patterns and events, instead of raw data to enhance existing hunting resources and highlight suspicious behavior.



One major issue is a communication gap between CISOs and other executives when it comes to understanding the importance of SOCs in both mitigating business risk, as well as having a direct impact on driving revenue.



**TAG CYBER:** *How does your solution implement AI-driven recommendations to assist in threat detection, investigation, and hunting?*

**ANVILOGIC:** Organizations need a method to ingest, enrich, and correlate alerts across disparate systems, as the number of managed solutions grows. By automating the time-consuming manual tasks of fine-tuning alerts, creating whitelists, and prioritizing observations, investigations become more straightforward, and organizations can save precious time during cyberattacks. With our unified threat detection process across hybrid logging platforms, teams can go from threat to detection in minutes. By leveraging AI-driven recommendations, our platform focuses on purposeful remediation steps, eliminating manual efforts to tune and maintain detections—all while encouraging collaboration across existing security operation teams. Detection engineering now has a co-pilot, thanks to our AI-powered recommendations for automated tuning, maintenance, and health monitoring insights. For more detection customization, our no-code scenario builder allows a company to correlate threat identifiers to form a threat scenario, thereby creating more flexibility to detect sophisticated threats and behavioral attack patterns based on the MITRE ATT&CK framework.

**TAG CYBER:** *Why do security operation centers generate such massive amounts of chaotic signals? What is the impact of these signals, and what can be done to improve the situation?*

**ANVILOGIC:** We've reached a tipping point in the world of security. Environments become chaotic, and requirements constantly change. The SOC is overrun with alerts, and SecOps teams spend too much time dealing with noisy signals and alerts. The art of detection engineering demands change. Our solution helps teams pinpoint the critical alerts through the noise with behavioral attack pattern detections driven by AI recommendations and frameworks. With Anvilogic, teams can continuously assess, prioritize, detect, hunt, and triage to mitigate risk. Data ownership costs are minimized, and security teams are empowered to respond to the incidents that matter most.

**TAG CYBER:** *Can you highlight the various integrations that work with Anvilogic and what benefits they provide?*

**ANVILOGIC:** Our solution unifies alerts by facilitating improved detection, investigation, hunting, and triage. The platform seamlessly integrates with the technologies producing alerts and signals used by a SOC team daily via API, allowing for easy normalization and navigation across all the signals,

workflows, and threat patterns in a company's cloud and hybrid ecosystems. By leveraging Anvilogic, an organization doesn't have to learn new languages and can leave its data on whatever logging platforms or data lakes it uses. The platform searches and queries across all data to bring in only the relevant signals and alerts, making it easy to unify detections across all signals. Our platform also helps teams adopt the best data strategy for their unique environment. Suppose you're adopting a security data lake strategy, as with Snowflake. In that case, the platform can help bridge legacy enterprise tech stacks to modern cloud architecture, reducing costs while improving security coverage across hybrid, multi-cloud environments and security data lakes. SOCs also can reduce the complexity of logging platforms like Splunk, helping to simplify data navigation and enhance the understanding of critical data. Teams that leverage multiple platforms or are going all-in on one (such as Azure, for example) leverage our platform to gain better visibility and improve enrichment, detection, hunting, and triage capabilities across their tools while maximizing the value of existing investments. Additionally, we offer thousands of customizable pre-built detections and AI-driven recommendations to help manage and guide security operations across on-premises, hybrid, and data lake environments.

***TAG Cyber: We'd love to get your take on any important trends you see in enterprise cyber security, offense and defense, along with any advice you might have for practitioner readers.***

**ANVILOGIC:** Security teams are facing significant challenges in keeping up with the pace of business risk mitigation. As a result, they are being forced to make difficult decisions that compromise their efficacy and efficiency. Nearly **all security professionals are making tradeoffs** to keep up with the demands of their job, and many believe that a moderate or transformational change is needed to continue mitigating business threats in the coming years. In this age of data-driven decision making, cybersecurity is essential for ensuring the accuracy and integrity of business-critical information. By investing in cybersecurity, businesses can make better decisions and ultimately drive revenue growth. One major issue is a communication gap between CISOs and other executives when it comes to understanding the importance of SOCs in both mitigating business risk, as well as having a direct impact on driving revenue. Cybersecurity teams will have better buy-ins from an organization if they have the ability to show how cybersecurity can boost revenue. Being able to clearly measure, report and maximize returns on investment help

Line of Business (LOB) executives understand that robust cybersecurity measures help the company build trust with its customers, protect its reputation, and ultimately increase revenue by driving customer loyalty and attracting new business. Teams that take a holistic approach to cybersecurity by integrating it into their overall business strategy are the ones that will improve operational efficiency, reduce risk, and amplify revenue growth. Another challenging newer trend is the skills gap within SOC teams, particularly in alert tuning and investigation. The detection lifecycle is also too lengthy, taking a week or more to identify the need, develop the detection, test it, and deploy it. Many organizations have only one person dedicated to threat engineering—or none at all. To address these challenges, it is necessary to democratize threat detection throughout the SOC. This facilitates threat detection across hybrid, multi-cloud, and data lake environments, thereby enabling organizations to optimize their detection engineering investments.



*“You may have hated this but it got a thousand likes on Instagram.”*



AN INTERVIEW WITH DROR DAVIDOFF,  
CEO AND CO-FOUNDER, AQUA SECURITY

# CLOUD NATIVE APPLICATION PROTECTION FROM AQUA SECURITY

When data assets and software began shifting to cloud environments, major new security issues soon became evident. Aqua Security was one of the first companies to identify the crucial need to develop an entirely new approach to cloud-native security. Since 2015, they have been leaders in the battle to protect cloud-native environments—and back up their expertise with a \$1M guarantee. We were happy to talk more with Aqua Security to learn about the unique requirements of cloud security and their approach to see and stop threats across every phase of the software development lifecycle.

**TAG CYBER:** *What is a cloud native application protection platform (CNAPP), and how does it differ from traditional approaches to cloud security?*

**AQUA SECURITY:** At Aqua, we often like to explain it backwards to simplify how to think about it. A CNAPP is a platform that protects applications in cloud-native environments. It is a category of security solutions that helps identify, assess, prioritize, and adapt to risk in cloud-native applications, configurations, and infrastructure. Unlike traditional approaches to cloud security, the goal of a CNAPP is to provide complete end-to-end security for cloud-native environments. CNAPPs should have the capabilities of several existing cloud security categories, mainly “shift left” artifact scanning, cloud security posture management (CSPM), Kubernetes security posture management (KSPM), infrastructure-as-code (IaC) scanning, cloud infrastructure entitlements management (CIEM), a runtime cloud workload protection platform (CWPP), and software supply chain security capabilities. From the beginning, our vision has been to deliver a single end-to-end security solution for the entire cloud-native application lifecycle in one holistic platform. We’ve always believed that to be a true CNAPP, a solution must include shift-left scanning, broad visibility, and crucially strong runtime controls that can detect and stop attacks in progress. Aqua offers the industry’s first and only unified cloud-native application protection platform. Our cloud security platform provides users with better context and prioritization when identifying threats to secure and protect cloud-native assets in real time from day one.

While most cloud breaches once resulted from cloud account misconfigurations, organizations have improved their security posture for cloud infrastructure, and now attackers have increasingly turned to exploiting vulnerabilities in cloud workloads.

**TAG CYBER:** *You recently launched a new solution to stop software supply chain attacks. Can you tell us more about it and what it does?*

**AQUA SECURITY:** High-profile cyber incidents, such as the infamous SolarWinds or SUNBURST attacks, have directed attention to the resilience of supply chains. These attacks demonstrated how vulnerabilities in third-party products and services can be exploited by cybercriminals to affect hundreds of thousands of organizations at the same time. As a result, software supply chain attacks are dramatically on the rise; our data shows a 300% increase year-over-year. This type of threat is now recognized as a security priority, including to the White House, which recently released executive orders to enhance software supply chain security. In September 2022, we released the industry's first, and only, end-to-end software supply chain security solution as part of our fully integrated CNAPP, thereby enabling DevOps teams to implement security throughout the software development lifecycle (SDLC), so they can proactively prevent and stop supply chain attacks on cloud-native applications. We identify software supply chain risks as threats coming from third-party artifacts, open-source dependencies and malicious actors targeting the unique developer toolset and environment. These capabilities make ours the only solution on the market that protects against supply chain risk, from code all the way through to runtime, across both the application and underlying infrastructure.

**TAG CYBER:** *You back your CNAPP with a \$1M Cloud Native Protection Warranty. Tell us more about this feature.*

**AQUA SECURITY:** As cloud-native applications are used for more and more business-critical applications, securing these applications is paramount. Traditional security tools have proven ineffective at protecting cloud-native environments, and recent research from Aqua Nautilus has shown that it takes less than 20 minutes to compromise a vulnerable cloud-native workload. Production workloads are the crown jewels in cloud-native environments, and that's what attackers are after. We are the only vendor that can thwart attacks across the entire development lifecycle, stopping them when they matter most: in production. The best way to demonstrate confidence in our platform is to put our reputation on the line with a warranty. No one else in our space can make this claim. Our warranty is available at no cost to all customers who have fully deployed the Aqua Platform and will pay up to \$1M USD in the event of a proven successful attack.



***TAG CYBER: Aqua is a pioneer in cloud security. How has the cloud cyberthreat landscape changed over the years, and how does your long-standing involvement in the sector help you meet today's challenges?***

**AQUA SECURITY:** While most cloud breaches once resulted from cloud account misconfigurations, organizations have improved their security posture for cloud infrastructure, and now attackers have increasingly turned to exploiting vulnerabilities in cloud workloads. We are seeing advanced cloud workload attacks that are in-memory or leave no trace on the workload's filesystem. We have also witnessed a rise in software supply chain attacks in recent years, and we now even see attacks on the development environment itself. All these attack vectors illustrate the need for a full application lifecycle approach to security—an approach we take at Aqua. We remain on the forefront of these evolving attacks with Aqua Nautilus, the world's only dedicated team of cloud-native security researchers. With a global network of honeypots, Nautilus catches more than 80,000 cloud-native attacks every month, specifically those unique to containers and microservices that other platforms lack the visibility to see. Nautilus uses eBPF to study patterns of executing processes in Linux kernels. It then defines behavioral attack signatures and codifies them into Aqua products so that customers can be protected out of the box, without even understanding the specifics of cloud-native attacks. Each month, Nautilus also finds tens of thousands of instances of in-memory and fileless attacks that wouldn't be seen or stopped without kernel-level visibility. As a result of ongoing research by Nautilus, Aqua has written and implemented over 200 behavioral signatures in its products to protect its customers to date.

***TAG Cyber: We'd love to get your take on any important trends you see in enterprise cyber security, offense and defense, along with any advice you might have for practitioner readers.***

**AQUA SECURITY:** Enterprises have been navigating misinformation about visibility and image snapshots, and now the truth is becoming clear; the reality is you can't see 100% of what is going on in your cloud with image snapshots. Enterprises need next-generation cloud security to be able to see all of what is happening in their cloud—from code and development to running workloads. And subsequently, they also need the ability to stop attacks. Aqua sees more and stops what others can't. We better prioritize, ultimately reducing workloads and automatically stopping attacks. This is the future of cloud-native enterprise security.



## AN INTERVIEW WITH THOMAS "TJ" JERMOLUK, CEO, BEYOND IDENTITY

# BEYOND IDENTITY'S ZERO TRUST AUTHENTICATION

It is estimated that 85% of cyberattacks start with stolen credentials. While passwords make businesses vulnerable to hacks, multi-factor identification (MFA) can be cumbersome and time-consuming for employees, often requiring multiple devices and one-time passcodes.

Beyond Identity offers a password-free, frictionless MFA solution that can be used in the workplace, as well as by remote workers, contractors, consultants and BYOD devices. This greatly protects an enterprise from phishing, ransomware and other attacks. It also makes the log-in process easier, cutting down on the support time needed for access issues and forgotten passwords. We recently talked with Beyond Identity to discover more about how their solution works, along with its advantages.


### ***TAG CYBER: What is Zero Trust authentication and what are its benefits?***

**BEYOND IDENTITY:** Zero Trust is a next-generation, multi-factor authentication that uses continuous, policy-based user and device verification to harness just-in-time signals from the components of an enterprise security stack, including mobile device management tools; endpoint detection and response solutions; and VPN and ZTNA systems, to name a few. In this way, it "shuts the front door" to suspicious users and dubious devices. This solution is based on private-public key cryptography rather than passwords and codes, so no information moves over the wire that can be phished. Moreover, MFA can be delivered with multiple factors from a single device, ending the need for users to juggle multiple devices in order to have multiple factors for authentication. The biggest benefit of our solution is that it enables security and IT teams to close the biggest security vulnerability—authentication via stolen credentials and compromised devices. This subsequently shrinks the attack surface that is available to hackers. For once, companies get to ratchet up security standards for their entire user population, while simultaneously making the user experience better. As every CISOs know, this is a rare occurrence, indeed!

### ***TAG CYBER: How does your solution secure remote workers and BYOD devices in a Zero Trust framework and why is it better than a VPN?***

**BEYOND IDENTITY:** One strength of our solution portfolio is its ability to increase confidence in user identity, thereby ensuring the security of the devices they use to access corporate assets. We provide full device fleet management, so

CISOs and their teams are beginning to realize that any old MFA simply isn't good enough. It is failing them on both the security front, as well as the usability front.



that IT teams can view and control what devices an individual user utilizes, while also binding the user's identity to those devices in a chain of trust, so that every action is verified and logged. Our solution is not a replacement for a first-generation VPN, a second-generation secure access service edge (SASE) or Zero Trust network access (ZTNA) solution. Instead, our solution complements the above technologies by continuously authenticating identities to these systems so they can broker access to applications with high confidence in the users, as well as the security of the device, before allowing them to reach key corporate applications and assets. It also continuously verifies them during the full duration of a session.

***TAG CYBER: How does Beyond Identity streamline the log-in process for end users? What is their log-in experience?***

**BEYOND IDENTITY:** First-generation MFA tools mistake multiple devices for multiple trusted factors, and transported credentials and codes over the wire, which were often picked off by hackers. We provide multiple secure factors on a single device, so users have a secure single-device MFA that transports no phishable factors over the wire. Users simply use a biometric, such as facial or fingerprint recognition, and are authenticated frictionlessly and without a password.

***TAG CYBER: What about admins? Is your authenticator relatively easy to use and manage?***

**BEYOND IDENTITY:** Behind the scenes, our cloud-native service matches a user's private cryptographic key to the public key in our cloud, processing just-in-time user and device signals to ensure that users are trusted, along with their behaviors and devices. It then passes authenticated, secure users to the application, single sign-on engine, or access broker. The IT department retains complete control over the devices allowed for use, as well as the applied policies that ensure secure access, and all authentication transaction records for forensics and compliance. While policies can be an intimidating concept, these are simple drag-and-drop rules that can be applied to different critical user populations—for example, one policy for executives, one policy for contractors, and one policy for regular, full-time employees. Our customers often use policies to monitor an entire fleet of devices accessing systems. This further ensures that device security controls, such as firewall and encryption, are configured properly to guarantee safe access.

***TAG CYBER: We'd love to get your take on any important trends you see in enterprise cyber security, offense and defense, along with any advice you might have for practitioner readers.***

**BEYOND IDENTITY:** CISOs and their teams are beginning to realize that any old MFA simply isn't good enough. It is failing them on

both the security front, since traditional MFA is easily hackable, as well as on the usability front, since MFA is rolled out to far below 30% of a user population, on average. Yet, entities—from the White House and New York Department of Financial Services to SaaS leaders and cyberinsurers—are asking for a complete rollout and movement to tools that can't be easily phished. MFA-based hacks were the story of 2022 (e.g., Uber, Cisco, Twilio, etc.), so clearly it's time to at least look at the successes and challenges that legacy MFA has generated in an organization and whether taking advantage of a newer, cryptographic, frictionless approach, such as the one we provide, can better serve a workforce and its customers.



*"I believe I now understand the true downside risk of AI."*



AN INTERVIEW WITH ANDY LUNSFORD,  
CO-FOUNDER AND CHIEF EXECUTIVE OFFICER,  
BREACHRX

## AUTOMATE INCIDENT RESPONSE AND READINESS WITH BREACHRX


In today's fast-evolving business landscape, companies not only need to stay on top of responding to the latest cyberthreats, but also have to deal with an ever-increasing pile-on of regulatory and contractual red tape with ever-decreasing response times. Making things worse, incident response and compliance are still often done manually. This is where BreachRx steps in with their automated, dynamic response plans that are custom made for each incident and each's organization's specific needs. We enjoyed discussing their solution at length, and how it helps streamline the incident response process.

**TAG CYBER:** *How does the BreachRx platform help streamline the chaos of incident response and management?*

**BREACHRX:** We founded BreachRx to help companies take back control of incident response. Incidents lead to chaos at most companies, given the complex set of processes that are typically underplanned and ineffectively practiced. Most organizations take a "wait and see" approach, relying on a static paper incident response policy and plan that might be updated or reviewed once a year, and often isn't even opened when incidents actually occur. And while they might have a handle on the technical security processes, most wave their hands at the other, more expensive aspects of incident response. Many leaders we talk to are surprised to learn that only about 30% of the cost of an average-sized incident is the security response. When the inevitable occurs, the key to a successful outcome is readiness. That's where the BreachRx platform comes in—it guides organizations by proactively preparing them for what we call integrated incident response, meaning a repeatable response that includes all aspects, teams, and stakeholders needed to effectively respond to incidents. We replace the legacy plan with intelligent automation by generating tailored response plans that are specific to that organization. The details of each incident are broken down by task and organized by phase, with deadlines. As an incident evolves, the platform adjusts the work required dynamically, bringing in new tasks as necessary and eliminating tasks that are no longer relevant. Our platform gives teams a safe haven to



Many leaders we talk to are surprised to learn that only about 30% of the cost of an average-sized incident is the security response.



operate and collaborate, while protecting legal privilege. We generate audit logs and incident reports automatically based on the actions a company has taken, so teams aren't digging around post-incident trying to figure out what they did.

***TAG CYBER: How are increasingly complex cybersecurity and privacy regulations, data breach directives, and compliance requirements affecting cybersecurity, and what can a company do to stay on top of things?***

**BREACHRX:** There are now over 180 regulations in over 120 countries related to cybersecurity and data protection, with more coming at a fast rate. Requirements can be onerous. Besides short deadlines of three-to-four days for regulatory notification, we're seeing potential penalties reach up to 10% of an organization's global revenue. The "best practice" for teams is throwing people at the problem, as well as using spreadsheets, documents, calls, and manual reviews, which clearly don't scale to meet the pace needed for such short timeframes. In addition, larger companies are demanding their suppliers and partners demonstrate security, leading to an onslaught of compliance requirements, spreadsheets, and huge questionnaires, all of which are now familiar to the CISOs and security compliance teams who must answer them to stay in business. In this day and age, it's remarkable how few teams address these problems with automation—particularly the privacy, legal and compliance aspects of incident response. Teams across the business need to know what applies to them and subsequently follow the shifting landscape. Our platform was purpose-built to fill that gap, and our regulatory and compliance libraries make it easy for companies to go from no coverage to full coverage overnight. One further recommendation: Don't assume it's taken care of, as there are myriad examples of breached companies where one team thought the other was prepared, but they weren't. Security and legal leaders need to work closely together to stay on top of this, or else it will be expensive chaos when an incident does occur.

***TAG CYBER: How does your platform help an enterprise take a proactive, as opposed to reactive, approach?***

**BREACHRX:** Our platform gives teams a place where they can pull together everything needed for an incident. Our customers think of our platform as their incident response hub, and our automated workflows help teams easily pull all an organization's requirements and efforts together into a single system of record that's easy to maintain. We provide our customers with libraries of regulatory and compliance requirements, playbooks, and procedures for a wide range of security and privacy incidents. We also make it easy for customers to capture their cyber insurance requirements, contractual terms, and any other obligation or task that needs to be accomplished if an incident or data breach occurs. This integrated

platform approach makes it extremely straightforward for our customers to demonstrate they have a best-in-class incident response program that exceeds the criteria of many of the top global voluntary and externally audited compliance frameworks, such as SOC 2, ISO 27001, CIS Controls, and NIST CSF. We've built automation workflows and tests for onboarding that guide customers through what's needed to achieve rapid compliance; we've had customers get fully prepared in under a week.

***TAG CYBER: You also provide training and practice exercises so a company will be prepared for real-life threats. Can you tell us more about those offerings and how they are different than a traditional tabletop?***

**BREACHRX:** Most companies focus solely on the security aspects of their incident response, and that goes for their tabletop exercises, as well. We hear lots of stories about handwaving the other parts of a response, regardless of the fact that those aspects generate 70% of an incident's cost. With our platform, companies can run cyber exercises and proactive assessments to determine what the impact of various types of incidents would be. It also gets the team well-versed in their procedures, ensuring all parts of the business are ready and prepared should an incident occur. We're big proponents of a "crawl, walk, run" approach to exercises. Many companies want to jump right into a big tabletop ransomware exercise with their executives without practicing beforehand. Our customers scale their simulations up, starting with phishing, stolen laptops, misdirected email, and malware infections, before working their way up to the big exercise, by refining their processes, testing their legal and privacy teams, and more. It's led to great success and more budget, because they demonstrate their proficiency and readiness.

***TAG Cyber: We'd love to get your take on any important trends you see in enterprise cyber security and compliance, along with any advice you might have for practitioner readers.***

**BREACHRX:** A few thoughts here. From a threat standpoint, we believe it's highly likely that attackers will continue to focus on software supply chains to get deeply embedded in their targets. The shared code from open source and commercial libraries is a prime target for threat actors, and we'll most likely see continued attacks with global repercussions moving forward. From a compliance and legal standpoint, a couple of thoughts. At some point we expect to see a lawsuit from a breached company targeting their compliance audit firm for misrepresenting their readiness. It might take a couple of years to come to fruition, but we feel it's only a matter of time. And in the near-term, we expect more C-level executives, including CISOs and CPOs, to be targeted personally by governments worldwide; the recent Drizly action by the FTC is a harbinger of things to come.



AN INTERVIEW WITH CAROLYN CRANDALL,  
CHIEF SECURITY ADVOCATE AND CMO,  
CYMULATE

# CONTINUOUS THREAT EXPOSURE MANAGEMENT WITH CYMULATE

---

In the world of cybersecurity, automation can help companies deal with the latest cyberthreats and regulatory pressures. Cymulate's platform allows companies reduce exposure by continuously monitoring, testing and validating the functionality and efficacy of their security systems.

**Last year, we had the pleasure of talking with Cymulate about their security posture management program,** and we recently met with the company again to learn more about their wide range of unique solutions, as well as hear their insights regarding future cybersecurity trends.

***TAG Cyber: What is a continuous threat exposure management (CTEM) program?***

**CYMULATE:** We are the first vendor to meet the full spirit of a continuous threat and exposure management program. CTEM is a multiyear initiative that helps organizations move beyond only tactical and technical remediation to reduce their long-term exposure. It also helps with communications between technical and business leadership in an effort to simplify complex technical information and issues. We deliver a unique, full exposure management program with a modular platform that automates and consolidates assessments from attack surface management (ASM), breach and attack simulation (BAS), and continuous automated Red Teaming (CART). Additionally, the platform can ingest exposure data from other sources to prioritize vulnerabilities and accelerate remediation. This innovation evolves traditional human-driven pen-testing, bringing forward self-service and automated breach feasibility and security control validation. Collectively, this reduces cyber risk by providing businesses of all sizes a cost-effective solution to frequently test and validate that security systems are operating and alerting correctly.

***TAG Cyber: Tell us about the benefits of your solution for security leaders who want to strengthen their organization's cyber resilience.***

**CYMULATE:** Using our technology, organizations can continuously assess, optimize, rationalize, and prove security efficacy and improvement. Our automated solution improves visibility to exposure, while reducing the risk of a breach

## Attackers are more aggressive and destructive than ever before, so many customers have set their 2023 focus on data-loss prevention (DLP).



by continuously validating security controls and testing breach feasibility. Businesses need to discover and prioritize exposures quickly, and this goes beyond simply understanding exposure by adequately prioritizing where you patch and where you focus. Due to the volume of vulnerabilities and often the inability to patch, security teams need to understand whether their security controls effectively detect, alert, and respond to threat activity, including whether compensating controls activate when other controls have been bypassed. We are also helping improve communications between security and business leaders with reporting that is tailored to each role and provides documentation that business leaders can understand, monitor, and act on.

***TAG Cyber: Tell us more about how enterprise teams can prioritize security decisions using your platform.***

**CYMULATE:** Exposure assessment and security validation are baseline security activities for businesses of all sizes. As companies mature in their programs, they need to optimize their environments and automate repeatable processes. Enterprises are experiencing increased pressures related to attack frequency and severity, regulatory issues, and staff shortages. Therefore, they need to turn to automation to keep up and respond to today's threat activity. Businesses of all sizes can easily achieve this using the Cymulate platform, which allows them to quickly assess their internal and external attack surface for exposures and prioritization. They can also leverage over 120,000 out-of-the-box attack simulations to test the efficacy of their security controls. Attack-based vulnerability testing and customized scenarios easily automate testing for emergent and advanced threats, which is appealing to sophisticated security teams. More mature organizations can leverage automated discovery operations and other aspects of Red Teaming that don't require direct supervision, allowing staff to perform more frequent testing in more areas of the organization. Large enterprises also appreciate that Cymulate limits the use of agents to one per environment, thereby simplifying deployment and maximizing scalability. In a time when vendor consolidation is a crucial focus, we provide modular licensing within a single platform, making it easy for customers to expand as their needs change. Attackers are more aggressive and destructive than ever before, so many customers have set their 2023 focus on data-loss prevention (DLP). Our platform validates that DLP and cloud access security broker (CASB) tools are detecting and alerting as needed, even when upstream security controls have failed.

***TAG Cyber: We'd love to get your take on any important trends you see in enterprise cyber security, offense and defense, along with any advice you might have for practitioner readers.***

**CYMULATE:** Due to unrelenting cyberthreat activity, organizations will shift from threat management to exposure management to be more proactive versus reactive in addressing cyberthreats. This is underpinned by regulatory and insurance pressures that are pushing companies to develop, maintain, and validate reasonable cybersecurity practices, as well as describe those practices in public filings by explaining how senior leadership oversees these programs effectively and promptly reports breaches. Another trend we see is around cybersecurity market consolidation. Economic anxiety, staffing challenges, and growing supply chain threats are impacting cybersecurity spending and the number of vendors that a business is willing to support. The global economic downturn has led to across-the-board consolidation among cybersecurity teams, specifically regarding the number of cybersecurity solutions and planned projects, along with staffing and training policies. This consolidation points to hard times for niche players and point solutions, while established companies with broad offerings are more likely to prevail, which might create merger and acquisition (M&A) opportunities for these bigger fish. Staff reductions could lead to a dangerous tipping point, creating a significant loss in cyber readiness and business production, thereby increasing breach feasibility. The automation of vulnerability assessment and security control validation can immediately enhance productivity for security teams dealing with limited skill sets that need help with repeatable tasks. Enterprise security is clearly consolidating, which will result in both customers and vendors needing to understand each security solution's role—where there are overlaps and where there are gaps. For Cymulate, this creates an opportunity for our customers to understand exposures, prioritize vulnerabilities, and test the efficacy of security controls. In the process of doing this, businesses will start to understand what test scenarios their business requires. During this process, they'll progress into new capabilities, such as automated Red Team testing, which will help offset the volume of testing they need to complete, while addressing the staffing challenges that businesses face today.





AN INTERVIEW WITH SONALI SHAH,  
CHIEF PRODUCT OFFICER, INVICTI SECURITY

## SCALABLE SECURITY TESTING FOR THE SDLC FROM INVICTI

During the software development lifecycle (SDLC), DevOps and DevSecOps teams can become overwhelmed by the number of manual tasks they need to do, with security challenges often mushrooming quickly out of control. Additionally, many scanning tools return false positives, creating a further bottleneck in the workflow. Invicti offers a scalable solution that provides security testing during every step of the SDLC, automating security tasks so security and development teams can stay on top of their workloads and accomplish the output of a team ten times their size. We had the opportunity to speak with Invicti and learn more about their highly accurate and efficient solution.

***TAG Cyber: What are the vulnerabilities found by Invicti that other tools miss, and how does this reduce vulnerabilities at scale?***

**INVICTI:** With 15 years of experience in dynamic application security testing (DAST), Invicti Security—which acquired and combined DAST leaders Acunetix and Netsparker in 2018—offers the most comprehensive results in the industry. We’re the only company that combines DAST, interactive security testing (IAST) and software composition analysis (SCA) in one scan, providing consolidated results at nearly 100% accuracy. IAST enables us to identify and scan hidden and unlinked assets beyond a traditional DAST vendor’s scope, while our SCA engine reveals vulnerabilities in open-source software. What really sets us apart, however, is the accuracy of our findings. Our customers care about the number of real exploitable vulnerabilities we find rather than the number of total possible vulnerabilities. Invicti’s high accuracy rate stems from our Proof-Based Scanning technology that works by safely exploiting an identified vulnerability and extracting sample data to prove an attack is possible. By providing accurate findings and guidance on what to fix first, our customers can scan all their applications and reduce vulnerabilities at scale.

***TAG Cyber: How does your solution assist in scaling up web security?***

**INVICTI:** Our customers scale by initially scanning only their most critical applications to subsequently scanning nearly all of their applications and APIs with Invicti. Our solution’s accuracy, speed and automation enable this scale. Proof-Based Scanning boasts a

**It has never  
been cheaper to  
launch an attack.  
Cyberattacks  
are among the  
most effective  
ways to get rich,  
make a political  
point, or damage  
an economy.**



confirmation accuracy of 99.98%, meaning only 0.02% of vulnerability confirmations could potentially lead to false positives. Without proof, every result from even the best DAST could be a false alarm until somebody checks it manually. Proof-Based Scanning cuts through the uncertainty by automatically showing—and proving beyond any doubt—what issues concretely exist and are not false positives. This eliminates guesswork and enables the move to fact-based web application security at scale. In addition to accuracy, the speed of finding and fixing vulnerabilities is also essential to scaling web application security and reducing risk. With development teams releasing code daily, long scan times for in-production applications and APIs can delay software releases and increase the risk of an exploit. The faster you can catch a vulnerability, the sooner you can fix it. Lastly, our automation capabilities help our customers scale their web application security programs. An automated scanning and remediation workflow, combined with integrations of the tools that developers and security teams use daily, allow security to be implemented efficiently into the software development lifecycle.

***TAG Cyber: Your product offers DAST, IAST and SCA scanning. Why is this unique, and what are its benefits?***

**INVICTI:** Our platform blends DAST, IAST and SCA, so you have an inside-out and outside-in perspective of your apps to ensure complete coverage and actionability. IAST works by running checks on the codebase of an application as the code is being executed by a web server or application server. This technology fills the gap between static application security testing, which involves code that is not running, and DAST, which only checks the application from the outside. IAST scans provide details about the problem, often down to the specific file name and line number. Depending on the technology and type of vulnerability, IAST insights can include injected payloads, exploit results and stack traces generated by errors. These additional details make it easier and faster for developers to remediate the code. Additionally, our SCA leverages its proprietary database to check for known vulnerabilities in open-source components. The explosive growth in the use of open-source components allows developers to build quality functionality faster but also creates risk when those components have vulnerabilities. Application security programs must test first- and third-party code to maximize risk reduction. In addition to the combination of technologies mentioned above, we win even more customers over because of integrations and automation.

***TAG Cyber: How can Invicti help developers produce more secure code?***

**INVICTI:** From our experience, developers take pride in building high-quality code that is both functional and secure. They

don't resist using application security tools, but they do resist using inaccurate and inefficient tools, causing delays in release schedules. Invicti's high accuracy rate, automation and fast scans help developers integrate security testing into their code more efficiently. Customers can scale their AppSec programs using the more than 50 integrations offered with the platform at no additional cost, including continuous integration and delivery (CI/CD), issue trackers, and collaboration tools. With automated scans within the CI/CD pipeline, validated findings are sent directly to the developer's issue tracker and fixes are automatically verified, allowing developers to produce more secure code efficiently. Our scans can occur in either the development or production phase for continuous security. In addition, developers can use Invicti to see if they are improving over time; we provide multiple ways to see trends by user, department or geography. Invicti Learn is an online hub for information on detecting, avoiding and mitigating web vulnerabilities. This great resource has become a destination for security professionals to learn about vulnerabilities, attack types, tools and more.

***TAG Cyber: We'd love to get your take on any important trends you see in enterprise cyber security, offense and defense, along with any advice you might have for practitioner readers.***

**INVICTI:** The biggest threat facing companies in 2023 is their own inaction. While the current economic climate is causing companies to delay hiring and investments, cybersecurity is definitely not the area to do so. A number of factors have increased the risk of a potential large-scale disruption due to a cyberattack. First, it has never been cheaper to launch an attack. Cyberattacks are among the most effective ways to get rich, make a political point, or damage an economy. Deloitte estimates that a phishing campaign costs **\$500 per month on average** (including host costs and the phishing kit), with prices starting at \$30 per month. At the same time, the number of breaches and the cost of cleaning them up are rising, **with the number of cyberattacks recorded in 2022 nearly 40% greater than the total volume observed in 2021**. Whether you are a government agency, educational institution, or company of any size, investing in protecting your digital assets should be a standard cost of doing business, just like investing in physical security to protect your bricks-and-mortar office. Unfortunately, we've seen many companies bury their heads in the sand, refusing to believe they will be breached, despite all the evidence. Inaction, either caused by budget cuts or foolish optimism, is the most significant risk facing companies in 2023.



AN INTERVIEW WITH PETER PRIZIO,  
CEO, SNAPATTACK

# THREAT-INFORMED CYBER OPERATIONS SUPPORT WITH PURPLE TEAMING FROM SNAPATTACK

Modern enterprise security teams demand effective commercial solutions to support operationally oriented threat hunting. This involves many different tasks, including removing doubts about preparedness for attacks, swiftly performing security operations and threat hunting, as well as validating whether SOC teams are escalating incidents properly and effectively deploying security tools. We recently sat down with SnapAttack to learn how the company helps enterprise teams drive toward a more continuous, automated validation of threat hunting and other operational cybersecurity goals.


**TAG CYBER:** *Let's start by understanding how your team helps enterprise security teams with proactive threat hunting and security operations. What is your approach?*

**SNAPATTACK:** Our platform proactively provides a multifaceted approach that combines cyberthreat intelligence, threat hunting, detection engineering, breach-and-attack simulations (BAS), and Purple Teaming capabilities in a single, easy-to-use platform. Along with all the above, we integrate over 30-and-counting popular, prominent, industry-leading SIEM and XDR platforms with a no-code detection builder and one-button content deployment method.

**TAG CYBER:** *Is your solution implemented by a SaaS platform, and do you offer services in support of your customers? What would a practical SnapAttack deployment involve?*

**SNAPATTACK:** Our solution is primarily SaaS-based for ease of deployment and integration with other platforms, but in certain cases or requirements, it can be installed and monitored on premises. When requested, our professional service personnel can provide SIEM and XDR migration, different types of maturity assessments based on client need, and request for information (RFI) credits, at a minimum. Other types of services can be discussed per client requirements. A typical deployment follows a standard project management methodology, consisting of project initiation, planning, execution, control and closure. During these phases, we take into account the client's unique requirements, as

Our adversaries take their “business” very seriously. If we do not devote significant time to staying current, we’ll quickly fall behind.



well as any deviations that might arise during deployment of the SnapAttack platform. We typically follow a “white glove” mindset during deployment to give the client the best possible experience.

***TAG Cyber: We frequently hear about serious skills gaps in the typical enterprise SOC. Is this an area that customers discuss with you, and does your platform help with this challenge?***

**SNAPATTACK:** There are skills gaps across the globe in the cybersecurity industry. Our platform can assist with this by providing thinly staffed teams with Purple Teaming capabilities where they didn’t previously exist, or by enhancing and accelerating detection engineering skills to the point where even a junior analyst can easily write and deploy low-noise, high-accuracy detections in short order, when this was unlikely before.

***TAG Cyber: It must be tough to keep up with all the advances in cyberoffensive tactics and techniques in use today. What is your approach to staying current?***

**SNAPATTACK:** We take several different approaches to staying current—how much time do you have? Our adversaries take their “business” very seriously. If we do not devote significant time to staying current, we’ll quickly fall behind. Our folks often attend various cybersecurity courses. Many universities, online platforms, and training institutes offer courses that cover offensive tactics and techniques, helping us gain a better understanding of different attack vectors, exploit techniques and penetration-testing methodologies. We are also constantly reading cybersecurity blogs and news to stay up to date on the latest trends and developments in the field, as well as any new techniques and tools used by attackers. SnapAttack has a robust [resources](#) page where anyone can find various blogs, whitepapers and ebooks on relevant topics. Next, we join cybersecurity groups, forums and other communities to learn from experienced professionals in the industry. These groups provide anyone with valuable insights and tips to keep abreast of the latest developments in cyberoffensive tactics. Attending cybersecurity conferences is another great way to learn about the sector’s latest trends and techniques, while also enjoying networking opportunities to connect with other professionals in the field. Finally, if we want to practice offensive tactics and techniques, we’re sure to practice in a legal and ethical manner. Participating in bug bounty programs, capture-the-flag events and other legal activities help us gain hands-on experience without risking legal repercussions.



***TAG Cyber: We'd love to get your take on any important trends you see in enterprise cybersecurity, both offensive and defensive, along with any advice you might have for practitioner readers.***

SNAPATTACK: If you ask five cybersecurity professionals this question, you'll get slightly different answers. There are several important trends shaping the enterprise cybersecurity landscape today. First, there is cloud security. The shift towards cloud computing and workloads has resulted in a growing need for cloud security solutions. Enterprises are increasingly relying on cloud services for data storage and processing and, therefore, need to implement proper security measures to protect their cloud infrastructure and data. Next, Zero Trust architecture is an approach to enterprise security that requires all users and devices be authenticated and authorized before they are granted access to enterprise resources. This approach is gaining popularity due to its effectiveness in preventing unauthorized access, while also limiting the impact and lateral movement of an attacker should there be a breach. Thirdly, AI and machine learning (ML) are being used to detect and respond to cyberthreats in real time. Enterprises are using these technologies to identify potential threats and automate security responses. For instance, our platform uses AI and ML to enable greater accuracy in threat detection. On the flip side, our adversaries are also using this technology to create their latest threats, so we have to remain vigilant. Internet of Things (IoT) security is also important. As the number of IoT devices in enterprises continues to increase, so does the need for IoT security solutions. Enterprises are implementing security measures to protect these devices from cyberattacks to ensure they don't become entry points for attackers to access the rest of the network. Most people don't think of the breadth of these devices—they span from the refrigerator in your home to the 18-wheeler on the open road and everything in between. The attack surface has simply grown larger. Finally, there is cyber insurance. With the increasing frequency and severity of cyberattacks, enterprises are turning to cyber insurance to mitigate the financial impact of a breach. Cyber insurance policies provide coverage for costs associated with data breach response, recovery and legal liabilities. Due to the sheer amount of recent breaches, this type of insurance can be more difficult to obtain. The above trends reflect the evolving nature of cyberthreats and the need for enterprises to implement a comprehensive cybersecurity strategy to protect their assets and data. Above all, enterprises need to stay vigilant and adapt their cybersecurity approach to stay ahead of the evolving threat landscape.



AN INTERVIEW WITH FREDY MARTINEZ-PARDO,  
HEAD OF CUSTOMER SUCCESS, SPHERE

## PROTECTING ASSETS THROUGH IDENTITY HYGIENE WITH SPHERE

All companies know you need to be prepared for an external security breach or hack, and privilege misuse is one of the main factors when it comes to financially motivated attacks. Identity hygiene helps companies keep their privileges and permissions squeaky clean, thereby eliminating open and inappropriate access, so that data quality is improved and assets are protected. SPHERE'S SPHEREboard solution is an end-to-end workflow that identify risks and remediate threats. SPHERE recently shared the platform's innovative features with us, as well as their insights on identity hygiene.


**TAG CYBER:** *What is identity hygiene, why is it important, and what is SPHERE's unique approach to this topic?*

**SPHERE:** Identity hygiene is the ongoing practice of knowing who has access to what, why and when—at all times. Organizations classify and categorize information based on its value to their ongoing activities. This information informs critical decisions about security controls that can be administrative, technical, or operational in nature. These controls depend upon “need to know” decisions—who inside or outside the organization requires (or does not require) the ability to create, modify, move, copy, or otherwise change the location, state, or characteristics of the data. Our identity hygiene platform provides a unique approach that helps organizations understand their identity posture with a unique end-to-end access management workflow—from discovery to remediation—of all identities across a company's technological assets.

**TAG CYBER:** *Explain the concept of an “evergreen IT strategy,” and how does SPHERE help achieve this goal.*

**SPHERE:** Essentially, something that's “evergreen” is timeless and sustainable. The earliest definition of an “evergreen IT strategy” was created a decade ago; it is defined as the cross-section between on-premises and cloud computing, and instrument provisioning and management processes. It requires a combination of people, processes, and technology to continuously update, upgrade, and manage an end user's software, hardware, and associated services like file storage, applications, and more. Just like personal hygiene, identity hygiene isn't

It's important to remember that every identity starts its lifecycle at the provisioning stage and ends when it is disabled and deprovisioned, but the latter doesn't always happen.



something you do just once. With SPHERE's ongoing remediation, we help our clients along the evergreen path by implementing a continuous identity hygiene process to support an organization's technical upgrades.

***TAG CYBER: How does SPHERE help a company gain visibility into its data BEFORE it migrates to the cloud, and why is this a good thing to do?***

**SPHERE:** Digital transformation is more important than ever for all organizations. Our practical knowledge and expertise are an essential part of the blueprint for action, because we initiate an assessment based on the current state of identities, assets, data, and users to help our clients map out the best route for their cloud migration. With our SPHEREboard platform, clients have full visibility into the identities, users, and data that should not be considered part of the migration. This approach impacts three main areas of account migration. First, it reduces costs by identifying target data, such as stale files out of audit compliance. Secondly, it enhances data security by removing toxic combinations, and finally, it reduces the implementation timeline.

***TAG CYBER: SPHEREboard is quite a powerful tool. Can you share its main features with us?***

**SPHERE:** Over the last few years, we have focused on building this robust identity hygiene tool. Our unique platform is continuously enhanced with new capabilities to help some of the largest and most highly regulated organizations improve security, enhance compliance, and achieve ongoing identity hygiene. Its main features include modules for unstructured data, accounts, and groups, as well as privileged accounts management. The platform's Unstructured Data Module enables end-to-end workflow on file storage devices, Office 365, and Confluence. Its capabilities support file store discovery, ownership correlation, access control reports (such as open and excessive access), and automated file access remediation. Data classification, privacy and lineage on file systems can be achieved as part of our partnership with BigID. Next, the Accounts Module is one of the platform's features that is most adopted by clients. It permits any organization to discover, detect, and remediate any account (human and nonhuman), ensuring that the access to assets is authorized and restricted based on business and security requirements. Additionally, the Groups Module helps organizations understand the current state of the AD groups platform (on prem or cloud), and its discovery engine can report and remediate use cases like stale and empty groups, nesting, structure analysis, excessive membership analysis, unclaimed accounts or groups, AD groups identified by Ddivision, groups with elevated permissions, group policy permissions and more. Lastly, Privileged Accounts Management is highly utilized by

organizations lacking a just-in-time strategy. It provides full visibility of users and accounts with elevated permissions across an organization's assets. Automated Privileged Accounts Vaulting can be achieved as part of our partnership with CyberArk.

**TAG Cyber:** *We'd love to get your take on any important trends you see in enterprise cyber security, offense and defense, along with any advice you might have for practitioner readers.*

**SPHERE:** As cyberattacks increase, a similar number of trends and tools arise to combat them. At SPHERE, we're constantly upgrading our platform and looking for new partnerships to provide our customers with the best tools. Above all, we try to stay focused on the basics of identity and access management (IAM) practices—the principle of the identity lifecycle. It's important to remember that every identity starts its lifecycle at the provisioning stage and ends when it is disabled and deprovisioned, but the latter doesn't always happen. It may sound simple, but as any organization operating in today's complex, threat-rich environment knows, it's not. Our clients turn to us as a trusted partner in their cybersecurity efforts and rely on our solutions as critical elements in their IAM programs. Sure, our SPHEREboard platform provides advanced technology, stringent controls, and ongoing reporting and monitoring, but we also have extensive in-house experience as boots-on-the-ground practitioners of risk reduction. In other words, we know the real-world challenges facing organizations when trying to protect their enterprise from ever-increasing threats.



*"I have no idea what your value proposition is."*



AN INTERVIEW WITH DAVE PURDY,  
VICE PRESIDENT OF SALES, NORTH AMERICA,  
TXONE NETWORKS

# GROUND-UP CYBERSECURITY FOR OT ENVIRONMENTS FROM TXONE NETWORKS

Operational Technology (OT) environments have their own specific needs, which require specialized knowledge. Instead of merely copying IT solutions to OT environments, completely new cybersecurity approaches need to be built from the ground up. TXOne Networks is a leading supplier of OT Zero Trust technologies for manufacturers and critical infrastructure operators. The company recently spoke with us to explain in greater detail how their solution is specifically tailored to provide real-time cybersecurity for mission critical devices and the OT network.

***TAG Cyber: What types of security weaknesses are specific to industrial environments?***


**TXONE NETWORKS:** Industrial environments operate using industrial control systems (ICS). ICS systems drive the instrumentation and automation used for industrial production processes that utilize highly specialized protocols. Control systems receive data from remote sensors that measure process variables (PVs) and then compare the collected data with desired setpoints (SPs), deriving command functions used to control a process through the final control elements (FCEs), such as control valves. Larger systems usually implement supervisory control and data acquisition (SCADA) systems or distributed control systems and programmable logic controllers (PLCs). These systems are extensively used in industries such as telecommunications, power generation, chemical processing, pulp and paper manufacturing, and oil and gas processing. What I have just described is also referred to as operational technology (OT).

When compared to information technology (IT), OT environments are much more prone to cyberattacks and ransomware for two primary reasons. First, IT security is more mature from a technology supplier, adoption, and skillset standpoint as compared to OT. Secondly, IT security solutions cannot effectively protect OT environments, because they do not understand the OT-native protocols that control ICS environments. TXOne exists to resolve both issues with a set of OT-native cybersecurity capabilities that protect ICS environments, without impacting industrial production.

Organizations that attempt to address OT risks with IT tools are dealing with attackers taking control of production assets by exploiting unpatched vulnerabilities, deploying malware, and hiding malware in updates or newly acquired devices. One example is control



Although many attacks that occur in OT environments cascade from IT systems, we are clearly seeing an upward trend of attacks directly assaulting OT-specific protocols.



logic manipulation, where untested changes to software or configuration settings could produce unpredictable results. The worst part about these types of attacks is that they shut down operations, as well as put human safety and product quality at risk. Companies have discovered that simply extending IT security products into industrial settings is not enough; they require cybersecurity approaches built from the ground up for OT. OT security requires real-time preventative measures, visibility, and threat detection. To accomplish this, the OT cybersecurity solution must be able to understand and act at the protocol instruction set level. TXOne Networks is that OT-native solution.

***TAG Cyber: What unique considerations are required when it comes to implementing Zero Trust methodology in OT and ICS settings, and how does TXOne fulfill these needs?***

**TXONE NETWORKS:** Zero Trust is a well-known term in cybersecurity. With its origins in IT, the primary focus and guidance was predominantly IT-based and constructed on a set of principles that do not translate to an OT environment. OT Zero Trust was developed as an answer to the problems associated with production assets. IT cybersecurity solutions have all been developed based on Confidentiality, Integrity, and Availability (CIA). OT network security, on the other hand, is based on asset activity, so that productivity is always the highest priority, requiring a different model, Availability, Integrity, and Confidentiality (AIC).

***TAG Cyber: Describe the solutions you provide for security inspection, endpoint protection and network defense.***

**TXONE NETWORKS:** TXOne's solutions meet the unique needs of diverse ICS verticals in device inspection, endpoint protection, and network defense to secure an organization's OT workforce, workload, and workplace. Our solutions are designed to deploy on levels of basic control, supervisory control, and site manufacturing operation and control of the Purdue model. Our security inspection solution, Portable Inspector, delivers software-free security capabilities that can be used not only by security teams, but by ops teams, as well. Integrating with existing procedures, the USB form factor drive can inspect new equipment before it is allowed entry to production; it also performs regular auditing and inventory management functions, as well as providing advanced security for out-of-band and isolated devices.

Additionally, our endpoint protection solution, **Stellar**, is the world's first OT solution capable of recognizing and preserving thousands of critical OT applications. It integrates with individual devices, becoming a native extension to its base functionalities, while defending modern and legacy devices by actively preventing unauthorized changes to baseline operations at an application and process level—all without

interrupting normal operations. Finally, our network defense solution, EdgeIPS, segments an organization's networks into productivity-based zones and shields vulnerable assets at the network level to improve defenses, streamline oversight, and prevent cyber incidents. It recognizes a wide variety of industrial protocols for OT inspection and control, allowing for seamless collaboration between OT and IT security system administrators, and granting comprehensive network visibility.

***TAG Cyber: What industry sectors do you specialize in, and how do you meet their specific demands?***

**TXONE NETWORKS:** TXOne secures the operations of more than 3,600 organizations globally and serves multiple industries worldwide, including the following sectors: semiconductors, automotive, manufacturing, critical infrastructure, oil and gas, transportation, utilities, and more. At the end of 2022, among all the public-sector entities that our company's research lab monitored, probing/hacking directly against governmental bodies accounted for 48 percent of the traffic. Targeted hackings require more vertical-specific tools that carry out different purposes and, therefore, require different countermeasures. Our portfolio addresses the security requirements of both legacy and modern devices using our software endpoint and network intrusion detection systems (IDS) and intrusion prevention systems (IPS). TXOne also provides early warning of potential risks and emerging vulnerabilities through our threat intelligence resources. TXOne's Threat Research team continuously monitors the ICS and industrial Internet of Things (IIoT) threat terrain via our large-scale threat-hunting system. Threat data is gathered through a worldwide network of hunting engines, submissions, feedback loops of customers, partners, and our own Threat Research Lab's researchers.

***TAG Cyber: We'd love to get your take on any important trends you see in enterprise cyber security, offense and defense, along with any advice you might have for practitioner readers.***

**TXONE NETWORKS:** For the rest of 2023, we anticipate that cybersecurity will become increasingly complex and challenging, due to the emergence in the previous year of numerous new Ransomware as a Service (RaaS) offerings, such as Black Basta, Pandora, and LockBit 3.0. As RaaS business model and revenue streams mature, attacks on the energy and critical manufacturing sectors are likely to persist, with a significant impact on manufacturers of automobile-related products. We believe that to combat OT cybersecurity complexity, an organization's security teams should have a higher level of specialized knowledge, rather than simply copying IT solutions to the OT environment. Although many attacks that occur in OT environments cascade from IT systems, we are clearly seeing an upward trend of attacks directly assaulting OT-specific protocols. Digital transformation is an unstoppable trend, resulting in more interconnected devices and intelligence gathered from cloud technologies, as organizations go smart. Every asset needs a multi-layered security deployment approach to ensure it's covered throughout its entire lifecycle and doesn't become a major weakness, now or in the future. By elevating cybersecurity standards from the ground up for the network and assets, we believe organizations can better respond to any OT cyberthreats that may arise in 2023.



AN INTERVIEW WITH MATT RADOLEC,  
SENIOR DIRECTOR, INCIDENT RESPONSE &  
CLOUD OPERATIONS, VARONIS

## SECURING MISSION-CRITICAL DATA WITH VARONIS

---

Traditional cybersecurity methods were focused on protecting the perimeters of a company's system to keep hacks and attacks at bay. However, with the move to the cloud and an increasingly remote workforce, firm borders have vanished, leaving a company's most valuable asset, its data, evermore vulnerable. Luckily, cybersecurity pioneer, Varonis, has stepped in to fill the gap with its data-first approach, strengthened by patented, powerful machine learning. We recently met with Varonis to learn more about their platform and the current cybersecurity landscape.

**TAG CYBER:** *Varonis was founded in 2005. How has the cybersecurity landscape evolved over the years, and what are the greatest challenges a company faces now versus back in the day?*

**VARONIS:** In 2005, the top concerns were "What happened to this file? Was it moved or deleted? Where did it go? Who did it?" While these questions are still important, data growth and increasing IT complexity have shifted the focus. Strict regulations, hybrid cloud environments, and a constant barrage of internal and external threats have reshaped the cyber landscape. Currently, the top concerns are cybercriminals, insider threats, APTs, privacy and compliance. One of the biggest events contributing to this landslide change in priorities was the shift to work-from-home during the COVID-19 pandemic in 2020. Most businesses had to prioritize productivity and availability over security, resulting in vast amounts of data being moved to the cloud and shared with minimal governance. One thing that didn't change, however, was the desire to protect data by prioritizing security on the data that matters most, controlling who can access it, and monitoring its usage. In 2023, the perimeter is eroding more and more, with organizations realizing the softest and most easily attacked part of their ecosystem is their data. This is why Varonis exists—to partner with organizations in taking a data-first approach to cybersecurity. We start with an enterprise's highest-value asset, its data, and protect it where it exists in the greatest concentrations and where it is at greatest risk. In 2023, this is probably a combination of a company's data centers, along with SaaS applications like M365, Salesforce, Google, Box and GitHub.

Intelligent automation is a key factor that sets Varonis apart in the market. It's a trend that we see becoming increasingly essential for successful data security programs.



**TAG CYBER:** *How do you use machine learning to automate the protection of data, and what do you envision as the future of machine learning in terms of cybersecurity?*

**VARONIS:** Machine learning is an integral part of our platform. We collect vast amounts of metadata and leverage it, allowing us to use machine learning to intelligently determine who needs access to data and who doesn't. For example, instead of just expiring access to data after a certain period, we look at how people are using data. We then make intelligent decisions on where unnecessary access can be removed and use automation to make these access changes continuously at scale as new risks arise. Intelligent automation is a key factor that sets Varonis apart in the market. It's a trend that we see becoming increasingly essential for successful data security programs.

**TAG CYBER:** *You like to say that you "see the world of cybersecurity differently." How so?*

**VARONIS:** Cyberattacks are always changing and will always happen. There will always be new ways to break in, new zero days, and new mistakes to be made; we call these vectors of attack. No matter the attack vector, the target is always the same—data. At Varonis, that's where we start. We know where an organization's sensitive data is, who can access it, and what they're doing with it, so we can not only detect an attack attempt, but also proactively limit the damage of an attack. We believe automated data security is the future, and we're here to help companies realize that vision.

**TAG CYBER:** *You did a recent study that found the average organization has "more than \$28 million in SaaS data-breach risk." What are some of the report's key findings, and what can a company do to protect itself?*

**VARONIS:** We start and continue our relationship with clients through data risk assessments. We give every company we meet with an opportunity to carry out a free data risk assessment showing where they have sensitive data and where it is exposed. Often, we even find active cyberthreats. We do more than a thousand assessments each year, and, in this report, we combine findings from several hundred assessments to look specifically at SaaS data risk. What we found is that 81% of organizations had sensitive SaaS data exposed. With the average company having more than 40 million unique permissions across SaaS applications, it's no surprise that this data exposure exists. The cloud introduces a paradigm for organizations to navigate where each end user creates their own permissions, and, in every instance, they share data. Often, it isn't feasible for business operations to restrict sharing, but there is hope. You can limit the risk of cloud collaboration links through actions such as enforcing

an auto-expiration date. Of course, we can help organizations solve these problems in an intelligent, scalable way, and that's exactly what our data risk assessment helps uncover before spending a dime.

***TAG Cyber: We'd love to get your take on any important trends you see in enterprise cyber security, offense and defense, along with any advice you might have for practitioner readers.***

**VARONIS:** At Varonis, we include help from our expert incident-response team in all our subscriptions and trials, giving us a unique perspective into the threat landscape. In addition to some of the latest security challenges that come from an increase in SaaS app usage, we also continue to see a rise in insider threats. Insiders won't trip any alarms trying to get into the network, but often they're so overprivileged that they can do the most damage. This is where our data-level visibility comes in. The fact that we're able to see when normal data activity deviates means that we're able to catch threats other solutions miss. With our least privilege automation, organizations can proactively limit the damage any one insider can do, without impacting their productivity. In addition, our proactive incident-response team watches and investigates our customers' alerts for them, so we're able to improve defenses even further. For any practitioner looking to improve their security posture, our best advice is to start with a data risk assessment. It's impossible to protect what you don't know exists. Once a company has a clear picture of its risk, it can start to harness automation and other cybersecurity expertise to optimize its risk reduction efforts.





**ANALYST  
REPORTS**

# TAG NAVIGATOR

## A NEW APPROACH TO COMMERCIAL CYBERSECURITY VENDOR COMPARISON

DR. EDWARD AMOROSO, MATTHEW AMOROSO, DR. JENNIFER BAYUK,  
SOURAJYOTI BOSE, IASSEN CHRISTOV, CARLIER HERNANDEZ,  
SHAWN HOPKINS, KHANJAN PATEL, JOHN J. MASSERINI,  
NICK WAINWRIGHT, CHRISTOPHER R. WILDER – TAG CYBER

---

This report introduces a new approach to comparing technology vendors and solutions called the TAG Navigator. The traditional methods, such as the Gartner Magic Quadrant and Forrester Wave, have drawbacks in that dimensions are limited and detail in assessment criteria with which to second-guess a rating is lacking. The TAG Navigator addresses these weaknesses by using well-defined values assigned to a series of comparison factors, resulting in a spider chart profile of a vendor, its company, and its solution. The comparison is based on 10 factors: the Company Stage, Pace of Innovation, Vision & Strategy, Message Efficacy, Financial Strength, Scalability, Support, Management Strength, Product Maturity, and Competitiveness are designed to provide insight for practitioners, buyers, and other consumers. The report also explains that this approach allows for granularity, transparency, and elements of fact-based in comparison.

## INTRODUCTION

As in any technology selection process, when selecting a cybersecurity solution, due diligence dictates reviewing the relevant options. This task is easier said than done, especially in cybersecurity, where many overlapping commercial and open-source choices exist. TAG Cyber tracks, for example, over 4200 different commercial vendors selling cybersecurity products and services and the **number continually increases**.

Perhaps the most recognizable methods for comparing commercial cybersecurity vendors today are the **Gartner Magic Quadrant** and the **Forrester Wave**. The quadrant and wave approach is familiar, but does exhibit drawbacks, including but not limited to limited details on assessment criteria and requirements for a client to fund construct development.

In this report, we introduce a new cybersecurity solution comparison approach that we believe addresses the weaknesses of these traditional approaches, while also providing insight for practitioners, buyers, and other consumers. The new method, called the TAG Navigator, is based on user-defined values being assigned to a series of comparison factors, resulting in a spider chart profile of a given vendor or open-source solution for cybersecurity.

## COMPARISON FACTORS

In a perfect world, multiple options for a cybersecurity solution would be reviewed and one would emerge that provides the greatest risk reduction at the lowest cost with the least trouble deploying and integrating. In live practice, however, the relative benefits associated with the various options are always more complex to compare – and it is almost always the case that trade-offs must be made, even for the top selection.

To address this complexity, industry analysts often suggest reviewing multiple factors to perform the comparison. For example, the Gartner quadrant mentioned above suggests two main factors for estimation and comparison: ability-to-execute and completeness of vision. The advantage of this approach is simplicity, but the great disadvantage is the lack of granularity, subjectivity, and insufficient detail for meaningful comparison.

In contrast, the TAG Cyber research team always strives for transparency in comparison criteria. We have experimented with richer sets of comparison factors and selected 10 (ten) to include in a transparent model. Each factor represents some aspect of a solution’s value proposition and has been deemed by TAG Cyber as a reasonable predictor of a vendor’s success in the solution’s discipline. Admittedly, this approach suffers from the need for subjective estimation (as does all its predecessors). Nevertheless, the more granular approach improves the odds of a fair comparison.

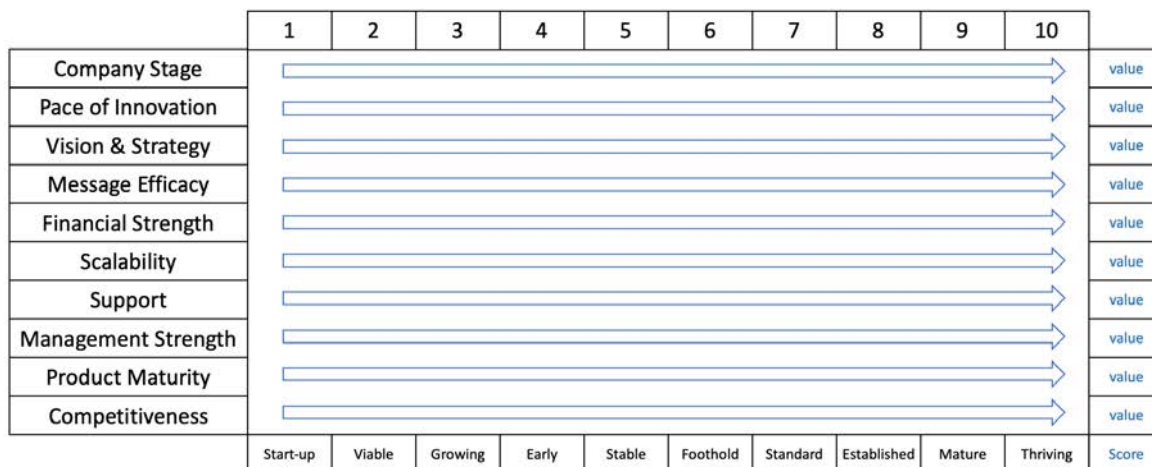


Figure 1. TAG Navigator Comparison Factors



The comparison factors included in the methodology and shown in Figure 1, which we refer to collectively as the TAG Navigator, are listed below. We assume that any observer can fill in estimates of the relative values for each factor – and as analysts, we reserve the right to inject our opinions. However, enterprise teams can and should adjust the factors to match up with local environmental conditions and context.

- 1. Company Stage:** This references where a given vendor currently resides in the corporate lifecycle. At one end of the scale are the start-up companies being driven by founding teams. Mature companies with experienced management teams driving the scale are at the other end of the scale.
- 2. Pace of Innovation:** This involves how rapidly the vendor is currently innovating. At one end of the scale are the vendors who are innovating at a rapid and impressive pace. At the other end of the scale are companies who either believe their product is mature enough or slow their innovation in favor of scale.
- 3. Vision and Strategy:** This addresses whether the vendor articulates their role and purpose. At one end of the scale are vendors still developing a future vision. At the other end of the scale are vendors who describe a clear vision and strategy for their company.
- 4. Message Efficacy:** This involves the vendor's marketing and value proposition message. At one end of the spectrum is an unclear description focused mostly on features. At the other end is a strong message of what solution is being addressed and why.
- 5. Financial Strength:** This addresses the company's funding, revenue, and profitability. At one end of the spectrum are companies with weak near-term prospects. At the other end are well-funded companies with growing revenue and profits.
- 6. Ability to Scale:** This addresses whether the solution can be provided to a growing number of customers. At one end of the spectrum are companies that can only handle growth by adding employees. At the other end are companies with a platform that can handle rapid growth.
- 7. Customer Support:** This involves whether the company can assist customers with deployment, training, integration, and maintenance. At one end of the spectrum are companies with no support team. At the other end is a mature support team.
- 8. Product Maturity:** This references whether a full-featured product exists that addresses the needs of its customers. At one end of the spectrum are companies with only an early prototype. At the other end are companies with a working solution that has been continuously used through multiple business cycles.
- 9. Competitiveness:** This references whether the solution is unique from other vendors in its space, perhaps with a high barrier to entry. At one end are companies in highly competitive categories. At the other end are companies filling needs in a new and emerging area.
- 10. Strength of Management:** This references whether a strong management team with capable advisors exists. At one end of the spectrum are companies with new managers in their first leadership roles. At the other end are companies with the mature, experienced leadership team.

Assigning values<sup>1</sup> to these ten factors is a combined subjective and objective process. For example, in the area of strength of management, it is subjective to determine whether founders appear to have good management skills – but it is entirely objective to review and measure the intensity, relevance, and scope of their experience. Being a new manager is objectively different from having many years of experience managing.

The selection of the ten factors was guided by our goal to highlight the relevant factors required to compare the potential effectiveness of a given commercial vendor to support a customer application. Obviously, what might be good for one buyer of a commercial platform might not be so good for another buyer of the same platform. Also, a vendor with multiple products may have different scores for each product. It is, therefore, imperative to support local adjustment of the values assigned to variable factors.

## TAG NAVIGATOR VISUALIZATION

The visualization approach developed here was to create a spider chart that allows for shapes to emerge based on the values assigned to the factors. By design, we consider higher-value variable factors more desirable in more contexts. This allowed us to make the claim that in most contexts, the area inside the spider web shape is directly proportional to a higher likelihood of effectiveness.

For example, consider that management in a start-up begins at 1 with a founding team that exhibits unclear strength, albeit potentially with great promise – and it continues up the scale toward a mature leadership team with visible, well-known management strengths. In most cases, the preference for enterprise teams would be toward the latter, especially for larger platforms with great consequences.

There are, however, cases where a start-up team might not only have great promise but might be amazing visionaries with an incredible future. This might stand in contrast to a well-known management team with a clear track record but who exhibit bad habits and who might be the overseers of a commercial vendor with a bad plan. In this case, the lower rating of 1.0 might correspond to a superior management team.

The TAG Navigator is developed as a spider chart where the various factors show the assigned values between 1 and 10 for a given cybersecurity start-up. The idea is that by showing a given spider chart shape for some vendor in the context of comparison with other comparable vendors, useful insights will be highlighted, resulting hopefully in better management decisions with respect to the vendor.

To help stakeholders better understand how the values impact the final score, we decided that simple declarative references would be associated with each of the ten possible scores to help provide context and assist in interpreting a given value. Obviously, local tailoring is required to translate a score into action, presumably to improve or maintain a given value. Here is a qualitative description of how the ordinal scores should be interpreted:

- 10 Thriving:** The attribute is indisputably best in class.
- 9 Mature:** The attribute is reflected in a satisfied and loyal customer base.
- 8 Established:** The attribute is well on its way to scaled mature operation.
- 7 Standard:** The attribute has achieved industry standard status in some industry.
- 6 Foothold:** The attribute is reflected in maturing operations and customer service.
- 5 Stable:** The attribute has achieved growth sufficient to maintain a multi-year going concern.
- 4 Early:** The attribute growth has steadily matured quarter over quarter.
- 3 Growing:** The attribute is in the first stages of growth with many great future opportunities.
- 2 Viable:** The attribute has a viable lifecycle and satisfies customers.
- 1 Start-up:** The attribute is not yet visible, this is more common in the case of new cybersecurity companies without a viable product or referenceable customers.
- 0 Not rated**

When these values are assigned in the spider chart, a shape inevitably emerges, and as suggested above the greater the area inside the shape, the better. But again, there are major exceptions, such as the pace of innovation, where a lower score could represent a highly creative vendor with great ideas and excellent prospects for inventing something truly meaningful.



### TAG Navigator Example

The example below shows the value the TAG Cyber analysts assigned to a cybersecurity company that had engaged the team for assistance with strategy, planning, and go-to-market execution. The TAG Navigator values shown below were used to guide the engagement and provided a framework for discussion, debate, and advice given from the analysts to the principals managing this particular vendor.

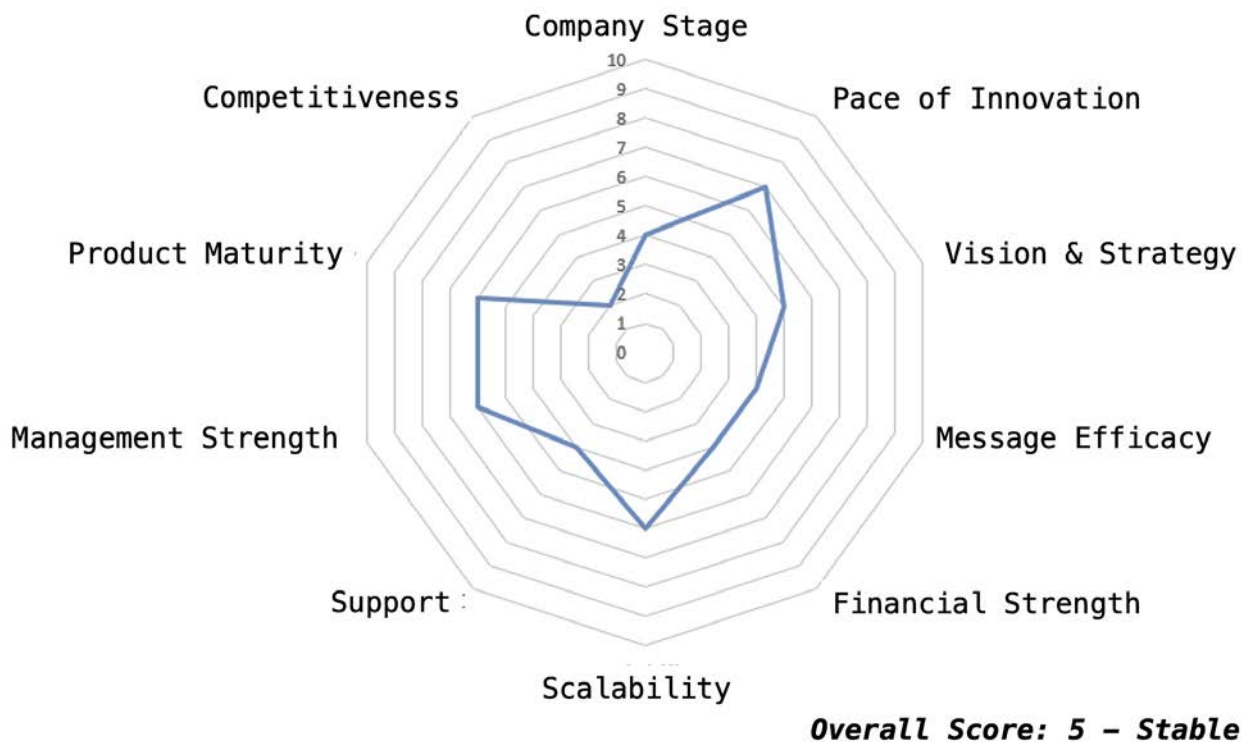


Figure 2. Example TAG Navigator Assessment

This example which comes from an actual cybersecurity company review<sup>2</sup>, shows an organization that can be summarized as follows:

8-10 – No attributes have these value, which is indicative of a cybersecurity company that has not reached maturity. This is not an issue on its own but could be a warning sign for a large buyer that prefers vendors with effective support teams.

7 – Pace of Innovation is high, which is highly indicative of a start-up vendor. This is one area where a smaller company might actually do better than a larger one, but again – larger buyers might prefer slower innovation from mature vendors.

5-6 – Several attributes hit this value including product maturity, ability to scale, vision and strategy, and strength of management – all indicative of a company developing well (these are good scores for start-ups).

4 – This shows that company stage, customer support, financial strength, and message efficacy are all just getting started. Buyers should pay close attention to these values since start-ups might struggle to scale their support.

2 – The only attribute showing early results is in the competitiveness area, which suggests a start-up doing work in an area with many competing options. Analysts look closely at this value, because it helps to determine whether the vendor pay special attention to developing a unique value proposition.<sup>3</sup>

The purpose of the TAG Navigator is to drive the type of structured, categorized discussion shown in the bullet list above. Certainly, considerable subjective opinion will drive these assignments – but for the authors, this is the essence of being an industry analyst. Stakeholders expect analysts to have opinions, and we believe that the TAG Navigator, as shown in the example, helps guide this process.

## CONCLUSION

The TAG Navigator challenges traditional methods of evaluating cybersecurity solutions by including more factors for evaluation, an auditable scoring approach, and an intuitive display of the reasons for vendor scoring differences. We have developed multiple real-world examples that have provided the basis for lively discussion. We will continue to use this model until either consensus is reached on its efficacy or lack thereof, in which case we will modify it. As the statistician George Box is often quoted: *All models are wrong, some models are useful.*

<sup>1</sup> It was determined that 1 would be a better starting point than 0 since it is unlikely that any cybersecurity vendor would exhibit zero value for any factor. Thus, we view 1 as the lowest reasonable value for a given factor. A zero would mean that the factor was not rated.

<sup>2</sup> We choose here not to mention the actual company involved since our process is still emerging for working out public relations, marketing, and related external approvals for sharing such data. Suffice it to say that this company, a promising start-up with high competition, matches well (in our estimation) the values shown in the example.

<sup>3</sup> Our TAG Cyber analysts team tends to spend considerable time with new cybersecurity start-ups to focus on their value proposition. Low competitiveness scores are a particular challenge because with many vendors working in the same area, the only meaningful differentiator for a start-up will be some unique statement of belief, an interesting founding story, or some other visceral attribute that separates the vendor from the competing pack.



*“I should have worked with TAG Cyber.”*

# ENGINEERING EFFECTIVE NETWORK DETECTION AND RESPONSE FOR THE ENTERPRISE

DAVID NEUMAN

---

Security architects and engineers are constantly faced with the challenge of how to best protect their networks from both internal and external threats. This paper addresses areas to consider when evaluating a network detection and response solution, including: 1) outlining the most common challenges faced when utilizing NDR, 2) highlighting how to gain real-time visibility, full-spectrum threat detection and advanced threat-hunting capabilities and 3) discovering how OpenText NDR provides complete visibility to hunt for and defend against threats.

## INTRODUCTION

Network security engineers and architects face numerous challenges in complex enterprises, equipping the security operations center (SOC) with valuable tools to defend against sophisticated cyber adversaries. Network detection and response (NDR) is an important part of network security, and it involves using various tools and techniques to detect, analyze and respond to threats on a network. Some of the most difficult challenges engineers and architects face when deploying NDR include:

**Scalability:** NDR tools can generate a large amount of data that needs to be analyzed in real-time to detect and respond to threats. As the network grows, it can become more difficult to scale and manage NDR tools to handle the increased volume of data.

**Advanced threats:** Attackers are constantly developing new and more sophisticated methods of evading detection. Network security engineers must stay updated with the latest tools, threat intelligence and techniques to detect and respond to these advanced threats.

**Integration:** NDR tools must integrate with other security tools and technologies by exporting data to a unified platform, such as security information and event management (SIEM), to allow for integrated response across the enterprise.

**False positives:** NDR tools can generate many alerts, and not all of them may be actual threats. Choosing a platform that provides a simple method for keeping the solution well-tuned is imperative to minimizing false positives.

The impact of not mitigating these challenges is the increased likelihood that security operations teams will miss intrusion and exploit attempts, resulting in material damage or disruption to a business. When teams lack visibility and fidelity into incidents, they lose the edge to intercept an attacker at the right time and place and with decisive action.

This paper will describe how an NDR helps enterprises gain real-time visibility, full-spectrum threat detection and advanced threat-hunting capabilities. We will also discover how [OpenText™ Network Detection & Response](#) provides complete visibility to hunt for and defend against threats.

## GAINING REAL-TIME VISIBILITY

The Russian critical infrastructure assaults on Ukraine from 2014 to 2016 were a series of cyberattacks that targeted key systems, including the power grid, financial institutions and government agencies. The attacks were part of a broader conflict between Russia and Ukraine that began in 2014 with Russia's annexation of Crimea and support for separatist rebels in eastern Ukraine. The attacks began in December 2015 with a coordinated power outage that left over 230,000 Ukrainians without electricity for several hours. The attack was carried out by a group of hackers known as Sandworm (Russian military intelligence), who used a sophisticated malware called BlackEnergy to access the control systems of the power grid. The attackers then used the malware to disconnect key power transmission stations, causing widespread disruption. In addition to the power grid attack, Ukrainian banks and financial institutions were also targeted with a series of distributed denial of service (DDoS) attacks in December 2015 and February 2016.

In June 2016, another cyberattack targeted the Ukrainian government, including the country's Ministry of Finance and State Treasury. The attack used malware called Petya, which encrypted files and demanded a ransom in exchange for the decryption key. The attack disrupted government operations and caused significant financial losses.

These attacks demonstrate the deep level of network access threat actors have across many organizations and the freedom of movement to launch these attacks to cause maximum damage. What is more concerning is that Ukraine was not nearly as connected as other countries, making real-time visibility into highly connected networks even more critical.

Threat actors thrive on network blind spots that allow them to blend with normal activity to escape detection and maintain significant dwell times in the highly sensitive parts of an enterprise. Advanced threat actors take a long-time horizon approach to persistent access, and engineers and architects must do the same with solutions for data collection in security operations.

Next-generation NDR solutions need to fuse real-time visibility, advanced detection, analysis, forensics, incident response and threat hunting into a single platform. This is how security teams battling advanced attackers gain complete insight with full context for immediate action. Instead of looking at events in isolation, teams collect all relevant information required for a successful investigation, including all indicators of compromise and detailed information about any other systems or clients—outside the network or within—where a suspected compromised host interacted.

## SMART PCAP

Traditional PCAP provides network insight by collecting all data packets throughout the network for analysis. While this is an important resource, it often leaves security analysts to parse vast amounts of data and alerts to get to the meaningful information they need. Smart PCAP captures the relevant data from packets associated with security events and then correlates that event to other necessary packet capture linked to logs and data to give the analyst historical and real-time information to make decisions. *The converged capabilities described above deliver real-time visibility while effectively using resources, reducing mean time to detect, capitalizing on investment by optimizing other technology stacks and applying the skills of security operating where they are most needed.*

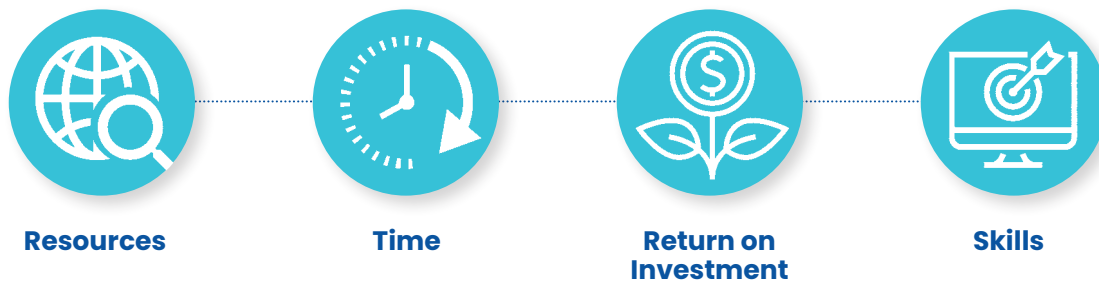


Figure 1: Value proposition to gaining real-time visibility

## FULL SPECTRUM THREAT DETECTION AND ADVANCED THREAT HUNTING

To detect advanced threats, you need to hunt them. These threats move in, out and laterally within an environment, often obfuscating their movements and activities in network blind spots or by hiding in normal traffic. With real-time visibility, a next-generation NDR solution can identify and allow for a rapid and efficient response to threats by focusing analysis on the most relevant traffic. For example, in a critical system that uses non-standard ports or protocols and which may generate seemingly anomalous behavior, an analyst with access to rich network visibility can recognize unexpected traffic based on endpoints, ports and observed applications. In this way, an advanced NDR solution provides the detection of threats that might otherwise go unnoticed in a sea of normal network traffic.

As new threats emerge, an NDR solution must adjust its rules and heuristics to identify relevant traffic, ensuring a team's hunting and detection techniques remain effective and efficient. These capabilities are essential to identify zero-day exploits or unknown, unidentified threats to give security operations advanced threat-hunting and detection capabilities, specifically in the following modalities:

**Threat intelligence:** Integrates with threat intelligence feeds, providing up-to-date information on known threats and attackers. Using full network visibility, indicators of compromise can be curated, tracked and used to engage adversaries.



**Automated response:** Automated response capabilities take action to block or mitigate potential threats as they are detected. For example, a solution may automatically block traffic from an IP address that is identified as a known threat or flag anomalous activity.

**Human expertise:** Advanced threat hunting often involves a combination of automated analysis and human expertise. Next-generation NDR solutions include tools and interfaces so security analysts can easily explore and visualize network data, enabling them to identify potential threats and take swift action to mitigate them.

The hunting and advanced-detection characteristics described above are essential to a security team's ability to observe, orient and act to disrupt adversaries before they can cause major damage to the business or operations. Architects and engineers must consider an NDR platform that empowers the team as a whole to stop the most advanced threats.

## OPENTEXT FOR NETWORK DETECTION AND RESPONSE

**TAG Cyber** recommends that any organization with network security and resiliency as part of their path to business success considers OpenText's NDR solution. OpenText NDR provides organizations with 360-degree protection, end-to-end visibility, the context for direct answers and powerful insight to take immediate action. The solution provides complete visibility of east-west traffic across network environments in real-time and full-spectrum threat detection that extracts and stores high-fidelity metadata, including an indexed threat-hunting repository.

A multifaceted suite of best-in-breed threat detection allows organizations to inspect network traffic thoroughly from every angle. Users can find unknown, hidden threats to conduct retrospective network traffic analysis and historical data testing to determine if threats infiltrated the environment prior to known indicators being available. They can use meaningful visualizations and flexible network views to see everything in a single view or create custom views for what matters most for their network.

*"Thanks in large part to [OpenText NDR], we can now detect and correlate events, investigate the data, and notify the client in an average of just 6.5 minutes—less than half our SLA."*

— Jeremy Conway, CEO, MAD Security

## OPENTEXT NDR ELIMINATES SECURITY BLIND SPOTS THROUGH REAL-TIME NETWORK VISIBILITY.

Organizations can see everything on their network via high-fidelity metadata and Smart PCAP, to take advantage of full-spectrum threat detection and reduce noise using multiple detection engines that examine the network from every angle. Users can proactively and with forensic precision investigate detected threats and hunt down unknown threats that did not generate an alert. With seamless response and extensive integrations, organizations can correlate alerts in real-time, enrich existing workflows, automate responses and prevent threats. OpenText NDR is an end-to-end network detection and response platform that allows security teams and the entire enterprise to collaborate better, reduce security risk and solve network problems faster than ever.

## Protect from all sides

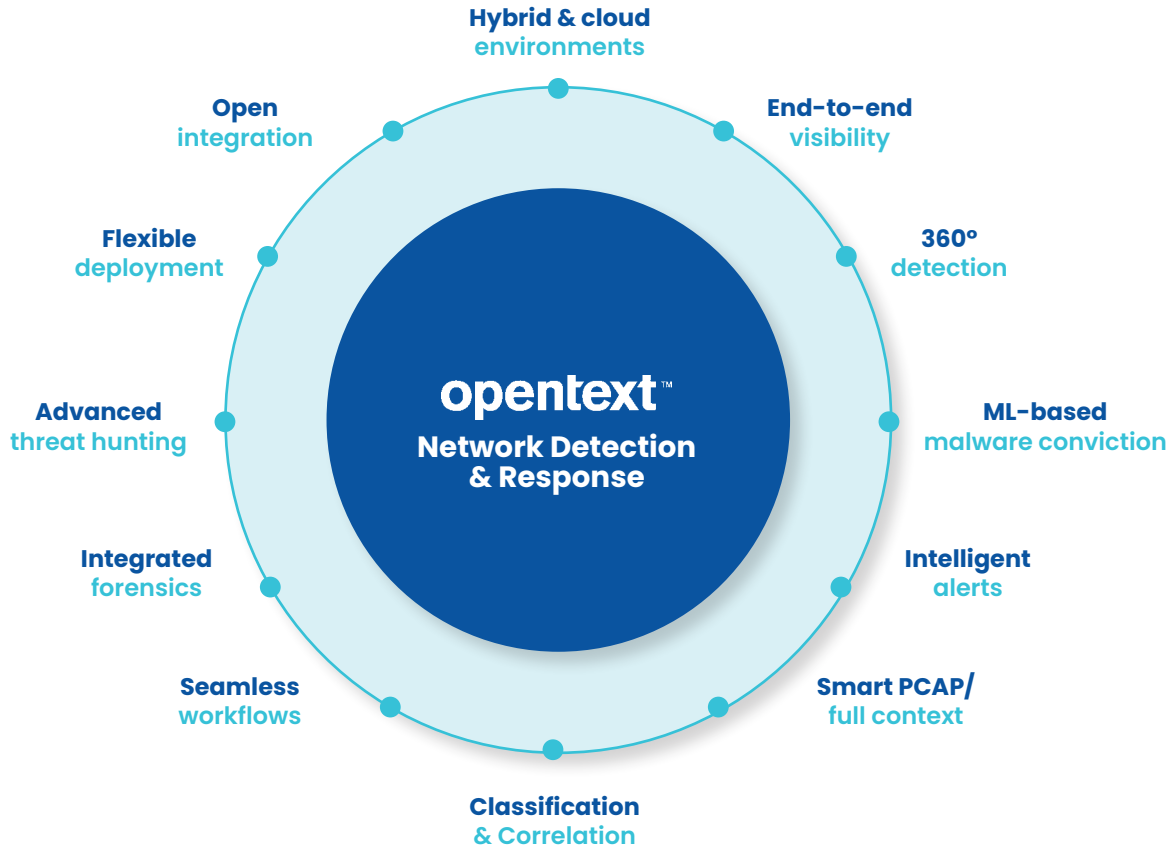


Figure 2: OpenText NDR

### OPENTEXT NDR HAS MANY ADVANTAGES.

**End-to-end visibility and meaningful visualization.** See high-fidelity metadata to know in real-time how users, devices, systems and applications are behaving on the network.

**Advanced 360 detection and powerful analytics.** Gain visibility into the known, unknown and pattern of unknown unknowns on your network with multiple threat detection engines, all while virtually eliminating false positives.

**Effective response and simple network instrumentation.** Respond to and correlate alerts in real-time with frictionless integrations to SIEM/SOC workflows and third-party threat intelligence tools and deploy smart sensors in just a few clicks to enhance your network.

**Advanced forensics and threat hunting.** Investigate and validate a threat with OpenText NDR's Smart PCAP, which provides enough data to follow the kill chain accurately. Follow a hypothesis to uncover an unknown threat or gain insight into normal operations. Even if you are using full PCAP today, ask the following questions: Is my current PCAP wasting SOC time and storage costs without the desired outcomes? Would we benefit from faster and more accurate threat hunting and incident response? Do I have the capability to identify, replay and solve for previously undetected threats that may return? If the answer is "yes," then you need a Smart PCAP solution.

Network engineers and architects researching an NDR solution should compare the following features:

Comparative Matrix		OpenText NDR	
Network Data Capture & Retention		Full network recording (first in, first out - FIFO)	X
		Smart PCAP recording (alert-based, retained for long periods)	X
		Network metadata, long-term retention (data nodes)	X
		High-speed (low-cost) sensor option, 10 Gbps+ in single appliance	X
Full-Spectrum Threat Detection	Keep Out	Package inspection	X
		Advanced malware detection (static - ML based)	X
		Network signature (e.g., TALOS, ET Pro)	X
	Find Within	Indicator of compromise (i.e., IP, URL or Hash)	X
		Threat-hunting workflows (non-alert driven) in-product (not via SIEM)	X
Threat Prevention		Intrusion prevention (inline) option	X
		Customizable signatures and scripts (bring, build or modify)	X
		Automated tagging & tuning of alerts (assignment, prioritization, severity)	X
		Multi-tenant data federation (single pane of glass)	X
		Cloud-based management & data retention options (not sensor)	X
		Customizable export options (Syslog, ECS, Netflow/IPFIX, JSON)	X
Deployment		Consumption-based pricing (pay for what you use)	X
		Cloud protection option (Google, Amazon, Microsoft)	X
		Software only solution option - bring your own hardware (at any speed)	X

Figure 3: OpenText Advantages

OpenText NDR (formerly Bricata) is a “hands-on” network detection and response platform that allows security teams and the entire enterprise to collaborate better, reduce security risks and solve network problems faster and more effectively. “Hands-on” can be interpreted in many ways, but OpenText NDR offers out-of-the-box features and capabilities at scale. In addition, by providing hands-on capabilities, OpenText allows security architects, engineers and analysts to meet mission needs unique to their SOC and the needs of their business. By fusing real-time visibility, advanced detection, analysis, forensics, incident response and threat hunting into a single platform, OpenText provides organizations with the most effective tools to find, understand and act on relevant threats to protect organizations from material damage.



# EDR AND CDR ARE DIFFERENT. HERE'S HOW.

TAG CYBER ANALYST TEAM  
SUPERVISED BY DR. EDWARD AMOROSO

---

This report proposes that endpoint detection and response (EDR) is a fundamentally different discipline than the various protection methods being increasingly referred to as cloud detection and response (CDR). The goal here is to help buyers differentiate between the marketing messages coming from commercial cybersecurity vendors.

## INTRODUCTION

The cybersecurity industry uses many different acronyms, such as SIEM, SOAR, CWPP, CDR, SOC, CIEM, CSPM, DSPM, SSPM, CNAPP, IAM, IDP and IGA, most of which were created to help differentiate between the various commercial products available for enterprise buyers.

The acronym EDR, which stands for endpoint detection and response, is used to designate modern endpoint security solutions which evolved from early antivirus and endpoint protection software. EDR generally references commercial products that provide continuous monitoring and malware protection for endpoints, often using behavior analysis and machine learning.

A new term is emerging, CDR, which stands for cloud detection and response. The term helps characterize products that are designed to modernize security operations and threat detection and response capabilities for cloud environments. Such environments include identities, service interactions, containerized workloads and virtualized workloads. This new category is prompted by the obvious shift of enterprises to cloud services and infrastructure.

In this article, we explain the differences between EDR and CDR. Our goal is to support the enterprise buyer who might be led by vendors to believe the two capabilities are the same. While it is fine for a commercial vendor to include both in their roster, EDR and CDR represent different technologies.

## WHAT IS ENDPOINT DETECTION AND RESPONSE?

Because the cybersecurity industry has not standardized any category of solution, acronyms will reference whatever a given vendor chooses to include. That said, an EDR solution typically includes the following set of capabilities to protect endpoints such as Windows PCs:

- *Activity Monitoring* – This involves collecting data from an endpoint to highlight relevant activity that might indicate a cyberthreat.
- *Continuous Analysis* – This references the ongoing and real-time nature of EDR solutions to analyze activity and data for threat evidence.
- *Automated Response* – This designates the goal to quickly respond to any detected issues with an automated task, usually in the form of an alert.

While EDR references activities—namely, detection and response—that are reactive in nature, most EDR solutions are installed specifically to prevent malware and other attacks that target endpoints. (It is worth mentioning that the types of protections that work for laptops, desktops and servers don't always work in cloud and cloud-native environments.)

It is beyond the scope to list all EDR vendors, but TAG Cyber analysts can help buyers in this regard. That said, CrowdStrike, SentinelOne and Microsoft are three of the larger EDR vendors, and we mention them to establish context. Buyers should select the EDR vendor that best matches their needs.

## WHAT IS CLOUD DETECTION AND RESPONSE?

As suggested earlier, no accepted standards exist to define acronyms in the cybersecurity industry, so buyers should pay close attention to the features included in a commercial offering. That said, we view references to CDR as typically including the following set of capabilities to protect cloud assets:

- *Containers and Kubernetes* – These include integrated protections for scanning images, fixing configurations, addressing threats to containers, benchmarking compliance, enforcing policy and avoiding risky activity related to Kubernetes.
- *Cloud Workloads* – These detect and remove threats and vulnerabilities from physical and virtual machines, containers, serverless workloads, and other cloud-hosted resources and assets.
- *Cloud Infrastructure* – This includes protection of cloud computing support and infrastructure to ensure best practice design and deployment, and to ensure that user access, entitlements and other cloud attributes are properly secured.
- *Cloud Identities* – These analyze user and machine identities and associated permissions for all assets in cloud and cloud-native environments.
- *Service Interactions* – These analyze how identities, workloads and functions interact with other resources across environments to inform event correlation and detect potential indicators of compromise.
- *Cloud Remediations* – This involves remediation of threats to the cloud, with a focus on the vulnerabilities involved and support for managing fixes, and planning root cause analysis.

As can be seen from the above descriptions, the various activities included in CDR range from detection and response activities inherent in most cloud protection suites, to security monitoring and reporting of metrics for operational, management and board-level teams.

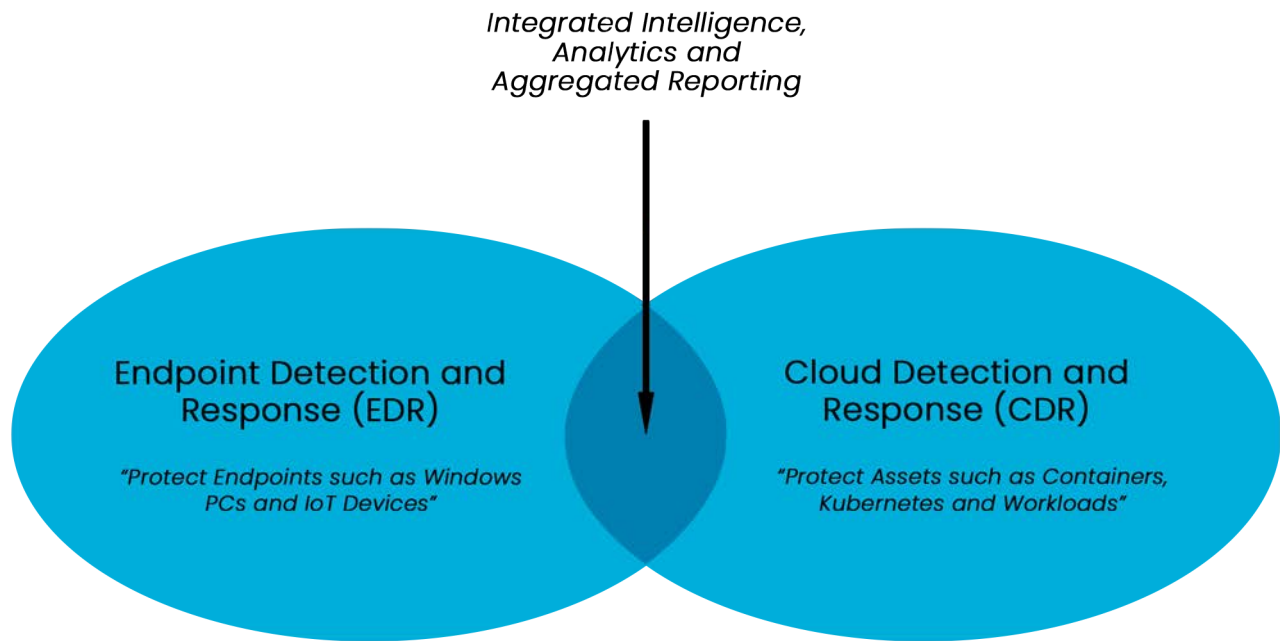
## HOW DOES THIS IMPACT CISOs?

The key observation for CISO-led teams is that EDR and CDR solutions might be marketed and presented as being closely linked, at least as far as vendors claims about protecting your assets. As analysts, we see them as largely separate tasks. Endpoint systems and cloud assets require different



handling, support and attention due to abstraction, virtualization and containerization. Therefore, when a vendor claims that workloads are “just a different type of endpoint,” we find the reference misleading.

Perhaps the best way to view EDR and CDR is via a Venn diagram where the respective security and functional concerns are represented separately, and where common sharing and support functions intersect. The result is a view of how EDR and CDR work together in a typical enterprise, and while this appeals to our observation as analysts, we say that buyers should handle source selection carefully for these important areas.



**Figure 1. Understanding the Roles of EDR and CDR**

Our advice to security professionals is to focus on the following three issues when selecting both EDR and CDR commercial offerings:

- *Details of Security Requirements* – The primary goal is to ensure that the EDR provider meets the desired security requirements of your diversified cloud assets and that the CDR provider meets the desired security requirements. This does not demand that the same vendor offers EDR and CDR. In fact, it will be common that EDR and CDR vendors will be different.
- *Select the Best Vendor* – The goal should be to select the best set of vendors with the optimal technology and support for both EDR and CDR. Endpoints and cloud are such important assets that enterprise teams should not compromise on quality or effectiveness. Good vendor selection will have a significant impact on cloud security operations.
- *Integration is Desirable* – The primary goal for EDR and CDR should be comfortable integration with available cyberanalytic support, common sharing with the SIEM or other security tools, and the ability to benefit from common resources such as threat intelligence.

If the selected vendor for EDR and CDR should happen to be the same provider, that’s fine, so long as the granular security requirements are met, integration is supported, and sufficient effectiveness and coverage are offered. However, we see only marginal benefit from the claim that EDR and CDR are essentially the same type of activity. Our observation is that this is misleading, and vendors specialize in different domains.

# WHY ENTERPRISE BROWSERS SHOULD BE INCLUDED IN COMPLIANCE FRAMEWORKS

DR. EDWARD AMOROSO

---

The emerging availability of commercial browsers with strong security-enhanced features for enterprise warrants inclusion in popular cybersecurity compliance frameworks.

## INTRODUCTION

One can make a reasonable case that a browser might be the most important application used in every modern enterprise organization today. And yet, curiously, many security teams do not include the browser as an application in their official inventory. Instead, teams often take browsers for granted, and this can lead to significant lost opportunities to strengthen enterprise cyberdefense.

Recently, our analyst team at TAG Cyber reviewed excellent commercial offerings that include desirable new security features that are embedded into the browser. These features are driven primarily by the needs of the modern enterprise and are consistent with both the cyberthreats experienced by most organizations, and the types of security controls that are considered desirable.

In this brief we make the case that commercially available enterprise browsers are now sufficiently mature that their associated functionality should be included in every cybersecurity framework. We pay particular attention to security features that support the concept of last-mile protection for security endpoints, which complement (or even supplant) many existing enterprise security controls.

## BENEFITS OF ENTERPRISE BROWSERS

The types of security requirements enterprise teams should demand from their browsers come in three distinct categories. First, browsers should be free from vulnerabilities. This has been an especially nagging issue since self-propagating malware could no longer rely on open access to target networks through open ports on the firewall. Entry points required exploitable vulnerabilities, so browsers became popular targets. This must therefore be prevented.

Second, creators should design browsers that provide reasonable options for individuals or organizations to either remove or avoid having to use other comparable tools. Consider, for example, that endpoint security has emerged as one of the most expensive line-items for IT and security teams. As such, if the browser can offer cheaper alternatives consistent with budget (or lack thereof), then this is desirable.

Finally, browsers should provide so-called *last-mile protection* for the end-user since the browser provides the most direct interface with the user of any applications. If malware finds its way through the typical gauntlet of controls that exists between a web application and a user, then the browser should provide a final safety net to protect local resources. This is also useful for risks that emerge from careless or unintentional misuse of data.

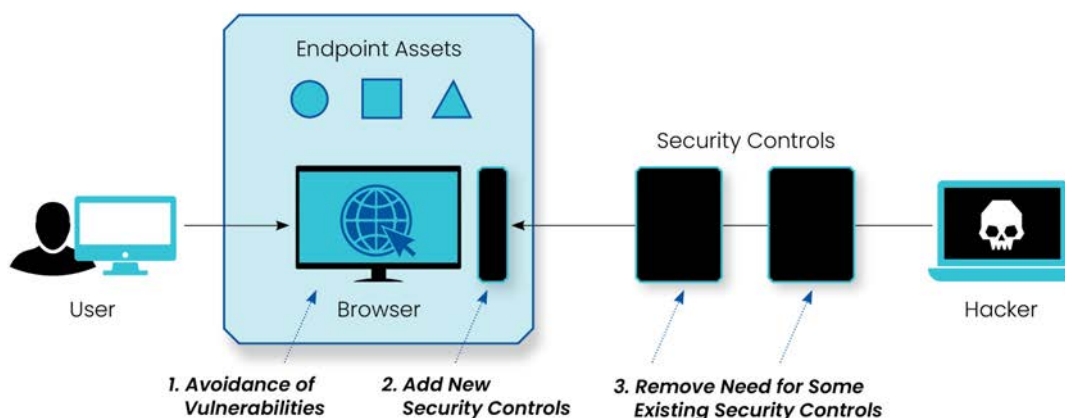


Figure 1. Security Roles for the Browser

The implication of last-mile browser defense is that we recommend pre-integration with existing PC and device controls such as endpoint detection and response, content disarm and reconstruction, and anti-malware security software. The business opportunities are significant for vendors, certainly, but the real value will come from enterprise teams who will experience better endpoint security.

## PROPOSED INCLUSION IN FRAMEWORKS

A significant issue in modern cybersecurity is that the existing popular frameworks dictating the protection control architecture for most enterprise teams are largely silent on last-mile browser security capabilities. This creates a gap in programs, especially ones that are highly influenced by formal frameworks, including in highly regulated industries such as financial services, utilities and telecommunications.

A review of existing popular frameworks,<sup>1</sup> including the NIST Cybersecurity Framework, Payment Card Industry (PCI) Data Security Standard (DSS), and International Standards Organization (ISO) 27000 series confirms this last-mile gap. None of the frameworks includes, for example, copy-and-paste controls for the browser and some barely scratch the surface of browser-based controls.

One excellent resource for information on browser security controls is the Chromium Security website maintained as part of [The Chromium Projects](#). The Chromium security team provides users of its open source (which is the basis for most enterprise offerings) with security features consistent with the following principles: help users safely navigate the web, design for defense in depth, security is a team responsibility, speed matters and be transparent.

Given such excellent resources, our TAG Cyber analyst team urges the purveyors of security frameworks and any other stakeholders to begin to address the standards gap. We believe that a set of simple requirements can be defined that will fit well into modern compliance frameworks. Even if enterprise teams opt not to address these requirements, their inclusion will increase awareness and help promote use where it will be most important.

We summarize the specific last-mile browser security requirements we recommend for inclusion in frameworks such as NIST 800-53 and PCI-DSS:

- **Data Management.** The browser should include functional controls for where and when users can copy and paste data, print and save pages into or out of applications.
- **Device Posture.** The browser should include means for confirming that device security status is acceptable before granting access.
- **Developer Tools.** The browser should govern whether to allow developer tools (e.g., viewing page source) for enterprise applications.
- **Screen Capture.** The browser should manage whether to allow or authorize requested screen captures.
- **Browser Extensions.** The browser should include controls that consider which extensions are acceptable for installation.
- **Data Storage.** The browser should include controls for how data is stored and under what types of conditions.
- **Geographical Controls.** The browser should use location as the basis for geo-fencing controls required by an enterprise.

We urge readers to consider improvements to the list presented above, and framework curators will likely have opinions about improved wording, references and other means for presenting the new control statements. Regardless of the implementation process, we hope that the industry starts to take last-mile browser security controls more seriously, and that this is codified in our major security frameworks.

<sup>1</sup>This technical review was performed in late 3Q22 by the TAG Data Research team including Iassen Christov, Carlier Hernandez, Shawn Hopkins, Khanjan Patel and Nick Wainwright.



**DISTINGUISHED  
VENDORS**



## DISTINGUISHED VENDORS

Q 2 2 0 2 3

**W**orking 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.



AccSenSe is an easy-to-use IAM business continuity platform for Okta, allowing Okta customers to easily and quickly recover from cyberattacks in minutes and misconfigurations with a click of a button. With a complete set of enterprise features, accSenSe provides resilience and peace of mind so organizations know IAM systems are no longer a single point of failure.



Adaptive Shield is a leading SaaS Security Posture Management (SSPM) company, enabling security teams to maintain a secure SaaS app stack by continuously monitoring SaaS apps, users and their devices, while also identifying misconfigurations, assessing SaaS-to-SaaS risk and fixing any weakness. Adaptive Shield works with many Fortune 500 enterprises to help them secure their SaaS threat landscape.



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.

# TAG CYBER DISTINGUISHED VENDORS

2 0 2 3

## appdome

Appdome is the one and only solution needed to protect, Certify Secure and monitor threats and attacks against Android & iOS mobile apps right inside the mobile DevOps CI/CD pipeline. Instantly defend mobile apps and customers from mobile app security breaches, mobile fraud, mobile malware, cheating and other attacks with ease.



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.



Balbix enables businesses to reduce cyber risk by automating cybersecurity posture. Our SaaS platform ingests data from security and IT tools to create a unified view of cyber risk in dollars. With Balbix, you can automate asset inventory, vulnerability management and risk quantification, leading to lower cyber risk, improved team productivity and tool cost savings.



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 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.

## CYBRARY

Cybrary is the industry-leading professional development platform designed to bridge the cybersecurity skills gap. With threat-informed training, advanced assessment capabilities, and certification preparation, Cybrary enables more than three million learners—from individuals, service providers and government agencies to Fortune 1000 organizations—to build the skills and knowledge needed to confidently mitigate the threats faced by their organization.

# TAG CYBER DISTINGUISHED VENDORS

2 0 2 3



Cyera is reinventing data security. Companies choose Cyera to: improve their data security and cyber resilience; maintain privacy and regulatory compliance; and gain control over their most valuable asset—data. Cyera instantly provides companies with a holistic view of their sensitive data and security exposure, while delivering automated remediation to reduce the attack surface.



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.



Finite State helps product security teams and connected product end-user organizations (asset owners) leverage comprehensive, context-aware vulnerability intelligence to assess or generate SBOMs to ensure a continuous state of risk reduction and improved software transparency. Regardless of any given product's software, firmware or component composition, Finite State helps reduce third-party software supply chain risk.



HUMAN is a cybersecurity company that protects 450+ enterprises by disrupting bots, fraud and account abuse with modern defense. We verify the humanity of more than 20 trillion digital interactions per week, protecting against account takeover attacks, fake account creation, payment fraud, content manipulation, content scraping, PII harvesting and denial of inventory/stockout attacks.



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.



RegScale frees organizations from manual, paper-based processes via its continuous compliance automation software. Our API-centric software integrates with security and compliance platforms to manage the security control state, shifting compliance left to deliver audit-ready documentation in the world's first real-time GRC platform. Heavily regulated organizations use RegScale to start and stay compliant.

# TAG CYBER DISTINGUISHED VENDORS

2 0 2 3



SnapAttack is an enterprise-ready platform that helps security leaders answer their most pressing question: "Are we protected?" By rolling intel, adversary emulation, detection engineering, threat hunting and purple teaming into a single, easy-to-use product with a no-code interface, SnapAttack enables a company to get more from its technologies and teams, making staying ahead of the threat not only possible, but also achievable.



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.



Swimlane provides cloud-scale, low-code security automation for organizations of all industries and sizes. Our technology is rated as the #1 trusted low-code security automation platform. Our mission is to prevent breaches and enable continuous compliance via a low-code security automation platform that serves as the system of record for the entire security organization.



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 together with leading manufacturers and critical infrastructure operators to develop practical, operations-friendly 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.



