

How Adaptive EDR Is Helping Agencies Keep Pace With AI-Driven Threats

As adversaries leverage AI to move at machine speed, federal security teams are using telemetry and automated defenses to detect threats faster while supporting compliance and cost efficiency.

Federal agencies are managing increasingly sophisticated artificial intelligence-based threats, but they also face constantly evolving compliance requirements and budget constraints. To balance mission protection with compliance, efficiency and budgets, they must adopt endpoint detection and response (EDR) security solutions that provide true network visibility without driving up cost.

During a recent [FedInsider webinar](#), industry experts shared how they're responding to cyber threats and leveraging EDR to strengthen federal network protection while helping them remain compliant and within budget.

Identity as a Control Plane

While identity has been considered a control plane for some time, the era of cloud computing exposed login interfaces to the public. This put identity at the forefront as "a set of compromised credentials could be keys to the kingdom," said Security Strategist of the Enterprise Security Group at Broadcom Paul Miller.

That drove the push for multi-factor authentication. "We still see it as a control plane because we don't foresee that cloud services will ever go away, and this will be a computing model probably into perpetuity," Miller said.

Identity is one of many control planes that organizations look for when taking a holistic and

effective approach to defending an environment. Other factors to consider are endpoints, the network and your data.

As vulnerability and threat velocity increase with automation, EDR is as significant as it has ever been – but alone, it's not enough. It's part of the puzzle but requires stronger data and metadata for effective analysis and visibility.

As AI continues to grow and get more capabilities, speed will also be an issue. "We have to continue to combine those data sources to react faster and understand what we are looking at in a quicker way," Miller said. For example, automated defense capabilities built into a system can help reduce that risk over time.

But for federal agencies with budget limitations and limited funds for a multiyear rip-and-replace project, EDR is a "critical linchpin when it comes to the visibility we need," said Channel Technical Director, Endpoint Security of the Enterprise Security Group at Broadcom Sam Romo.

EDR can sit on top of an existing stack and get telemetry from endpoints, the network and security tools that is needed for data protection. It can then be used to provide holistic visibility and maximum ROI from the tools already in place.

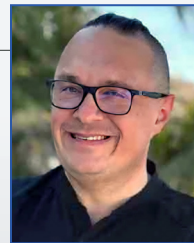
"I've seen people take various EDRs and put it on top of what they have to get the additional visibility and coverage required as the threat landscape evolves," Romo said.

Featured Experts:

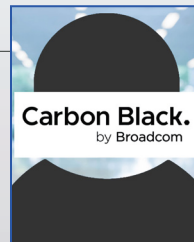
■ **Sam Romo**
Channel Technical Director, Endpoint Security, Enterprise Security Group, Broadcom



■ **Paul Miller**
Security Strategist, Enterprise Security Group, Broadcom ESG



■ **Craig Picken**
Technical Services Consultant, Broadcom



Evolving With the Threats

Security teams need visibility into what's normal in their network environments so that the tools they have can more effectively and quickly detect abnormalities, vulnerabilities and AI-driven threats.

"Any anomalies will be a lot easier to identify if you have that telemetry and system in place already. To understand what a given workflow looks like, especially when you get into the critical systems where they won't be as active, you want to be able to identify the anomalous activity quickly to be able to react to that," said Technical Product Manager at Broadcom Craig Picken.

That reaction, panelists say, can be human driven while also evolving over time to become more automated. According to Romo, CISOs need the high level of operational resilience that automation offers because it reduces the risk at machine speed.

"If the anomaly is detected at 2:00 a.m., I don't have to generate an alert and wait for the human to wake up," he said, "I can take steps automatically and sandbox the process, and it will give me both resilience and comfort."

And while EDR is still helping to protect metadata and detect AI-driven threats, Miller said it's more reactive than it needs to be. What is needed is stronger predictive analysis to predict the next several moves of an attacker so analysts can develop an attack timeline.

"That's the technology we are all going to be needing to use in the next few years," Miller said. "It's the kind of tech we will see emerge that allows us to get an advantage further left, where we would have stopped attacks before."

Understanding and Adapting to Adversaries

Panelists agree that adversaries are weaponizing AI to launch machine-speed attacks and using techniques that bypass old detection

methodologies. "To truly understand the context of an attack in real time, we can't rely on legacy methodology, we have to fight AI with AI," Romo said.

From a deployment perspective, adaptive endpoint architectures can autonomously detect, analyze and neutralize the threat at that speed, and that's where organizations need to be.

Romo also said having smart AI that understands exactly what the behavior is, that observes beyond triggers and can distinguish between a simulation in a sandbox and a real attack is going to be key.

Those types of solutions aren't meant to replace humans. Rather, they're meant to filter metadata that may require further human analysis so that security experts can spend time on what matters. Considering security information and event management providers are expensive over time, this can also help to cut organizational costs, Miller said.

Agencies are also faced with fragile legacy systems that are too much of a risk or too expensive to replace. This is where adaptive EDR comes in. Once the EDR learns a system's exact operational baseline, it can start doing instant blocks of any anomalous deviations. "Adaptive EDR will modernize the security wrapper around your legacy infrastructure, safely expanding its lifespan," Romo said.

And while having adaptive EDR and effective reactivity are great, EDR systems and tools that first gather data are critical, because they help agencies remain compliant. "Once the data is there, good EDR can understand what it is and then quickly figure out what you are

looking for and whatever compliance mandates apply," Picken said.

Rather than going out and getting that data, it's automatically reported to security teams and can also be sent to auditors and compliance teams faster. And once an organization's security posture is the highest level it needs to be, compliance is already taken care of. "Compliance just needs to be part of everyday life, rather than an audit that comes in from time to time," Picken said.

Ultimately, adopting these technologies, telemetry and methodologies through EDR and AI-driven solutions correctly will make it so that even if an attacker crosses the threshold (breaches are bound to happen), they are still easily detected and stopped.

"We have to apply this technology to push left on the timeline as far as we can," Miller said. "If we can't do that, then we are leaving capability on the table in terms of our response times."



Hosky Communications Inc.
3811 Massachusetts Avenue, NW
Washington, DC 20016
Contact: [John Hosky](#)

☎ (202) 237-0300
✉ Info@FedInsider.com
🌐 FedInsider.com
📘 Facebook.com/FedInsiderNews
🌐 LinkedIn.com/company/FedInsider
🐦 [@FedInsider](https://Twitter.com/FedInsider)



Carahsoft
11493 Sunset Hills Road, Suite 100
Reston, VA 20190
Contact: [Avery Reynolds](#)

☎ (571) 662-3260
✉ BroadcomBD@Carahsoft.com
🌐 Carahsoft.com/Broadcom
📺 Youtube.com/user/BroadcomCorporation
🌐 LinkedIn.com/company/Symantec
🌐 LinkedIn.com/company/Carbon-Black



© 2026 Hosky Communications, Inc. All rights reserved. FedInsider and the FedInsider logo, are trademarks or registered trademarks of Hosky Communications or its subsidiaries or affiliated companies in the United States and other countries. All other marks are the property of their respective owners.

