



# Fall 2024 Advisory Council Meeting

19 November 2024 | The Yale Club of New York City

 Forgepoint



# 1:00 Welcome and Kickoff



**Alberto Yépez**  
Co-Founder and Managing Director  
**Forgepoint Capital**



**Tanya Loh**  
Chief Marketing Officer  
**Forgepoint Capital**

---

HOSTS



# Housekeeping

- Chatham House Rules (no media; photographer present)
- To make calls, visit 2F phone booths or 2M Grill Room
- See program for Wi-Fi access and QR codes:



## AGENDA

<https://forgepointcap.com/site/acmd24/>



## FEEDBACK

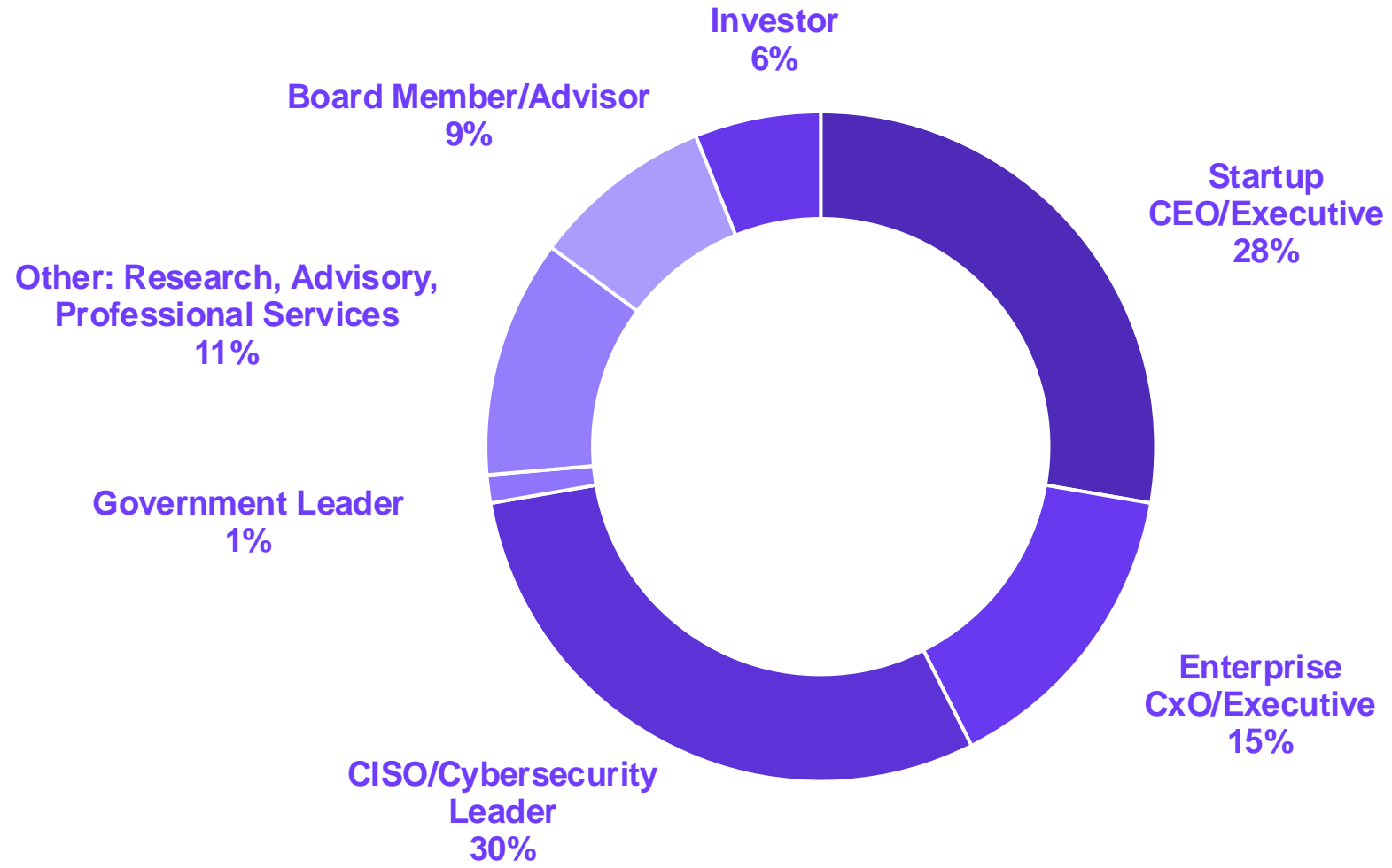
<https://forgepoint.typeform.com/acmd24>

## Wi-Fi

The Yale Club NYC  
notshirtsnotanks

# Audience Mix

Let Us Begin





# Agenda

- 1:00 PM Welcome and Meeting Kickoff
- 1:10 PM Cybersecurity Market Update: Fall 2024
- 1:40 PM Cybersecurity Issues and Observations for 2025
- 2:10 PM Guardians of the G-AI-laxy: AI & Data Governance Concerns and Opportunities
- 2:50 PM Nudge Security: Securing the Workforce Edge
- 2:53 PM [15 Min Networking Break](#)
- 3:08 PM The Great Debate: Reevaluating Public vs. Private in the Cloud Era
- 3:38 PM AKA Identity: Identity Analytics and Automation
- 3:40 PM Anatomy of a Ransomware Incident
- 4:05 PM Fireside: The CISO Playbook
- 4:30 PM Hyperproof: Next Level Risk and Compliance Management
- 4:33 PM Fireside: An Innovator's Journey, from CTO to CEO
- 4:58 PM [Meeting Close > 5:00 Rooftop Reception > 6:30 Celebration Dinner \(back here!\)](#)



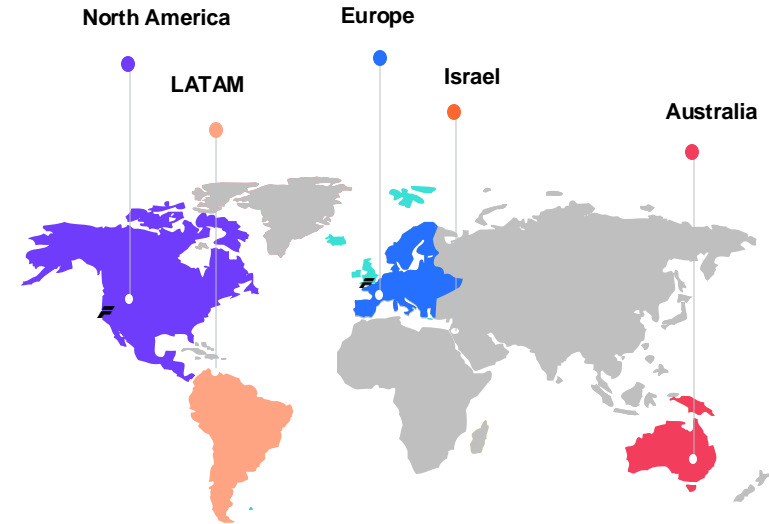
# Forgepoint Updates

19 November 2024



<b>2015</b> Founded	<b>3</b> Funds	<b>\$1B+</b> AUM
<b>50</b> Investments	<b>24</b> Team Size	<b>14</b> Investors
<b>33</b> Active Investments	<b>100</b> Global Advisory Council	<b>\$5-50M</b> Investment per Company

## Cybersecurity, AI & Infrastructure Software Series A & B and Select Growth (First Institutional Investor)

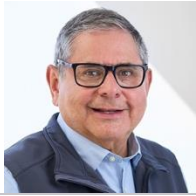


**Investing Globally**  
Cybersecurity is a global mission

# Forgepoint Capital Team

An Experienced and Diverse Team of Company Builders

## / INVESTMENT – FORGEPOINT US /



**J. Alberto Yépez**  
Managing Director &  
Co-Founder



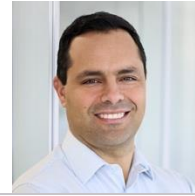
**Donald R. Dixon**  
Managing Director &  
Co-Founder



**Lisa Lee**  
Chief Financial Officer



**Leo Casusol**  
Managing Director



**Ernie Bio**  
Managing Director



**Andrew McClure**  
Managing Director



**Reynaldo Kirton**  
Vice President



**Casilda Angulo**  
Senior Associate

## / INVESTMENT – US /



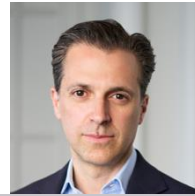
**Jimmy Park**  
Senior Associate



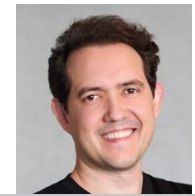
**Shane Shook, PhD**  
Venture Partner



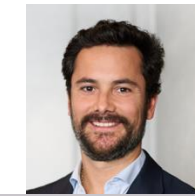
**Kathryn Shih**  
Venture Partner



**Damien Henault**  
Managing Director  
International



**Michael Cortez**  
Partner  
International



**Jaime Goyarrola**  
Chief Financial Officer  
International



**Andres Andreu**  
Venture Consultant



**Tom Kelley**  
Venture Consultant

## / INVESTMENT – FORGEPOINT CAPITAL INTERNATIONAL /

## / GROWTH /

## / GROWTH /



**Sanjay Uppal**  
Venture Consultant



**Mercy Caprara**  
Portfolio Operations



**Tanya Loh**  
Chief Marketing Officer



**Karl Sharman**  
Talent Management



**Jessie Huang**  
Controller



**Huzefa Sharafali**  
Information Technology



**Sue Chung**  
Operations &  
Administration



**Stacey Holmes**  
Operations &  
Administration

## / OPERATIONS /



# Forgepoint Capital Team

An Experienced and Diverse Team of Company Builders

## / INVESTMENT – FORGEPOINT US /



**J. Alberto Yépez**  
Managing Director &  
Co-Founder



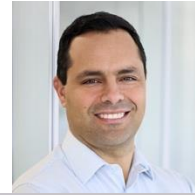
**Donald R. Dixon**  
Managing Director &  
Co-Founder



**Lisa Lee**  
Chief Financial Officer



**Leo Casusol**  
Managing Director



**Ernie Bio**  
Managing Director



**Andrew McClure**  
Managing Director



**Reynaldo Kirton**  
Vice President



**Casilda Angulo**  
Senior Associate

## / INVESTMENT – US /



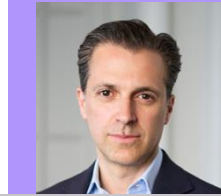
**Jimmy Park**  
Senior Associate



**Shane Shook, PhD**  
Venture Partner



**Kathryn Shih**  
Venture Partner



**Damien Henault**  
Managing Director  
International



**Michael Cortez**  
Partner  
International



**Jaime Goyarrola**  
Chief Financial Officer  
International



**Andres Andreu**  
Venture Consultant



**Tom Kelley**  
Venture Consultant

## / INVESTMENT – FORGEPOINT CAPITAL INTERNATIONAL /

## / GROWTH /

## / GROWTH /

## / OPERATIONS /



**Sanjay Uppal**  
Venture Consultant



**Mercy Caprara**  
Portfolio Operations



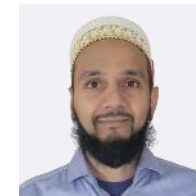
**Tanya Loh**  
Chief Marketing Officer



**Karl Sharman**  
Talent Management



**Jessie Huang**  
Controller



**Huzefa Sharafali**  
Information Technology



**Sue Chung**  
Operations &  
Administration



**Stacey Holmes**  
Operations &  
Administration

# Global Advisory Council

Since January 1, 2024, 8 new industry leaders have joined us



**Elizabeth "Liz" Butwin Mann**

Advisor, Board Member; Former Strategy and Growth Leader- Americas Technology Consulting, EY



**Hazel Diez Castaño**

Global Chief Information Security Officer, Santander; Former Head of Security Consultancy, Architecture and Design, Aviva



**Don Duet**

Public Cloud Strategy Lead, Fortinet; Former CEO & Co-Founder of Concourse Labs (acq. Fortinet) and Technology Leader at Goldman Sachs



**Justin Foster**

CTO, Forescout; Former CTO and Co-Founder, Cysiv (acq. Forescout)



**Brian T. Geffert**

Vice President of Cyber Defense, 3M; Former Global Chief Information Security Officer, KPMG



**Paul Lanzi**

Founder and Principal Consultant, IDenovate; Former Founder and COO, Remediant (acq. Netwrix)



**Hector Saldaña**

Senior Advisor to Boston Consulting; Managing Partner, Invention Global Fund, Former VP Asia Pacific at Wolfram Alpha, Former Sr. Executive at Entrust and Apple



**Sandip Wadje**

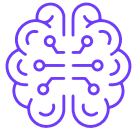
Managing Director – Global Head of Emerging Technology Operational Risks and Intelligence, BNP Paribas





# Forgepoint Investment Themes

Grounded in Customer Priorities and Key Market Drivers



## Securing AI, AI for Security

How cybersecurity can secure AI and how AI can improve cybersecurity



## Continuous Trust and Identity Management

Creating fully secured digital identities and perfect data that connects in real time



## Cybersecurity for the Long Tail

Protecting the underserved Small and Midsize Businesses (SMBs) that power the global economy



## Proactive Cybersecurity and Risk Management

It's not *whether* a company will get breached – it's a matter of *when*, and *what* to do about it



## Securing Infrastructure, from Cloud to Edge and Beyond

Establishing a robust digital grid to access business-critical resources to drive immediate outcomes

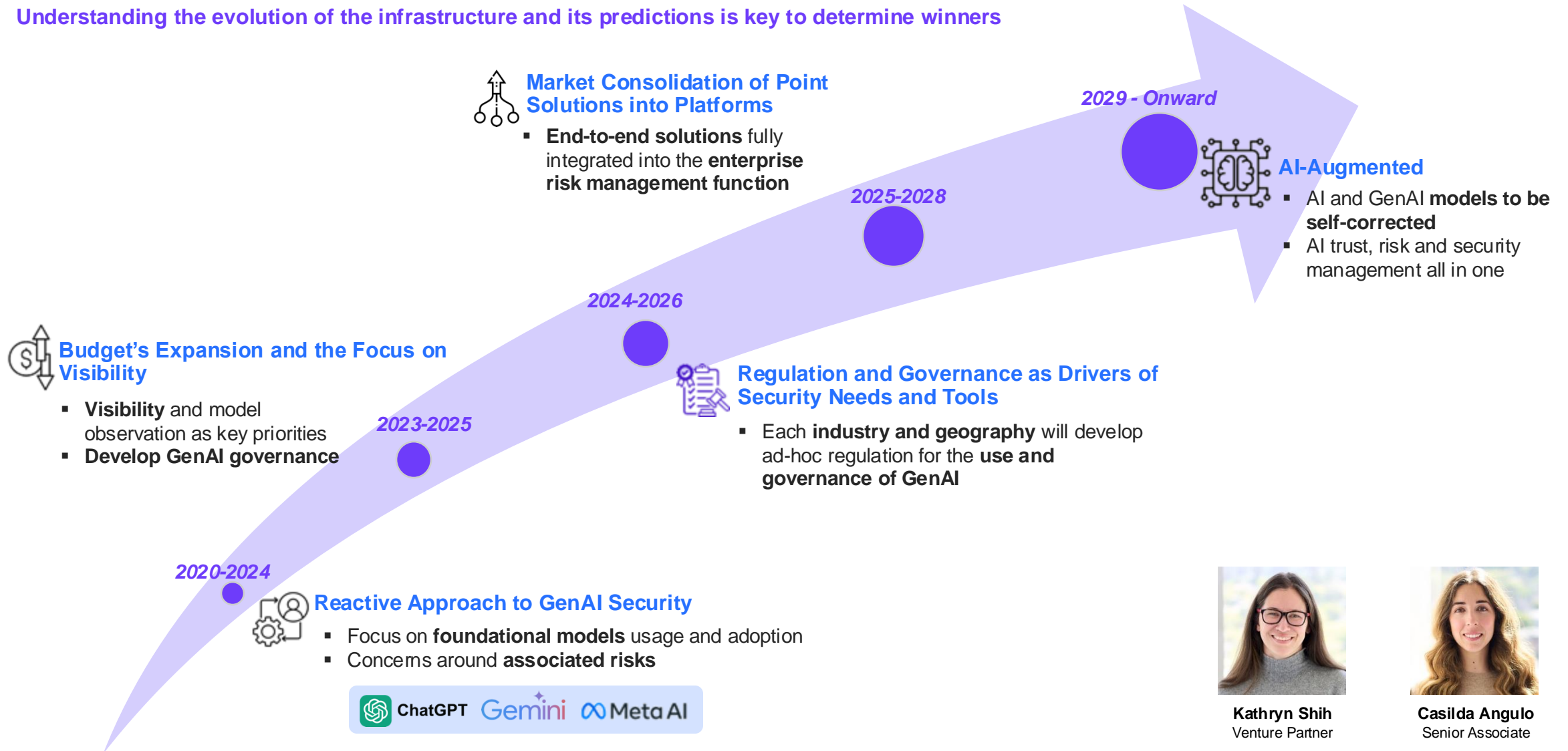


## Trust in Software

The future of software is secure components flowing through a resilient supply chain

# Market Direction of GenAI Security Management

Understanding the evolution of the infrastructure and its predictions is key to determine winners



**Kathryn Shih**  
Venture Partner



**Casilda Angulo**  
Senior Associate



# AI Security Strategy – Two Parallel Tracks

## Security for AI

Tools to secure AI systems from attack



## AI for Security

AI-native tooling to solve existing security challenges



# Welcome to the Forgepoint Family

New Investments in 2024



[akaindentity.io](https://akaindentity.io)

Data and intelligence layer simplifying identity access management (IAM)

Identity



[hyperproof.io](https://hyperproof.io)

Automated security assurance and compliance operations

Risk Management  
Security Operations



[nudgesecurity.com](https://nudgesecurity.com)

SaaS security discovery, monitoring and management

Applications  
Security Operations  
Risk Management



[synadia.com](https://synadia.com)  
[nats.io](https://nats.io)

Next generation digital communications to securely unify cloud, edge, and IoT

Infrastructure  
Data



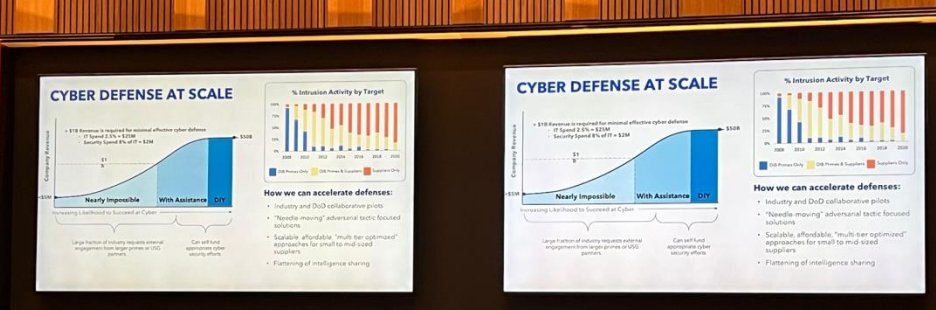
# Community Highlights

## 2024 Events

**Guests include entrepreneurs, CISOs/CxOs, government leaders, co-investors, and senior executives from industry partners**

- National Cyber Innovation Forum (Washington, DC), cohosted with Carahsoft, Microsoft, Forescout, and Snowflake
- Private Cyber Leadership Dinner (NYC)
- RSAC '24 (SF) Security VC Reception cohosted with Sapphire, Norwest, and Gula Tech Adventures
- RSAC '24 (SF) National Security Social cohosted with Gula Tech Adventures, IQT, and Shield Capital
- RSAC '24 (SF) 14<sup>th</sup> Annual Executive Dinner at RSA Conference cohosted with PwC and Google Cloud
- RSAC '24 (SF) CISO Dinner cohosted with MunichRe Ventures and Trace3
- Black Hat '24 (LV) Executive Security Lunch cohosted with Foundation Capital
- Black Hat '24 (LV) CISO Dinner cohosted with IQT and SVB
- Black Hat '24 (LV) Vision & Voice Breakfast cohosted with NightDragon, Keyfactor, Uptycs, and MarketBridge
- Roll Call '24 (SF) in support of Vets in Tech, cohosted with a16z, Beyond Capital, Meritech, SecondFront, Shield Capital, Point72 Ventures





National Cyber Innovation Forum – Embassy of Australia in Washington, DC





14<sup>th</sup> Annual Executive Dinner at RSA Conference 2024



# The Forgecast


<https://forgepointcap.com/forgecast/>

Listen to /The Forgecast/

The who's who and what's what in cybersecurity, AI, and infrastructure software.

[LISTEN NOW](#)

LATEST



Proactive Network Threat Detection with Ricardo Villadiego

NOVEMBER 13, 2024 • 44 MINUTES

APPLE PODCASTS SPOTIFY YOUTUBE AMAZON MUSIC




Securing the 99% with Kyle Hanslovan

Episode 9 January 30, 2024



Secure Elections and Defending Democracy with Cait Conley

Episode 15 November 1, 2024



From Bootstrapped to Venture-Backed with Vinnie Liu

Episode 14 October 30, 2024



Cybersecurity as a Business Enabler with Eddie Borrero

Episode 13 September 23, 2024

**The who's who and what's what in cybersecurity, AI, and infrastructure software.**



A Blueprint for Building Cybersecurity Startups with Ross Haleliuk

Episode 12 April 27, 2024



Quantifying Cyber Risk with Pascal Millaire

Episode 11 March 28, 2024



Staying Clear and Focused on the Mission with Billy Gouveia

Episode 10 March 7, 2024

# Agenda

- 1:00 PM Welcome and Meeting Kickoff
- 1:10 PM Cybersecurity Market Update: Fall 2024
- 1:40 PM Cybersecurity Issues and Observations for 2025
- 2:10 PM Guardians of the G-AI-laxy: AI & Data Governance Concerns and Opportunities
- 2:50 PM Nudge Security: Securing the Workforce Edge
- 2:53 PM [15 Min Networking Break](#)
- 3:08 PM The Great Debate: Reevaluating Public vs. Private in the Cloud Era
- 3:38 PM AKA Identity: Identity Analytics and Automation
- 3:40 PM Anatomy of a Ransomware Incident
- 4:05 PM Fireside: The CISO Playbook
- 4:30 PM Hyperproof: Next Level Risk and Compliance Management
- 4:33 PM Fireside: An Innovator's Journey, from CTO to CEO
- 4:58 PM [Meeting Close > 5:00 Rooftop Reception > 6:30 Celebration Dinner \(back here!\)](#)



# 1:10 Cybersecurity Market Update - Fall 2024



**Brian White**

Co-Head of Security & Defense Technology

Piper Sandler



# 1:40 Cybersecurity Issues and Observations for 2025



**Dr. Ed Amoroso**

Founder & CEO  
TAG InfoSphere



The TAG logo is displayed in white, bold, sans-serif capital letters on a solid blue rectangular background. The background of the entire slide is a photograph of a modern, multi-story building with a glass and metal facade, set against a clear blue sky. The building's architecture features a prominent cantilevered upper section. In the foreground, there are green trees and a white canopy tent.

**TAG**

# Cybersecurity Issues and Observations for 2025 (with Free Publications)

Prepared by

Dr. Edward Amoroso

CEO, TAG Infosphere Inc. and Professor, New York University

Former SVP/CISO AT&T, Former Board Member, M&T Bank

[eamoroso@tag-cyber.com](mailto:eamoroso@tag-cyber.com)



## Predicting the Impact of Trump's Election on Cyber



**Edward Amoroso**

Founder and CEO of TAG Infosphere



November 17, 2024

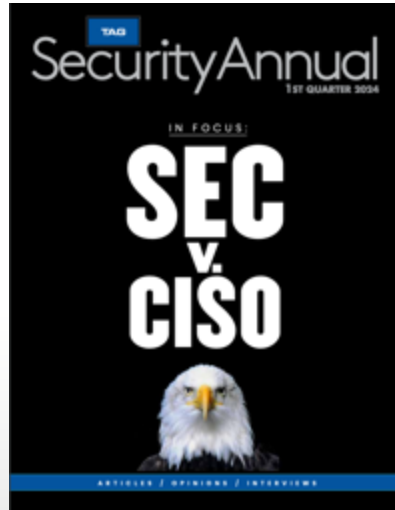
Below are seven predictions from our team at [TAG](#) for how the recent Trump election of 2024 will impact U.S. business practitioners, government agencies,



# Cybersecurity Issue 1: SEC vs. CISOs

(Image generated by DALL-E)





FOCUS: SEC ACTIONS PROMPT QUESTION: WHAT IS THE CISO'S ROLE?

### 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** first posted an article on LinkedIn that called the SEC for changing its stance and its CISO for allegedly defaming 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 caution to condemnation in search of a suitable partner for a debate. TAG's editor contacted **Matthew Rosengate**, who had posted one of the comments attacking the SEC. A cybersecurity industry veteran and former Cybersecurity Strategist at Intel, **Rosengate** also hosts the Cybersecurity Insight podcast. He quickly invited Amoroso to join him for an in-depth conversation. An edited version of the transcript follows.

**Matthew Rosengate:** I'm going to be talking with Ed Amoroso, the founder and CEO of TAG Computer, who in addition, several episodes of late has been, I think, rightly respected, long-time member of the cybersecurity community. There are lots of things that we're going to be discussing, so please let me know if there's anything that you'd like to see. It's been a controversial one of these, right?

**Ed Amoroso:** As there is. There's a lot of different perspectives here. I certainly feel the same great. I would like to see the infrastructure move towards the to see business-level events. It's a lot of people in the same direction. It's just there are a lot of different paths, and there's different opinions about the right way to go. There's a lot of people who are in the same great but right now, I think there's a little bit of confusion about the right way to proceed.

**Matthew Rosengate:** Similarly, there's a tremendous amount of ambiguity and noise that causes confusion. And then we start getting some of the regulations coming in. The particular complaint against SolarWinds was that CISO is ill-equipped, very vulnerable. And then we start to see that. It's a lot of people who are in the same direction. It's just there are a lot of different paths, and there's different opinions about the right way to go. There's a lot of people who are in the same great but right now, I think there's a little bit of confusion about the right way to proceed.

**Amoroso:** I would really love to agree that the fact that you seem to be hearing all things that don't have a lot to do with the CISO question or industry are

FOCUS: SEC ACTIONS PROMPT QUESTION: WHAT IS THE CISO'S ROLE?

## ROUNDTABLE: SEC AND THE CISO'S PLIGHT



Joel Caminer

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



Randy Milch

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



Ed Amoroso

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.



Joe Sullivan



## Cybersecurity Issue 2: Securing AI vs. Using AI

(Image generated by Wombo)





FOCUS: ARTIFICIAL INTELLIGENCE

### HOW SHOULD ARTIFICIAL INTELLIGENCE BE REGULATED?

BY DAVID NEUMAN

Artificial intelligence has drawn much attention in early 2023, as recent advances that have been made available to everyone by the general public, such as ChatGPT, have impressed many people. But the power of AI has left many, including some experts in the field, alarmed. They worry if the technology can be used to threaten human life, and some have advocated legislation to slow and oversee its rapid advance. The question is whether and how to regulate it, and what, if any, already exists.



**FIVE STATES HAVE ENACTED LAWS**

Our research found that over the past few years, five states and three cities in the United States have enacted laws designed to monitor or control artificial intelligence, or at least monitor how others use existing similar legislation of their own. A number of the laws were written in the wake of incidents of facial recognition technology. They also create task forces and agencies to monitor the use of AI and to recommend relevant policy changes.

More than 200 countries, Colombia, and 30 states have enacted laws designed to monitor the use of AI, and many are not just AI-specific but address the rights of individuals, while limiting protection of the rights of monitoring and, ultimately, use of facial recognition technology that is not the only means for control. The law prohibits either facial or voice enhancement agencies from using facial recognition technology to monitor results, and prohibits individuals in a criminal investigation or under arrest. Other law enforcement seeks to establish prohibitive rules that are only permitted to use the technology to match results in conjunction with

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

FOCUS: ARTIFICIAL INTELLIGENCE

### CAN AI PROTECT HUMANS FROM HUMANS?

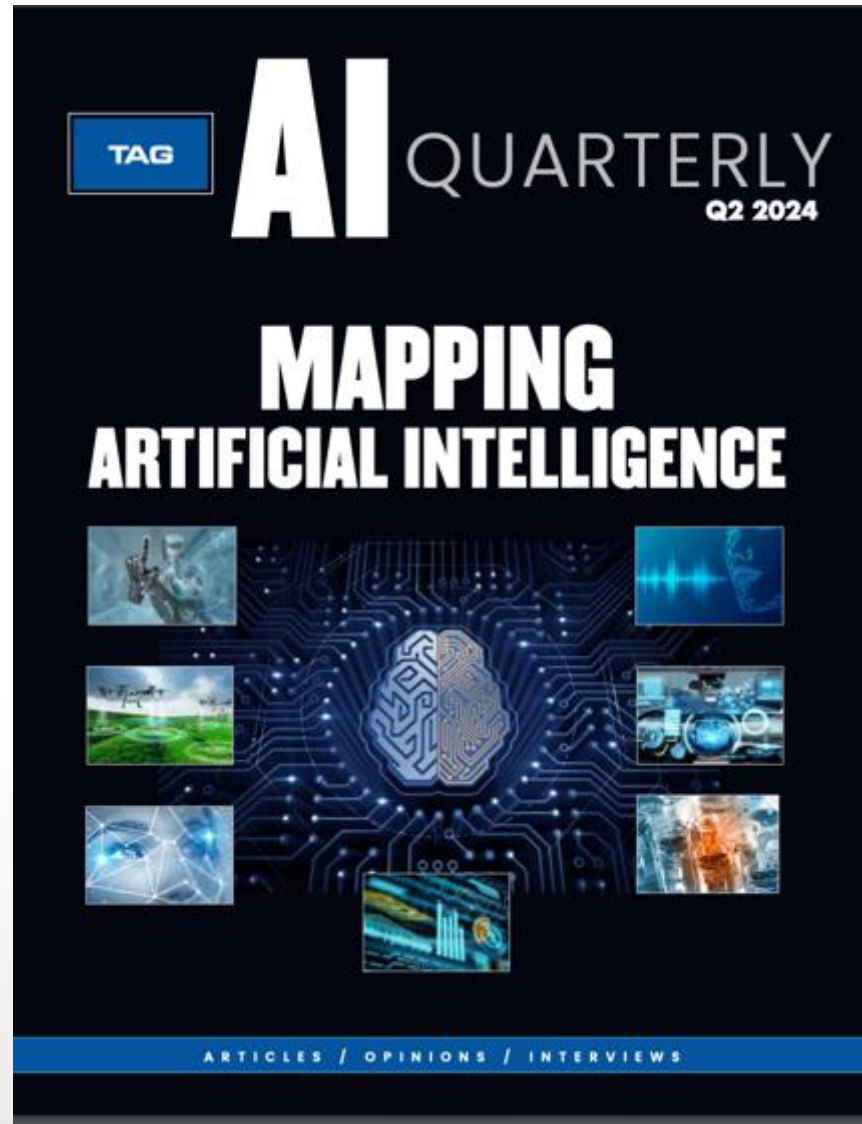
BY DAVID HECHER

From November 2022, when ChatGPT-3.5 was first made available to the public, to sample for free, it has been written about, analyzed, and discussed in addition to the high-profile ChatGPT launch. In good luck, the OpenAI website about its unpredictability, as various journalists probed the necessity of its development together. When the program seemed to lose its balance during some of these conversations, commentators pointed out that the data it trained on comes from people, its unpredictability, mirrors ours.



As time comes a long way, it's clear that programs like ChatGPT will continue to advance rapidly in coming years. It will be much more reliable. That's a prediction that bears the risk that it will not be.

It's hard to predict the future, but when people write with confidence about the future, they are not sure they can predict their own responsibility. What we do know about the way it all shapes the world we live in comes from the way we shape it.







## Cybersecurity Issue 3: Enterprise Security vs. Nation-State Cyber Actors

(Images created with Microsoft Co-Pilot)



## WHAT'S THE ROLE OF THE U.N.? WHERE'S THE LINE ON NEUTRALITY?

RUSSIA'S INVASION OF UKRAINE HAS RAISED INTERNATIONAL LEGAL QUESTIONS LIKELY TO PROVOKE DISCUSSION FOR YEARS.

AN INTERVIEW WITH ERIC JENSEN

Thirty after Russia invaded Ukraine on February 24, an *International Business Times* interviewee said, Jensen asked the question that was in its earliest stages: "Jensen is an expert on the use of armed conflict and national security law. There was a lot to talk about—the right to intervene in pre-emptive. For example, we'd asked the expert on the United Nations whether any international agreements were in question to change the way Russia acted. We asked him to comment on developments that followed our earlier conversation, including any other work in Ukraine. He also asked if the countries supporting Ukraine have crossed the neutrality line. That's an aspect of the conflict that he predicted will be one of the things that most profoundly affects international law in the next couple of decades."

**TAG Cyber:** We want to ask you some questions about the United Nations. The Security Council was asked to take action against Russia for its invasion of Ukraine but Russia has a permanent seat on the Security Council. Is there anything the U.N. can do about it or in which one of the parties has only power over any resolution?

**ERIC JENSEN:** Well, unfortunately the U.S. doesn't have a veto. It's a permanent member, but it doesn't have a veto. For the U.S. to have a veto, it would need to be a permanent member of the Security Council or an issue in which they have an interest. And, of course, that's been important to the United States ever since World War II. The United States has been very happy to have a veto. It's been very important when it was engaged in military operations to make sure that the Security Council's backing or it was designed for that. You could certainly envision a scenario where the Security Council, through something called the "Uniting for Peace" resolution, could exert control of those international security issues. It's a member of the Security Council who's involved. But that's not how the current UN structure and membership works.



The United Nations Security Council chamber.

## CHINA & CYBERSECURITY

### WHY U.S. RESTRICTIONS ON CHINESE SOFTWARE WILL HAVE NO IMPACT ON CYBER RISK

DR. EDWARD AMOROSO



The actual cybersecurity benefit of Chinese product avoidance is nearly zero.

There's something that every Washington insider knows: Products from companies such as Huawei and ZTE are regarded as being "trusted" under the direction of the Chinese government. This means that such products would be considered trustworthy and not subject to rigorous and frequent security reviews at the United States.

Despite that, the purchase policy restrictions on the purchase of Chinese products would seem to be a good idea, and we know from the "Threats to National Security" studies, based on the work of Bill Lida, that there is a strong likelihood that we can't rely on the availability of Chinese products without having a negative impact on cyber risk.

Unfortunately, the actual cybersecurity benefit of Chinese product avoidance is nearly zero. Furthermore, focusing on reducing energy on the impact of the



### HOW CHINA'S WORLD COLONIZATION PLAN IMPACTS CYBER

CHRISTOPHER WILBER

Telecommunications infrastructure, especially the Internet, is a massive challenge and opportunity in Africa and the Middle East (MENA). While each has an enormous population, it has limited access to the Internet. The governments across MENA and other developing countries struggle to bring connectivity to their people. The increased demand for connectivity has created openings for foreign telecom providers, especially from China, to step in and offer their predatory lending, expertise and technology providers, like China's own Huawei, ZTE and others.

#### CONNECTIVITY AND SECURITY AT A COST

China's belt and road initiative (BRI) is the country's strategy to meet its global infrastructure projects worldwide. In the past decade, China has provided significant investments in infrastructure projects across the globe. The investments have been made in order to create a global network of infrastructure projects. China's BRI initiative has provided most of the major investment in the Middle East and the world. Underneath the surface, there are many risks involved worldwide. They are responsible for bringing heavy infrastructure to the door of the countries, creating significant cybersecurity and data handling challenges for China.

# TAG Cyber Security Annual

3RD QUARTER 2022



# CHINA & CYBERSECURITY

A SPECIAL SECTION

ARTICLES / OPINIONS / INTERVIEWS





## Cybersecurity Issue 4: Corporate Narrative vs. Fake News

(Images generated by Dreamstudio)

FOCUS: DEEPFAKES

## DEEPFAKES REPRESENT THE EVOLUTION OF CYBERSECURITY

DAVID NEUMAN

**EXTRACTION  
TIP** On Thursday, Elon Musk, who has 183 million Twitter followers, tweeted a video apology for the death of an unlicensed driver of Tesla vehicles after their mission engineers were hacked by cybercriminals who streamed the autonomous driving program and forced Tesla to crash. Musk stated that Tesla had brought in outside experts to investigate, but information about the hackers was scarce. He urged extreme caution when operating Tesla vehicles, especially with children as passengers.

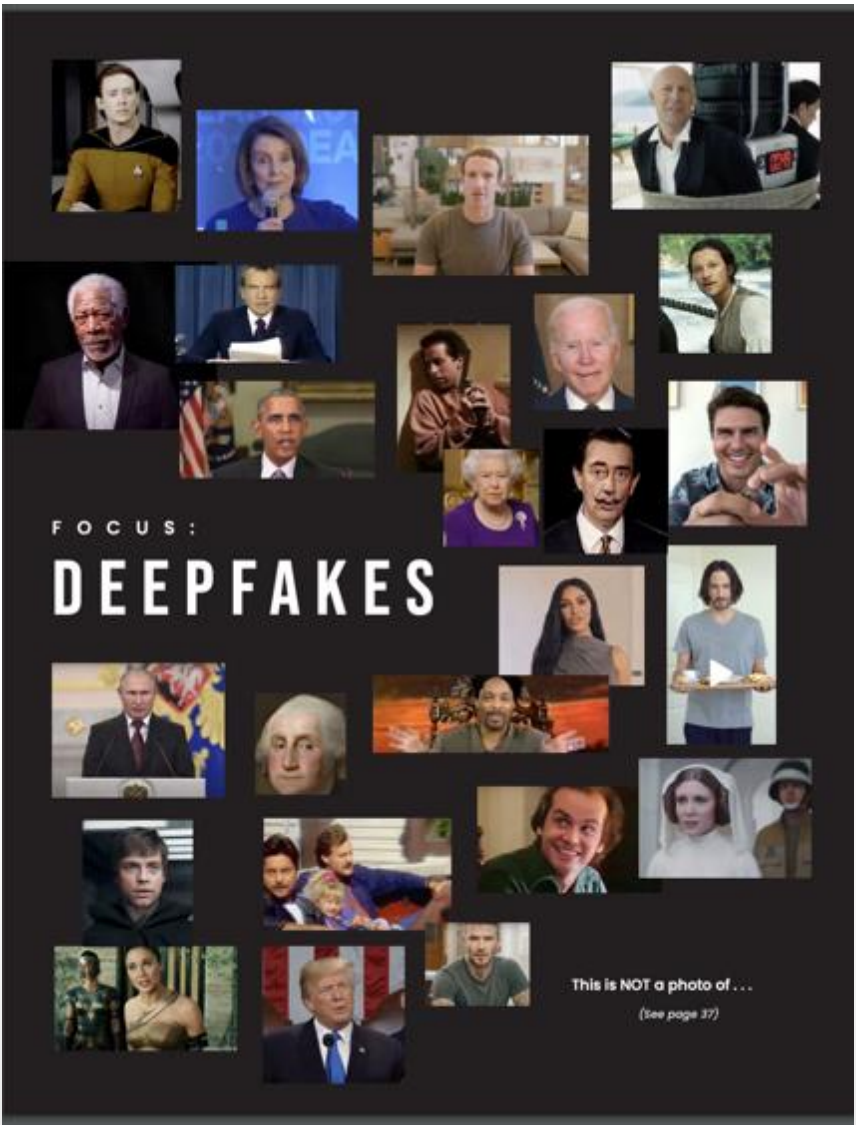
The most video apology there is an example of a deepfake **DEEP FAKE** video, but it could be argued that the very act of cybercrime itself is a challenge. It's not always technology that's so dangerous but the convergence of deepfakes, manipulation, and phishing (including using the name of which people are convinced through the email). The biggest challenge remains of the potential effects on human performance, opinion, and decision-making. This is not to suggest that deepfakes are a threat from more traditional cybercriminals who find security means are exponentially more difficult to detect than information and cyberattacks in real-time.

Influenced through the cybercrime in risk may, for instance, social media platforms. Facebook, Twitter, Instagram, etc. have become home to millions of social media influencers. Subscribers gather data on social media users and their content. According to a 2017 estimate, there were 33 million users on Twitter (around 15% of all accounts), 44 million users on Facebook (up to 15% of accounts), and 63 million users on Instagram (3% of the accounts). That's 142 million users on social media. What is quickly changing is the advancement of deepfake technology that can be used to generate media.

In this article, I will explore the potential effects deepfakes can have on cognitive behavior and decision-making, and the challenge they present for cybersecurity in business.

FOCUS: DEEPFAKES | 30 | QUARTER 2023

FOCUS:  
**DEEPFAKES**



This is NOT a photo of ...  
*(See page 37)*

FOCUS: DEEPFAKES | 30 | QUARTER 2023

TAG Cyber  
**Security Annual**  
1<sup>ST</sup> QUARTER 2023

# DEEPFAKES

A SPECIAL EDITION

BY  
CHRISTOPHER J. DREHMING, J. OBIDIAUNA

INTRODUCTION

## REACHING ENLIGHTENMENT WITH TAG CYBER

BY HIS HOLINESS THE 14<sup>TH</sup> DALAI LAMA

Lama Rinpoche is congratulated by Iliana Salazar on the publication of the **Deepfakes** volume. And Lama Rinpoche says that you will receive your 'divine' subscription. The entire content will remain Western. Thank you folks to TAG Cyber - and you will be happy.

Lead the **Deepfakes** publication with great intention - and deeply appreciate the work that has gone into its development. As the moderator or contributor - can tell you with confidence. To combine complete enlightenment you must work with TAG Cyber.

My daily routine includes a steady stream of TAG Cyber settings. After my morning shower, I take a job interview's morning workout - and engage with my meditation. Then during my hot yoga, I listen videos of 14th Dalai Lama's talks. The topic will discuss.

After some morning office work, I like to read letters from David Neuman, David Neuman and Iliana Salazar - and Iliana Salazar's response. This helps me practice my meditation in the day, with morning (and) noon. I have to make sure my tag cyber is in my mind.

I am particularly taken with the topic of this volume - **Deepfakes**. To share the progress of all, please, could help me and Iliana Salazar with their spiritual activities. But do it before the end of the process to work, especially with TAG Cyber, working the program. As it goes.

By the way, I'd mention that you should attend your subscription to Iliana. Just don't forget to TAG Cyber. The subscription will give you insight, and it will help you better to see. They're better than anything, but only a bit. Start with TAG Cyber, for enlightenment.

That is enough for now. To be happy, and please do not trust or believe everything you read. It must be a **fact**. Or a **deepfake**.

FOCUS: DEEPFAKES | 30 | QUARTER 2023





## Cybersecurity Issue 5: Cyber Underwriters vs. Ransomware Threats

(Images generated by Google Gemini)



## DOES YOUR COMPANY HAVE THE RIGHT CYBER INSURANCE?



FOUR QUESTIONS YOU SHOULD BE ASKING AND ANSWERING  
**JOANNA BURKEY**

**T**o insure or not to insure? When it comes to cyber insurance, this is often posed as a binary question. The reality is that many companies don't have a choice. They must insure. In a world where no entity is safe from a cyberattack, it is advisable for companies to defend against not only the attack itself, but potential collateral effects as well. Especially for public companies, the risk of a poor search shareholder derivative lawsuit is a very real threat, and having cyber insurance is part of a prudent risk and reputation defense strategy.

Most operational uses of cyberattacks and ransomware for 30 years, and during the last 20 the type of cyber insurance policy if one came up, the last 10 years have brought a sea change in the area, one in which those that have not seen that as a global CISO have a professional responsible for the policy. Cyber insurance was demanded not at my discretion over the last decade. In 2011, I was often leading the annual effort for my employees, generally in partnership with our CISO. This activity was primarily centered around engaging with vendors, evaluating options, and working to best align coverage with enterprise policies.



## WHAT'S NEXT IN CYBER INSURANCE



**DAVID HECHER**

**W**hile most can relate to a person's discomfort or change, **Anthony DiNapoli** remembers when he got his 8th grade 2003. He'd been taking in the cyber insurance business for nearly a decade, and had just learned that Target Stores had been hit with a massive data breach. He saw Target's CEO underwriter at AIG (now Chubb), and he was soon on the phone with claims handlers, lawyers, and the Social Service. Somewhere along the way, someone told him that the data hadn't been protected. "This is crazy," he said. "I've been told otherwise by the company itself. That's when he learned that his understanding of technology and cybersecurity did not match what he knew about insurance. Target's underwriter was point of sale, he was told not to and to send. "After in the morning the difference he asked: "That was a major point in my career." He added: "You need to always be a student."



Anthony DiNapoli

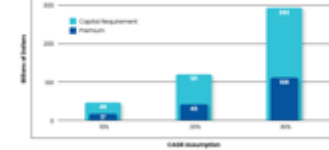
## PROJECTING CYBER INSURANCE GROWTH: A 10-YEAR U.S. MARKET OUTLOOK

TAG CYBER INSURANCE JOURNAL OFFERS BELOW AN EXCERPT FROM A CYBERCUBE REPORT ON THE FUTURE OF THE U.S. CYBER INSURANCE MARKET. YOU CAN READ THE FULL REPORT [HERE](#).

**At CyberCube**, we provide the world's leading analytics to quantify cyber risk. In this report, we apply our quantitative lens to the growth trajectory of the U.S. standalone cyber market in the next 10 years, from 2024 to 2034. We have chosen based on premium growth numbers, market capital requirements to support the growing line of business, and other what structural changes would be required to meet the projections. Our key findings are:

1. Cyber insurance is projected to grow rapidly over the next decade, driven by increasing digitization of the global economy and rising concerns about cyber risk. CyberCube has modeled three compound annual growth rates (CAGR) for the U.S. insurance industry in 2024-34, resulting in \$17 billion of premiums, 25% growth resulting in \$40 billion of premium and 85% growth resulting in \$100 billion of U.S. cyber premium.

10-year Premium and Capital Requirements Across a Range of U.S. Insurance Market Growth Assumptions



TAG

# Cyber Insurance Journal

2025



ARTICLES / OPINIONS / INTERVIEWS





**NYU CCS  
Brooklyn and Manhattan**



**Thanks!**



**eamoroso@tag-cyber.com**



**TAG Global HQ  
45 Broadway**



# 2:10 Guardians of the G-AI-laxy: AI & Data Governance



**Drew Cukor**  
Former Chief AI and Data  
Officer  
**JPMorgan Chase**



**Elena Kvochko**  
Adjunct Professor  
**Cornell SC Johnson**  
School of Business



**Scott Miller**  
Director, Cybersecurity  
Services  
**Lowe's Companies, Inc.**



**Sandip Wadje**  
Managing Director & Head  
of Emerging Tech Risks  
**BNP Paribas**



**Kathryn Shih**  
Venture Partner  
**Forgepoint Capital**

---

**PANELISTS**

**MODERATOR**



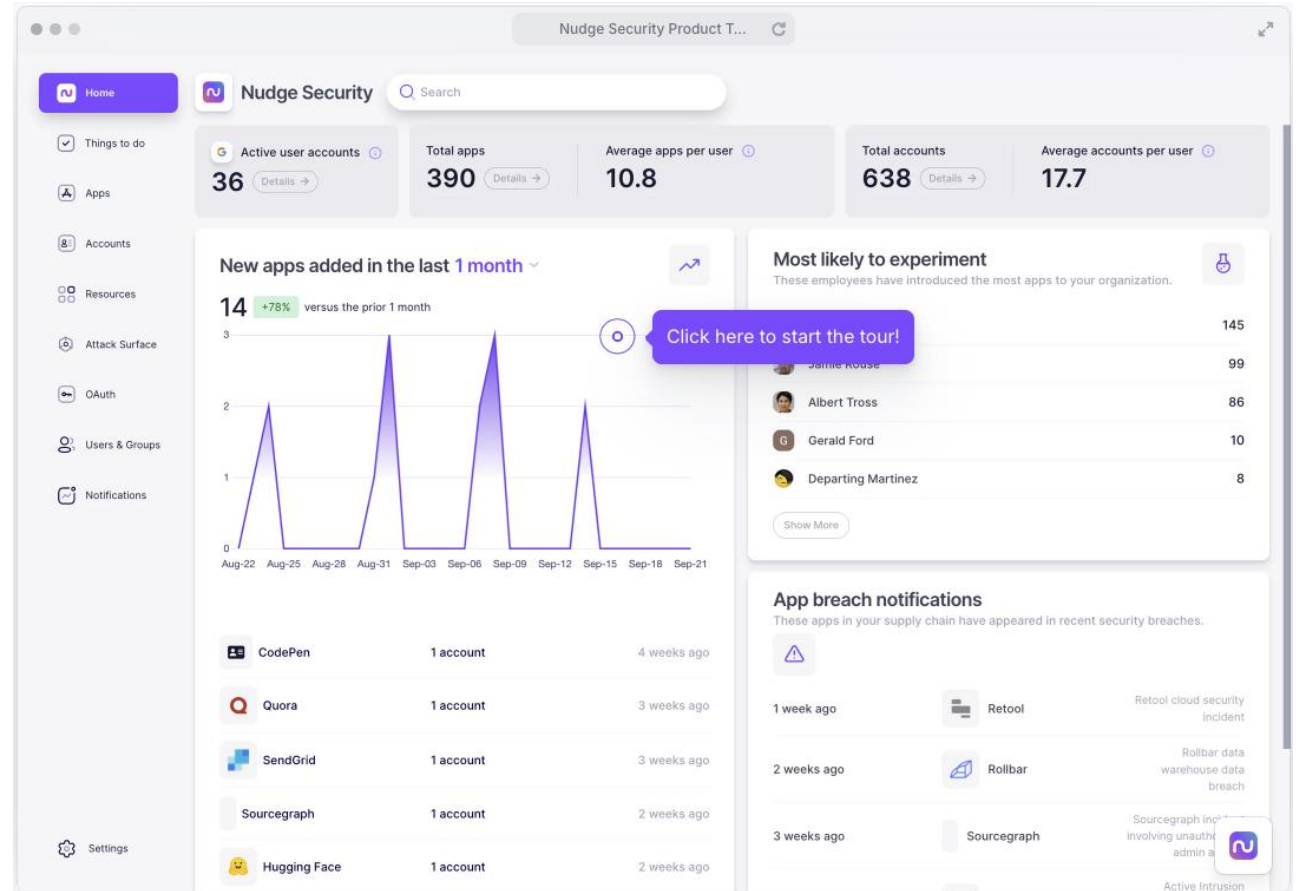


SaaS security that inventories and monitors every cloud and SaaS account



Russ Spitler  
Co-Founder & CEO  
Nudge Security

<https://nudgesecurity.com/>



### Sample Customers and Relationships





## Securing the *Workforce Edge*



**Russ Spitler**  
Co-founder & CEO

15+ years building security products at AlienVault (AT&T) and Fortify (HPE)



**Jaime Blasco**  
Co-founder & CTO

World-renowned security researcher and former head of AT&T Alien Labs



AT&T Cybersecurity

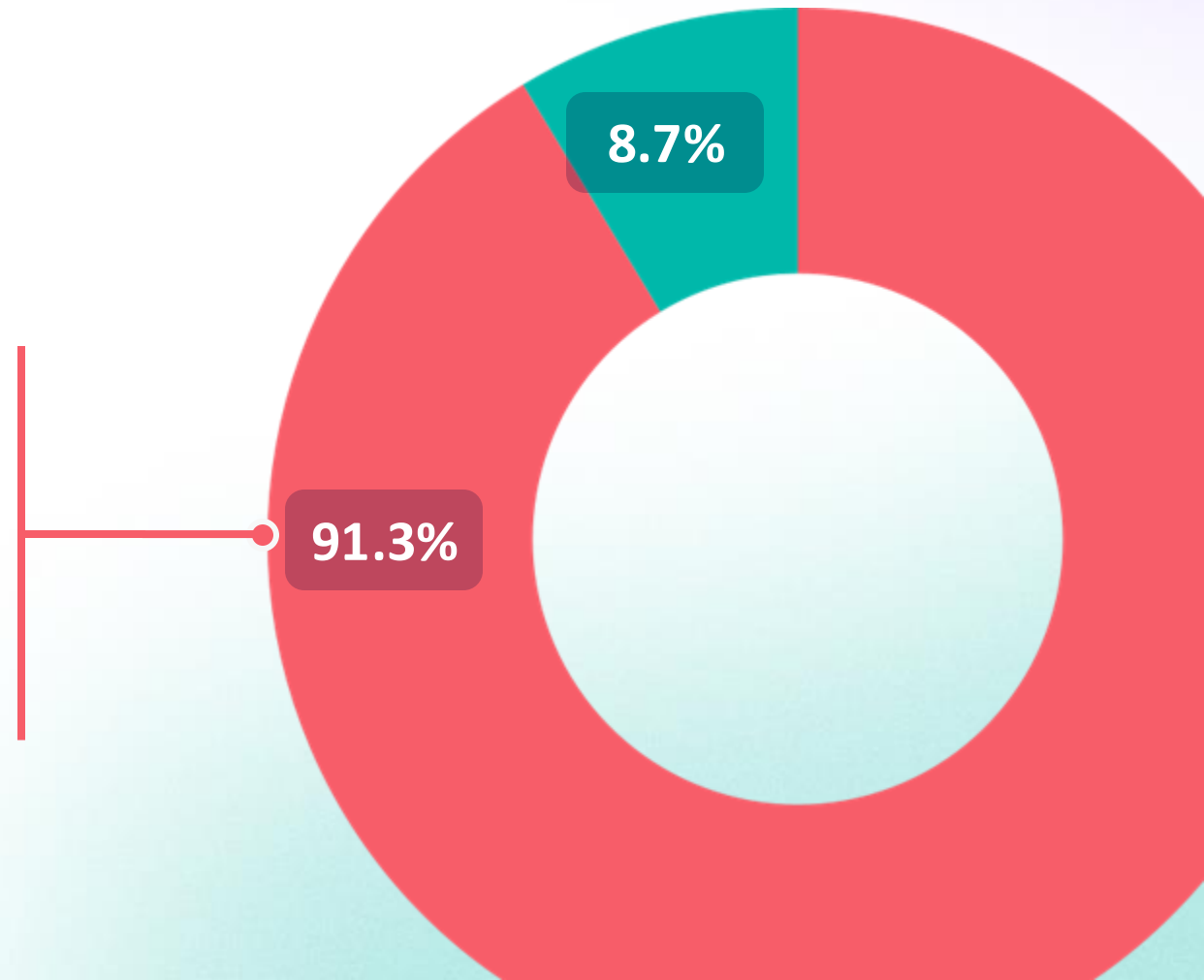


## Example Customers:

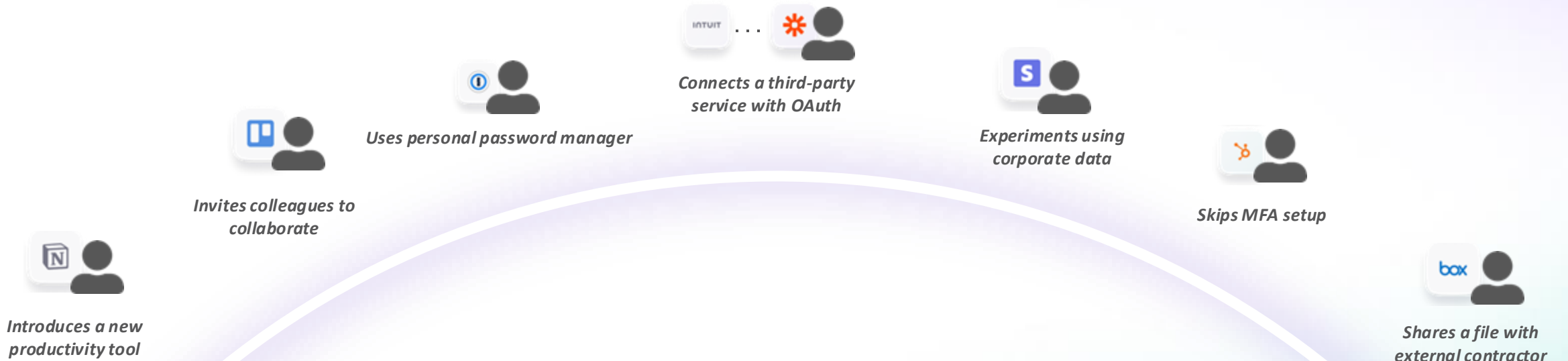




**Over 90% of all apps  
are adopted *outside*  
of IT.**



# Risk is created at the Workforce Edge™



*Without the right visibility and controls in place,  
**risk** and **sprawl** run wild at this edge.*



# Traditional approaches aren't cutting it anymore.



IT service request portals...

...assume that work will wait.



Network-based controls

...lack visibility and context.

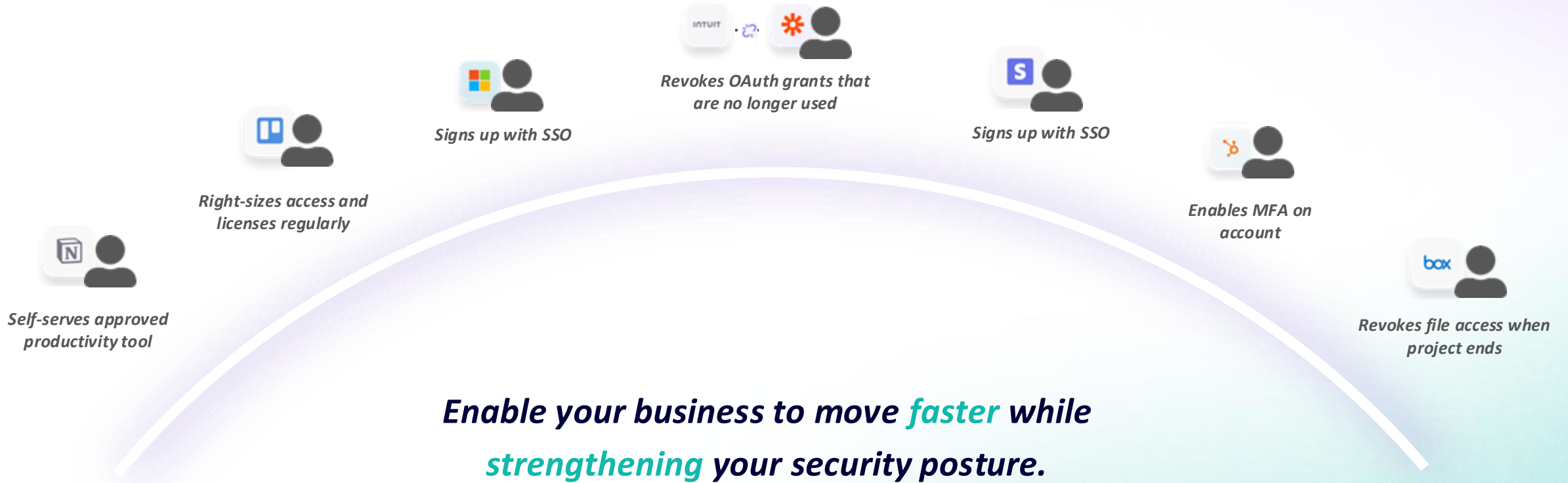


API-based integrations (SSPM)

...require prior knowledge & access.

***Organizations need a new approach to protect and govern all apps, identities, and data across thousands of clouds.***

# What if **security** was created at the Workforce Edge?





An aerial photograph of the New York City skyline at dusk. The sky is a mix of deep blue and orange, with scattered clouds. The city's lights are beginning to glow, with the One World Trade Center being the most prominent, brightly lit skyscraper on the right side. Other buildings of varying heights and architectural styles are visible, all illuminated from within. In the background, a body of water and a bridge can be seen under the twilight sky.

**15 minute Networking Break**  
*Please return by 3:08 PM*

# Agenda

- 1:00 PM Welcome and Meeting Kickoff
- 1:10 PM Cybersecurity Market Update: Fall 2024
- 1:40 PM Cybersecurity Issues and Observations for 2025
- 2:10 PM Guardians of the G-AI-laxy: AI & Data Governance Concerns and Opportunities
- 2:50 PM Nudge Security: Securing the Workforce Edge
- 2:53 PM 15 Min Networking Break
- 3:08 PM The Great Debate: Reevaluating Public vs. Private in the Cloud Era
- 3:38 PM AKA Identity: Identity Analytics and Automation
- 3:40 PM Anatomy of a Ransomware Incident
- 4:05 PM Fireside: The CISO Playbook
- 4:30 PM Hyperproof: Next Level Risk and Compliance Management
- 4:33 PM Fireside: An Innovator's Journey, from CTO to CEO
- 4:58 PM Meeting Close > 5:00 Rooftop Reception > 6:30 Celebration Dinner



# 3:08 Re-evaluating Public vs. Private in the Cloud Era



**Derek Collison**  
Creator of NATS.io and  
Founder & CEO  
**Synadia**



**Hector Hoyos**  
Chief Strategy Officer &  
Head of Cybersecurity  
**GHS**



**Anjana Rajan**  
Assistant National Cyber  
Director  
**The White House**



**Marc Sorel**  
Partner & Cybersecurity  
Practice Lead  
**McKinsey & Co.**

---

**PANELISTS**

---

**MODERATOR**





Globally connect all your applications and data- in the cloud, on premise, and at the edge



**Derek Collison**

Founder & CEO

Synadia

<https://synadia.com/>

Creator of NATS.io

<https://nats.io/>



**Scalability**

NATS can easily scale to millions of clients across a global deployment, providing services that can live anywhere and are easily discoverable.



**Resilience**

Built-in fault tolerance and self-healing capabilities ensure high availability.



**Performance**

Low latency and high throughput make NATS ideal for real-time applications.

**Key advantages of NATS include**



**Security**

A zero trust approach for protection inside or outside the network perimeter with secure interactions between applications, services and devices across multiple clouds, regions and edge environments.



**Simplicity**

NATS provides a foundation for massively distributed systems, without the need for the glue logic, shim layers, specialized tools and middleware required by other technologies. NATS also has a clean, straightforward API that developers love.



**Flexibility**

It supports M:N communication across various use cases, including simple messaging, request-reply, complex data streaming, and real-time materialized views, as well as a key-value store and object store.

**Sample Customers and Relationships**







## Identity Analytics and Automation



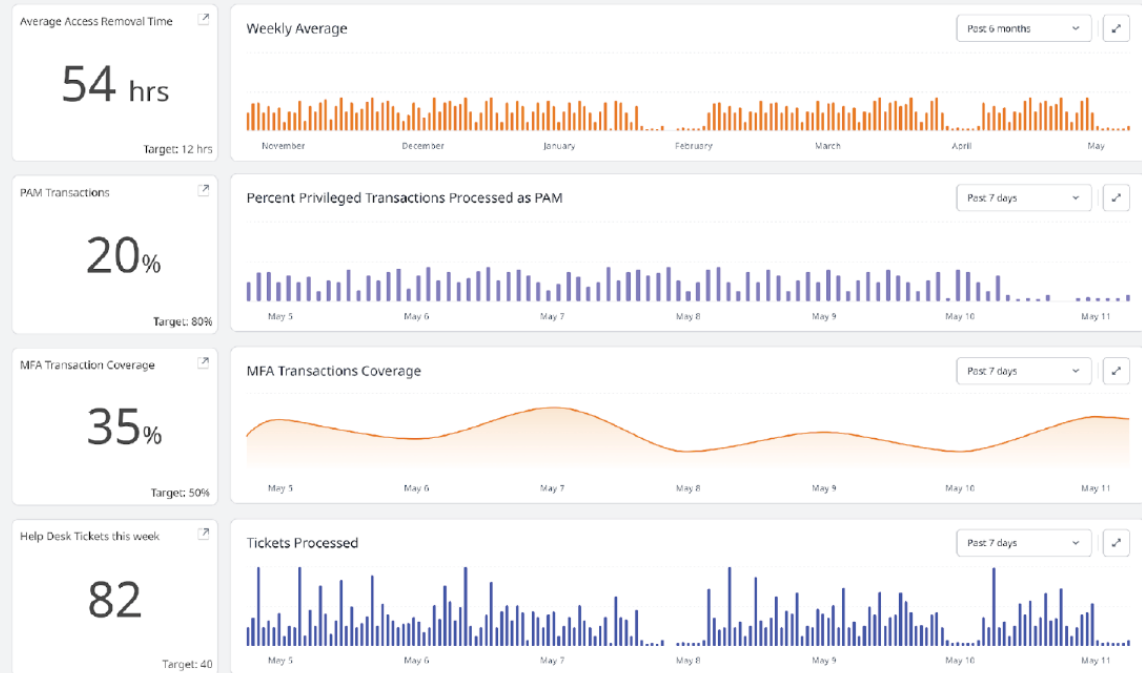
**Will Lin**

Co-Founder & CEO

**AKA Identity**

<https://akaindentity.io/>

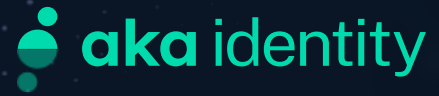
### Outcome Driven Metrics (ODM) Dashboard



### Sample Customers and Relationships



Fortune 500 enterprise organizations across Finance, Healthcare and High Tech.



# AKA Identity: Identity Analytics and Automation

Q4 2024

CONFIDENTIAL & PROPRIETARY



# The Next Convergence in IAM is finding its name:

“Identity Analytics and Automation”

“Identity Visibility and Observability”

“Source of Truth in IAM”

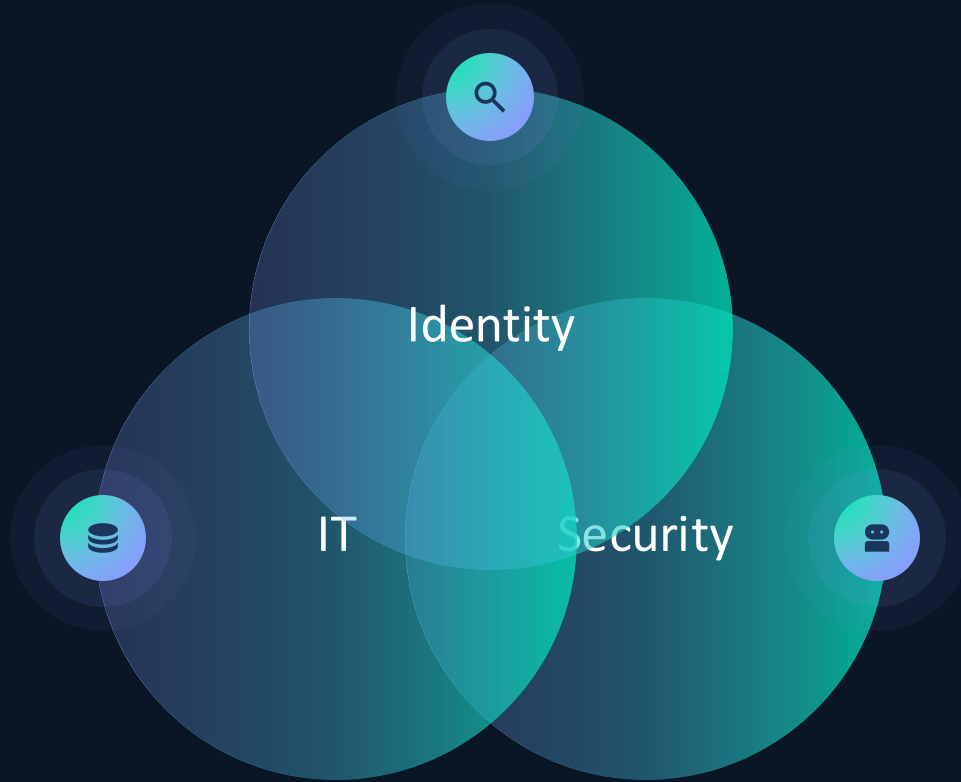
“SIEM for Identity”

“Unified Identity Lifecycle Management”

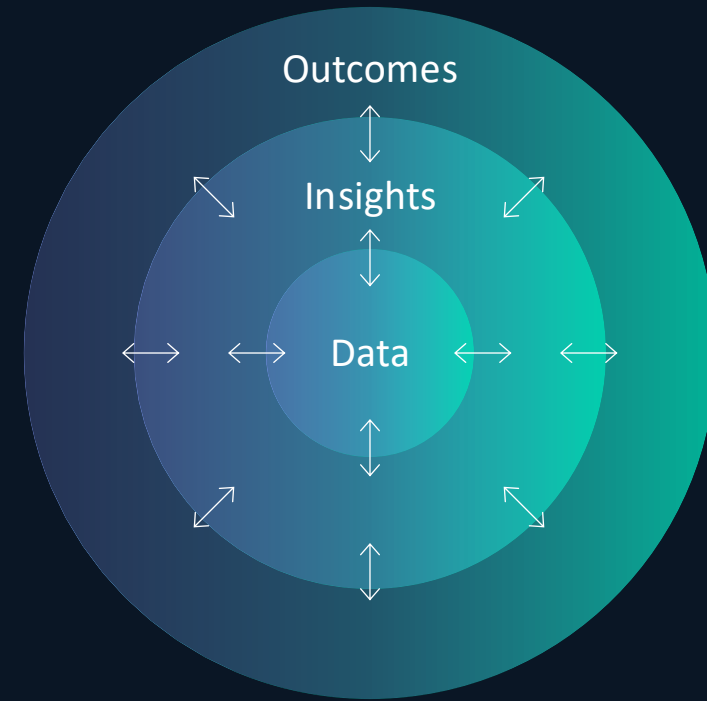
“Identity Security”

# What do Identity Programs Look Like

Today: Legacy



Future: AKA





# Clarity from Chaos



# Mining Data for Value

- Find over-provisioning day 1 based on usage
- Identify “zombie” accounts, eliminate orphaned accounts
- Untangle the complexities of your IAM landscape
- Improve your hygiene, reduce your risk



# Customer Traction

We re-grouped proven talent at AKA. **We're now deploying and through procurement** with multiple referenceable customers with qualified budget

## Closed/Won



Healthcare



Tech



Fintech

## Procurement Stage



Tech



Industrial



Consumer

## Mid-Enterprise: 1,000 – 10,000 employees



**Powered IAM Programs** (not Google Workspace)

**10,000+**

**Entitlements under Management**  
(500+ of Human/Machine Identities x 20+ of Applications/Systems)

**CISO or IAM Leader**

**One Champion/Budget**

## Enterprise: 10,000 – 100,000 employees



**100,000+**  
entitlements  
under mgmt

**2 or more  
champions**

# 3:40 Anatomy of Ransomware Incident



**Billy Gouveia**  
Founder and CEO  
Surefire Cyber

**PRESENTER**



**Cyndi Gula**  
Co-Founder and Managing Partner  
Gula Tech Adventures

**INTRODUCED BY**



# Ransomware – A Multifaceted Problem

- What is ransomware?:
  - A threat actor encrypts data demands a ransom in exchange for a decryption key, or
  - A threat actor steals data and demands a ransom in exchange for a promise to not publish it, or
  - Both (referred to as *double extortion*)
- Ransomware is the perfect crime:
  - Easy to commit,
  - Enormously lucrative, and
  - Done with (near) impunity
- Ransomware is a multidimensional problem:
  - Network Intrusion
  - Data Theft
  - Business Interruption
  - Legal, Regulatory, & Reputational Risk



# Stages of a Ransomware Attack

1

**Reconnaissance**  
Finding the target

2

**Point of Entry**  
Breaking in

3

**Privilege Escalation**  
Getting more access

4

**Lateral Movement**  
Moving around

5

**Exfiltration**  
Stealing data

6

**Encryption**  
Locking up your files



# Stage 1 Reconnaissance

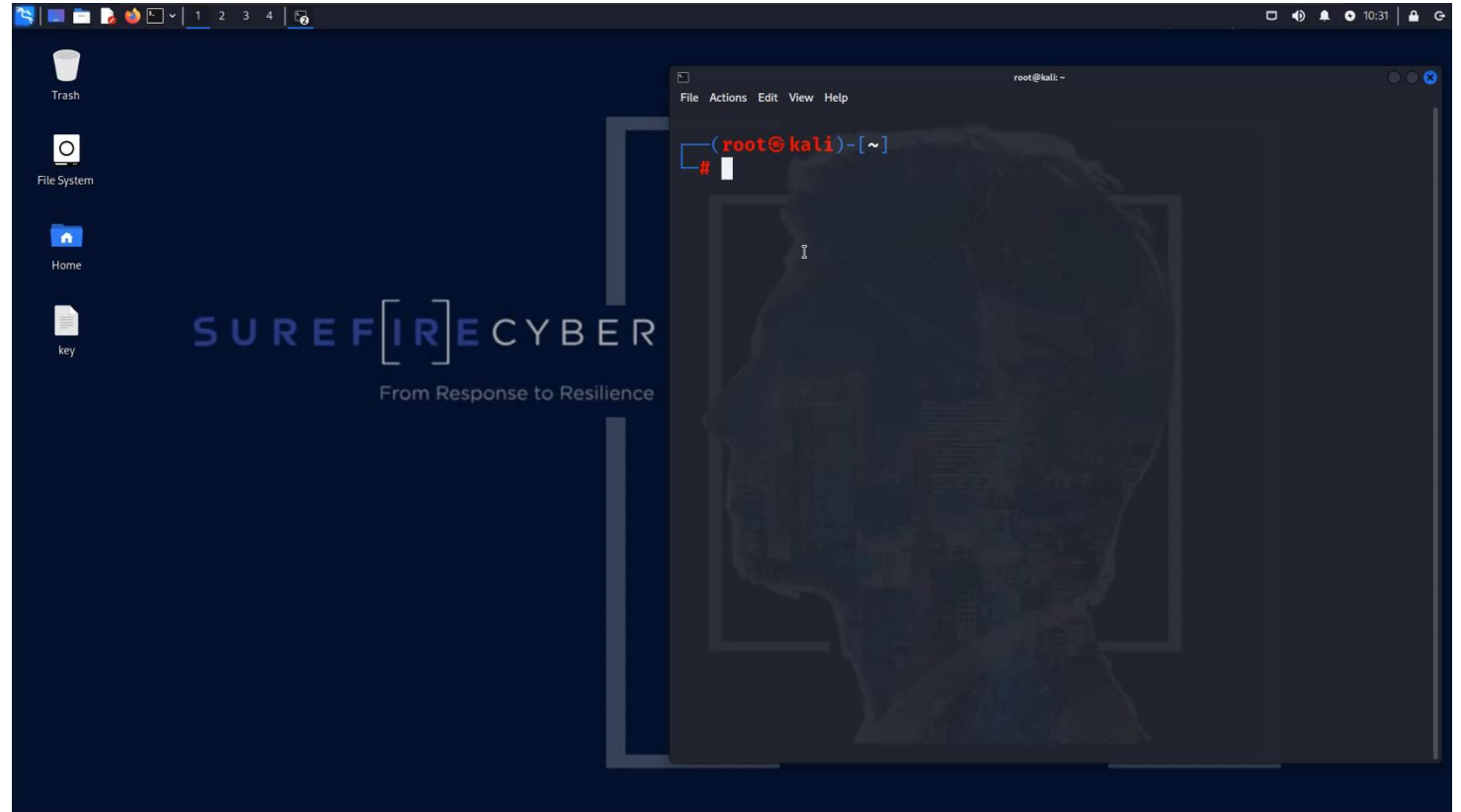
## Finding the Target

### Setting the Scene

- Threat actors are ALWAYS scanning the complete internet to find weaknesses or looking to buy access
- Full scan of the internet can take as little as 45 minutes

### Takeaways

- Threat actors don't need to be "targeting" you to discover an exploitable weakness
- Securing your internet-facing perimeter will help prevent cyber incidents



# Stage 2 Point of Entry

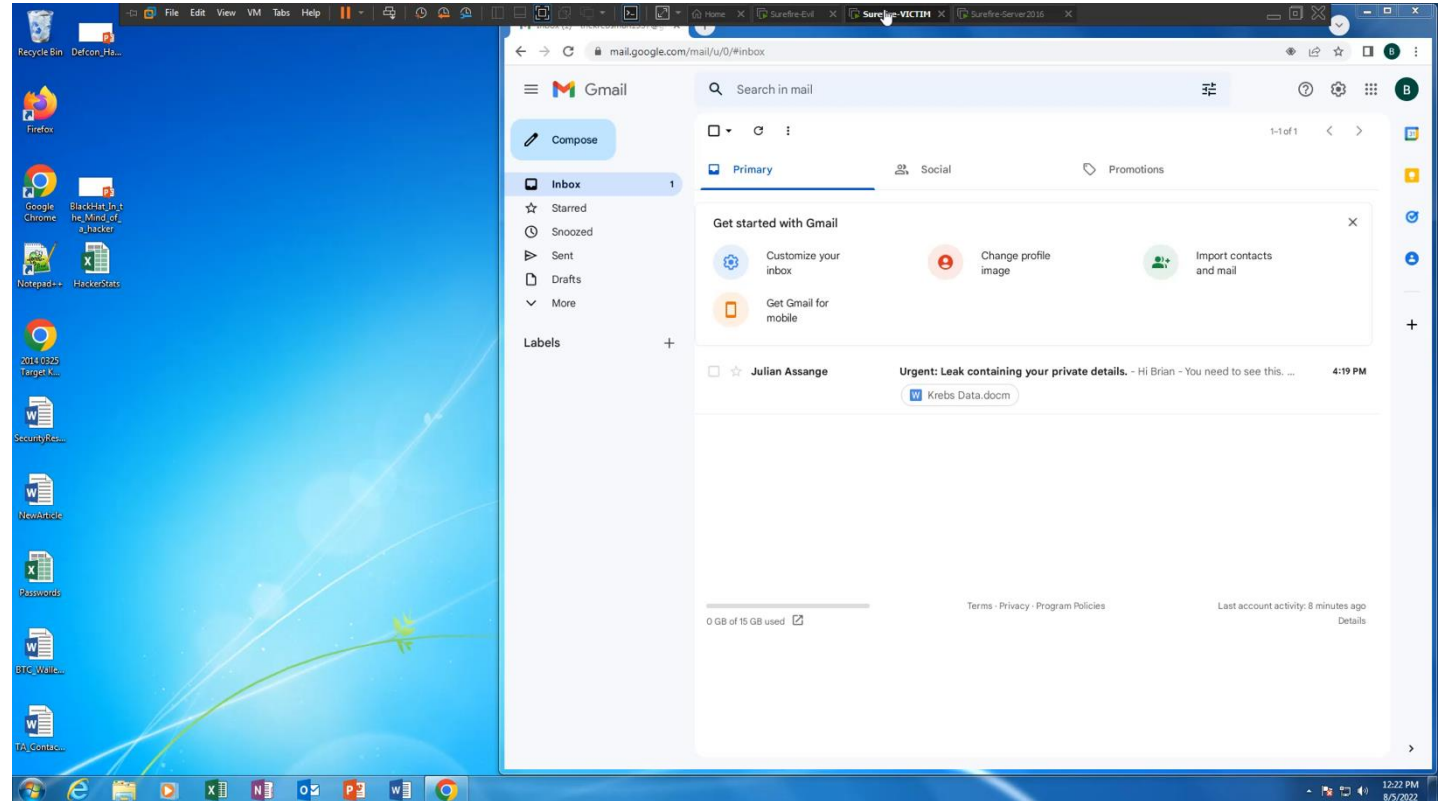
## Patient Zero

### Setting the Scene

- Not finding an external weakness, the threat actor sends an email embedded with malware
- Phishing is very common and can be generic (“Singles in Your Area”) or targeted (“Kevin’s Year End Bonus”)

### Takeaways

- User awareness training and email filtering lower risk of phishing
- Multi-factor authentication is the best way to stop phishing
- Endpoint Security Solution





# Stage 3 Privilege Escalation

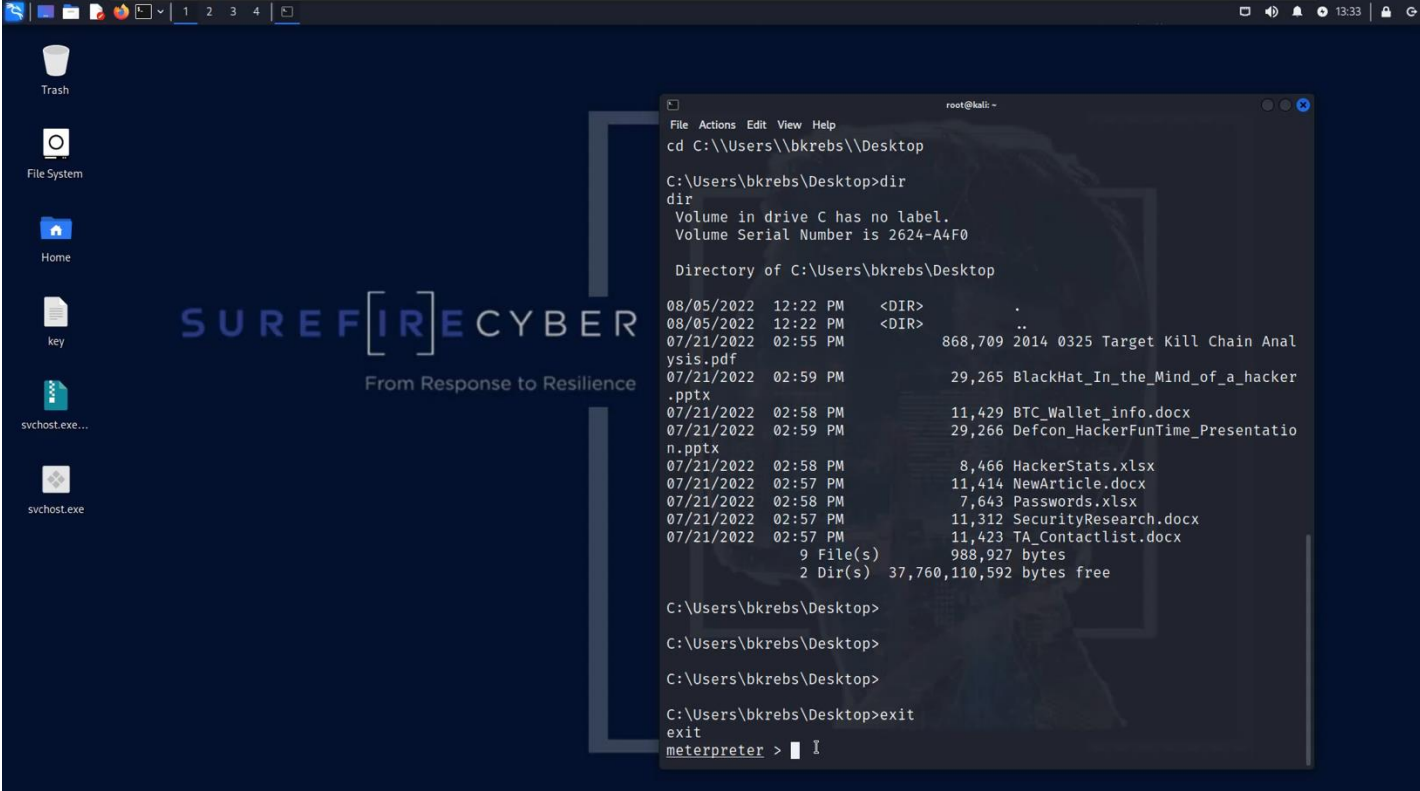
## Getting More Access

### Setting the Scene

- The threat actor's goal is to move from a normal user account to the network administrator's account
- Threat actor gains elevated permissions using a common tool called Mimikatz

### Takeaways

- Minimize privileged accounts and administrative access
- Invest in tools that detect and stop malicious actions
- Keep systems up-to-date with patches



```
root@kali: ~  
cd C:\Users\bkrebs\Desktop  
C:\Users\bkrebs\Desktop>dir  
dir  
Volume in drive C has no label.  
Volume Serial Number is 2624-A4F0  
  
Directory of C:\Users\bkrebs\Desktop  
  
08/05/2022 12:22 PM <DIR>      .  
08/05/2022 12:22 PM <DIR>      ..  
07/21/2022 02:55 PM      868,709 2014 0325 Target Kill Chain Anal  
ysis.pdf  
07/21/2022 02:59 PM      29,265 BlackHat_In_the_Mind_of_a_hacker  
.pptx  
07/21/2022 02:58 PM      11,429 BTC_Wallet_info.docx  
07/21/2022 02:59 PM      29,266 Defcon_HackerFunTime_Presentatio  
n.pptx  
07/21/2022 02:58 PM      8,466 HackerStats.xlsx  
07/21/2022 02:57 PM      11,414 NewArticle.docx  
07/21/2022 02:58 PM      7,643 Passwords.xlsx  
07/21/2022 02:57 PM      11,312 SecurityResearch.docx  
07/21/2022 02:57 PM      11,423 TA_Contactlist.docx  
          9 File(s)      988,927 bytes  
          2 Dir(s)  37,760,110,592 bytes free  
  
C:\Users\bkrebs\Desktop>  
C:\Users\bkrebs\Desktop>  
C:\Users\bkrebs\Desktop>  
C:\Users\bkrebs\Desktop>exit  
exit  
meterpreter > |
```

# Stage 4 Lateral Movement

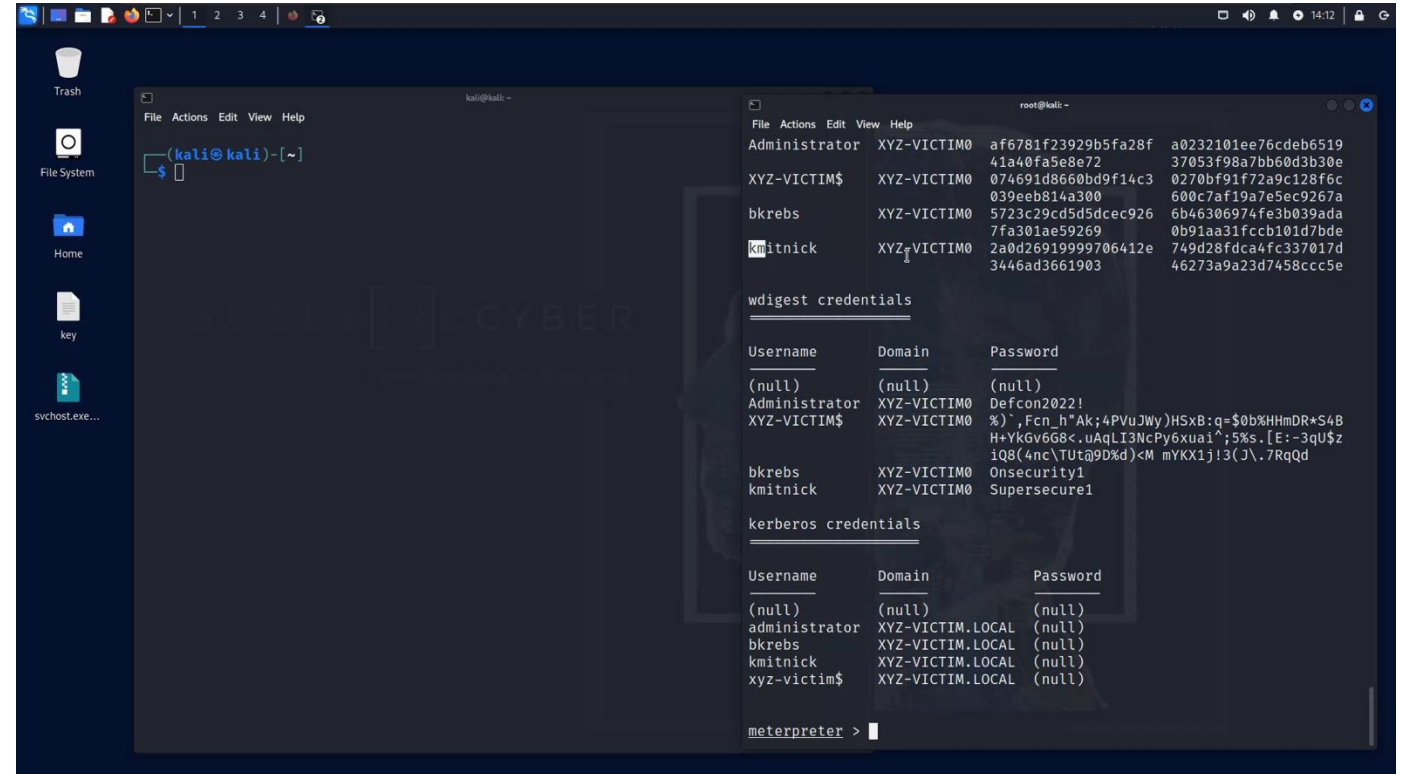
## Moving Around

### Setting the Scene

- Threat actor cracks the password and uses the administrator's credentials to login
- In the middle of the night, the threat actor accesses the server with everyone's passwords

### Takeaways

- Use strong and long passwords
- Network tools detect internal scans and malicious activity, so you stop a hacker in their tracks





# Stage 5 Exfiltration and Backup Deletion

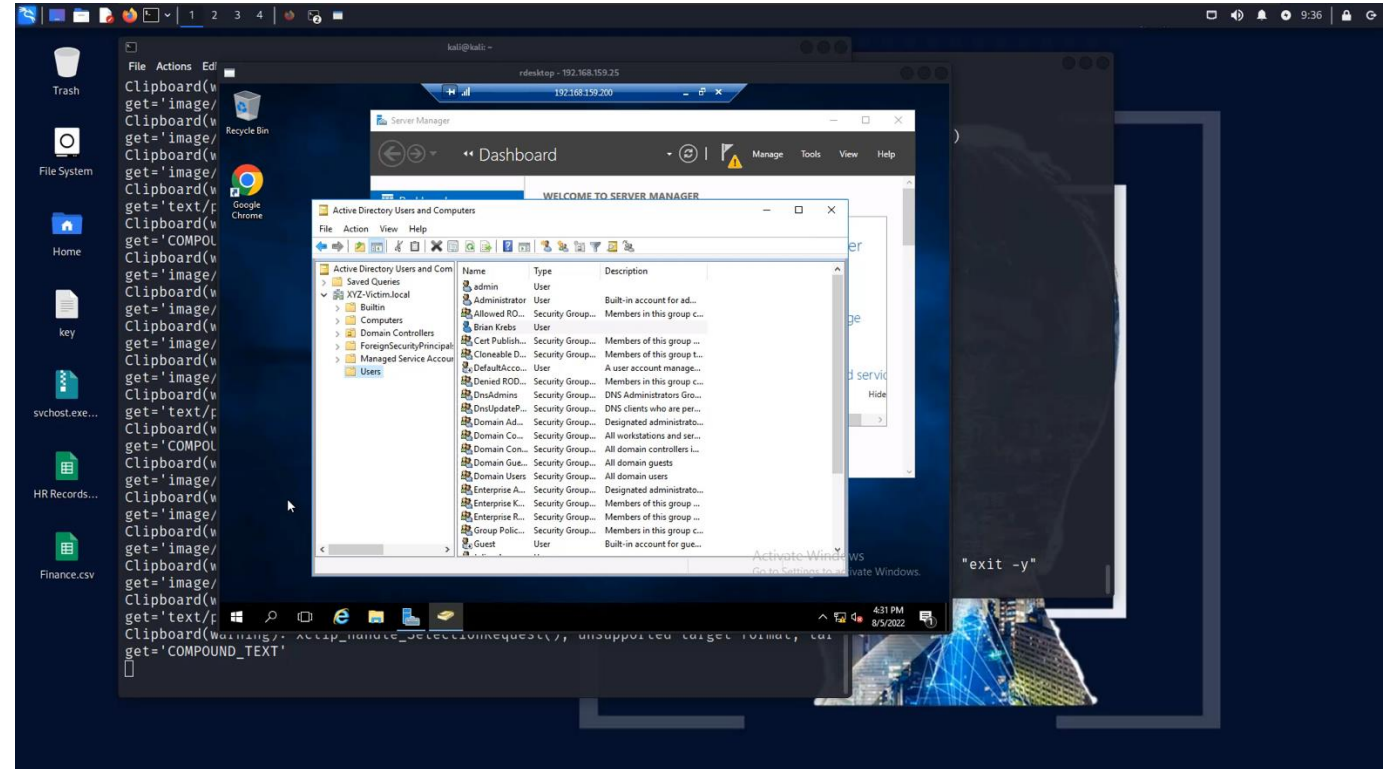
## Stealing Data

### Setting the Scene

- Threat actor will look for sensitive files and steal them
- Threat actor will then delete any backups they discover
- Data could be uploaded to the dark web or sold

### Takeaways

- Unauthorized access to personal information can trigger legal obligations (even if files weren't taken)
- Use a strong backup solution and test it often



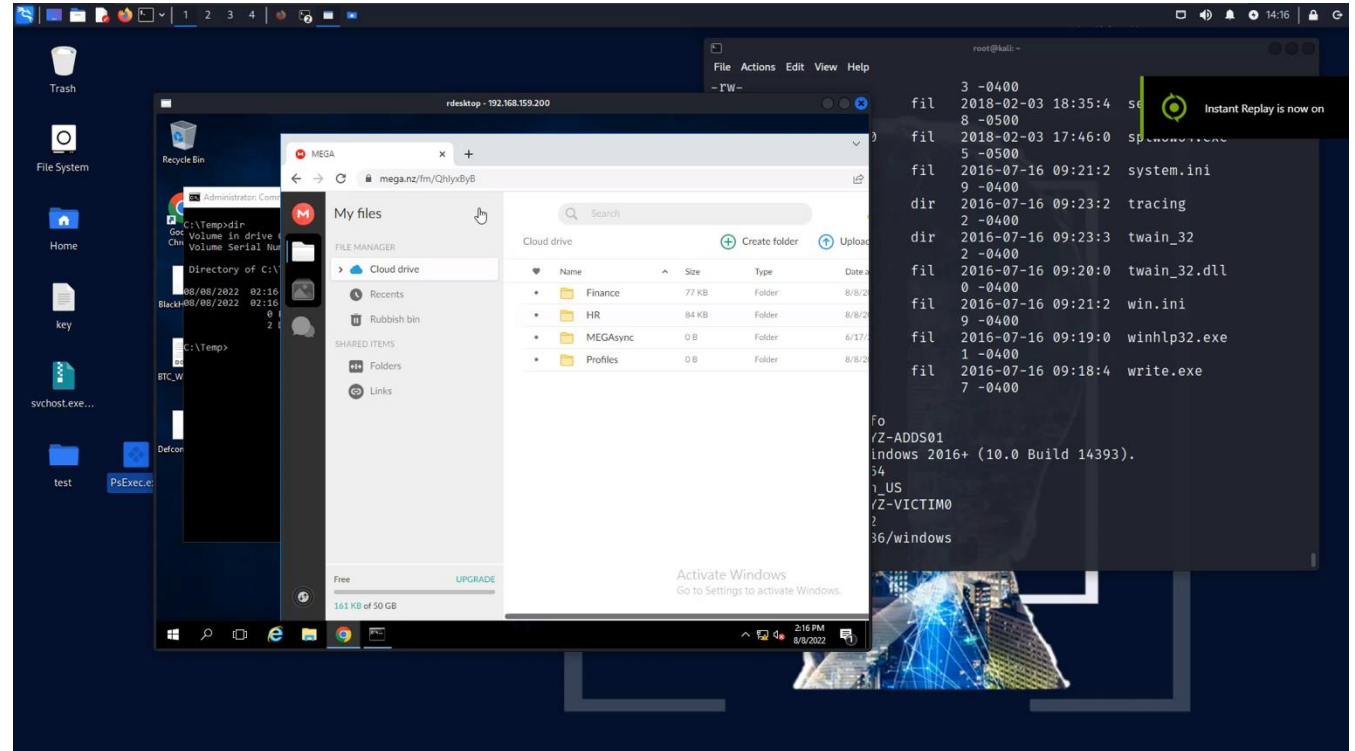
# Stage 6 Ransomware Execution

## Setting the Scene

- Threat actor executes the ransomware as quickly as possible on as many systems as possible
- This is often done on a Friday night or Thanksgiving morning

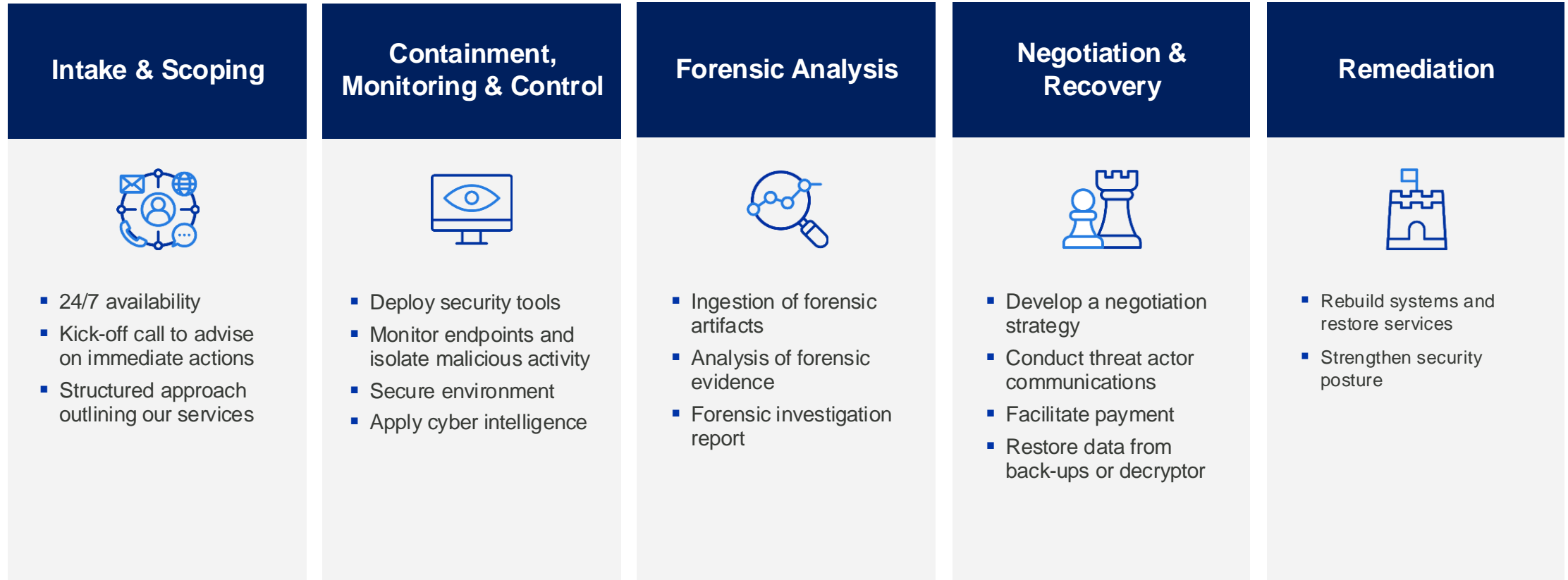
## Takeaways

- Disconnect, don't power off, encrypted systems to preserve evidence
- Have a plan for how you are going to access resources to help you through this





# Ransomware Response Framework



# Contact Us



**Billy Gouveia**

CEO

[billy@surefirecyber.com](mailto:billy@surefirecyber.com)

+1 301 938 1542

[response@surefirecyber.com](mailto:response@surefirecyber.com)

[1-800-270-9034](tel:1-800-270-9034)

This document (including any attachments) may contain privileged, confidential, or protected information intended only for the intended recipient. If you are not the intended recipient, any unauthorized review, use, disclosure, or distribution is prohibited. If you have received this document in error, you are required to notify the sender, then delete this document and any attachment from your computer and any of your electronic devices where the document is stored.



# 4:05 The CISO Playbook



**Andres Andreu**  
Deputy CISO  
Hearst



**Leo Casusol**  
Managing Director  
Forgepoint Capital

---

FIRESIDE



# The CISO Playbook

Now available online...and for one lucky guest per table, check under your chair!



**amazon** books

<https://www.amazon.com/CISO-Playbook-Security-Audit-Leadership/dp/1032762071>

**ROUTLEDGE**  
 **Routledge**  
Taylor & Francis Group

<https://www.routledge.com/The-CISO-Playbook/Andreu/p/book/9781032762074>





Automated security assurance  
and compliance operations



**Craig Unger**  
Founder & CEO  
Hyperproof

<https://hyperproof.io/>



**90%**  
increased visibility in risk  
and compliance posture

Sample Customers and Relationships



# Cybersecurity Risk is simply out of control



## Cannot meet increasing Regulatory Burden

95% of companies do not manage controls to mitigate risks due to high manual costs



## Rising Costs of Data Breaches

\$4.88M is the average cost of a data breach in 2024 and increasing annually.



## Ineffective Risk Management

56% of companies experience a breach due to a third party vulnerability



# The market has spoken and it requires: A Modern, Integrated Risk and Compliance platform



**Lower Costs**

**20%**

cost reduction with fewer redundancies and streamlined processes



**Greater Efficiency**

**40%**

improvement in operational efficiency due to automated workflows



**Smarter Decisions**

**60%**

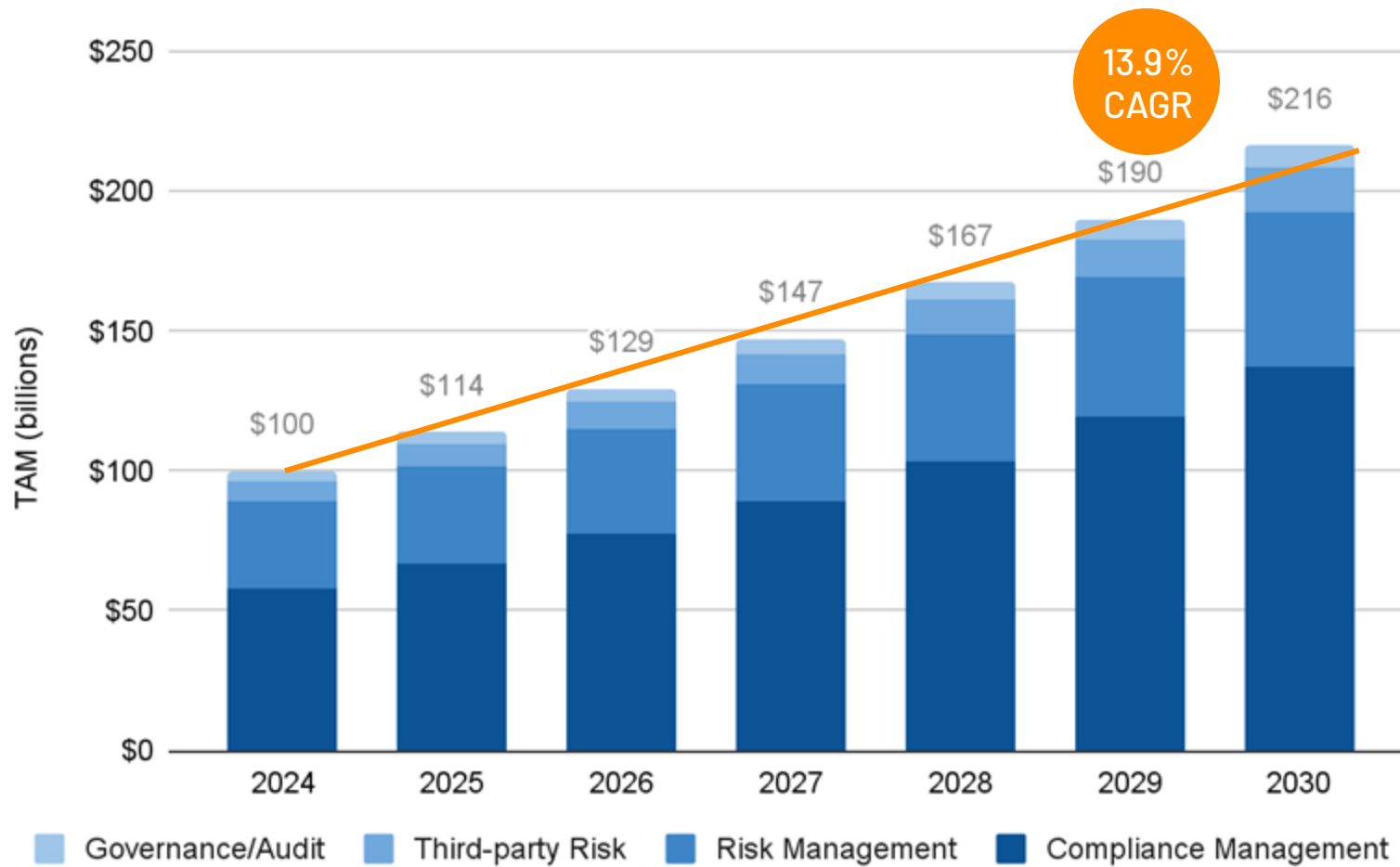
of companies reported improved decision-making unifying risk & compliance



**Better Compliance**

**30%**

fewer compliance failures compared to those using non-integrated systems



## A fast growing and evolving market ripe for disruption

Four high growth business critical markets converging into a single platform **\$216 billion**.

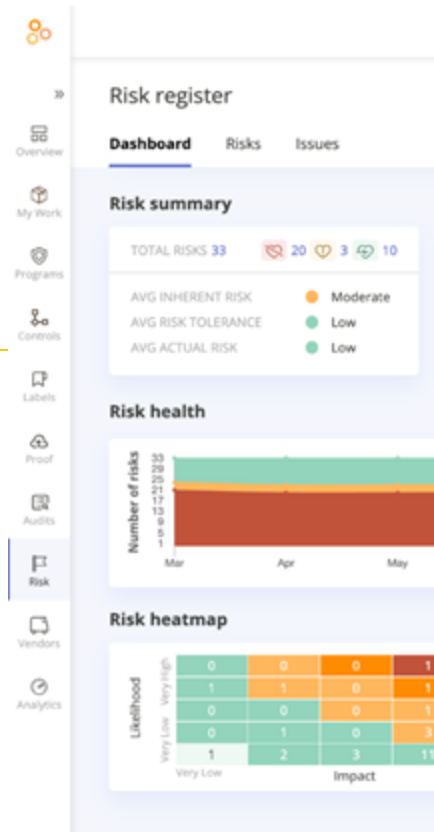
**13.9% CAGR** through 2028 according to Verified Market Research, Future Market Insights, and Databridge Market Research.

**Hyperproof** uniquely positioned to disrupt and capitalize on the convergence.

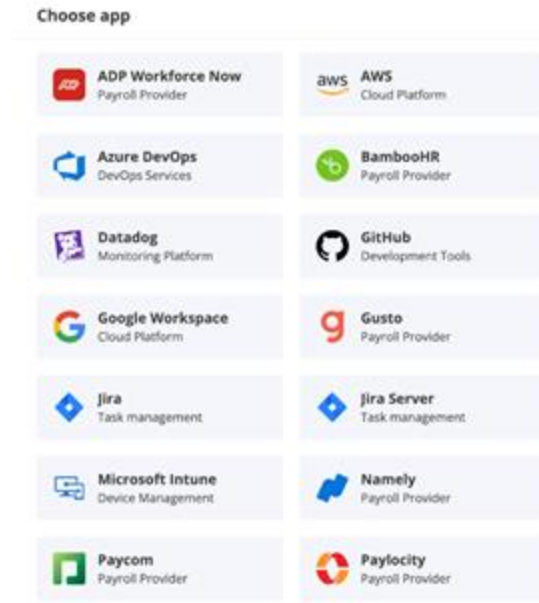


# Hyperproof is the innovator- Compliance Operations

## Real Time Risk



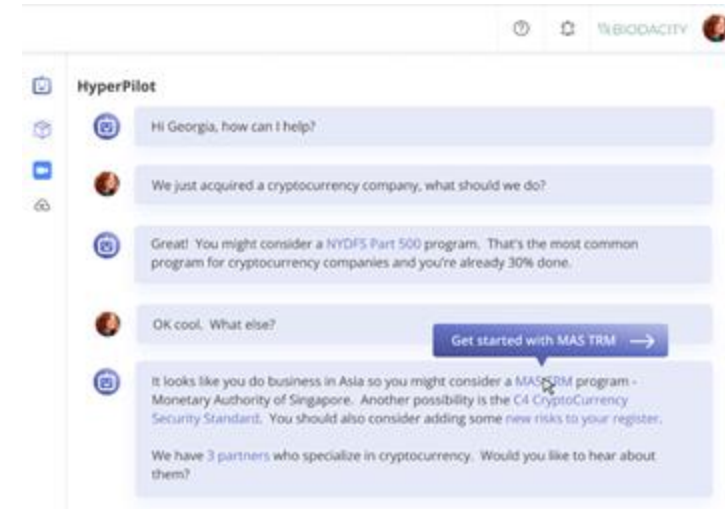
## HyperSyncs



## Golden Controls



## Hyperpilot



# Success across industries

## Manufacturing

stryker®

Rockwell Automation

TVH

ITT

Energizer

PAULO

## Services/Consulting

大成 DENTONS

IBDO

accenture

pwc

Grant Thornton

Wilhelmsen

## Finance/Banking

NOMURA

acorns

The Blackstone Group®

IBI Broadview  
Federal Credit Union

Openbank™

swyftx

## Healthcare/ Life Sciences

solventum

omada

ECRI

CareFirst

PRIMA  
HealthCredit

AKOYA  
BIOSCIENCES®  
THE SPATIAL BIOLOGY COMPANY™

## Transportation

Airbus TRANSIT

Breeze

Aviation group

allegiant

VOLKSWAGEN  
GROUP



# 4:33 The Innovator's Journey, from CTO to CEO



**Joe Levy**  
CEO  
Sophos



**Alberto Yépez**  
Co-Founder and Managing Director  
Forgepoint Capital

---

FIRE SIDE



An aerial photograph of the New York City skyline at dusk. The sky is a mix of deep blue and orange, with scattered clouds. The city's buildings are illuminated with warm yellow and white lights, creating a vibrant contrast against the darkening sky. The Freedom Tower stands prominently on the right side of the frame. In the background, the Hudson River and the George Washington Bridge are visible. The overall scene captures the energy and beauty of the city at twilight.

**Rooftop Reception!**  
***Please return by 6:30 PM***



An aerial view of the New York City skyline at dusk. The sky is a mix of deep blue and orange, with scattered clouds. The city is illuminated with warm yellow and white lights from the buildings. The Freedom Tower is the most prominent skyscraper on the right side of the image. In the background, the Hudson River and the George Washington Bridge are visible.

**Welcome to our Fall 2024  
Celebration Dinner**



# TIPS: Print Edition Coming Soon

<https://forgepointcap.com/tag/tips/>



TIPS #22: The IGA-IAM-UEBA Triad for Identity-First Security

Shane Shook November 13, 2024

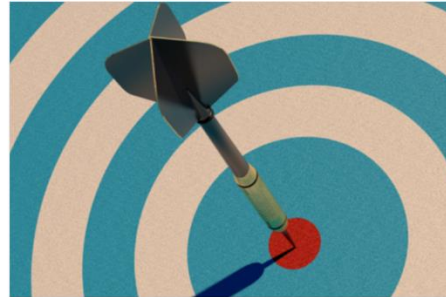
[BLOG POST](#) [TIPS](#)



TIPS #21: The Disinformation/Misinformation Dual Threat

Shane Shook October 28, 2024

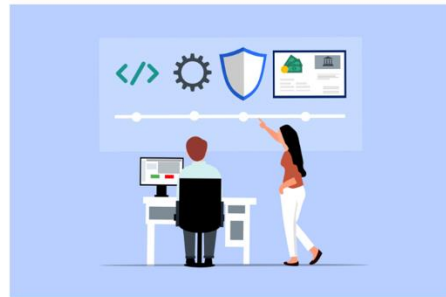
[BLOG POST](#) [TIPS](#)



TIPS #20: Building Resilience with Contingent Business Interruption (CBI) Insurance

Shane Shook September 26, 2024

[BLOG POST](#) [TIPS](#)



TIPS #19: Shift Left for Finance

Shane Shook August 26, 2024

[BLOG POST](#) [TIPS](#)



TIPS #18: How Secure in Operation Builds on Secure by Design

Shane Shook August 5, 2024

[BLOG POST](#) [TIPS](#)



TIPS #17: Subversion: The silent third dimension of cybercrime

Shane Shook June 25, 2024

[BLOG POST](#) [TIPS](#)



# Forgepoint Forward

New Quarterly Reports!



New reports on the most critical emerging spaces in cybersecurity, artificial intelligence, and infrastructure software.

Forgepoint Forward presents findings from extensive research and interviews with experts across our network- including our [Global Advisory Council](#).

Our goal is to highlight investment trends, M&A activity, and market projections as well as promising startups to identify key opportunities for entrepreneurs and technology leaders across the cybersecurity community.

First Four Topics:

- AI Governance
- Application Security Posture Management
- Security Log Data Management
- Enabling Applications at the Edge



**Reynaldo Kirton**  
Vice President







**F 100**

**Thank you, Global Advisory Council!**





## Elena Kvochko

Adjunct Professor  
Cornell SC Johnson School of  
Business

## Impact Award: Trailblazer

Elena Kvochko is a seasoned cybersecurity industry professional. In 2020, after holding cybersecurity leadership roles at several financial institutions, she was appointed the first Chief Trust Officer for the enterprise software giant SAP which operates in over 200 countries. There, she and her global team work to prevent and ward off cybersecurity threats while building trust with SAP customers, end users, partners and stakeholders.

Prior to working at SAP, Kvochko was a data security mastermind in the banking industry. She focused on global security as Senior Vice President and Technology Executive at Bank of America and Divisional Chief Information Officer at Barclays Bank in New York and London. Elena is also an inventor of 30+ patent-pending and patented technologies in security, privacy, digital payments technology, and quantum computing. One includes an information card silent coercion alarm that prompts an institution to review fraudulent activity on behalf of a customer. Her many accolades include being named among the Top 100 CIOs; Leading CIOs – Who Happen to be Female by the CIO Magazine, Business Role Model of the Year by the Women in IT Awards, and Fortune Magazine's Most Powerful Women – International."



**Aaron Hughes**  
Chief Information Security Officer  
Albertsons Companies

## Impact Award: Catalyst

Aaron Hughes is CISO at Albertsons Companies. In this role he is responsible for enabling the business and securing the infrastructure, digital assets, and payments for a network of over 2200 supermarkets operating under 20 brands across the United States serving 30 million customers per week and driving \$70B in annual revenue.

Previously, he was VP for Information Security and Deputy CISO at Capital One where he led the team providing security services across all Capital One lines of business. Aaron is also the former Deputy Assistant Secretary of Defense for Cyber Policy where, as the senior DoD cyber official, he was the primary interface with the broader USG, Congress, the public, and foreign governments for all defense related cyber policy matters. His office was responsible for overseeing the development and implementation of cyber policies, strategies, operations, and plans for the DoD.

Aaron is on the Board of Directors for SentinelOne (NYSE \$S) and is Vice Chairman of the Board of Directors for privately held Advanced Technology International (ATI), a leading provider of consortium services to the largest departments and agencies in the US Government. He is a Colonel in the United States Air Force Reserve currently serving as a Senior Advisor to the Commander USCYBERCOM. He received his BS in Mechanical Engineering from the University of Virginia, MS in Telecommunications and Computers from George Washington University, and MBA from the Stanford Graduate School of Business.





**Jerry Kowalski**

Chief Information Security Officer  
Jefferies

**Impact Award:  
All-star**

Jerry Kowalski is the Chief Information Security Officer at Jefferies LLC.

As CISO, he is responsible for designing, building and operating the cyber security program that enables Jefferies to run its core businesses securely.

At Jefferies, he heads Security Engineering, Operations Security, Access Identity Management and Application Security practices. Prior to this, Jerry was head of Application Security Risk for Barclays Capital and Wealth. During his 5-year tenure, Jerry built the Application Security practice that consisted of security assessments, architecture design, risk management and developer training.

Earlier in his career, Jerry was a Senior Security Engineer/Team Lead at Ernst & Young Advanced Security Center, and Computer Engineer Researcher at Air Force Research Laboratory where he provided R&D services to federal government and homeland security.

Jerry earned his BA in Computer Engineering and MS in Computer Security at Syracuse University.





**THANK YOU,  
CURRENT  
DEFENDERS**

**SEE YOU  
NEXT YEAR!**



**Thank you for  
joining us.**

**Let the  
conversations  
continue!**

- Agenda will be updated with Resources
- 5:00 Rooftop Reception on 22F
- 6:30 pm Celebration Dinner back here in the Ballroom



**FEEDBACK**

<https://forgepoint.typeform.com/acmd24/>



**STAY IN THE KNOW**

<https://forgepoint.typeform.com/acmd24/>





# Fall 2024 Advisory Council Dinner

19 November 2024 | The Yale Club of New York City

 Forgepoint