TAG

Security Annual

1ST QUARTER 2024

IN FOCUS:

SEC v. CISO

ARTICLES / OPINIONS / INTERVIEWS

CONTENTS

TAG Cyber SecurityAnnual
1ST QUARTER 2024

Lester Goodman, Director of Content

David Hechler, Editor

Contibutors

Dr, Edward Amoroso
Joanna Burkey
Pete Dinsmore
David Hechler
Moriah Hara
David Neuman
Al Palimenio
John Rasmussen
Joe Sullivan
Jay Wilpon

Editorial & Creative

Lester Goodman
David Hechler
Jaimie Kanwar
Miles McDonald
Rich Powell
Stephanie Amoroso

Research & Development

Matt Amoroso
Shawn Hopkins

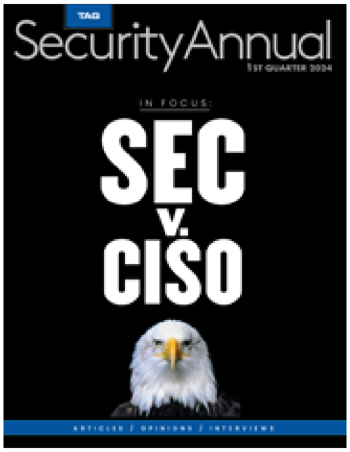
Sales & Customer Relations

Rick Friedel
Michael McKenna
Laurie Mushinsky
Julia Almazova
Jane Mangiamele

Administration

Liam Baglivo

Dr. Edward Amoroso, Founder & CEO



Volume 10, No. 1

Publisher: TAG, a division of TAG Infosphere, Inc.,
45 Broadway, Suite 1250, New York, NY 10006.
Copyright © 2024 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 Infosphere, Inc. assume any liability for any injury and/or damage to persons or organizations as a matter of products liability, negligence or otherwise, or from any use or operation of any products, vendors, methods, instructions, recommendations, or ideas contained in any aspect of the TAG Security Annual volumes.

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

The opinions expressed in this document are those of the writers and contributors and in no way reflect those of its Distinguished Vendors.

January 24, 2024

IN FOCUS:

SEC ACTIONS PROMPT QUESTION:

WHAT IS THE CISO’S ROLE?

INTRODUCTION

A TOPIC WE COULDN'T IGNORE

DAVID HECHLER, EDITOR

We try to focus on a variety of subjects in the feature section of the Quarterly. We don't want to be too predictable. But sometimes a subject is simply unavoidable. That was the case here.

If we had any doubts, they were quickly erased when our founder, Ed Amoroso, posted a provocative **article** on LinkedIn in November. It was his response to the SEC's **charges** against SolarWinds and it's CISO, Tim Brown.

The SEC **alleged** that between the company's IPO in October 2018 and its disclosure of a nearly two-year long cyberattack known as "SUNBURST" in December 2020, SolarWinds and its CISO had "defrauded investors by overstating SolarWinds' cybersecurity practices and understating or failing to disclose known risks."

What Ed wrote was a call to arms. He urged the SEC to lay down its own. The SEC should acknowledge that all companies are being hacked, he said. He advised the agency to publicly proclaim: "Investors should expect and assume that all public companies are in some stage of being attacked. You do not need to be informed by their CISO or any other official."

The responses to Ed's article confirmed what we already knew. This is a topic about which our audience is passionate. Many of the comments were unusually long and articulate. They ranged from high-fives to adamant dissents.

The next step was a roundtable conversation in December that Ed helped arrange with colleagues from New York University, where he teaches. The **recorded discussion** featured Joe Sullivan, the former Uber CISO and a former federal prosecutor; Randy Milch, who teaches law and is co-chair of NYU's Center for Cybersecurity; Joel Caminer, who is a senior director at the center; and Ed. We transcribed and edited the presentation for length and clarity. The resulting article, "Roundtable: SEC and the CISO's Plight," is the first of two.

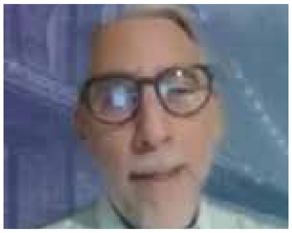
The roundtable covered a lot of ground. But we wanted to add an article that would vigorously argue the SEC's position. We considered the comments Ed's LinkedIn post had elicited, and we contacted one commenter: Matthew Rosenquist, a former Cybersecurity Strategist at Intel and now a cybersecurity industry adviser. Rosenquist had compellingly defended the SEC, and he hosts a podcast called The Cybersecurity Vault. He quickly agreed to invite Ed to join him for an energetic discussion. We transcribed and edited the **podcast**, and we called the article "The Great Debate: SEC Rules, the SolarWinds Case, and the CISO's Role."

The articles are long, but we think you'll find the conversations move swiftly. There's more depth than we usually find in discussions of this sort, drawing readers into areas they probably have not considered. And each can stand on its own.

Please let us know what you think.

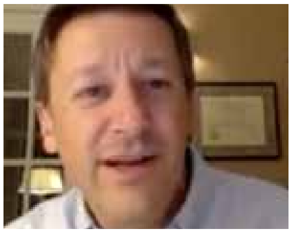
"I'm looking for a sympathy card for a colleague just promoted to CISO."

ROUNDTABLE:
SEC AND THE CISO'S PLIGHT


Joel Caminer

Randy Milch

Two actions by the Securities and Exchange Commission late last year provoked anger and anxiety in the cybersecurity industry—particularly among chief information security officers. First came the enforcement action against SolarWinds and its CISO, Tim Brown. Then the finalization of the SEC's rule that requires companies to report cybersecurity incidents within four days after determining they are "material." TAG Cyber CEO ***Ed Amoroso*** *and his colleagues at New York University, where he teaches at the engineering school, decided to record a video of a roundtable conversation about the implications of these events. Amoroso was joined by* ***Randy Milch****, who teaches law at NYU and is co-chair of its Center for Cybersecurity. Previously he was the general counsel and head of public policy at Verizon Communications. They invited* ***Joe Sullivan****, the former chief security officer at CloudFlare, Facebook, and Uber to join them. Sullivan, a former federal prosecutor, was the first prominent CISO who found himself in the crosshairs of law enforcement when he was convicted of obstructing a Federal Trade Commission proceeding and concealing a felony in the wake of a hack at Uber. He remains widely respected in the field. The discussion was moderated by* ***Joel Caminer****, a senior director at NYU's Center for Cybersecurity, the institution's interdisciplinary research center which brings together faculty from NYU and other schools to discuss the most relevant topics. What follows is an edited version of their talk.*


Ed Amoroso

Joe Sullivan

Randy Milch: The first thing we're going to talk about is the SEC action against SolarWinds and its chief information security officer. This is a federal court action. It's somewhat unusual in the sense that most of these are administrative proceedings from the SEC, which also tend to settle. But this clearly did not. The SEC went ahead and filed this fraud action in federal court in the Southern District of New York. Condensing a 200-paragraph complaint into something that's a little bit more digestible, the idea is that SolarWinds and Brown, because of statements that were made from the time of SolarWinds' IPO in 2018 until its third statement about the SUNBURST hack in early 2021, had issued a set of assertions about the security practices that they would undertake. This was in the so-called security statement that Mr. Brown put out. And then in their initial filings to register themselves when they became public again, they had a series of risk factors. And one of them was about cybersecurity.

Timothy Brown, identified by the SEC in its complaint as SolarWind's "then-Vice President of Security and Architecture"

The gravamen of the complaint is that even at the time of the security statement, but certainly thereafter, announcements were made about the processes—things like password management, access control, whether SolarWinds followed secure development lifecycle, whether SolarWinds had followed the NIST Framework, and there were significant deficiencies in following these processes. The actual practices deviated at times from what was in the statement, and the risk factors and particularly the vulnerabilities were insufficient when compared to the SEC's allegations. As time went on, the SEC pointed to new facts and repeatedly suggested that Brown and SolarWinds should have updated its risk factors. It didn't through that two-and-a-half-year period, and that's something I think we ought to talk about.

There are also allegations about what happened after the SUNBURST hack. There are allegations about some additional blog posts that Mr. Brown made, but the gravamen is that this was fraud on the investing public because a reasonable investor would have wanted to know that they didn't follow the NIST Framework in its entirety and that access control was weak. That is the basic complaint. Generally these things settle, and the failure to settle here indicates that SolarWinds was not interested in what the SEC wanted from them. In particular, given the fact that they're going personally against Mr. Brown, SolarWinds was not eager to throw Mr. Brown under the bus. They were going to support him. And they've continued to support him. I think that, in part, is what has driven the wedge here, and how we end up in a federal lawsuit. There are questions about how far the SEC has pushed its rules and its precedents. There are questions about whether they're trying to substantively regulate cybersecurity for a nonfinancial company, where they don't really have direct regulatory control. And there's a question about if you have to disclose the status of your vulnerabilities, how do you do it in a way that is meaningful but doesn't give the bad guys a great roadmap?

Joe Sullivan: I don't sit in the CISO role any longer, but I do spend a lot of time talking with security executives. And in fact, I led a two-hour Chatham House rule conversation today with 25 CISOs. We literally talked for two hours about this case. I got to hear what a lot of them are really thinking. And I've been hearing the same things over the preceding weeks. I've talked to Tim at SolarWinds about the case. And so I would say that the security leadership community is shaking in their shoes. They feel completely misunderstood, both in terms of the SEC's expectations of them and their ability to have influence and actually get stuff done. The reality for them as security leaders is that they don't get an unlimited budget, they don't get an unlimited team. And even when they raise issues, it's a risk judgment debate that often goes above the security executive for a decision. So they're not the ultimate decider on everything security inside their organization. Lots of them don't even own all the different aspects of security. And they definitely don't own the implementation of everything. Some of them are very much auditors. Others have engineering teams. But they're all over the place in terms of who they report to, how big their teams are, what percentage of company expense goes through them, how much of a strong voice they have in leadership. That's the first part.

The second part is they don't understand this expectation that they're supposed to be the reviewer of content coming out of their company. CISOs have talked for years about how it's not their job to decide whether something is a quote unquote data breach. They investigate and respond to incidents, but it's someone else who decides whether the company is transparent, and how transparent, and where they're transparent. And so they're panicking and thinking that they need to start reading every single thing that their company says about security. Where are all the things that my company is saying about security? I understand in Tim's case that the SEC is alleging that he personally wrote some of the content. It sounds like that was in 2018. So often we're talking about things that happened five years ago, It'll probably be six or seven years by the time this thing works its way through court. And the last thing I would say is that the SEC referenced a lot of internal texting between security team members. Every single CISO believes that their teams have exactly the same type of internal conversations, because who do you hire for your security team? You hire people who want perfection, who are going to fight hard to champion perfection and improve security inside their company. And their job is to spot issues and try and get them fixed. It's a natural kind of tendency of security team members to be like: "The sky is falling. We need more resources." One of the questions they asked me today was, "Do I need to tell my team to stop talking about security?" And we all agreed: "No, absolutely not. We want to have those kinds of conversations. That's the healthy direction." And it's scary that that can be used against them.

"SAFETY CULTURES DON'T BEAT UP PEOPLE WHO REPORT, AND THEY DON'T MAKE EXAMPLES OF THEM. THAT'S NOT A SAFETY CULTURE. THAT'S A RETRIBUTIVE CULTURE."

Ed Amoroso: Randy and Joe, really good observations and very clear thinking. Joel, I've been nervous for years that there is a paradox in our industry that probably only people like us know, but anybody even two steps away from us may not get. And here's the paradox. I think all of us would agree to the truth of the following statement: "Nation-states coming after you, or just a really capable actor, they're gonna get you." And Randy and I both worked for really big companies with really big budgets and really big teams. And I would have said it then, and I would say it now. The reason there's a paradox is because implicit in much of what we hear from the government is, "Hey, clean up your act and make sure nobody's getting in." I mean, that's a very logical thing. The paradox is we work hard to try to do that knowing full well that, at least right now, you really can't. So life becomes this weird version of a game. You know that joke where two guys are in the woods and a leopard's coming after them? And one guy puts his sneakers on, and the other guy says, "You can't outrun a leopard." And the guy with the sneakers responds, "I don't have to. I just need to outrun you." Cybersecurity is sort of like that. It's like trying to keep your house in order and—this is going to sound terrible—hoping that nobody has it in for you. Because if they do, they're gonna get you.

Now, here's the other paradox. This is for the SEC. And I had quite a few collisions the last few weeks on social media when I was saying things I thought were utterly obvious. But maybe some people don't agree. And it's this—it's my message to all investors, particularly investors in cybersecurity companies. Everybody is in some stage of either having been hacked, or being hacked right now. Mueller said that. Remember [FBI Director] Robert Mueller on the big stage? He said: "There are two kinds of companies. Ones that know they've been hacked, and ones that have been hacked but don't know it yet. There's all kinds of versions of that. But what it extrapolates to is a former director of the FBI stating on the record that everybody's being hacked, which further drives home this idea that investors should factor that in and recognize that there are vulnerabilities in a company like SolarWinds. Name a cybersecurity company. I won't put any on the spot, but pick one and I'm pretty sure they're not following NIST. I'm pretty sure that Joe or myself could go in there with our little team and find 1000 things that are wrong. And that's true everywhere. So it's sort of like, "Hey, investors, this is the great leveler. We're all in this problematic posture. We're working as hard as we can." And I don't think there's a CISO on the planet that is just sitting there negligent, saying, "I'm going to be negligent. Who needs to be stopping cyberattacks?"

The Securities and Exchange Commission building in Washington, D.C.

Milch: I think there's one important point here in addition to what you said—which I agree with 100%. This disclosure regime has always been a bit bizarre to me. On one hand, what are you going to say that's meaningful to an educated investor that is not incredibly meaningful to your antagonist? So there's this desire for perfection in the disclosure that seems bizarre. But take this one step further. The SEC was very clear in this complaint that if the SUNBURST hack had never happened, they would have regarded both SolarWinds and Mr. Brown as already having committed fraud. So you didn't need the hack. Their comparison is between the stated desire in the security statement to follow NIST, the stated desire to have strong passwords, the stated desire to have a least-access regime, and failing to do that. You're supposed to disclose something about your failure to meet your stated goals. This is a big expansion. We have seen the SEC go after folks who have internal processes with risks that are too hypothetical, they would say. And there have been four or five actions by the SEC. All were administrative and all settled. [See examples here and here and here.] They were actual breaches, and there were failures associated with the breach. This takes it back a big step. The notion that you're supposed to generate some sort of meaningful disclosure about your failure to have strong passwords everywhere is sort of ludicrous. I don't even know what you would say. I mean, if you were to do that, as the lawyer who used to help craft these disclosures, I don't know what I would say to my CISO. "What can I say about this?" And then they would look at me and say, "I don't know, Randy, this is your problem. This is not my problem." Exactly what you said, Ed. But this goes a step further, because we're in the vulnerability realm. We're in the risk realm. We're not in the you've-been-hacked realm. I guess you would say everyone's in the process of being hacked, but there seems to be an event at a certain point. This is in the precursor stage.

Sullivan: One of the questions that kept coming up with the group of CISOs—since you have the experience of crafting these things: Is there going to be a tension between what the legal department and the company want to say versus what the security leader wants to say? Because the security leaders are thinking right now, "We want to be really, really transparent and paint a very dire picture." They're also worried that their lawyers will say no, because every time we file one of these, someone's just going to sue us. Like the plaintiff's lawyers are just going to have an automatic. "Oh, you just said your security's not good? Now we're going to sue you." So they're trying to figure out how active they, as operational professionals, need to be in micromanaging the disclosure statements that the lawyers are going to write. And is there going to be a tension there?

Milch: I don't see how there's *not* going to be a tension. As a general matter, you generate these risk statements, and then it's an iterative process. You're going to the experts in your company to make sure that they ring true, that you haven't missed anything, that you're not overstating something. If you look at the SolarWinds risk statement that they put out in 2018 and didn't materially change, it seems pretty comprehensive. It says pretty much, "We're in a risky business. We're going to try. We may not be successful. We may not have the resources. It's going to be expensive." I mean, they say all these things, right? "And if we have a breach, it's going to be horrific" is what they basically say. And the SEC will say, "Well, you said 'if,' and that leads people astray." Two things are true. One, it's a huge waste of time if your chief information security officer is spending more than a nanosecond worried about SEC disclosures. That is not their job. It's not what they should be worried about. I would think it's good governance to run it by them and good practice to make sure that it's comprehensive. If there's some aspect you've missed, you want to put it in there at a high level. And number two, there will be a lawsuit. There is always a lawsuit. There's someone who writes on Bloomberg who has said very clearly that everything is securities fraud now. If your stock goes down a tick, it's because of securities fraud. And I think there may just have to be this wave. I personally would be very supportive, Ed, of absolutely dire disclosures. Because if everyone does it, then there won't be an appreciable diminution of your stock vis a vis your competitors.

Amoroso

"THIS IS WHAT I GOT ON SOCIAL MEDIA: 'ED, YOU BIG JERK, YOU'VE BEEN SAYING YOU WANT MORE RESOURCES. THIS IS GOOD. TAKE ADVANTAGE OF IT, MOVE UP INTO THE C-SUITE.' AND I WOULD SAY, 'I DON'T THINK MOST OF US WANT TO BE THERE.'"

Amoroso: The thing that we've been coaching to CISO teams, consistent with what Joe said, is preplanned language and automated workflow. Joe and I would say every cybersecurity problem breach breaks down to 20 or 30 things. Mitre Att&ck would say 200, but you can group them. So you could probably write with your lawyers 10 sentences where you just leave out something. And then when there's a problem in workflow, I say it should all be automated. Because if I need something dependable in real-time four days [the SEC's stated timeline for reporting breaches], could be it happens on Thursday. My daughter's getting married Friday. We have family over Saturday and Sunday, and oh my God, Aunt Gladys, who's 100, passes away on Sunday. I could be a public company that makes shoes. And suddenly there was an attack and what, I'm negligent?

If you're telling me it has to be real-time, the only thing I've ever been able to depend on in my whole career of doing this over those 40 years is automation. You can't depend on people or process. It just breaks down. So I've been saying the incentive here is to preplan a bunch of different notifications.

That's what an 8-K is. But I'm just talking about the specifics of the incident. Get those worked out with your lawyers, and then from the SOC all the way through GRC through your whole team, embed the workflow. When there's something going on, there should be automation that involves the lawyers' workflow. I think the insurance companies should be involved as well. It should just happen. And boom, it gets shipped off to the SEC. I know, they don't want that. But I think that if they get 10,000 a day, maybe they'll rethink this.

Joel Caminer: Joe, you were talking earlier about talking to CISOs and what they're feeling right now. I read what the SEC was claiming [SolarWinds was] not truthful about. And I know many CISOs who have had to explain that even to their boards of directors—that I can't guarantee you certain things won't happen. It's a risk management conversation. And so to the CISOs that are sitting there not just trying to figure out disclosures and their own personal risks now, but still have to manage their staffs and manage a security program, I'm wondering how they're thinking about communicating and managing and dealing with all the operational aspects that sit in an enterprise security program.

Sullivan: One thing that they're all doing right now is they're using this case as an opportunity to have a conversation with the entire exec team at the company. This is a rare opportunity for security leaders to actually try and get more resources. But they're worried because they feel like the SEC has picked on one officer—they called Tim Brown an officer. I don't know if he's an officer or not, I always thought that that was kind of like a term of art. And maybe we should change our title.

Milch: We don't know the way SolarWinds had him though, right? He was a VP.

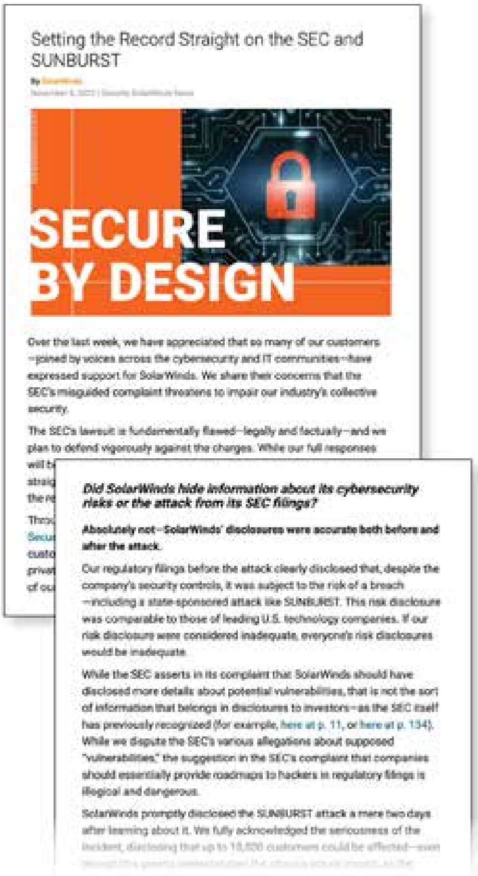
Amoroso: Let's assume he is. But here's the problem. I think the majority of CISOs that I interact with are kind of gearheads. I'm not saying that they're just tech nerds, but gearheads in the sense that they're not trained to be a general-purpose executive. That's not why you go into this. Maybe this shifts things. Maybe you get a general-purpose risk executive who becomes the CISO's boss. I don't hate that. And I'll bet 99% of CISOs would say, "I would welcome it. Please bring someone in to do risk." CISOs are not equipped to do it. From the teams that I've always been around, the texts are always, "Holy shit." And then they name 50 things. "Call the CEO and say they need to fix this tomorrow!" Not realizing that the CEO has to do the calculus of about 100 factors. And there might be things way more urgent than fixing some vulnerabilities in legacy routers. So I don't like the idea when people go—this is what I got on social media—"Ed, you big jerk, you've been saying you want more resources. This is good. Take advantage of it, move up into the C-suite." And I would say, "I don't think most of us want to be there. We want to do our job. We're not

Caminer

"THERE'S BEEN SO MUCH GREAT ACTIVITY, AN OPENNESS, A COLLABORATION WITH DHS AND CISA, AND OTHER ORGANIZATIONS. IT FELT LIKE WE WERE MAKING REALLY GOOD PROGRESS THE LAST COUPLE OF YEARS. AND THIS HAS THE POSSIBILITY OF UNDERMINING SOME OF THAT."

trying to be sitting across from the CEO doing strategy for the corporation. That's not why people do this."

Sullivan: You're exactly right. I said at the beginning that CISOs feel misunderstood. The reality of the CISO profession is that it barely existed 20 years ago. Most of the people didn't have a title, didn't sit in an exec room. Most of them, when they got into the role or they started in this profession and started moving to the top, the ceiling was at a very different place. It was somewhere around director of IT level at best. And so the people who are at the top of the profession right now, when they got in, they thought the top was a very different place. And if we did a survey of 100 CISOs, we'd find probably 100 different backgrounds in terms of technical capabilities, types of schooling, degrees, who they report to, what type of resources they get. If you go into any of the CISO Slack groups that I'm in, CISOs love to talk about where should we report because some of them are buried, and some of them report to the CEO. It's all over the place. If we stopped one of our CFO friends and said, "Hey, my kid wants to be a CFO someday," they'd say. "I want them to go major in this, I want them to intern in that. I want them to have these seven things, and then they'll be ready." There is not a CISO in the world right now who got that guidance and aimed that high. A bunch of people who were aiming lower are all of a sudden on a very different, very hot seat.



Setting the Record Straight on the SEC and SUNBURST

By SolarWinds

November 8, 2023 | Security SolarWinds News

Over the last week, we have appreciated that so many of our customers—joined by voices across the cybersecurity and IT communities—have expressed support for SolarWinds. We share their concerns that the SEC's misguided complaint threatens to impair our industry's collective security.

The SEC's lawsuit is fundamentally flawed—legally and factually—and we plan to defend vigorously against the charges. While our full responses will b
straig
the re

Throu
Secu
custo
privat
of ou

Did SolarWinds hide information about its cybersecurity risks or the attack from its SEC filings?

Absolutely not—SolarWinds' disclosures were accurate both before and after the attack.

Our regulatory filings before the attack clearly disclosed that, despite the company's security controls, it was subject to the risk of a breach—including a state-sponsored attack like SUNBURST. This risk disclosure was comparable to those of leading U.S. technology companies. If our risk disclosure were considered inadequate, everyone's risk disclosures would be inadequate.

While the SEC asserts in its complaint that SolarWinds should have disclosed more details about potential vulnerabilities, that is not the sort of information that belongs in disclosures to investors—as the SEC itself has previously recognized (for example, here at p. 11, or here at p. 134). While we dispute the SEC's various allegations about supposed "vulnerabilities," the suggestion in the SEC's complaint that companies should essentially provide roadmaps to hackers in regulatory filings is illogical and dangerous.

SolarWinds promptly disclosed the SUNBURST attack a mere two days after learning about it. We fully acknowledged the seriousness of the incident, disclosing that up to 18,000 customers could be affected—even [illegible]

Nine days after the SEC filed its complaint, SolarWinds fired back by posting an article on its website called "Setting the Record Straight on the SEC and SUNBURST."

Amoroso: We call those tribes. You could come up from government, you could come from compliance, you could come from audit, you can come from tech, you could come from development, you can come from any number of things. And these are all very different tendencies. Think about the difference between somebody who was doing internal audit and slid over into the job, versus some hacker who was really good at pen testing, got promoted, and is still wearing sneakers to work every day. And suddenly you're the CISO. Completely different backgrounds. Those two people can barely have a conversation. In fact, if they have a conversation, they'd probably be arguing.

Sullivan: I ran a mentoring program for CISOs a couple of years ago. The goal was to teach CISOs business because most of them didn't know how to read a P&L. It was all foreign to them. And all of a sudden they're getting pushed into these exec rooms with the CEOs and the board and are expected to be able to keep up. Like you said, they lived over in a technical or audit corner of the company, and now they have a lot more attention and a language they don't speak.

Amoroso: Joe, we probably have to bring some folks from [NYU's] Stern [Business School] to help us with our master's program. Randy, you and Joel are the bosses. Why don't you guys get a little bit of Stern influence into our program. Maybe one or two lectures on basic corporate finance.

Caminer: At the same time, it'd be great to bring Joe into our CISO executive certificate program and share some of those insights with our aspiring CISOs. Joe, I want to go back. You had a really nice post about this, talking about how much this really impacts a lot of the progress that we had been seeing recently. There's just been so much great activity, an openness, a collaboration with [the Department of Homeland Security] and [the Cybersecurity and Infrastructure Security Agency], and other organizations. It felt like we were making really good progress the last couple of years. And this has the possibility of undermining some of that.

Sullivan: Yeah, another reason this case is such a kick in the gut to the security leaders in the private sector is because most of them did, and do, love the job because it's very mission-oriented. You're fighting the bad guys. You come to work every day protecting people. You represent the customers of your company, and you fight to keep them safe. That's why everybody does it. They love the mission. That's why so many people who are ex-government are doing security inside companies. It's the only place inside a corporate environment where you are fighting the bad guys. But we can't win against the bad guys by ourselves in the private sector, and the government can't win in fighting the bad guys without the private sector. That's the reality of the internet. We expect government to protect us as citizens everywhere in the world. Most of those contexts, the government has 100% control, visibility, access. But on the internet, it's all run in the servers of private companies. And if the goal is to get everybody working better together, actions like this are not helping, because it's not going to be a good, healthy transparency. It's going to be a CYA [cover your ass] transparency. We're not feeling like we're on the same team anymore.

Sullivan

"I THINK CISOS WANT REGULATION. THEY WANT REALLY CLEAR LINES. BUT CISOS DON'T HAVE A VOICE IN THAT CONVERSATION. THERE'S NOT A SITTING CISO WHO CAN GO TO CONGRESS AND SAY, 'I WANT MORE REGULATION.' BECAUSE THEIR COMPANY WILL FIRE THEM."

But I want to throw a curveball at you guys. Let's imagine for a second we're in the shoes of the SEC. I think that government enforcement agencies feel the need to do something about internet crime. Unfortunately, Congress hasn't acted. There's no federal data breach law, even though it's been discussed a million times. And I think partially it's because our companies have blocked it. A lot of the big companies don't want regulation. I think CISOs want regulation, they want really clear lines. But CISOs don't have a voice in that conversation. There's not a sitting CISO who can go to Congress and say, "I want more regulation." Because their company will fire them. And so it's us ex-CISOs who are the only ones who can speak up. And I think we want more regulation. We want more clarity out of Congress. But in the absence of that, we have these enforcement authorities saying, "I can fix this." But they're using inexact tools. They're bringing a bazooka to a knife fight, because that's the tool that they have. The SEC, they have one tool, right? They can go after companies for their statements, if they don't like those statements. So they're going to keep doing that. Is that the right way to get companies to invest more in security? Is that the right agency to be doing it? I don't know.

Amoroso: That's not a curveball. Let's take your sentence: "Government enforcement agencies feel the need to do something." Now let's think back in history. How does that usually turn out? Not quite sure what to do, but we've got to do something. Are there a lot of cases where that works out, or does that usually lead to some colossal mistake? Usually leads to mistakes.

Sullivan: Especially if it's an agency that's not full of people who are experts in this area. I think one of you referenced this earlier. CISA has done a great job of building partnerships with the private sector, hiring people from the private sector. They actually understand the challenges of CISOs. Every security conference I go to I see people from CISA in the hallways talking to practitioners, understanding their pain, asking, "What can we put out that will help you?" They're a small and growing agency, but DHS is backing them. And they're partnering with the private sector, and we get better security.

Milch: It's critical, Joe, that we remember that CISA is not an enforcement agency. They deliberately decided not to be an enforcement agency in order to foster the exact kind of partnership that you're talking about. And I think that that's critical. If I were advising a CISO, I would say, "Don't ask for more regulation, because the way that regulation is going to pan out is not going to give you the warm and fuzzies. You're never going to get regulation or a law that says, "Joe, Ed, Joel, do the following 17 things and you're safe." That's not the way that's going to work. It's always going to end up being something that is dealt with in hindsight, the way this is being dealt with in hindsight. And it's effectively diminishing the notion that this risk management function ought to be left to the designs of experts within the company to deal with. I do think it's important, as you do, Joe, to look at the other side of this from the SEC perspective, or any government agency's perspective. They all want to be in cyber, because otherwise they're not relevant. There's a perception that companies ought to be spending more on cybersecurity. How do you get companies to spend more on cybersecurity? There are two general ways. One is you could play with their taxes. If they spent more on cybersecurity, they get a credit on their taxes. That might be valuable. That usually is the way we incent things in our country.

Sullivan: Or we could give them immunity for quick reporting [of breaches] by companies.

Milch: Quick reporting? That would be another way of doing it. Anything that you want, you can bring it on by things like taxes, immunity, safe harbors. The plaintiffs lawyers hate them. The administrative agencies hate them. Because here in particular, just think of what that safe harbor rule would be. Joe, you undertake reasonable cybersecurity practices in your company, we'll give you a safe harbor. That's great until the shit hits the fan, and we're going to have a big argument about what reasonable is. And here, through the backdoor of materiality, they're essentially doing the same thing, right? They're deciding that certain things that SolarWinds didn't do, they should have reported because they were material. And essentially it's turned that word into a substantive cybersecurity standard on an ad hoc basis. It's like you had SolarWinds123 as a password. That was material.

Sullivan: Every company has a version of that. That's the circle of this conversation. We're back to the beginning again. Randy, I guess the ultimate question is: What's the definition of materiality in this context? And are we ever going to get more clarity?

Amoroso: I think that the SEC was clear. I don't know that I agree. It creates these odd scenarios. For example, Community Bank Acme has $100 million in revenue. And they have a breach that's a $10 million breach, which is 10% of their revenue. By any reasonable interpretation, that's material. So they're in the process of figuring out what to do. But suddenly, Community Bank gets bought by Wells Fargo, which makes $200 billion. Now suddenly the $100 million is just a little blip. The $10 million thing is like change that fell out of your pocket. It's not material anymore. So they're very clear that it's about investors, not about operational. Joe, you, Randy, and I would say it's the same breach, the same impact, same problem, same community bank structure. But if they're in the context of a larger company, now for investors it's not material. That's why as operators we look at it, and you can't help but roll your eyes and say, "This is voodoo economics we're dealing with here."

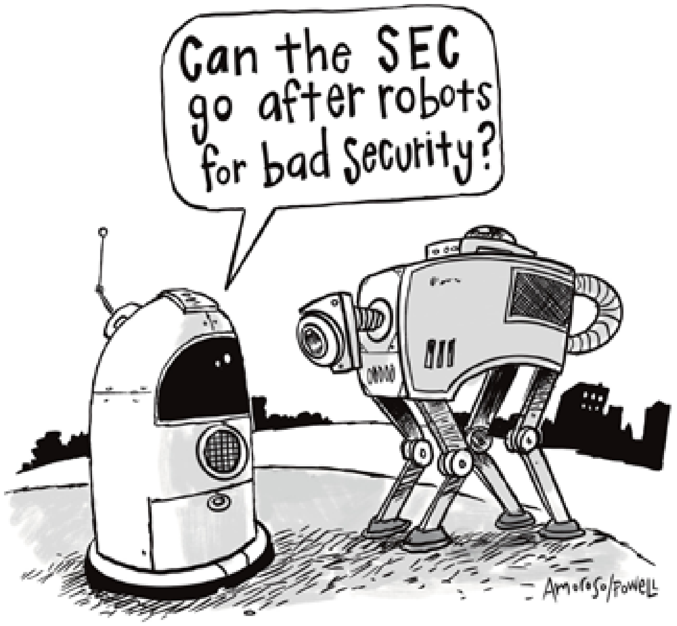
Caminer: There's a lot to unpack on this issue. But we're running a little close on time. So why don't I just do a quick roundtable for final thoughts. Randy, maybe I can start with you.

Milch: I would simply add to my CISO friends that they've got to stay strong. There will be some changes from this storm. But the changes we don't need are failing to communicate with people, failing to encourage communication up through your chain, and failing to communicate up the ladder as well. If that happens, that's a real big problem. I think that from a longer term, we really need to adopt a safety culture about this. And safety cultures don't beat up people who report, and they don't make examples of them. That's not a safety culture. That is a retributive culture. So if we could come up with ways to incent better behavior, that'd be great. But kicking people is not going to get us there.

Sullivan: Yeah, if anything good comes out of this, it will be that the rest of the executive teams at these companies will be taking notice, and hopefully helping the CISO prioritize the work. What we don't want is good people to not want to go into this profession out of fear. And that's something I worry about. I've seen some good people step down from CISO roles and say, "Wow, I have like 100 pounds lifted off my shoulders." I remember last October when I stepped down from Cloudflare's CSO role, and the next morning I woke up and I'm like, "I don't have the weight of 20% of the internet getting hacked because of me on my shoulders anymore." And it just felt liberating. I was worried about doing my job—the protective side—not worried so much about an enforcement action coming against me. The job is really hard as it is. Because we're the only people in the executive and business world who have adversaries on the other side: intentional, active, smart, funded adversaries. Nobody else in business has to worry about that.

Amoroso: My only comment here is I don't think the SEC is going to change their mind. They're not going to back down. They're probably going to turn this up. So my advice to anybody who's a practitioner is to develop the language in advance, build automation, and work it into your workflow. And then once you've done that, you can just do your work. I think it meets the letter of the law. It's probably a little passive-aggressive, but it really does match up with the sensibility of the language that's being thrown at us

View the full roundtable discussion.



THE GREAT DEBATE

THE SEC RULES, THE SOLARWINDS CASE, AND THE CISO'S ROLE

The discussion below was adapted from a podcast. TAG CEO ***Ed Amoroso*** *had posted an article on LinkedIn that criticized the SEC for charging SolarWinds and its CISO for allegedly defrauding investors by overstating the company's cybersecurity practices and understating or failing to disclose known risks. Amoroso's article was greeted by comments that ranged from ovation to consternation. In search of a suitable partner for a debate, TAG's editors contacted* ***Matthew Rosenquist****, who had posted one of the comments defending the SEC. A cybersecurity industry adviser, and a former Cybersecurity Strategist at Intel, Rosenquist also hosts The Cybersecurity Vault podcast. He quickly invited Amoroso to join him for an in-depth conversation. An edited version of the transcript follows.*

Matthew Rosenquist: I'm going to be talking with Ed Amoroso, the founder and CEO of TAG Infosphere. He's an author, research professor at New York University, and a highly respected, longstanding member of the cybersecurity community. Thank you for joining and weighing in and providing some perspectives on this. It's been a controversial kind of case, don't you think?

Ed Amoroso: I do think so. There's a lot of different perspectives here. Everybody has the same goal. We'd like to see our infrastructure more secure, like to see businesses more secure. So we're all paddling in the same direction. It's just there are a lot of different paths, and there's different opinions about the right way to get there. I hope eventually we reach a common goal. But right now I think there's a little bit of confusion about the best way to proceed.

Matthew Rosenquist: Normally, there's a tremendous amount of ambiguity and chaos that causes confusion. And then we start getting some of the regulators coming in. This particular complaint against SolarWinds and their CISO is 68 pages. Very articulate. And they're calling out fraud. It's about knowingly misrepresenting or attesting to something on SEC forms that go to shareholders or people looking to invest. What's your read?

Amoroso: Hopefully you'd agree that the first thing you want to do is factor out things that don't have a lot to do with the CISO position or industry. Like

GRAPHIC DESIGN BY STEPHANIE AMOROSO

if there was stock bought or sold. That's not really a cyber thing. So, in my mind, it's more about the SEC's points that they're trying to make, the kinds of things that they've been pushing with the recent ruling around the four-day reporting.

Rosenquist: Which just went active. I heard a lot of tears hitting buckets out there.

Amoroso: You and I in some sense came out with slightly different positions on this. Here's what I wanted to ask you. I'm not the greatest investor in the world, I think the idea here, if I'm getting it right, is that if you and I were lawyers at the SEC, we're there to protect investors. That's why we get up every day. And you and I are glad they do that. I'm for that.

Rosenquist: That's our tax money, by the way. So we better be glad about that.

Amoroso: Here's what I think they have in mind. Let's say you have Acme Industries over here and Consolidated Manufacturing over there. Two little companies, and you and I might decide to invest in one or the other. They're both public companies that do something similar. And we ingest information from the internet to decide whether we're going to buy stock. Let's say that Acme has a cyber breach that they don't tell me about, and I buy their stock and it goes down. But I could have bought the other guy's. If they had just told me, then I would have bought this other thing, and I'd have made money. "Hey SEC, I'm mad. Make sure that they tell me in the future." Do I have that right?

Rosenquist: Yeah. Let's take a step back and ask, "Why was the SEC even created?" The SEC was created in 1934. It was coming off the heels of the 1929 stock disaster. And in 1933 and 1934, a couple of legislations were passed that basically said, "Shareholders have rights. They have the right to be informed of important things in companies that they either may invest in or currently invest in." Public companies had to report quarterly numbers, which they still do. They had to report certain material events with the 8-K form. They still do. They have to report if they're going to release more stock. They have to release other financials for prospective investors. The whole idea is investors have rights. They have the right to be informed. Otherwise, what you get is a small group of people that have insider information—better information than the shareholder or prospective shareholder—and they can make trades on that and you get market manipulation. After these rules were created, the SEC was formed to say, "Hey, not everybody is going to actually abide by these. So we need an institution to set the rules up and then go investigate and prosecute these things."

Amoroso: Let's take my earlier example of Acme and Consolidated. The presumption is that Consolidated doesn't have the same problem that Acme has, and I think that's wrong. I say 100% of companies do. And that's what James Comey said. He said, "There's only two kinds of companies, ones that know they're getting hacked, and ones that are getting hacked and they don't realize it." And that's Consolidated. So the SEC is creating a perverse incentive for CISOs to automate the 8-K [quarterly form] process, and just say "I'm always under attack." I'll give you an example. I made a joke one time when I was working in telecom. I thought it was a joke, and then I think the lawyers thought I was serious.

Rosenquist: They don't have much of a sense of humor.

Amoroso: I said, "When we hire people, why don't we just tell them, 'Listen, we didn't lose your identity yet. But we probably will. So just sign here, and I'm telling you now that I'm probably going to do something stupid later.'"

> **"IF YOU'RE GOING TO SAY, 'NO, I THOUGHT IT WASN'T MATERIAL,' THEY'RE GOING TO SAY, 'WHAT'S YOUR PROCESS?' 'OH, WELL, I THREW A DART.'"**

Rosenquist: It's the stupidity clause. You want them to sign a stupidity clause saying you understand that, as your employer, I'm stupid. And you recognize that. You missed your calling. You should have been an attorney. I would have hired you.

Amoroso: I'm just saying that the simple solution to the reporting exercise is to go into workflow. And as your SOC generates problems, and they mark them as potentially sev 1 [severity 1] or something, start workflow. Get it all reviewed. And if the lawyers don't have the time–if it happens on a Thursday night and everybody's away for the weekend–then the workflow just goes right through to the SEC and says, "Look, our SOC detected this problem that could be an issue. We didn't have four days to figure it out. So we're just telling you now that this could look serious." Or if you're a CISO and you're sick with the flu or something for two weeks, or you're away, you've done a lot of traveling. I just think it's creating an incentive for people like me, who automate everything, to automate the process. I don't want my team sending texts around saying this could be bad, because that's what security teams do. And it's my job as the CISO to let my SOC team say, "Oh, my God, this is horrible. The whole place falling apart." And then I say, "Wait a minute. No it's not." And a week later they realize, and you realize, that this isn't such a big deal. But in four days, I would have no choice but to go to the SEC and say, "Listen, we're still hashing this out, but this could be bad. So I'm telling you now." I think what's going to happen is that this will create volume.

I fundamentally believe that cybersecurity resilience and achieving a high state of protection posture is still a research question. I don't think it's a matter of doing the risk management and being better organized. I don't think CISOs right now know how to stop a nation-state. So my advice has been: This is still research. You can yell at me all you want. I can't do it better than I'm doing it now. If the SEC is going to say, "We're going to put a hammer down. You've got to tell us," I think that the right thing would be for 100% of the Fortune 500 to report every Friday that they've gotten hacked.

Rosenquist: I'm going to challenge you on this, because I think there is a healthy amount of tension in the system. The 8-K is really designed to say that there is a material event. And let's delineate. This has nothing to do with the four-day requirement that just came into effect. This is something that happened back in 2000.

Amoroso: It was a different world back then, by the way.

Rosenquist: It absolutely was. And I think that should be taken into account. But before I go into this, about the healthy tension, we do have to recognize our form of justice means everyone is innocent until proven guilty. We can talk about these things, but I am presuming that the people at SolarWinds and the CISO are innocent until proven guilty in a court of law by a jury of their peers or a judge. But when it comes to filing that 8-K—and I don't think there's going to be a flood of them—companies file them all the time. They need to be timely. And they need to be something that is material. And there are materiality thresholds. Every big company has materiality thresholds. If you go to finance, they'll tell you what it is.

Amoroso: But it's a funnel, Matthew. For example, in a larger company it might be several hundred things per day that pop up that could be material.

Rosenquist: Right, but they've got a process to deal with that.

Amoroso: Not in four days. I'm just saying there's an awful lot of companies where you don't know inside four days if I have to report it.

Rosenquist: Yeah, but we're talking about the SolarWinds one, right?

Amoroso: Well, I'm trying to generalize.

Rosenquist: OK, then let's generalize.

Amoroso: Let's say you and I, you're the CISO and I'm the Deputy CISO for some bank. I understand that the SEC would like us, because we work for a public bank, to make sure if there's something an investor should know that they know it. All I'm saying is that when it comes to cybersecurity, it's a different game because even if you think and I think that we're fine right now, I'm telling you that we're not fine. When did you hire a pen tester that didn't find something horrible?

Rosenquist: They always find something.

Amoroso: Why would I hire a pen tester? I'd rather not know.

Rosenquist: Because there are different thresholds, right? There are things that happen in an organization every single day that may cause issues.

Amoroso: I'm not talking about the simple stuff.

Rosenquist: We're talking about the major things. And the rule as it's currently written is once you realize it is material. So let's just take the Acme example. If we go to finance an Acme Company and go, "Hey, CFO, what's your materiality threshold when you have to file 8-Ks?" And they go, "Oh, well, for our company, size of revenue, it's $1 million. If it's $1 million, I've got to write an 8-K. So if we lose a major client that was giving us $1 million in revenue, I've got to write an 8-K." OK, cool. I'm going to go back to cyber. And now I'm going to say, "OK, our threshold are impacts we believe with a high degree of confidence will be $1 million." So we've got so many customers. All right, if we lose data for 20% of our customers, we believe that's the $1 million threshold.

Amoroso: Who are you talking about? Who is this person? Who in the company is realizing this?

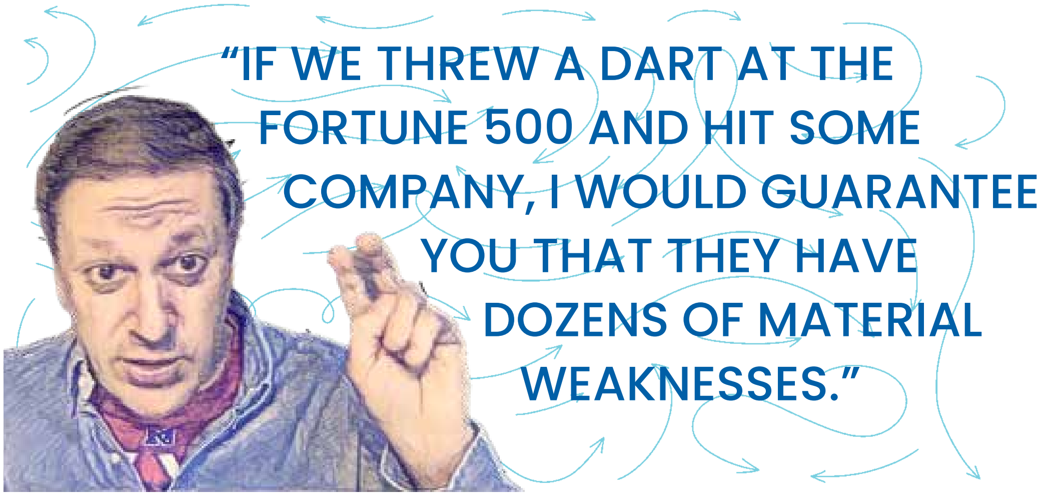
Rosenquist: The CFO has their numbers, because they have to file 8-Ks all the time.

Amoroso: This is the CFO realizing materiality?

Rosenquist: The CFO does have materiality, because they have the work—

Amoroso: The Chief Financial Officer, not the CISO.

Rosenquist: Right. But for the company, the materiality that's impacting the stockholders the CFO understands, because they've been in this role for a while—



“IF WE THREW A DART AT THE FORTUNE 500 AND HIT SOME COMPANY, I WOULD GUARANTEE YOU THAT THEY HAVE DOZENS OF MATERIAL WEAKNESSES.”

Amoroso: And CFO, it’s not a real-time position. They could go three days to their daughter’s wedding, and not be available. What happens when there’s a material issue and I don’t have the CFO available?

Rosenquist: You don’t need to. This is a process. If you understand your company’s materiality per $1 million dollars of impact—

Amoroso: Let’s go through an example. We’re in a SOC: “Oh, my God, there’s S-3 buckets open. Holy crap, there’s customer data in there. This could be a disaster.” You don’t know. You call the CISO.

Rosenquist: You activate your incident response team, your—

Amoroso: I’m not sure. I’m saying I don’t know. I haven’t realized, but it might be bad. So I have to report, correct? If I’m pretty sure this is a problem, but then later on I realize I was wrong—

Rosenquist: Let’s make it a clear process, because that’s part of what they’re going to look for. If you’re going to say, “No, I thought it wasn’t material,” they’re going to say, “What’s your process?” “Oh, well, I threw a dart. We’ve got a dart board and—”

Amoroso: I advise 120 companies, and I’ve spent my life on this. This is complicated stuff.

Rosenquist: It is. And at Intel I spent 24 years, and I was their first incident commander. I was involved with every major issue that occurred.

Amoroso: I think this is a research issue as well.

Rosenquist: There were situations where something is coming in. And you think, “OK, let’s say it’s a data breach. The trip wires have been fired. We know somebody inappropriately went into an area. We don’t necessarily know if the data has been compromised. If the confidentiality or integrity could have been tampered with, we don’t know yet. OK, let’s start doing our investigation.” And one of the first things is how important is that data? It’s not important at all. You mean, we could lose it all, and it wouldn’t be a material impact to the investors? OK, I know I’m not going to be reporting this to the investors. Oh, wait, this is the core code to Microsoft Windows or to Intel’s chips. OK, that’s a little bit more important. The moment we realize, hey, that’s now been exfiltrated out, that’s when I’m sitting down—

Amoroso: One hundred percent of companies are in that state right now for everything.

Rosenquist: But you need to have proof to say that it’s actually occurred.

Amoroso: I can just tell any investor I’m probably really hosed up by a nation-state.

Rosenquist: What’s your evidence? Are you really sure?

Amoroso: I can predict that I’m probably hacked.

Rosenquist: Prediction is for the future. That's different. The 8-K isn't about "I believe something in the future is going to happen." It's something has happened, You need to know. And it needs to be tangible. It needs to be something you can justify, especially if you're going to give bad news to your investors.

Amoroso: Here's what I mean. And by the way, you layout a very reasonable point. I'm not a good investor, but I am an investor. I'm for the SEC doing this. You and I both want more security. We're all there. I'm just saying that right now, it's a question. It's sort of A or B. It's either this is something that the government can jump into and start driving good behavior, or it's premature for them. I feel like it's premature. I think you're more on the side of they should do something now.

Rosenquist: I think they're late. Honestly, I think they're late. These 8-K rules have been around forever. Why wasn't cyber automatically embedded in them?

Amoroso: Here's the depressing part that I believe freaks a lot of people out when I say this. I really fundamentally believe that if we threw a dart at the Fortune 500 and hit some company, I would guarantee you that they have dozens of material weaknesses, serious breaches, and it's just a matter of going and looking.

Rosenquist: Wait. You just said going and looking. And let's go back to what the SEC is about. It's about making sure everybody has the same level of information. So if a company does not know that they are breached—let's say China, Russia, Iran, North Korea, they all own them—but they don't know. Well, the executives and the investors had the same amount of information. There's no difference. The moment the executives know, they need to share that.

Amoroso: Well Matthew, if you and I are investing our money, just assume every company is hosed. It's true. Like every single company is hacked.

Rosenquist: It's true. But as an investor, the moment the executives know something significant that I don't know—

Amoroso: Then don't tell the executives, It creates a weird perverse incentive to not tell the execs.

Rosenquist: I think the incentive is the execs do want to know so they can get ahead of this.

Amoroso: No, because once they realize, they've got to go tell. So don't tell me.

Rosenquist: You could get executives going, "Hey, don't send me any email at all. I don't want to know of any bad news." You could have executives, but they're probably not going to be in business very long. They're not going to be adaptive to the industry—

Amoroso: I don't agree with that. You and I both have a lot of experience. We can think of cases—I know you can—where there's a Bad Thing A that happens and a Bad Thing B that happens, and they both have their lifecycles. And one unravels and the other unravels. Both of them can look just horrible. But one turns out to be nothing and one turns out to be a really simple thing.

Rosenquist: Yes.

Amoroso: And what you're saying is the SEC would say, "Well, don't tell me until you're really sure that it's this terrible thing, then you've got four days." And I'm saying I have control over that. And it creates a perverse incentive to not get to that point for a very long time.

Rosenquist: I would say it creates a positive incentive for the organizations to drive their process procedures to be able to come to a determination faster, better, and more confident. And the disincentive is if I don't do that, then I have to report it. And that's going to go to my shareholders.

Amoroso: I'm rooting for you to be right. Because it's a positive story. Let's hope that I'm all wet. And what you're saying is the SEC's activity does drive better goals. You're describing a future where we make more progress. And I'm describing one where everything has already gone to hell.

Rosenquist: Which, if you look at our industry, probably it's closer toward yours that the idealistic viewpoint of where I want it to go.

Amoroso: For our audience, I think the right thing here is that the correct approach is to do what's right. There's a red-face test. We hold the mirror up. And I think, Matthew, what you're saying makes perfect sense. There are times when you realize that there is a big problem. And the SEC is saying, "For God's sakes, when you hit that point, tell me." It's just I'm not sure who the "you" is. What if it's the deputy CISO, who realizes it but can't find the CISO and is afraid to call the CFO?

Rosenquist: I think there just has to be a process. Because there's coverage. We're going to go through this process. These five people come into the room, we've got our different materiality, we say yes, we say no, we document the heck out of that conversation. Otherwise, there may be a legal case, and calling you out specifically as the CISO or Deputy CISO. But you better document it and show what process you used and in good faith. Just don't lie, right? That's the other thing. Don't lie on the forms.

Amoroso: I don't think people are lying. I think that things can be screwed up for sure. But I'm not convinced that there's a lot of intentional "I'm not going to tell you." That's my observation.

Rosenquist: Let's go back to the SolarWinds case. And let's take a very specific example. And then I'm going to ask you three questions. If we look at the complaint, and if you go to paragraphs 14 through 17—and again, these are the claims of the SEC; the SEC still has the burden of proof, they still have to prove this—but paragraphs 14 through 17 basically say that SolarWinds and its CISO knew that there were three different customers in May 2020, in October 2020, and in December 2020. All were attacked. And these companies came to them and said, "Hey, we were attacked by your product. Here's the issue." Now in the December one, this was when Kevin Mandia called them up on the phone. And this was FireEye. And I knew their CFO at the time. They had grabbed the code and grabbed the binaries and reverse engineered it. Actually went to Microsoft as well and helped reverse engineer it. And came back with definitive proof: "SolarWinds, this is exactly the problem in your product." And at that point SolarWinds filed an 8-K and said, "As of December, we have an attack." They didn't mention the fact that they knew these attacks were going on with two other customers. One, which was a government agency, dating back six months. And again, this form is to inform the shareholders.

Amoroso: Wouldn't that have the effect of informing the adversary as well?

Rosenquist: No. The requirement is not new.

Amoroso: It doesn't bother you that when you're in the middle of a situation, you're telling the adversary exactly what you know?

Rosenquist: You're not telling them exactly what you know. You're telling them "We've detected you." And by that point—

Amoroso: I'm asking you: Do you worry about the transparency on the defense?

Rosenquist: Actually I don't. Because I think there are sane minds that say, "You don't have to give logs, you don't have to say exactly what you found. You don't have to give binaries. All you have to say is, "Hey, we were attacked in one of our major products six months ago." Because that's all the shareholders need to know. They're not security experts. They do want to know when their investment has been compromised in their primary product. That would be important, just as if their major manufacturing hub went down, and was going to be down for two months. They should probably know that. OK, three questions in this situation.

Amoroso: Am I going to get graded on these?

Rosenquist: You are. If you were a CISO in this case, would you fill out that 8-K form and choose to omit the fact that you knew, and your team knew, that several customers dating back six months had actually been attacked? Would you have omitted that?

Amoroso: I would have never gone anywhere near the 8-K, because there isn't a CISO on the planet that even knows what the hell it is.

Rosenquist: OK.

Amoroso: Let me finish. If I'd gone mucking around with 8-Ks, I'd have been fired in one second. As a CISO. That's what the lawyers do.

Rosenquist: OK, so if the lawyers say we have to file an 8-K—

Amoroso: Then let them figure out what to do. I don't know why you need a CISO here.

Rosenquist: Well, you as the CISO, you are the top dog when it comes to cybersecurity.

Amoroso: In this case, this is not top dog. This is little o officer, not big O officer.

Rosenquist: But you are the top representative in that organization, the top expert for cybersecurity.

Amoroso: Lawyers have to fill out the 8-K, not the CISO.

Rosenquist: OK, but would you allow it?

Amoroso: They outrank you by so much it's not even funny.

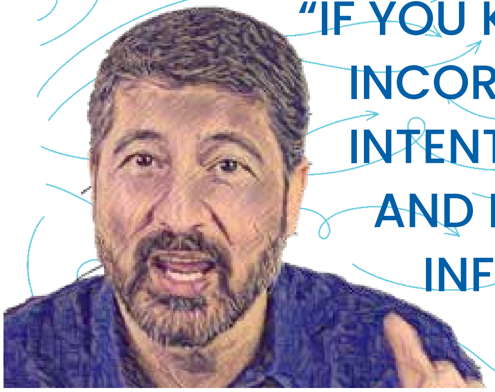
Rosenquist: I don't know about that. I've had plenty of lawyers—

Amoroso: If you want to be pissed at somebody, it's the CEO and the chief counsel that should be held accountable, not the CISO.

Rosenquist: You're bringing the CISO to the big table for a reason.

Amoroso: When did the CISO get to the big table? Here, I'll give you an example. I sat and looked at the Fortune 500. I looked at the fancy pictures, the posed pictures. There's no CISO in there. We're not in the room. That'll never happen. I've been on boards of directors of Fortune 500 companies, I worked for a Fortune 10 company. There's no CISO at that type of table. The CISO's outside the room, brought in for 15 minutes, makes the delivery, gets kicked out, and then the real leadership team decides what to do.

Rosenquist: OK. So then let me turn that around. Let's say you as CISO, your company decides in this case,



“IF YOU KNOW IT’S FACTUALLY INCORRECT, AND INTENTIONALLY MISLEADING, AND IS INSUFFICIENT TO INFORM, THEN YOU HAVE TO STEP UP.”

in the 8-K we’re going to file, we’re not going to mention any of these other pertinent facts. Would you allow that to happen? Or would you take—

Amoroso: Would I then be a whistleblower?

Rosenquist: No. I am not saying whistleblower. Would you take an action as simple as sending an email to the attorney to the CEO and say, “This is not correct. This is not accurate.”

Amoroso: In most companies, that email would get you fired. Now maybe we’ll change that. Maybe that’s a good thing. But most CISOs would never send that. “Who the hell is this guy or gal telling me what to do?” I would have never sent something like that. And I had a lot of stature. Now, if you’re going to change that, then let’s change it. That’s why I call this research.

Rosenquist: I think we do. I think we need to.

Amoroso: Research means change and innovation and coming up with new knowledge, not going back five years, and saying this is how something should have been. If you’re saying the CISO should be at the table and should make the claim, then let’s do it. But there isn’t a damn one of them that’s there. Now if you’re saying would I allow it to happen? The only legal process I have right now if I don’t want it to happen is to go whistleblow, and I’ve been advising my clients to learn the whistleblower laws.

Rosenquist: Yeah, whistleblowing—making sure you’ve got an ethics board, things of that sort.

Amoroso: You can practice it, you can go to the general counsel and say, “Listen, it’s my neck on the line, not yours. Here’s what I’m going to do. If four days pass and I see you haven’t reported this thing, then I’m going to whistleblow. Here’s how I’ll do it. Here’s the preloaded form. Here’s the approach. I’m telling you now, and if you don’t like it, fire me.” Now the minute you go tell the general counsel you’re going to go whistleblow, you’ve destroyed your career. So you’re asking people to go to their leadership and say, “I’m going around you. And I’m going to whistleblow if you do something wrong.” I think it’s premature, because this hasn’t been worked out yet. So you’re putting the CISO in an impossible situation.

Rosenquist: I don’t agree. I’ve been in similar situations, and I won’t get into—

Amoroso: When you were at Intel, you’d have gone around your CEO and lead counsel?

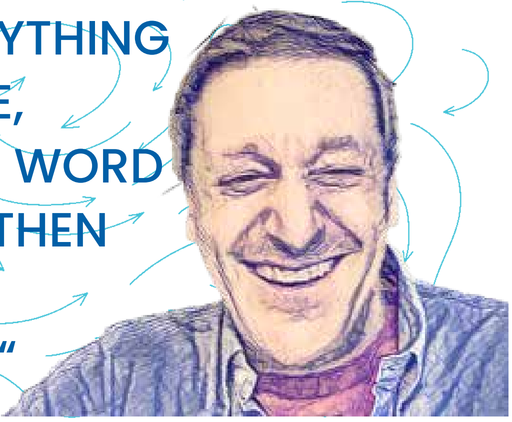
Rosenquist: I’m not going to give particular details, but let’s talk hypothetically. In a situation where the attorneys or even a senior executive wants a certain statement to go out that is factually incorrect having to do with my ownership of cybersecurity, I then communicate to them, in email, and say, “The following information is incorrect.” Or “I am not behind this, I am not assuming this risk. If you want to make these statements fully knowing that I’m telling you that they’re incorrect, that is your choice. But you have to own that.”

Amoroso: You’d tell your boss that?

Rosenquist: I told my boss that. I told my boss's boss that.

Amoroso: But your boss is probably not the CFO. And the boss should be the one who decides, not the CISO. Because most CISOs report to a CIO or CEO.

“IF YOU TAKE EVERYTHING THE SEC HAS DONE, AND JUST PUT THE WORD CEO IN FOR CISO, THEN I HAVE A LOT LESS PROBLEM WITH IT. “



Rosenquist: They have to realize that you are not the scapegoat. They have to own it, even though they're being told. Then it's not the SEC against SolarWinds and the CISO. It's the SEC, SolarWinds and whatever that executive's name is, because there's going to be that email that says, “Hey, the CISO told you that was false, and you decided to file that report anyway? You signed off on it?” That's where it's going to go. It comes back to transparency and accountability.

Amoroso: That's where it should go. I think we're together. But I'm just saying that right now, as we go into 2024, there isn't a damn CISO that has that situation, a comfortable state. It's a mess. And now this SEC is putting the CISO in an impossible situation.

Rosenquist: I think they are putting them in an uncomfortable situation. I will agree. I don't think it's impossible, because I think we can get better and better and better over time.

Amoroso: If I've got three kids in college and I need the money, and I've got to go to the legal counsel and say, “That's wrong. You listen to me. What you said is wrong.” That's an impossible situation.

Rosenquist: It's not. It's ethical, by the way.

Amoroso: Most of the time in my career, as things unfold, they become clearer a month, six months, a year, even two years later, so you're afraid to say that's wrong, because you're not sure. You know how this works.

Rosenquist: Understood. But if you know it's factually incorrect, and intentionally misleading, and is insufficient to inform, then you've got to step up. I mean come on, we should be at the top of the ethical pile in organizations. There should be no question about ethics. If we're saying, “Well, I've got kids in college,” then you shouldn't be a CISO. If you're not willing to step up and make the hard decisions, you don't deserve a seat at the big table.

Amoroso: I've had two CISO roles. One was little o, one was big O. CISO little o means CISO but you're not an officer. You're not able to speak for a corporation. You know what that means: a legal officer. And I've had that. But I also had CISO where you are an officer. They're very different. So that's the first problem: When we refer to a chief information security officer, there's two different states of that. And I don't think people understand that. Then the second thing is if you take everything the SEC has done, and just put the word CEO in for CISO, then I have a lot less problem with it.

Rosenquist: Fair enough.

Amoroso: Wouldn't that make more sense to you? If you're going to go after somebody, what about the freakin' CEO? What am I missing?

Rosenquist: OK, let's take that. But first, whether you're a big O or a little o, ethics still apply.

Amoroso: I agree.

Rosenquist: And if you know there is a lie, and if you know that there is a massive omission that leads to deception, you've got to step up. It doesn't matter whether you're a big O or a little o, you should step up.

Amoroso: What does step up mean?

Rosenquist: Step up means let them know. "Hey, I am informing you that I know that this is materially false."

Amoroso: Corporations don't work by incenting executives to be vocal, jump up and down, and scream. That's not how businesses work. You inform your boss.

Rosenquist: No, no, you should be professional about this. And I have been, and I've gotten results from this. It's not a threat. It's: "I'm informing you what you just said was materially false, and you did so on a federal form. So if I ever get called to court, I'm going to let them know that I informed you on this date and time. You're going to have to answer to that. So I'm here for the company. But I'm duly informing you because maybe you didn't know."

Amoroso: You and I are very much in agreement on the transparency. Those are all reasonable.

Rosenquist: I'd say the CISO, they should be at the big table. But they need to be competent, ethical. We need to make sure that they're empowered as well. Because that makes things go smoothly. If they're not empowered, it's rough waters.

Amoroso: They need to get training.

Rosenquist: We agree on that. How do you think this case will change that? Or do you think this case—

Amoroso: I think it will. Because of what we're doing right now. You and I wouldn't be having this discussion. So I love that. I think that people will talk about it. It gets the discussion going. The CISO does move a little closer to the executive room. The board realizes, "Hey, I better figure out who the hell my CISO is."

Rosenquist: If they're any good.

Amoroso: I'm all for that, If I had to boil my whole thing down to one little nub, it would be this: I think there's a lot of work to be done before we start holding people accountable and calling them liars. For example, I have been involved in the preparation of materials that go out to investors. I've been a board member of a large company. There's last minute changes all the time that a CISO would have no clue are being made. So are you saying the CISO needs to have final readout on anything that goes out? And before it goes out I need to read it in case you see something wrong?

Rosenquist: Honestly, I think if it has anything to do with cybersecurity or claims or issues or impacts or risks, yeah. That's part of their friggin' job.

Amoroso: That process is not in place for any company on the planet. If you're for that, then fine. Let's figure out how to do that. I'm saying there's a whole lot of stuff here that you better go change, fix, and improve before we start going in a courtroom and have an issue. You and I are probably way more in agreement than disagreement.

Rosenquist: Yes, absolutely. It's the nuances though.

Amoroso: The nuances: Should they be aggressive now, or is there still a lot of stuff we better work out before you start going after individuals? I'm more on the latter.

Rosenquist: I'm more on the former.

View the full pocast on The Cybersecurity Vault.

INTERVIEWS

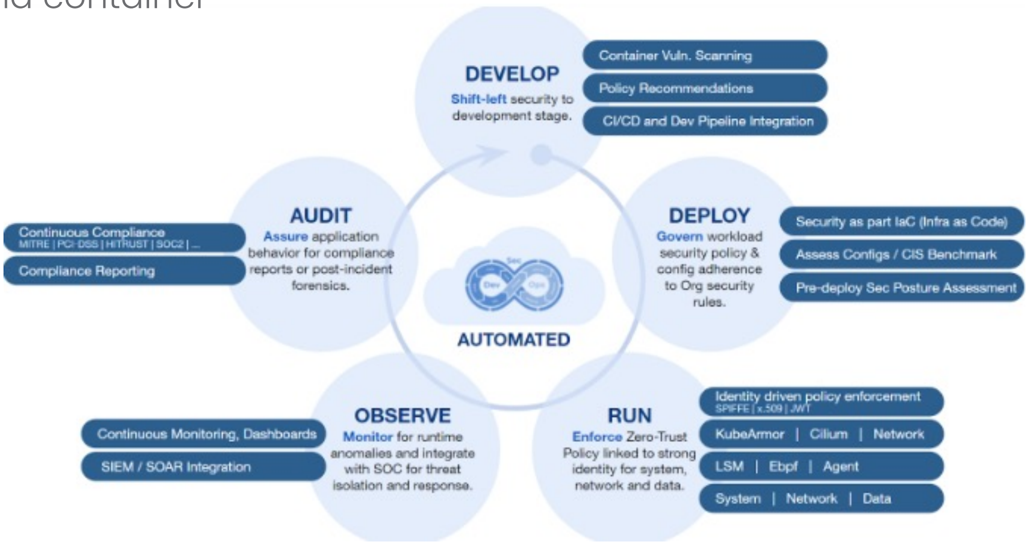
INTERVIEW WITH NAT NATRAJ,
CO-FOUNDER & CEO, ACCUNKNOX

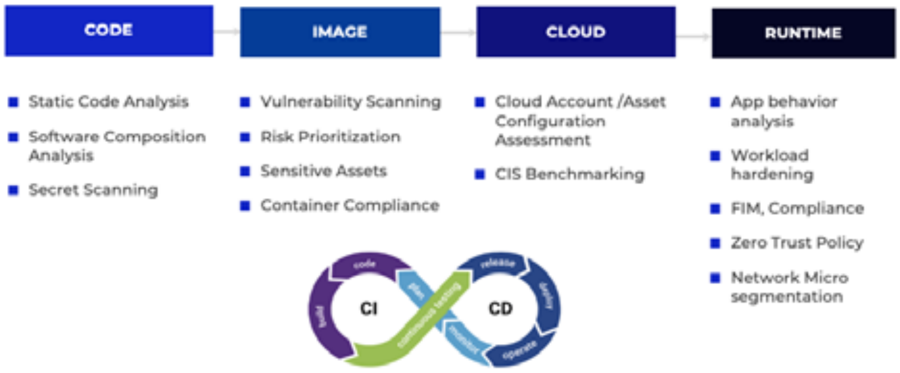
EXPLORING INNOVATIONS IN CLOUD SECURITY STRATEGIES

Accuknox, a leading security vendor in comprehensive multi-cloud and hybrid cloud security, has garnered significant attention in recent years for its innovative solutions. As companies increasingly adopt multi-cloud and hybrid cloud architectures, Accuknox is at the forefront, providing effective cybersecurity measures to safeguard critical assets. The TAG analyst team recently sat down with executives from Accuknox to learn more about the company's DevSecOps model for CI/CD security, its flexible SaaS and On-Premises models, and its commitment to offering detailed telemetry for auditing and container forensics.

TAG: Can you elaborate on Accuknox's approach to DevSecOps and how it aids in ensuring CI/CD security in multi-cloud and hybrid environments?

ACCUKNOX: In the past decade, our industry has witnessed transformative shifts. A notable change is the move towards a "developer-centric" tech model, emphasizing "development at the speed of business" rather than the conventional "development at the speed of IT." Simultaneously, security has been intricately woven into the development process, adopting a proactive "shift left" approach instead of the traditional practice of treating it as an "afterthought." This document provides an overview of our Zero Trust CNAPP (Cloud Native Application Protection Platform) seamlessly integrated into a CI/CD DevSecOps model.


DEVELOP
Shift-left security to development stage.
Container Vuln. Scanning
Policy Recommendations
CI/CD and Dev Pipeline Integration
AUDIT
Assure application behavior for compliance reports or post-incident forensics.
Continuous Compliance
MITRE | PCI-DSS | HITRUST | SOC2 | ...
Compliance Reporting
DEPLOY
Govern workload security policy & config adherence to Org security rules.
Security as part IaC (Infra as Code)
Assess Configs / CIS Benchmark
Pre-deploy Sec Posture Assessment
Sec
Dev
Ops
AUTOMATED
OBSERVE
Monitor for runtime anomalies and integrate with SOC for threat isolation and response.
Continuous Monitoring, Dashboards
SIEM / SOAR Integration
RUN
Enforce Zero-Trust Policy linked to strong identity for system, network and data.
Identity driven policy enforcement
SPIFFE | x.509 | JWT
KubeArmor | Cilium | Network
LSM | Ebpf | Agent
System | Network | Data



CODE

- Static Code Analysis
- Software Composition Analysis
- Secret Scanning

IMAGE

- Vulnerability Scanning
- Risk Prioritization
- Sensitive Assets
- Container Compliance

CLOUD

- Cloud Account /Asset Configuration Assessment
- CIS Benchmarking

RUNTIME

- App behavior analysis
- Workload hardening
- FIM, Compliance
- Zero Trust Policy
- Network Micro segmentation

With flexibility as our hallmark, we offer unparalleled adaptability by seamlessly supporting public, private, airgapped, and hybrid clouds.

TAG: Accuknox offers both SaaS and On-Premises models for its security solutions. Could you discuss the advantages of each model and how they cater to your client's needs?

ACCUKNOX: When the market grew at a heady pace, companies defaulted to adopting a "Cloud First" approach. It offered them time-to-market advantages but came at a steep cost overhead. The market growth tolerated this margin impact. However, in recent times, given the slower growth and increased focus on margins, companies are adopting a more deliberate and rational approach that factors in the security, cost, flexibility, and scalability needs of the business and mapping the right On-Prem, Cloud, and in most cases a blended approach. AccuKnox is uniquely poised to deliver Zero Trust Security to organizations looking for a flexible and blended approach.

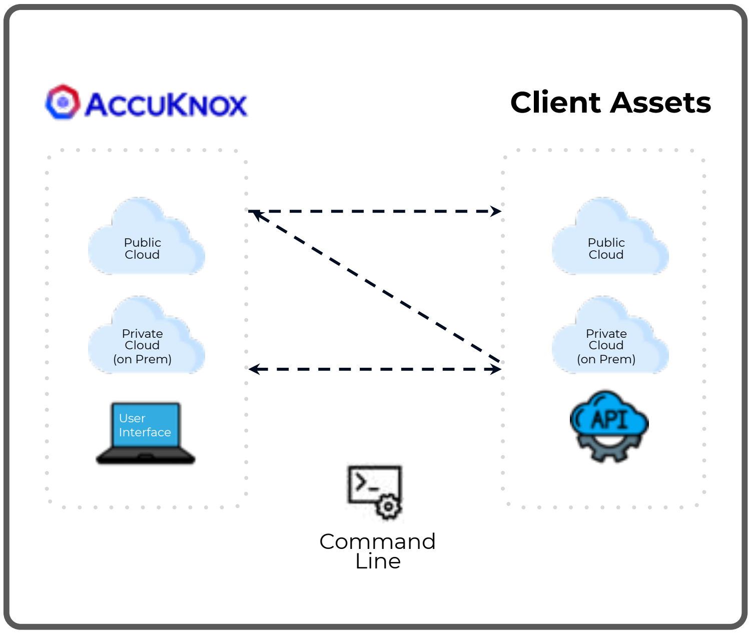
Since most of the advanced attacks in the Cloud are runtime attacks, we provide unique value here through our Inline Security. The distinctive features that set us apart encompass an extensive offering, providing agentless CSPM (Cloud Security Posture Management) and eBPF-powered CWPP (Cloud Workload Protection Platform). We distinguish ourselves through the effectiveness of Inline security, deviating from the common post-attack mitigation approach taken by other vendors.

With flexibility as our hallmark, we offer unparalleled adaptability by seamlessly supporting public, private, airgapped, and hybrid clouds. Our commitment to open-source principles is reflected in our solution's foundation in the KubeArmor project, which has garnered an impressive 600,000+ downloads.

Versatility defines our approach, securing modern (Kubernetes) and traditional (Virtual Machine) workloads.

Our innovative edge is underlined by 10+ patents, demonstrating our prowess across every facet of Zero Trust, from discovering assets and ascertaining security exposure to the automatic formulation and enforcement of Zero Trust policies, ensuring continuous compliance.

Support for Public & Private Cloud



TAG: Accuknox is known for providing detailed telemetry for auditing and container forensics. How does this level of visibility enhance security and compliance in modern cloud-native applications?

ACCUKNOX: Containers, Microservices, and Kubernetes bring unparalleled flexibility, allowing for incremental development, streamlined launches, and cost advantages. However, the transient nature of Kubernetes necessitates leveraging telemetry for compliance assurance, threat hunting, and more.

We provide agentless Cloud Security Posture Management solutions that ensure fundamental security, including comprehensive multi-cloud security, compliance posture discovery, and protection achieved through native APIs. Our commitment extends to application security, ensuring a robust defense from code to runtime, and deploying a lightweight industry-standard (eBPF) sensor agent-based Cloud Workload Protection Platform (CWPP).

We employ advanced techniques such as eBPF-based observability for Container Forensics and auditing, facilitating the auto-discovery of application behavior at a granular, process-level scale. We also adhere to the NSA Kubernetes Hardening Guide in Workload Hardening and Zero Trust Security. Our approach involves leveraging eBPF for observability and utilizing Linux Security Modules (LSMs) to transition from audit-focused observability to active enforcement.

TAG: A crucial feature of Accuknox's offerings is integration with various security tools, such as EDR, SIEM, AppSec, and SOAR. Can you provide some examples of how these integrations benefit organizations?

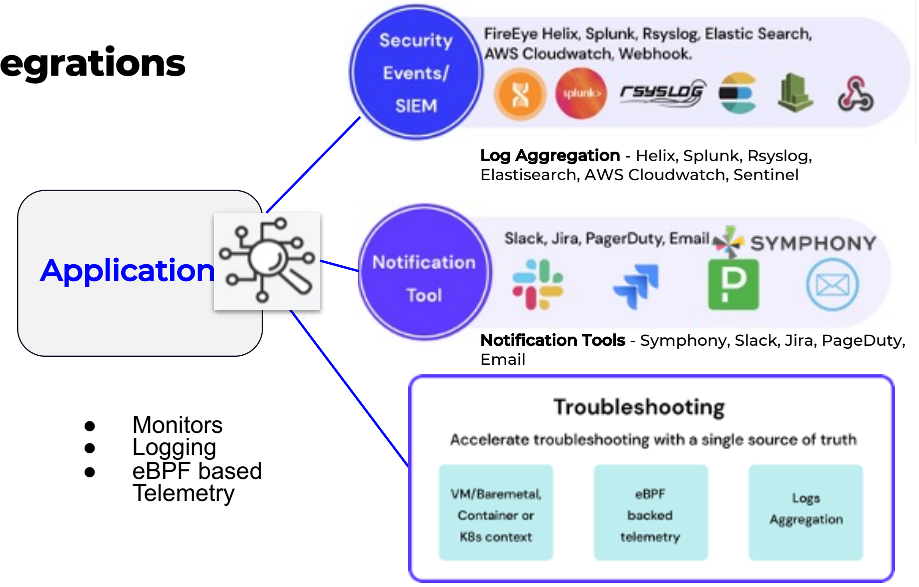
ACCUKNOX: No security solution can remain an "island." It needs to inter-operate and integrate with other investments that an organization has in place (SIEM, Ticketing System, etc.). We provide a complete suite of integrations, as depicted below.

TAG: What innovative strategies or technologies can we expect from Accuknox to address emerging threats and challenges in the multi-cloud and hybrid cloud environments?

ACCUKNOX: In the realm of Cloud Security, we're harnessing the power of Large Language Models (LLMs) to bring about efficiency. The goal is to automate routine tasks, allowing experts to focus on more intricate aspects.

AccuKnox Integrations

- Our lightweight agent and agentless provides us deep telemetry for workload and resources respectively.
- It can seamless integrate with existing security and IT-tool



Application

Security Events/ SIEM

FireEye Helix, Splunk, Rsyslog, Elastic Search, AWS Cloudwatch, Webhook.

Log Aggregation - Helix, Splunk, Rsyslog, Elastisearch, AWS Cloudwatch, Sentinel

Notification Tool

Slack, Jira, PagerDuty, Email

Notification Tools - Symphony, Slack, Jira, PageDuty, Email

Troubleshooting

Accelerate troubleshooting with a single source of truth

VM/Baremetal, Container or K8s context

eBPF backed telemetry

Logs Aggregation

- Monitors
- Logging
- eBPF based Telemetry

This extends to a comprehensive defense strategy for LLMs, protecting against potential threats like Prompt Injection, Data Poisoning, and Denial of Service, emphasizing fortifying the core of our systems.

Moving forward, we ensure the secure accessibility of AI/ML models within Jupyter Notebooks, reinforcing the broader scope of data security. On the frontier of Identity and Entitlement Management, particularly in Cloud and Kubernetes environments, we're actively involved in initiatives such as Data CIEM/KIEM.

API Security takes precedence in our approach, addressing vulnerabilities to maintain the integrity of our systems. Integrating Service Mesh becomes integral, enhancing the overall security infrastructure and operational efficiency.

In tandem with emerging trends, dedicated support for Serverless architectures is a focus, aligning with evolving technological landscapes. Lastly, we're developing solutions for Data Security Posture Management (DSPM) to further fortify our data security measures as a holistic initiative.

INTERVIEW WITH EDUARDO HOLGADO, DIRECTOR OF PRODUCT MANAGEMENT, ALLOT

TRANSFORMING CYBERSECURITY WITH ZERO-TOUCH PROTECTION

In an era where cybersecurity is increasingly essential, Allot Secure stands at the forefront with its cutting-edge solutions for consumers and small to medium-sized businesses. Our exclusive Q&A dives deep into how Allot Secure transforms the user experience, elevates revenues, and fosters unwavering brand loyalty. Discover the innovative zero-touch approach, unique for the mass market, and explore how Allot ensures carrier-grade security in the 5G landscape.

TAG: How does Allot Secure uniquely position itself to enhance user experience, increase revenues, and foster brand loyalty?

ALLOT: Our Allot Secure service is a cutting-edge cybersecurity and content filtering solution that leverages the network, the ISPs' most valuable asset, to provide top-notch protection for consumers and small to medium-sized businesses. The core solution strength lies in delivering zero-touch activation with premium protection and intuitive controls at a price anyone can afford.

This solution enhances the user experience by enabling subscribers to protect their devices easily. It also increases revenues by providing value (while minimizing friction) and fostering brand loyalty by allowing the operator to own the solution and use their corporate look and feel—or even integrate it into an existing customer care app.

TAG: Can you please outline how the zero-effort solution offered by Allot Secure is unique for the mass market and how it helps service providers achieve high adoption rates?

ALLOT: Consumer and SMB mass markets understand that cybersecurity is a critical issue that must be addressed. Most do not know how, and those who rely on traditional endpoint solutions find themselves in a complex and lengthy download and installation process that they often struggle to complete successfully. That is why a zero-touch approach, delivered from the network without requiring installation, is unique and conducive to high adoption rates.

After the customer activates the service, it is crucial to provide valuable features that lead to consistent business retention. This can be achieved by effectively preventing the latest and most sophisticated threats. The ISP can select from various means of communication, such as email, SMS, and push notifications. Additionally, the ISP can integrate the service into its own portal or app or utilize the built-in GUI.

TAG: In a 5G environment, where networks face an expanded attack surface and distributed architecture, how does Allot ensure carrier-grade security for service providers, considering they are both targets and conduits for DDoS attacks?

ALLOT: Allot Smart utilizes scalable inline volumetric anti-DDoS architecture and AI/ML anomaly detection techniques to perform automated and real-time mitigation of large-scale volumetric attacks over the network, both inbound (downlink) and outbound (uplink), with high precision and rapid mitigation (<30sec) while maintaining QoE for critical and sensitive applications.

Allot Smart utilizes scalable inline volumetric anti-DDoS architecture and AI/ML anomaly detection techniques to perform automated and real-time mitigation of large-scale volumetric attacks.

Leveraging its distributed architecture and advanced traffic management capabilities, Allot Smart can meet the needs of 5G networks (both NSA and SA) and enable deployment at the core and network edge to provide the CSP/MNO complete protection from DDoS attacks.

TAG: How does SmartVisibility help optimize network performance, enhance quality of experience (QoE), and contribute to business success and profitability?

ALLOT: SmartVisibility is a software product powered by DPI that runs on an Allot Service gateway and delivers a clear, granular view of the network, application, user, and security data. This granular visibility helps to prioritize and control traffic, secure the network, ensure it meets business requirements, and optimize user experience. Some use cases include Customer usage segmentation, performance and quality issues detection, planning capacity expansion, identifying high-risk churners, and analytics as a Service for the enterprise.

TAG: Could you elaborate on how Digital Experience Monitoring safeguards business efficiency, contributes to customer satisfaction, and aligns technology KPIs with business metrics?

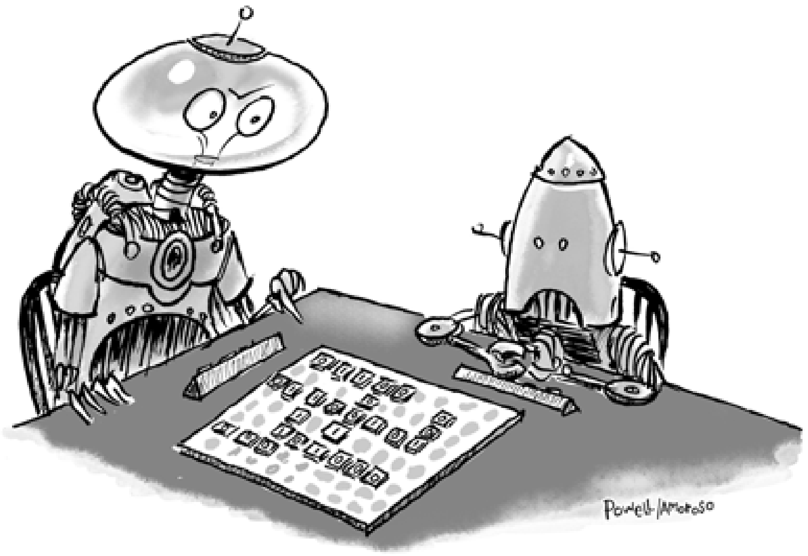
ALLOT: Traffic Intelligence, a comprehensive suite of Digital Experience Monitoring (DEM) solutions, caters to the diverse needs of Corporate Customers:

In terms of Network and service Visibility, Allot NetXplorer emerges as a vital tool, delivering SLA troubleshooting graphs, real-time reports, notifications, and alarms. It aids Network and IT teams engaged in network optimization and maintenance, providing insights such as measuring peak bandwidth for mission-critical apps, branch sites, top-used applications, and identifying bandwidth top consumers.

QoE and Traffic Analytics take center stage with Allot ClearSee, offering a versatile blend of pre-defined and self-service dashboards. These dashboards provide insights into the long-term evolution of App QoE, supporting Network Planning for bandwidth expansions and SLA assurance. Key services SLA is measured based on Quality of Experience, factoring in variables like RTT, packet drops, latency, etc., analyzed per user, application, and branch, with comprehensive C-level reporting.

The realm of Closed-Loop Dynamic Policy leverages Allot's DEM for the automated triggering of Allot's Enforcement Policies. This dynamic approach ensures the delivery of corporate Services and Applications SLAs assurance and WANaaS. Notably, it enables self-service policy creation with configurable network KPI threshold triggers based on criteria such as apps, services, and SaaS application acceleration.

Allot Cloud Traffic Intelligence stands out as a visibility package, facilitating the extraction of SLA insights over Cloud Traffic and Apps. This functionality spans multiple Cloud environments, encompassing Private Cloud, Public Clouds (AWS, Azure, GCP, and Oracle Cloud), and Hybrid Clouds (including Managed Cloud Service Providers - MSPs/MCSPs). This comprehensive package also extends to automated SLA assurance for dedicated VPC/ Applications and optimization of corporate Cloud-Pipes, focusing on maximizing Cloud Pipe utilization.



"Hey, 01100101 is not a word!"

AN INTERVIEW WITH GAURAV BANGA, FOUNDER AND CEO, BALBIX

DECODING CYBER THREATS: A STRATEGIC APPROACH

Balbix has carved a niche in the complex cybersecurity world with its pioneering AI-driven Cyber Risk Management platform. In a recent Q&A, we explored how Balbix leverages advanced analytics and automation to provide a unified view of cyber risk in monetary terms. We also delved into how Balbix addresses critical challenges, ensuring continuous asset discovery, accurate inventory management, and risk mitigation, and learned more about the platform's unique approach to unifying asset inventory, ingesting data from diverse cybersecurity tools, and its role in facilitating faster decision-making for organizations.

TAG: Can you share how Balbix's Security Cloud leverages advanced analytics and automation to provide a unified view of cyber risk in monetary terms?

BALBIX: As an AI-powered Cyber Risk Management platform, Balbix helps organizations measure and reduce their cyber risk to acceptable levels, integrating with hundreds of IT, security, and business tools to understand and quantify cyber risk in monetary terms.

Balbix uses AI and ML to eliminate duplicates and correlate and normalize asset and application data. With Balbix, organizations can get a comprehensive inventory of assets, applications, and software components along with their associated vulnerabilities, misconfigurations, threats, and controls. Additionally, Balbix provides executives and operational teams with actionable recommendations to resolve and mitigate security risks.

Using this data-driven approach, security teams can accurately understand their cyber risk and take steps to mitigate any vulnerabilities, misconfigurations, and lack of controls that might put the organization at risk.

TAG: Asset discovery and inventory accuracy are critical challenges in cybersecurity. How does Balbix address these challenges, ensuring continuous, automatic, and comprehensive IT asset discovery and inventory management?

BALBIX: Our platform integrates with hundreds of IT and security tools to gain a comprehensive understanding of their assets, applications, and software inventory. The Balbix asset model

Balbix implements an asset-level risk model, updated continuously in near real-time, to compute estimates of Breach Likelihood and Breach Impact using data-driven inputs.

incorporates 450+ individual attributes per asset, including system details, hostname, MAC Address, IP address(es), network interface, operating system, patch level, full software inventory with versions and patch history, ports, services, users, associated applications, asset type and subtype, business tags, technology roles, and many more.

Using these signals from dozens of tools, Balbix ensures that assets are accurately identified, categorized, tagged, and reported, which forms the foundation of vulnerability management and risk quantification. Organizations partnering with Balbix see a significant improvement in their asset accuracy, typically by 12x. Additionally, With Balbix, organizations can identify 30-50% more assets than previously visible.

TAG: How does Balbix use its continuous analysis of time-varying signals to provide risk insights, prioritize vulnerabilities, and automate the mitigation process for security teams?

BALBIX: Today, Organizations face a constantly evolving IT environment, with new assets, applications, micro-services, APIs, and cloud services deployed while others are decommissioned or spun down. This dynamic environment poses a significant risk to organizations, with new threats and vulnerabilities emerging daily. Security teams must take steps to mitigate vulnerabilities and deploy security controls to reduce cyber risk.

For large organizations, monitoring cyber risk can be daunting. They may have billions of time-varying signals to consider, making it challenging to prioritize vulnerabilities effectively. Balbix's Risk-Based Vulnerability Management provides real-time insights into vulnerabilities and misconfigurations, analyzing every vulnerability's severity, threats, controls, exposure, and business impact. Additionally, it incorporates signals from the National Vulnerability Database (NVD) and CISA Known Exploited Vulnerabilities (KEV) to understand and prioritize vulnerabilities.

Compared to CVSS, Balbix can reduce critical vulnerabilities by almost 95%, enabling security teams to focus on the vulnerabilities that genuinely impact their risk. Furthermore, automated workflows, such as ticketing, patch recommendations, and patch verification, can enable IT teams to resolve critical vulnerabilities faster.

TAG: Could you elaborate on how Balbix unifies asset inventory by ingesting data from various cybersecurity and IT tools?

BALBIX: Our Cyber Asset Attack Surface Management (CAASM) provides a unified and comprehensive asset inventory, which forms the foundation of Risk-Based Vulnerability Management (RBVM) and Cyber Risk Quantification (CRQ).

Balbix auto-categorizes and deduplicates assets and cleanses/normalizes associated attributes using specialized machine-learning models leveraging data from various enterprise data sources. These sources include CMDB (such as ServiceNow), GRC, IT asset management, endpoint protection, EDR/XDR, IoT/OT, cloud, cloud security posture management (CSPM), vulnerability scanners, control configuration scanners, network equipment and management tools, IP address management (IPAM), software management, mobile device management (MDM),

custom in-house systems and other categories via a wide range of out-of-the-box data connectors.

Balbix provides over 100+ integrations, and we can create new integrations within days. Balbix also integrates with the above tools via API and/or file-based snapshot automation.

TAG: Can you outline how Balbix's unified cyber risk model facilitates faster decision-making, enabling organizations to mitigate vulnerabilities and security issues?

BALBIX: Our platform quantifies cyber risk by computing the risk calculation: "Breach Risk = Breach Likelihood x Breach Impact" for every asset across all assets. Breach Risk represents the expected "per event" monetary loss due to a breach of the assets in scope, Breach Likelihood represents the likelihood of a breach of these assets by a typical adversary applying typical effort, and Breach Impact represents the maximum "per event" monetary loss due to a major breach of these assets.

Balbix implements an asset-level risk model, updated continuously in near real-time, to compute estimates of Breach Likelihood and Breach Impact using data-driven inputs. Breach likelihood is computed across multiple risk vectors based on the nature of discovered vulnerabilities, associated global threat level, vulnerability exposure, and mitigation due to discovered security controls (based on efficacy). Breach Impact is computed based on automatically computed asset criticality ranking, modeled breach loss, and provided user inputs.

Balbix uses AI and ML models to categorize and enumerate assets and infer vulnerabilities, associated threats, level of exposure, deployed controls, and efficacy of those controls vs. detected vulnerabilities, applying confidence thresholds to all of the above. Using these risk calculations, Balbix can prioritize vulnerabilities affecting assets with the most significant business expressed in monetary terms, enabling security teams to get alignment on specific vulnerabilities they need to mitigate and resolve.

INTERVIEW WITH RUSS KENNEDY, CHIEF PRODUCT OFFICER, NASUNI

UNLOCKING HYBRID CLOUD EXCELLENCE IN FILE STORAGE

In the ever-evolving landscape of cybersecurity and hybrid cloud storage, Nasuni has emerged as a key player. Delving into their innovative approach, this Q&A explores how Nasuni addresses the shifting needs of businesses. From their unique security measures to ensuring a seamless transition, Nasuni sheds light on the future of hybrid cloud storage, offering valuable insights for organizations navigating this complex terrain.

TAG: Can you elaborate on how Nasuni's hybrid cloud storage platform stands out and addresses the evolving needs of businesses?

NASUNI: The era of file storage silos has ended. Relying on outdated infrastructures with isolated technologies at various locations no longer satisfies users or supports strategic business goals. Cloud-only solutions pose performance challenges. Nasuni's File Data Platform offers a hybrid cloud storage solution, surpassing traditional options. It breaks free from NAS limitations, enabling scalable storage, significant risk reduction, and lowered operating costs.

Nasuni is the preeminent hybrid cloud storage solution, excelling across three crucial value pillars. Effortless scalability allows on-demand provisioning of SMB and NFS file shares globally, managed seamlessly through Nasuni and object storage subscriptions. The high-speed read/write performance at the edge ensures a smooth transition without disrupting existing workflows. Nasuni offers unmatched data security, providing real-time ransomware protection, up-to-the-minute recovery points, and the ability to recover petabytes of data in seconds, all at the edge. This eliminates the need for backup or disaster recovery considerations for file data.

TAG: How does Nasuni ensure data security, including encryption, role-based access, and protection against hacking or compromise?

NASUNI: We see the worlds of security teams and the CISO coming together with the world of storage and infrastructure. A company's precious data, and more importantly, its file data, is often a target for hackers. Having cyber-storage capabilities built into whatever file data platform you use is a must.

With Nasuni, you get a platform with a robust security model that combines strong AES-256 encryption and local authentication with the native capabilities of top-tier cloud storage solutions such as Amazon Simple Storage Service (Amazon S3), Microsoft Azure Blob object storage, and Google Cloud Storage.

Nasuni offers ransomware detection for file activity, attack mitigation, and recovery support. Nasuni's ransomware solution detects attacks in real time and looks for known signatures and anomalous behavior that signify ransomware activity. These activities are immediately mitigated, and the recovery process can handle millions of files in minutes using a patented rapid recovery process based on dialing back an unlimited number of immutable snapshots.

In addition, Nasuni can help accelerate ecosystem-wide threat response posture via SIEM solutions like Microsoft Sentinel. Your SecOps team gets an early warning from edge detection to launch automated responses, perform investigations, and meet compliance requirements.

With Nasuni, you get a platform with a robust security model that combines strong AES-256 encryption and local authentication with the native capabilities of top-tier cloud storage solutions.

TAG: Traditional backup and recovery solutions often require significant hardware and software. How does Nasuni render traditional backup obsolete and provide faster and more precise ransomware recovery?

NASUNI: Conventional backup solutions require significant hardware and software to run a typical 3-2-1 data protection strategy. Replication strategies introduce substantial risk, and by the time a security breach is detected, the damage has spread across multiple backup copies. Recovery is often lengthy and problematic—extending downtime and impacting productivity.

Nasuni changes all that. You can recover entire volumes in minutes with infinite file versioning and immutable snapshots. Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) are measured in minutes to protect file data without additional backup software. These snapshots are unlimited, incorruptible, can be retained indefinitely, and stored in cloud object storage.

Regarding recovery from a disaster or an attack, Nasuni can recover millions of files in a minute since there is no need to move or restore any data—you simply "dial back" to a point before the attack occurred. Likewise, Nasuni lets you focus on restoring only affected files vs. an entire volume or folder – realizing even greater time efficiencies.

This recovery and detection at the edge is an important line of defense for any security stack with an advantage over traditional storage methods that rely on analyzing and recovering from completed backups.

TAG: Could you elaborate on how Nasuni ensures a seamless transition for businesses, allowing them to realize the scalability, security, and performance benefits without disruption?

NASUNI: A Nasuni migration process is a well-thought-out, thoroughly tested process trusted by hundreds of customers. The data movement from your legacy infrastructure parallels regular file access. The cutover to Nasuni happens quickly and easily—often a simple matter of remapping drive letters to point to Nasuni. Users are frequently unaware that migration has even occurred.

Your corporate data is your most valuable asset. Ensuring there's no opportunity for data loss or exposure is essential. The phrase "data loss" strikes fear in any IT professional, but there is no opportunity for data loss when moving to Nasuni.

Moving your global file-share platform to Nasuni will directly impact your bottom line thanks to the cost savings, unlimited scale, and significant performance gains.

TAG: How does Nasuni's architecture allow for greater AI/ML and data intelligence use?

NASUNI: Unstructured data locked away in storage silos represents a vast and underutilized asset for most companies. While traditionally viewed as a cost and compliance burden, this data can provide immense value when made available to AI systems. However, realizing this benefit requires transforming scattered storage silos stores into an accessible single–source–of–truth.

Companies relying on existing traditional file storage infrastructure, including Windows File Servers, Network Attached Storage (NAS), backups, and more, are not designed to handle the complexities of modern industry, artificial intelligence, or machine learning capabilities. With a hybrid cloud solution like Nasuni, organizations can consolidate, secure, and access their files in one shared global file system and deliver powerful new insights and visibility within the Nasuni File Data Platform. Administrators can quickly assess file data usage patterns, make proactive data management decisions, and better enable the delivery of intelligent insights.

Consolidating scattered and unstructured file data must be the foundation for an AI strategy. By migrating the disconnected contents into a unified file storage lake armed with consistent access permissions, metadata schemas, and governance, it's possible to tap into previously trapped insights, artificial intelligence, and machine learning capabilities to gain traction.

AN INTERVIEW WITH ROB HARRISON, SENIOR VICE PRESIDENT OF PRODUCT MANAGEMENT, SOPHOS

TAILORED SOLUTIONS FOR DIVERSE CYBERSECURITY CHALLENGES

The TAG team recently spoke with the renowned security firm Sophos. During our discussion, Sophos showcased its remarkable expertise in providing managed detection and response (MDR) and integrated cybersecurity solutions. Sophos stands out with its practical approach to securing organizations in the current dynamic landscape of cybersecurity challenges. This summary delves into how Sophos ensures comprehensive cybersecurity defense, shedding light on its practical strategies for proactive threat detection and response, all while upholding the integrity of integrated cybersecurity solutions.

TAG: How does Sophos' integrated cybersecurity platform cater to the unique security challenges of different industries, and what specific industry-focused features or solutions do you offer?

SOPHOS: At Sophos, we sell to organizations of all sizes and verticals. Our top verticals include healthcare, state and local governments, education, financial services, retail, and manufacturing. Customers choose Sophos for our strong protection, continuous innovation, breadth of security offerings, ease of use, and intuitive workflows. The powerful Sophos Central platform manages customers' security operations—or we can manage it for them.

Sophos has purpose-built features in its network security solutions for educational institutions, and policy settings comply with local regulations to ensure student safety online. These features include pre-defined activities like "Not Suitable for Schools," SafeSearch, YouTube restrictions, and keyword filtering without restricting learning.

Sophos' solutions address healthcare security challenges. For example, Sophos MDR provides 24/7 monitoring of healthcare environments to secure sensitive ePHI and comply with regulatory mandates. Sophos ZTNA allows secure access to healthcare data from remote locations. Integrating Sophos Endpoint and Sophos ZTNA helps prevent compromised hosts from accessing networked resources.

Sophos X-Ops can contain and neutralize adversaries that are often too advanced and organized for organizations to combat alone.

Finance and banking organizations face several industry regulations like ISO 27001, GLBA, GDPR, SOX, and PCI DSS. Encrypting financial records, transactions, and sensitive data is crucial to avoid data breaches. Sophos provides full-disk encryption for Windows and macOS to protect devices and data and ensure compliance.

TAG: Can you provide examples of organizations that have simplified their security operations and improved threat protection by adopting Sophos' managed detection and response (MDR) solutions?

SOPHOS: The Sophos MDR solution safeguards more than 20,000 organizations globally. The inaugural Gartner Voice of the Customer Peer Insights Report 2023 recognized it as a Customer Choice for Managed Detection and Response, with a "Willingness to Recommend" score of 97%.

CyberMetrics, a SaaS Provider in Phoenix, Arizona, recognized that their in-house resources were not security experts and chose the Sophos MDR service to protect their organization. With Sophos, CyberMetrics' technical team focused on strategic projects to serve more than 12,000 organizations worldwide.

The Independent Parliamentary Standards Authority (IPSA) is the UK independent body that regulates and administers the business costs, pay, and pensions of elected MPs and their staff. IPSA identified the need for an external cybersecurity solution with instant access to expertise and resources to maximize protection. By investing in Sophos MDR, IPSA has experts working to identify, investigate, and resolve security threats 24/7, 365 days a year.

With 35 branches and an ever-increasing customer base in India, Sangli Urban Bank wanted to focus on securing exponential growth and protecting its systems and data from a constantly expanding attack surface. Sophos MDR strengthened Sangli's security posture with a proactive approach to preventing security incidents.

TAG: How does Sophos keep its threat intelligence up-to-date and ensure its solutions effectively protect against emerging threats, including zero-day attacks?

SOPHOS: Our Sophos X-Ops solution is a cross-operational team that links SophosLabs, Sophos Security Operations, and Sophos AI to help organizations defend against constantly changing and increasingly complex cyberattacks.

Sophos X-Ops leverages each group's predictive, real-time, real-world, and deeply researched threat intelligence to deliver stronger, more innovative protection, detection, and response capabilities. The team provides unparalleled insights into how threats are built, delivered, and operated in real time. With this deep understanding, Sophos's entire customer base benefits from powerful, effective defenses against advanced threats.

Sophos X-Ops combines expertise from different sources to identify emerging threats and prevent attacks. By analyzing incidents and taking appropriate actions, Sophos X-Ops can contain and neutralize adversaries that are often too advanced and organized for organizations to combat alone. With its unique operational efficiency, Sophos X-Ops provides a solution to combat these threats.

TAG: Can you elaborate on the interoperability and integration options Sophos provides to help organizations streamline their security stack and enhance overall security efficacy?

SOPHOS: Organizations can scale security without scaling resources by consolidating protection, detection, and response into a single SaaS solution, Sophos Central.

Sophos Central is a unified management and data platform that manages all Sophos products, delivering real-time information sharing to enhance and streamline organizations' operations. Sophos Central can integrate and ingest the telemetry and detections from Sophos products and a broad, open ecosystem of third-party integrations, including endpoint, firewall, network, email, identity, cloud security, and backup and recovery solutions.

The Sophos Central platform enables organizations to detect, investigate, and respond to multi-stage threats across their entire ecosystem. Sophos XDR and MDR provide visibility and insights into evasive threats by integrating, consolidating, and analyzing telemetry from multiple native Sophos solutions and third-party technologies.

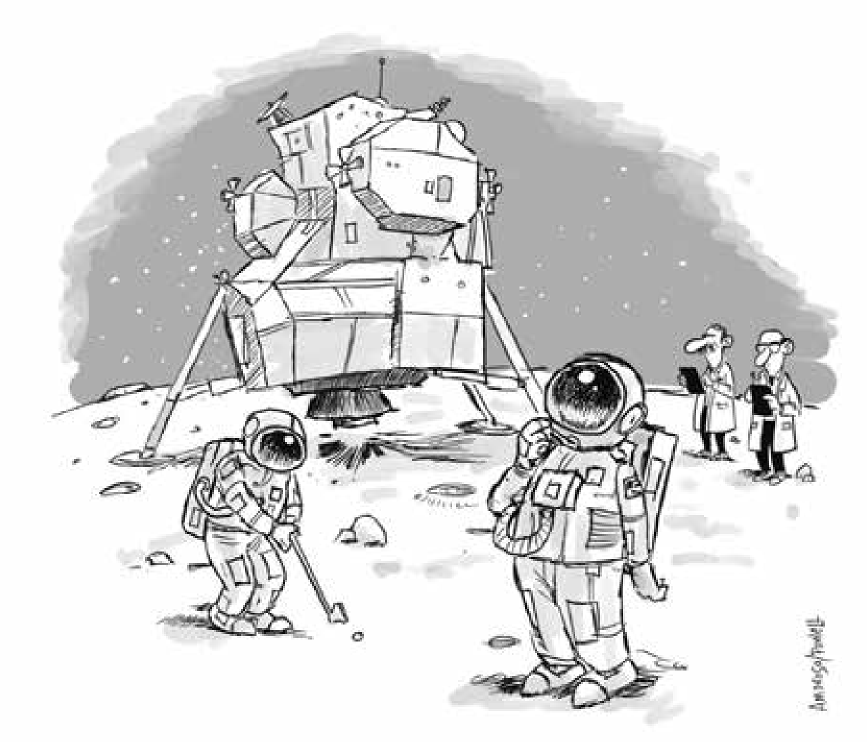
The centralized operations dashboard and management-level reports provide insights into security investigations and cases, actions taken, and security posture status. The result is fewer incidents, a faster response to threats, and less time spent managing IT security.

TAG: What are Sophos's critical focus areas in terms of ongoing product development and innovation, especially for MDR, to address evolving cybersecurity threats?

SOPHOS: We will continue to invest in our protection-first product strategy in the coming years. By intercepting more threats up-front, we allow Sophos MDR analysts—or a customer/partner security team using Sophos XDR—to focus their investigation and response activity where it matters.

In 2023, we launched Adaptive Attack Protection (AAP) to disrupt and contain hands-on-keyboard attacks, providing more time for response team engagement. In early 2024, we plan to enhance AAP by adding adaptive device network isolation and protecting Safe Mode against malicious kernel drivers. Administrators will have greater control of AAP for incident responders.

We're expanding our XDR and MDR third-party vendor integrations to provide defenders with the required visibility. Delivering technology-agnostic solutions can make Sophos XDR and MDR more accessible to all organizations, regardless of their technology choices. We also plan to use Generative AI to address multiple use cases to enhance XDR and MDR capabilities and workflows. These changes will enable analysts to investigate and respond to novel cybersecurity threats quickly. For example, generating detailed case descriptions that automatically map new detection data to the MITRE ATT&CK framework.



The first Deep Fake

INTERVIEW WITH JOHN FRAZZINI, PRESIDENT & CEO, X-ANALYTICS

DECODING THE CYBERSECURITY CONVERSATION FOR BUSINESS LEADERS

Cybersecurity is a journey of continuous technological, process, and cultural changes. Businesses can turbocharge their cybersecurity strategies by engaging their top business leaders in the process. Unfortunately, many business leaders tune out of the cybersecurity conversation because the conversations are largely technical and don't relate to business outcomes. X-Analytics solves this problem by delivering the insights business leaders need to understand business exposures, develop mitigation strategies, and track progress over time. In an exclusive Q&A, X-Analytics delves into how it helps organizations develop the right cyber strategy for their business.

TAG: How does X-Analytics leverage historical cybersecurity data to create customized risk profiles, and how does this contribute to a more effective cybersecurity strategy?

X-ANALYTICS: We provide organizations with insights into potential business and financial exposure from cyber risks and then outline the most effective mitigation strategy to reduce the identified business exposure. These insights are built on three dynamic pillars: entity-specific business dynamics (revenue, digital assets, new markets, M&A activity, etc.), industry-aligned threat and cyber loss data, and entity-specific cyber control implementation.

By incorporating these elements continuously, X-Analytics provides dynamic and evolving insights into an organization's business and financial exposure to cyber risk. With this approach, an organization can develop an effective cybersecurity strategy to reduce the impact of cyber risk on their business and effectively communicate these activities as part of risk governance initiatives.

TAG: Can you elaborate on how X-Analytics helps organizations translate cyber metrics into financial metrics?

X-ANALYTICS: Our approach involves integrating cyber control capabilities, such as deployed technologies, cyber threat context, and an organization's digital profile, to determine the potential impact of cybersecurity events on an organization's business, operations, and finances. X-Analytics can illuminate these exposures across 110 pre-built risk scenarios specific to an organization by leveraging the open-source VERIS taxonomy. As a result, X-Analytics helps our customers gain insights into the risk scenarios most likely to impact them and presents a prioritized view of the mitigation options available to reduce potential future impacts.

TAG: With the SEC's latest rules requiring detailed cybersecurity risk disclosures, how does X-Analytics support businesses in preparing for these disclosures?

X-ANALYTICS: We play a crucial role in supporting an organization's SEC cybersecurity disclosure endeavors across three key areas. Firstly, for governance, X-Analytics summarizes an organization's exposure to cyber risk and delivers board-friendly analysis and reporting to facilitate effective Board governance discussions. Board reporting includes the threats and risk scenarios most likely to introduce business, operational, and financial exposure to cyber risk and details that can identify the most effective mitigation strategies to reduce risk to the organization. This includes setting achievable risk resilience targets, risk appetitive analysis, and post-incident financial exposure details.

Secondly, in Risk Management Strategy, X-Analytics enables the development of an enterprise cyber risk strategy proactively aligned to managing financial exposure to cyber risk effectively. Further, X-Analytics can simulate specific incidents and present the range of potential financial exposures related to a particular cyber security incident to support impact materiality analysis.

Lastly, for Material Cybersecurity Incidents, X-Analytics provides financial loss simulation tables for cyber incidents in support of efforts to determine materiality.

For those incidents deemed material, X-Analytics can be used to estimate cyber incident severity values and provide easy and efficient support for filing efforts.

The National Association of Corporate Directors (NACD) has endorsed X-Analytics as their recommended approach for cyber risk governance and oversight.

TAG: In terms of cybersecurity governance and oversight, how does X-Analytics assist boards in understanding the business context for cyber risk?

X-ANALYTICS: The National Association of Corporate Directors (NACD) has endorsed X-Analytics as their recommended approach for cyber risk governance and oversight. X-Analytics provides directors with a business-aligned context to understand the most effective strategy to reduce business, operational, and financial exposure to cyber risk. This includes the cyber security strategy and mitigation plan most effectively addressing cyber risk in a board-friendly presentation.

TAG: Could you explain how X-Analytics aligns with the latest industry trends and regulatory changes, especially in the Public Company, Private Equity, and Consulting sectors?

X-ANALYTICS: In addition to the SEC requirements listed above, public companies have a general "fatigue" around cybersecurity spending. Executive management and boards are increasingly asking how cybersecurity spending benefits businesses. X-Analytics illuminates how new technology investments can reduce financial exposure to the business – helping prioritize efforts based on business risk-reducing benefits, not just technical outcomes. X-Analytics also aligns how cyber insurance can be optimized as part of the organization's efforts to reduce the potential impact of cybersecurity events by presenting the business context of risk mitigation and transfer; business leaders can apply a business-aligned strategy to manage cyber risk effectively.

The risk of portfolio devaluation resulting from cyber incidents is top of mind for private equity firms. Private equity firms have deployed X-Analytics across hundreds of portfolio companies to facilitate a portfolio-wide cyber governance approach to demonstrate a reduction of cyber risk exposure as part of the firm's value creation activities.

Consulting firms need to differentiate value and avoid the commoditization of services. With X-Analytics, consulting firms have been "leveling up" their offerings with an eye toward deeper strategic client relationships. X-Analytic also provides the foundation for long-term strategic client relationships by elevating the cyber risk conversation from a compliance, maturity, and technical conversation to a business-aligned financial and executive leadership and board-friendly conversation. Consulting teams are developing ROI examples for future project roadmap items. They are elevating legacy cyber control assessments into a business-aligned discussion on mitigation vs. transfer vs. risk acceptance.

X-Analytics is the next-generation version 4.0 approach for cyber risk governance and oversight. As a market, we've come a long way. Version 1.0 stated, "Information security is important," Version 2.0 used "compliance as a hammer" to build urgency, and version 3.0 (where most are today) used maturity scores to benchmark cyber readiness without an understandable business context. Version 4.0 – business-aligned financial insights on cyber risk – is the answer. X-Analytics has solved that need.

ANALYST REPORTS

TAG

ANALYST REPORT

HOW 42CRUNCH ADDRESSES SCALING REQUIREMENTS FOR API SECURITY IN TELECOMMUNICATIONS

DR. EDWARD AMOROSO, CHIEF EXECUTIVE OFFICER, TAG

This TAG report introduces the scaling requirements that exist to support application programming interface (API) security for large telecommunications firms. Commercial cybersecurity company 42Crunch is shown to effectively support these scaling requirements for API security.

INTRODUCTION

Telecommunications firms (telecoms), like all major industries, are now using application programming interfaces (APIs) to drive increased efficiencies through automation of their business processes. Such usage typically involves provision of services such as location data, billing information services, voice and video content, and number porting services to consumers through telecom-hosted APIs, but it also involves consumption by ISPs of API-provided services from other entities such as public cloud providers.[1]

The security aspects of this API landscape for telecoms are greatly complicated by the size, scope, and scale of their businesses. In fact, it is easy (and common) to underestimate the reach of the Tier 1 service providers. In the United States, for example, Verizon and AT&T work with virtually 100% of the Fortune 500 and provide mobile services to hundreds of millions of individual consumer customers. Such coverage can only be described as massive.

What this means is that securing telecom infrastructure comes with a set of functional requirements to support massive scale. Such requirements are reviewed here in the context of API security, both in terms of provision and consumption of APIs by telecoms. To illustrate the practical application of these concepts, cybersecurity vendor 42Crunch is shown to effectively support these scaling requirements for API security in the context of telecom usage.

[1] *This author, while working as the CISO for a large telecommunications firm, first experienced the massive scaling requirements that exist in this industry for the first iPhone launch, soon after which, new mobile app developers desired API-based access to location data from this iconic device, them operating over 2G networks.*

It is also worth reinforcing the obvious and potentially lucrative target that telecommunications firms represent for malicious cyber actors. The reach of telecommunications firms and Internet service providers across so many different industries provides adversaries with the ability to scale their attacks beyond just one target – but rather to a broad assortment of downstream customers of the service provider.

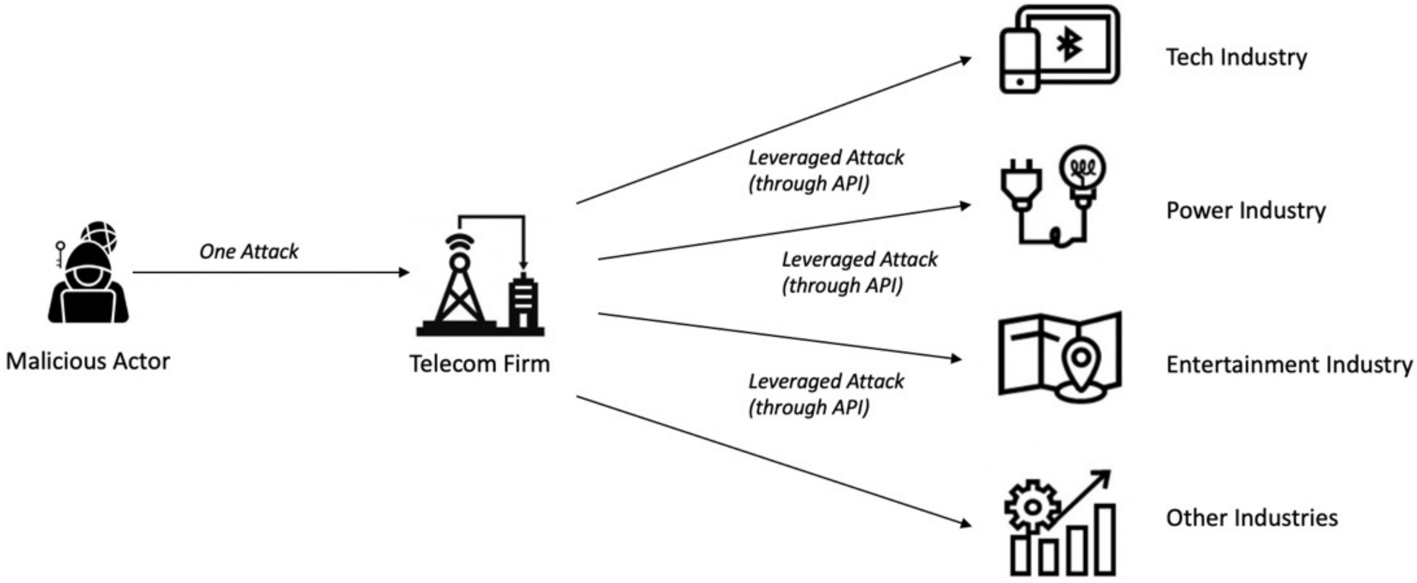


Figure 1. Attack Leverage Gained When Targeting a Telecom Firm

It is also worth mentioning that the global telecommunications industry handles vast amounts of sensitive customer data, making it imperative to adhere to global data protection regulations such as CCPA and GDPR. Additionally, there is an urgent need to comply with industry specific standards such as PCI-DSS for payment and NIST CSF and ISO 27001 for implementation of network security services.

Identifying and mitigating vulnerabilities early ensures that systems are more stable and secure, minimizing the risk of downtime, and ensuring that APIs are robust and secure. Such focus also supports consistent service availability, which is crucial for maintaining customer satisfaction and adherence to Service Level Agreements (SLA) from the outset of the software development cycle.

The leverage that emerges with an attack on a telecom firm is perhaps best achieved through APIs connecting the service provider with its customers. Using such target allows for offensive actors to take advantage of the automation, pre-integration, and convenience of API connectivity between telecoms and their enterprise users. This underscores the importance of implementing proper cybersecurity across telecom infrastructure.[2]

TELECOM SCALING REQUIREMENTS FOR API SECURITY

The primary over-arching requirement to scale API security for telecoms is automation. That is, unlike environments where there might be certain use-cases in which manual processes will suffice to address a given issue, in telecom environments this is never possible. Scale implies large numbers, and any security expert in this industry understands that without automation, workflow, and continuous processing, large gaps can emerge in security coverage.

An additional over-arching requirement that emerges with this industry is complexity. Anyone who spends even a modest amount of time working to secure telecommunications infrastructure and services (as has this author for decades) immediately recognizes the staggering complications that

[2] *In the twelve months preceding publication of this report, there have been several high-profile API-targeted attacks against telcos that have resulted in the exposure of sensitive customer ID. Information on these attacks is available at* ***https://apisecurity.io/issue-203-optus-data-breach-api-security-guide-authn-authz-vulnerabilities/****.*

arise with transport services, control services, maintenance support, application interfaces, data storage, customer support, and on and on.

Let's now focus more specifically on the security requirements for APIs. It should come as no surprise that telecoms utilize APIs to streamline the automated coordination, service implementation, and data sharing with ecosystem components such as vendor services, tiered support, adjacent network infrastructure, customer networks, and standard industry services that support key functions such as naming, routing, and other network capabilities.

In each case, the API – whether provided by a telecom for its ecosystem partners or utilized by the telecom to interact with external services – represents a point of attack by a malicious adversary. This implies the need to perform automated API security testing and to support a program of API threat protection. Three specific functional requirements that arise for such a need in the context of telecom usage are listed below:

1. **Vast API Ecosystem**: As implied above, telecoms will manage a plethora of APIs, each serving different purposes, from user authentication to data transmission. Ensuring the security of this extensive API ecosystem demands the ability to scale.

2 **Constantly Changing Environment:** The telecommunications industry is dynamic, with new services and technologies being introduced regularly, not to mention frequent mergers and acquisitions. API security must adapt to these changes seamlessly.

3. **Global Reach:** Most telecoms serve customers worldwide, which means that their APIs are accessed from diverse locations and devices. Security solutions must be globally scalable and adaptable to regional variations in security requirements.

An important consideration in the context of API security for telecoms is the degree to which their infrastructure has shifted toward a more software-defined approach. Previous generations of telecom infrastructure, especially supporting mobility, required expensive upgrades to equipment as speeds, capacities, and features improved with each successive new generation of service.

With the global advent of 5G, however, telecom infrastructure is highly software-defined, which underscores the relevance of APIs in how interactions occur between telecoms, their customers, their environment (including other telecoms), and the major service providers supporting cloud and software as a service (SaaS). API security thus emerges as a primary component of overall telecom security.

HOW 42CRUNCH SUPPORTS API SECURITY FOR TELECOMS

Commercial cybersecurity vendor 42Crunch provides an innovative API security solution that includes the right set of capabilities to address the unique scaling needs of telecommunications firms referenced above.[3] 42Crunch addresses the API Security challenge by supporting a Shift-Left approach in its platform. Capabilities are delivered to provide a range of tools and solutions that help organizations secure their APIs throughout the entire software development lifecycle, from design and development to deployment and monitoring.

42Crunch achieves its objectives by providing the following comprehensive suite of commercial tools and protection features designed to scale with the industry's tough functional requirements:

1. **API Audit for Design-Time Security Testing:** 42Crunch's API Audit is well-suited to the need of telecommunications firms as they make development investments in their infrastructure. The 42Crunch capability offers instant security scoring for APIs during the design phase. This proactive

[3] *More detailed technical and architectural information on 42Crunch can be obtained from the company's public website at* ***42crunch.com****.*

approach allows teams to identify and prioritize security issues early in the development process, reducing the risk of vulnerabilities making their way into production.

2. **API Scan for Conformance and Vulnerability Detection:** 42Crunch's API Scan is a powerful tool that scans APIs to ensure conformance to best practices. This not only ensures that APIs meet telecommunications industry standards but also helps detect vulnerabilities at both testing time and runtime. With hundreds of cybersecurity checks, 42Crunch provides a comprehensive assessment of API security.

3. **Actionable Reports with Zero False Positives:** 42Crunch's reports are designed to be actionable, which is essential for telecommunications teams. The 42Crunch solution provides clear insights into cybersecurity issues, prioritizing them based on severity. Moreover, the API security solution is engineered to minimize false positives, ensuring that telecommunications teams can focus their efforts on genuine security concerns.

4. **Integration with IDEs and CI/CD Pipelines:** To meet the complex demands of the telecommunications industry, 42Crunch seamlessly integrates with development environments (IDEs) and continuous integration/continuous deployment (CI/CD) pipelines. This means that API security is not an afterthought but an integral part of the development process, which has emerged as a requirement in the context of any software project.

5. **Instant Visibility and Early Detection of OWASP API Security Top 10 Issues:** 42Crunch offers instant visibility for telecommunications teams into their API security status. This allows such teams to proactively address security issues, including those outlined in the OWASP API Security Top 10, which is commonly used by telecommunications teams to protect their infrastructure from common vulnerabilities during the software development process.

6. **Runtime Threat Protection:** 42Crunch also offers an API firewall that can be deployed in production environments to monitor and protect APIs from malicious traffic and attacks. While this is more focused on runtime security, it complements the proactive approach by providing security coverage throughout the API lifecycle.

TELECOM API SECURITY CASE STUDY

A specific telecommunications case study was shared by 42Crunch with the TAG team during the analysis associated with this report. The company involved is a leading US service provider that has responsibility to protect its internal and external API-based services. The service provider uses APIs throughout its infrastructure to enable a variety of internal and external facing services for employees, partners, and customers.

As part of a defence-in-depth strategy, the provider sought out an API security specialist that could complement their DevSecOps approach to creating applications. After initially reviewing their existing WAF and API Gateway providers' solutions, they selected the 42Crunch API security platform as being well-suited and capable of directly addressing their API security testing and threat protection requirements.

The project involved 300 software professionals working on 800 APIs. Both the 42Crunch API Audit and Scan services were adopted to successfully enable the development and application security teams to implement a shift-left approach to coding in security from API design time in both the IDE and CI/CD pipelines. Key outcomes from the project included the following:

- Senior executives recognized the value of adopting a positive security model based on standardized API contracts for their APIs. This led to the adoption on a large scale of a DevSecOps API security program across the entire telecom organization with improved visibility and control for security.

- The automation of Static and Dynamic API security testing was enabled across the SDLC through integration in all CI/CD pipelines at scale.
- Compliance objectives were achieved via adoption of API standards and governance of all API-based services.
- A reduction of security bottlenecks and development timeframes occurred, leading to faster times to market for new API-based services.
- Cost reduction was achieved for application security testing tasks engaged by red and blue teams.

API SECURITY ACTION PLAN FOR TELECOMS

As explained above, automated, commercial API security platforms are essential for telecommunications firms dealing with massive infrastructure requirements. 42Crunch's impressive suite of tools and features, including API Audit and API Scan, offers scalable and highly adaptable support to address the massive size, scope, and scale required by developers working in the telecommunications industry.

We recommend that telecommunications teams take the following steps to ensure that they are leveraging API security capabilities such as those from 42Crunch:

1. **Inventory –** First, developing an accurate inventory of currently deployed API security tools and platforms is a useful step.
2. **Requirements –** A cross referencing of current API security methods against key scaling and functional requirements is advised next.
3. **Platform –** Review of the best platform for implementation of API security, and we recommend inclusion of 42Crunch in such review, will help to ensure a good result.

These three API security planning steps would appear to be well-suited to the needs of modern telecoms in 2024 and beyond, as their services continue to serve as the backbone for emerging hybrid enterprise networks.

ANALYST REPORT

AN INTEGRATED APPROACH WITH CYMULATE MITRE FRAMEWORKS

DAVID NEUMAN, SENIOR SECURITY ANALYST, TAG

This joint technical report from TAG and Cymulate explores the benefits of integrating MITRE frameworks and the Cymulate platform for more effective cyber defense and organizational resilience.

INTRODUCTION

In cyber defense, it is essential to continually adapt and refine strategies to address the ever-evolving threat landscape. With over 38 years on the frontline of cybersecurity, I've observed the transformation from basic network defense to advanced threat hunting. The inception of MITRE ATT&CK and the recently introduced MITRE Engage framework have further expanded the horizon of defense strategies. The ATT&CK framework, with its adversary-centric approach, has offered unparalleled insights into potential threats. However, with the introduction of Engage, focusing on the defender's perspective, a novel dimension has been added to cyber defense. While some critics argue that the additional layer Engage introduces might complicate cyber defense operations, if employed in the proper context, Engage can be a game-changer. The amalgamation of Engage, ATT&CK, and Attack Surface Management (ASM) ensures an enterprise is hardened, resilient, agile, and primed to counter sophisticated threats. There are several beneficial outcomes of a unified approach:

Defining Success in Cyber Defense Operations: Success in cyber defense is no longer just about preventing breaches; it's about how quickly and efficiently we can detect, contain, and mitigate them. With its defender-centric approach, Engage provides a robust framework for achieving these goals, enhancing our success metrics.

Focus on TTP Countermeasure Development: Adversaries are ever-evolving, and so should our countermeasures. By integrating insights from both ATT&CK and Engage, defenders can develop proactive strategies against specific TTPs, making our defense mechanisms more targeted and effective.

Continuous Training for Defenders: With the complex landscape of tactics and techniques outlined in Engage and ATT&CK, defenders are equipped with a vast knowledge base. It is paramount to invest in continuous training, ensuring they are always at the forefront of understanding and countering threats.

Deep Integration of Engage, ATT&CK, and ASM: These frameworks, when isolated, offer valuable insights. But when integrated, they provide a holistic view of the cyber defense domain. ASM focuses on reducing vulnerabilities by identifying potential threat vectors, ATT&CK offers insights into adversary behaviors, and Engage provides strategies for active defense. The confluence of these three ensures a layered, in-depth defense strategy.

This report will explore a comprehensive cyber defense strategy with the following objectives:

- Understanding the characteristics of MITRE Engage and ATT&CK and the integration with ASM.
- Challenges and opportunities of using MITRE's Engage.
- When and how Engage can be used in conjunction with an ASM platform.
- Final considerations on how to best defend your enterprise.

UNDERSTANDING THE CHARACTERISTICS OF ENGAGE, ATT&CK, AND THE INTEGRATION WITH ASM

In the ever-evolving cybersecurity domain, three primary approaches consistently stand out as cornerstones: MITRE ATT&CK, MITRE Engage, and ASM. To harness the unparalleled potential of their synergy, it's crucial to navigate the intricacies of each.

MITRE's ATT&CK framework operates as a groundbreaking shift in cybersecurity. It functions as a near-exhaustive database, precisely cataloging the tactics, techniques, and procedures (TTPs) cyber adversaries employ. At its core, ATT&CK provides a technical roadmap for analysts, illuminating every stage of a cyber-attack from inception to culmination. It equips the industry with a systematic lens to anticipate and comprehend threat behaviors.

Parallel to this adversary-centric model, MITRE Engage emerges. Engage, in its essence, represents the next phase, pivoting from merely understanding threats to actively countering them. While ATT&CK deciphers the "how" of cyber-attacks, Engage addresses the "how to counter." It outfits defense teams with diverse strategies, allowing them to interact with, redirect, and even confront threats in real time. Through Engage, the traditional defense paradigm transforms, incorporating a layer of active defense. [insert sentence with a few examples of what's in in Engage and how it maps to ATT&CK tactics and techniques.

Concurrently, ASM addresses the vast expanse of vulnerabilities in technology and processes inherent in an organization's digital infrastructure. The ASM model focuses on systematically identifying and analyzing these weak spots. ASM perpetually assesses and strengthens these points by operating across an organization's digital assets, from on-premise systems to cloud integrations, ensuring threat actors encounter minimized entry routes.

In their collective application, the capabilities of ATT&CK, Engage, and ASM establish formidable defensive mechanisms. The integration of Engage into the ASM framework means that vulnerabilities aren't merely identified and patched; they transform into strategic engagement points for understanding and countering adversaries. By harnessing ATT&CK's insights, defense teams actively anticipate potential threat vectors. Using Engage, they strategize to challenge or divert these threats, enhancing their defense depth.

The real-time collaboration of ATT&CK, Engage, and ASM delivers a multi-layered approach to cybersecurity. By understanding threats, engaging them head-on, and systematically curtailing vulnerabilities through prioritized mitigation, organizations craft an anticipatory and active cyber defense. This multi-faceted defense approach remains crucial for organizations to maintain a resilient digital stance amidst today's dynamic cyber challenges.

CHALLENGES AND OPPORTUNITIES IN THE REALM OF MITRE ENGAGE

In the sprawling panorama of cyber defense, the MITRE Engage framework emerges as a pioneering beacon, simultaneously introducing novel opportunities and intricate challenges. As we navigate this landscape, it becomes imperative to address the dual nature of Engage, dissecting its complexities while also appreciating the potential it unlocks.

At the outset, Engage's emphasis on active defense and adversary engagement diverges from traditional defense mechanisms, thrusting organizations into the relatively uncharted territory of proactive cyber warfare. This shift brings with it inherent challenges. Engage's strategies, by nature, are more aggressive and interactive, urging defense teams to repel adversaries and engage, redirect, and sometimes even ensnare them. While conceptually appealing, this approach necessitates an intricate understanding of the cyber adversary's mindset, capabilities, and intentions. Without this expertise, there's a potential risk of missteps—be it prematurely revealing one's defense strategies or inadvertently amplifying the attack surface.

Furthermore, the complexity of the Engage framework demands a significant upskilling of the cybersecurity workforce. Implementing its techniques requires personnel who are technically proficient and adept in strategy and tactics. Organizations must invest in continuous training and simulations to ensure their teams can harness Engage's full potential.

However, it's within these challenges that Engage's unparalleled opportunities lie. By championing the cause of active defense, Engage allows organizations to shift from a passive, reactive stance to one of anticipation and initiative. Instead of merely waiting for threats to manifest, defenders proactively seek out adversaries, often gaining critical intelligence. This proactive approach provides invaluable insights into an adversary's TTPs and disrupts their operations, reducing their overall efficacy.

Moreover, the very act of adversary engagement acts as a deterrent. When adversaries realize they're contending with an active defense system, they're more likely to reconsider their attack vectors or abandon their campaigns altogether. This psychological edge, paired with the tangible intelligence gained through engagements, can dramatically enhance an organization's security posture.

While the Engage framework introduces complexities that demand careful navigation and a commitment to workforce development, its potential benefits are profound. By embracing the opportunities Engage presents, organizations can transition from mere defense players to strategic cyber warriors, actively shaping the battlefield and redefining the rules of engagement.

INTEGRATING ENGAGE WITH THE CYMULATE PLATFORM: A TECHNICAL BLUEPRINT FOR ENHANCED DEFENSE OPERATIONS

The confluence of MITRE's Engage framework with Cymulate's platform promises to redefine defense dynamics. As organizations strive to fortify their digital infrastructures, understanding when and how to harness the combined might of Engage and Cymulate becomes critical.

Within cyber defense, Cymulate continually monitors an organization's digital assets, taking the attacker's view to identify weaknesses that could serve as potential entry points for adversaries. Cymulate excels at identifying attack paths and validating attack feasibility. With the integration with Engage and its active defense methodologies, Engage transforms these identified vulnerabilities from mere points of weakness to potential engagement zones—areas where organizations can interact with and gain intelligence on cyber adversaries.

Scenarios Benefiting from the Engage-Cymulate Symbiosis:

- **Threat Hunting in Real-time:** While Cymulate highlights potential weaknesses, Engage can facilitate real-time threat hunting within these areas, actively seeking signs of adversary activity and intent.
- **Deception Operations:** Can create honeypots or decoy systems around the vulnerabilities identified by Cymulate, luring adversaries into controlled environments, thereby protecting genuine assets while gathering intelligence on attacker TTPs.
- **Incident Response Augmentation:** In security breaches, the insights gained from Engage can supplement Cymulate data, offering a more comprehensive understanding of the breach and facilitating quicker, more effective responses.

Seamlessly Integrating Engage within Cymulate: *A Step-by-Step Approach*:

- **Assessment & Alignment:** Start by cross-referencing the output of Cymulate tools against the components of MITRE Engage most important to the organization.
- **Define Interaction Protocols:** Establish clear protocols dictating how interactions with adversaries will be conducted to avoid potential escalations or unwanted disclosures before active engagement. Test those protocols with Cymulate automated red-teaming.
- **Integrate Data Streams:** Ensure a bidirectional data flow between Engage and Cymulate. Vulnerabilities identified by Cymulate should seamlessly feed into Engage for action, while insights from Engage should inform Cymulate's security assessments.
- **Continuous Training:** Given Engage's active nature, regular training sessions should ensure that defense teams can adeptly handle engagements, making the most of the intelligence gleaned.
- **Automate & Optimize:** Utilize automation tools to ensure that the Engage-Cymulate integration operates in real-time, with immediate actions taken based on the insights from both platforms.
- **Regular Review & Iteration:** Review the combined system's efficacy, updating strategies and tactics based on the evolving threat landscape and the intelligence garnered from engagements.

The synthesis of Engage with Cymulate offers organizations a proactive and enriched defense strategy. By identifying vulnerabilities and then actively leveraging them for engagement and intelligence, organizations can not only defend but also dictate the terms of cyber engagements, establishing a posture of dominance in the digital arena.

CRAFTING A COHESIVE DEFENSE STRATEGY: TAILORING ENTERPRISE PROTECTIONS IN TODAY'S DIGITAL LANDSCAPE

As enterprises navigate the multifaceted challenges of today's cyber environment, a holistic defense strategy—grounded in integrating MITRE's Engage framework, the Cymulate platform, and actionable insights—becomes the linchpin for digital security. Drawing from the intricate tapestry of the previous discussions, it is imperative to synthesize a consolidated approach, ensuring a robust defense posture tailored to the unique attributes of enterprises, irrespective of their scale or sector.

Consolidated Strategy:

Intelligent Integration: The heart of a modern defense strategy lies in the intelligent integration of frameworks. Organizations craft a two-pronged defense by melding the proactive adversarial engagement of Engage with the vulnerability management capabilities of ASM. While ASM continuously identifies potential vulnerabilities, Engage transforms these points from passive weaknesses to prescient engagement zones.

Active Defense Evolution: Traditional defense mechanisms predominantly operating in a reactive mode are no longer sufficient. Instead, organizations should emphasize real-time threat hunting, deception operations, and incident response augmentation—all hallmarks of the Engage approach—to actively confront and confound adversaries.

Continuous Adaptation: In the cyber domain, static strategies are recipes for obsolescence. Defense mechanisms must perpetually evolve, informed by real-time data, emerging threat intelligence, and technological advancements.

Actionable Recommendations Tailored for Diverse Enterprises:

For Small to Medium Enterprises (SMEs):

- **Resource Optimization:** Given typically limited resources, SMEs should prioritize integrating scalable, cloud-based ASM solutions, complemented by select Engage techniques that offer maximum impact, such as deception operations.
- **Outsource when Necessary:** Consider leveraging Managed Security Service Providers (MSSPs) specializing in active defense to bridge the expertise gap without incurring substantial in-house costs.
- **Employee Training:** Human error remains a vulnerability even with the best systems. Regular cybersecurity awareness programs can mitigate this risk.

For Large Enterprises:

- **Holistic Integration:** With more extensive digital landscapes, these entities should aim to seamlessly integrate ASM platforms and the Engage framework, ensuring real-time data flows and automated responses.
- **Dedicated Threat Intelligence Teams:** Establish in-house teams focused exclusively on threat intelligence gathering and adversarial engagement, deriving insights from the Engage-ASM synergy.
- **Sector-specific Customizations:** Given their diverse operations, tailor defense strategies to sector-specific threats, be it financial fraud mechanisms for the finance sector or industrial control system attacks for manufacturing.

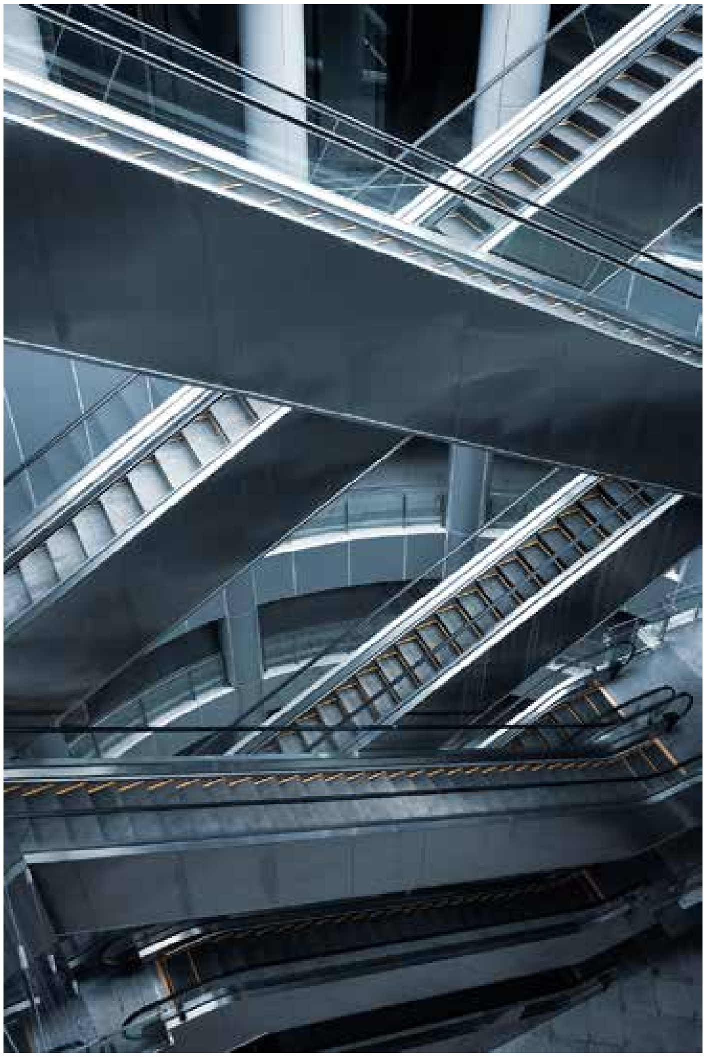
For Critical Infrastructure & High-risk Sectors:

- **Red Teaming & Simulations:** Regularly conduct advanced adversarial simulations with platforms like Cymulate to test and improve the defense posture, ensuring readiness against high-stakes attacks.
- **Deep Engagement:** Deploy advanced Engage techniques, such as active engagement zones and high-interaction honeypots, to gain granular insights into adversary TTPs.
- **Regulatory Compliance:** Ensure alignment with sector-specific regulatory guidelines, often more stringent given the elevated risks.

Enterprises must champion an equally dynamic defense approach as cyber threats grow in complexity and sophistication. By cohesively integrating the forward-leaning strategies of Engage with ASM's foundational strength and tailoring the blend to the unique requirements of different enterprise scales and sectors, organizations fortify their digital fortresses, prepared and proactive in the face of evolving digital threats.

CONCLUSION

In the contemporary digital era, the cyber realm is in perpetual flux, marked by relentless advancements and ever-mutating threats. The union of MITRE ATT&CK, MITRE Engage, and Cymulate signifies more than just a strategic collaboration; it epitomizes the forward-thinking mindset that organizations must adopt. As adversaries continue to innovate, so must we – to stay abreast and preemptively counteract emerging threats. By synchronizing the insights from these frameworks and tailoring their application to an enterprise's unique footprint, we don't just strengthen our cyber defenses; we revolutionize them. In this age of digital ubiquity, merely reacting is no longer sufficient; organizations must evolve, anticipate, and actively engage to safeguard their digital frontiers. The synthesis of these tools isn't just a recommendation – it's an imperative for a secure digital future.



QUESTIONS AND ANSWERS FOR CISOS ON THE NASUNI SOLUTION OFFERING

DR. EDWARD AMOROSO, CHIEF EXECUTIVE OFFICER, TAG

This report offers brief answers to common questions modern chief information security officers (CISOs) ask regarding the Nasuni file data protection solution. The objective is to offer practical guidance on how Nasuni supports both security and compliance requirements..

INTRODUCTION

This report provides guidance for chief information security officers (CISOs) in the form of answers to a series of questions commonly posed with respect to the commercial Nasuni offering. This is important because Nasuni offers file data services that are increasingly being utilized in the context of cybersecurity – and the mitigation of ransomware in particular.

The TAG team of analysts was engaged to support this process to ensure that the explanations are consistent with the practical day-to-day concerns of the modern CISO. All vendors, including Nasuni, will offer their own unique perspective, so the discussions below were generated based on live interactions with working CISOs, rather than based on marketing conjecture.

BRIEF OVERVIEW OF NASUNI

Nasuni employs an approach known as UniFS (Universal File System), which serves as the basis for its services. UniFS combines cloud storage with traditional file systems, delivering a scalable solution that utilizes cloud resources to expand storage capacity, enabling businesses to cost-efficiently manage their data growth.

One of Nasuni's features is its data security framework, which includes data encryption support, both in transit and at rest, thus ensuring that sensitive data avoids unauthorized access. Nasuni's continuous versioning and snapshot capabilities facilitate data protection and recovery, which are key elements in any ransomware prevention or response scheme.

Nasuni's customers come from many different industries and are all sizes and shape. Its services help organizations seeking simplified data management, streamlined collaboration, and obviously, support for security requirements driven by ransomware and related data attacks. Nasuni's value proposition can be summarized as follows:

- **Scalable and Agile Data Management** – Nasuni frees enterprises from the constraints of traditional storage solutions, offering a cloud-native architecture that can accommodate data growth while maintaining optimal performance.
- **Rigorous Data Security** – With encryption, versioning, and snapshot capabilities, Nasuni empowers businesses to protect their data from breaches and mishaps – including ransomware, thus improving security posture.
- **Holistic Approach to File Services** – Nasuni's comprehensive platform covers a wide spectrum of data-related needs, including backup, disaster recovery, global file sharing, and remote work enablement.
- **Fast Edge Performance** – Nasuni enables customers to access data everywhere with no changes to apps or user workflows, zero-latency edge performance, smart data synchronization, and elimination of file data duplication and replication costs.

QUESTIONS AND ANSWERS FOR CISOS ON NASUNI

The questions and answers posed below are offered for CISOs and their team members in the context of general enterprise usage. Any highly specialized usage or tailoring of the platform in a local context might result in slightly different answers. For the most part, however, we would expect that the material shared below will be generally useful and applicable.

As suggested earlier, these questions are commonly posed by CISOs to the Nasuni team, and the issues raised are consistent with what TAG sees from CISOs on a daily basis. It should come as no surprise that CISOs gravitate to Nasuni based on ransomware concerns. What occurs after, however, is that they come to appreciate the more general benefits of the platform.

QUESTION: DOES NASUNI PREVENT RANSOMWARE ATTACKS?

ANSWER:

It should come as no surprise that no storage, backup, and recovery solution can prevent ransomware attacks. To properly avoid such incidents, security teams must engage a comprehensive plan that combines protections across all aspects of the infrastructure with dramatic emphasis on simplification of systems and avoidance of complexity. Engaging in the prevention of ransomware is beyond the scope of this report and certainly beyond the scope of what Nasuni brings to the table. What can be said, however, is that Nasuni is an attractive, perhaps even essential, aspect of any security solution that minimizes the consequences of a ransomware attack on the enterprise. Professional and experienced CISOs fully understand the distinction here, but it is worth reinforcing, especially for any less-informed readers, that prevention of an attack and minimization of the consequences are different, but complementary aspects of a working enterprise security program.

Nasuni offers ransomware detection for file activity, attack mitigation, and recovery support. The company's ransomware solution is focused on detecting attacks in real time at the edge. Its detection looks for both known signatures and anomalous behavior that signify ransomware activity at certain thresholds. These activities are then immediately mitigated by isolating them from the rest of the network. The recovery process can handle millions of files in minutes using a patented rapid recovery process based on dialing back an unlimited number of immutable snapshots. This recovery and detection at the edge is an important line of defense for any security stack that has an advantage over traditional storage methods which rely on analyzing and recovering from completed backups.

QUESTION: HOW DOES NASUNI HANDLE DATA ENCRYPTION AND ESCROW?

ANSWER:

CISOs are wise to recognize first that storage, backup, and recovery vendors such as Nasuni will properly leave the data encryption decisions to the data owners. This is no deficiency but is rather an important and desirable design goal. Accordingly, Nasuni offers two options for customers regarding the encryption of their data. First, the encryption scheme can be employed without escrow support from Nasuni, which would leave all obligations for key management and encryption to the customer. Law enforcement requests, for example, to Nasuni for access to data would not be possible for fulfillment, based solely on the non-escrow of keys with Nasuni, which implies non-access. Nasuni does, however, offer a second option for customers who choose to partner with the company on escrow-related operations. In this operational case, Nasuni would provide escrow support, which would oblige Nasuni to provide on-demand support for law enforcement seeking access, should such occasion arise. Obviously, the robustness benefits of outsourced escrow would apply as well, especially during times of great stress, where external assistance truly helps.

QUESTION: HOW DOES NASUNI DEAL WITH INSIDER THREATS FOR ITS OWN ADMINISTRATORS?

ANSWER:

Like all modern companies, including vendors, Nasuni understand the challenges of having insiders who might be disgruntled or compromised. This is a fact of modern business, and it exists in every company, regardless of size or scope. To that end, Nasuni has taken steps to adhere to proper security compliance requirements including the salient aspects of ISO 27001 and SOC 2 assessment. Nasuni also employs a suite of modern security functionality and tools designed to protect against inappropriate data leaks or improper administrative activity. All administrative activity is logged and managed, and the company employs commercial identity and access management solutions using Okta in its infrastructure. CISOs should thus view Nasuni as providing reasonable, state-of-the-art security across its operation, with the observation that security schemes can always be improved.

QUESTION: WHAT SECURITY RISKS EMERGE WITH A SINGLE CONSOLE ACCESS TO STORED DATA IN THE NASUNI CLOUD SERVICE?

ANSWER:

This is a common question from CISOs who might be dependent on the decentralized nature of their unstructured data to provide security-through-obscurity protection of this important base of information. (By the way, this is an ill-advised approach to protecting data scattered across an enterprise.) While Nasuni does offer a means for gaining more centralized reporting and management of this data, the platform addresses this single-point-of-risk by providing support for multiple volumes with access controls that can be deployed to reduce the risk of a single console for all stored unstructured data. This approach can help security teams avoid the reliance on security through obscurity toward a more controlled deployment that supports review, monitoring, and compliance.

QUESTION: IF A DATA LEAK IS EXPERIENCED FOR MY COMPANY, HOW CAN I BE CERTAIN THAT NASUNI WAS NOT INVOLVED IN THE DISCLOSURE?

ANSWER:

Such assurance of non-involvement could never be provided with 100% certainty, so every situation would have to be reviewed to determine root cause. TAG has confirmed, however, that Nasuni offers direct support for customers who are experiencing a security incident and would provide best effort assistance in situations where Nasuni might be helpful. This support would be initiated via the normal ticketing process. Nasuni does have its own incident response plan in case of local situations requiring attention. CISOs are reminded, however, that most breaches targeting their data will tend to occur at the application layer and through interfaces that operate above and beyond the underlying infrastructure. Assuming that the underlying infrastructure could be involved is a reasonable aspect of any analysis during or after a breach, but experience dictates that most attacks operate at the application and data layers.

QUESTION: WHAT SUPPORT DOES NASUNI OFFER CISOs WHO HAVE COMPLIANCE AND QUESTIONNAIRE REQUIREMENTS AROUND DATA STORAGE SECURITY?

ANSWER:

Nasuni offers pre-completed compliance answers to typical questionnaires made available through trustcenter.nasuni.com. This includes support through OneTrust and CyberGRX, and information can be obtained from Nasuni on demand. This is an increasingly common question, by the way, despite the straightforward nature of the inquiry. Sadly, many CISOs are spending a greater portion of their time dealing with compliance inquiries and offering detailed answers to long questionnaires on commercial governance, risk, and compliance (GRC) platforms. Nasuni cannot help customer avoid this trend, but they do have useful resources to help with the answering and response process.

QUESTION: WHAT ARE THE GEOGRAPHIC FOOTPRINTS FOR PHYSICAL STORAGE OF DATA IN THE NASUNI CLOUD?

ANSWER:

Nasuni is back ended by Amazon Web Services, Microsoft Azure, and Google Cloud Platform. The customer works their own hosting deal with the major service provider to ensure compliance with any physical facility requirements, and Nasuni offers its solution consistent with design and deployment decisions made by the customer. Nasuni should not introduce any geographic problems for customers who are required by law to host in a particular country. Nasuni services work independently of this arrangement.

QUESTION: HAS NASUNI EVER HAD ANY PUBLICLY REPORTED CYBERSECURITY INCIDENTS OR BREACHES?

ANSWER:

To date, the TAG analysts have been unable to identify any publicly reported breaches for Nasuni. As any expert knows, this provides a level of confidence that extends only to known and reported breaches, but it is nevertheless a good result. Discussions with Nasuni confirm that no major breaches have had to be reported publicly. This is not to say, however, that no cyber vulnerabilities, minor incidents, and other security situation have every occurred, for this would be inconsistent with any company operating non-trivial infrastructure. From what TAG can see, however, the track record to date has been good.

QUESTION: WHAT IS THE NASUNI CYBERSECURITY ARCHITECTURE FOR ITS INFRASTRUCTURE PROTECTION?

ANSWER:

This is question best answered by customer through perusal of two excellent reports provided by Nasuni on its data security solutions. The first white paper covers the Nasuni Access Anywhere Security Model and offers an overview of the Nasuni Access Anywhere solution. The second white paper covers the Nasuni File Data Platform which is designed to leverage cloud object storage. Both documents are updated frequently by Nasuni and provide technical and operational insights into the security design decisions embedded in the platform.

ADDRESSING API SECURITY REQUIREMENTS IN THE CONTEXT OF AUTHORIZATION AND POLICY-BASED ACCESS CONTROLS

DR. EDWARD AMOROSO, CHIEF EXECUTIVE OFFICER, TAG

This TAG report provides an overview of API security requirements in the context of enterprise authorization and policy-based access controls (PBAC). Commercial vendor PlainID is shown to effectively implement authorization and PBAC for API security.

INTRODUCTION

Early generation computing involved mostly human beings interacting with digital systems – and the *human-machine interface (HMI)* that emerged was the subject of consideration time and attention for early security experts. Even today, security issues emerge as humans are exposed to phishing attacks on their computer screens, and research continues around how best to reduce this nagging risk.

More modern computing now relies increasingly on software interacting with its environment through so-called *application programming interfaces (APIs)*, which is how software systems such as applications and workloads communicate and share data. As one might expect, the corresponding security issues for APIs can be challenging, and enterprise teams are wise to seek capable commercial vendor partners to address the risk.

In this note, we explain how API security demands complementary focus on two additional aspects of modern cybersecurity – namely, *authorization* and *policy-based access control (PBAC)*. Both of these security controls are essential for good enterprise protection, but neither has been traditionally viewed as elements of the API security suite. We explain here why this has since changed and what this means for security teams.

AUTHORIZATION AND PBAC

It’s helpful first to explain what we mean by authorization and PBAC, since both concepts have tended to be under-attended by security teams. Authorization involves ensuring that the right individuals or systems have access to specific resources and functionalities while denying access to unauthorized entities. For APIs, this process is made more difficult by the diversity of users and the granular control required for API access.

The complementary method known as Policy-Based Access Controls (PBAC) has evolved as a practical approach to addressing the complexities of authorization and access control. PBAC leverages well-defined policies to determine access rights, thus providing a structured framework for API authorization. Experience has shown, however, that implementing PBAC within an API ecosystem can be non-trivial.

To illustrate, consider that a fundamental aspect of API security involves distinguishing between authentication and authorization. Authentication, as practitioners know, involves validation of a reported identity from some user or system. Authorization, on the other hand, defines what actions the authenticated entity is allowed to perform. Addressing the interplay between these two facets of cybersecurity is where authorization and PBAC can be useful.

ENTERPRISE API SECURITY REQUIREMENTS

For most developers, the connection between API security and authentication involves the use of so-called *API keys* – and developers will be the first to share their frustration regarding the challenge of managing API keys, especially for large development projects. The most common problems involve administering key rotation, key revocation, and ensuring that keys are not inadvertently exposed. None of these tasks lend well to manual effort.

Where authorization challenges emerge is when users and systems require access to APIs. This is done in the context of authorization policies that rely on API keys and other controls to implement proper access rights. Enterprises deal with vast numbers of users and systems that require API access. Ensuring that authorization policies scale efficiently while maintaining performance is a formidable challenge.

Slow or inefficient authorization processes can hinder operational agility. Furthermore, effective API security demands granular control over access rights. Enterprises may need to define policies governing different aspects of API access. This complexity can lead to challenges in policy management and enforcement. Real-time decision-making regarding API access is thus essential.

Traditional access control mechanisms struggle to keep pace with the dynamic nature of API interactions. Real-time policy evaluation and enforcement are prerequisites for effective API security. In addition, comprehensive logging and auditing are crucial for API security. Enterprises require detailed records of API interactions for security and compliance, and this necessitates logging mechanisms to capture relevant data without impacting performance.

ZERO TRUST, CONTEXT, AND INTEGRATIONS

The concept of Zero Trust, invented at Forrester several years ago, advocates for the continual verification of entities and devices attempting to access resources. The model gained prominence across the enterprise security community as perimeters became less effective at protecting hybrid networks. Implementing Zero Trust principles within the context of API security requires the integration of authentication and authorization controls.

To enact granular authorization and PBAC, enterprises must be aware of not only the identity of the entity seeking access but also the context in which the access request is being made. This includes factors such as the user's role, location, time of access, and the device being used. Integrating these various contextual elements into the authorization process is a non-trivial task for enterprise teams, especially if APIs are involved.

Enterprises must also contend with an ever-evolving external threat landscape. Malicious actors continually probe for vulnerabilities within APIs to gain unauthorized access. This necessitates continuous monitoring, threat detection, and proactive measures to safeguard APIs from external threats. An entire industry has emerged specifically to address API security weaknesses in the context of hybrid cloud deployment.

Finally, enterprises rely on third-party APIs to extend the functionality of their applications. Integrating external APIs introduces a layer of complexity in ensuring that third-party access aligns with internal authorization policies. This is a key consideration in practice, as most CISOs would view the risk associated with third parties as being perhaps the most challenging aspect of their overall cyber risk management program.

API REQUIREMENTS FOR SECURITY

As TAG analysts, we believe that API security in the context of effective authorization security and PBAC involves a tough balancing act. On the one hand, enterprises must enforce strict controls to mitigate the risk of unauthorized access and data breaches. On the other hand, however, overly restrictive access controls can impede productivity and hinder the seamless flow of data and functionality within the organization.

Accordingly, we recommend that modern enterprise security teams grappling with API security in the context of their authorization and PBAC implementation requirements focus their planning, design, and deployment attention in the following areas:

1. *Comprehensive Policy Framework*: Enterprise teams should first develop a well-defined and comprehensive policy framework that encompasses all facets of API access. This should link to the organizational mission and should consider the threats targeting the resources offered behind the API layer.
2. *Contextual Awareness*: Identity and context awareness are essential focus areas to enable granular control over API access. A problem with modern access controls is that the level of granularity for rights and permissions is usually insufficient – and with the added need to support authorization, including delegation, focusing on granularity and context is required.
3. *Automation*: Enterprise teams must leverage automation for real-time decision making and policy enforcement. This is best done in partnership with a great commercial vendor and TAG obviously recommends that PlainID be included in any source selection for partners in this area.
4. *Logging and Monitoring*: Implementation of robust logging and monitoring mechanisms to capture and analyze API interactions is a key consideration. This is a familiar enterprise security requirement, so transposing this to an API context should not raise any implementation concerns.
5. *Threat Detection*: Security teams must deploy proactive threat detection mechanisms to identify and mitigate potential security breaches. This corresponds to shift-left focus, so any focus on advance indications and warning will provide effective cyber risk management during development.

6. *Third-Party Risk Management*: Exercising due diligence when integrating third-party APIs will help to ensure that external access aligns with internal security policies. This is increasingly identified by API security experts as a requirement since third parties introduce uncertainty in terms of the robustness of their API implementations.
7. *Zero Trust Integration*: Seamlessly integrating Zero Trust principles into the API security frameworks will help ensure continuous verification and authorization. With the reduction of perimeter dependency for most organizations, it is essential that Zero Trust guide design decisions across the board, including for APIs.

HOW PLAINID ADDRESSES AUTHORIZATION AND PBAC FOR API SECURITY

Cybersecurity vendor PlainID supports authorization and PBAC requirements through a commercial offering that modernizes access management and supports dynamic authorization in real time. The PlainID solution is powered by PBAC, which allows enterprises to create, manage, and enforce fine-grained authorization policies for all trusted identities, workforces, customers, and external third parties.[1]

A key component of PlainID's architecture is its Policy Manager, which supports centralized enforcement management in a decentralized enforcement architecture. This provides a focused view to control who has access to what across the enterprise. This function also provides improved visibility of access risks through advanced access control analytics. The result is a means for deploying predictive and prescriptive access control.

The platform also includes so-called pre-built third-party authorizers, which provide access control for authorization enforcement patterns. This is relevant for use in the context of micro-segmented services, Big Data analytic services, API gateways, and other applications. Integrations are included to control authorizations with Istio, Apigee, AWS API Gateway, Okta, Google BigQuery, and Snowflake Authorizer.

The PlainID platform is well-suited to the concept of centralized management of authorization with PBAC based distributed enforcement. Key functions supported in such capability include policy creation, policy investigation, delegated authorization, approval workflows, and audit & governance. All of these tasks support data and data lakes, cloud infrastructure, applications, and identity-related services.

CONCLUDING REMARKS

API security, in the context of effective authorization and PBAC, is characterized by nuanced challenges that demand solid practical solutions. Enterprises must strike a balance between stringent cybersecurity controls and maintaining operational efficiency.

By adopting a holistic approach that encompasses policy development, contextual awareness, automation, logging, threat detection, third-party risk management, and Zero Trust integration, organizations can manage their API security and protect against evolving threats.

As shown in this report, PlainID is an excellent commercial vendor option to support these key requirements for authorization and PBAC. Enterprise buyers working on rationalization or selection of authorization and PBAC vendors are welcomed to be in touch with the TAG analyst team for assistance.

[1] More detailed information on PlainID is available from the company's website where excellent eBooks and reports can be downloaded – see https://www.plainid.com/.

DISTINGUISHED VENDORS

TAG

DISTINGUISHED VENDORS

Q1 2024

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

ACCUKNOX

Accuknox innovates in comprehensive multi-cloud and hybrid cloud security solutions. With a decade of industry influence, Accuknox excels in delivering Zero Trust Security through its Cloud Native Application Protection Platform (CNAPP). Their commitment to flexibility, openness, and integration ensures robust cybersecurity for organizations navigating dynamic cloud environments.

allot

Allot Ltd. (NASDAQ: ALLT, TASE: ALLT) is a provider of leading innovative network intelligence and converged security solutions. Allot's multi-service platforms are deployed by over 500 mobile, fixed, and cloud service providers and over 1000 enterprises worldwide. Our industry-leading Security-as-a-Service solution is already used by many millions of subscribers globally.

Balbix®

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.

CLOUD RANGE

Cloud Range, the leading cyber range-as-a-service, measurably decreases exposure to cyber risk and overcomes the staggering skills gap by preparing security teams to defend against complex attacks through a customized, full-service, simulation-based cyber attack training program, including live-fire team simulations, IT/OT/IoT environments, skill development labs, assessments, reporting, and more.

TAG CYBER DISTINGUISHED VENDORS

2024

NASUNI

Nasuni is a leader in hybrid cloud storage, revolutionizing file data solutions. Their File Data Platform offers unmatched scalability, edge performance, and data security, eliminating traditional NAS limitations. With innovative features like ransomware protection and seamless transitions, Nasuni empowers businesses to scale efficiently, reduce risks, and optimize operational costs.

Panorays

Panorays is a rapidly growing third-party security risk management software provider offered as a SaaS-based platform. The company serves enterprise and mid-market customers primarily in North America, the UK, and the EU. Top-tier banking, insurance, financial services, and healthcare organizations have embraced the platform.

REDSEAL

RedSeal delivers actionable insights to close defensive gaps across the entire network, on-premises, and in the cloud. Hundreds of Fortune 1000 companies and over 75 government agencies, including five branches of the U.S. military, depend on RedSeal for exceptionally secure environments. Visit www.redseal.net to learn more.

SafeBreach

SafeBreach is a cybersecurity company headquartered in Sunnyvale, California. Founded in 2014, it offers a comprehensive platform for simulating and optimizing security postures. SafeBreach enables organizations to proactively identify and mitigate security risks, providing valuable insights to enhance their overall cybersecurity resilience. Their innovative approach helps safeguard businesses from emerging threats.

SOPHOS

Sophos is a worldwide leader and innovator of advanced cybersecurity solutions, including Managed Detection and Response (MDR) and incident response services and a broad portfolio of endpoint, network, email, and cloud security technologies that help organizations defeat cyberattacks. As one of the largest pure-play cybersecurity providers, Sophos defends more than 500,000 organizations and more than 100 million users globally from active adversaries, ransomware, phishing, malware, and more.

valicyber

Established in 2020, Vali Cyber, Inc. is dedicated to addressing Linux security needs. We've developed ZeroLock™, a security platform based on DARPA-funded MIT and CMU research. It offers comprehensive lockdown and superior threat detection, all with minimal resource consumption compared to legacy Linux security tools.

TAG CYBER DISTINGUISHED VENDORS

2024

VECTRA

Vectra AI is the leader in hybrid attack detection, investigation, and response. The Vectra AIPlatform delivers integrated signals across the entire hybrid cloud attack surface in a single solution. Organizations worldwide rely on the Vectra AI Platform and MDR services to power their XDR strategy.

X-ANALYTICS

Secure Systems Innovation Corporation (SSIC), the innovators behind X-Analytics, are on a mission to help organizations make the best cyber risk decisions for their business. X-Analytics helps organizations drive continuous improvement through effective C-suite and board-level engagement. For more information, please visit www.x-analytics.com.

TAG

© 2024