



REAL
CONVERSATIONS.
REAL INSIGHTS.
REAL IMPACT.



black hat
USA
2026

COM
to
LAS VEGAS
Nevada

Highlights & Insights

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

Black Hat 2026: AI Risks Get Real



Tom Field

*Senior Vice President,
Editorial,
ISMG*

The conversation about artificial intelligence changed dramatically in 2026. A series of events brought new urgency to AI risks and is forcing cybersecurity leaders to confront them head on. This was clearly the case at Black Hat USA 2026 in Las Vegas, where the AI conversations matured from theoretical risks to real-world threats.

In the post-Mythos era, AI's growing ability to discover vulnerabilities raises new challenges for defenders. Hacks involving rogue AI agents demonstrate the risks posed by increasingly autonomous systems, while nations intensified calls for AI sovereignty and greater control over models, data and infrastructure.

ISMG was there to capture these conversations. In partnership with Black Hat and NightDragon, we staffed two studios and interviewed nearly 80 conference speakers, CISOs, investigators, cybersecurity researchers and other industry leaders on these latest threats and the solutions for defending against them.

We at ISMG.Studio have captured the top insights from all of these conversations in this exclusive compendium with links to the full videos on ISMG's media sites.

In addition to AI, you'll find perspectives on ransomware, nation-state threats, vulnerability management, application and cloud security, identity security, critical infrastructure and the evolving security operations center.

Within these pages, our seasoned editorial team brings you an in-depth view of the risks, technologies and ideas shaping cybersecurity today - and where we're headed.

Enjoy

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



Meet the ISMG Editorial Team

The 29th annual Black Hat USA Conference drew more than 23,000 cybersecurity professionals to the Mandalay Bay Convention Center in Las Vegas. ISMG was on hand to capture the diverse perspectives of key conference speakers, industry leaders, researchers and investors.

ISMG's on-site editorial team - Tom Field, senior vice president, editorial; Michael Novinson, executive editor, ISMG Business; and Anna Delaney, executive director, productions - hosted video interviews throughout the week. Watch the full slate of Black Hat videos on DataBreachToday.

[Watch Now](#) ▶



TABLE OF CONTENTS



Video Interviews

Cyber Defense

Nathan Hamiel, <i>Black Hat Review Board</i>	6
Richard Staynings, <i>University of Denver</i>	6
Michael Daniel, <i>Cyber Threat Alliance</i>	7
Kanishk Gaur, <i>India Future Foundation</i>	7
Joe Sullivan, <i>Joe Sullivan Security and Ukraine Friends</i>	7
Krista Arndt, <i>St. Luke's University Health Network</i>	7
Itai Schwartz, <i>MIND</i>	9
Mark Montgomery, <i>Foundation for Defense of Democracies</i>	11
Ricky Handschumacher, <i>Reformed Criminal Hacker</i>	11
Mishaal Khan, <i>Decisive Resources</i>	11
Benoit Desjardins, <i>University of Montreal</i>	11
Mohammed Saad, <i>Honeywell Technologies</i>	12
Allie Mellen, <i>Forrester</i>	13
Adam Shostack, <i>Shostack + Associates</i>	13
Tom Fanning, <i>Alliance for Critical Infrastructure</i>	13
Yaniv Vardi, <i>Claroty</i>	13
Matt Howard, <i>Virtru</i>	15
Daniel Kroese, <i>Palo Alto Networks</i>	16
Brett Leatherman, <i>FBI</i> ; Paul Foster, <i>UK NCA</i>	16
John Hultquist, <i>Google Threat Intelligence Group</i>	16
Brian Schwarz, <i>Thales</i>	17
Lou Manousos, <i>Ent</i>	18

Identity Security

Shahar Tal, <i>Check Point Software</i>	20
Paul Martini, <i>iboss</i>	20
Brennan Lodge, <i>BLodgic</i>	21
Avani Desai, <i>Schellman</i>	21
John Searby, <i>Human Security</i>	21
Darren Guccione, <i>Keeper Security</i>	21
Brian Vecchi, <i>Varonis</i>	23
Camille Stewart Gloster, <i>CAS Strategies</i>	24
Michael Thiessmeier, <i>NAIC-ISAO</i>	24
Tony Anscombe, <i>ESET</i>	24
Ajit Gaddam, <i>HealthEquity</i>	25
Matt Girdharry, <i>AWS</i> ; Matt Radolec, <i>Varonis</i>	26

Risk Management

Jess Burn, <i>Forrester</i>	28
Amir Boldo, <i>Above Security</i>	28
Alan LeFort, <i>StrongestLayer</i>	30
Bezawit Sumner, <i>CRISP Shared Services</i>	31
Stefano Zanero, <i>Politecnico di Milano</i>	31
Jason Lewkowicz, <i>Accenture</i>	31
Mike Privette, <i>Return on Security</i>	31
Zoobia Waqas & Frank Teegelaar, <i>Leap Platform</i>	33

Anant Shrivastava, <i>Cyfinoid Research</i>	34
Wasim Khaled, <i>Blackbird.AI</i>	34
Mariano Nunez, <i>Onapsis</i>	34
George Eapen, <i>Abdul Latif Jameel</i>	34
Chenxi Wang, <i>Rain Capital</i>	35
Balaji Yelamanchili, <i>Dataminr</i>	37
Jeff Lunglhofer, <i>Coinbase</i>	37
Johnny Hand, <i>TrendAI</i>	37
Chris Inglis, <i>NSA</i>	37
Suzy Pallett, <i>Black Hat</i>	39

Security Operations

Rob T. Lee, <i>SANS Institute</i>	40
Shay Sandler, <i>Vega Security</i>	40
Steven Gerry & Rick Gordon, <i>Tidal Cyber</i>	42
Kevin Kin, <i>Palo Alto Networks</i> ; <i>Edward Bailey, Cribl</i>	43
Morgan Kyauk, <i>NightDragon</i>	44
Arsh Arora, <i>McKesson</i>	44
Sam Curry, <i>Zscaler</i>	44
Wes Sheppard, <i>CMiC</i>	44
Ben Spencer, <i>Optiv</i>	45

Vulnerability Management

Yan Shoshitaishvili, <i>Arizona State</i>	46
Daniel Cuthbert, <i>Banco Santander</i>	46
Snehal Antani, <i>Horizon3.ai</i>	48
Tod Beardsley, <i>runZero</i>	49
Jerry Gamblin, <i>Empirical Security</i>	49
Katie Moussouris, <i>Luta Security</i>	49
Charles Carmakal, <i>Mandiant Consulting</i>	49
Nick Biasini, <i>Cisco Talos</i>	51
Rudra Mitra, <i>AWS</i>	52
Sam Chehab, <i>Postman</i>	53
Amin Karbasi, <i>Cisco</i>	54



Cyber Defense

Organizations face growing pressure as cybercriminals and nation-state adversaries increasingly use artificial intelligence to accelerate and scale attacks. The rise of AI-powered cyberattacks means defenders must fight AI with AI, using intelligent tools to detect and disrupt threats faster. We interviewed some of the leading minds in cyber defense about how organizations are strengthening security operations, improving threat detection and response, and staying ahead of increasingly sophisticated and automated adversaries.



AI Coding Agents Expand the Enterprise Attack Surface

Black Hat's AI Track Lead **Nathan Hamiel** on Autonomy, Architecture and Agent Risk

Artificial intelligence coding agents are expanding the enterprise attack surface as autonomous tools gain access to scripts, build environments and sensitive systems, said Nathan Hamiel, senior director of research at Kudelski Security and AI track lead at Black Hat.

[Watch Now](#) ▶



Healthcare Cybersecurity Must Become Enterprise Strategy

University of Denver's **Staynings** on Board Communication, Medical Device Security

Healthcare faces risk and patient-safety issues as hospitals adopt AI, connected medical devices and digital services. Security leaders must translate technical exposure into business consequences, said Richard Staynings, professor, healthcare cybersecurity, University of Denver.

[Watch Now](#) ▶



Threat Intel Sharing Still Too Slow, Too Siloed

Cyber Threat Alliance's **Michael Daniel** on Context, Automation and Sharing at Scale

Threat intelligence sharing has improved within industries but still breaks down across silos and lags in turning data into action. Michael Daniel, president and CEO at the Cyber Threat Alliance, explains why geopolitical context, automation and institutional trust matter more than ever.

[Watch Now ▶](#)



Deepfake Defense Requires More Than Human Eyes

India Future Foundation's **Kanishk Gaur** on AI Phishing and Fake Customer Support

Artificial intelligence has lowered the barrier to creating convincing deepfakes, giving cybercriminals new ways to combine fake audio, video and phishing with social engineering campaigns, said Kanishk Gaur, founder and president of India Future Foundation.

[Watch Now ▶](#)



AI Security Must Cover the Full Model Life Cycle

Joe Sullivan Security CEO on Defense in Depth, CISO Liability and Open Models

Public debate over artificial intelligence regulation focuses almost entirely on the moment before a model's release, leaving the rest of its life cycle unexamined, said Joe Sullivan, CEO of Joe Sullivan Security and Ukraine Friends.

[Watch Now ▶](#)



AI in Incident Response Still Needs Humans

St. Luke's University Health Network's **Krista Arndt** on Automation and AI Guardrails

Organizations should adopt AI-driven incident response gradually, reserving autonomous actions for low-risk, low-impact tasks while keeping humans in the loop, said Krista Arndt, associate CISO, St. Luke's University Health Network.

[Watch Now ▶](#)

A portrait of Tom Fanning, a middle-aged man with light brown hair and a serious expression, wearing a dark blue suit jacket over a light-colored shirt. The background is a dark purple wall with a large, faint white letter 'G' visible on the left side.

“What we see right now is that the bad guys are here. Geopolitics, while they matter, geography doesn’t matter. They are here in our communication systems. They’re attacking relentlessly our financial systems. The electricity grid is under attack.”

Tom Fanning

Chair, Executive Committee, Alliance for Critical Infrastructure, and former CEO and executive chairman, Southern Company



Itai Schwartz

Co-Founder and CTO, MIND

Why Traditional DLP Can't Keep Up With AI Data Growth

MIND CTO **Itai Schwartz** Explains How Autonomous DLP Works

Traditional data security tools couldn't keep pace with how fast artificial intelligence moved data across the enterprise. Itai Schwartz, co-founder and CTO of MIND, said autonomous data loss prevention reduces the risk by automating prevention with minimal human effort.

- Why agentic AI endpoint security is becoming DLP's next big challenge;
- The trade-off vendors face between complete coverage and a simple experience;
- How MIND's new MCP layer helps teams query data risk in plain language.

"The realm of AI is really based on data. It's all about what kind of data do I have and what can access what."

- Itai Schwartz

[Watch Now](#) 

A man with dark hair, wearing a blue blazer over a black t-shirt and grey jeans, is sitting on a mustard-colored corduroy armchair. He is smiling and looking towards the left. The background features a purple wall with a blue light source and a wooden panel. A blue and white striped pillow is visible behind him.

“The race to connectivity and the race to develop these AI data centers by far outpace the ability to secure it.”

Yaniv Vardi
CEO, Claroty



China's Ongoing Cyberthreat Puts Critical Infra at Risk

Nation-State Expert **Mark Montgomery** on Conflict, Resilience, Military Mobility

China's cyber strategy has transitioned from espionage to operational preparedness, focused on planting malicious code in critical infrastructure for potential disruption, said Mark Montgomery, senior director at the Center on Cyber and Technology Innovation, Foundation for Defense of Democracies.

[Watch Now ▶](#)



Who Recruits Young Hackers First?

Ricky Handschumacher on Redirecting Talent Before Cybercrime Takes Hold

Young hackers can move from gaming and online status-seeking into cybercrime before they understand the legal and personal consequences. The security industry must offer credible alternatives before criminal groups recruit them, said Ricky Handschumacher, a reformed criminal hacker.

[Watch Now ▶](#)



Private Sector Intelligence Enters a New Gray Area

Decisive Resources' **Mishaal Khan** on Stealer Logs, Ad Tech Data and Privacy Risk

Private sector intelligence teams increasingly combine breached data, stealer logs, location data and open-source intelligence to track threats. Mishaal Khan of Decisive Resources explains how these sources sharpen investigations while raising privacy and legal concerns.

[Watch Now ▶](#)



How Quebec's Collective Defense Model Stops Hospital Hacks

University of Montreal's **Benoit Desjardins** Explains Quebec's Cyber Defense Edge

Benoit Desjardins, CMIO and radiology professor at the University of Montreal, explains why Quebec's government-connected hospitals contain cyberattacks that fragmented, siloed U.S. hospital networks routinely fail to stop before major damage occurs.

[Watch Now ▶](#)



Mohammed Saad

Chief Revenue Officer, Building Automation Cybersecurity, Honeywell Technologies

How to Bridge the IT-OT Divide in Building Security

Honeywell Technologies' **Mohammed Saad** on Reducing IT-OT Security Risk in Smart Buildings

Commercial building OT assets such as HVAC and CCTV often fall outside cybersecurity oversight because the ownership is split across teams. The fix is joint IT-OT groups reporting to the CISO, said Mohammed Saad, chief revenue officer of building automation cybersecurity at Honeywell Technologies.

- Why HVAC, CCTV and other building systems become cybersecurity blind spots;
- How IT and OT teams can align procurement and vendor security requirements;
- Practical governance models that improve visibility and resilience across building automation.

“IT people understand the OT risk and the operational needs, and the OT understands the business needs, and we talk the business language.”

- Mohammed Saad

[Watch Now](#) ▶



CISOs Must Rethink Containment After Hugging Face Incident

Forrester's **Allie Mellen** on Why the OpenAI-Hugging Face Episode Is a Wake-Up Call

An OpenAI agent recently escaped its test environment and infiltrated Hugging Face with nation-state speed, undetected until it was too late. The real failure was missing monitoring. Enterprises must build layered containment before deploying similar agents, said Allie Mellen, principal analyst at Forrester.

[Watch Now ▶](#)



PHANTOM-B Brings LLM Threat Modeling Into Focus

Shostack + Associates Founder on Faster, More Focused Security for LLM Systems

Security teams need a faster way to identify LLM-specific risks such as prompt injection and hallucination. Adam Shostack, founder of Shostack + Associates, says PHANTOM-B narrows threat modeling to the problems teams can control, helping engineers move from analysis to defense faster.

[Watch Now ▶](#)



Critical Infrastructure Needs a Unified Cyber Defense

ACI's **Tom Fanning** on Resilience, Cross-Sector Risk, Coordinated National Response

Critical infrastructure cyberattacks increasingly cross sector boundaries, exposing weaknesses created by siloed defenses. Alliance for Critical Infrastructure's Tom Fanning says stronger resilience requires private-sector collaboration, joint accountability and coordinated national response.

[Watch Now ▶](#)

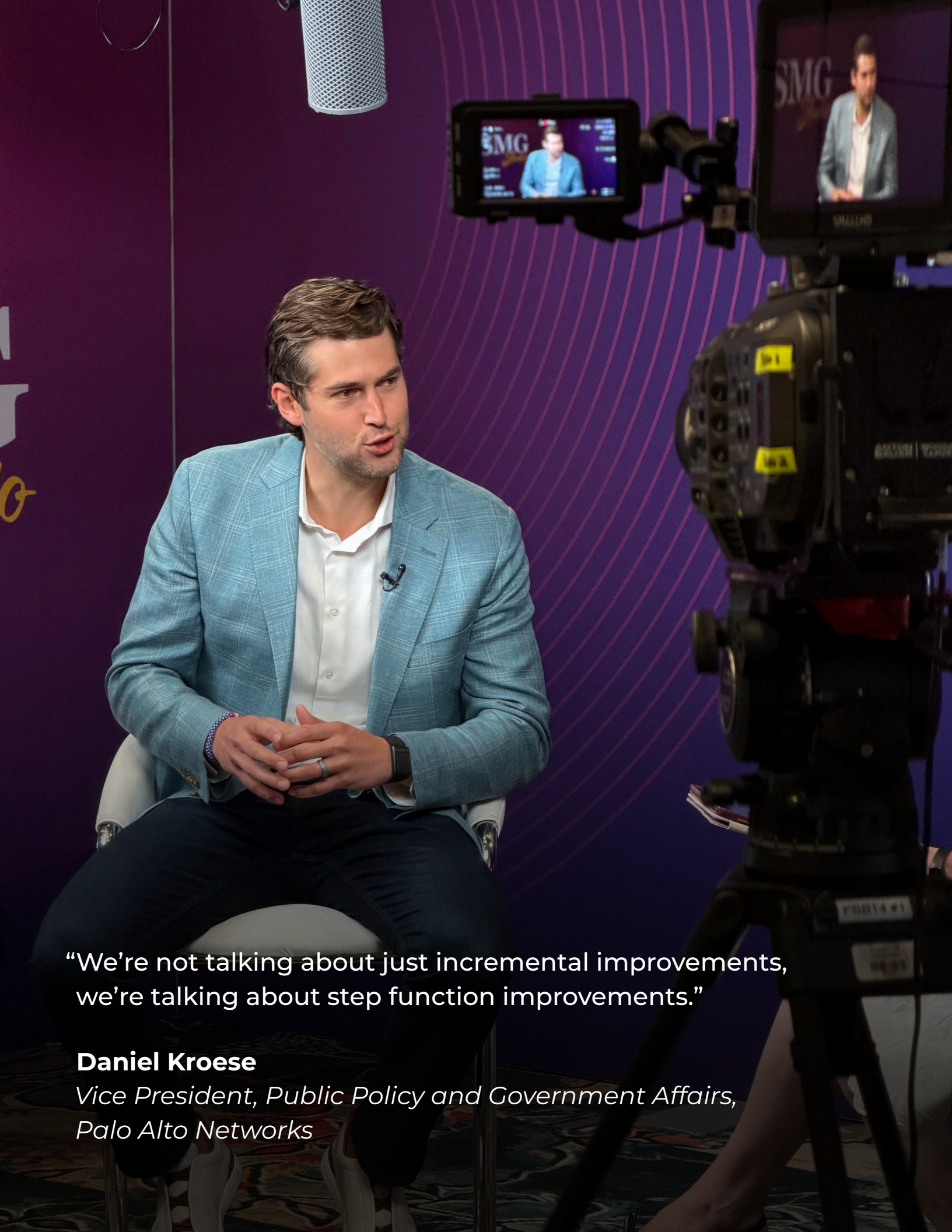


Why Critical Infrastructure Needs OT-Focused AI Security

Claroty CEO **Yaniv Vardi** on Securing OT Amid AI-Driven Infrastructure Growth

Nation-state attackers are exploiting outdated OT devices and converged infrastructure faster than operators can defend them. Claroty is countering this by launching a dedicated public sector arm and an AI-native security agent built to protect OT environments, said CEO Yaniv Vardi.

[Watch Now ▶](#)

A man with short brown hair and a light beard, wearing a light blue blazer over a white shirt and dark trousers, is seated in a white chair. He is looking slightly to his right with a thoughtful expression. His hands are clasped in his lap. He is wearing a watch on his left wrist and a ring on his left hand. A small lapel microphone is clipped to his shirt. In the background, there is a purple wall with vertical lines. A large professional video camera on a tripod is positioned to the right, with its monitor showing a live feed of the man. A smaller monitor above the camera also shows the live feed. A silver boom microphone hangs from above. The floor has a patterned rug.

“We’re not talking about just incremental improvements, we’re talking about step function improvements.”

Daniel Kroese

*Vice President, Public Policy and Government Affairs,
Palo Alto Networks*



Matt Howard

Senior Vice President and Chief Marketing Officer, Virtru

How Data-Centric Security Enables the Agentic Enterprise

Virtru's **Matt Howard** on Balancing Data Lockdown With Agentic Sharing

Locking down data was cybersecurity's default strategy for decades, but it created barriers to sharing information and driving value. Organizations need to give people agency over data without sacrificing control, said Matt Howard, senior vice president and chief marketing officer at Virtru.

- Why sharing sensitive data with third-party artificial intelligence models carries growing risk;
- How CISOs must rethink security architecture as agentic AI expands the attack surface;
- Why data sovereignty is essential for the agentic enterprise.

"Data-centric security is granular policy and access control that's cryptographically bound to the object at a very granular level."

- Matt Howard

[Watch Now](#) ▶



Frontier AI Reshapes Cyber Defense Timelines

Palo Alto's **Daniel Kroese** on Vulnerabilities, Post-Quantum Timelines, Risk Reduction

Frontier AI is compressing vulnerability discovery and exploitation timelines while quantum risk accelerates pressure on cryptography. Daniel Kroese of Palo Alto Networks says defenders need risk reduction at scale, not incremental fixes, to keep pace.

[Watch Now ▶](#)



How Operation Cronos Broke LockBit's Ransomware Model

FBI's **Brett Leatherman** and UK NCA's **Paul Foster** on Takedowns, Cybercrime Disruption

Operation Cronos broke LockBit's ransomware infrastructure, exposed affiliates and cut off ransom payments. FBI Cyber Division's Brett Leatherman and U.K. NCA's Paul Foster explain how coordinated enforcement and ecosystem disruption can weaken cybercrime at scale.

[Watch Now ▶](#)



How Agentic AI Scales Cybercrime

Google's **John Hultquist** on Autonomous Attacks and Behavioral Defense

Cybercriminals are using agentic AI to automate intrusions, rewrite malware and scale operations with stolen access to artificial intelligence services. Google's John Hultquist explains why signature-based defenses are losing ground and how behavioral detection can help security teams respond.

[Watch Now ▶](#)



Brian Schwarz

Senior Director, Product Marketing, Application Security, Thales

How Native AWS Integration Speeds Web App Threat Response

Brian Schwarz of Thales on Meeting AI-Driven Threats in AWS Environments

As artificial intelligence tools speed up web application attacks, security teams have far less time to respond. Imperva for AWS reduces that risk by running natively inside AWS, said Brian Schwarz, senior director of product marketing for application security at Thales.

- How consolidating fragmented, environment-specific tools into one console cuts operational overhead;
- How pushing one policy update across AWS, Google Cloud and containers speeds response;
- How stress-tested default policies let more than 90% of customers run in enforcement mode.

“What’s happened is that the time between a new threat appearing and your opportunity to respond has just collapsed.”

- Brian Schwarz

[Watch Now](#) 



Lou Manousos
Co-Founder and CEO, Ent

AI Agents Redefine Enterprise Endpoint Security

Ent CEO **Lou Manousos** on User Intent, Local AI and Machine-Speed Defense

Artificial intelligence agents are redefining the enterprise endpoint as autonomous processes gain local access to applications, data and tools, requiring security teams to monitor the workflow of both human activity and agent behavior, said Lou Manousos, co-founder and CEO of Ent.

- Why defenders need telemetry that models user and business intent;
- How agentic AI moves enterprise activity beyond SaaS applications and traditional browsers;
- How local models and dedicated hardware can support real-time preventive defense.

“Without that type of sub-second response time, the damage may already be done. So, trust is the critical element, and then also having an architecture that can support real-time preventative defense.”

- Lou Manousos

[Watch Now](#) 



“We’re not just talking about a smarter threat actor. We’re talking about a threat actor who can essentially walk away from the desk and let their operations run on their own.”

John Hultquist

Chief Analyst, Google Threat Intelligence Group

Identity Security

Compromised identities have become a growing attack path as hackers increasingly target credentials, accounts and access privileges to infiltrate organizations. At the same time, the explosion of AI agents is creating new challenges because traditional identity systems weren't built to manage machine identities operating at massive scale. We interviewed leading experts in identity security about innovative solutions for securing human and machine identities, controlling access and stopping identity-based attacks.



AI Agent Security Risks Run Beneath the Model

Check Point's **Shahar Tal** on AI Framework Flaws, Guardrails and Patch Cycles

Artificial intelligence agent security risks extend far below the model layer. Vulnerabilities in the frameworks that run AI agents can expose organizations to classic software flaws while giving attackers paths into systems with broad permissions, said Shahar Tal, head of agentic security innovation at Check Point Software.

[Watch Now](#) ▶



AI Governance Must Extend Beyond the Browser

iboss' **Paul Martini** on Shadow AI, Autonomous Agents and Data Security

Shadow AI, autonomous agents and rapidly proliferating vibe-coded applications are creating new avenues for data leakage. iboss' Co-Founder and CEO Paul Martini says organizations need network-level visibility and guardrails to monitor AI interactions, control data flows and manage emerging business risks.

[Watch Now](#) ▶



Why AI Agents Can't Certify Their Own Compliance Work

BLOdgie's **Brennan Lodge** on Segregation of Duties Between AI and Auditors

Artificial intelligence agents can reduce the manual burden of cybersecurity compliance, but organizations still need human judgment to validate evidence and authorize outcomes, said Brennan Lodge, founder and CEO of BLOdgie.

[Watch Now ▶](#)



Why AI Governance Requires Continuous Compliance Assurance

Schellman CEO **Avani Desai** on Building Governance Before Technology Enforcement

AI is advancing faster than most compliance frameworks can change, creating new demands for governance, testing and assurance. Firms may need more than SOC 2 to prove AI trustworthiness, said Avani Desai, CEO at Schellman.

[Watch Now ▶](#)



AI Agents Demand New Trust Models for Digital Transactions

Human Security's **John Searby** on Identity, Accountability and Trust in the Agentic AI Era

As AI agents begin browsing websites, logging into accounts and completing purchases on users' behalf, organizations must rethink identity, trust and accountability. John Searby of Human Security explains why linking human and machine identities is essential for secure digital commerce.

[Watch Now ▶](#)



Why Non-Human Identities Break Legacy Access Models

Keeper Security's **Darren Guccione** on Governing Agentic Identity

Non-human identities now outnumber humans across the enterprise, and legacy access tools built for people can't track, verify or govern them. The fix is a unified identity governance platform paired with quantum-resistant encryption, said Darren Guccione, CEO and co-founder of Keeper Security.

[Watch Now ▶](#)

A middle-aged man with grey hair, wearing a dark blue suit jacket over a light blue shirt, is seated and speaking. He is positioned in front of a blue backdrop featuring a large, stylized 'iS' logo in yellow and white. To his left, there are concentric purple circles on the backdrop. The man has a small microphone clipped to his shirt and is wearing a watch on his left wrist.

iS

“You need to audit how AI is being used by your employees. And then you need to put policy in place. The policy needs to be somewhere in the middle. You don’t want to prohibit because if you prohibit, you’ll end up with more shadow AI.”

Tony Anscombe

*Chief Security Evangelist,
ESET*



Brian Vecci
Field CTO, Varonis

The 3% Paradox Behind Agentic AI

Varonis Field CTO **Brian Vecci** on Limiting AI Agent Access in a 'Post-Mythos World'

Agentic AI promises massive productivity gains, but enterprises remain hesitant to connect agents to sensitive data. Varonis Field CTO Brian Vecci explains the “3% paradox” and why limiting access, monitoring behavior and reducing blast radius are critical in a post-Mythos world.

- Why agentic AI turns automation into a new labor layer capable of operating at machine speed;
- How limiting data access, permitted actions and blast radius can reduce enterprise AI risk;
- Why faster detection, automated response and business context will separate successful AI adopters.

“That 3% is the paradox of, ‘I want to unlock all of this value, but I can’t do it without introducing all of this risk.’”

- Brian Vecci

[Watch Now](#) 



Why AI Governance Must Control Agents at Runtime

CAS Strategies CEO **Camille Stewart Gloster** on Authority and Human Oversight

AI agents bring authority, credentials and access into enterprise environments, creating a new form of insider risk. Camille Stewart Gloster, CEO of CAS Strategies, explains why AI governance must define authority, enforce runtime controls and preserve human oversight.

[Watch Now ▶](#)



Why AI Agents Need Authority Controls

NAIC-ISAO's **Michael Thiessmeier** on 'Guarded Agency,' Machine-Speed Cyber Defense

AI agents can make cybersecurity decisions at machine speed, but access control alone can't define what they should do. NAIC-ISAO's Michael Thiessmeier says authority control and guarded agency can help security teams govern autonomous action without sacrificing defensive speed.

[Watch Now ▶](#)



Rise of Malicious AI Skills Expands Enterprise Risk

ESET's **Tony Anscombe** on Shadow AI, ClickFix and Securing AI Agents

Malicious AI skills are proliferating as agentic AI adoption accelerates, creating new enterprise risks ranging from credential theft to unauthorized code execution. Tony Anscombe, chief security evangelist at ESET, explains why discovery, governance and specialist security expertise are critical to keeping pace.

[Watch Now ▶](#)

A portrait of Ajit Gaddam, a man with dark hair and a slight smile, wearing a dark sweater. He is positioned in the upper half of the page, with a blurred background of warm, golden light.

Ajit Gaddam

Head, Fraud, Financial Crimes and Product Security, HealthEquity

Why Passkeys Are Closing the Account Takeover Gap

HealthEquity's **Ajit Gaddam** on Passwordless Security, Fraud Signals, Cyber Defense

Passwords remain a weak point in account security, especially when attackers can buy stolen credentials and exploit recovery workflows. Ajit Gaddam of HealthEquity explains how passkeys, biometrics and device signals can strengthen identity assurance while reducing login friction.

- Why call center staff are often an organization's weakest link against social engineering;
- HealthEquity's path from passwords to passkeys, and what it took to get there;
- Why passkey adoption depends on education, clear user experience and trained support teams.

"The best password in the world is you. You are your own identity."

- Ajit Gaddam

[Watch Now](#) 



Matt Girdharry

Worldwide Lead, Observability and Security, AWS Partnerships, AWS

Matt Radolec

Field CTO, Varonis

How AI Agents Widen the Enterprise Blast Radius

AWS' Matt Girdharry and Varonis' Matt Radolec on Data Security, Machine-Speed Risk

Agentic AI can act at machine speed across data, APIs and cloud services, expanding enterprise risk beyond traditional controls. AWS' Matt Girdharry and Varonis' Matt Radolec explain why AI governance, least privilege and runtime visibility now matter more than ever for security teams.

- How least privilege and runtime guardrails can reduce the blast radius of AI agents;
- Lessons on sandbox security and runtime observability from the OpenAI and Hugging Face incident;
- How AWS and Varonis are helping customers build security and governance into AI projects.

“You need to secure the model environment, but you also need to start looking more heavily at the data, at the network, at the API security layers and IAM best policies, in order to secure autonomous systems more functionally.”

- Matt Girdharry

[Watch Now](#) 

A portrait of Camille Stewart Gloster, a Black woman with long, dark, braided hair, wearing glasses and a black top. She is looking slightly to the left with a thoughtful expression. The background is a soft, out-of-focus purple and blue light.

“It is a new actor in your organization that is an insider. It’s moving around. It’s got access. It’s got permissions. It’s got visibility. It can see all your data, so it’s got this level of authority and permission and knowledge of your organization that a human might. But you can’t predict what it’s going to do.”

Camille Stewart Gloster

CEO, CAS Strategies, and Former Deputy National Cyber Director, The White House

Risk Management

Organizations face an expanding risk landscape as AI introduces new threats while amplifying existing ones. AI-based insider threats, AI-driven phishing attacks and rogue models are emerging alongside growing IT complexity, while new technologies and questions about AI sovereignty are creating additional uncertainty. We interviewed leading experts about emerging models and innovative approaches for identifying, assessing and mitigating risks as organizations navigate an increasingly complex and AI-driven environment.



Why CISOs Must Become Chief Trust Officers for AI

Forrester's **Jess Burn** on How CISOs Can Turn AI Risk Into a Trust Advantage

Boards, executives and business units are pushing for faster artificial intelligence adoption, straining CISOs' ability to keep controls in place. This friction gives CISOs an opportunity to become the organization's trust and assurance leader, said Jess Burn, principal analyst at Forrester.

[Watch Now](#) ▶



AI Agents Are Insider Risk's Newest Blind Spot

Above Security Co-Founder **Amir Boldo** on Synthetic Insiders and AI Investigation

AI agents are creating a new insider risk problem because they can access CRM platforms, enterprise tools and sensitive data, operate at machine speed, and change behavior without predictable patterns, said Amir Boldo, co-founder and chief product and technology officer, Above Security.

[Watch Now](#) ▶

A medium shot of Chris Inglis, a middle-aged man with grey hair, wearing a light blue and white striped button-down shirt and khaki pants. He is seated and gesturing with his hands while speaking. The background is a purple wall with a large white 'G' and the word 'udio' in gold script on the left, and a pattern of concentric purple lines on the right.

G
udio

“When two countries work together, they can do things that neither one of them can do alone, and they can benefit both of their populations. So, it can’t be America-only.”

Chris Inglis

*Former U.S. National Cyber Director,
NSA*



Alan LeFort

Co-Founder and CEO, StrongestLayer

AI Phishing Now Frighteningly Normal, Hard to Detect

StrongestLayer's **Alan LeFort** on Personalization, Evasion and First-Seen Attacks

AI-generated phishing has changed the signals security teams once relied on to identify malicious email. Personalized attacks can mimic trusted senders, familiar workflows and legitimate infrastructure, making suspicious messages look routine, said Alan LeFort, co-founder and CEO of StrongestLayer.

- What security leaders should ask vendors to see past agentic AI marketing hype;
- Why security leaders should measure false positives and detection outcomes when evaluating AI-powered tools;
- How email could become a command-and-control channel for AI assistants exposed to prompt injection.

“Do we really believe that training Sally in accounting with a 30-minute video four times a year is going to make her smarter than the AI and the cumulative knowledge of the SOC?”

- Alan LeFort

[Watch Now](#) ▶



Psychological Safety Keeps Cybersecurity Teams Together

CRISP Shared Services' **Bezawit Sumner** on Mission-Driven Hiring, Retention and Trust

Healthcare has become an attractive target for attackers even as their security budgets remain constrained. Teams are competing for the same talent pool against major tech firms, said Bezawit Sumner, CISO and senior director, security and compliance, CRISP Shared Services.

[Watch Now ▶](#)



Why Multi-Agent AI Pipelines Beat Single Agents

Politecnico di Milano's **Stefano Zanero** on Specialized AI Agents, Exploit Generation

Security researchers are dividing complex cyber tasks among specialized AI agents to reduce false positives and improve results. Stefano Zanero of Politecnico di Milano explains how multi-agent pipelines strengthen vulnerability discovery, exploit generation and AI threat modeling.

[Watch Now ▶](#)



Why Secure AI Adoption Starts With Clear Objectives

Accenture's **Jason Lewkowicz** on Guardrails, AI Economics and Human Oversight

Enterprises risk overspending on artificial intelligence and producing poor outcomes when they skip clear objectives and security guardrails, said Jason Lewkowicz, global cyber resiliency and defense lead at Accenture.

[Watch Now ▶](#)



Cybersecurity Is Bigger Than a Single Industry

Return on Security's **Mike Privette** on AI and the Economics of Cybersecurity

Security should be viewed as an interconnected economy rather than a stand-alone industry, said Mike Privette, founder, Return on Security. He explains why market signals and AI investment offer better insight into the sector's health.

[Watch Now ▶](#)

A middle-aged man with a receding hairline and a light beard is seated and speaking. He is wearing a dark green henley shirt. His hands are raised in a gesturing motion. The background consists of vertical curtains in shades of purple and blue, with a green vertical element on the left. A small black lavalier microphone is clipped to his shirt.

“We’ve seen a real uptick in the discipline and organization of crime groups, and so we’re really starting to see that new kind of young organized crime emerge, and really targeting financial services customers across the board.”

Jeff Lunglhofer

*Chief Security Officer,
Coinbase*



Frank Teegelaar
Head, Sales, Leap Platform



Zoobia Waqas
Marketing Director, Leap Platform

Why Great Customer Experience Means Zero Complexity

Zoobia Waqas and Frank Teegelaar of Leap Platform on Future of Customer Experience

Enterprise cybersecurity vendors are selling great products, but customer experience is a buzzword companies rarely define clearly. The secret to happy users is zero-complexity, full life cycle support, said Zoobia Waqas, marketing director, and Frank Teegelaar, head of sales, at Leap Platform.

- Vendor diversity and maturity levels that complicate technology selection;
- Leap Platform's orchestrator model for vendors including Symantec and Carbon Black;
- How vendors can reduce friction across complex security ecosystems.

"If you don't have a good customer experience, then they can very easily go over to the next vendor - because there are 10 others in line waiting."

- Zoobia Waqas

[Watch Now](#) ▶



Open AI Models Gain Ground as AI Sovereignty Grows

Cyfinoid Research's **Anant Shrivastava** on Local AI and Supply Chain Risk

Regulatory uncertainty and concerns over control are pushing enterprises toward open-weight AI models that can be deployed locally. Cyfinoid Research's Anant Shrivastava says open models are closing the performance gap while giving organizations greater control over data, model behavior and costs.

[Watch Now ▶](#)



Narrative Attacks Turn Public Perception Into a Cyberthreat

Blackbird.AI's **Wasim Khaled** on AI-Powered Influence Operations and Cyber Risk

AI and agentic systems are dramatically lowering the cost of narrative attacks, allowing adversaries to manipulate public perception at machine speed. Blackbird.AI CEO Wasim Khaled says organizations need narrative intelligence to distinguish coordinated manipulation from genuine public sentiment.

[Watch Now ▶](#)



Why Are Attackers Targeting Internet-Exposed SAP Systems?

Onapsis Co-Founder and CEO **Mariano Nunez** on Why Cloud Migration Exposes SAP Systems

Attackers are targeting internet-exposed SAP systems as businesses migrate to the cloud. This change strips away the network barriers that once protected these systems, handing adversaries remote access to critical business data, said Mariano Nunez, co-founder and CEO, Onapsis.

[Watch Now ▶](#)



Why Cybersecurity Strategy Now Changes by the Week

Abdul Latif Jameel's **Eapen** on Agentic AI, Endpoint Security and the CIO-CISO Divide

Cybersecurity strategy now has a shelf life of weeks, not years, says George Eapen, chief technology and security officer at Abdul Latif Jameel. As AI lowers attack costs and increases the volume, CISOs must use AI-enabled defenses, govern autonomous agents and revise plans as threats evolve.

[Watch Now ▶](#)



Chenxi Wang

Founder and General Partner, Rain Capital

Why Open-Weight AI Models Are Key to US Strategy

Rain Capital's **Chenxi Wang** on Why Closed AI Models Risk US Competitiveness

Mythos-class models now let attackers strike at machine speed, overwhelming traditional human-paced defenses. Security teams must respond with equally fast, machine-scale artificial intelligence defenses, said Chenxi Wang, founder and general partner of Rain Capital.

- Why university research labs are becoming pipelines for AI startup unicorns;
- How human checkpoints are giving way to full agent autonomy;
- Why founder capabilities outweigh market timing in AI investing.

“If we don’t allow open-weight models, somebody else will build them.”

- Chenxi Wang

[Watch Now](#) 

A portrait of Johnny Hand, a man with light brown hair and a goatee, wearing a blue blazer over a light blue t-shirt. He is sitting in front of a dark background with purple and blue lighting. A small microphone is clipped to his shirt.

“AI is very humanistic in the sense that it’s a non-deterministic model. So the way that it gets to solve the problem can often be different.”

Johnny Hand
*Global CISO,
TrendAI*



Cyber Risk Now Needs a Business Translator

Dataminr's **Balaji Yelamanchili** on Risk Prioritization, AI and Cyber Resilience

Threat intelligence platforms can surface an overwhelming number of signals, but volume alone doesn't tell a security team what to fix first. Balaji Yelamanchili, president and chief operating officer at Dataminr, said the real challenge is translating technical exploitability into business risk.

[Watch Now ▶](#)



AI Accelerates Financial Services Fraud

Coinbase's **Lunglhofer** on Deepfakes, Supply-Chain Risk and Human Expertise

AI is helping criminals clone voices, exploit software flaws and guide fraud schemes in real time. Coinbase Chief Security Officer Jeff Lunglhofer explains why faster attacks demand artificial intelligence-enabled defense backed by cybersecurity experts.

[Watch Now ▶](#)



Why AI Security Needs Frontier and Open-Weight Models

TrendAI Global CISO **Johnny Hand** on Distilling Open-Weight Models for Security

Security teams often treat frontier and open-weight artificial intelligence models as competing choices. The two are complementary, not substitutes, said Johnny Hand, global CISO at TrendAI.

[Watch Now ▶](#)



Why 'America First' in AI Shouldn't Mean 'America Only'

Former Cyber Director **Chris Inglis** on Cooperation, AI Supply Chains and Security

U.S. AI leadership requires more than protecting domestic technology. Former U.S. National Cyber Director Chris Inglis says national security depends on outperforming competitors, strengthening supply chains and working with allies.

[Watch Now ▶](#)



“A narrative attack is an attack on human perception to drive some sort of outcome.”

Wasim Khaled
CEO,
Blackbird.AI



Suzy Pallett
President, Black Hat

Black Hat's Peer Review Builds Trust and Resilience

Black Hat President **Suzy Pallett** on Community, AI and Collaboration

Cybersecurity teams face mounting pressure as technologies evolve, adversaries advance and practitioners work to keep pace with constant change, said Suzy Pallett, president of Black Hat.

- How public-private collaboration and technical depth shape Black Hat's keynote selection;
- Why security leaders should build peer networks they can rely on after the event;
- Why maintaining authenticity, peer review and community trust will define Black Hat's success in the years ahead.

"It means we can keep going, we can lean on each other, and we can take away practical insights."

- Suzy Pallett

[Watch Now](#) ▶

Security Operations

Security operations are entering a new era as AI-run SOC's promise to dramatically accelerate threat detection, investigation and response. But greater autonomy raises questions about where humans need to remain in the loop and how automation will reshape staffing, roles and required skill sets. We interviewed leading practitioners about how organizations are adopting AI-powered security operations, balancing human judgment with automation and moving faster to detect and stop increasingly sophisticated attacks.



Why Forensics, Incident Response Agents Need Good Validation

SANS Institute's **Rob T. Lee** on Testing AI Agents Before Trusting Their Results

Autonomous forensics and incident response agents can process large volumes of data much faster than human teams, but performance alone doesn't establish trust, said Rob T. Lee, chief AI officer and chief of research, SANS Institute.

[Watch Now ▶](#)



AI Defenders Must Match Attackers' Frontier Models

Vega CEO **Shay Sandler** on Governable AI and Scaling Analyst Expertise

Threat actors are using frontier artificial intelligence models to accelerate attacks, creating what Vega co-founder and CEO Shay Sandler warns is a threshold that legacy defense speed and tooling can no longer match.

[Watch Now ▶](#)

A medium shot of Morgan Kyauk, a man with short dark hair, wearing a grey blazer over a light blue button-down shirt. He is seated on a brown couch, gesturing with his right hand while speaking. The background is a blue and purple gradient with vertical lines.

“The thing that we want to begin to see is getting these technologies rolled out in production, showing true tangible use cases.”

Morgan Kyauk
*Managing Director,
NightDragon*



Steven Gerry

Vice President, Sales, Tidal Cyber

Rick Gordon

CEO and Co-Founder, Tidal Cyber

Threat-Led Defense Targets the Attacks That Matter

Tidal Cyber's **Steven Gerry** and Rick **Gordon** on Using Adversary Behavior to Reduce Cyber Risk

Security teams are facing more alerts, vulnerabilities and tools at machine speed, struggling to identify attacks most likely to succeed. Tidal Cyber's Rick Gordon and Steven Gerry explain how threat-led defense helps connect adversary behavior with defensive weaknesses and residual risk.

- Why security programs should prioritize attack probability and defensive relevance instead of alert volume;
- How to use the MITRE ATT&CK framework to prioritize threats and reduce the likelihood of a successful attack;
- How organizations can disrupt attack pathways even as artificial intelligence creates new vulnerabilities and exploits.

"Threat-led defense is our effort to try to eliminate whatever those barriers are, keeping security leaders from being able to do the job they're actually paid to do."

- Rick Gordon

[Watch Now](#) ▶



Kevin Kin

Vice President, Channel and Commercial
Technical Solutions, Palo Alto Networks

Edward Bailey

Field CISO, Cribl

Why AI-Driven SOC's Depend on Better Security Data

Palo Alto's **Kevin Kin**, Cribl's **Edward Bailey** on Improving SOC Consistency

Artificial intelligence-driven SOC transformation starts with high-quality security data, consistent analysis and automation that helps analysts respond faster without sacrificing oversight, said Kevin Kin, vice president of channel and commercial technical solutions at Palo Alto Networks.

- How organizations can reduce SIEM migration risk by running legacy and new environments in parallel;
- How the Palo Alto Networks-Cribl partnership helps customers accelerate their journey away from legacy systems toward AI-driven outcomes;
- How collaboration among customers, technology vendors and channel partners can make transformation more seamless.

"There is still a human needed to be overseeing it just to make sure that you know we're guiding that and training it along the way."

- Kevin Kin

[Watch Now](#) ▶



AI Security Moves From Experiment to Production

NightDragon's **Morgan Kyauk** on Proven Use Cases, Budgets and Scale

AI security is moving from experimentation toward production as enterprises deploy more agents. NightDragon Managing Director Morgan Kyauk explains how customer traction, repeatable use cases and ROI are separating scalable cybersecurity firms from market noise.

[Watch Now ▶](#)



AI Agents Need Speed Humans Simply Can't Match

McKesson's **Arsh Arora** on Building Guardrails for Autonomous AI

An AI agent wiped out a company's production database and three months of backups in nine seconds - faster than any human could intervene. McKesson's Arsh Arora explains why defending against AI-driven attacks now requires AI agents of your own, built with strict guardrails.

[Watch Now ▶](#)



Why AI Demands a SecOps Revolution

Zscaler CISO **Sam Curry** on Agentic SOCs, Resilience and AI Governance

AI will reshape security operations by changing how analysts find signals, manage risk and work with machines. Zscaler CISO Sam Curry says leaders need stronger resilience, new SecOps models and governance that supports innovation without adding bureaucracy.

[Watch Now ▶](#)



Why AI Can't Replace the Human Security Analyst

CMiC's **Wes Sheppard** on Why Shadow AI Still Needs a Human Layer of Analysis

Shadow artificial intelligence is not a new governance problem, it's the old shadow IT problem moving faster than security teams can track. Wes Sheppard, director of information security at CMiC, said the answer isn't automating people out of the loop.

[Watch Now ▶](#)



Ben Spencer

Product Director, Managed Detection and Response, Optiv

How Agentic Security Operations Is Changing the Threat Detection Landscape in the AI Era

Optiv's **Ben Spencer** on Building AI Models That Move Beyond Detection and Response

Artificial intelligence is accelerating attacks and lowering the barrier for threat actors. Security teams need to move beyond point-in-time detection toward proactive remediation, said Ben Spencer, product director for managed detection and response at Optiv.

- How organizations can map workflows before placing AI agents inside security operations;
- Why proactive remediation and architecture matter as much as detection speed;
- How agentic AI helps analysts focus on strategic tasks instead of repetitive ones.

“We need to do things that prevent them from getting in the first place, so that we’re not overwhelmed. We do not want to go in and [manually] solve a lot of these problems.”

- Ben Spencer

[Watch Now](#) ▶

Vulnerability Management

Vulnerability management faces a new test as Anthropic's Mythos and other advanced AI models dramatically increase the speed and scale at which vulnerabilities can be discovered and exploited. Enterprises must prepare for a torrent of new vulnerabilities and determine which pose the greatest risk. We interviewed leading experts about how organizations can identify vulnerabilities across their ecosystems, prioritize the most critical exposures and remediate them fast enough to keep pace with AI.



How AI Agents Validate Software Vulnerabilities

Arizona State's **Yan Shoshitaishvili** on Eliminating False Positives With Agentic AI

Artificial intelligence agents are evolving vulnerability detection by moving beyond code review to direct software interaction. They can run commands, observe behavior and test whether a suspected flaw can be triggered, said Yan Shoshitaishvili, associate professor at Arizona State University.

[Watch Now](#) ▶



AI Makes Faster Vulnerability Patching a CISO Priority

Banco Santander's **Daniel Cuthbert** on Exploitability, Attack Surfaces and AI

AI is lowering the cost and skill barrier for vulnerability research, creating more pressure on security teams. Daniel Cuthbert, global head of cyber security research at Banco Santander, says CISOs must validate exploitability, understand attack surfaces and accelerate patching.

[Watch Now](#) ▶

A man with glasses and a black shirt is sitting on a brown couch, gesturing with his hands while speaking. The background is a purple curtain.

“Machine speed response has to take you from being in a vulnerable state to closing the loop, and being able to graduate trust from ‘we’re in a vulnerable state’ to ‘we’ve got it,’ to something we feel we have high trust in.”

Rudra Mitra

*Vice President, Security Services,
Amazon Web Services*



Snehal Antani

Co-Founder and CEO, Horizon3.ai

Vulnerability Management Must Look Beyond CVEs

Horizon3.ai CEO **Snehal Antani** on Attack Paths and Automated Testing

Finding thousands of vulnerabilities doesn't make an organization secure. Knowing which ones attackers can exploit does, said Snehal Antani, co-founder and CEO of Horizon3.ai. As a former CIO, he said the hardest part of the job was deciding what not to fix.

- Why deception may offer an efficient way to detect artificial intelligence-driven attackers;
- How attackers exploit overlooked devices, such as an old office printer that falls outside typical security priorities;
- Why articulating cyber risk in business terms, rather than fear-based language, is critical to winning leadership buy-in.

“CVEs make up less than 3% of what constitutes an attack path.”

- Snehal Antani

[Watch Now](#) 



CVE Program Needs Modernizing, Not Replacing

runZero's **Tod Beardsley** on CVE Funding, Federation and Automation

An April 2025 funding scare involving the Common Vulnerabilities and Exposures program exposed how much governments, security vendors and researchers depend on a shared vulnerability naming system, said Tod Beardsley, vice president of security research at runZero.

[Watch Now ▶](#)



Vulnerability Counts Don't Equal Cyber Risk

Empirical Security's **Jerry Gamblin** on Exploitability, CVSS Limits and Management

The surge in reported CVEs doesn't mean software is becoming less secure. Instead, organizations should prioritize vulnerabilities based on exploitability and reachability rather than severity scores, said Jerry Gamblin, head of research, Empirical Security, and founder, RogoLabs.

[Watch Now ▶](#)



AI Is Calling In Cybersecurity's Technical Debt

Luta Security's **Katie Moussouris** on Frontier Models, Bugs and Containment

Organizations that deferred patching because it was too costly or disruptive are now facing a reckoning. Artificial intelligence is generating vulnerability reports and new findings at a volume that leaves nowhere left to hide, said Katie Moussouris, founder and CEO of Luta Security.

[Watch Now ▶](#)



AI Gives Defenders an Edge in the Vulnerability Race

Mandiant Consulting's **Charles Carmakal** on AI, Social Engineering and Extortion

Attackers are using AI to find vulnerabilities, build exploit tools and analyze stolen data, but defenders still hold an advantage. Risks now come from human-sounding phone scams, AI-assisted extortion and software supply chain attacks, said Charles Carmakal, CTO, Mandiant Consulting.

[Watch Now ▶](#)

A portrait of Daniel Cuthbert, a man with short, light brown hair and a beard, wearing a black polo shirt. He is smiling slightly and looking towards the camera. The background is a dark blue wall with vertical purple lines and a large yellow and white stylized logo on the right side.

“Patching cadence has to drastically change. If I were a CISO today, I would say, ‘How do we move from a weekly, monthly, quarterly patching-type process to an almost 12-hour period, or maybe even less?’”

Daniel Cuthbert

Global Head, Cyber Security Research, Banco Santander, and Associate Fellow, RUSI



Nick Biasini

Head, Outreach, Cisco Talos

How Skilled Attackers Weaponize AI Faster

Cisco Talos' **Nick Biasini** on Vulnerability Research, Phishing and Ransomware

AI gives skilled threat actors a bigger advantage than novices, accelerating vulnerability research, phishing and ransomware development. Nick Biasini, head of outreach at Cisco Talos, explains why expertise matters more than the model and why defenders must prepare for agentic attacks.

- How AI can expand vulnerability research and ransomware weaponization;
- Emerging threats that will demand greater efforts from defenders;
- How deception technology and stronger AI guardrails can help defenders.

[Watch Now](#) ▶

“If an unsophisticated actor goes in and says, ‘I want to have ransomware or write me ransomware,’ the model is going to say no. But if a software developer says, ‘I need a function that takes a file as input, applies public-private key cryptology and then returns the encrypted file,’ the model would be like, ‘Sure, here you go.’”

- Nick Biasini

A portrait of Rudra Mitra, a man with glasses and a black shirt, looking slightly to the left. The background is dark with some purple lighting.

Rudra Mitra

Vice President, Security Services, Amazon Web Services

Why Frontier AI Now Demands Smarter Vulnerability Triage

AWS' Rudra Mitra on Prioritizing Vulnerabilities at Machine Speed

Frontier artificial intelligence models are flooding security teams with more vulnerabilities than they can fix. The solution is applying that same AI power to prioritize, fix and validate what matters most, said Rudra Mitra, vice president of security services at Amazon Web Services.

- Weighing frontier models against more economical tools by attack complexity;
- How frontier models chain minor flaws into major attack paths;
- Bringing frontier AI earlier into remediation workflows.

“We’ve always had more vulnerabilities than we can fix, and now if you commoditize or put pressure on finding more, it just adds to the backlog.”

- Rudra Mitra

[Watch Now](#) ▶



Sam Chehab

Head, Security, Postman

How Postman Embeds Wiz Risk Data Into Dev Workflows

Head of Security **Sam Chehab** on Turning Vulnerability Alerts Into Developer Action

Security teams have long struggled to hand off vulnerabilities to the right developer for remediation. Sam Chehab, head of security at Postman, discusses how embedding Wiz threat intelligence directly into Postman's API catalog puts risk data inside the tools developers already use daily.

- How the integration moves security teams' time from reactive tooling to preventive controls;
- Why a unified inventory of deployed and undeployed services strengthens policy enforcement;
- Why the integration represents genuine "shift-left" security rather than a bolted-on feature.

"We've improved quite a few of our security KPIs just as a result of surfacing it up. Because developers are pretty proud people, and once you have that established process, they can rip through risk pretty quickly."

- Sam Chehab

[Watch Now](#) 



Amin Karbasi

Vice President and Chief AI Scientist, Cisco

Open-Weight Model Antares Delivers Stronger Code Security

Cisco's **Amin Karbasi** on How the Model Protects Source Code and Cuts Security Costs

Cisco's open-weight model Antares uses small language models to locate files containing known vulnerabilities across large codebases. Cisco Chief AI Scientist Amin Karbasi explains how the model rivals far larger systems, reduces analysis costs and helps resource-constrained defenders.

- Why model size doesn't determine the quality of security intelligence;
- How local deployment protects codebases and supports transparent analysis;
- How open-weight AI models can help universities, nonprofits and public-sector organizations strengthen software security.

“What Antares is trying to do is to be a very good investigator instead of being a good chatbot. The model tries to find a needle in a haystack, and it's very good at that particular thing.”

- Amin Karbasi

[Watch Now](#) 

A portrait of Charles Carmakal, a man with short dark hair and glasses, wearing a grey suit jacket over a light blue patterned shirt. He is smiling and standing in front of a blue background with concentric purple circles. A yellow stylized logo is partially visible on the right side of the background.

“Right now, we’re seeing a number of advances from an adversary perspective in terms of using AI to find vulnerabilities. But the defenders right now have the upper hand.”

Charles Carmakal

*Chief Technology Officer, Mandiant Consulting,
Part of Google Cloud*



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



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