

RSAC 2025: Agentic AI, Identity And The New Rules Of Cyber Defense

By [Tony Bradley](#), Senior Contributor. ⓘ Tony Bradley covers the intersection ...

May 12, 2025, 05:59pm EDT

[Share](#)

[Comment 0](#)



Cybersecurity leaders gather at RSAC 2025 to explore AI innovation, identity threats, and the future ... [More](#)
GETTY

Now that RSAC 2025 has wrapped, it's a good time to look at the top takeaways from the event—and what they mean for the future of cybersecurity.

This year's conference ended with a mix of urgency and cautious optimism. The theme, "*Many Voices. One Community,*" reflected a core idea: cybersecurity is moving too fast for any one group to manage alone. The field now faces bigger attack surfaces, faster AI-driven threats and a new reality where identity—not the network—is the main point of defense.

Last year was about the *promise* of AI. This year focused on the *reality*: the need for accountability, automation and smarter adaptation. There's still plenty of buzz, but it's now grounded in practical progress.

Agentic AI and the Rise of the Autonomous SOC

AI was front and center again, but with a new focus: agentic AI. This type of AI doesn't just assist—it acts. These systems can reason and take steps without being told exactly what to do.

CrowdStrike introduced [Charlotte AI Agentic Workflows and Response](#), aimed at automating detection and response tasks. Torq made a similar push by adding multi-agent RAG capabilities to its HyperSOC 2.0 platform [after acquiring Revrod](#). The goal is to handle alerts and responses at machine speed—faster than humans can manage.

These changes are less about flashy tech and more about keeping up with threats that move in milliseconds.

Identity Takes the Spotlight

As traditional perimeters fade, identity has taken over as the frontline of security. RSAC 2025 made it clear: identity is now both the starting point and last line of defense.

Proofpoint [rolled out a platform](#) that monitors access across email, endpoints, web and cloud. CrowdStrike [introduced Falcon Privileged Access](#), designed to protect against identity-based attacks through every stage—from the initial breach to lateral movement.

The message was simple: if you can't manage identity at scale, you can't secure your environment.

Passwordless Moves Forward

Passwordless authentication has been on the radar for years. Now, it's finally gaining ground.

Passkeys, biometrics and adaptive authentication are catching on. Vendors at RSAC showed tools to help organizations shift away from passwords—especially in complex, hybrid environments. The push is clear: fewer passwords, fewer phishing risks and a smoother experience for users.

Defending With—and Against—AI

AI is helping us secure systems—but it's also being used by attackers. Organizations now face two challenges: how to use AI safely and how to protect against it.

Cyera [launched Omni DLP](#), a smarter, AI-native approach to data loss prevention. Vanta [shared a new AI security assessment tool](#) to help teams evaluate how AI is being used and where it might introduce risks.

From fake media and AI-generated phishing to attacks that fool models, AI threats are growing. Many companies aren't ready yet and RSAC made it clear that preparation can't

wait.

Cloud Visibility Gets a Boost

Seeing what's happening across cloud environments is still a problem. RSAC vendors showcased new tools aimed at fixing that.

Illumio [introduced a cloud detection and response solution](#) powered by AI. Rapid7 [launched an enterprise-grade MDR service](#) and a [new Intelligence Hub](#) to deliver context and insights in real time. These updates all pointed toward the same goal: make sense of complex environments and take action faster.

Insider Threats: Hiding in Plain Sight

While much of the focus stays on outside attackers, RSAC 2025 brought attention back to insider risks.

DTEX [shared new research on a troubling tactic](#): North Korean operatives getting hired under fake identities at global companies—sometimes with admin-level access. In a remote-first world, this kind of threat is hard to spot and harder to stop. The message? Trust, but verify—and then verify again.

Smarter, More Unified Data Security

Data protection often feels like a puzzle with missing pieces. This year, vendors tried to change that.

Snyk [added dynamic application security testing](#) to its platform. Cyera's data-first approach drew a lot of interest. NinjaOne [launched tools that bring together patching and vulnerability management](#). These moves all aim to make data security easier to manage and more effective in practice.

Email Threats Aren't Going Anywhere

Even as AI and quantum security grab headlines, old threats persist. Email remains a top attack vector.

Barracuda's new [report found that nearly 25% of HTML attachments are malicious](#). Attackers are hiding dangerous content in files to dodge detection. It's a reminder that even mature tools like email still need attention.

A Lighter Moment—With a Monster Truck

Not everything at RSAC was serious. Torq drew a crowd with a 12,000-pound surprise—Grave Digger, the legendary monster truck. It was a playful break from the usual vendor booths and a reminder that cybersecurity events can still be fun.

Looking Ahead

RSAC 2025 showed us a field in the middle of transformation. The network perimeter is gone. Passwords are fading. AI is changing everything—from how we defend systems to how they're attacked.

Complexity is rising, but so is innovation. The next phase of cybersecurity will belong to those who can simplify, integrate and automate without losing visibility or control.

This year's message was clear: it's not about building walls. It's about preparing for a world without them.

Follow me on [LinkedIn](#). Check out my [website](#).

Join The Conversation

Comments 0

One Community. Many Voices. Create a free account to share your thoughts. Read our community guidelines [here](#).

[See All Comments \(0\)](#)

Forbes

© 2025 Forbes Media LLC. All Rights Reserved.

[AdChoices](#) [Privacy Statement](#) [Do Not Sell or Share My Personal Information](#) [Limit the Use of My Sensitive Personal Information](#)
[Privacy Preferences](#) [Digital Terms of Sale](#) [Terms of Service](#) [Contact Us](#) [Send Us Feedback](#) [Report a Security Issue](#) [Jobs At Forbes](#)
[Reprints & Permissions](#) [Forbes Press Room](#) [Advertise](#)

