



RSAC | 2025
Conference
San Francisco • April 28 – May 1 • Moscone Center

Highlights & Insights

Video Interviews, News, Photos and More From the ISMG Team

RSAC Conference 2025: Many Voices. One Community.



New cyberthreats, emerging technologies, an uncertain economy and a changing regulatory environment. This year's RSAC Conference couldn't have come at a more pivotal time for the cybersecurity industry.

Over four days in San Francisco, RSAC Conference 2025 brought together thousands of cybersecurity professionals and industry leaders under the theme "Many Voices. One Community." While there are plenty of issues still keeping CISOs awake all day (they were already up all night), the RSAC community also brought a host of solutions to the event - from new ways to stay ahead of the cybercriminals using agentic artificial intelligence technology to deeper commitments to information sharing and collaboration. Once again, AI dominated the conversations, but this year we saw many examples of how security organizations are putting AI to work in areas such as identity security, security operations, cloud security and data protection.

Once again, we staffed two video studios at the conference, and we produced nearly 150 interviews. CEOs, CISOs, government leaders, investors, analysts and industry association representatives - they all were represented in our interviews and featured in this RSAC Compendium. Inside you'll find summaries of every interview by ISMG.Studio and links to the full reports on ISMG's media sites.

We brought our ISMG team from around the world to RSAC Conference 2025. Within these pages, you'll find insightful interviews by our seasoned editorial team and an in-depth view of the latest research, trends and thought leadership - all from the many voices of the RSAC community.

Enjoy,

Best,

A handwritten signature in black ink, appearing to read 'Tom Field', written in a cursive style.

Tom Field
SVP, Editorial
Information Security Media Group
tfield@ismg.io

Visit us online for more ISMG at RSAC coverage:

ismg.studio



Meet the ISMG Editorial Team



ISMG editorial team members Aseem Jakhar, Michael Novinson, Tom Field, Anna Delaney, Rahul Neel Mani and Mathew Schwartz

Over four days from April 28 to May 1, ISMG's team of editors interviewed more than 150 attendees at RSCA Conference. In this Editors' Panel at ISMG Studio in San Francisco, the team wraps up the news and trending topics at this year's event.

Meet the ISMG editorial team:

[WATCH ONLINE](#)



iSMG
Studio

See more at ismg.studio

Video Interviews

TABLE OF CONTENTS

CISO

Jason Clinton, <i>Anthropic</i>	8
Mandy Address, <i>Elastic</i>	8
Sean Atkinson, <i>Center for Internet Security</i>	9
Vaughn Hazen, Kenneth Townsend, Tiauna Ross	11
Tim Brown, <i>SolarWinds</i>	12
Stacey Cameron, <i>Halcyon</i>	13
Sameer Ratolikar, <i>HDFC Bank</i>	13
Ray Heffer, <i>Veeam</i>	13

GOVERNMENT OFFICIALS

Tanel Sepp, <i>Estonia</i>	14
Hans de Vries, <i>ENISA</i>	14
Herman Brown, <i>San Francisco District Attorney's Office</i>	16
Brett Leatherman, <i>FBI</i>	16
Matt Turek, <i>DARPA</i>	16
Craig Jones, <i>Interpol</i>	16
Cynthia Kaiser, <i>FBI</i>	17
Stacy Bostjanick, <i>U.S. Department of Defense</i>	18
Anne Neuberger, <i>White House</i>	20
Andre Luiz Bandeira Molina, <i>Institutional Security Office, Brazil</i>	22
Sanjay Virmani, <i>FBI, San Francisco</i>	22

ANALYSTS/ASSOCIATIONS

Jon France, <i>ISC2</i>	23
Kayle Giroud, <i>Global Cyber Alliance</i>	23
Lynn Dohm, <i>Women in CyberSecurity</i>	24

Jim Dempsey, <i>IAPP</i>	26
Lisa Plaggemier, <i>National Cybersecurity Alliance</i>	27
Brian Essex, <i>JPMorgan Chase & Co.</i>	27
Daniel Kennedy, <i>S&P Global Market Intelligence</i>	27
Ulla Coester, <i>Fresenius University of Applied Sciences</i>	27
Keith Weiss, <i>Morgan Stanley</i>	28
Jeff Pollard, <i>Forrester</i>	29
Avivah Litan, <i>Gartner</i>	30
Kelley Misata, <i>Sightline Security</i>	31

INVESTORS

Arik Kleinstein, <i>Gililot Capital Partners</i>	32
Sidra Ahmed Lefort, <i>Munich Re Ventures</i>	32
Dave DeWalt, <i>NightDragon</i>	33
Chenxi Wang, <i>Rain Capital</i>	34
Alex Doll, <i>Ten Eleven Ventures</i>	34
Rick Grinnell, <i>Glasswing Ventures</i>	34
Alberto Yépez, <i>Forgepoint Capital</i>	34
Bob Ackerman, <i>AllegisCyber Capital</i>	35
Art Coviello, <i>SYN Ventures</i>	36
Collin Gallagher, <i>Thoma Bravo</i>	38
Umesh Padval, <i>Thomvest Ventures</i>	39
Rama Sekhar, <i>Menlo Ventures</i>	39
Andy Ellis, <i>YL Ventures</i>	39
Kevin Mandia, <i>Ballistic Ventures</i>	39

TECHNOLOGY AND SERVICES EXPERTS

AI & MACHINE LEARNING

Peter McKay, <i>Snyk</i>	41
Dan Streetman, <i>Tanium</i>	41
Kara Sprague, <i>HackerOne</i>	43
Edna Conway, <i>EMC Advisors</i>	44
Lingping Gao, <i>NetBrain</i>	44
Sage Wohns, <i>Jericho Security</i>	44
Nikesh Arora, <i>Palo Alto Networks</i>	44
Richard Bird, <i>Singulr AI</i>	47
Jim Routh, <i>Saviynt</i>	47
Yotam Segev, <i>Cyera</i>	47
Jeetu Patel, <i>Cisco</i>	47
Liran Grinberg, <i>Team8</i>	49
Sam Curry, <i>Zscaler</i>	51
Danny Milrad, <i>Palo Alto Networks</i>	53
Sam Rubin, <i>Palo Alto Networks</i>	53
DJ Sampath, <i>Cisco</i>	53
Mohammed Aboul-Magd, <i>SandboxAQ</i>	53
Suja Viswesnan, <i>IBM</i>	55
Sandra Joyce, <i>Google Threat Intelligence</i>	58
Jay Chaudhry, <i>Zscaler</i>	58

TECHNOLOGY AND SERVICES EXPERTS

APPLICATION SECURITY

Ash Kulkarni, <i>Elastic</i>	59
Jeff Shiner, <i>IPassword</i>	59
Chris Wysopal, <i>Veracode</i>	61
Pieter Danhieux, <i>Secure Code Warrior</i>	62

TECHNOLOGY AND SERVICES EXPERTS

CLOUD SECURITY

Matt Cohen, <i>CyberArk</i>	63
John Hultquist, <i>Google Cloud</i>	63
Ami Luttwak, <i>Wiz</i>	65
Yogesh Badwe, <i>Druva</i>	65
Dean Fantham, <i>Edgile</i> , and PJ Hamlen, <i>AWS</i>	65
Phil Venables, <i>Google</i>	65
PJ Hamlen, <i>AWS</i> , and Julie Bernard, <i>Deloitte & Touche</i>	66
Narayan Sundar, <i>Palo Alto Networks</i> , and Pritish Sinha, <i>Google Cloud</i>	67

TECHNOLOGY AND SERVICES EXPERTS

DATA SECURITY & PRIVACY

Mickey Bresman, <i>Semperis</i>	69
Michelle Dennedy, <i>Abaxx Technologies</i>	69
Dean Sysman, <i>Axonius</i>	71
Dimitri Sirota, <i>BigID</i>	71
Robin Das, <i>DataBee a Comcast Company</i>	71
Kabir Barday, <i>OneTrust</i>	71
Sebastien Cano, <i>Thales</i>	72
Jim O'Boyle, <i>Varonis</i> , and Adam McGill, <i>Concentrix</i>	72

TECHNOLOGY AND SERVICES EXPERTS

ENDPOINT SECURITY & EMAIL SECURITY

Joshua Motta, <i>Coalition</i>	73
Bradon Rogers, <i>Island</i>	73
Ofar Ben-Noon, <i>Palo Alto Networks</i> , and Jamie Fitz-Gerald, <i>Okta</i>	75
Ofar Ben-Noon, <i>Palo Alto Networks</i>	77
Adam Meyers, <i>CrowdStrike</i>	77

Video Interviews

TABLE OF CONTENTS

TECHNOLOGY AND SERVICES EXPERTS

IDENTITY SECURITY

Rohit Ghai, <i>RSA</i>	78
Sumit Dhawan, <i>Proofpoint</i>	78
Dave Merkel, <i>Expel</i>	81
Alex Weinert, <i>Semperis</i>	82
Mike Towers, <i>Veza</i>	82
Arvind Nithrakashyap, <i>Rubrik</i>	82
Nadir Izrael, <i>Armis</i>	82
Mark McClain, <i>SailPoint</i>	84

TECHNOLOGY AND SERVICES EXPERTS

OT/IOT SECURITY

Ian Tien, <i>Mattermost</i>	85
Rajesh Khazanchi, <i>ColorTokens</i>	85
Shivkumar Pandey, <i>Adani Group</i> , & Burgess Cooper, <i>Adani Enterprises</i>	87
Darron Antill, <i>Device Authority</i>	87
Anup Savla, <i>Sasken Silicon</i>	87
Robert Lee, <i>Dragos</i>	87
Harry Coker, <i>Maryland</i> <i>Department of Commerce</i>	89
Helena Huang, Gil Baram & Derek Manky.....	90
Phillip Wylie, <i>Phosphorus Cybersecurity</i>	90
Rafael Narezzi, <i>Cyber Energia</i>	90
Stefano Zanero, <i>Politecnico di Milano</i>	90
Colin Soutar, <i>Deloitte</i> , and Eric Trexler, <i>Palo Alto Networks</i>	91
Travis Rosiek, <i>Rubrik</i>	92

TECHNOLOGY AND SERVICES EXPERTS

SECURITY OPERATIONS

Kelly Ahuja, <i>Versa Networks</i>	93
--	----

Todd Nightingale, <i>Fastly</i>	93
Dmitri Alperovitch, <i>Silverado</i>	94
Ken Huang, <i>DistributedApps.ai</i>	94
Joe Carson, <i>Segura</i>	94
Manoj Srivastava, <i>Blackpoint Cyber</i>	94
Kevin Simzer, <i>Trend Micro</i>	95
Andrew Rubin, <i>Illumio</i>	96
Marty Momdjian, <i>Ready1</i>	96
Mike Nichols, <i>Elastic</i> , and Matt Muller, <i>Tines</i> ...96	
Tamar Bar-Ilan, <i>Cyera</i> , and Sheetal Venkatesh, <i>Cohesity</i>	96
Seemant Sehgal, <i>BreachLock</i>	97
Brad Arkin, <i>Salesforce</i>	98
Jon Baker, <i>Mitre</i>	98
Jeff Crume, <i>IBM</i>	98
Dale Zabriskie, <i>Cohesity</i> , and Paul Zimmerman, <i>BCSD</i>	98
John Pirc, <i>NetWitness</i>	99

TECHNOLOGY AND SERVICES EXPERTS

RISK MANAGEMENT

Jon DiMaggio, <i>Analyst1</i>	100
Derek Manky, <i>Fortinet</i>	100
Perry Carpenter, <i>KnowBe4</i>	102
Chris Novak, <i>Verizon Business</i>	103
Matt Kunkel, <i>LogicGate</i>	104
Hany Farid, <i>GetReal</i>	104
Andres Andreu, <i>Constella</i>	104
Kevin Gosschalk, <i>Arkose Labs</i>	104
John Kindervag, <i>Illumio</i>	105
Niloofer Razi, <i>Capitol Meridian Partners</i>	106

Video Interviews

TABLE OF CONTENTS

Aly Shivji, <i>Splunk</i> , and Bruce Johnson, <i>TekStream</i>	107
John Fokker, <i>Trellix</i>	107
Wade Baker, <i>Cyentia Institute</i>	107
John Barker, <i>CISO Law Firm</i>	107
Ronald Raether, <i>Troutman Pepper Locke</i> , and Jon Olson, <i>Blackbaud</i>	108
Christopher Seusing, <i>Wood Smith Henning & Berman</i> , and Peter Hedberg, <i>Corvus</i>	109
James Lee, <i>ITRC</i>	109
Sumedh Thakar, <i>Qualys</i>	109
Allan Liska, <i>Recorded Future</i>	109
Christiaan Beek, <i>Rapid7</i>	111
Martin Zugec, <i>Bitdefender</i>	112
Alexander Leslie, <i>Recorded Future</i>	112
Tod Beardsley, <i>runZero</i>	112
Anupam Upadhyaya, <i>Palo Alto Networks</i> , and Arnab Bose, <i>Okta</i>	113

BEHIND THE SCENES

ISMG at RSAC 2025	114
-------------------------	-----

CISO

Ransomware threats, deepfake phishing, multi-cloud environments, the AI explosion and the specter of personal legal liability for mishandling a data breach. CISOs face complex challenges in communicating risk to DevOps teams as well as the board of directors. We spoke with leading CISOs across multiple industries about how they're leading through these tumultuous times, and what technologies they're looking toward to secure the enterprise and respond to incidents.

Rethinking Cybersecurity With AI Agents

Anthropic's **Jason Clinton** Discusses the Benefits and Challenges of AI Agents



AI agents will be crucial in the software development life cycle to eliminate bugs, improving the quality of software, which could significantly reduce security vulnerabilities. Although managing AI agents for identity and access controls will be hard, said Jason Clinton, CISO at Anthropic.

[WATCH ONLINE](#)

Use of Agentic AI in Cybersecurity Needs More Transparency

Elastic CISO **Mandy Andress** on Deploying More AI Agents for Cybersecurity Tasks



Agentic AI has introduced significant changes in cybersecurity operations in terms of efficiency and speed. Mandy Andress, CISO at Elastic, discussed why more needs to be done to trust AI agents to perform cybersecurity tasks and how to enhance transparency in AI decision-making.

[WATCH ONLINE](#)

A man with short brown hair, wearing a light-colored sweater over a checkered shirt, is seated at a glass table. He is gesturing with his hands while speaking. A woman with long brown hair, wearing a black top, is seated across from him, holding a tablet. The background is a large window showing a city skyline with a prominent skyscraper.

Sean Atkinson

CISO, Center for Internet Security

Bridging Cyber and Physical Threats

CISO **Sean Atkinson** on Proactive, Integrated Approach to Hybrid Threat Defense

Center for Internet Security CISO Sean Atkinson calls for integrated threat intelligence, stronger community collaboration, and enhanced playbooks to confront rising hybrid threats that exploit gaps across cybersecurity and physical domains.

In this video interview with Information Security Media Group at RSAC Conference 2025 Atkinson also discussed:

- The need for integrated cyber-physical threat detection and prevention;
- The importance of community building, free tools and low-cost resources for defense;
- Enhancing tabletop exercises to simulate complex hybrid attacks.

[WATCH ONLINE](#)

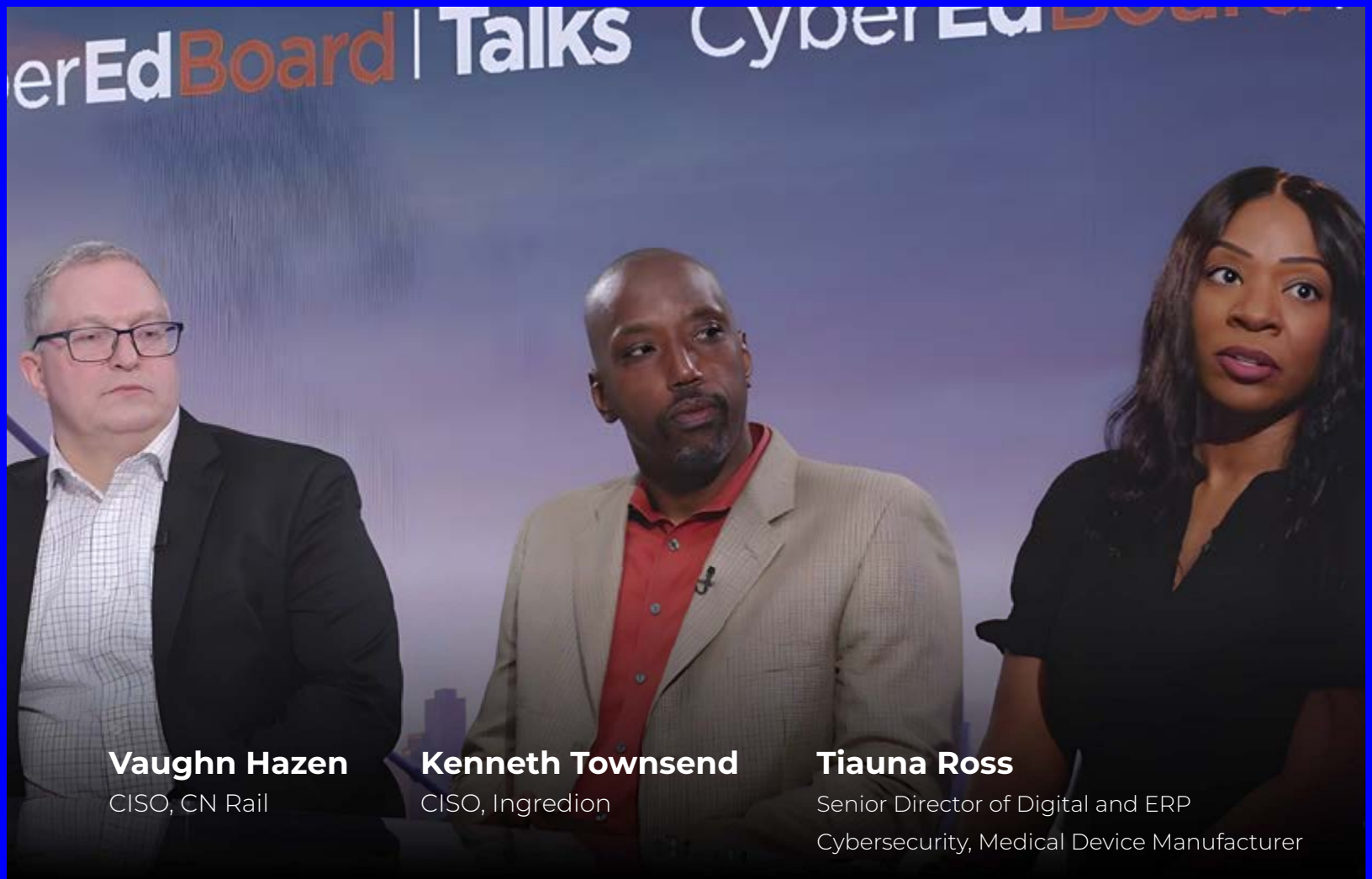
“We should be using that in exactly the same way, in terms of information threat awareness and information sharing.”

- **Sean Atkinson**



“As defenders, we need to be thinking about what we can do to adopt models on the defensive side to help protect our networks and help protect our systems.”

Jason Clinton
CISO, Anthropic



Vaughn Hazen

CISO, CN Rail

Kenneth Townsend

CISO, Ingredion

Tiauna Ross

Senior Director of Digital and ERP
Cybersecurity, Medical Device Manufacturer

CyberEdBoard | Talks: Tailored Strategies for OT Security

Panelists Call for Real-Time Data Integration, Better IT-OT Collaboration

OT systems are inherently complex, purpose-built and often don't require many changes - if any. Unlike traditional IT, these cyber environments have their own set of unique requirements that vary by industry ranging from manufacturing to healthcare, according to members of a CyberEdBoard panel.

In this video interview with Information Security Media Group at RSAC Conference 2025, the panel also discussed:

- The growing need for real-time data integration;
- Regulatory issues and OT security challenges;
- The need for a collaborative approach to building secure OT environments.

WATCH ONLINE

CyberEdBoard | Member

“When you put in the firewalls, the network security controls, you may limit something that somebody forgot to mention that they're dependent on for the communication flow, and then all of a sudden, stuff stops working. You really have to be careful when you touch OT environments.”

- Vaughn Hazen



Tim Brown

CISO, SolarWinds

Inside the Relentless Liability Pressures Facing CISOs

SolarWinds CISO **Tim Brown's** Case Shows Personal, Legal and Health Risks for CISOs

CISOs face tremendous stress in dealing with regulatory scrutiny and legal exposure in the wake of a data breach. SolarWinds CISO Tim Brown shares the personal and professional impact of Securities and Exchange Commission charges against him after the 2020 SolarWinds supply chain attack.

In this video interview with Information Security Media Group at RSAC Conference 2025, Brown also discussed:

- Cyber Sarbanes-Oxley - a legal framework that establishes clear processes and accountabilities in cybersecurity;
- The importance of organizational support during crisis;
- The role of company culture and formal agreements in supporting CISOs..

“The month after the incident, I lost about 25 or 30 pounds. I don't recommend that as a diet program.”

- *Tim Brown*

[WATCH ONLINE](#)

The State of Ransomware and Data Extortion

Stacey Cameron, CISO of Halcyon, on Latest Cybercrime Trends



While a few ransomware groups have disbanded in the face of law enforcement takedowns, proposed bans on ransom payments and other developments, there's still money to be made by cybercriminals, who continue to evolve their attacks, said Stacey Cameron, CISO at Halcyon.

[WATCH ONLINE](#)

AI Bots Take Over Cybersecurity at HDFC Bank

HDFC Bank's **Sameer Ratollikar** on the Automation Shift in Security



HDFC Bank's CISO Sameer Ratollikar shares the bank's vision of becoming an AI-first institution, emphasizing architectural simplicity, agentic AI for threat detection and balancing automation with human expertise to enhance cybersecurity and customer experience.

[WATCH ONLINE](#)

How Generative AI Enables Solo Cybercriminals

Ray Heffer, Field CISO of Veeam, on the AI Threats Posed by 'Lone Wolves'



While artificial intelligence is a "double edged sword" for both enhancing security and enabling cybercriminals, the defenders are thankfully currently "ahead of the game," said Ray Heffer, field CISO of Veeam. But there's the worrisome threat that the advantage could shift the other way, he said.

[WATCH ONLINE](#)

GOVERNMENT OFFICIALS

Government agencies are on the front lines of the war between threat actors and society, but this year a new administration, budget cuts and new priorities are raising concerns about cybersecurity and privacy at a time when nation-state adversaries are on the offensive. We interviewed some of the leading minds in government about their efforts to disrupt cybercriminals, protect critical infrastructure and expand public-private partnerships.

AI Trust Is the New Cyber Currency

Estonia's Cyber Diplomat **Tanel Sepp** Urges Trust-First AI Strategy



Estonia's Ambassador at Large for Cyber Diplomacy Tanel Sepp emphasizes the need for global cooperation and trust in AI adoption in digital economies. He discusses Estonia's whole-of-society model, the importance of regional partnerships and why digital sovereignty still lacks clear definition.

[WATCH ONLINE](#)

EU Confronts Rising Cyberthreats With Joint Resilience Push

ENISA's **Hans de Vries** Addresses Cyberthreat Interdependencies in European Security



European nations face increasing risk from rapidly evolving threats, especially within interconnected supply chains. The region still lags behind in ensuring overall resilience against these threats, said Hans de Vries, chief cybersecurity and operations officer at ENISA.

[WATCH ONLINE](#)



“You need to fight like you train, train like you fight. You have to make sure you know each other and what's really happening.”

Hans de Vries

Chief Cybersecurity and Operations Officer, ENISA

Inside the San Francisco District Attorney's Digital Journey

Herman Brown, CIO at the DA's Office, on Balancing Access, Security and Privacy



The court system has historically relied on manual, paper-based processes, but prosecutors in San Francisco are now embracing digital change. The District Attorney's Office is modernizing its systems without compromising core legal functions or public trust, said Herman Brown, CIO at the DA's office.

[WATCH ONLINE](#)

Nation-State Hackers Embed Stealthily in US Infrastructure

FBI's **Brett Leatherman** Urges Private-Sector Collaboration to Detect Stealthy Threats



State-backed cybercriminals use stealth and persistence to infiltrate U.S. infrastructure. Brett Leatherman, deputy assistant director of cyber operations at the FBI, shares how early collaboration with private firms is key to identifying and containing advanced cyberthreats.

[WATCH ONLINE](#)

DARPA Doubles Down on Cybersecurity with AI-Powered Initiatives

DARPA's **Matt Turek** on Using AI to 'Find and Fix' Software Vulnerabilities



As nation-state cyberthreats continue to intensify, the Defense Advanced Research Projects Agency is ramping up efforts to help protect U.S. critical infrastructure using artificial intelligence technology, said Matt Turek, deputy director for the Information Innovation Office at DARPA.

[WATCH ONLINE](#)

Cybercrime Cooperation Has Become More Regional

Ex-Interpol Director **Craig Jones** on How Geopolitics Affects Global Cybercrime



Geopolitical conflicts have affected intergovernmental cooperation. Craig Jones, immediate past director of cybercrime at Interpol, says geopolitical instability has pushed countries to shift their focus toward data sovereignty, scrutinizing data storage, access and regulations.

[WATCH ONLINE](#)



Cynthia Kaiser

Deputy Assistant Director, FBI

Criminals Are Using AI to Put a New Face on Old Schemes

FBI's **Cynthia Kaiser** on How AI Is Helping to Evolve Cyberthreats

Artificial intelligence is changing the way people work, including cybercriminals and fraudsters. But instead of introducing new types of cybercrime, AI has enhanced existing criminal activities, said Cynthia Kaiser, deputy assistant director at the FBI.

In this video interview with Information Security Media Group at RSAC Conference 2025, Kaiser also discussed:

- The legal complexities involved in tackling AI-driven cyberattacks;
- The legal landscape, which is complex and requires nuanced thinking to navigate, especially when dealing with AI-generated content;
- How international cooperation plays a crucial role in countering AI-driven cyberthreats.

WATCH ONLINE

“Malicious actors are leveraging AI to enhance their efficiency in cyberattacks, from creating fake profiles at scale to refining deception tactics and evading detection more effectively.”

- **Cynthia Kaiser**



Stacy Bostjanick

Deputy Chief Information Officer, U.S. Department of Defense

Defense Industrial Base Strengthens Cybersecurity With CMMC

DOD's **Stacy Bostjanick** Shares Cyber Strategies for Enhancing Cyber Resilience

Stacy Bostjanick, deputy CIO and chief of Defense Industrial Base Cybersecurity at the Department of Defense, shared a robust plan to protect the DIB from relentless cyberattacks through stronger standards and proactive cyber strategies.

In this video interview with Information Security Media Group at RSAC Conference 2025, Bostjanick also discussed:

- Aligning closely with NIST to foster robust, industry-led security practices;
- Enhancing continuous monitoring for real-time threat protection;
- Building a future-ready DIB through zero trust architecture and advanced cyber defenses.

“My A-team worked their rear ends off for the last year to get us there.”

- **Stacy Bostjanick**

[WATCH ONLINE](#)



“For the development of AI here, we're primarily focused on, 'How do we use some of the latest advances in AI to find and fix vulnerabilities in software at speed and scale?’”

Matt Turek

Deputy Director, Information Innovation Office, DARPA

A portrait of Anne Neuberger, a woman with long dark hair, smiling and wearing a black leather jacket and a cloud-shaped earring. The background is a blurred blue and purple stage setting.

Anne Neuberger

Former Deputy National Security Director, Cyber and Emerging Technologies, White House

AI and Infrastructure Resilience Are Keys to US Security

Ex-Deputy NSA **Anne Neuberger** on Preparing for AI-Driven Threats

Anne Neuberger, former deputy national security advisor for cyber and emerging technologies, White House, outlines the urgent need for resilient critical infrastructure, strategic AI use in cybersecurity, and enhanced federal-state coordination to protect against evolving cyberthreats.

“AI has advantages on both offense and defense.”

- **Anne Neuberger**

In this video interview with Information Security Media Group at RSAC Conference 2025, Neuberger discussed:

- Why cyber resilience must focus on infrastructure that serves large populations;
- AI's role in both detecting threats and automating defenses;
- Why states must collaborate to protect local assets.

[WATCH ONLINE](#)



“In the past few years, the FBI, working with our partners, have had a number of successes, operations and disruptions. The LockBit one was a perfect example of that with the FBI working with nine other countries to go after the main actors.

Sanjay Virmani

Special Agent in Charge, FBI, San Francisco

Brazil's Cyber Push: AI Strategy, Regulatory Oversight

Security Office's **Andre Molina** on Building a Resilient, AI-Enhanced Cyber Future



Brazil is modernizing its cybersecurity infrastructure, placing AI at the heart of its strategy. Andre Luiz Bandeira Molina, secretary of information and cybersecurity at the Institutional Security Office of Brazil, outlined AI capabilities, regulatory policies and public-private partnerships.

[WATCH ONLINE](#)

Private-Public Partnership Vital for Fighting Cybercrime

FBI's **Sanjay Virmani** Discusses Recent FBI Takedowns



Developing strong relationships with private sector and international partner organizations is vital for tackling cybercrime. A proactive approach ensures more efficient incident responses, said Sanjay Vermani, the special agent in charge of the FBI in San Francisco.

[WATCH ONLINE](#)



ANALYSTS/ASSOCIATIONS

While hundreds of companies offer a variety of tools and services, a community of analysts and associations provides research, advice and training to help security leaders make the right decisions and prepare for the future. We spoke to a variety of analysts and association representatives about the current state of cybersecurity technology and the best bets for the future.

Prepare to Start Implementing Quantum-Safe Algorithms

ISC2 CISO **Jon France** on Why Quantum Resilience Falls Squarely Under the CISO



Quantum computing is at a tipping point, moving from theoretical math to deployable physics, said Jon France, CISO at ISC2. So, security teams need to start addressing the implementation of quantum-safe algorithms now, beginning with the five new safe algorithms released by NIST.

[WATCH ONLINE](#)

Building Cyber Resilience Through Equitable Funding

Global Cyber Alliance's **Kayle Giroud** on Common Good Cyber Initiative



The Global Cyber Alliance's initiative aims to secure vital but underfunded cyber infrastructure by mapping nonprofit efforts, providing shared resources and launching a sustainable funding model. "We want to ensure that the infrastructure is resilient so everyone has equitable access," said Global Cyber Alliance's Kayle Giroud.

[WATCH ONLINE](#)

A portrait of Lynn Dohm, a woman with short brown hair and black-rimmed glasses, wearing a light blue blazer. She is speaking and looking slightly to the right. A small microphone is clipped to her blazer.

Lynn Dohm

Executive Director, Women in CyberSecurity

Breaking the Glass Ceiling in Cybersecurity Careers

WiCyS Director **Lynn Dohm** on Key Strategies for Women's Career Advancement

WiCyS research identifies a critical advancement barrier for women in cybersecurity six to 10 years into their career. The organization helps mid-career professionals build essential leadership skills for senior positions, said Lynn Dohm, executive director at Women in Cybersecurity.

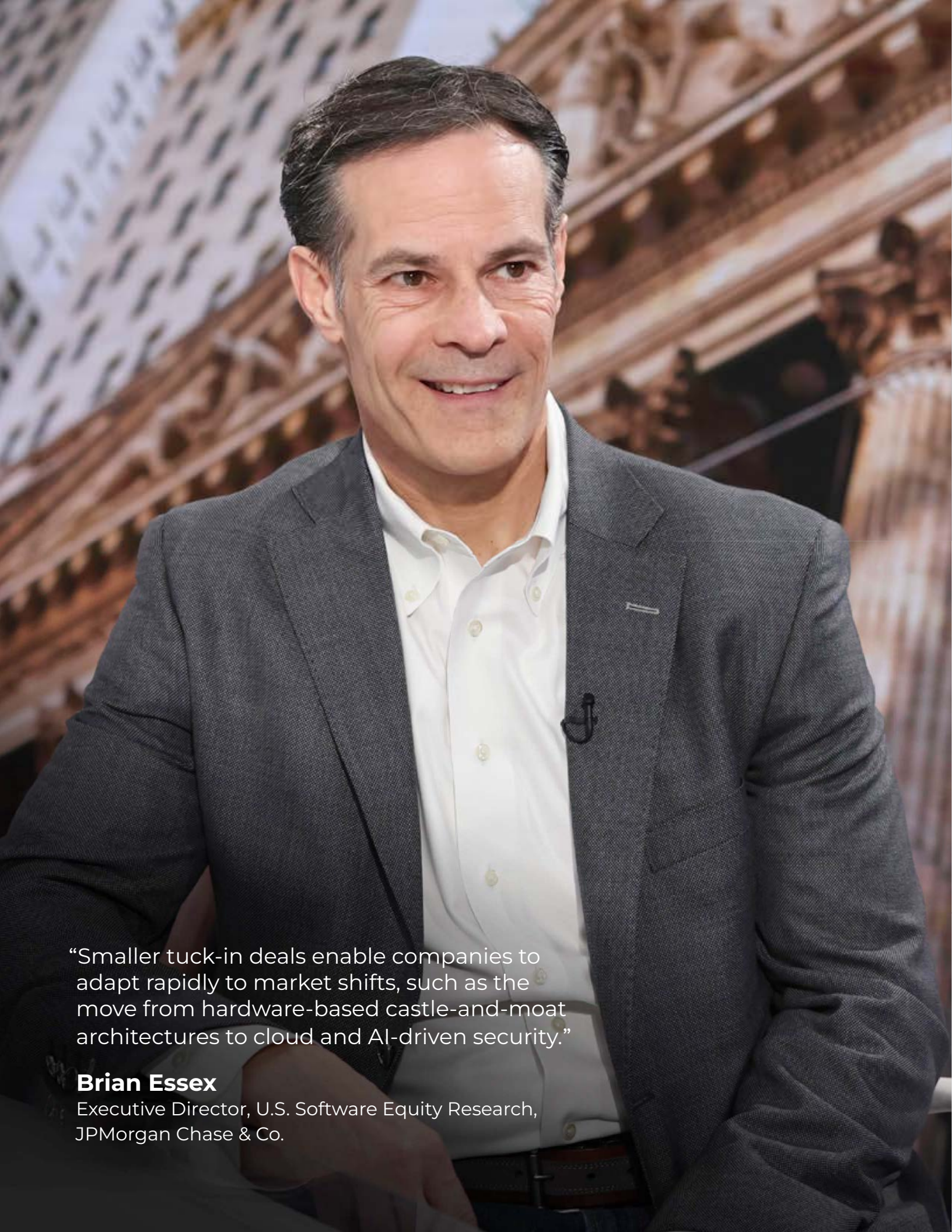
In this video interview with Information Security Media Group at RSAC Conference 2025, Dohm also discussed:

- Building cohort-based mentoring programs that benefit both parties;
- Bridging cybersecurity and artificial intelligence knowledge through specialized learning series;
- Preparing for the 2030 retirement wave of technical baby boomers.

WATCH ONLINE

“We went to our senior professionals of all our industry partners that support us, and said, ‘What got you from mid-career into that senior position?’”


- Lynn Dohm



“Smaller tuck-in deals enable companies to adapt rapidly to market shifts, such as the move from hardware-based castle-and-moat architectures to cloud and AI-driven security.”

Brian Essex

Executive Director, U.S. Software Equity Research,
JPMorgan Chase & Co.

A portrait of Jim Dempsey, a man with grey hair and glasses, wearing a dark suit jacket over a light-colored shirt. He is looking directly at the camera with a slight smile. The background is a blurred cityscape at night with various buildings and a blue sky with some clouds.

Jim Dempsey

Managing Director, Cybersecurity Law Center, IAPP

SEC Rule Elevates Cybersecurity to the Boardroom

IAPP's **Jim Dempsey** on How CISOs Can Stay Protected and Transparent

The SEC's cybersecurity disclosure rule didn't add new requirements but forced companies to confront security transparency. "It made it clear that this was a board-level matter ... cybersecurity has long been a board issue," said Jim Dempsey, managing director of the Cybersecurity Law Center at IAPP.

In this video interview with Information Security Media Group at RSAC Conference 2025, Dempsey also discussed:

- How EU laws such as NIS2 and the Cybersecurity Resilience Act affect global product readiness;
- California's proposed audit rule defining "reasonable" cybersecurity standards;
- IAPP's goal to foster collaboration among legal, cybersecurity and policy stakeholders.

"I think there was way too much confusion around the rule. I think some of that's settling down now."

- **Jim Dempsey**

WATCH ONLINE

Cybersecurity Nonprofits Pivot Toward Private Funding

National Cybersecurity Alliance's **Lisa Plaggemier** on Replacing Shrinking Public Funds



Lisa Plaggemier, executive director of the National Cybersecurity Alliance, urges nonprofits to embrace private-sector partnerships and creative outreach to protect vulnerable groups such as senior citizens as federal funding support wanes.

WATCH ONLINE

Cybersecurity M&A: Why Small Deals Are the New Big Play

J.P. Morgan Equity Research Analyst **Brian Essex** on M&A, IPOs and Security Spending



Cybersecurity deal-making is evolving. J.P. Morgan's Brian Essex breaks down why small, strategic acquisitions and not blockbuster buys are driving innovation, scalability and investor confidence in today's cloud-first, artificial intelligence-ready market.

WATCH ONLINE

AI Delivers AppSec Gains, but Ransomware Overconfidence Persists

Daniel Kennedy on Gen AI, Code Remediation and Misplaced Faith in Endpoint Tools



Cybersecurity leaders are embracing generative AI for its practical value in security operations and application security. But as ransomware tactics evolve, S&P's Daniel Kennedy warns that overconfidence in tools and assumptions about attack outcomes could leave teams exposed.

WATCH ONLINE

Restoring Trust in AI Through Governance

Ulla Coester on Ethical Design and the Role of the EU AI Act



Unclear threats and unpredictable behavior complicate global trust in AI. Building a shared understanding through adaptable governance helps create consistent expectations for responsible development across societies, said Ulla Coester, project director, Fresenius University of Applied Sciences.

WATCH ONLINE

A portrait of Keith Weiss, a man with a beard and dark hair, wearing a dark suit jacket over a light blue shirt. He is looking slightly to the right with a serious expression.

Keith Weiss

Head of U.S. Software Research, Morgan Stanley

Platform Shift: Why CISOs Are Embracing Consolidation

Morgan Stanley's **Keith Weiss** on Economic Pressure Impact on Security Budgets

Tight budgets and data challenges are driving enterprises away from best-of-breed security solutions toward more consolidated platforms. Consolidation offers streamlined security and better data visibility and integration, said Keith Weiss, head of U.S. software research at Morgan Stanley.

In this video interview with Information Security Media Group at RSAC Conference 2025, Weiss also discussed:

- How concerns over data sovereignty could shift global cybersecurity spending;
- How the adoption of artificial intelligence and large language models is expanding the attack surface;
- The emerging risks and rewards of agentic AI in security operations.

WATCH ONLINE

“When you get this more consolidated buying from your end customer, your retention rates go up. The customers become stickier. They stick with you longer, and they're going to buy more solution over time.”

- **Keith Weiss**

A man with glasses and a blue blazer is speaking, gesturing with his hands. The background is a blurred conference setting with orange and blue structures.

Jeff Pollard

Vice President and Principal Analyst, Forrester

Bracing for Volatility in an Unpredictable Threat Landscape

Forrester's **Jeff Pollard** Shares Security Strategies for Driving Cyber Resilience

Volatility in business environments compels security leaders to adopt flexible security approaches. Jeff Pollard, vice president and principal analyst at Forrester, outlines security strategies, including scenario planning and budget protection, to drive cyber resilience amid budget cuts.

In this video interview with Information Security Media Group at RSAC Conference 2025, Pollard also discussed:

- How security leaders can optimize spending without losing capabilities;
- Using flexible licensing agreements to save costs and avoid vendor sprawl;
- How proactive communication after major breaches builds leadership credibility.

[WATCH ONLINE](#)

“As a security leader, this is a trying time to figure out how you're going to bounce between scenarios where you could look at cutting your team or where you may need to look at growing your team.”

- **Jeff Pollard**

A portrait of Avivah Litan, a woman with shoulder-length brown hair and bangs, wearing a dark blazer over a patterned top and large hoop earrings. She is smiling slightly. The background is a blurred cityscape at night with warm lights and a bridge structure.

Avivah Litan

Vice President, Distinguished Analyst, Gartner

Rethinking Cyber Risk for Nonprofits

Gartner's **Avivah Litan** Warns of New AI Threats and Urges Better Security Models

AI has become mainstream thanks to tools such as ChatGPT, though most enterprises are still early in their adoption journey. But Avivah Litan, vice president and distinguished analyst at Gartner, predicts that by 2026, over 80% of companies will be using some form of AI agents.

In this video interview with Information Security Media Group at RSAC Conference 2025, Litan also discussed:

- Gartner's new concept of Guardian agents;
- How the TRISM - trust, risk and security management - framework addresses the exponential expansion of attack surface created by interconnected AI agents;
- Why human-centric monitoring approaches fall short under the speed and complexity of agentic AI behavior.

[WATCH ONLINE](#)

“When you think about the rise of AI agents, it's still new, but we predict that by 2026, at least 80% of companies will be using some form of agents.”

- **Avivah Litan**

A portrait of Kelley Misata, a woman with long blonde hair, wearing a light blue blazer over a dark top and a colorful necklace. She is looking slightly to the right with a thoughtful expression. The background is dark with blue and red light streaks.

Kelley Misata

Founder and CEO, Sightline Security, and President, The Open Information Security Foundation

AI Agents Rise, but Risks Demand Smarter Governance

Sightline Security's **Kelley Misata** on Why Myths Hinder Real Security Progress

Nonprofit organizations are often labeled as low-risk when it comes to cybersecurity, but that perspective misses the diversity and importance of these organizations, said Kelley Misata, founder and CEO, Sightline Security, and president, the Open Information Security Foundation.

In this video interview with Information Security Media Group at RSAC Conference 2025, Misata also discussed:

- Common myths that undermine cybersecurity funding of nonprofits;
- How Sightline Security is pushing for stronger protections across the sector;
- The types of sensitive data nonprofits manage and why they are attractive targets.

[WATCH ONLINE](#)

“Many times when we think about nonprofits, we are thinking about them in that paradigm of being poor, being underresourced, not having too much data.”

- **Kelley Misata**



INVESTORS

Market and economic uncertainties are posing both challenges and opportunities for cybersecurity firms and the venture capitalists and investors who take huge risks to create and nurture startup companies. But a wide range of investors we spoke with at RSAC Conference are optimistic about agentic AI technologies and automation that are transforming the way security organizations operate.

Gen AI Startups Are Embedding AI Into Product Architecture

Glilot Capital Partners' **Kleinstei**n on How Gen AI Transforms the Security Landscape



Arik Kleinstei, co-founder and managing partner, Glilot Capital Partners, says startups have an advantage over incumbents because they don't have to deal with legacy technology. But he shared some steps startups can take to secure their data and AI models.

[WATCH ONLINE](#)

Cybersecurity Investors Bet Big on Early-Stage Startups

Munich Re Ventures' **Sidra Ahmed Lefort** on Why Seed Funding Dominates Cybersecurity



Cybersecurity attracted \$13 billion in investments in 2024, a 40% jump in funding compared to 2023, with nearly half going to early-stage startups. "A lot of the investors are very interested in getting that early ownership," said Sidra Ahmed Lefort, director at Munich Re Ventures.

[WATCH ONLINE](#)



Dave DeWalt

Founder, Managing Director, CEO, NightDragon

AI Narrows the Cyber Gap Between Attackers and Defenders

NightDragon CEO **Dave DeWalt** Sees Cautious Optimism With Agentic AI

Advances in scalable AI and agentic technologies are creating a long-awaited shift in the defender-offender dynamic. With autonomy and agentic capabilities entering production, CISOs may soon deploy 100,000 autonomous agents instead of hiring more staff, said Dave DeWalt, CEO of NightDragon.

In this video interview with Information Security Media Group at RSAC Conference 2025, DeWalt also discussed:

- Federal leaders' positive cybersecurity outreach despite administrative transitions;
- Platformization versus best-of-breed solutions amid AI's rise;
- Rising investment in quantum and hybrid GPU-QPU architectures.

WATCH ONLINE

“Vulnerabilities create exploits. Exploits create opportunities for attackers.”

- **Dave DeWalt**

AI's Double-Edged Sword in Software Development

Rain Capital's **Chenxi Wang** Warns About AI's Emerging Role in Coding



AI can significantly accelerate code generation - helping developers go from idea to implementation in minutes - but AI-generated code is frequently based on insecure or flawed examples found in public code repositories, explains Chenxi Wang, founder and general partner at Rain Capital.

[WATCH ONLINE](#)

AI's Role in Cybersecurity: VC Alex Doll Breaks It Down

AI's Revolutionary and Evolutionary Reshaping of Data Security and Code Scanning



Alex Doll, founder of Ten Eleven Ventures, explains how the conversation has shifted toward AI's role in distinct areas of cybersecurity. For venture capital firms like Ten Eleven Ventures, this categorization is essential for identifying opportunities with clear use cases and market needs.

[WATCH ONLINE](#)

Agentic AI Faces Slow Adoption in Cybersecurity

Glasswing Ventures' **Grinnell** on Agentic AI's Maturity Curve, Risks and Deployment



As security leaders explore agentic AI's potential to transform SOC efficiency and reduce manual workloads, the path to adoption will be slow and steady. Rick Grinnell, founder and managing partner at Glasswing Ventures, shared why industry leaders are in no rush to dive in.

[WATCH ONLINE](#)

AI, Geopolitics and Cybersecurity Collide

Alberto Yépez of ForgePoint Capital on Emerging Global Risks and Enterprise Strategy



Never before have artificial intelligence, enterprise strategy and geopolitics intersected at such scale, speed and automation, said Alberto Yépez, managing director of ForgePoint Capital. Adversaries have already weaponized AI to launch more scalable, sophisticated and automated attacks.

[WATCH ONLINE](#)

A portrait of Bob Ackerman, a middle-aged man with short, light-colored hair, smiling. He is wearing a dark blue suit jacket over a light blue button-down shirt. The background is a blurred mix of blue and green. On the right side of the image, there is a large, semi-transparent, close-up portrait of a man's face, likely a historical figure, in a reddish-orange hue.

Bob Ackerman

Founder and Managing Director, AllegisCyber Capital

The AI Arms Race in Cybersecurity

AllegisCyber Capital's **Bob Ackerman** Examines Machine-Speed Defense Requirements

Traditional security analysts can no longer keep pace as attackers use AI to compress breach timelines from months to mere hours, fundamentally altering the cybersecurity landscape, said Bob Ackerman, founder and managing director at AllegisCyber Capital.

In this video interview with Information Security Media Group at RSAC Conference 2025, Ackerman also discussed:

- Why non-nation-state actors are increasingly targeting operational technology;
- How the democratization of attack toolkits has expanded critical infrastructure threats;
- The need for national-level coordination to protect interconnected systems such as electrical grids.

WATCH ONLINE

“AI-powered attacks are going to require AI-powered responses, and it will be about velocity.”

- **Bob Ackerman**



Art Coviello

Investment Committee Chair, SYN Ventures

Cybersecurity Market Evolves Toward Platform Consolidation

SYN Ventures' **Art Coviello** Says AI Integration Now Essential for Vendor Survival

The cybersecurity landscape continues to transform as enterprises seek to reduce their vendor footprint. With approximately 4,500 security companies competing for limited enterprise attention, consolidation has become inevitable, said Art Coviello, investment committee chair at SYN Ventures.

In this video interview with Information Security Media Group at RSAC Conference 2025, Coviello also discussed:

- Anti-ransomware, IoT/OT security and identity management as high-potential investment areas;
- How today's cybersecurity market resembles the biotech industry's innovation model;
- The challenge of balancing platform consolidation with the need for multiple vendors.

[WATCH ONLINE](#)

“If CrowdStrike doesn't adopt AI and embed it into their capabilities, they are going to go the way of other companies that haven't kept up with innovation.”

- **Art Coviello**



"You're going to see two things happening: There's going to be an acceleration of AI adoption. Secondly, we may have to do more with less, but that's the promise of AI. A CISO has to think about the things he can function without, and how can they do things differently."

Kevin Mandia

General Partner, Ballistic Ventures



Collin Gallagher

Senior Vice President, Thoma Bravo

Tapping the Resilience of the Cybersecurity Software Market

Thoma Bravo's **Collin Gallagher** on the Firm's Cybersecurity Investment Strategy

Amid macroeconomic headwinds and a cautious IPO market, Thoma Bravo's Collin Gallagher shares insights into why cybersecurity, especially identity and access management, continues to stand out as a resilient and strategically vital sector.

In this video interview with Information Security Media Group at RSAC Conference 2025, Gallagher also discussed :

- Why Proofpoint's use of large language models to analyze email "intent" marks a breakthrough in AI-powered threat detection;
- How cybersecurity investors are recalibrating their expectations amid economic uncertainty;
- Why building strong, enduring businesses is key to long-term value creation.

[WATCH ONLINE](#)

“There’s always room in the market for high-quality businesses.”

- **Collin Gallagher**

IPOs, M&A Depend on Market Stability and Scalable Platforms

Thomvest Ventures' **Padval** on Data Privacy, AI Regulation, Cyber Innovation Cycles



Tariff-related volatility and regulatory scrutiny have slowed IPOs and M&As. Umesh Padval, managing director at Thomvest Ventures, outlines how broad platforms, investor confidence and forward-looking architecture shape the future of cybersecurity startups.

[WATCH ONLINE](#)

Beyond Models: Securing AI's Real-World Use

Menlo Venture's **Rama Sekhar** on AI Threats and Opportunities



Public attention has been focused on the dangers of large language models such as hallucinations or harmful output, but the most pressing security risks are no longer rooted in the models, but in how they are integrated with real-world tools, said Rama Sekhar, partner at Menlo Ventures.

[WATCH ONLINE](#)

The Myth of the Perfect CISO: A Multitalented Master of All

Ellis of YL Ventures on How Modern CISOs Must Lead, Not Master Every Discipline



There were never many 'do everything' CISOs. Today there are even fewer. But with a specialist area, strong overview and ability to channel expertise, CISOs can align with business goals, embrace the business enabler role, demonstrate quick wins, and ensure their organization makes better risk decisions.

[WATCH ONLINE](#)

Security Professionals: Stay Aware of Current Events

Ballistic Ventures' **Kevin Mandia** on How CISOs Can Lead Through Economic Turbulence



In uncertain times, CISOs must balance people and technology, says Kevin Mandia, general partner, Ballistic Ventures. Security budgets face less risk, but efficiency is crucial. AI adoption will accelerate, vendor consolidation will strengthen defenses and SMBs may benefit from outsourcing security.

[WATCH ONLINE](#)

TECHNOLOGY AND SERVICES EXPERTS

Cybercrime groups and nation-state threat actors are constantly trying new tactics to compromise vulnerable systems. It's up to relatively small group of cybersecurity vendors to innovate and stay ahead of the hackers with technologies designed to secure identities, identify threats and vulnerabilities, and rapidly respond to incidents. We spoke to a host of leading cybersecurity technology and services experts about the latest solutions for safeguarding the enterprise.

- AI & Machine Learning
- Application Security
- Cloud Security
- Data Security & Privacy
- Endpoint & Email Security
- Identity Security
- OT/IoT Security
- Security Operations
- Risk Management





TECHNOLOGY AND SERVICES EXPERTS

AI & MACHINE LEARNING

Overcoming Fragmented Cyber Rules and AI Risks

Snyk CEO **Peter McKay** on Addressing Cyber, AI Regulatory Challenges



Multinational CEOs, CISOs and CIOs are struggling to comply with 20 to 30 different regulatory regimes, making adoption of a unified framework by governments essential, so that companies can innovate securely rather than simply react to shifting mandates, said Snyk CEO Peter McKay.

[WATCH ONLINE](#)

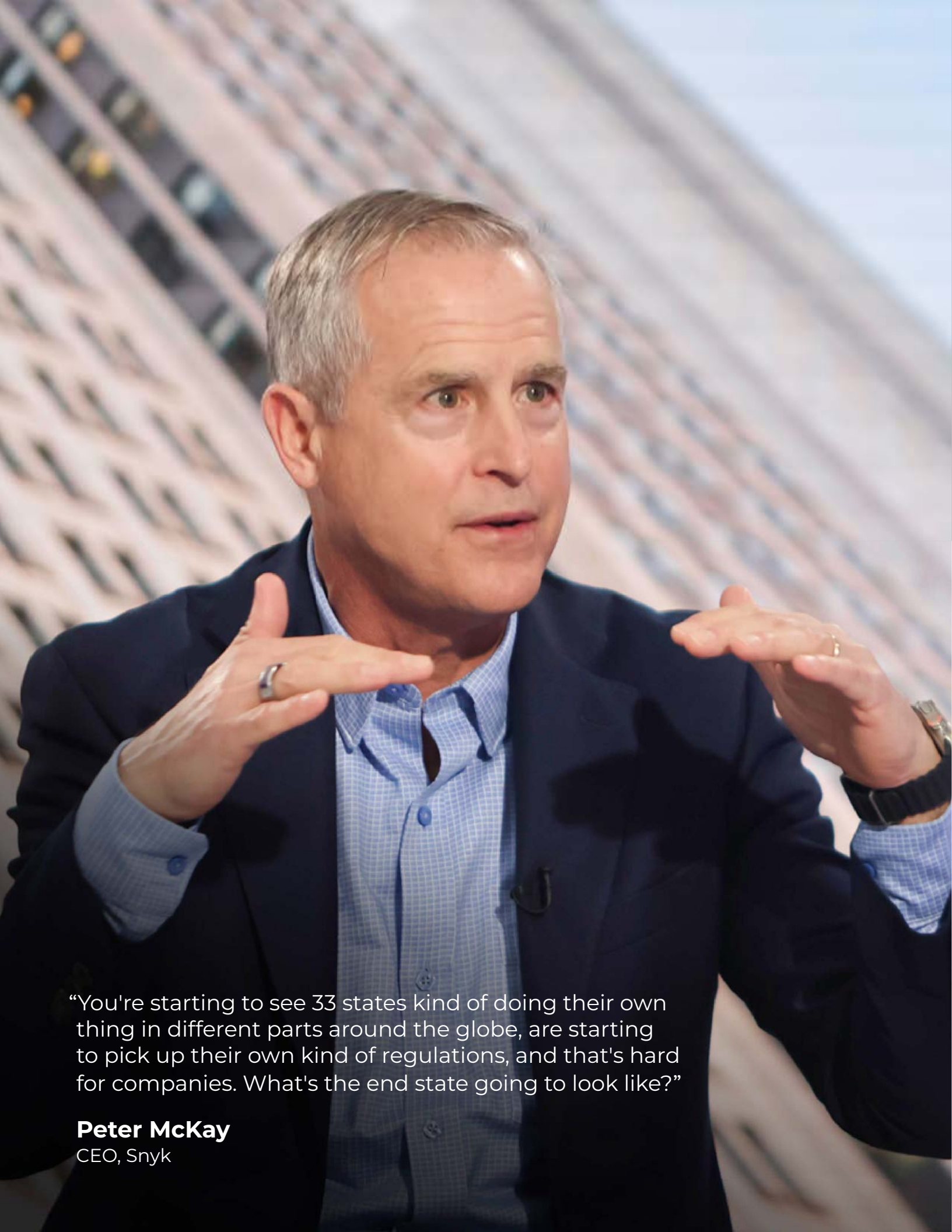
Cyberattacks Grow 40%, but Budgets Not Keeping Up

Tanium's **Dan Streetman** on Why Defenders Need to Optimize Tooling



Good AI defense requires real-time visibility across all endpoints, according to Tanium CEO Dan Streetman. He shared how Tanium's "confidence score" framework enables organizations to monitor operational impact on every endpoint when a change is rolled out, helping teams remediate threats at scale.

[WATCH ONLINE](#)



“You're starting to see 33 states kind of doing their own thing in different parts around the globe, are starting to pick up their own kind of regulations, and that's hard for companies. What's the end state going to look like?”

Peter McKay
CEO, Snyk

A portrait of Kara Sprague, CEO of HackerOne, with long reddish-brown hair, wearing a patterned jacket, looking slightly to the right.

Kara Sprague

CEO, HackerOne

Human Ingenuity Still Crucial in Cybersecurity Defense

HackerOne CEO Warns AI Can't Replace Creativity, Intuition in Cyber Defense Efforts

Despite AI advances, human intuition remains essential in security, says HackerOne CEO **Kara Sprague**. Machines detect patterns, but only people can anticipate the unexpected. Ethical hackers and human-led defense are vital to addressing evolving threats and the cybersecurity talent gap.

In this video interview with Information Security Media Group at RSAC Conference 2025, Sprague also discussed:

- Bug bounty programs as part of a broader offensive security strategy;
- A look ahead at AI playing a growing role in streamlining vulnerability triage and supporting both customers and the hacker community;
- Expanding the ethical hacker ecosystem, promoting diversity and inclusion, and ensuring that the crowd remains a central force in offensive security.

WATCH ONLINE

“Machines follow patterns; humans detect the anomalies that don't fit. In cybersecurity, it's the unexpected that causes the most damage - and only human intuition can truly anticipate it.”

- **Kara Sprague**

Supervisory Tech Critical to Managing Agentic AI

EMC Advisors' **Edna Conway** on Minimizing Risks of Agentic AI Through Oversight



Agentic artificial intelligence has the potential to transform businesses, but Edna Conway, chief executive officer of EMC Advisors, discusses the top risks associated with agentic AI solutions and why supervisory technologies are needed to monitor and control the technology.

[WATCH ONLINE](#)

Agentic AI Tackles Network Outage Prevention Challenges

NetBrain CEO **Lingping Gao** on How Agentic AI Decodes Intent to Automate Diagnosis



Agentic AI combined with intent-based automation offers proactive problem-solving within a network infrastructure, said Lingping Gao, CEO and chairman of NetBrain. The solution is not just reacting to outages but understanding and enforcing the underlying "intent" behind every function in a network.

[WATCH ONLINE](#)

Conversational Phishing Meets AI: Empowering Employees to Outsmart

Jericho Security CEO **Sage Wohns** on Emulating Attackers to Educate Users



Static training modules are no longer enough to combat modern phishing. Jericho Security CEO Sage Wohns explains how agentic AI and attacker emulation can transform security awareness into proactive defense at scale, across channels and in real time.

[WATCH ONLINE](#)

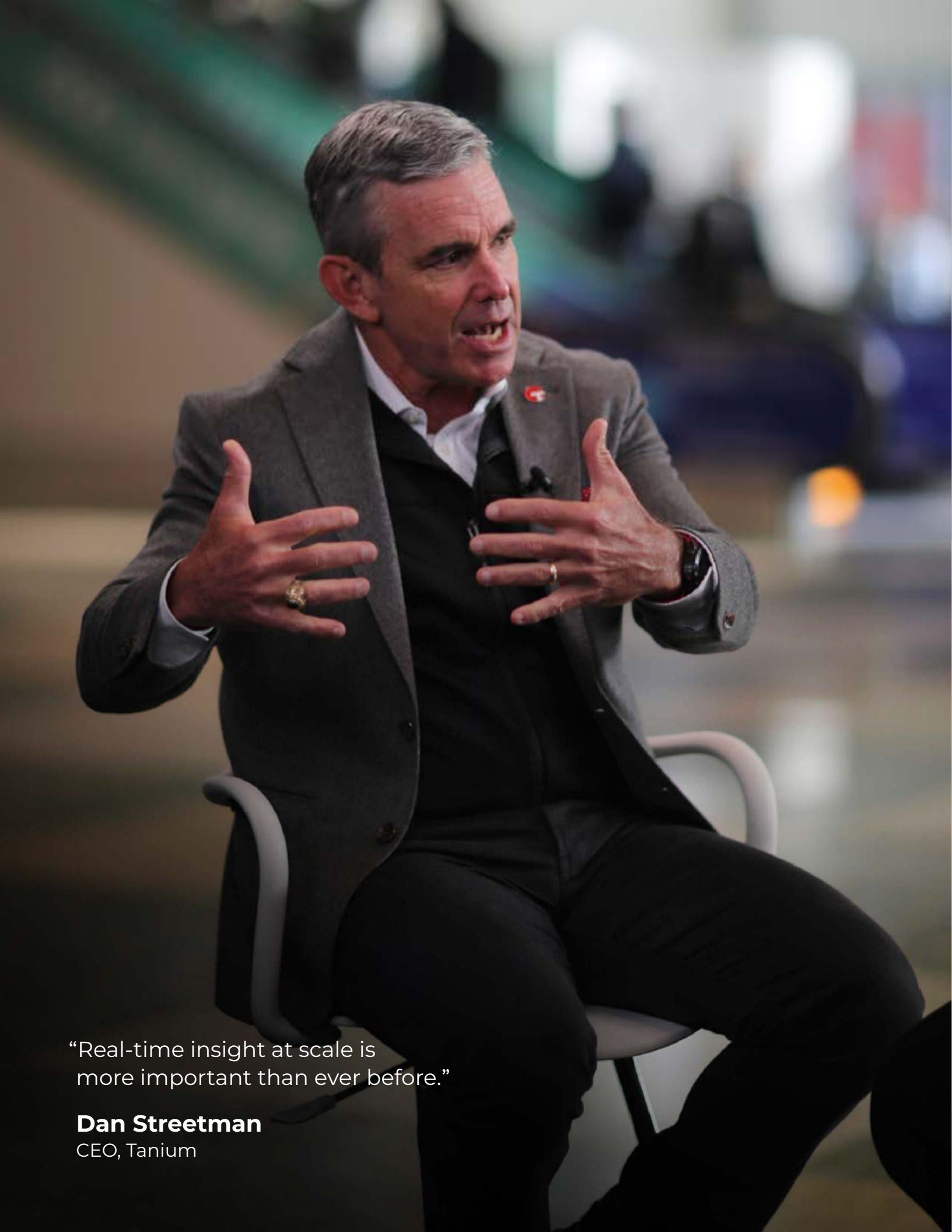
Strengthening AI Security With Platform Strategy

Palo Alto Networks' **Nikesh Arora**: Browser Security Will Surpass EDR in Importance



As enterprises rush to deploy AI across operations, Palo Alto Networks is securing models and agents through its platform approach and recent acquisitions. CEO Nikesh Arora predicts browser security will outpace EDR as a foundational requirement.

[WATCH ONLINE](#)



“Real-time insight at scale is more important than ever before.”

Dan Streetman
CEO, Tanium



“The cost of fragmentation is friction. Friction causes time delay, latency. Latency is the enemy of real-time cybersecurity.”

Nikesh Arora

Chairman and CEO, Palo Alto Networks

AI: Are We Prepared?

Richard Bird, CISO of Singulr AI, on Balancing Expectations With Reality

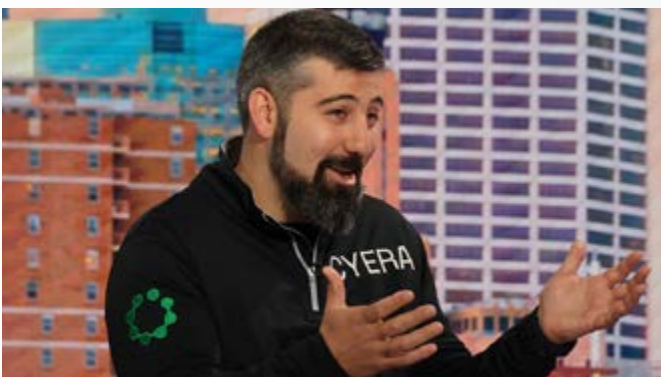


Expectations about the benefits of artificial intelligence are still running high, even though many of the results to date have been lackluster. But AI is still in its dawn and evolving rapidly, and the best is yet to come, said Richard Bird, chief security officer of Singulr AI.

[WATCH ONLINE](#)

AI's Invisible Data Risks and AI-Driven Insider Threats

Cyera CEO **Yotam Segev** on Data Security Risks From Copilot, ChatGPT, Other AI Bots



Artificial intelligence tools such as Microsoft Copilot, ChatGPT and Cortex AI offer enterprises incredible gains in workplace productivity and automation, but they also pose new risks to data security to the business, said Yotam Segev, co-founder and CEO of Cyera.

[WATCH ONLINE](#)

Balancing AI Innovation With Security

Accountability Is Key as Enterprises Adopt AI at Scale, Says Saviynt's **Jim Routh**



AI governance must balance innovation with security, making it vital that organizations adopt flexible, consensus-driven approach to ensure responsible AI deployment while addressing risks such as data exposure and software resilience, said Jim Routh, chief trust officer at Saviynt.

[WATCH ONLINE](#)

Securing AI Models Against Unpredictability and Exploitation

Cisco's **Jeetu Patel** on Open-Source Security and Building Safer AI Systems



AI is transforming cybersecurity from the ground up. Security teams battle skills shortages, alert fatigue and bloated technology stacks. Jeetu Patel, Executive Vice President and Chief Product Officer at Cisco, said AI can augment capacity and simplify defenses when applied thoughtfully.

[WATCH ONLINE](#)



“These tools really shine a light on some of the gaps we've always had but have become more painful once the challenges no longer run at human speed. They've become Olympic sprinters with AI behind them.”

Yotam Segev

Co-Founder and CEO, Cyera

A portrait of Liran Grinberg, a man with dark hair and a beard, wearing a dark suit jacket over a light blue shirt. He is looking slightly to the right with a thoughtful expression. The background is a blurred blue-toned image of a modern building or structure.

Liran Grinberg

Co-Founder and Managing Partner, Team8

The Expanding Role of CISOs in Tech and Corporate Governance

Team8's **Liran Grinberg** on How CISOs Influence Boardrooms and Enterprise Security

With cyber risk ranked as one of the top threats to business continuity, cybersecurity has now become a core component to business survival. Liran Grinberg, co-founder and managing partner at Team8, said the CISO's role has transformed into one of the most critical positions in any enterprise.

In this video interview with Information Security Media Group at RSAC Conference 2025, Grinberg also discussed:

- How Team8's CISO Village fosters critical peer-to-peer collaboration among cybersecurity leaders;
- How artificial intelligence is changing both the threat landscape and defense strategies;
- Using large language models and generative AI to understand business context and software architecture as well as improve efficiency.

“Any change in technology needs to be very much security aware, and you have to implement cybersecurity from the get go. This is why CISOs are so influential today.”

- **Liran Grinberg**

WATCH ONLINE



“When DeepSeek came out, in the first 48 hours, we were able to go and have 100% attack success rate against DeepSeek.”

Jeetu Patel

Executive Vice President, Chief Product Officer, Cisco



Sam Curry

Global Vice President, CISO in Residence, Zscaler

Battling AI With AI: Smarter Attacks Meet Smarter Security

Zscaler CISO **Sam Curry** on How AI Assists Both Targeted Phishing and Cyber Defense

Phishing is no longer a numbers game. Attackers have moved away from casting wide nets and instead are launching precise, hyper-personalized campaigns. Sam Curry, global vice president and CISO in residence at Zscaler, said this transformation is driven by defenders becoming smarter with AI.

In this video interview with Information Security Media Group at RSAC Conference 2025, Curry also discussed:

- Using AI across data in transit, at rest and in the cloud for risk-based decisions;
- Enabling comprehensive, conditional authorization through zero trust models;
- Why the future demands bold security innovation and investments.

[WATCH ONLINE](#)

“One of the reasons for a drop in phishing isn't just what the attackers are doing, it's what the defenders are doing.”

- **Sam Curry**



“When employees use public AI tools, this could be ChatGPT, this could be Gemini of the world. As soon as you submit your information, it belongs to them.”

Jay Chaudhry

Founder, Chairman and CEO, Zscaler

AI Gap Leaves Defenders Struggling Against Cyberattacks

Palo Alto Networks' **Danny Milrad** on Rise in Attack Speed and Cloud-Powered Threats



Threat actors increasingly use AI to scale their operations, but Palo Alto's 2025 Global Incident Response Report shows 86% of analyzed cases led to business disruption as organizations fail to adopt AI defenses quickly, said Danny Milrad, head, product marketing, Unit 42, Palo Alto Networks.

[WATCH ONLINE](#)

Hackers Are Testing Out Agentic AI Too - and Getting Faster

Palo Alto Networks' **Sam Rubin** on the Latest Ways Hackers Are Abusing AI



Artificial intelligence isn't just accelerating innovation. It's reshaping the cyberthreat landscape at an unprecedented pace. Adversaries are learning how to use AI and now agentic AI to scale up attacks, said Sam Rubin, SVP of consulting and threat intelligence at Unit 42, Palo Alto Networks.

[WATCH ONLINE](#)

Why Better Security in AI Use Will Fuel Wider Adoption

DJ Sampath of Cisco on Improving the Security of AI Tools and Practices

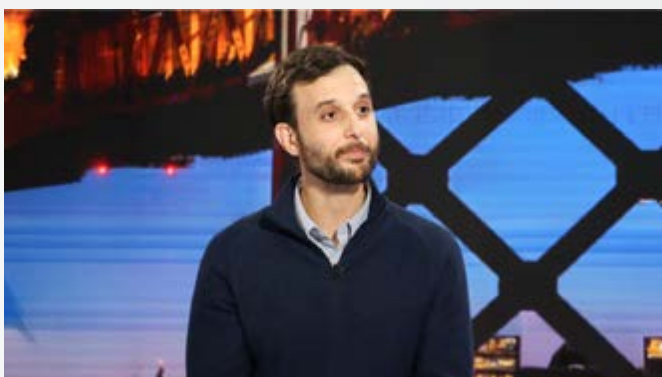


While adoption of artificial intelligence tools and development is soaring, security of these technologies - through model validation and other techniques - will fuel even wider adoption of AI, said DJ Sampath, vice president of AI software and platform at Cisco.

[WATCH ONLINE](#)

AI Agents: The Security Blind Spot You Can't Afford

SandboxAQ's **Mo Aboul-Magd** on Security in the AI Agent and Post Quantum Era



Mo Aboul-Magd, vice president of product, Cybersecurity Group, SandboxAQ, discusses the rapid adoption of AI agents and security challenges that come with it. AI agents are increasingly being integrated into business processes, while security considerations lag behind innovation, increasing risks.

[WATCH ONLINE](#)



“Defenders are using AI. They're not using AI enough. They need to use AI more to be able to keep up with the pace of attacks. We've seen a 250% increase in the speed of attacks over the past three or four years.”

Danny Milrad

Head, Product Marketing, Unit 42, Palo Alto Networks

A portrait of Suja Viswesan, a woman with dark, curly hair, wearing a red and grey patterned sweater. She is looking slightly to the right with a thoughtful expression. The background is blurred, showing green and white architectural elements.

Suja Viswesan

Vice President, Security and Runtime Products, IBM

Why Agentic AI Security Must Be Baked In - Not Bolted On

IBM's **Suja Viswesan** on Embedding Trust and Oversight Into Next-Gen AI

As autonomous agents reshape digital ecosystems, IBM Vice President Suja Viswesan, who leads the company's security and runtime products, says organizations must embed security into artificial intelligence systems from the start rather than treating it as an afterthought.


In this video interview with Information Security Media Group at RSAC Conference 2025, Viswesan also discussed:

- The critical need for human oversight of AI tools and systems;
- How unvetted AI responses can lead to risks and a lack of trust;
- What organizations can do to integrate enterprisewide security protocols.

[WATCH ONLINE](#)

“Systems need to be built with security in mind, not something you add after.”


- **Suja Viswesan**

A woman with long dark hair, wearing a dark blue blazer over a white top, is smiling and looking towards the camera. She is standing on a stage with a blurred background of colorful lights. To her left, the arm and shoulder of a man in a blue patterned jacket are visible.

“Threat actors are using these tools to help them with scripting, to help write spear-phishing emails so that they look authentic. So, we know they are using them for these normal functions.”

Sandra Joyce

Vice President, Google Threat Intelligence

A man with dark, wavy hair, wearing a light blue button-down shirt under a dark navy blazer, is speaking and gesturing with both hands. He is looking slightly to his right. The background is a blurred image of a large bridge with blue structural elements and a building with a prominent red-tiled dome and spires, possibly a cathedral or historic building, under a clear blue sky.

“Threat actors are experimenting just like we are.”

Sam Rubin

Senior Vice President, Consulting and Threat
Intelligence, Unit 42, Palo Alto Networks

Public AI Tools Need Governance to Avoid Data Leakage Risk

Zscaler's **Jay Chaudhry** on Visibility and Policy Enforcement to Secure AI Usage



Organizations face significant risks when employees use public AI tools without governance, but security platforms can provide visibility, policy controls and data protection to safeguard sensitive information from unauthorized exposure, said Jay Chaudhry, founder, chairman and CEO, Zscaler.

[WATCH ONLINE](#)

Breaking Through the Hype of AI in Cyber

Sandra Joyce, VP of Google Threat Intelligence, on AI Use by Attackers, Defenders



There is a lot of concern about artificial intelligence in the hands of cybercriminals, but so far the use of AI and related tools for innovative offensive tactics appears to be overhyped, said Sandra Joyce, vice president of Google Threat Intelligence.

[WATCH ONLINE](#)



Open-Source Platforms Are More Secure Than Proprietary Ones

Elastic CEO **Ash Kulkarni** on How AI Transforms Security Data Analysis



Ash Kulkarni, CEO at Elastic, discussed how bug bounty projects and close scrutiny by millions of developers worldwide have made open-source projects more secure than proprietary solutions. He recommends open APIs and interoperability as the future of effective security solutions.

[WATCH ONLINE](#)

Bridging the Access Trust Gap in a Hybrid Workplace

1Password's **Shiner** on Managing Unsanctioned Apps, Personal Devices and AI Agents



Employees rely on personal and company devices, using unsanctioned applications that increase productivity that can introduce significant risk. Traditional tools fail to monitor or control this dynamic environment, creating an "access trust gap," said Jeff Shiner, co-CEO of 1Password.

[WATCH ONLINE](#)



“You tend to see better quality code, you tend to find issues in that code faster because you have millions of people who have access to it and can spot issues.”

Ash Kulkarni

CEO, Elastic



Chris Wysopal

Chief Security Evangelist, Veracode

Unpacking the Effect of AI on Secure Code Development

Chris Wysopal of Veracode on How AI Boosts Code Production and Vulnerabilities

AI delivers a 50% increase in developer productivity, but with more code comes more vulnerabilities. Chris Wysopal, chief security evangelist at Veracode, shares developments in secure code practices and how regulatory pressures are improving prioritization of secure code.

In this video interview with Information Security Media Group at RSAC Conference 2025, Wysopal also discussed:

- The growing impact of regulatory and market pressures on software security;
- Critical measures for managing vulnerability backlogs efficiently;
- Why third-party open-source vulnerabilities take longer to fix than first-party code issues.

“More code to someone who does application security means more vulnerabilities.”

- Chris Wysopal

WATCH ONLINE



Pieter Danhieux

Co-Founder and CEO, Secure Code Warrior

Secure by Design: Moving Beyond Checkbox Compliance

Secure Code Warrior CEO **Danhieux** Urges Clarity Around Secure-by-Design Practices

Secure-by-design practices vary widely and often risk becoming a checkbox exercise. Pieter Danhieux, co-founder and CEO of Secure Code Warrior, warns that without a standard definition and shared framework, software design will continue to produce insecure code.


In this video interview with Information Security Media Group at RSAC Conference 2025, Danhieux also discussed:

- Why developers - and not just AppSec teams - must own threat modeling responsibilities;
- How scaling security knowledge for developers creates stronger software defenses;
- The need for clear policies as AI rapidly reshapes coding protocols and risks.

[WATCH ONLINE](#)

“We shouldn't be wasting our time on doing secure by design just to be compliant. We need to do it with a certain purpose to make the fundamentals of the software architecture stronger.”

- **Pieter Danhieux**



TECHNOLOGY AND SERVICES EXPERTS

CLOUD SECURITY

How AI and Cloud Are Driving New Machine Identity Threats

CyberArk's **Matt Cohen**: AI Agents Add New Category to Exploding Identity Landscape



Matt Cohen, CEO of CyberArk, explains how cloud-native applications have exponentially increased machine identities, with AI agents now creating an entirely new identity type requiring similar authentication and life cycle management approaches.

[WATCH ONLINE](#)

How China and North Korea Are Industrializing Zero-Days

Google Cloud's **Hultquist** on How State Hackers Exploit Code and Corporate Hiring



John Hultquist, chief analyst at Google Threat Intelligence Group, Google Cloud, discussed how China and North Korea are transforming cyberattacks into organized, factory-like operations. Alongside zero-day exploits, North Korean IT operatives are quietly infiltrating Fortune 500 companies under false identities.

[WATCH ONLINE](#)



“Each application in a modern environment can have multiple machine identities. This increases complexity because we have multiple different types of machine identities within any given application.”

Matt Cohen

CEO, CyberArk

AI-Enabled App Development Outpacing Cybersecurity Controls

Wiz's **Ami Luttwak** on Managing the 'Speed of AI' Trade-Off in Security Control



"AI is the fastest adopted technology in the history, in the enterprise," said Ami Luttwak, co-founder and chief technology officer at Wiz, explaining how AI-enabled application development has outpaced the speed at which security personnel try to attain complete visibility over stored data.

[WATCH ONLINE](#)

Major Shifts Are Redefining Cloud Security

Druva's **Yogesh Badwe** on Platformization and AI-Driven Detection



Cloud security is undergoing a major transformation. "Over the next year or two, you will potentially see a single platform solving most of the cloud security use cases," said Druva CSO Yogesh Badwe. He also warns of growing threats from non-human identities in digital ecosystems.

[WATCH ONLINE](#)

Cloud Security Strategies Focus on Operational Resiliency

Edgile's **Dean Fantham** and AWS' **PJ Hamlen** on Cloud Security Evolution



As organizations migrate critical workloads to the cloud, the focus has shifted from basic protection measures to building out integrated, resilient and intelligent security frameworks, said Dean Fantham at Edgile and PJ Hamlen at Amazon Web Services.

[WATCH ONLINE](#)

CISOs Transform Into Business-Critical Digital Risk Leaders

Google's **Phil Venables** on How AI Creates Structural Advantage in Security



Amid rising cyberthreats, security leaders are using AI tools to drive business enablement and risk management across their organizations, creating unprecedented opportunities for team transformation and career advancement, said Phil Venables, strategic security advisor at Google.

[WATCH ONLINE](#)



PJ Hamlen

World-Wide Leader, Global Partner Security Initiative, Amazon Web Services

Julie Bernard

Principal, Cyber and Strategic Risk, Deloitte & Touche

Global Tensions Spark Surge in Cyberthreats to IoT, Cloud

Experts From AWS and Deloitte Discuss Expanding Threat Landscape

As geopolitical tensions rise, companies face an expanding threat landscape - particularly through IoT and OT vulnerabilities that leave cloud infrastructures at risk, said PJ Hamlen at Amazon Web Services, and Julie Bernard at Deloitte & Touche LLP.

In this video interview with Information Security Media Group at RSAC Conference 2025, Hamlen and Bernard also discussed:

- IoT-based attacks and the growing threat landscape;
- Maintaining cyber and cloud hygiene;
- Co-developed services between Deloitte and AWS.

WATCH ONLINE

“You’ve got this healthy tension between threat actors and the geopolitical environment and a business’s desire to grow.”

- Julie Bernard



Narayan Sundar

Director, AI GTM, Palo Alto Networks

Pritish Sinha

Senior Product Manager, Google Cloud

Agentic AI Drives Enterprise Productivity and Innovation

Palo Alto's Sundar and Google's Sinha on Agentic AI's Role in Modern Enterprises

Agentic AI is moving from research to real-world enterprise use. Organizations are rapidly adopting agents to streamline workflows, boost productivity and drive innovation. But this evolution also increases exposure to risk as AI agents interact with sensitive data, opening new threat vectors.

In this video interview with Information Security Media Group at RSAC Conference 2025, Sundar and Sinha also discussed:

- How Google's Agent Development Kit enables rapid agent creation and deployment at scale;
- How Agentspace helps build, run and consume AI agents;
- Integration of Palo Alto Networks' runtime security APIs into Agentspace to embed security.

[WATCH ONLINE](#)

“There are more threats and risk. Users are exposed to more data as well. That's one of the areas that needs to be protected.”

- **Pritish Sinha**



“Organizations need to inculcate a spirit of trust between security, development and engineering teams to ensure everyone is on the same track and understands core concerns about data visibility and security. The rapid pace of application development affects visibility and data security.”

Ami Luttwak

Co-Founder and CTO, Wiz



TECHNOLOGY AND SERVICES EXPERTS

DATA SECURITY & PRIVACY

Backup Roles Key to Cyber Resilience Success

Mickey Bresman Discusses Gaps in Preparedness and Tabletop Execution



Security leaders are placing more focus on cyber resilience as regulations tighten worldwide. Mickey Bresman, CEO at Semperis, said frameworks such as the SEC's cybersecurity disclosure rule and Europe's DORA regulation are forcing organizations to build and test disaster recovery plans.

[WATCH ONLINE](#)

Privacy in the Age of AI: Return of 'Get Over It' Thinking

Michelle Dennedy of Abaxx on Why Privacy Demands Curiosity and Accountability



AI has reignited a debate on privacy. While some argue the era of personal data protections is over, others see AI as an opportunity to apply precision, nuance and contextual decision-making to data governance, said Michelle Dennedy, chief data strategy officer, Abaxx Technologies.

[WATCH ONLINE](#)



“Companies have focused in the last several years on maximizing their data collection.”

Kabir Barday

Founder, Chairman and CEO, OneTrust

Turning Visibility and Exposure Management Into Action

Axonius CEO **Dean Sysman** on How 'Actionability' Defines Next-Gen Cybersecurity



Security teams today are overwhelmed by alerts, blind spots and fragmented infrastructure. Dean Sysman, co-founder and CEO of Axonius, said the real challenge isn't data scarcity. It's turning that data into prioritized, actionable intelligence for more effective defenses.

[WATCH ONLINE](#)

AI Models Retain Sensitive Data, Risking Exposure

BigID CEO **Dimitri Sirota** on Risks of Training AI Models on Proprietary Data



Companies are increasingly relying on proprietary data to train AI models, but few realize the lasting implications. Sensitive data used for fine-tuning commercial AI models can resurface through prompt engineering, exposing companies to regulatory and security risks, BigID CEO Dimitri Sirota said.

[WATCH ONLINE](#)

Dealing With Data Explosion Challenges and Pain Points

Robin Das of DataBee, a Comcast Company, on Continuous Control Monitoring Benefits



The explosion in the amount data being produced has fueled a complex set of challenges for security professionals charged with monitoring that data, said Robin Das, executive director, market growth strategist and business development, DataBee, a Comcast Company.

[WATCH ONLINE](#)

Why AI Data Governance Is Now a Business Imperative

OneTrust CEO **Kabir Barday** Warns of Risks in Lacking AI Governance



Companies have collected oceans of data - but how much of it is actually usable for new artificial intelligence tools and technologies? OneTrust CEO Kabir Barday explains why ethical governance - not just infrastructure - will determine the real winners of the AI era.

[WATCH ONLINE](#)

Beyond Visibility: Why DSPM Solutions Need Robust Remediation

Thales' **Sebastien Cano** on Moving From Discovery to Action to Mitigate Data Risks



The effectiveness of data security posture management depends on remediation capabilities. As sensitive data spreads across environments, organizations need integrated approaches to maintain control, said Sebastien Cano, senior vice president of cyber security products at Thales.

[WATCH ONLINE](#)

Is Your Data Security Program Ready for the AI Explosion?

Varonis' **Jim O'Boyle** and Concentrix's **Adam MaGill** on Data Protection Imperatives



Nearly every organization these days has an AI pilot or new program underway. These fledgling AI models are being trained with hundreds of thousands of files and that's leading to a massive overexposure of data, said Concentrix's Adam MaGill and Varonis' Jim O'Boyle.

[WATCH ONLINE](#)



TECHNOLOGY AND SERVICES EXPERTS

ENDPOINT SECURITY & EMAIL SECURITY

Humans, Emails and Endpoints Are Hacker Gateways

Insurer **Joshua Motta** Says Firms Recover More When They Report Incidents Within 72 Hours



Attackers follow three predictable paths to commit crimes: social engineering, compromised email and vulnerable network devices. Understanding these primary vectors helps defenders prioritize their security investments, said Joshua Motta, co-founder and CEO of cyber insurer Coalition.

[WATCH ONLINE](#)

Why Consumer Browsers Don't Satisfy Enterprise Needs

Island's **Bradon Rogers** on How Purpose-Built Enterprise Browsers Enhance Security and IT



Enterprise browsers provide a purpose-built solution for corporate environments, unlike consumer browsers. The familiar interface helps maintain productivity while protecting organizational assets, said Bradon Rogers, chief customer officer at Island.

[WATCH ONLINE](#)



“The browser we all use every day is a consumer-grade piece of technology. It's serving billions of people around the world, and that's great, but at the end of the day, it wasn't built for the rigors of the enterprise.”

Bradon Rogers

Chief Customer Officer, Island



Jamie Fitz-Gerald

Vice President, Product Management, Access Management, Devices, Security and Risk, Okta

Ofer Ben-Noon

CTO, SASE, Palo Alto Networks

Securing the 'Gateway to Identity' With an Enterprise Browser

Experts From Palo Alto and Okta on Ways to Secure AI Agents, Machine Identities

In today's changing cybersecurity threat landscape, user identity has quickly morphed into the new attack surface for threat actors. Commercial browsers are now central to most enterprises' authentication and cross-platform workflows, and hackers are catching on.

In this interview with Information Security Media Group at RSAC 2025 Conference, Ben-Noon and Fitz-Gerald discussed:

- The rise of AI-propagated identity attacks and token hijackings;
- Threats to enterprises by insecure browsers;
- How Okta and Palo Alto Networks' integrated tools seek to secure identities and the enterprise browser.

“In a sense, the browser is becoming now the gateway to identity because at the end of the authentication flow, you are getting a cookie, a token, which is becoming now your digital identity as a user, as an employee.”

- **Ofer Ben-Noon**

[WATCH ONLINE](#)



“Adversaries want to work less, easier and faster, and so we've seen them going after the softer targets. Identity has been a massive issue for organizations.”

Adam Meyers

Senior Vice President, Counter Adversary Operations, CrowdStrike

Tackling the Significant Rise in Browser Attacks

Palo Alto Networks' SASE CTO **Ofer Ben-Noon** on Securing Browsers



Over the past 12 months, enterprises have experienced a significant increase in attacks targeting browsers, with 90% of organizations experiencing incidents including phishing, cookie theft and identity theft, said Ofer Ben-Noon, CTO for SASE at Palo Alto Networks.

[WATCH ONLINE](#)

Cyberthreats Surge as Attackers Target Compromised Identity

CrowdStrike's **Adam Meyers** on Cybercriminals Moving From Endpoints to Softer Targets



With EDR making it difficult for cybercriminal to carry out attacks, they are now shifting focus to exploit vulnerabilities in compromised identities and unmanaged devices to move laterally across organizations, said Adam Meyers, senior vice president of counter adversary operations at CrowdStrike.

[WATCH ONLINE](#)



TECHNOLOGY AND SERVICES EXPERTS

IDENTITY SECURITY

Cyber Resilience Demands Rethinking Risk, Identity, AI Trust

RSA CEO **Rohit Ghai** on Security Amid Evolving Threats, Tech Disruption



AI, geopolitical instability and sophisticated cyberthreats are reshaping how organizations must think about risk, resilience and identity. RSA CEO Rohit Ghai discusses identity overhaul for enterprises, moving beyond passwords and an approach to AI-based threats.

WATCH ONLINE

AI Agents Are Set to Redefine Security Operations

Proofpoint's **Dhawan** on Agentic AI Transforming Threat Response and Risk Management



Agentic AI is set to transform enterprise cybersecurity by enabling faster and effective threat response and risk management. Proofpoint CEO Sumit Dhawan outlined how AI agents - modeled as virtual humans - can triage threats at scale, reduce noise and manage repetitive, high-volume tasks.

WATCH ONLINE



“Enterprises must consider three power plays for identity in 2025: passwordless, posture management and platformization.”

Rohit Ghai
CEO, RSA



“Think of agents as
virtual humans.”

Sumit Dhawan
CEO, Proofpoint



Dave Merkel

Co-Founder and CEO, Expel

Why Identity Is the New Battleground in Cyber Defense

Expel CEO **Dave Merkel** Says Defenders Must Rethink Strategies Amid Shifting Threats

Credential theft is eclipsing ransomware as one of the top threat vectors targeting victims around the world, according to Expel's Dave Merkel, who explains how defenders can stay ahead by improving their strategies to counter new cyberthreats in real time.

In this video interview with Information Security Media Group at RSAC Conference 2025, Merkel also discussed:

- Why threat actors are prioritizing identity-based attacks;
- Technical and organizational challenges related to protecting identities;
- What security leaders should ask when evaluating AI-enabled tools.

“When you steal credentials from someone working at a large enterprise, it gives you keys to the kingdom.”

- **Dave Merkel**

WATCH ONLINE

Hybrid IT Infrastructure, Identities Are Still a Prime Target

Semperis' **Alex Weinert** on Why Identity Is Still the Weakest Link in Cybersecurity



Despite advancements in cybersecurity, identity is still the most vulnerable security perimeter for attackers. Alex Weinert, chief product officer at Semperis, said that entrenched technical debt and reliance on legacy infrastructure make identity the weakest link in cybersecurity.

[WATCH ONLINE](#)

Why Identity Security and Access Are Still Misunderstood

Mike Towers of Veza on Seeing the 'True Picture' of Identity Security



The "true picture" of access and "true picture" of identity security is not whether users can log in, but rather the permissions they have and actions they can take once inside. It's something some enterprises still don't fully understand, said Mike Towers, chief security and trust officer at Veza.

[WATCH ONLINE](#)

How Linking Identity, Data Security Can Help Cyber Response

Arvind Nithrakashyap, Co-founder and CTO of Rubrik, on Ever-Expanding Challenges



A growing reliance on complex identity systems has made identity a popular attack surface for several reasons, said Arvind Nithrakashyap, co-founder and CTO, Rubrik, discussing the ever-expanding security risks and difficulties faced by organizations.

[WATCH ONLINE](#)

How Agentic AI Is Redefining Cybersecurity

Armis's **Nadir Izrael** on How Defenders Can Use AI, Agentic AI in Cybersecurity



Armis CTO Nadir Izrael shared how agentic artificial intelligence is redefining cybersecurity, shifting defense strategies from reaction to anticipation, and why enterprises must trust automation to stay ahead of AI-powered attackers.

[WATCH ONLINE](#)



“The easiest way to bring an organization down is bringing down their identity systems.”

Arvind Nithrakashyap

CTO & Co-Founder, Rubrik

A portrait of Mark McClain, an older man with white hair, smiling. He is wearing a dark blue blazer over a light-colored checkered shirt. The background is blurred, showing green and purple elements.

Mark McClain

Founder and CEO, SailPoint

AI Agents Create Hybrid Identity Security Challenges

SailPoint's **Mark McClain** on the Need to Integrate Identity and Security Operations

Autonomous AI agents represent a revolutionary shift in enterprise identity management, combining human-like learning capabilities with machine scalability. Organizations must adapt their security frameworks to manage these dynamic entities, said Mark McClain, founder and CEO at SailPoint.

In this video interview with Information Security Media Group at RSAC Conference 2025, McClain also discussed:

- How decentralized agents challenge traditional security boundaries and authorization models;
- The convergence between SOC and identity landscape for real-time threat detection and response;
- The need to protect data beyond application-based access controls.

[WATCH ONLINE](#)

“For the most part, machine identities are going to be single purpose, single use - they're going to be capable of performing a function, and perform that function over and over.”

- **Mark McClain**



TECHNOLOGY AND SERVICES EXPERTS

OT/IoT SECURITY

Future of Secure Communications for Critical Infrastructure

Mattermost's **Ian Tien** Urges Secure Communications to Defend Critical Infrastructure



As geopolitical tensions rise and adversarial threats grow more sophisticated, critical infrastructure sectors such as energy, telecom and emergency services face mounting pressure to modernize their cybersecurity postures, said Ian Tien, CEO of Mattermost.

[WATCH ONLINE](#)

A Containment Strategy Can Protect Interconnected Systems

ColorTokens' **Rajesh Khazanchi** on Securing Convergent IT, OT and IoT Systems



The rise of insider attacks, OT-IT convergence and vulnerabilities in IoT devices are threats to previously isolated manufacturing systems. Rajesh Khazanchi, CEO at ColorTokens, says an enterprise microsegmentation platform and a containment strategy can protect interconnected IT, OT and IoT systems.

[WATCH ONLINE](#)



“An attack on a power plant or chemical facility doesn't just compromise availability, it threatens safety.”

Burgess Cooper

CEO, Cybersecurity Division, Adani Enterprises

Adani's OT Cyber Lab Targets Real-World Threats

Adani's **Pandey** and **Cooper** on How OT Simulations Fortify India's Infrastructure



Adani Group has launched an Operational Technology Cybersecurity Experience Center, an OT-focused lab designed to simulate real-world attacks, test industrial systems and foster a pipeline of OT cyber talent, said Group CISO Shivkumar Pandey and Cybersecurity Division CEO Burgess Cooper.

[WATCH ONLINE](#)

Zero Trust and Automation Crucial for Securing IoT Devices

Device Authority's **Antill** on Secure-by-Design and Continuous Authentication



Many IoT devices were never designed with modern authentication - making them easy targets. Even when certificates are used for authentication, Darron Antill, CEO of Device Authority, points out that frequent expiration and limited visibility create operational and security risks over time.

[WATCH ONLINE](#)

Chip-Level Security Moves to the Forefront

From AI and Edge Devices to IoT, Hardware-Level Security Is a Design Priority



In an era of smart devices and connected systems, embedded technology is in a quiet revolution. For those working in silicon or AI innovation, hardware-level security is no longer an optional feature. It's essential for success, said **Anup Savla**, CEO, Sasken Silicon.

[WATCH ONLINE](#)

Digitization Creates New OT Security Blind Spots

Dragos' **Robert Lee** on Why Ransomware Groups Target OT for Faster, Larger Payouts



Ransomware attacks on OT systems rose to 87% in 2024. With industrial systems becoming more connected and digitized, threat actors are able to scale attacks more effectively across critical infrastructure, said Robert Lee, co-founder and CEO of Dragos.

[WATCH ONLINE](#)



“We're seeing a lot more digitization and automation being put into [OT systems]. The more digital, the more connected and the more complex these operations environments become, the more attack surface there is.”

Robert Lee

CEO and Co-Founder, Dragos



Harry Coker

Secretary, Maryland Department of Commerce

Harry Coker Urges Unified Public-Private Cyber Defense

Ex-National Cyber Director Emphasizes a Unified Approach to Cybersecurity

Public-private partnerships are of grave importance to tackle cyberthreats, given their ability to transcend geographical boundaries and affect individuals regardless of location, says Harry Coker, secretary of the Maryland Department of Commerce and former U.S. national cyber director.

In this video interview with Information Security Media Group at RSAC Conference 2025, Coker also discussed:

- The importance of transitioning from reactive crisis responses to proactive resilience building;
- Building trust and sharing threat intelligence between the government and private sector are crucial for effective cybersecurity;
- A call for smart regulations and regulatory harmonization to reduce compliance costs and enhance national security.

“The biggest complication, from my perspective, is that cyber has victimized American residents. Cyber that come from nation-state adversaries, and up until now, the United States government has defended every American resident from nation-state adversaries.”

- Harry Coker

[WATCH ONLINE](#)

Insights From Theoretical to the Realities of AI-Enabled Cybercrime

Researchers on Custom LLMs, Expertise Requirements, Global Collaboration



Cybersecurity experts from Fortinet, UC Berkeley and Singapore's Rajaratnam School of International Studies emphasize that while AI isn't creating entirely new cyberthreats, it's making existing attacks more precise and accessible to less skilled actors through tools like FraudGPT and WormGPT.

[WATCH ONLINE](#)

Are IoT Devices the New Attack Vector for Ransomware Groups?

Phosphorus Cybersecurity's **Phillip Wylie** on Asset Inventory, Password Hygiene



Organizations inadvertently create cybersecurity gaps by trusting connected devices. Threat actors are shifting tactics to exploit IoT vulnerabilities when traditional attack vectors strengthen, said Phillip Wylie, xIoT security evangelist at Phosphorous Cybersecurity.

[WATCH ONLINE](#)

Building Cyber Resilience for Renewable Energy

Cyber Energia's **Narezzi** on Why Decentralized Energy Models Demand Stronger Security



Rafael Narezzi, managing director of Cyber Energia, warned that legacy protections do not fit decentralized energy models. Only 1% of cybersecurity efforts focus on renewables, despite mounting threats and critical operational risks.

[WATCH ONLINE](#)

Human Insight Is Key to Securing Cyber-Physical Systems

Politecnico di Milano's **Zanero** on Evolving Malware Detection and Hardware Security



Machine learning excels at identifying repetitive patterns and anomalies, but human insight remains vital for understanding the broader context of cyberattacks - especially in cyber-physical ecosystems, said Stefano Zanero, professor at Politecnico di Milano.

[WATCH ONLINE](#)



Colin Soutar

Managing Director, Risk and Financial
Advisory, Cyber and Strategy Risk, Deloitte

Eric Trexler

Senior Vice President,
Public Sector, Palo Alto Networks

Critical Infrastructure Faces Visibility, Cooperation Gaps

Deloitte's **Soutar** and Palo Alto Networks' **Trexler** on Strategies for Resilience

With adversaries actively embedding in networks, organizations must focus on cooperation rather than just technology acquisition, said Eric Trexler, senior vice president, public sector, Palo Alto Networks and Colin Soutar, managing director, cyber and strategy risk, Deloitte.


In this video interview with Information Security Media Group at RSAC Conference 2025, Soutar and Trexler also discussed:

- How federal guidance must balance with state-level implementation autonomy;
- The effectiveness of outcome-focused frameworks like NIST for diverse entities;
- Why technology partnerships deliver better results than isolated product purchases.

[WATCH ONLINE](#)

“We've got over 4.2 million miles of roads in [America], 140,000 miles of railways. We've got to protect shipping, the ports. There's so much we have to do, so we need to put a plan in place, and we need to work against that.”

- **Eric Trexler**

A portrait of Travis Rosiek, a man with short grey hair, wearing a dark suit jacket over a light-colored shirt. He is looking off to the side with a serious expression.

Travis Rosiek

Public Sector Chief Technology Officer, Rubrik

Are Nation-State Actors Pre-Positioning for Cyberwarfare?

Quick Recovery Plans Needed as Nation-State Groups Target Critical Infrastructure

Nation-state threats have been outpacing defenses for decades, adapting and evolving much faster. Now they're also changing motivations, from information gathering and seeking economic advantage to apparently pre-positioning to cause disruption in future hybrid war, Rubrik's **Travis Rosiek** said.

In this video interview with Information Security Media Group at RSAC Conference 2025, Rosiek also discussed:

- Recovering from a backup without allowing the adversary back in;
- How to isolate, contain, quarantine and recover quickly;
- Tackling software supply chain attacks, including an increase in insider threats.

[WATCH ONLINE](#)

“We're at the point now where organizations, state, local government, commercial, critical infrastructure need to start being much more aggressive and proactively deal with these problems.”

- **Travis Rosiek**



TECHNOLOGY AND SERVICES EXPERTS

SECURITY OPERATIONS

AI, Zero Trust and SASE: Modernizing Security

Versa Networks CEO **Kelly Ahuja** on a Universal SASE Approach to Combat AI-Driven Threats



Artificial intelligence-driven threats are emerging faster than most organizations can respond. CEO Kelly Ahuja explains how Versa Networks is helping organizations modernize security strategies through unified SASE, AI-powered visibility and control, and a data-centric zero trust model.

[WATCH ONLINE](#)

Why Simplicity is the Future of Cybersecurity

Fastly CEO **Todd Nightingale** Makes the Case for Security Without Compromise



Power, speed and security don't have to be mutually exclusive for organizations aiming to integrate innovative new solutions into their systems and networks. Fastly's Todd Nightingale outlines how a unified, simplified approach can help organizations fight complex threats - without compromise.

[WATCH ONLINE](#)

Cyber Warfare's Limitations: Lessons for Future Conflicts

Silverado's **Dmitri Alperovitch** on Why Cyber Is Not Effective for Deterrence



Recent real-world conflicts have limned the potential and limitations of cyber operations in warfare, said Dmitri Alperovitch, co-founder of Silverado Policy Accelerator. The United States must reassess its approach to resilience and operational integration in cyber defense, he said.

[WATCH ONLINE](#)

Red Teaming AI: Tackling New Cybersecurity Challenges

DistributedApps.ai's **Ken Huang** on Agentic AI Risks and Threat Modeling



As AI agents gain autonomy and access dynamic tools, organizations must adopt new threat modeling approaches like mixture threat modeling, a new method that accounts for AI's unpredictability, said Ken Huang, chief AI officer at DistributedApps.ai.

[WATCH ONLINE](#)

Cyber Defenders Save the Country of Berylia - Once Again!

CISO **Joe Carson** on How NATO's Locked Shields Sharpens Defenders for the Next Attack



Each year, the tiny northern Atlantic Ocean island country of Berylia comes under a massive cyberattack. It's all part of one of the world's largest red team-blue team exercises called Locked Shields, which has attracted thousands of cyber professionals including Joe Carson, advisory CISO, Segura.

[WATCH ONLINE](#)

Why the Future of Cybersecurity is Unified

Blackpoint Cyber's **Manoj Srivastava** on Orchestration, Context and Unified Cybersecurity



The traditional notion of a fixed security perimeter has become obsolete, and the threat surface has expanded significantly due to remote work, cloud adoption, IoT devices and third-party vendor integrations, said Manoj Srivastava, chief technology and product officer at Blackpoint Cyber.

[WATCH ONLINE](#)



Kevin Simzer

Chief Operating Officer, Trend Micro

Cybersecurity Trends: Impact of Tariffs and Data Sovereignty

Trend Micro's **Kevin Simzer** on How Tariffs and Data Sovereignty Shape Cybersecurity

Organizations are beginning to be more cautious in the wake of the ongoing tariff war in terms of budgeting, although the situation is an opportunity for the cybersecurity industry to improve performance overall, said Kevin Simzer, chief operating officer at Trend Micro.

In this video interview with Information Security Media Group at RSAC Conference 2025, Simzer discussed:

- The impact of trade tariffs on cybersecurity;
- How data sovereignty is driving on-premises deployments;
- Cybersecurity skill and talent challenges.

[WATCH ONLINE](#)

“We do have 10% of our business that does fall into that, and that's all network security appliances that are manufactured here in the U.S. So, we're trying to stay up on what the impact of those tariffs will be and sourcing components, but we don't see it as a big impact right now.”

- *Kevin Simzer*

Segmenting to Strengthen Cyber Defense

Rubin of Illumio on Nation-State Threats, Segmentation and Firewall Strategies



Andrew Rubin, founder and CEO of Illumio, outlines how segmentation of critical networks and unified policy enforcement improve lateral movement control, reduce risk and strengthen cybersecurity defenses against nation-state cyberthreats.

[WATCH ONLINE](#)

Why Incident Response Plans Must Prioritize Identity Recovery

Ready1's Marty Momdjian on Closing Cyber Resilience Gaps by Prioritizing Identity



Incident response strategies must prioritize rapid identity recovery to minimize downtime, according to Semperis' Marty Momdjian, who explains why Active Directory is often the single point of failure and how organizations can harden their recovery posture before attacks happen.

[WATCH ONLINE](#)

Security Workflow Automation Cuts Complexity

Elastic's Nichols and Tines' Muller on Joining Forces to Streamline Cybersecurity



Security teams are overwhelmed with fragmented tools and scattered data. Elastic and Tines addressed this challenge by combining their strengths - Elastic's data platform and Tines' automation engine - into a unified solution.

[WATCH ONLINE](#)

Protecting Enterprise Infrastructure From Data Exfiltration

Cyera's Bar-Ilan and Cohesity's Venkatesh on AI's Role in Protecting Sensitive Data



Cyberattacks have become sophisticated, exploiting the very data enterprises depend on. "Attackers are increasingly going after the backup infrastructure ... if they compromise the backup, it compromises the customer's ability to recover from a catastrophic attack," Cohesity's Sheetal Venkatesh said.

[WATCH ONLINE](#)



Seemant Sehgal

Founder and CEO, BreachLock

AI vs. AI: The New Cybersecurity Battlefield

BreachLock CEO **Seemant Sehgal** on AI's Role in Offensive Cybersecurity

Offensive cybersecurity is gaining momentum, driven by frameworks such as Gartner's Continuous Threat Exposure Management and advancements in generative AI. Organizations are increasingly adopting proactive strategies to secure their digital assets, said BreachLock CEO Seemant Sehgal.

In this video interview with Information Security Media Group at RSAC Conference 2025, Sehgal also discussed:

- The best use cases and potential risks of cybersecurity defenders and adversaries using gen AI;
- Automation in security operations centers to improve threat detection and response;
- BreachLock's growth and innovation strategy through 2026.

[WATCH ONLINE](#)

“It's crazy to see how quickly that thing can turn out reports of that quality with screenshots and everything else.”

- **Seemant Sehgal**

Applying AI Agents in Cybersecurity With Trust, Transparency

Salesforce's **Brad Arkin** on How Agents Are Transforming Security Ops



AI agents are no longer a future promise; they are already reshaping incident response and compliance at scale. Salesforce Chief Trust Officer Brad Arkin shared how security teams can deploy these digital teammates, navigate early challenges, and ensure trust and explainability remain at the core.

[WATCH ONLINE](#)

Stopping Attacks Fast: AI in Cybersecurity Today

AI's Capability to Process at Scale Will Be Promising, IBM's **Jeff Crume**



AI is transforming cybersecurity by detecting anomalies in real time, summarizing complex threats, and scaling across hybrid environments, empowering faster, smarter responses to evolving attacks, said Jeff Crume, IBM's distinguished engineer and master inventor.

[WATCH ONLINE](#)

Breaking Down Silos With Threat-Informed Defense

Mitre's **Jon Baker** on Aligning SOC, Red Teams and Intel Units



Misaligned incentives between security teams often stall collaboration. Some organizations have begun merging their SOCs, red teams and threat intel groups under a shared leadership role to break silos, Jon Baker said, director at the Center for Threat-Informed Defense at Mitre.

[WATCH ONLINE](#)

Ransomware Recovery Hinges on Preparedness and Backups

Cohesity's **Zabriskie** and BCSD's **Zimmerman** Share Real-World Attack Response Lessons



Ransomware preparedness requires immutable copies and practiced recovery plans. Blaine County Schools showed this when attackers encrypted 60% of their virtual environment before Thanksgiving break, said Blaine County School District's Paul Zimmerman and Cohesity's Dale Zabriskie.

[WATCH ONLINE](#)



John Pirc

Vice President and Head of Product Management, NetWitness

Practical Approaches to Unleashing Autonomous AI Defenders

NetWitness' **John Pirc** on Ensuring Actionable Workflows for Incident Response Teams

With cyberthreats growing more advanced, incident response and cyber defense teams must constantly adapt. To move faster, security teams are consolidating fragmented tools into integrated platforms, streamlining workflows and using AI and automation, said John Pirc, vice president at NetWitness.

In this video interview with Information Security Media Group at RSAC Conference 2025, Pirc also discussed:

- Turning AI outputs into actionable, clear workflows for incident response teams;
- How an integrated platform can mitigate data security risk;
- NetWitness' partnership with BforeAI to autonomously predict, block and preempt malicious campaigns.

[WATCH ONLINE](#)

“Innovation is great, but if it's too complex, then it defeats the purpose.”

- **John Pirc**



TECHNOLOGY AND SERVICES EXPERTS

RISK MANAGEMENT

Attribution in Cybersecurity Needs Evidence, Not Speculation

Analyst1's **Jon DiMaggio** on Critical Thinking Framework for Threat Research



Recent ransomware developments showed a concerning lack of rigorous methodology in attributing security incidents to specific threat actors, with many researchers making claims without sufficient evidence to support their conclusions, said Jon DiMaggio, chief security strategist at Analyst1.

[WATCH ONLINE](#)

Attackers Leveraging AI, Reconnaissance for Targeted Ops

Fortinet's **Derek Manky** Says Cybercriminals' Scanning Activity Is Up Nearly 18%



Technology advances in AI and a growing sophistication in reconnaissance tactics are reshaping cyberthreats, and attackers are targeting manufacturing and healthcare sectors, said Derek Manky, chief security strategist and global vice president threat intelligence, Fortinet.

[WATCH ONLINE](#)



“We broke the report down to look in the eyes of an attacker. We’re following the Mitre attack framework, all the different phases that an attacker has to go through.”

Derek Manky

Chief Security Strategist, Global Vice President,
Threat Intelligence, Fortinet



Perry Carpenter

Chief Human Risk Management Strategist, KnowBe4

AI Deception Is a Story, Not Just Code

KnowBe4's **Perry Carpenter** Urges Cognitive Defenses, Not Code Fixes

Perry Carpenter, chief human risk management strategist at KnowBe4, explains how generative AI is shifting cybersecurity from technical perimeters to cognitive battlefields, how narrative-driven training matters, and why intent matters more than authenticity in AI-driven deception.

In this video interview with Information Security Media Group at RSAC Conference 2025, Carpenter also discussed:

- Generative AI as a cognitive threat;
- Adversarial prompting risks;
- Storytelling as a defense tool.

“The battlefield is of
and for the mind.”

- **Perry Carpenter**

WATCH ONLINE

A portrait of Chris Novak, a man with a beard and glasses, wearing a dark suit jacket over a light blue shirt. He is looking slightly to the right of the camera.

Chris Novak

Vice President, Global Cybersecurity Solutions, Verizon Business

Third-Party Data Breaches Are on the Rise

Verizon's **Chris Novak** on Defending Against Growing Supply Chain Risks

This year's Verizon data breach report highlights how increasingly interconnected software supply chains pose an increased risk to organizations. About 30% of breaches last year resulted from third-party and even fourth- and fifth-party risk, said Verizon Business' Chris Novak.

In this video interview with Information Security Media Group at RSAC Conference 2025, Novak also discussed:

- Why fewer organizations are paying ransomware demands;
- Why multi-factor authentication, though imperfect, is essential to every organization;
- How infostealers may be fueling credential-based hacks.

[WATCH ONLINE](#)

“Organizations are doing a reasonably good job of protecting their enterprise, but the challenge becomes the third party or the third party of the third party. We often hear about fourth-party and fifth-party risk now, things that we weren't really talking about before.”

- **Chris Novak**

Cyber Risks and Regulations Drive Rapid Growth in GRC Market

LogicGate CEO **Matt Kunkel** on Why GRC Is Growing Faster Than the Software Industry



Cyber risks, regulatory changes, increased third-party vendors and interconnectivity are driving rapid growth in the GRC market, said LogicGate Co-Founder and CEO Matt Kunkel. Businesses and strategies are constantly evolving, requiring a GRC platform capable of adapting with equal agility.

WATCH ONLINE

Deepfakes Pose Growing Threat to Enterprise Security

GetReal's **Hany Farid** on How Deepfakes Fuels Real-Time Deception and Fraud



Deepfakes have become a growing threat to enterprises as generative AI tools get faster, cheaper and easier to use. Hany Farid, co-founder and chief science officer at GetReal, shares how the low barrier of entry invites widespread abuse by cybercriminals for real-time deception and fraud.

WATCH ONLINE

Agentic AI Expands the Corporate Attack Surface

Constella's **Andres Andreu** on AI Bots Making Cybersecurity a Challenge



Andres Andreu, COO and CISO at Constella Intelligence, discussed how a proliferation of artificial intelligence bots has complicated cybersecurity and expanded the attack surface. Andreu advises security leaders to be both technical and business-centric in their approach.

WATCH ONLINE

AI-Based Fraud: Criminals Are 2 Years Ahead of Defenders

Arkose Labs' **Kevin Gosschalk** on How Criminals Exploit Generative AI for High ROI



Underground marketplaces offer sophisticated AI tools for creating synthetic identities and executing scams at scale, with some technologies available through \$10,000 monthly subscriptions targeting financial accounts and loyalty programs, said Kevin Gosschalk, CEO of Arkose Labs.

WATCH ONLINE



John Kindervag

Creator of Zero Trust, Chief Evangelist, Illumio

Misaligned Incentives Impede Zero Trust Implementation

Zero Trust Creator **John Kindervag** on Barriers to Security Success Beyond Tech

Growing executive engagement with zero trust signifies a change from technical discussions to strategic business focus. Boards now view cybersecurity as fundamental to operations and seek solutions beyond products, said John Kindervag, creator of zero trust and chief evangelist, Illumio.

In this video interview with Information Security Media Group at RSAC Conference 2025, Kindervag also discussed:

- How proper incentives rather than technology are key to cybersecurity success;
- The partnership with Nvidia bringing zero trust capabilities to OT environments;
- Why organizations spend more time discussing zero trust than implementing it.

WATCH ONLINE

“I would argue what we have is not a technological problem. The technology is here. It's an incentive problem, and we're not incentivizing people to do the right thing for their organization.”

- John Kindervag



Niloofar Razi

Operating Partner, Capitol Meridian Partners

Adapting to AI: The Future of Security and Workforce

Capitol Meridian Partners' **Razi** on Smarter AI Use, Strong Leadership and Diversity Demands

Many AI models prioritize speed over security, exposing organizations to significant risks. Niloofar Razi, operating partner at Capitol Meridian Partners, stressed the need for companies to evaluate models carefully before adoption.

In this video interview with Information Security Media Group at RSAC Conference 2025, Razi also discussed:

- Risks of private sector offensive cyber activities;
- AI's dual impact on enterprise workflows, security and workforce transformation;
- Effective leadership strategies for navigating global uncertainty.

[WATCH ONLINE](#)

“The opportunities with respect to AI are transformative, which is why everyone's embracing it. Deployment is happening faster than anyone expected.”

- **Niloofar Razi**

Cyber Workforce Demands Specialized Skills Amid AI Growth

Splunk's **Shivji** and TekStream's **Johnson** on Workforce Development Challenges



Increased AI adoption is widening the skills gap in cybersecurity, driving a demand for specialized roles. Targeted training and public-private initiatives to develop specialized cybersecurity skills are critical to address this gap, said Bruce Johnson, director of enterprise security at TekStream.

[WATCH ONLINE](#)

Nation-State Actors Continue to Exploit Weak Passwords, MFA

Trellix's **John Fokker** Advises CISOs to Prioritize Patching, MFA, Network Visibility



Threat actors aren't rushing to adopt AI tools to exploit vulnerabilities. "They still prefer a victim with weak passwords, bad MFA, bad patching. It is the easiest way to make money for criminals so they don't have to invest in AI," said John Fokker, head of threat intelligence at Trellix.

[WATCH ONLINE](#)

Advancing Cybersecurity Through Evidence-Based Insights

Cyentia Institute's Data Finds Critical Delays and Escalating Cybersecurity Risks



The average time to remediate critical flaws 67 days - despite guidance to fix critical flaws within two weeks, said **Wade Baker**, partner at Cyentia Institute. Human-validated exploits, such as those uncovered in pen tests, are especially dangerous yet remain unresolved far too long, he said.

[WATCH ONLINE](#)

AI in the Office: Navigating New Risks, Cyber Challenges

CISO Law Firm's **John Barker** on Good Governance, Leadership for AI Risk Mitigation



As AI agents and identities continue to drastically reshape what lies ahead for the modern day workplace, organizations are facing a new kind of internal threat - backlash from employees worried about losing their jobs, said John Barker, partner at the CISO Law Firm.

[WATCH ONLINE](#)



Ronald Raether

Partner, Troutman Pepper Locke

Jon Olson

Chief Legal Officer, Blackbaud

Lessons Learned From the Blackbaud Hack and Legal Fallout

Attorneys **Ronald Raether** and **Jon Olson** Unpack 2020 Ransomware Attack, Data Breach

Effective response to a devastating cyberattack from a technical, legal and business perspective requires serious advance planning, said attorneys Ronald Raether of Troutman Pepper Locke and Jon Olson, general counsel of Blackbaud, which dealt with severe fallout from a major ransomware attack.

In this video interview with Information Security Media Group at RSAC Conference 2025, Raether and Olson also discussed:

- The importance of planning a "holistic" response to cyber incidents in advance, and what that encompasses;
- Tips for more effective table top exercises for incident response;
- Other top lessons emerging from the Blackbaud attack saga, and similarly serious cyber incidents.

[WATCH ONLINE](#)

“There's a convergence of events when there's a ransomware event that not only makes it a technical issue, but also a legal issue and even maybe an existential issue for some companies.”

- **Jon Olson**

Cyber Hygiene - a Great Way to Control Insurance Costs

Insurance, Privacy Experts Share Tips on Reducing Risks in Uncertain Times



The cyber insurance industry is undergoing a noticeable shift. Insurance decisions used to be the CFO's responsibility, but now coverage is influenced by CISOs and IT directors, said **Christopher Seusing** at Wood Smith Henning & Berman LLP and **Peter Hedberg** at Corvus.

WATCH ONLINE

Why Many Fraud Victims Don't Report Attacks

ITRC's **James Lee** on Shame, Fatigue and Precision Targeting



Many fraud victims stay silent due to shame, fatigue or fear. James Lee, president of the Identity Theft Resource Center, explains why underreporting is rising and how better data sharing could help reduce the impact of identity-driven cyberattacks.

WATCH ONLINE

The Importance of Quantifying Security Risk for the Board

Sumedh Thakar of Qualys on Taking a 'Risk Operations Center' Approach



Quantifying the potential cost impact of a cyberattack on a critical business operation and demonstrating how to reduce that risk to a more acceptable level is crucial for CISOs gaining cybersecurity budget buy-in from the CFO, board and others, said Sumedh Thakar, president and CEO of Qualys.

WATCH ONLINE

Ransomware Attacks Up 9% but Payments Are Down

Recorded Future's **Liska** on What Happens Next When Ransomware Gets Less Profitable



Data theft-only ransomware attacks have reached 50% of incidents in Q1 2025, said Allan Liska, senior security architect at Recorded Future. Law enforcement has disrupted the major players, leaving less-skilled actors scrabbling for a payday or stealing information.


WATCH ONLINE



“Whenever you talk about risk reduction, you have to know how much risk you're trying to eliminate because that dictates how much you spend reducing that risk.”

Sumedh Thakar

President and CEO, Qualys

A close-up portrait of Christiaan Beek, a middle-aged man with short, light-colored hair, looking slightly to the right. He is wearing a dark jacket.

Christiaan Beek

Senior Director, Threat Analytics, Rapid7

Why Cyberattackers Continue to Succeed - And What's Next

Threat Analyst **Christiaan Beek**, of Rapid7 on Advanced Attack Strategies

Attackers are still so successful in their assaults year after year because the foundational security of too many organizations remains too weak, said Christiaan Beek of Rapid7. Without strengthening security, cybercriminals will menace enterprises with even more devious and advanced attacks.

In this video interview with Information Security Media Group at RSAC Conference 2025, Beek also discussed:

- How cybercriminals could potentially tap agentic AI to fine-tune their attacks and extortion schemes in more devious ways;
- Potential evolving attacks involving firmware, CPUs and other scenarios;
- A call to action for what potential victim organizations - and the security industry at large - need to do to change the trajectory for defenders.

WATCH ONLINE

“After 25-plus years in the business, we're still shouting, 'Fix your passwords, do your vulnerability management, please deploy multifactor authentication! And even if they do, it still sometimes goes wrong.’”

- **Christiaan Beek**

Why Cyberattackers Love 'Living Off the Land'

Martin Zugec, Technical Solutions Director at Bitdefender, on Improving Defenses



Nearly 70% of cyber incident and data breaches these days involve "living-off-the-land" attacks, in which hackers take advantage of tools that already exist on a network rather than deploying new malware, said Martin Zugec, technical solutions director at Bitdefender.

[WATCH ONLINE](#)

Marko Polo: the Inner Workings of a Global Infostealer Empire

Recorded Future's **Leslie** on How to Respond to Cybercrime Groups



A massive cybercrime operation, publicly referred to as "Marko Polo," has recently been exposed, revealing a global infostealer cartel responsible for infecting well over 30,000 victims and stealing more than \$10 million, said Alexander Leslie, threat intelligence analyst at Recorded Future.

[WATCH ONLINE](#)

CISA's KEV List: Essential for Real-World Cyber Defense

RunZero's **Beardsley** on CVE Program Role in Securing US Agencies



The Known Exploited Vulnerabilities catalog, or KEV, has quickly become a cornerstone in most organizations' cybersecurity strategies. "When we put a vulnerability on the KEV, agencies must act," said Tod Beardsley, vice president of security research at runZero.

[WATCH ONLINE](#)



Anupam Upadhyaya

VP, Product Management, Prisma SASE, Palo Alto Networks

Arnab Bose

Chief Product Officer, Okta

SASE and Zero Trust: The Backbone of Integrated Security

Okta's **Bose** and Palo Alto's **Upadhyaya** on Identity-Based Attacks, Unmanaged Devices

With applications and users distributed globally, SASE and zero trust have evolved into essential security frameworks for managing identity-based attacks and unmanaged devices, said Arnab Bose, chief product officer, Okta, and Anupam Upadhyaya, vice president, Prisma SASE, Palo Alto Networks.

In this video interview with Information Security Media Group at RSAC Conference 2025, Upadhyaya and Bose also discussed:

- How identity has become the top target for attackers seeking "keys to the kingdom";
- Securing dynamic workforces, including contractors and temp staff;
- New identity-aware features in Prisma Access Browser 2.0 that address AI app risks.

[WATCH ONLINE](#)

“Identity is becoming one of the most targeted vectors for hackers to come in, because if you take control of identity, you have keys to the kingdom.”

- **Anupam Upadhyaya**

● REC

00:00:01:00



GOV INFO SEC

1H 20M

4K HD 1080

MENU III

Behind the Scenes

Information Security Media Group, the largest media sponsor team at RSAC Conference 2025, conducted video interviews with top leaders in cybersecurity, information security, risk management and privacy. Here's a look at the team behind the scenes.



Former Interpol agent Craig Jones with ISMG's Anna Delaney prior to an interview



ISMG CEO Sanja Kalra welcomes Peter McKay, CEO at Synk, behind the scenes.



Above, ISMG's Tom Field interviews Varonis' Jim O'Boyle and Concentrix's Adam MaGill.



ISMG's Tom Field and Sanjay Kalra with Gartner's Avivah Litan, vice president and distinguished analyst.



ISMG's global brands encompass world-class events, programs and services focused on helping organizations gain cybersecurity insights.

Department of Defense Deputy Chief Information Officer Stacy Bostjanick with ISMG's David Elichman



ISMG.Studio captured more than 150 interviews at RSAC Conference.



Behind the scenes with Sean Atkinson, CISO, Center for Internet Security, and ISMG's Anna Delaney.



RSA CEO Rohit Ghai discusses identity security with ISMG's Tom Field.



Behind the scenes with ISMG Director of Global Creative Strategy Alexandra Perez, SVP of Editorial Tom Field and Chandraprakash Singh, Senior Manager APAC, Digital & Brand Marketing.



Zscaler CEO Jay Chaudhry discusses AI risks with ISMG's Michael Novinson.

The ISMG editorial team breaks down events of the day at RSAC Conference.



Adani Group CISO Shivkumar Pandey, ISMG's Rahul Neel Mani, ISMG's Sanjay Kalra, Adani Enterprises' Cybersecurity Division CEO Burgess Cooper and EXPLIoT's Aseem Jakhar.



ISMG CEO Sanjay Kalra, ISMG Chief Collaboration Officer David Elichman and General Manager Mike D'Agostino.

Robin Das of DataBee, a Comcast Company, with ISMG CEO Sanjay Kalra.



Above, Palo Alto Networks CEO Nikesh Arora with ISMG's Michael Novinson.

ISMG CEO Sanjay Kalra with SYN Ventures' Art Coviello



Above, Maryland Department of Commerce Secretary Harry Coker speaks with ISMG's Michael Novinson. Right, ISMG's Mike D'Agostino and Julie Jordan at the news desk.



Right, Forgepoint Capital Managing Director Alberto Yépez and ISMG CEO Sanja Kalra.





iSMG.Studio, the leading platform for cybersecurity and technology leaders.



iSMG's video production team recorded 150 interviews across two studios.



See you at RSAC Conference 2026!



The entire ISMG team comes together at the end of the conference for one last photo.



About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to cybersecurity, information technology, artificial intelligence and operational technology. Each of our 38 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment, OT security, AI and fraud. Our annual global summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

Contact

(800) 944-0401
info@ismg.io

Sales & Marketing

North America: +1-609-356-1499
APAC: +91-22-7101 1500
EMEA: + 44 (0) 203 769 5562 x 216

