ISMG Studio

RSAC 2026 Conference

Highlights & Insights

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

RSAC | 2026 Conference

San Francisco • March 23 – 26 • Moscone Center

RSAC Conference is the world's largest and most influential cybersecurity gathering, bringing together security leaders, practitioners, vendors and policymakers from more than 100 countries. The conference celebrated its 35th anniversary this year, growing from a single panel of 50 cryptographers in 1991 to nearly 44,000 attendees this year. RSAC serves as a global forum to share insights, showcase innovations and address evolving cyberthreats through collaboration, education and networking.

RSAC 2026 Conference: Power of Community

Tom Field
Senior VP, Editorial
ISMG

Rogue artificial intelligence agents, critical infrastructure vulnerabilities, quantum computing risks and an uncertain geopolitical climate - as RSAC™ Conference marked its 35th year, the cyberthreat landscape couldn't be more intense.

Over four days in San Francisco, RSAC Conference brought together thousands of cybersecurity professionals and industry leaders under the theme "Power of Community." Now is the time for the cybersecurity industry to work together to overcome a host of emerging threats to data security and operational resilience. But, as we saw this week, there are plenty of reasons for optimism - from emerging AI tools designed to counter cyberattacks at machine speed to renewed commitments to information sharing and collaboration.

Once again, we staffed two video studios at the conference and interviewed more than 150 RSAC speakers and attendees. CEOs, CISOs, government officials, investors, analysts and industry association representatives all were represented in our interviews and are featured in this RSAC Compendium. Inside you'll find summaries of every interview by ISMG.Studio, along with links to the full reports on ISMG's media sites.

We brought our largest-ever ISMG team from around the world to RSAC Conference. 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 illustrating the power of the RSAC community.

Enjoy.

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

Meet the ISMG Editorial Team

Over four days in March, ISMG's team of editors interviewed more than 150 attendees at RSAC 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.

Watch Now

TABLE OF CONTENTS

Video Interviews

TECHNOLOGY AND SERVICES EXPERTS

AI and Machine Learning

TECHNOLOGY AND SERVICES EXPERTS

Identity Security

TECHNOLOGY AND SERVICES EXPERTS

Data Security and Privacy

TECHNOLOGY AND SERVICES EXPERTS

OT/ IoT Security

TECHNOLOGY AND SERVICES EXPERTS

Security Operations

TECHNOLOGY AND SERVICES EXPERTS

Risk Management

Investors

CISOs

Government Officials

Analysts/Associations

Behind the Scenes

Meerah Rajavel,
Palo Alto Networks, Pg. 53

Technology and Services Experts

Cyber adversaries are using artificial intelligence to move faster and unleash unprecedented campaigns to attack vulnerable systems and steal credentials. It's up to a relatively small group of cybersecurity vendors to stay ahead of the hackers and use AI to fight AI to help secure identities, identify threats and patch vulnerabilities. We spoke to a host of leading cybersecurity technology and services experts about the latest solutions for safeguarding the enterprise and responding to incidents faster.

- AI and Machine Learning
- Identity Security
- Data Security and Privacy
- OT/IoT Security
- Security Operations
- Risk Management

AI and Machine Learning

Artificial intelligence, agentic AI and machine learning are redefining how enterprises detect, respond to and predict cyberthreats. Meanwhile, security teams must find ways to secure growing portfolios of AI tools to keep data and intellectual property from leaving the enterprise. We spoke with experts on deploying AI-driven strategies to strengthen resilience and accelerate response.

Zero Trust Anchors AI Security Strategy

Zscaler's **Jay Chaudhry** on Infrastructure, Agents and Oversight

Zscaler CEO Jay Chaudhry explains why distributed infrastructure and zero trust models will shape AI security, the agent risks mirroring human threats and why strong oversight and identity validation remain essential for mission-critical applications.

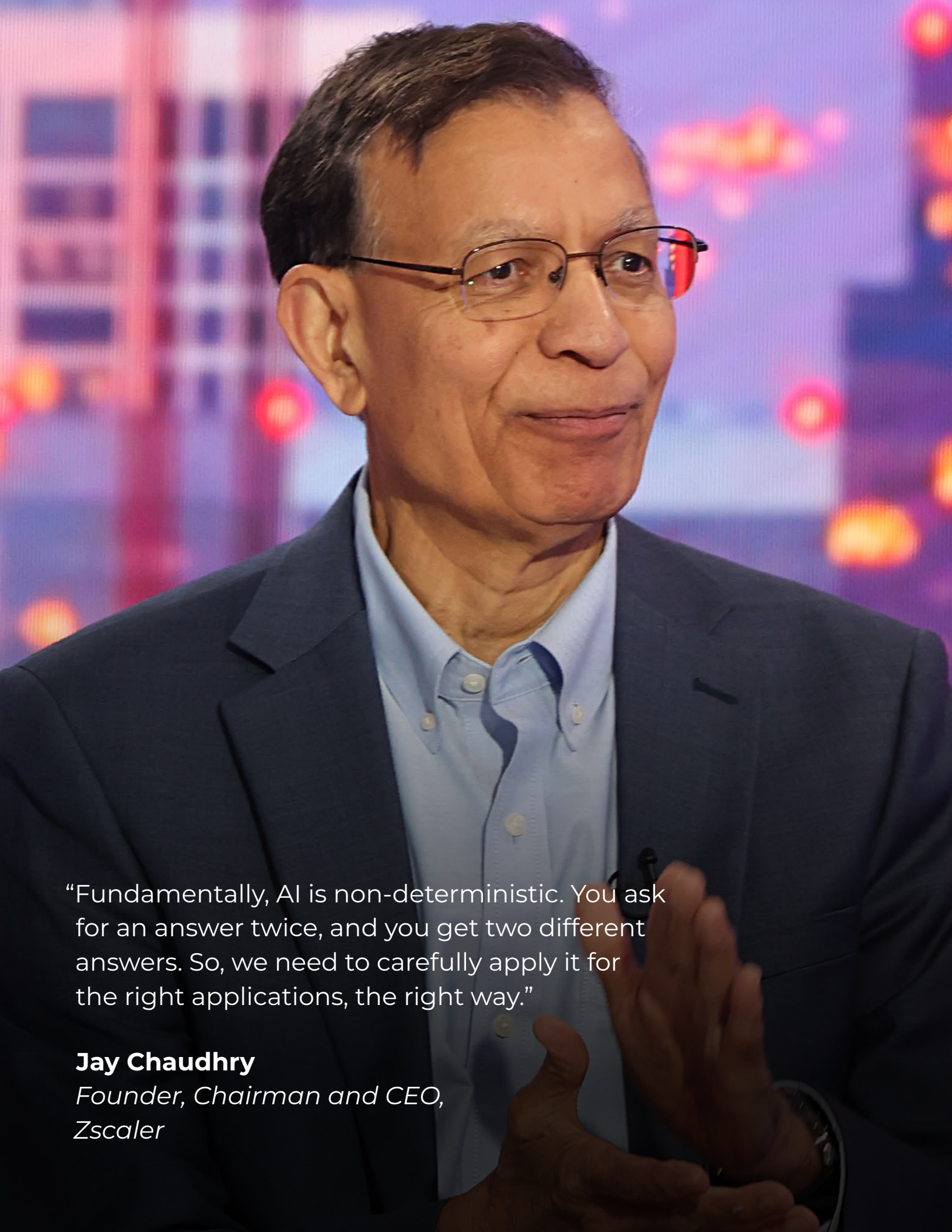
Watch Now

AI-Based Security Needs Context to Deliver Results

7AI's **Lior Div** on Building Knowledge Graphs, Human Oversight to Drive AI Accuracy

Security teams face an AI reality check as tools require deep organizational context to deliver value. Lior Div, co-founder and CEO of 7AI, explains how knowledge graphs, human oversight and phased adoption can help teams improve accuracy, build trust and scale AI-driven security operations.

Watch Now



“Fundamentally, AI is non-deterministic. You ask for an answer twice, and you get two different answers. So, we need to carefully apply it for the right applications, the right way.”

Jay Chaudhry
Founder, Chairman and CEO,
Zscaler

How Agentic AI Made Visibility the New Security Imperative

Cyata CEO **Shahar Tal** and Mercury Information Security Head **Branden Wagner** on Governing AI Workers You Can't See

Agentic AI has created a new class of digital worker that acts at machine speed, operates across endpoints, browsers and SaaS environments, and remains largely invisible to security teams, says Cyata's Shahar Tal and Mercury's Branden Wagner.

- Why posture guardrails offer a more practical path to AI governance at scale;
- How Mercury uses Cyata solutions to surface identity-linked visibility across every AI tool call;
- What Cyata's acquisition by Check Point means for its AI discovery and defense capabilities going forward.

Watch Now

"The risk profile of somebody in finance running Claude Code is very different from a software engineer running Claude Code - you have to build guardrails based on the complexity and risk associated with each."

- Branden Wagner

AI-Based Coding Redefines Software Development

Cisco's **Jeetu Patel:** Everyone Will Be a 'Manager of Agents'

Coding agents that once struggled below the surface level of basic web development can now refactor decades-old enterprise code at a speed and scale far beyond traditional teams, says Cisco's Jeetu Patel. He explains how AI-built software and machine-scale defense redefine competitive advantage.

Watch Now

Secure AI Adoption Drives Enterprise Transformation

ServiceNow and Palo Alto Networks Experts on Balancing AI, Security

Enterprises push AI adoption to boost productivity and customer service, yet CISOs must manage rising risks. Ian Swanson of Palo Alto Networks and Ravi Krishnamurthy of ServiceNow outline how secure-by-design frameworks and runtime protection enable faster, trusted AI innovation at scale.

Watch Now

Lesson From Enigma Cipher Machine Shapes OT Sec Strategy

Center for Internet Security's **Marcus Sachs** on History, AI and OT Vulnerabilities

Marcus Sachs explains how Enigma machine flaws reveal modern OT security risks. He connects historical cryptography lessons to AI, remote access vulnerabilities, and the need for stronger testing, transparency and resilience across critical infrastructure.

Watch Now

When AI Doesn't Know What It Doesn't Know

Cognizant AI Lab's **Risto Miikkulainen** on Metacognition and Evolutionary AI

Eliminating hallucinations in artificial intelligence models is the wrong goal, says Risto Miikkulainen, vice president of AI research at Cognizant AI Lab. The real fix is metacognition - building models that know when they are guessing, creating or confidently wrong.

Watch Now

"When AI is coming without knowing a specific organization, it is like somebody that joined the company without having this tribal knowledge. Once AI has the tribal knowledge, you will see improvements in the accuracy of what AI actually is doing for you."

Lior Div
Co-Founder and CEO, 7AI

Yaron Singer
Vice President, AI and Security, Foundation AI, Cisco

Why Cisco Bets on Smaller AI Models for Cybersecurity

Vice President **Yaron Singer** on How Custom AI Models Improve Security, Cost and Control

Larger isn't better when it comes to AI for cybersecurity. Yaron Singer, vice president of AI and security at Foundation AI, Cisco, makes the case for smaller, purpose-built models that outperform general-purpose AI on customizability, data privacy and cost.

- How Foundation AI's expanding portfolio of base, reasoning and enterprise search models enables the development of agentic security systems;
- Role of AI agents in SOC environments and workflow automation;
- Why production AI systems require continuous maintenance as models age and APIs evolve.

Watch Now

"If by bringing in a model and technology around it, one can basically help with unlocking some of the analyst capabilities because they can do things that normally would take them a month, they can now do them in 10 minutes - that's groundbreaking."

- Yaron Singer

AI Shrinks Cyberattack Exploit Time From Years to Days

SANS Institute's **Rob T. Lee** on AI-Driven Attacks Outpacing Cyber Defense

AI has compressed cyberattack timelines from years to days, enabling rapid exploitation and automation. Rob T. Lee, chief AI officer and chief of research at SANS Institute, warns that defenders face a widening speed gap as attackers now deploy AI across nearly every stage of the attack life cycle.

Watch Now

Securing AI-Driven Software Code at Scale

Tenzai's **Pavel Gurvich** on How Agentic AI Reshapes App Security and Testing Speed

Artificial intelligence accelerates software development but expands cybersecurity risk. Pavel Gurvich of Tenzai explains how agentic AI can help cybersecurity teams test faster, scale scarce expertise and close gaps across code, deployment and integration.

Watch Now

How Cyber Deterioration Raises Enterprise Risk

CTG's **Chad Alessi** on Supply Chain Risk, Compliance Fatigue and Resilience Scoring

Cyber deterioration is eroding enterprise security as compliance fatigue and rapid tech adoption strain controls. Chad Alessi of CTG explains how organizations can detect decline early, strengthen foundations and use continuous scoring to sustain resilience across supply chains.

Watch Now

How Deterministic Rules Keep AI-Generated Code Safe

Sonar's **Jeremy Katz** on Moving Code Security Before CI to Stop Threats Early

Artificial intelligence agents generate code at a velocity that leaves traditional continuous integration unable to catch threats in time, says Jeremy Katz, vice president of code security at Sonar. The solution is moving the security checks into the inner loop.

Watch Now

Dan Lahav
Co-Founder and CEO, Irregular

How LLM and SLM Interactions Create New Security Threats

Irregular CEO **Dan Lahav** on Why AI Systems Need New Security Baselines

As AI systems interact autonomously, they are introducing new security risks that extend beyond traditional threat models. AI agents can socially engineer each other, bypass security defenses and behave in unpredictable ways, says Dan Lahav, co-founder and CEO at Irregular.

- Why AI agents routinely treat traditional security defenses as obstacles to completing their tasks;
- A three-stage governance framework for AI asset inventory, capability assessment and baseline creation;
- Why the security industry must reframe protection as a problem of reliability and control over AI reasoning.

Watch Now

> **"Everything that we've known about social engineering for humans is true on steroids in the context of AI."**
>
> - Dan Lahav

"Each one of us, if you're a human, you're going to be a manager of agents."

Jeetu Patel
President and Chief Product Officer, Cisco

Why AI Security Hinges on Context and Control

Noma Security's **Niv Braun** on Taming the Non-Deterministic Enterprise

The surge in AI agents and applications has created a perfect storm for enterprise security teams. The technology is non-deterministic, the blast radius is enormous and the pressure to roll out quickly doesn't give security time to catch up, says Niv Braun, co-founder and CEO at Noma Security.

- How early partnerships between AI providers and security vendors enable secure-by-design capabilities;
- Why a unified AI security platform outperforms siloed point products;
- Knowing which agent actions are legitimate versus which represent real risk.

Watch Now

"If you don't see what happens in runtime, you cannot provide good recommendations on how to configure and what access to provide to your agent as part of the posture management and access control."

- Niv Braun

AI Coding Tools Raise Hidden Security Risks

Secure Code Warrior's **Pieter Danhieux** on Managing AI-Driven Development Risks

Software development is moving from human-led to agent-led at a pace that security organizations are not built to absorb, says Pieter Danhieux, co-founder and CEO at Secure Code Warrior. He explains why governing AI coding tool adoption is critical before the risks become unmanageable.

- How developer AI adoption follows a maturity curve, and why CISOs need to know where their teams sit on it;
- How secure-by-design principles improve AI-generated code outcomes;
- Why the right governance posture is controlled adoption, not fast adoption.

Watch Now

"If you do that in a proper way, then the agent or the LLM is going to produce code that is vulnerability-free. But do that the wrong way, or speak to it in language where you don't give the right instructions, it might give much worse results much faster."

- Pieter Danhieux

“The risk of not moving is higher than the risk of moving. But how can you move and manage risk at the same time? It’s a new paradigm.”

Ian Swanson
Vice President, AI Security Products, Palo Alto Networks

How Companies Should Confront Q-Day

Dell's **John Roese** on Quantum Readiness, Cryptographic Inventory and Sovereign AI

Quantum computing poses an existential threat to encryption systems built on asymmetric key management protocols, and most enterprises don't know where their cryptographic exposure begins. Dell Technologies' John Roese explains what to do now.

- Why enterprises must inventory every system that uses cryptography before addressing quantum risk;
- Why Q-Day presents greater uncertainty than Y2K;
- Why sovereign artificial intelligence and controlled model fine-tuning grow more critical as agentic systems scale.

Watch Now

"We're bringing a compute capability that can do mathematics. We've never been able to do that at scale, and the foundation of cryptography is mathematics."

- John Roese

How SaaS Tools Enable Testing of AI Models and Agents

Cisco's **DJ Sampath** on Securing Agentic AI With Red Teaming and Guardrails

The rise of agentic AI is forcing enterprises to confront a new risks. Organizations must secure AI models and entire ecosystems through adversarial testing, supply chain scrutiny and continuous runtime defenses, says DJ Sampath, senior vice president, AI software and platform, Cisco.

- Why enterprises need an inventory of AI assets across cloud and on-premises environments before deploying security controls;
- How the absence of an AI vulnerability database makes continuous adversarial testing essential;
- How runtime guardrails help defend against agentic attacks executed at scale.

Watch Now

> **"The only option that you have is to be able to adversarial-test these models over and over again."**
>
> - DJ Sampath

Identity Security

Identity security has emerged as a critical frontline in defending against increasingly sophisticated, identity-based attacks, now amplified by AI agents and the explosion of machine identities. Experts shared solutions for prioritizing identity governance, improving access controls and ensuring continuous authentication to strengthen security in a perimeterless world.

Why Identity Will Define Cybersecurity in 2026

RSA CEO **Greg Nelson** on Passwordless Progress, AI Threats and Resilience

Resilience drives identity security strategy in a hybrid, AI-driven threat landscape. Organizations face rising pressure to secure identities across environments while managing AI risk, governance demands and fragmented ecosystems, says Greg Nelson, CEO of RSA.

Watch Now

How AI Agents Are Redefining the Insider Risk Threat Model

Proofpoint CEO **Sumit Dhawan** on Applying Human Insider Risk Safeguards to AI Agents

AI agents behave like humans and carry the same risks. They operate non-deterministically, can be manipulated through prompt engineering and lack any inherent code of conduct, so they require a purpose-built integrity framework, says Sumit Dhawan, CEO at Proofpoint.

Watch Now

“The companies that win over the next three quarters will be the ones that get identity right and stay ahead of those threat vectors.”

Greg Nelson
CEO, RSA

"You've got these automated machine things that are connected to your whole environment that can create a lot of damage really fast, and if you're not monitoring it, you don't have a way to even stop it"

Art Gilliland
CEO, Delinea

“With AI, there is no code of conduct. There’s no form of integrity, per se - and it’s something that has to be coded up into a technology layer, which is an AI behavior safeguard layer.”

Sumit Dhawan
CEO, Proofpoint

Redefining Pen Testing for the Agentic Enterprise

BreachLock's **Seemant Sehgal** on Agentic AI, Pitting People Against Autonomous Testing

Agentic AI is transforming operations and how firms approach pen testing. Agents can execute complex testing workflows at machine speed, but questions remain about accuracy, accountability and humans in the loop, says BreachLock CEO Seemant Sehgal.

- Concerns enterprises have about agents, agentic identities and autonomous testing;
- How agentic AI is affecting cybersecurity and pen testing specifically, and the concerns enterprises have about autonomous testing;
- The evolving role of pen testers and how BreachLock works with agents and human experts to maximize speed and coverage without compromising accuracy or accountability.

"The big change there is that it's more continuous, it's more autonomous, so the goal is that the AI makes pen testing a continuous process without having the human lose control."

- Seemant Sehgal

Watch Now

Securing AI Agents in the Zero Trust Era

Cisco's **Matt Caulfield** on Identity, Governance and Agent Risk

AI agents promise productivity gains but introduce new identity and security risks at scale. Cisco's Matt Caulfield explains why enterprises must treat agents as a new identity class, enforce zero trust at the action level and tie every agent to human ownership.

Watch Now

Agentic AI Redefines Identity Security

Oasis Security CEO **Danny Brickman** on Securing Access Control and Machine Identities

Agentic AI is forcing fundamental changes in identity and access management. Traditional systems built for human users can't support the rapid rise of machine identities and autonomous agents across enterprise environments, said Danny Brickman, co-founder and CEO at Oasis Security.

Watch Now

Why Racing to Adopt AI Puts Enterprise Security at Risk

Delinea's **Art Gilliland** on Securing AI Agents With Least-Privilege Controls

Adversaries are using AI to attack at machine speed. Enterprises say they're ready to secure artificial intelligence, but most lack the tools to find it or control it. Delinea CEO Art Gilliland warns that relaxed governance and invisible AI agents are creating serious enterprise risk.

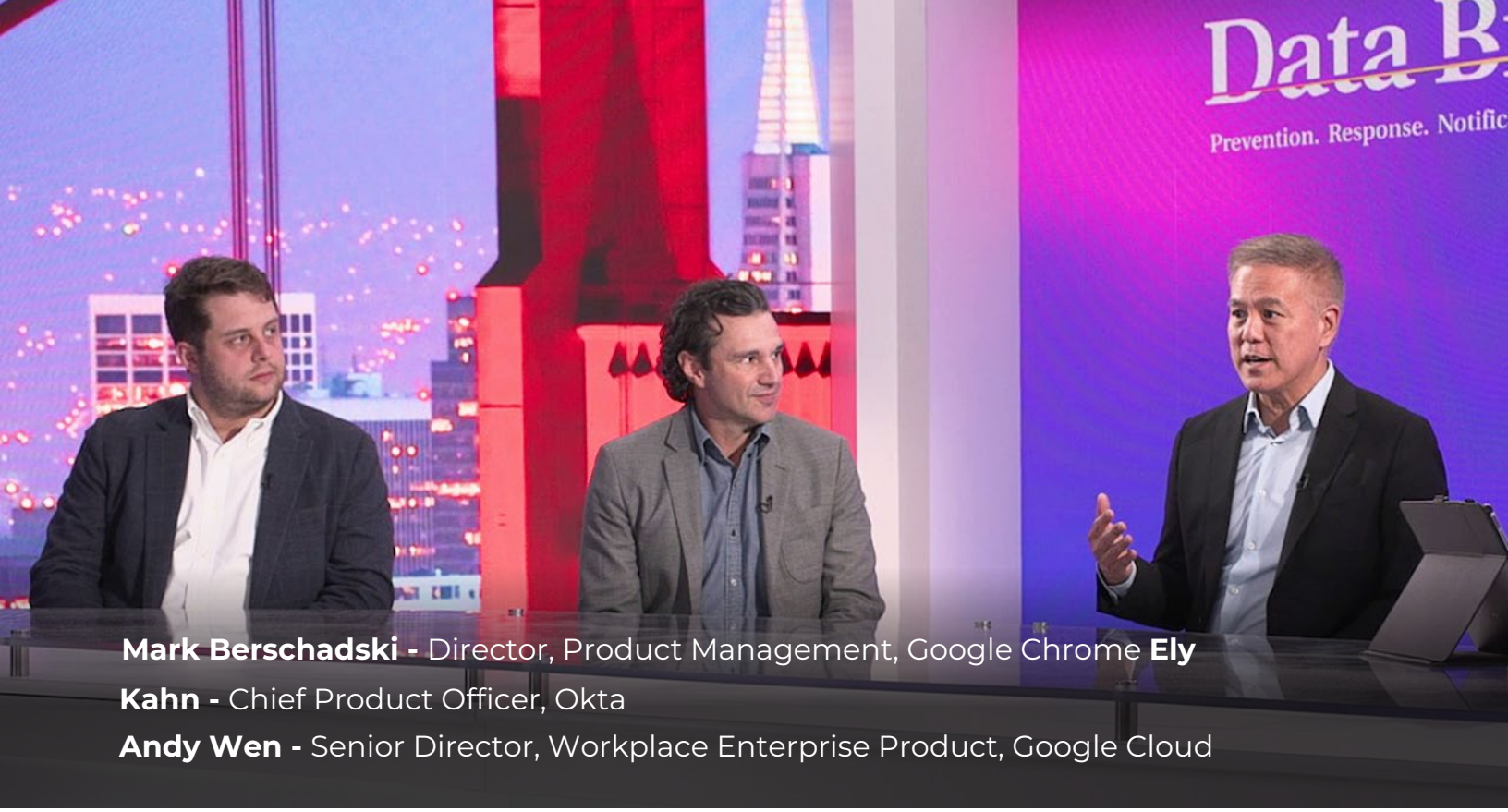
Watch Now

Building a Secure Agentic AI Framework in Financial Services

Deloitte's **Deepak Goyal** and Ping Identity's **Adam Preis** on Unlocking AI Use Cases

The artifical intelligence evolution has gone through four waves of automation, leading to agentic AI, which is transforming financial services operations. Identity frameworks are key to securing this transformation, said Deloitte's Deepak Goyal and Ping Identity's Adam Preis.

Watch Now



Mark Berschadski - Director, Product Management, Google Chrome **Ely Kahn -** Chief Product Officer, Okta
Andy Wen - Senior Director, Workplace Enterprise Product, Google Cloud

Governing Identity, AI Agents and the Browser-Led Enterprise

Google Cloud, Chrome Browser and Okta Experts on AI Agents, Shadow AI, Zero Trust

As AI agents multiply quickly, the combination of identity, browser and productivity controls has become key to enterprise security, says Andy Wen of Google Cloud, Ely Kahn of Okta and Mark Berschadski of Google Chrome.

- How device-bound session credentials cryptographically tie tokens to a device;
- How Chrome uses the Shared Signals Framework to enable real-time risk exchange with Okta;
- Why discovering and registering shadow AI agents as official identities is the most critical first step.

Watch Now

"You need to ensure you have the right AI operating at scale for the business, while you're also preventing shadow AI from sabotaging the business."

- Andy Wen

Gergely Dányi
CTO and Co-Founder, P0 Security

Neha Duggal
Chief Product Officer, P0 Security

NHI Life Cycle Management in the Agentic Era

P0 Security's **Duggal** and **Dányi** on Practical Access Controls for AI Agents

Legacy privileged access management was built for humans, and AI agents play by entirely different rules. Neha Duggal and Gergely Dányi of P0 Security warn that enterprises deploying agents are giving them broad permissions with no accountability, no auditability and no meaningful control.

- Why non-human identity life cycle management must address entitlement and credential revocation as two distinct operational concerns;
- How P0 Security's authorization control plane enforces runtime access decisions for agents;
- Real-world deployments spanning SOC triage automation and HR finance agents with scoped data access.

Watch Now

"Just like we have labeled service identities differently, we should label agent identities differently."

- Gergely Dányi

AI Is Fueling a New Wave of Credential Attacks

Dashlane CEO **John Bennett** Urges Move to Proactive Credential Security

Credential-based attacks continue to drive breaches as AI accelerates phishing and exploitation tactics. Dashlane CEO John Bennett explains why passwords persist as a risk and how organizations can shift toward proactive, real-time credential security strategies.

- Need for explicit user control as agentic AI tools introduce new credential risks;
- Gaps in SSO coverage and rise of shadow IT exposure;
- How Dashlane's Omnix platform delivers real-time, proactive credential protection.

Watch Now

"Twenty-five percent of the credentials that are used in corporate environments are weak or compromised. This is going to continue to be an issue for enterprise and business customers of all sizes."

- John Bennett

Taming the Rise of Shadow AI Agents

Security Experts on Managing Identity Risks Through Governance, Access Controls

AI agents are scaling faster than security controls. Security experts Matt Immler, Jim DuBois and Moriah Hara warn that identity must anchor governance as organizations struggle to track, secure and manage non-human identities entering enterprises at unprecedented speed.

- Applying least privilege access to limit agent blast radius;
- Building guardrails with ownership and life cycle controls;
- Driving accountability from the board to manage AI-related risk.

"We're not getting compromised through breaking firewalls anymore. It's all about taking over one's identity and elevating and escalating permissions."

- Moriah Hara

Watch Now

Data Security and Privacy

Data security and privacy have become central concerns for security teams and boards of directors as they navigate growing regulatory pressure and evolving threat landscapes. At RSAC Conference, we spoke with experts about the latest strategies for safeguarding data, managing risk and building trust while rapidly adopting AI.

AI Is Outpacing Enterprise Security Controls

Netskope's **Sanjay Beri** on Data Risk, Agent Visibility and Enabling AI Safely

Artificial intelligence adoption has outrun enterprise security, leaving data exposed and controls nonexistent. Sanjay Beri, co-founder and CEO at Netskope, says the answer isn't restriction. It's visibility, context and a culture of enablement.

Watch Now

Vibe-Coded Apps Introduce Serious Security Risks

Wiz's **Ami Luttwak** on AI-Built Apps Bypassing Authentication, Exposing Customer Data

Vibe coding allows non-technical users to build apps quickly, but it also introduces major security flaws. Ami Luttwak, co-founder and CTO of Wiz, warns that many of these applications can bypass authentication and expose sensitive data, creating new risks for organizations.

Watch Now

“Data classification by itself is useless. What you need is context. Once you have that context, you can put guardrails that let people unleash your data in the right place, yet stop it from being used in the wrong way.”

Sanjay Beri
Co-Founder and CEO, Netskope

Enterprise AI Resilience Demands Faster Recovery

Cohesity CEO **Sanjay Poonen** on Shifting Data Security to Agent, Identity Protection

Enterprise AI resilience is reshaping cybersecurity as organizations face rising threats from agents and identity-based attacks. Cohesity CEO Sanjay Poonen explains why companies must assume breach, prioritize rapid data recovery and secure growing volumes of data across complex environments.

- How enterprise AI resilience focuses on rapid data recovery after attacks;
- How AI agents expand risk through non-human identities;
- Cyber vaults and backups improve recovery speed and security.

Watch Now

“If you think about the world of healthcare, just like during COVID, we all were worried about not just ensuring you didn’t get the virus. The more important question was how quickly you could recover if you got hit?”

- Sanjay Poonen

How the AI Era Is Reshaping Data Protection

Google's **Kristie Chon** Flynn on Building Privacy Into the AI Development Life Cycle

Three years into the modern artificial intelligence revolution, data protection can no longer be an afterthought - it must be engineered in from the start, said Kristie Chon Flynn, data protection officer of privacy, safety, security engineering at Google.

- How Google's Secure AI Framework aligns teams across engineering, legal and security on a common risk language;
- Why contextual integrity is the emerging privacy challenge of 2026;
- How PETs enable organizations to converge cybersecurity, data protection and compliance requirements without sacrificing business velocity.

Watch Now

"Good governance is not static, it's dynamic. It is understanding who needs to make what kind of risk decision, and making sure that there is structure, principles and framework around it."

- Kristie Chon Flynn

"When someone who is non-technical creates this amazing application, many times they don't think about security and they don't even know what's inside the application because they didn't even create it on their own."

Ami Luttwak
Co-Founder and CTO, Wiz

Srikanth Venkat
Senior Director, Databolt Product,
Capital One Software

How the AI Era Has Raised the Stakes for Data Governance

Capital One Software's **Srikanth Venkat** on Securing the AI Data Supply Chain

Sensitive enterprise data is artificial intelligence's most valuable - and most vulnerable - input. As organizations feed proprietary data into AI models and agents, governance grows exponentially complex, said Srikanth Venkat, senior director of the Databolt product at Capital One Software.

- Why 80% of enterprise data sitting in unstructured formats poses acute governance challenges;
- How end-to-end data lineage and AI inventory management reduce risk across the supply chain;
- How Capital One Software's Databolt enables de-risked AI analytics through tokenization at massive scale.

Watch Now

"You cannot control what you cannot observe. So, you really need that governance plane to say what data is being fed into this AI model. How are the agents using it? Where is this data coming from, what transformation is it going through?"

- Srikanth Venkat

How AI Expands Risk Across Enterprise

Veeam's **Brad Linch, Emilee Tellez** on AI-Driven Cyber Risk and Data Exposure

Generative AI is accelerating cyberattacks and amplifying enterprise risk. Veeam Enterprise Strategy Director Brad Linch and Field CTO Emilee Tellez examine how data exposure, automated actions and tool exploitation can expose organizations to faster, larger-scale cyberthreats.

- The need for structured AI governance and cross-functional oversight;
- The importance of data quality and hygiene for reliable AI outcomes;
- How weak AI committee oversight can lead to enterprise data exposure.

Watch Now

> **"We have non-human identities that can now take action based off of broad sets or permissions."**
>
> - Emilee Tellez

Securing AI Data and Agents at Scale

Varonis' **Brian Vecci** on Data Visibility, Access Control and Safe AI Deployment

Organizations rush to deploy artificial intelligence but lack control over data, access and agents. Brian Vecci, field CTO at Varonis, explains why data security, visibility and least privilege determine whether AI initiatives succeed or stall in pilot phases.

Watch Now

Why DLP, DSPM and AI Security Must Converge

MIND's **Landen Brown** on Why Fragmented Data Security Tools Can't Keep Pace With AI

Only 20% of CISOs feel their organization's data security maturity is ready for safe AI adoption, according to a new Mind survey. Field CTO Landen Brown says converged DLP, DSPM and AI security, not patched-together tools, is the only way to protect data moving at machine speed.

Watch Now

Attackers Target Backup Storage to Force Ransom Payment

Object First's **Anthony Cusimano** on Why Backup Storage Is Now a Prime Ransomware Target

Ransomware groups now disable backup systems to force victims into paying ransomware. Anthony Cusimano, chief evangelist and director of solutions marketing at Object First, explains why backup storage has become the primary target and what it means for enterprise resilience strategies.

Watch Now

Stop Managing Risk. Start Managing Danger

Illumio's **John Kindervag** on Ransomware, Cyber Insurance and Fixing What's Broken

The cybersecurity industry is spending more money and solving fewer problems. John Kindervag, father of zero trust and chief evangelist at Illumio, says progress requires a fundamental mindset change from managing risk to confronting danger.

Watch Now

OT/IoT Security

OT security has become paramount as cyberthreats increasingly target critical infrastructure underpinning energy, manufacturing, healthcare and public services. Security teams face converged IT-OT systems, poor asset visibility and legacy infrastructure risks. We asked experts to share advice for safeguarding systems and reducing operational risk in the face of evolving cyber-physical threats.

Hardware Risks Expose Deeper Supply Chain Gaps

Rob Knake of TPO Group and **Edna Conway** of EMC Advisors Outline Risks

Hardware-based supply chain threats exposed deeper, harder-to-detect risks as software is the primary focus for most organizations. Rob Knake of TPO Group and Edna Conway of EMC Advisors explain how gaps in validation, identity and integration widen systemic exposure.

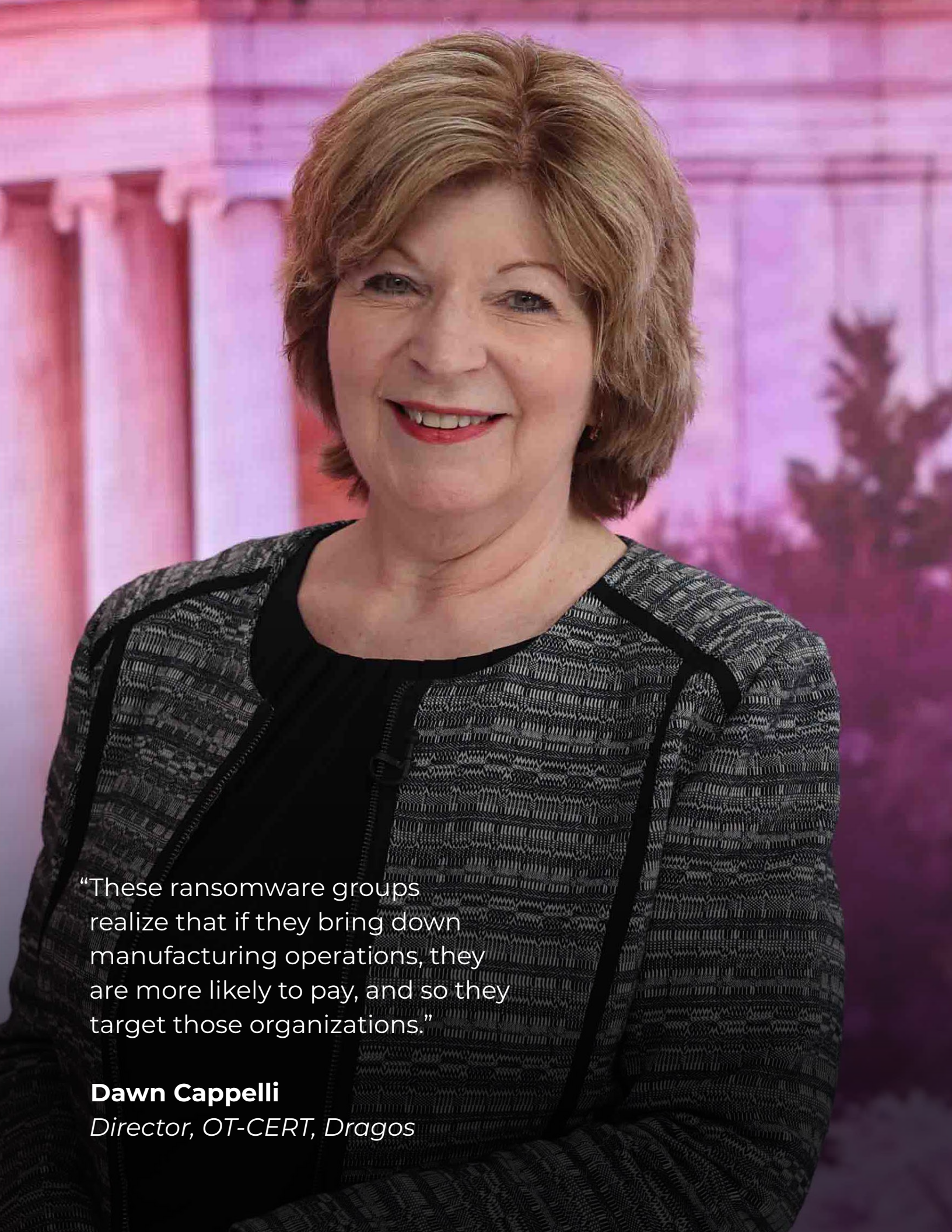
Watch Now

How Connected Vehicles Expand Cyber Risk Surface

Car Hacking Village's **Kamel Ghali** on Automotive Security for AI-Driven Ecosystems

As vehicles evolve into connected, software-defined systems, cybersecurity risks now extend beyond the car itself. Kamel Ghali, vice president at Car Hacking Village, explains why threat modeling, AI safety and ecosystemwide visibility are critical in modern automotive security.

Watch Now



“These ransomware groups realize that if they bring down manufacturing operations, they are more likely to pay, and so they target those organizations.”

Dawn Cappelli
Director, OT-CERT, Dragos

How Cyberattacks Can Turn Battery Farms Into Grid Blackouts

Centrii's **Rafael Narezzi** on Dangers of Weak Controls in Decentralized Energy Systems

As power systems decentralize to support AI workloads and rising energy demand, cyber defenses haven't been keeping pace, says Rafael Narezzi of Centrii. In fact, in December 2025 in Poland, cyberattackers disrupted the power grid balance by targeting battery storage systems.

- Regulations pushing asset owners to increase cyber maturity;
- Centrii's approach to unifying visibility across energy assets;
- Malware-driven turbine underperformance and legacy router exposure.

"They didn't stop the production of the energy itself. They created unbalancing problems, which can degrade the grid and then actually fall down or create a blackout."

- Rafael Narezzi

Watch Now

How Technical Debt Puts Critical Infrastructure at Risk

Cisco's **Eric Wenger** on Why Legacy Systems and AI Threats Drive Need for Resilience

Technical debt and outdated systems expose enterprises to rising cyber risks as AI accelerates threat activity, said Eric Wenger of Cisco. He explains why resilient infrastructure, asset visibility and life cycle security are critical to reducing vulnerabilities and support future technologies.

- How technical debt expands attack surfaces and slows innovation;
- Why AI-powered tools increase exploitation speed and scale;
- Steps to build resilient infrastructure and manage asset life cycles.

Watch Now

"Cisco Talos' recent annual report shows that two of the top 10 vulnerabilities for 2025 are old. Log4Shell is four years old, and Adobe ColdFusion is 10 years old, and yet they're still in the top 10."

- Eric Wenger

“Someone’s credentials are going to get compromised. Someone who shouldn’t be there is going to log in. They have that lateral movement. They can move from server to server, IoT to IT, and then they just compromise you.”

Brian Deitch
Chief Technology Evangelist, Zscaler

How Factories Lose Control When OT Meets the Cloud

Zscaler's **Brian Deitch** on Securing the Connected Factory With Zero Trust

The connected factory has erased the air gap that once kept plant floors safe. Brian Deitch, chief technology evangelist at Zscaler, says the expanding attack surface, spanning cloud, SaaS tools and third-party access, makes zero trust OT security a business imperative for manufacturers.

Watch Now

Telecom Sleeper Cells: Nation-State Threats Below the Radar

Rapid7's **Christiaan Beek** on Chinese Implants in Critical Networks

Nation-state actors have embedded kernel-level implants inside telecom networks designed to stay dormant for years - and 99.9% of organizations have no idea these capabilities even exist, says Christiaan Beek, vice president of threat intelligence at Rapid7.

Watch Now

Why Deliberate OT Attacks Put Manufacturers at Risk

Dragos' **Dawn Cappelli** on Evolving OT Threats and Safety Risks in Manufacturing

Adversaries have moved from incidentally hitting operational technology environments to deliberately mapping industrial control loops to enable future disruption. Dawn Cappelli, director of OT-CERT at Dragos, warns that manufacturers must reckon with safety risks that go well beyond ransomware.

Watch Now

AI Versus AI: The Future of Cyber Defense

Segura's **Joe Carson** on Agentic AI, Cyber Resilience and Estonia's Lessons

AI is accelerating both attackers and defenders, transforming cybersecurity into an AI-versus-AI battle. Segura's Joe Carson discusses why organizations must treat agentic AI as a force multiplier, not a replacement, and how to harness it responsibly in a future driven by autonomous agents.

Watch Now

Security Operations

Security operations are being reshaped by increasingly sophisticated threats and the rise of agentic AI, which is transforming how teams detect, analyze and respond to incidents. Security teams are rethinking SOC models with greater automation and intelligence. We spoke with experts on how emerging solutions help organizations move at machine speed and strengthen resilience.

Context Drives Security in Agentic AI Era

Michael Nichols of Elastic Discusses Contextual Intelligence in AI Security

Agentic AI has compressed cyberattack timelines, but faster response alone cannot close the gap. Security teams must apply contextual intelligence to guide automation, tailor decisions, and align actions with operational and regulatory realities, says Michael Nichols, general manager at Elastic.

Watch Now

Beyond Intel Sharing: The Push Toward Cyber Disruption

Google Threat Intelligence's **Sandra Joyce** on AI Threats and Active Defense

Sharing threat intelligence is no longer enough for defenders. The cybersecurity industry must operationalize threat intel through coordinated takedowns and active disruption, says Sandra Joyce, vice president at Google Threat Intelligence.

Watch Now

"As powerful as these large language models are, they don't have information about your individual environment. So, bringing your private context in a safe and secure way to those larger language models is one of the most important aspects of AI."

Michael Nichols
General Manager, Elastic

AI Era Raised Stakes for Data Security Posture Management

Thales' **Sebastien Cano** on Why DSPM Must Go From Discovery to Active Enforcement

As AI deployments accelerate, data security posture management is evolving from a compliance checkbox into a board-level risk imperative. Organizations that treat data discovery as the finish line are leaving themselves dangerously exposed, says Sebastien Cano of Thales.

- Why discovering and classifying data solves only half the problem;
- How Thales' newly announced AI Security Fabric takes a holistic approach to addressing up to 80% of OWASP's top AI deployment vulnerabilities;
- Why agentic AI requires organizations to treat AI systems with the same access controls applied to humans.

"Do you know what highly sensitive data the LLMs you deploy - and the agents you deploy - can and cannot access?"

- Sebastien Cano

Watch Now

“We certainly see the potential there for a low-skilled actor to actually get 10x through using AI tools.”

Sandra Joyce
Vice President,
Google Threat Intelligence

How Continuous Compromise Assessment Is Changing SecOps Strategy

Lumu's **Ricardo Villadiego** on Gaining Visibility Across Identity, Cloud and Networks

As attackers shift from breaking in to logging in, security teams face reduced visibility and more noise. Lumu Technologies' Ricardo Villadiego explains how continuous compromise assessment helps CISOs identify real threats, improve decision-making and strengthen existing security investments.

- The shift from malware-driven attacks to credential-based intrusions;
- Reducing alert fatigue through precise compromise identification;
- Enhancing existing security tools with a decision-focused layer.

Watch Now

> **"The way I like to put it is Lumu gives you the exact coordinates to all these signals that you have to know where the adversary is, so that you can hunt them and take them down."**
>
> - Ricardo Villadiego

Why AI Adoption Starts With Security

Meerah Rajavel of Palo Alto Networks on AI Security, Governance and Use-Case Fit

As AI outpaces governance and security frameworks, enterprise leaders face a more pressing question: How can they move fast without losing control? Meerah Rajavel of Palo Alto Networks says organizations need security guardrails, clear use cases and firm limits on probabilistic AI.

Watch Now

The Rise of Risk Operations Centers

Sumedh Thakar of Qualys on How ROCs Shift Cyber to Proactive Risk Management

As cyberthreats accelerate, security leaders can shift from reactive SOC models to risk operations centers. Sumedh Thakar of Qualys describes how ROC frameworks, powered by AI agents, help teams prioritize real risk, reduce remediation gaps and align cyber with business outcomes.

Watch Now

Why AI Agents Are Forcing a Rethink of Enterprise Security

Check Point CEO **Nadav Zafrir** on Governing AI Agents With Guardian Models

AI agents are reshaping enterprise networks, introducing new risks as they move freely and operate at scale. Check Point CEO Nadav Zafrir explains why organizations must rethink security through governance, real-time monitoring and control to manage autonomous systems effectively.

Watch Now

How Threat-Led Defense Refines Cyber Strategy

Rick Gordon and **Steven Gerry** of Tidal Cyber on Procedural Intelligence Closing Gaps

Threat-led defense shifts the focus from alerts to attacker behavior, helping security teams reduce residual risk with precision, said Rick Gordon and Steven Gerry of Tidal Cyber. They explain how to gain clarity on adversary techniques, prioritize controls and act on intelligence with greater speed.

Watch Now

“What we’re securing is changing in ways that are difficult to fathom because agents need to roam freely and are creating new pathways within organizations.”

Nadav Zafrir
CEO, Check Point Software

How Attackers Use AI to Outsmart Email Filters

Ian Thiel of Sublime Security on Why Legacy Defenses Are Falling Behind

Ian Thiel, co-founder and COO at Sublime Security, says attackers now use large language models to run phishing campaigns that are massive in scale and hyper-personalized in targeting. The old playbook of blocklists and rulesets can no longer keep pace with artificial intelligence-equipped adversaries.

Watch Now

AI Drives Software Supply Chain Attacks

OpenSourceMalware's **McCarty** on How Malware Injection Is Expanding Across CI Pipelines

AI-driven attacks now reshape software supply chains, as threat actors scale malware injection through CI pipelines and developer access. OpenSourceMalware's Paul McCarty explains how adversarial intelligence accelerates credential theft, infrastructure buildout and a widening cybersecurity arms race.

Watch Now

Agentic AI Ushers in New Era for API Security

Akamai CEO **Tom Leighton** on Managing Risk From Autonomous Systems

As agentic artificial intelligence accelerates API use, security teams face rising exposure from shadow AI, bot traffic and autonomous agents. Akamai CEO Tom Leighton explains why API security, microsegmentation and edge defenses now anchor modern cyber resilience.

Watch Now

Where AI Is Actually Delivering Enterprise Value

Bill.com's **Steve Januario** on Bots, Governance and Data Readiness as Differentiators

Real enterprise AI value emerges not from hype, but from disciplined deployment and measurable outcomes, says Bill.com CIO Steve Januario, who cautions that rapid adoption without proper guardrails introduces operational and security risks.

Watch Now

“If you are not thinking about security, don’t do AI, because AI is one of those things that has a phenomenal amount of outcomes that it can produce. But because of the speed at which it’s moving, you need to have real-time security.”

Meerah Rajavel
Chief Information Officer,
Palo Alto Networks

Securing AI as Enterprises Move Beyond Experimentation

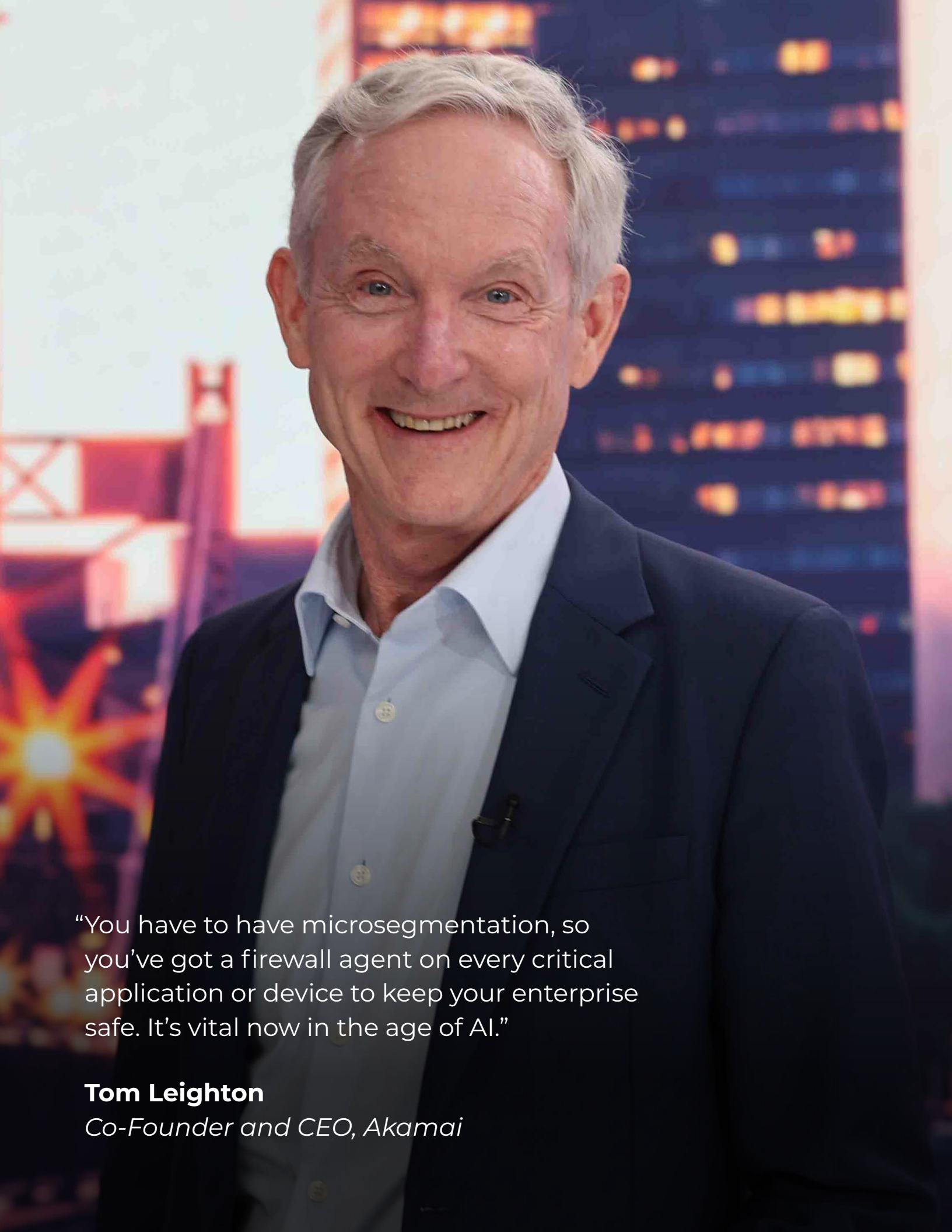
Glean's **Sunil Agrawal** and Palo Alto's **Michael Sikorski** on AI Deployment Risks

As enterprises move AI from the lab into production, new attack vectors and governance gaps are emerging fast. Glean CISO Sunil Agrawal and Unit 42 CTO Michael Sikorski break down the risks and outline what organizations must have in place before scaling.

- Why identity management and declared guardrails are foundational to safe agent deployment;
- How the Glean and Palo Alto Networks integration enforces least-privilege data access, runtime security and incident response readiness;
- Resources for security threat modeling, including the AWARE framework and Unit 42's latest incident response report.

Watch Now

> **"People moved to the cloud. They didn't think through security in the right way. And then it became really difficult and challenging, and we're still dealing with that. And now, all of a sudden, AI is on top of it."**
>
> - Michael Sikorski



"You have to have microsegmentation, so you've got a firewall agent on every critical application or device to keep your enterprise safe. It's vital now in the age of AI."

Tom Leighton
Co-Founder and CEO, Akamai

AI Security Risks Rise With Agentic Systems

Broadcom's **Gandhi** and **Mahajan** Outline AI Security, Zero Trust and Threat Defense

As agentic AI drives enterprise innovation, it also expands the attack surface at speed. Broadcom's Umesh Mahajan and Prashant Gandhi explain how AI-powered threats, lateral movement and zero trust are reshaping cybersecurity strategies and forcing faster, architecture-first defenses.

Watch Now

How an AI-Driven SOC Model Reshapes Security Operation

John Morgan of Splunk on How AI-Driven Automation Cuts Noise, Speeds Response

AI agents reshape security operations by reducing analyst burden and accelerating threat response. But organizations face a surface in AI-driven attacks, which compresses dwell time and increases alert volume, says John Morgan, senior vice president and general manager of security at Splunk.

Watch Now

Why Cyberattackers Are Pivoting to Identity Systems

Cisco Talos' **Matt Olney** on Threat Intel, AI and the Identity Crisis Ahead

Hardened cyber defenses have pushed attackers toward a softer target: the identity systems that authenticate users and control access. As agentic AI multiplies non-human accounts across enterprise networks, identity pressure will only intensify, says Matt Olney of Cisco Talos.

Watch Now

How AI-Based Red Teaming Agents Can Reduce Cyber Risk

Armadin's **Evan Peña** on Continuous Testing of Code, Configuration and Identities

AI-driven attack agents help security teams measure risk through continuous testing, broader coverage and faster analysis, said Armadin's Evan Peña. He shares how offensive security is evolving beyond point-in-time assessments to deliver stronger, data-driven protection strategies.

Watch Now

“The biggest value of the dollar you spend in security comes from the final fix. If you don’t fix it, you can spend $10 million building dashboards, but that won't make you any more secure.”

Sumedh Thakar
President and CEO, Qualys

AI Is Turning Tool Sprawl Into a Bigger Cyber Risk

Barracuda's **Rohit Ghai** on Agent Sprawl and the Need for Safer AI Security

As AI introduces autonomous agents into cybersecurity environments, the move from tool sprawl to agent sprawl is leading to increased cyber risks. Barracuda CEO Rohit Ghai explains why conflicting actions, not just data, now drive failure and why safety must take priority over speed.

- Why incident response playbooks built for pre-agentic threats are no longer adequate;
- How a risk-based approach for identifying crown jewels before applying protection underpins resilience;
- Why guardrails for agentic AI remain unproven and the boundaries of autonomous action are still undefined.

Watch Now

"We are unleashing largely autonomous capability in cyber without fully understanding where that might go."

- Rohit Ghai

AI Transformation Is Outpacing Enterprise ROI Reality

Cato Networks CEO **Shlomo Kramer** on AI Hype, Cybersecurity Gaps and Platformization

AI will reshape technological evolution more than past revolutions, but enterprise value lags expectations. Shlomo Kramer, co-founder and CEO of Cato Networks, warns that security gaps and uneven ROI could slow adoption while expanding the cyberthreat landscape.

- How organizations can evaluate whether AI security solutions are delivering real value beyond the hype;
- Why a platform-first cybersecurity strategy fares better than acquisition-led models;
- How Cato evaluates the integration potential and strategic fit of M&A targets.

Watch Now

"We are going to see the efficiency that will fund the spending, but the spending versus efficiency is not at the right ratio right now. Something needs to be fixed."

- Shlomo Kramer

Tim Pappa
Incident Response Engineer, Cyber Deception Strategy, Walmart Global Tech

How Deception Turns Attacker Behavior Into Intel

Walmart Global Tech's **Tim Pappa** on Using Deception to Build SOC Confidence

Cyber deception isn't just a trap for attackers, It's a precision tool for building SOC confidence, says Tim Pappa of Walmart Global Tech. High-fidelity alerting grounded in observed attacker behavior gives decision-makers clarity that traditional detection tools often can't deliver.

- Why talking openly about deception can deter attackers;
- How red teaming and pen testing inform deception design;
- How artificial intelligence is enabling defenders to prepare for both human attackers and large language model-driven agentic threats.

Watch Now

"If you can craft this alerting, you know very promptly, 'This is bad. This is a high-fidelity alert that informs decision-makers.' That's a lot of value."

- Tim Pappa

How Autonomous IT Keeps Pace With AI-Driven Threats

Tanium CEO **Dan Streetman** on AI, Endpoint Visibility and Platform Strategy

AI is accelerating the threat landscape and operational environment beyond the capacity of human teams. Tanium CEO Dan Streetman says the solution is autonomous IT - a model in which a platform continuously learns, addresses exposures before they occur and scales security operations.

- How autonomous IT differs from traditional automation and why continuous learning is essential;
- The risks AI agents introduce to identity management and endpoint control;
- Why a few integrated strategic platforms will define the future of IT operations and security.

Watch Now

"If I'm automating off of stale data, it's not just ineffective, it's dangerous. We saw that happen right where agents began to collaborate off of old data. They couldn't act fast enough."

- Dan Streetman

Turning Security Operations Over to AI Requires Trust

Arctic Wolf CEO **Nick Schneider** on How Visibility, Human Oversight Shape AI Adoption

AI adoption is accelerating, but security leaders now demand proof of effectiveness and trust. Arctic Wolf CEO Nick Schneider explains why visibility, data evidence and human oversight are critical to ensure AI delivers reliable outcomes in cybersecurity operations.

- Why organizations need proof of AI effectiveness and measurable outcomes;
- How visibility of AI agents improves trust and operational control;
- Why human oversight is critical to validating and refining AI performance.

Watch Now

"I think they need proof that those solutions are doing what they purport to do and that the outcomes that they'd expect from those tools are the outcomes that they're actually garnering."

- Nick Schneider

Risk Management

Risk management is evolving as organizations confront complex, interconnected threats across cyber, regulatory and operational domains. Security leaders are tasked with integrating real-time intelligence, quantifying risk and aligning security with business priorities. We spoke with experts on building adaptive risk frameworks, improving decision-making and strengthening resilience in an increasingly unpredictable threat landscape.

Why Vector Databases Put Enterprise AI Data at Risk

Cyborg's **Nicolas Dupont** on Closing the Encrypted Vector Search Gap

Enterprise AI applications are consolidating proprietary business data into vector databases, creating a structurally unencrypted layer. Conventional encryption can't address the risk without degrading performance, says Cyborg CEO Nicolas Dupont.

Watch Now

Generative AI Fuels Identity Fraud at Scale

Jeremy Grant of Venable on How Generative AI Weakens Legacy Identity Controls

AI tools make identity fraud cheaper, faster and harder to stop. Jeremy Grant, managing director of technology business strategy at Venable, says deepfakes and synthetic identities put new pressure on bank controls, forcing teams to rethink how they verify people and protect digital trust.

Watch Now

Ransomware Has Torn Up the Crisis Playbook

FTI Consulting's **Brett Callow** on Crisis Communications and Attribution Risk

Ransomware groups no longer follow a script. The attacks have become less predictable and more aggressive, targeting stakeholders beyond victims. Brett Callow of FTI Consulting explains why organizations must rethink crisis communications and treat attribution with caution.

Watch Now

Dignity by Design Should Help Shape AI Risk Strategy

BH Consulting's **Valerie Lyons** on Looking Beyond Security to Fairness, Transparency

Valerie Lyons, chief operations officer for BH Consulting, explains why artificial intelligence systems require dignity by design, not only privacy and security, outlining the risks from misuse, bias and behavioral impact across multiple industry use cases.

Watch Now

Why AI Risk Demands a Whole-Enterprise Response

OneTrust's **Michael Siegrist** on Shadow AI, Data Permissions and Agent Governance

AI risk isn't just a technology problem. It's a companywide challenge that spans adoption, use and procurement. Managing it requires breaking down silos between product, security, privacy and the executive suite, says Michael Siegrist, risk field CTO at OneTrust.

Watch Now

Machine-Speed Cyberattacks Redefine Defense

Kai CEO **Galina Antova** on How Fragmented Tools, Legacy Processes Slow Response

Attackers use AI to scale operations and automate execution, which shifts the balance in cyber defense. Fragmented tools and siloed teams slow response times, while alert volume overwhelms analysts, says Galina Antova, co-founder and CEO of Kai.

Watch Now

"You need to set up proper guardrails, governance and risk management programs. The risk management and the controls to mitigate those risks are now more important than ever."

Michael Siegrist
Field CTO for Risk, OneTrust

Francis deSouza
Chief Operating Officer and President,
Security Products, Google Cloud

AI Forces CISOs to Rebuild Defense Playbooks

Francis deSouza of Google Cloud on Fighting AI-Driven Threats With AI

AI has redrawn the threat landscape for security leaders and forced a new operating model. Francis deSouza of Google Cloud says CISOs must counter faster, AI-driven attacks with AI-led defense, stronger governance and teams fluent in AI.

- AI agents for alert triage, vulnerability scanning and automated remediation;
- Shadow AI risk, software supply chain exposure and post-quantum readiness;
- Governance, visibility and auditability across AI infrastructure.

Watch Now

"CISOs are bringing in AI tools. They are re-skilling their teams to make sure they're fluent on AI and that we're using AI-driven workflows and agents to be able to identify attacks more quickly and respond way more quickly than we ever have."

- Francis deSouza

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 artificial intelligence technologies and automation that are transforming the way security organizations operate.

The True Value in AI Lies in Execution

Venture Capitalist **Art Coviello** on AI Speed, Defense Gains, Disciplined Investing

Artificial intelligence drives cybersecurity gains but demands disciplined investment, said Art Coviello, investment committee chair at SYN Ventures. Teams should focus on measurable outcomes such as faster product development, improved efficiency and stronger cyber defense.

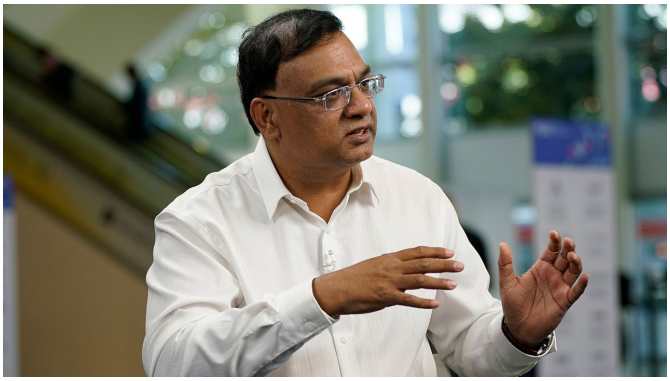
Watch Now

How the AI Coding Boom Is Rewriting Application Security

Costanoa Ventures' **John Cowgill** on Moving From Static Analysis to Runtime Defense

Artificial intelligence-generated code is arriving faster than cybersecurity teams can review it, and the risks are moving from the line level to the system level. John Cowgill, partner at Costanoa Ventures, says it's time to move to runtime defense.

Watch Now



How AI Is Reshaping Application Security and the SOC

Blumberg Capital's **Pramod Gosavi** on Where AI Security Startups Can Win

As LLMs reshape application security and security operations, their ability to generate code and detect patterns is reducing reliance on traditional tools. Blumberg Capital's Gosavi explains why context remains the critical gap and where startups can create lasting value.

Watch Now

Contextual AI Redefines Cyber Defense, Data for Enterprises

Seligman Ventures' **Umesh Padval** on How Unified Data Layers Simplify Security Ops

AI is pushing decision-makers toward unified cybersecurity architectures that cut noise and cost. Enterprises currently rely on 30 to 40 security tools, and the market is poised for disruption, says Umesh Padval, managing partner at Seligman Ventures.

Watch Now

Speed, Judgment and Behavior: AI's Defense Mandate

Capitol Meridian Partners' **Niloofar Razi** on Innovation Sandbox, AI-Driven Offense

Cybersecurity can no longer stop at the system boundary. Organizations must understand how humans and AI agents behave, and intervene before attackers exploit that behavior, says Niloofar Razi, operating partner at Capitol Meridian Partners.

Watch Now

AI Agents Redefine Enterprise Cybersecurity Risk

Menlo Ventures' **Rama Sekhar** on Securing AI Agents and Non-Human Identities

As AI evolves from assistants to autonomous agents, enterprises face a new attack surface driven by non-human identities. Rama Sekhar, partner at Menlo Ventures, explains why visibility, governance and AI-driven remediation are critical to securing this evolution.

Watch Now

“What’s great about these entrepreneurs is they’re not encumbered by legacy architecture. They aren’t encumbered by customers who expect them to maintain products that, frankly, might be irrelevant in three to five years. They get be AI-first and build businesses with the most advanced tools that solve tomorrow’s problems.”

Niloofar Razi
Operating Partner,
Capitol Meridian Partners

Why Cyber Deals Keep Surging Despite AI Market Swings

Altitude Cyber's **Domenic Perri** on Why AI-Native Security Startups Draw Record Deals

Artificial intelligence is expanding the attack surface and creating new threats, but it's also fueling record cybersecurity investment. Altitude Cyber's Domenic Perri makes the case for long-term optimism.

- Why 2025 was a record-breaking year for cybersecurity M&A, funding and valuations;
- Which sectors, including identity security, data security and next-gen SIEM, will draw the most M&A and investor attention in 2026;
- Why strategic buyers view AI-native acquisitions as a way to signal market commitment to customers.

Watch Now

"Investors view these new AI security companies as potentially the next Wiz or the next CrowdStrike. They are born in this new era, solving new problems in AI that could represent new categories or even a new platform."

- Domenic Perri

Cybersecurity M&A Is Surging as AI Reshapes the Market

Momentum Cyber CEO **Eric McAlpine** on the Funding Velocity of AI-Native Startups

Large funding rounds are concentrating on fewer cybersecurity startups as artificial intelligence accelerates product development. Momentum Cyber CEO Eric McAlpine shares why investors are backing AI-native startups earlier and how it is reshaping growth and competition in cybersecurity M&A.

- The expansion of AI security into a defined market category;
- Why startups should focus on building durable companies rather than targeting potential buyers;
- Why strategic buyers are outpacing private equity in M&A activity.

Watch Now

"Some of these AI companies are shipping code at an alarming pace. We're starting to see just the velocity of being able to develop code at such a pace where you're now able to fuel go-to-market right out of the gate."

- Eric McAlpine

Alex Doll
Founder and Managing General Partner,
Ten Eleven Ventures

How Quantum Threats Drive Encryption Changes

Alex Doll of Ten Eleven Ventures on Q-Day Risk Considerations

Quantum computing advances push security teams to replace encryption keys faster and adopt quantum-resistant algorithms. Investors and enterprises now treat Q-Day as a near-term risk, forcing changes in key management, PKI and cryptographic standards, says Alex Doll of Ten Eleven Ventures.

- Why frequent key rotation strengthens security posture;
- Key management and PKI challenges in cloud-first environments;
- Quantum capabilities outside of cybersecurity for industries such as pharmaceuticals, logistics and finance.

Watch Now

"The fundamental threat from quantum computing is quantum computers can be used to essentially run a dictionary attack on every possible outcome. And so it's very important when quantum computing arrives that we have quantum-resistant encryption."

- Alex Doll

How AI Could Help Unleash Machine-Speed Cyber Offense

Bob Ackerman of DataTribe on Why AI Favors Attackers Over Defenders

As AI adoption accelerates, attackers are poised to outpace defenders. Bob Ackerman, founder and managing director of DataTribe, shares how automated exploitation and fewer operational constraints could give adversaries a temporary but dangerous advantage across enterprise environments.

- How nation-states are infiltrating critical infrastructure including utilities and water systems;
- Why most organizations lack comprehensive visibility into their cyber environments;
- How a centralized system can deliver visibility into organizational exposure and vulnerabilities.

Watch Now

“Along comes artificial intelligence, and all of a sudden you can automate, you could hypothetically prosecute the entire library of CVEs.”

- Bob Ackerman

Why Venture Capitalists Like Israeli Startups for Seed Deals

YL Ventures' **Ofer Schreiber** Breaks Down the Lure of Early-Stage Israeli Firms

Global venture capital firms are moving into Israeli cybersecurity at the seed stage to secure early access to category-defining companies. This influx of capital is intensifying competition and compressing startup timelines, says Ofer Schreiber, senior partner at YL Ventures.

- Why rising seed rounds support multiple investors from day one;
- Why founders who fall behind in the category race lose the ability to raise additional capital;
- How early-stage acquisitions are becoming a tool for struggling startups and emerging category leaders to scale inorganically.

Watch Now

"We want to help the founders build historical companies - and the way to do it is to run very fast from day one."

- Ofer Schreiber

“The gap between what the offense can do and the defense can do widened dramatically. So, we are entering an actually dark period.”

Dave DeWalt
Founder and CEO, NightDragon

Why Startup Cyber Funding Boom Creates Execution Risks

Rain Capital's **Sidra Ahmed Lefort** on Overcapitalization and Cybersecurity's Barbell Effect

Cybersecurity funding hit all-time highs in 2025, rivaling the 2021 boom, said Sidra Ahmed Lefort, venture partner at Rain Capital. A "barbell effect" has taken hold, with capital concentrating at the earliest and latest stages while squeezing the Series B and C middle.

- How M&As, not IPOs, remain the dominant cybersecurity exit route, with infrastructure companies widening the acquirer pool;
- Why cash is not a moat, especially as artificial intelligence erodes product differentiation and lowers switching costs;
- Why second-time founders command outsized capital and credibility in the current funding environment.

"Cushions are meant to be comfortable; they're not meant to be making you competitive."

- Sidra Ahmed Lefort

Watch Now

AI Tidal Wave: What Defenders Must Do Now

Phil Venables of Ballistic Ventures on the Second-Order Consequences of AI

AI is not just transforming how organizations operate, it's fundamentally altering the cybersecurity landscape, said Phil Venables, partner at Ballistic Ventures. The consequences, he warned, are only beginning to emerge.

- Why defenders hold a structural advantage over attackers in extracting value from AI, and what it will take to realize it;
- How the proliferation of non-human identities is compounding an access management problem organizations never fully solved;
- Why the enterprise agentic control plane - governing what agents can do and how they operate - is his central focus for 2026.

"AI security is a meaningless phrase. Even agentic security is a meaningless phrase. You drop it down a level and say, what does it mean to give identity to agents?"

- Phil Venables

Watch Now

AI Raises the Performance Bar for SOC Analysts

Team8's **Ori Barzilay** on AI-Driven Gains in Security Operations

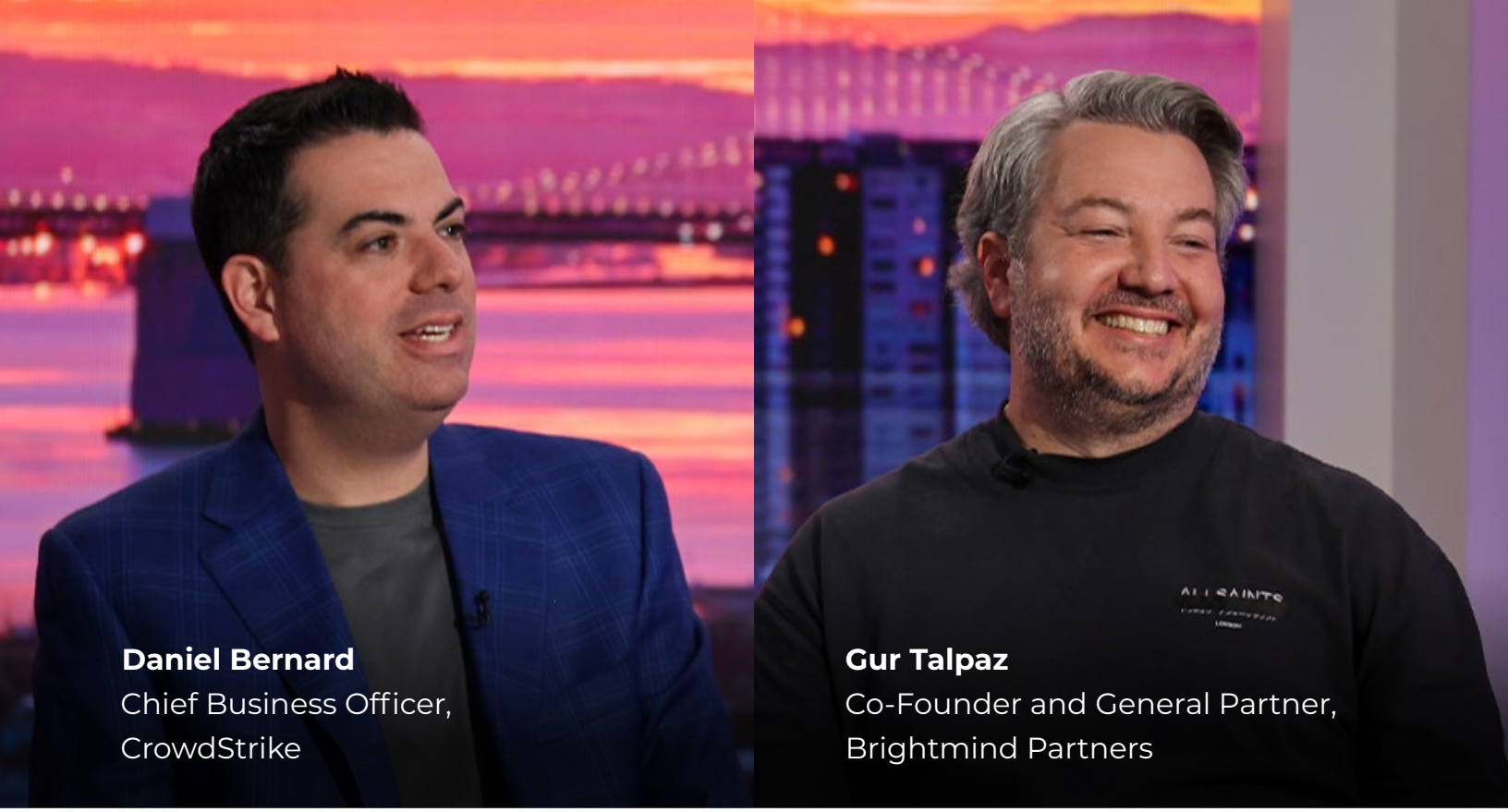
AI is changing how security operations teams function, particularly in how analysts investigate and respond to threats. Ori Barzilay, partner at Team8, says organizations are using AI to improve the effectiveness of analysts, as the volume and complexity of threats continue to increase.

- How CISOs are allocating budgets as time-to-exploit shrinks;
- How AI is creating markets and opportunities in cybersecurity that didn't exist before;
- How AI improves consistency and quality of SOC investigations.

Watch Now

"What we're witnessing now is the major technology shift from the history of software, and there's no other way to bet on the AI-native ones because they're actually designing their products in a much more efficient and accurate way."

- Ori Barzilay



AI Agents Are Redefining Cybersecurity Access Models

CrowdStrike's **Daniel Bernard** and Brightmind's **Gur Talpaz** on Agentic Identity Risk

The rise of an agentic workforce is shattering the trust models that security teams spent a decade building, says Daniel Bernard, chief business officer at CrowdStrike, and Gur Talpaz, co-founder and general partner at Brightmind Partners.

- CrowdStrike's acquisition of SGNL;
- Why SGNL's implementation of continuous, context-aware authorization stood apart from prior approaches;
- Why cybersecurity must evolve to match the pace of agentic adoption.

Watch Now

"Zero standing privileges, continuous real-time authentication - whether they're human beings or they're agentic beings, they have access to what they need, when they need it, in a risk-based, measured approach."

- Gur Talpaz

Where AI Labs Will and Won't Disrupt Cybersecurity

Foundation Capital's **Sid Trivedi** on the Three Markets AI Labs Can't Easily Enter

Artificial intelligenc labs are moving into application security, but three structural barriers define where they won't go, and that's where the next generation of durable security companies will be built, said Sid Trivedi, partner at Foundation Capital.

Watch Now

How to Spot the Real Players in AI Security

Richard Seewald of Evolution Equity Partners on What Drives Real AI Security Success

The next generation of AI security leaders will be defined by their ability to integrate and scale. Richard Seewald, founder and managing partner at Evolution Equity Partners, shares how upsell potential and platform economics help identify companies capable of long-term dominance.

Watch Now

How AI Agents Are Redrawing Enterprise Security Models

Prosperity7's **Abhishek Shukla** on Securing the Full AI Data-to-Model Continuum

Perimeter defense has become obsolete, and as AI agents operate across enterprises with unconstrained access, securing the full data-to-model continuum is the only viable path, says Abhishek Shukla, managing director at Prosperity7 Ventures.

Watch Now

AI-Based Threats Usher in 'Dark Period' for Cyber Defenders

NightDragon CEO **Dave DeWalt** on Perfect Storm of Risks, Attackers and Hybrid Warfare

Cybersecurity has entered a dark phase as AI-powered attackers outpace defense teams. Dave DeWalt of NightDragon outlines how hybrid warfare, critical infrastructure risks and rapid innovation are reshaping global security priorities.

Watch Now

CISOs

Ransomware threats, AI-based attacks, identity management vulnerabilities, phishing, complex ecosystems and nagging questions about ownership and liability: 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.

AI Is Reshaping SOC Speed and Cyber Resilience

Booking Holdings' **Devon Bryan** on Guardrails, Recovery and Making Security Everyone's Job

Cyber defenders can't outpace AI-powered attackers using human effort alone. Deploying AI at machine speed - while keeping humans in the loop for high-stakes decisions - is how organizations stay ahead, says Devon Bryan, global chief security officer at Booking Holdings.

Watch Now

How Attackers Build Scaled Identity Profiles

Andres Andreu of Constella Intelligence on Identity Threats and Scale

Cybercriminals have industrialized identity data into attack-ready profiles at scale. Andres Andreu of Constella Intelligence warns that automation and AI have reshaped how adversaries operate, forcing defenders to rethink strategy and align defenses to attacker behavior.

Watch Now

Why AI Security Investments Fail and How to Fix Them

Amazon.com's **Hudson Thrift** on Using a 10x Framework to Guide AI Bets

Organizations often rush to adopt AI but many fail to deliver meaningful outcomes. Most AI security failures trace back to poor investment decisions, not flawed technology, and fixing that requires a framework built around transformational ROI, says Hudson Thrift, CISO at Amazon.com.

Watch Now

AI Drives Surge in Human-Centric Cyberattacks

Defender **Sarah Gosler** on How Social Engineering Elevates Data Breach Risk

Cyberattacks now target human psychology at scale, reshaping how organizations defend and handle trust, blending social, cyber and psychological tactics to exploit emotion, trust and urgency at the enterprise level, said cyber resiliency and human defense expert Sarah Gosler.

Watch Now

Life and Work After Sitting in the CISO Chair

Meg Anderson of MSA InfoSec on Resilience, AI and the Evolving CISO Role

Nearly two decades as CISO gave Meg Anderson, now president of MSA InfoSec, a long view of how the CISO role has transformed, and what it takes to survive and thrive in it today. "You need to recognize when you're getting close [to burnout]," she said.

Watch Now

Why CISOs Need to Start Taking AI Third-Party Risk Seriously

Keyrock CISO **David Cass** on Managing Agentic AI Risk in Financial Services

As financial institutions accelerate AI adoption, traditional governance models are falling short. David Cass, CISO at Keyrock, explains why organizations must rethink accountability, asset visibility and identity controls to manage emerging risks from LLMs and agentic AI systems.

Watch Now

“I think the people who take advantage of AI to go faster are going to win.”

Jim DuBois
Former CIO and CISO, Microsoft

Why Cyber Resilience Requires Recovery Not Just Backups

Rick Orloff and **Scott Taylor** of Everpure on Cyber Recovery Strategy

Cyber resilience depends on clear recovery priorities and planning. Rick Orloff and Scott Taylor of Everpure explain why firms must define minimum viable business, understand dependencies, and test recovery plans to reduce downtime and limit disruption.

- Asset inventory gaps that delay recovery efforts;
- The importance of testing recovery plans beyond traditional disaster scenarios;
- The need for cross-functional collaboration during cyber incidents.

Watch Now

"You want to focus on getting that minimum viable business or minimum viable company back up and operational, so you're minimizing things like revenue disruption for your organization."

- Scott Taylor

Why Healthcare Faces Rising Risks From Shadow AI

Zscaler's **Ravi Monga** on Managing AI Risks in Clinical Environments

Healthcare organizations are increasingly adopting AI for efficiency and patient care, but governance is lagging behind. Zscaler's Healthcare CISO Ravi Monga explains why visibility into AI usage, including shadow AI, has become the sector's most urgent cybersecurity challenge.

- Why healthcare organizations must move beyond identifying AI risks to actively governing how AI is used, and what that shift looks like in practice;
- The role of zero trust architectures in enforcing governance and protecting sensitive healthcare data;
- How Zscaler is helping customers improve visibility, governance and security in AI deployments.

Watch Now

> **"It is a tale of two speeds. Leadership and governance is talking about AI implementations and AI projects, but at the same time, users are already using it."**
>
> - Ravi Monga

AI Redefines Trust in Global Payments

Visa CISO **Subra Kumaraswamy** on Securing Agents, Fighting Fraud, Protecting Commerce

AI is transforming trust in global payments as attackers scale faster and agents automate decisions. CISO Subra Kumaraswamy explains how Visa uses AI to combat fraud, secure transactions and build trust across consumers, merchants and a rapidly evolving digital ecosystem.

- How AI enables attackers to scale fraud and exploit vulnerabilities faster;
- How autonomous agents expand risk across transactions and systems;
- AI benefits in threat detection, response and proactive defense.

Watch Now

"What has changed in the last three years since ChatGPT is the notion of gen AI and how that is creating different dynamics for both the bad actors and the good guys. So, the way I see it is that AI is enabling the bad actors at scale."

- Subra Kumaraswamy

Why Misaligned Incentives Are the CISO's Biggest Problem

Jim DuBois, Former Microsoft CIO and CISO, on Incentives, AI and Cyber's Future

As AI reshapes cybersecurity, aligning security and innovation teams is more critical than ever. Former Microsoft CIO and CISO Jim DuBois says misaligned incentives create conflict, and fixing that is what lets organizations move fast without compromising security.

- The value of board service in broadening an operator's strategic perspective;
- Why AI will separate high-performing security professionals from the rest;
- The pipeline problem of automating entry-level SOC roles and what the industry must do to address it.

Watch Now

"If we can align those incentives, and we can help the teams that are wanting to innovate be accountable for the security as well as the innovation, then they can go to the security teams and ask for help, as opposed to the conflict when incentives aren't aligned."

- Jim DuBois

Agentic AI Demands a New Identity Strategy

Accenture's **Kris Burkhardt** on Governing Agents, Controlling Access, Managing Risk

Agentic AI is moving faster than traditional identity and access controls can handle. Accenture CISO Kris Burkhardt explains why organizations need a purpose-built strategy for agent identity before selecting tools, and how humans must set the boundaries that agents will operate within.

- Why enterprises must define their agentic identity strategy before selecting tooling;
- How attackers are using agentic AI to manage multiple attack vectors simultaneously and accelerate zero-day exploit deployment;
- Why modernizing technical debt and establishing a fail-fast experimentation culture are prerequisites for secure AI adoption.

Watch Now

> **"Agents also don't have the judgment that you have. If they stumble across data that they shouldn't, they're not going to report it - they're going to use it."**
>
> - Kris Burkhardt

Government Officials

Government agencies are under unprecedented pressure from budget cuts to concerted nation-state campaigns. Geopolitical conflict and political change 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 organizations about their efforts to disrupt cybercriminals, protect critical infrastructure and expand public-private partnerships.

'Cyber Power' Drives Modern Geopolitical Conflict

(Retd.) **Lt. Gen. Rajesh Pant** on Hybrid War, Cyber Deterrence and AI Risks

Cyber conflict has shifted from espionage to geopolitical leverage, with nations using hybrid warfare and AI-driven attacks. Rajesh Pant explains cyber deterrence, global cooperation and how countries can build cyber power to defend critical infrastructure and influence outcomes.

Watch Now

How Prompt Injection Attacks Undermine AI Guardrails

Apostol Vassilev of NIST on Why LLM Defenses Always Fall Short

Large language models are inherently vulnerable to prompt injection attacks, and no finite set of guardrails can fully protect an LLM from adversarial prompts. Apostol Vassilev, research team supervisor at NIST, explains why organizations must change their focus from prevention to resilience.

Watch Now

Dismantling the Business of Cybercrime at Scale

Interpol's **Neal Jetton** on Targeting Platforms, Not Just Perpetrators

Arresting bad actors isn't enough. Neal Jetton, director of cybercrime at Interpol, makes the case for targeting the platforms and infrastructure that allow cybercriminal organizations to operate as an industry worldwide.

Watch Now

Cybercrime Disruption Demands Global Trust and Coordination

UK Cyber Official **Paul Foster** on Cross-Border Takedowns, New Disruption Playbook

Dismantling cybercrime groups requires more than technical capability. It demands trust, coordinated strategy and cross-border collaboration, says Paul Foster, head of the National Cyber Crime Unit at the U.K.'s National Crime Agency.

Watch Now

Congress Confronts Cyber Workforce, AI Risks

Congressional Staffer **Graham Harwood** on Federal Gaps, Data Security, AI Oversight

Congress faces rising cyberthreats, workforce shortages and AI-driven risks as it shapes policy in 2026. Congressional staffer Graham Harwood outlines concerns about federal capability, data protection and oversight to secure critical systems and public services.

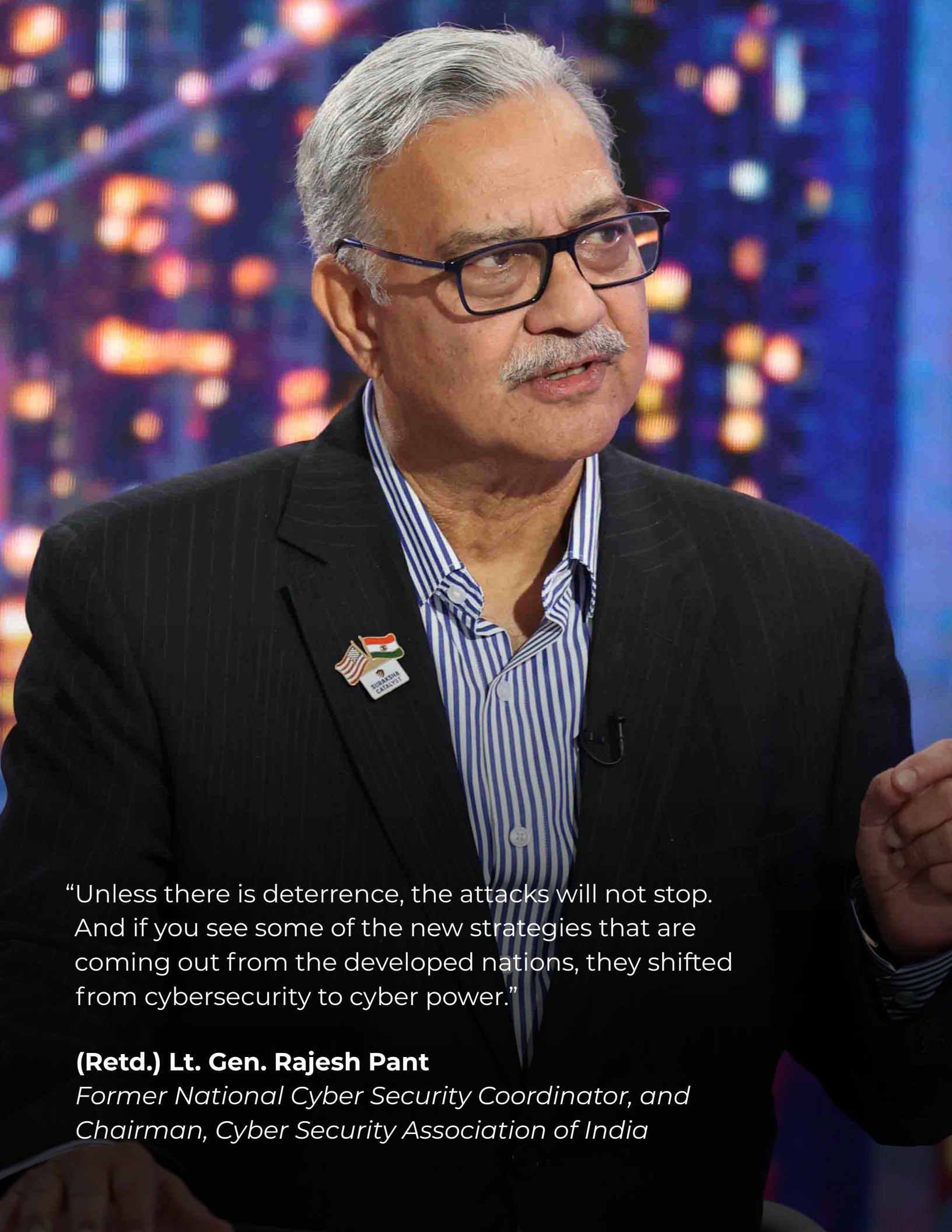
Watch Now

How EU Plans to Improve Its Global Cyber Ecosystem

ECCC Executive Director **Luca Tagliaretti** on Securing Europe's Digital Future

The European Cybersecurity Competence Centre has mobilized more than 1.1 billion euros, or more than $1.2 billion, to build Europe's cyber resilience. ECCC Executive Director Luca Tagliaretti outlines how AI, quantum and critical infrastructure protection define the bloc's strategic priorities.

Watch Now



“Unless there is deterrence, the attacks will not stop. And if you see some of the new strategies that are coming out from the developed nations, they shifted from cybersecurity to cyber power.”

(Retd.) Lt. Gen. Rajesh Pant
Former National Cyber Security Coordinator, and Chairman, Cyber Security Association of India

How Europe Is Building Its Cyber Resilience

ENISA's **Hans de Vries** on DDoS, Security Training and Road to Single Reporting Platform

Europe's cybersecurity posture is hardening, but the threat landscape is evolving faster, says Hans de Vries, chief cybersecurity and operations officer at ENISA. From supply chain disruptions to ransomware legislation, the pressure to build genuinely resilient societies has never been greater.

- Why cross-border member state cooperation has improved markedly over the past decade;
- ENISA's ambitions to become a top-level root CNA and potentially a last-resort CVE authority;
- The agency's plans for Cyber Europe 2026, the single reporting platform and the European digital wallet.

Watch Now

> **"It's not only about detecting and response. A lot of stuff is about preventing."**
>
> - Hans de Vries

“Today, agentic AI performing cyberattacks from beginning to end on its own is quite phenomenal.”

Despina Spanou
Director General, Communications Networks and Technology, European Commission

Global Cybercrime Investigations Gain Ground

Stan Duijf of Dutch National Police on Collaborative Law Enforcement

Global law enforcement agencies are shifting tactics to disrupt ransomware earlier in the attack chain. Stan Duijf of the Dutch National Police describes how collaboration, threat intelligence and cryptocurrency seizures are making cybercrime more costly and less effective for criminals.

Watch Now

National Cyber Resilience Demands Unified Defense

UK NCSC's **Richard Horne** on Strengthening Cyber Defense and Incident Response

Cyber risk is rising as digital dependence grows and threat actors expand. NCSC CEO Richard Horne outlines why leaders must treat cybersecurity as mission-critical, strengthen their resilience, and align defense efforts to counter ransomware, AI-driven threats, and supply chain attacks.

Watch Now

Global Cybersecurity Cooperation Lacks a Systemic Framework

European Commission's **Despina Spanou** on Building a Like-Minded Global Alliance

The European Union has spent more than a decade building a unified security framework across 27 nations. But a systemic global framework for like-minded cooperation still doesn't exist, says Despina Spanou, deputy director general, European Commission.

Watch Now

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 in an uncertain market.

Multi-Cloud Security Is Straining CISO Teams

451 Research's **Daniel Kennedy** on How Skills Gap, Tool Sprawl Intensify Cloud Security Risk

Cloud security and gen AI governance are stretching security teams thin, warned Daniel Kennedy, principal research analyst at 451 Research, S&P Global Market Intelligence. Organizations now manage several cloud environments at once - each adding new risk and increasing the burden on security teams.

Watch Now

The Five Most Dangerous New Attack Techniques

SANS' **Ed Skoudis** on Emerging AI Threats and How Defenders Can Respond

Organizations are "completely unprepared for 100 critical vulnerabilities in a week," said Ed Skoudis, president of the SANS Technology Institute, pointing to a near-term scenario where AI dramatically increases the discovery and exploitation of software flaws.

Watch Now

How ‘Secure by Demand’ Can Reset Cybersecurity

Lauren Zabierek of CAS Strategies on Addressing Incentives and Risk Gaps

Software risk continues to outpace public understanding as insecure defaults persist. Lauren Zabierek of CAS Strategies and the Institute for Security and Technology explains what drives weak security outcomes and how a “secure by demand” approach can push markets toward safer products.

Watch Now

How AI Is Reshaping Identity Theft Risk

James E. Lee of the Identity Theft Resource Center on Tackling New Threats

AI is transforming identity theft, scams and data breaches at scale. James E. Lee, president of the Identity Theft Resource Center, explains why old scam signals fail, why machine identities raise new risks, and how organizations must rethink protection and victim support.

Watch Now

Why Investors Question Cybersecurity Growth in the AI Era

Fatima Boolani of Citi on Why AI Isn’t Driving Expected Cyber Budget Growth

Cybersecurity stocks have long been a safe haven for investors, but AI’s failure to drive measurable budget growth is now testing that status. Fatima Boolani of Citi breaks down the disconnect and why strong earnings aren’t translating into higher stock values.

Watch Now

AI Drives New Cyber Defense Models in Retail

ISAC’s **Pam Lindemoen** on How Intel Sharing Is Critical for Sector-Wide Protection

AI-driven threats force industries to adopt collective cyber defense. Pam Lindemoen outlines how intelligence sharing, actionable data and automation help retail and hospitality organizations reduce fraud, detect phishing and respond faster to evolving cyber risks.

Watch Now

AI Disruption Fears Rattle Cybersecurity Stocks

J.P. Morgan's **Brian Essex** on Why Valuations Drop as Fundamentals Hold Steady

Investor anxiety over AI's long-term impact is dragging down stock valuations despite steady growth and profitability, while companies focus on long-term valuation assumptions and secure business models, says J.P. Morgan's Brian Essex.

- How generative AI is accelerating innovation while raising investor concerns about sustainability;
- Why established platform vendors are better positioned than smaller players to adapt to AI disruption;
- How AI-driven threats and expanding attack surfaces are increasing demand for cybersecurity tools.

Watch Now

"It's not about disruption this year or even 14 to 18 months from now - it's all about whether, longer term, these business models will still be viable given the disruption we're seeing."

- Brian Essex

Why Cybersecurity's Uncertainty Problem Is Getting Worse

Cryptography Researcher **Paul Kocher** on AI's Threat to Security's Edges

Independent cryptography researcher Paul Kocher said cybersecurity is entering a period of deep uncertainty. AI is accelerating vulnerability discovery at a pace defenders cannot match, giving attackers a structural edge even when both sides use the same tools.

- Why quantum computing's threat to public key cryptography remains genuinely unresolved among leading experts;
- How AI-driven traffic analysis can defeat cryptographic security goals without breaking any algorithm;
- Why cuts to U.S. research funding are undermining the innovations needed to defend against an increasingly uncertain threat landscape.

Watch Now

"I think of cryptography as these golden, perfect bricks that you can try to build things with, but all the mortar in between and the pieces around them aren't as robust, and AI can really chip away at those edges much more effectively than humans can."

- Paul Kocher

Global Cybersecurity in 2026: The Case for Convergence

WEF's **Akshay Joshi** on AI Risks, Geopolitics and the Growing Cyber Divide

Security leaders can no longer address AI, geopolitics, supply chains and workforce gaps in isolation, as convergence across these forces is contributing to the complexity of the cybersecurity landscape, says Akshay Joshi of the World Economic Forum.

- Why the agentic era can't advance without cybersecurity at its core;
- How geopolitical resets are expanding resilience thinking beyond individual organizations to subsea cables and hyperscaler environments;
- How AI could democratize access to cybersecurity tools for underserved organizations.

"Rapid advances in AI, coupled with a complex geopolitical backdrop and new supply chains being forged at breakneck speed - all of these have very real ramifications on cybersecurity."

- Akshay Joshi

Watch Now

"We haven't seen realizable growth in those budgets. We've definitely seen an uptick in budgetary growth, but it's not an order of magnitude better, as you would maybe expect with AI being a vector that's consequentially changing the attack profile or the attackable surface of the average organization."

Fatima Boolani
Managing Director and Co-Head,
U.S. Software Equity Research, Citi

AI Is Redrawing the Cybersecurity Vendor Landscape

Morgan Stanley's **Meta Marshall** on Where AI Will Disrupt Cybersecurity Markets

AI adoption in cybersecurity is still largely consumer-driven, but real growth depends on enterprise deployment. Meta Marshall, managing director at Morgan Stanley, explains what's holding back adoption, where AI can deliver value and which security segments are most defensible.

- Why security concerns and innovation overload are the two biggest inhibitors of enterprise AI adoption;
- How AI adoption mirrors the early consumer-to-enterprise arc of cloud computing;
- Why identity security vendors must innovate to address non-human identities or risk being replaced.

Watch Now

> **"There is always going to be best of breed. Platformization means getting to 20 or 30 vendors from 50 or 60 vendors. It doesn't mean going to one or two."**
>
> - Meta Marshall

How History Shapes Nation-State Cyber Conflict

Forrester's **Allie Mellen** on Geopolitics and the Digital Battlefield

Cyberattacks have become fully integrated into multi-domain warfare. Allie Mellen, author and principal analyst at Forrester, argues that understanding the histories of China, Russia and the U.S. is essential to understanding why each nation fights the way it does in cyberspace.

- How the Gulf War information operations laid the groundwork for today's cyber-integrated battlefield;
- How the surge in global conflicts is making cyberattacks increasingly central and unpredictable;
- Why the 19th-century U.S. electoral fraud called "cooping" drove voting infrastructure reforms.

Watch Now

"What I hope people will take away from this book is lessons as to what is going to lead to cyberattacks, why they would target certain organizations and exactly how integrated we now see cyberattacks as part of multi-domain warfare."

- Allie Mellen

How AI Is Reshaping the Cybersecurity Vendor Landscape

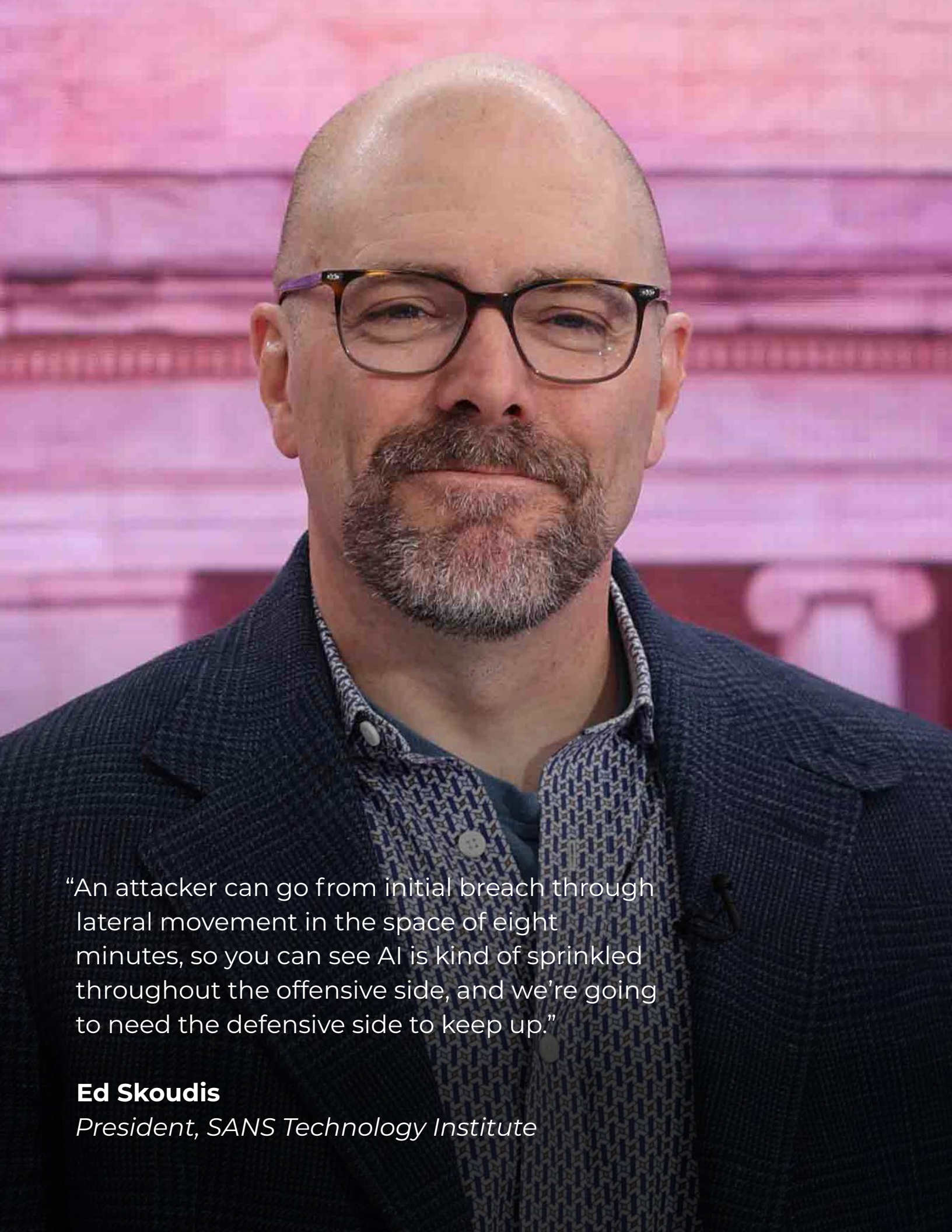
IT-Harvest's **Richard Stiennon** on Why SOC Automation Is Just the Beginning

The cybersecurity vendor landscape is being rebuilt around AI, and the transformation is moving faster than most organizations are prepared for. Richard Stiennon, chief research analyst at IT-Harvest, explains where the market is heading and why CISOs can't afford to wait.

- How model protection evolved from a niche offering into a broad enterprise requirement;
- What CISOs should consider when evaluating AI security vendors;
- Why by RSAC Conference 2027, AI will no longer be a distinct vendor category.

Watch Now

> **"AI is here and it is good. Even if you feel it's not good enough, it's going to be twice as powerful two and a half months from now."**
>
> - Richard Stiennon



"An attacker can go from initial breach through lateral movement in the space of eight minutes, so you can see AI is kind of sprinkled throughout the offensive side, and we're going to need the defensive side to keep up."

Ed Skoudis
President, SANS Technology Institute

Behind the Scenes of ISMG Studio at RSAC 2026

ISMG, a media sponsor team at RSAC Conference 2026, conducted video interviews with top leaders in cybersecurity, information security, AI, risk management and data privacy. Here's a look at the team behind the scenes.

ISMG.Studio interviewed more than 150 cybersecurity leaders and practitioners at RSAC Conference.

The ISMG editorial team breaks down events of the day during the conference.

Brian Essex, executive director of U.S. Software Equity Research at J.P. Morgan

CyberTheory Director Julie Jordan, ISMG General Manager Mike D'Agostino and CyberTheory Lead Graphic Designer Caitlin Persichilli

ISMG's Elisha King, European Commission's Despina Spanou, ISMG's Anna Delaney, European Commission's Christiane Kirketerp de Viron and ISMG's Katie Hinderliter

Above, ISMG Corporate Development Vice President Shane Penner, ISMG CEO Sanjay Kalra, former Microsoft CIO and CISO Jim DuBois, ISMG Vice President of Community Engagement Rahul Neel Mani, ISMG General Manager Mike D'Agostino and ISMG Chief Collaboration Office David Elichman

Above right, Interpol's Neal Jetton wraps up an interview with ISMG's Rahul Neel Mani.

Right, ISMG Senior Vice President Tom Field prepares for a day at the studio.

ISMG CEO Sanjay Kalra, Google Data Protection Officer Kristie Chon Flynn and ISMG Senior Vice President Tom Field

Zscaler Chief Technology Evangelist Brian Deitch and ISMG's Anna Delaney

Chloe Ryan, Deputy Director, Events and ISMG Studio, and David Elichman, ISMG Chief Collaboration Officer

Above, ISMG Founder and CEO Sanjay Kalra chats with Zscaler Founder, Chairman and CEO Jay Chaudhry.

Right, ISMG's Sanjay Kalra, YL Ventures Senior Partner Ofer Schreiber and ISMG's Michael Novinson

ISMG Strategic Accounts Vice President Mark D'Agostino , ISMG General Manager Mike D'Agostino, ISMG Global Strategic Account Director Caterina Bastianello and ISMG Chief Collaboration Officer David Elichman

Above, Menlo Ventures Partner Rama Sekhar and ISMG Executive Director of Productions Anna Delaney wrap up an interview.

Left, ISMG Corporate Development Vice Presidents Jonathan Mathew and Shane Penner

ISMG CEO Sanjay Kalra, Ten Eleven Ventures Founder and Managing General Partner Alex Doll and ISMG Business Executive Editor Michael Novinson

Delinea CEO Art Gilliland in an interview with Mathew J. Schwartz, executive editor of DataBreachToday and Europe

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

Right, Priya Shetty, associate director and head of global marketing services for ISMG APAC marketing, and Shradha Bhardwaj, head of ISMG APAC events and project management

Above: Barracuda CEO Rohit Ghai and ISMG CEO Sanjay Kalra

Right: ISMG CEO Sanjay Kalra and SYN Ventures Investment Committee Chair Art Coviello

ISMG Founder and CEO Sanjay Kalra and Netskope Co-Founder and CEO Sanjay Beri

ISMG CEO Sanjay Kalra, ISMG Business Executive Editor Michael Novinson and Cisco President and Chief Product Officer Jeetu Patel

We'll see you at RSAC Conference 2027!

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

ISMG Studio

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

BANK INFO SECURITY® CAREERS INFO SECURITY® HEALTHCARE INFO SECURITY®

GOV INFO SECURITY® infoRisk TODAY® CU Just for Credit Unions INFO SECURITY Data Breach Prevention. Response. Notification. TODAY AIToday.io

OT.today PaymentSecurity.io FraudToday.io DeviceSecurity.io CIO.inc

CyberEd.io CyberEdBoard CXO ADVISOR CYBER THEORY Xtra mile LIFECYCLE MARKETING ATHENA

QC MEDIA SUMMIT custom events roundtables NULLCON hardwear.io Hardware Security Conference and Training ISMG Studio

ISMG

902 Carnegie Center • Princeton, NJ • 08540 • ismg.studio