GlobalData

September 2026

Amy Larsen DeCarlo

Faster Than the Attack: How the Right Network-Based Solution Can Turn AI into the Optimal Cyber Defense

Adversaries have been quick to leverage AI to find and exploit enterprise vulnerabilities at machine speed. With the right AI-powered defense platform, enterprises can outpace aggressive threat actors.

AI has the potential to revolutionize the way the world innovates and advances. But in the wrong hands, AI brings danger. Threat actors are adept at quickly leveraging technology developments to advance their campaigns, employing AI is no different. Adversaries have been fast to use AI to expedite the finding and exploiting of vulnerabilities in their targets' systems and doing so at lightning speed.

AI, in conjunction with automation, brings a unique power to cybercriminals. Malware can adapt in real-time to evade detection without requiring human intervention. Cybercriminals are using AI to scan entire networks and find weak spots in seconds. Palo Alto Networks' research notes that in one attack, adversaries scanned more than 230 million unique targets for high-value data. Data exfiltration occurs within the first hour of a breach in nearly 20% of incidents.

More than a quarter of enterprises that suffered a cyberattack in the last year said it was AI-driven, according to IBM's Cost of a Data Breach Report 2026. These incidents have a steep cost, with the average expense associated with a breach up 12% from the prior year and nearing $5 million.

This comes at a time when confidence in cybersecurity is in freefall. A Fortinet survey of 871 cybersecurity and IT professionals reports that the level of adequacy of their corporate security postures has slid to 29%. That number is even lower for AI-generated attacks, with just 12% expressing confidence in their ability to stave off those incidents.

There is also recognition that enterprises are still failing to identify breaches and mitigate the impact in a timely manner. Palo Alto's Unit 42 Global Incident Report found the median attacker dwell time is seven days.

Turning the Tables

As overwhelming as the threat environment can be, particularly to an organization with gaps in its own cybersecurity resources and limited AI experience, with the right toolset and strong alliances, enterprises can rise to beat their adversaries at their own game.

Network-based managed service providers (MSPs) offer critical assets that can support enterprises in building their best defenses against AI-driven attacks. The answer is a combination speed and knowledge. Leading network operating MSPs have gained deep levels of expertise and understanding through securing their own vast multi-national infrastructures.

MSPs have extensive experience in AI-model development built on the data from many millions of network and cybersecurity incidents across their own surfaces. This insight translates into crucial elements necessary to secure enterprise customer environments.

Enterprise and public sector customers rely on MSPs to apply advanced AI to do more than optimize network performance; they look to operator partners to lay the secure, reliable, and resilient foundation that creates a new and highly effective cyber defense.

The objective of this approach is to not just contain threats but to accelerate both threat identification and incident response through AI that is applied to network-owned telemetry. This encompasses all key data sources, including NetFlow, DNS, BGP, and DDoS traffic culled from

millions of endpoints and thousands of customers, providing critical perspective on all relevant activity.

Straight to the Source Data

Key Telemetry Sources:

- NetFlow telemetry maps IP transmission data, including which endpoints communicated over what period; how much data was transferred using which ports and protocols; and transmissions without any payload. NetFlow data offers information indicative of potential threats including command-and-control patterns that demonstrate telltale signals including unusual destinations and ports, signs of data exfiltration, lateral movement, and potential malware/bot activity. This data can help in rapid scoping, isolating threats, meeting compliance requirements, and mapping attackers and targets.

- DNS telemetry delivers statistics on queries and responses that can denote scenarios such as malicious domain use, tunneling/exfiltration using DNS, fast flux/infrastructure churn, and it also shows spikes in lookups and resolved domains near the time of a credential incident revealing phishing. This data can help identify which internal clients queried a malicious domain first – information that can be used to block adversarial actions, monitor other attempts, and reconstruct incident timelines.

- Border Gateway Protocol (BGP) telemetry shows internet routing changes that can spot route hijacks and leaks, as well as traffic inception attempts and infrastructure instability that can camouflage attacks or suggest degradations in defenses. This data can discern actual attacks from routing problems when services become unreachable. BGP telemetry also provides information to better coordinate mitigation and continuous monitoring for asset protection. The is also useful in forensic analysis.

- DDoS traffic telemetry collected from scrubbing centers, edge routers, and sensors reveals attack vectors, targeted services, and situational changes over time. This data classifies attacks and identifies botnet infrastructure and multi-vector campaigns. DDoS traffic telemetry can help with mitigation actions, providing capacity and impact assessments. The data also supports post-incident reporting.

Adding AI to the Mix

All this source data makes for a clearer picture of network activity, highlighting disruptive and potentially nefarious activity. When isolated for every individual customer, the information creates a baseline of activity allowing for detection and response capabilities for each discrete enterprise.

Some MSPs are limited to the data and visibility available within their shared environments, which can restrict the capabilities they deliver. As a result, they often cannot provide a dedicated, customer-specific instance and may only address a portion of an organization's security and operational requirements. This puts their customers at a significant disadvantage.

MSPs who have full visibility into a discrete enterprise environment and apply AI-driven insights into that data can provide their clients with a more effective security defense. Internet-backbone

visibility helps clients spot critical issues like botnets, mass common vulnerabilities and exposures (CVE) exploitation, and coordinated campaigns. This data helps clients gain more productive insights from their existing security infrastructure tools such as security information and event management (SIEM) solutions.

Other elements in the security infrastructure also pick up essential information from data sourced from the network backbone. Vulnerability management solutions can use this data to correlate a client's asset inventory with live observation of which CVEs are actively being probed across the network. Identity and access management (IAM) solutions use visibility into the enterprise network to gather identity signals for continuous risk-adaptive authentication.

Customers get better protection leveraging solutions including secure access service edge/zero trust network architecture (SASE/ZTNA) for more effective threat intelligence and preemptive mitigation. MSPs can use AI for behavioral risk scoring and insights. This provides continuous authentication and helps with a resistant security posture, optimizes the tool stack, and delivers access analytics.

Incident response can also be exceptionally strong. By executing agentic runbooks that isolate and contain threats across compatible services such as managed firewalls and SD-WAN devices, the appropriate steps to mitigate an incident can be taken. The key is data accuracy, which gives time compression from detection to remediation, delivering prioritized, automated responses.

AI is the distinguishing factor when it marries perspective with execution and enforcement to create proactive and positive security and performance outcomes. The result is faster and more accurate threat identification stemming from a dramatic drop in false positives and better discernment of true threats from harmless anomalies. Combined with automation, this leads to a marked decrease in risk and operational disruption with a corresponding increase in trust and productivity.

Preemptive Security Progresses, with a Human Touch

In a threat environment where AI gives adversaries an edge in speed and force, the enterprise can’t rely on reactive tools. To mount a truly effective defense, organizations need to have a proactive mindset, and the technology to back this approach.

It is critical for an MSP to establish and learn from a customer’s baseline network activity to recognize any potential harmful patterns. How does this translate to a production environment? At a high level, an effective MSP-delivered cybersecurity solution will need to find and fix network vulnerabilities and accurately spot and mitigate threats. To achieve optimal outcomes at scale, the solution will ingest, analyze, and apply AI to learn behavioral patterns from the data at a rapid pace. Using techniques like continuous firewall policy assessment to make sure rules meet industry standards and conditions MSPs can expedite threat identification and minimize threat impact.

Also, an MSP should run proactive CVE database scans and vulnerability assessments to identify and remediate security gaps. MSPs need to offer corrective actions and guide customers on how to prioritize them based on their environment.

Agentic AI's potential as a critical part of advanced security solutions introduces questions about how autonomous a role it will play. While automated remediation is on the table, organizations are approaching the concept with awareness, education, and caution. Many security organizations today are evaluating changes in their runbook with agentic AI in mind to better understand where to leverage AI with human oversight vs. human directed actions.

Many enterprises lack internal AI expertise, and in many cases sufficient overall security resources, so they often lean on their MSP and other trusted partners. These providers should be able to offer a full complement of consulting services encompassing AI policy assessment, asset inventory, data integration, software upgrades, and policy refreshes.

What support is needed to build the best cybersecurity defense in today's environment?

An effective and well-executed policy is at the heart of any preemptive security approach. Enterprises often need third-party support in evaluating their threat assessment in the AI era. This can involve on-demand analysis of network and security device configurations.

Enterprise security practitioners also need a way to visualize threats to understand potential impacts and prioritize responses. MSPs play a crucial part in delivering real-time, interactive models of the customer's enterprise environment, revealing relationships, communications and dependencies between hosts to enable AI-driven detection, correlation, and remediation. Through this interface, MSPs can deliver agentic AI-generated recommendations to allow the customer to execute the appropriate action.

Aligned for the Best Defense

While it goes without saying in the current threat environment, having the right combination of technology and human insights is critical to protect enterprise assets, too many organizations lack sufficient resources. In the SANS Institute 2026 Cybersecurity Workforce Research Report, the training and certification organization reported 60% of CISOs lack the "right staff" to support their current security requirements.

This ongoing deficit puts organizations at security risk. Enterprises in this position need a trusted network partner to help them better protect their resources. The right network-based MSP is uniquely positioned to meet the AI-driven security moment with the network speed, scale, perspective, and expertise to deliver what other providers cannot.

Legacy security controls are no longer enough to keep up with advanced threats – only a proactive AI security approach can match the speed requirement driven by adversarial AI-powered campaigns. Network providers are much more than connectivity service providers, they are critical partners in facilitating the network operations that are essential to meet business requirements.

The time is now for stakeholders to meet the moment, choosing the right collaborative network and security partner. Only through this kind of well-crafted alliance can the enterprise's CIO and CISO ensure the level of performance, resilience, and security of their enterprise against AI-powered adversaries.