

WHITE PAPER

Closing the GenAI Velocity Gap with AI and Converged Networking and Security



Executive Summary

Artificial intelligence (AI) is changing cybersecurity on both sides of the battlefield. Attackers are using AI to automate reconnaissance, weaponize vulnerabilities faster, create convincing social engineering campaigns, and accelerate lateral movement. As a result, breakout times are shrinking from days and hours to minutes. At the same time, defenders are investing heavily in AI-powered security tools to improve visibility, detection, and investigation. Yet many organizations continue to experience the same outcome: Threats are detected, but containment and enforcement lag.

The problem is not a lack of intelligence. It's the generative AI (GenAI) velocity gap: the critical delay between how fast GenAI detects a threat and how quickly the network can contain it. Many security operations teams still depend on human coordination across disconnected security and networking tools. Analysts investigate alerts in one console, validate identities in another, examine network context elsewhere, and coordinate enforcement through multiple systems. Every handoff introduces latency. Every delay increases risk.

As AI accelerates the pace of cyberattacks, organizations cannot rely on workflows designed for human-speed operations. The latency caused by pivoting between consoles to validate and contain an identity increases risk. Closing the GenAI velocity gap requires two capabilities working together:

- AI-powered defenses to rapidly analyze, prioritize, and recommend action
- Converged networking and security to immediately execute those decisions across the environment

AI without convergence creates insight without action everywhere it's needed. Convergence without AI creates action without speed. Organizations need both.

The New Cybersecurity Reality: Machine vs. Human Speed

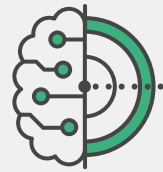
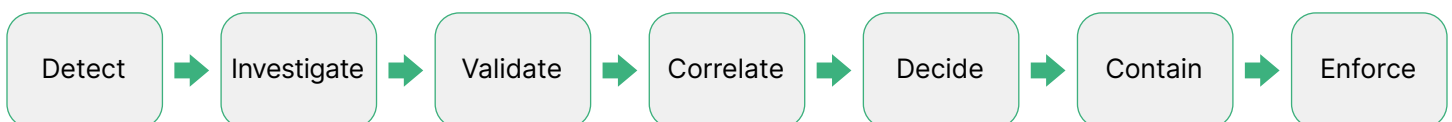
Cybersecurity has entered a new era when time has become a primary battleground. Historically, security teams focused on detection, coverage, and visibility. Today, they must also respond at the pace of AI-driven attacks. GenAI is enabling adversaries to:

- Automate research and reconnaissance
- Accelerate vulnerability discovery
- Scale phishing and impersonation campaigns
- Rapidly adapt malware and attack techniques
- Compress attack timelines from hours to minutes

The result is a growing mismatch between attacker speed and defender operations. Many organizations can identify a threat quickly. Far fewer can validate, contain, and enforce protections quickly enough to prevent expansion.

The Detection Illusion

Many cybersecurity programs still assume that better detection equals better security. Detection is important, but it's only the first step. Between detection and enforcement lie multiple operational steps:



Attackers are increasingly weaponizing AI, using it to automate the attack lifecycle, scale operations, and refine the sophistication of their attacks. This year's research shows the impact: More than one in four organizations that experienced a malicious attack reported it was AI-driven, a 56% increase over last year.¹

This gap between detection and enforcement has become more dangerous than at any point in modern cybersecurity. A security analyst may identify a compromised identity in seconds. Yet containment may require coordination between security tools, network infrastructure, endpoint controls, identity systems, and cloud platforms. While teams coordinate, the threat continues moving.

In an AI-driven threat environment, those delays are increasingly dangerous. For the enterprise, these unacceptable delays greatly increase costs. When containment lags behind detection, the blast radius of an attack expands exponentially. The cost is no longer measured solely by security metrics, but also by business downtime, emergency incident response fees, potential regulatory penalties, and the long-term erosion of customer trust. In short, human-speed latency in a machine-speed threat environment is a high business expense.

Human Judgment Is Still Required

Contrary to popular narratives, AI does not eliminate the need for human expertise. In fact, AI increases the value of human judgment. Security leaders still need experienced professionals to interpret context, assess business impact, evaluate risk, determine response priorities, and make final containment decisions.

While AI can accelerate analysis, humans need to provide judgment. Once a decision has been made, execution cannot depend on slow, fragmented workflows. This is where convergence enables swift action.

Why Convergence Changes the Equation

Most organizations still operate networking and security as separate domains. This separation creates operational friction precisely when speed matters most. In these environments, security identifies the threat, networking controls the path, identity validates the user, and operations coordinates the response. Each transition introduces a delay.

Converged networking and security eliminates these boundaries. When networking and security share visibility, telemetry, context, and enforcement capabilities, organizations can move from insight to action within a unified workflow. This results in faster validation and containment, consistent enforcement, reduced operational complexity, and shorter exposure windows.

- Faster validation
- Faster containment
- Consistent enforcement
- Reduced operational complexity
- Lower exposure windows

The outcome is not simply efficiency. It is a measurable reduction in cyber risk. Conversely, managing disparate tools forces organizations to absorb significant hidden operational costs. Maintaining separate networking and security siloes means higher costs caused by overlapping software licenses, heavy shelfware, and severe resource drain as highly skilled analysts spend their days separately managing tools instead of defending the enterprise. True convergence shifts security from a cost center that slows down operations into a business enabler that actively protects the bottom line.

Why Architecture Matters More in the Age of AI

For years, cybersecurity discussions about platforms focused primarily on operational efficiency. The value proposition centered on reducing the number of vendors, consolidating contracts, simplifying management, and lowering costs. Those benefits still matter. But the rise of AI has fundamentally changed the conversation.



Organizations take an average of 181 days to discover an active network intrusion and require an average of 60 additional days to isolate and contain the threat.²



Security teams extensively using AI and automation shortened their breach times by 65 days and lowered their average costs by \$1.93 million compared to those that didn't use these solutions.³

Today, platform architecture is no longer enough. A fabric is what’s needed.

Over the past decade, many organizations adopted a best-of-breed strategy, purchasing specialized point products to address individual security challenges. In many cases, these solutions were called a platform, but were not truly integrated to share intelligence, management, and consistent security policies. While well-intentioned, this approach frequently created fragmented architectures composed of disconnected tools, isolated data sets, and operational silos. As a result, security teams often possess dozens of security controls yet lack a unified understanding of what is happening across the environment.

An organization’s AI-enhanced security solution is only as intelligent as the data it can access and the actions it can perform. If security data is distributed across disconnected tools, the AI’s understanding of the attack is inherently incomplete. If enforcement capabilities are fragmented across separate systems, response actions become slower and less effective.

In other words, the defender’s AI can only see part of the battlefield. This creates what can be described as automated incompetence. Consider a security agent that detects malicious activity on an endpoint and reports that the threat has been contained. Meanwhile, the attacker has already moved laterally through the network, compromised another asset, or established persistence elsewhere. The AI reports success because it can only observe the portion of the environment it controls.

The attack continues beyond its field of view. In a fragmented architecture, this scenario becomes increasingly common as AI systems make decisions based on incomplete context. To operate at machine speed, defenders require more than AI. They require an architecture that provides comprehensive visibility, shared context, and coordinated enforcement across the entire environment.

This is where fabric architecture becomes essential. An AI-native cybersecurity fabric enables AI to:

- Observe activity across network, security, identity, endpoint, cloud, and application environments
- Correlate signals into a unified understanding of risk
- Execute coordinated actions across multiple control points
- Learn continuously from every investigation, response, and attack

Deploying AI in individual solutions is ineffective. A fabric, with AI at its core, spanning solutions, enables AI to respond quickly and effectively across the network. Organizations seeking to close the GenAI velocity gap should evaluate not only the sophistication of an AI capability but also the breadth of visibility and enforcement behind it. In the age of AI, fragmented intelligence creates a fragmented defense.

The AI + Convergence Advantage

Together, AI and convergence create a force multiplier. AI identifies what should happen. Converged networking and security make it happen immediately. This combination enables organizations to operate at machine speed while preserving human oversight and control.

What AI Provides	What Convergence Provides
 Threat prioritization	 Unified visibility
 Behavioral analysis	 Shared context
 Risk correlation	 Coordinated policy enforcement
 Investigation acceleration	 Automated containment
 Recommended actions	 Consistent response across environments

Table 1: The strongest cybersecurity model combines AI-driven intelligence with converged execution.

For example, consider a compromised credential detected by abnormal behavior. With a traditional approach:

- The analyst receives an alert.
- The identity team validates the account.
- The network team investigates access paths.
- Security requests enforcement actions.
- Multiple consoles are used to implement controls.

But the threat continues moving while teams coordinate, causing more damage. Now, let's examine the AI + convergence approach:

- AI correlates user behavior, device posture, network activity, and threat intelligence.
- The analyst reviews the recommended action.
- A single decision triggers coordinated enforcement across users, devices, applications, network segments, and cloud environments.

Investigation and containment time are reduced, resulting in less exposure and damage.



According to Gartner, “Network infrastructure, operations, and services are going through some of the biggest changes that we have seen in years (perhaps decades). These include the impacts of AI on infrastructure and operations, the impact of cloud adoption and work-from-anywhere trends on architectures, and the convergence of networking and security.”⁴

Closing the GenAI Velocity Gap

Organizations can no longer afford operational models where analysts pivot between disconnected systems while attacks move at machine speed. Defending against today's sophisticated, AI-driven attacks requires a new approach.

While AI accelerates understanding, human expertise provides judgment, and converged networking and security translate decisions into immediate action. The organizations that close the GenAI velocity gap will be better positioned to reduce cyber risk, improve resilience, and confidently embrace AI-driven innovation. Because in the age of AI, the question is no longer whether you can detect a threat.

Closing the gap between detection and response requires more than deploying AI-powered tools. It requires an architectural shift to a fabric composed of converged networking and security solutions that provide the visibility, context, and enforcement necessary for AI-driven operations. The organizations that succeed will combine human judgment, AI-driven intelligence, and converged networking and security in an architecture that enables all three to operate as a single system.

¹ Cost of a Data Breach Report 2026, IBM, July 29, 2026. <https://www.ibm.com/reports/data-breach>

² Ibid.

³ Ibid.

⁴ Gartner, Predicts 2026: Transformation of Network Infrastructure, Operations and Services, Jonathan Forest, Andrew Lerner, Mike Leibovitz, September 2025. <https://www.gartner.com/en/documents/6983966>