Enterprise Strategy Group by TechTarget

SHOWCASE

FEBRUARY 2025

Modernizing Security Operations in an AI-driven World

Dave Gruber, Principal Analyst

Abstract: As security leaders invest in modernizing security operations to defend a growing and increasingly diverse operating infrastructure in an AI-powered world, new strategies are needed to scale security operations safely. Modernization necessitates the move to more consolidated, AI-driven security platforms capable of automating the aggregation, correlation, and analysis of security data. AI-driven security operations provide faster detection, investigation, and remediation of threats while improving the efficiency of the security operations process. Driven by new advancements in generative AI and large language models, security technologies that leverage AI are at the heart of the modernization effort.

The Imperative to Transform Security Operations

Lack of innovation with traditional security operations approaches makes it difficult for security teams to scale and still meet the needs of today's rapidly changing businesses. For the fifth consecutive year, approximately half of security leaders (45%) reported that security operations are more complex today than two years prior.[1] Security teams struggle to keep up despite continued investment in upgrading security tools, program process improvements, and a focus on centralizing security data. AI-based attacks are a key driver for AI-driven defenses, significantly increasing the complexity of security operations processes. Attackers are embracing AI, which is decreasing the time spent on weaponization and continuous attack automation. They are quickly adapting their offensive strategies, outpacing traditional defensive techniques. In response, security operations teams must manage the increased pace and innovation of these attacks, increasing the day-to-day complexity.

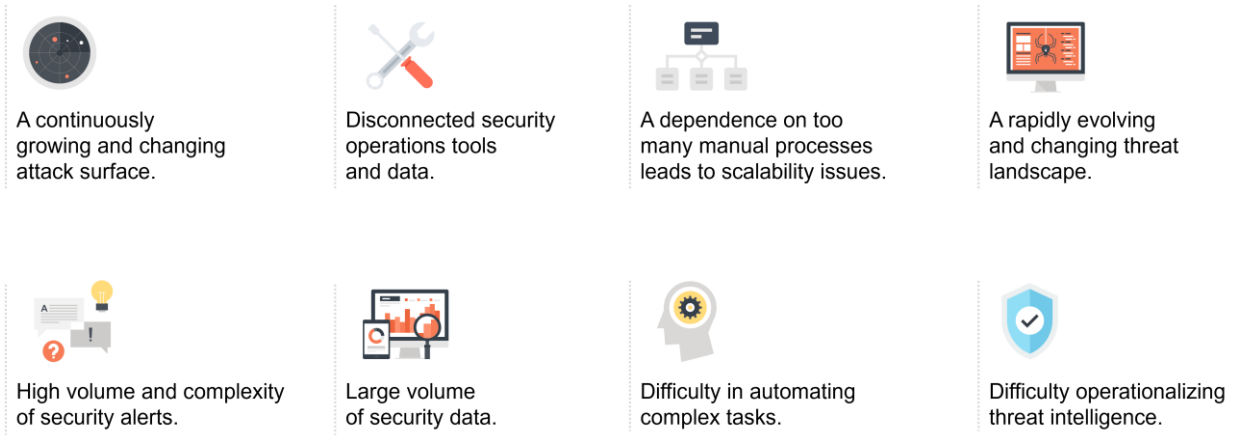
As the AI era further accelerates the overwhelming rate of change in IT infrastructure, security leaders must reconsider strategies to reverse this alarming trend. AI-driven security platforms enable security operations teams to remain competitive against an ever-expanding attack surface and threat model. Using AI to automate the discovery of assets and threats, tracking of vulnerabilities and risks, and automation of security operations processes is the only way to win the battle between attackers and defenders.

Security Operations Challenges Persist

Challenges within security operations center (SOC) teams stem from the expanding attack surface, too many point solution products, siloed teams, and inefficient processes. The quantity of raw security and asset data that must be analyzed makes operationalization and execution of results difficult and time consuming. Organizations report utilizing an overwhelming number of security tools, making it challenging to keep up with the pace of security operations. Tool consolidation is desired by most security leaders, with more than two-thirds (69%) investing in consolidation initiatives. Evolving threats, an expansive attack surface in both on-premises and ephemeral cloud models and too many siloed cybersecurity technologies have created an environment where SOC efficiency suffers, and attacks linger. These SOC challenges pose a natural spot where AI and large data analysis capabilities can create an outsized value for security teams. The SOC is ready to be modernized, returning a balance in operational efficiency.

[1] Source: Enterprise Strategy Group Complete Survey Results, *2024 SOC and XDR Modernization Trends*, May 2024. All Enterprise Strategy Group research references are from this survey results set, unless otherwise noted.

Figure 1. Key Security Operations Center Challenges



Source: Enterprise Strategy Group, a division of Informa TechTarget

The Security Operations Transformational Journey

Traditional SOC Models Are Failing

Traditional security operations center models were designed before the rapid ascent of AI, primarily to support a human-intensive process in a world where highly skilled cybersecurity talent was limited. This "tiered model" enabled basic alert review, correlation, and triage activities to be performed by more junior analysts so scarce, highly skilled personnel could focus on priority incidents.

Alert prioritization in this model is based on threat scoring, with minimal context into risk profiles, contextual threat intelligence, and potential attack paths within the environment. Lacking this context, security teams have little means of determining which threats pose the most material risk to the operation, forcing analysts to spend time investigating every alert. As alert volumes increase, tier 1 analysts quickly become overwhelmed and need help to keep up. Tier 2 and tier 3 analysts also suffer after being tasked with completing a large number of investigations without proper operational risk analysis and AI automated tooling.

Security Data Lake With AI Overlay Will Bring Relief

Two key industry megatrends are providing opportunities for security operations teams to overcome many of these challenges. First, the move to a more centralized security data strategy creates an opportunity for new levels of visibility and context in support of threat investigation and response. According to Enterprise Strategy Group research, 90% of organizations' current security data strategy is either completely or mostly centralized.[2] Second, AI-driven analytics applied throughout detection, investigation, and response processes are creating an opportunity to gain new levels of threat understanding, throughput, and response accuracy. Together, these two megatrends are enabling security teams to improve detections, analyst efficiency, intelligence sharing, and time to remediation.

What's Needed: The SOC of the Future

Keeping up with the rapid rate of change happening within IT, security teams need a scalable, intelligent, and automated solution to power SecOps. The SOC of the future must provide an AI-driven, highly scalable data

[2] Source: Enterprise Strategy Group Research Report, *The Triad of Security Operations Infrastructure: XDR, SIEM, and MDR*, June 2024.

analysis engine (connected to a Data Lake) that brings together multiple layers of output from different security technologies.

The SOC of the future is built on an efficient and performant security data lake with an automated, intelligent means of aggregating and correlating vulnerability, asset, and threat data. This provides visibility into advanced threats involving multiple attack vectors across the entire asset surface.

Monitoring and applying contextual threat intelligence to detections and investigations is required. This results in a centralized and correlated view of incidents across all attack stages, including orchestration and automation of remediation processes.

Finally, the SOC of the future must have an automated means of identifying and containing active attacks in progress earlier in the attack chain.

Consolidation Is Top Priority

With high growth in security tools and data, consolidation initiatives are required, with 69% of organizations actively consolidating or integrating their security operations tools and another 29% considering doing so.

Informa TechTarget's Enterprise Strategy Group sees tool consolidation as an ongoing, long-term strategy required to optimize security operations, while enabling the adoption of new tools required to secure IT innovations.

With these capabilities, security teams can redirect their focus from time-consuming manual activities to more strategic security activities designed to stop attacks sooner and before damage occurs. Security analysts can spend more time improving security posture and working collaboratively with IT and line-of-business leaders. This effort incorporates AI-driven security tactics that align with overall risk mitigation objectives.

How Fortinet Can Help

The Fortinet Security Operations solution's integrated platform approach, built on AI and automation, helps security teams move from a response-based approach to a proactive cyber-defense model across the entire attack surface and cyber kill chain.

Utilizing AI and advanced analytics, the Fortinet Security Operations solution:

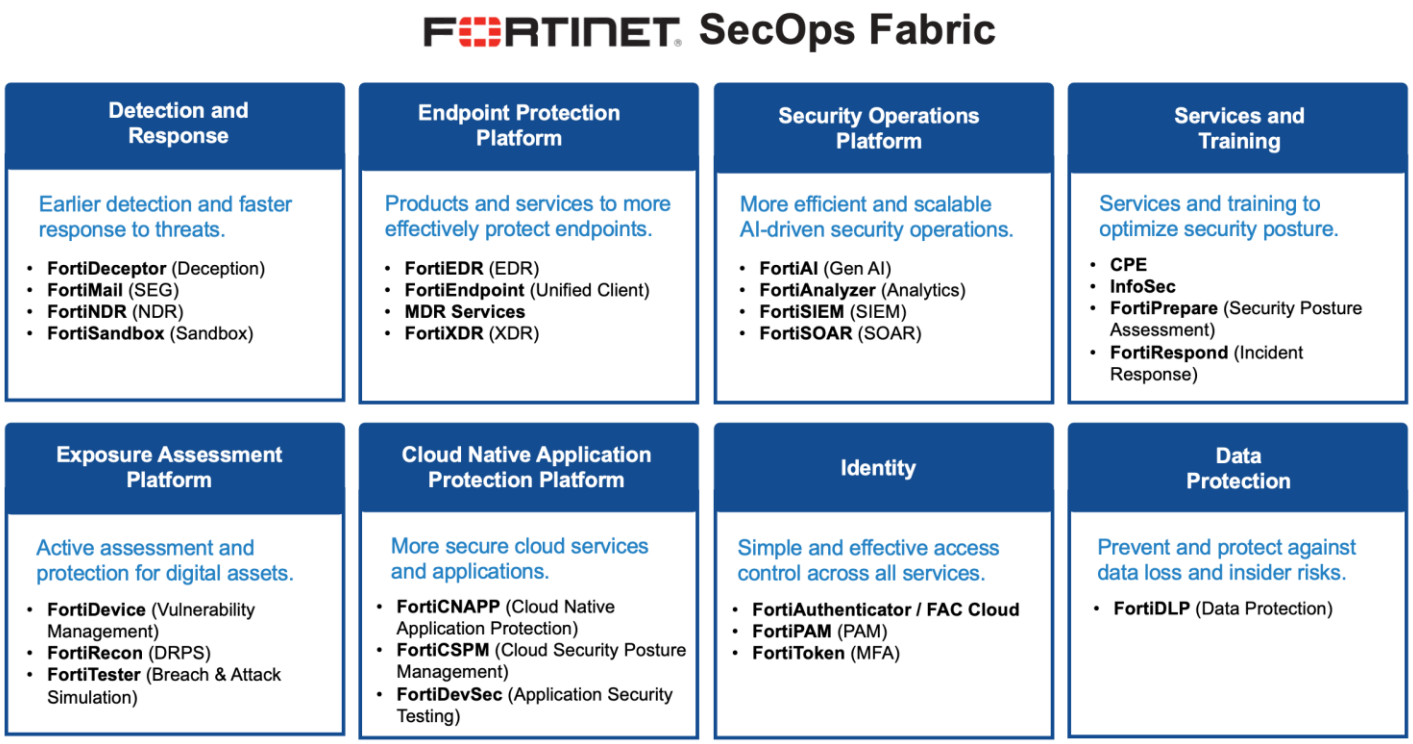
- **Identifies and contains threats earlier in the attack chain** using AI as an integrated part of a platform. This changes the game from "detect and respond" to "detect and disrupt," then "investigate and respond." Fortinet's platform shifts an organization's security approach from reactive to proactive.
- **Rapidly identifies anomalous activity** by applying AI inside and outside the organization, on and off devices, within and across domains, using domain-specific early detection and prevention sensors. Anomalous actions don't limit themselves to a single point of attack. A platform for data analysis from all ingestion points is required to build the ultimate cyber-risk context.
- **Accelerates investigation and remediation** by providing a centralized and correlated view of incidents across stages. Fortinet Security Operations delivers the ability to orchestrate and automate established processes with its SOC Automation framework, incorporating natural language guidance from a generative AI assistant.
- **Automatically shares contextual threat intelligence and response actions,** leveraging native integrations through the Fortinet Security Fabric across the integrated solution. With more than 500 cybersecurity threat experts staffing a global threat intelligence team, the combination of FortiGuard Labs and AI-fueled analytics ensures that every Fortinet-powered resource is threat-aware and ready.

Enterprise Strategy Group validated the power of the solution, quantifying and publishing its results in an Economic Validation report.[3] This report concluded that Fortinet Security Operations will provide customers with significant savings and benefits across the following three categories:

- **EDP.** Fortinet EDP technologies helped to provide earlier detection and protection against known and unknown threats for customers, employees, and partners (e.g., supply chain vendors).
- **SOC platforms and services.** Fortinet SOC platforms and services provided the insight and automation to better identify and act against threats and reduce the burden on existing security resources.
- **Improved training and preparation.** Fortinet-provided training helped cybersecurity professionals and employees quickly gain the security-related skills they require and offered services to help customers better assess and plan for efficient incident response.

The Fortinet Security Operations solution and its integrated platform approach create an opportunity for organizations to consolidate siloed security tools, providing unified threat visibility across the entire attack surface while reducing operational management complexity (see Figure 2).

Figure 2. AI-driven SecOps: Consolidate to Detect and Respond Faster



Source: Enterprise Strategy Group, a division of Informa TechTarget

[3] Source: Enterprise Strategy Group Economic Validation, *The Quantified Benefits of Fortinet Security Operations Solutions*, January 2025.

Conclusion

As the AI era fuels rapid change in IT infrastructure, applications, and services, security leaders must transform antiquated security operations functions to keep up. Nearly all (96%) of those surveyed by Enterprise Strategy Group believed that generative AI will be used for SecOps use cases soon. A more integrated, automated, AI-driven approach is required—one capable of more intelligently automating security operations. The collection of security context from all vantage points within a platform that conducts holistic analysis with AI models is the future of cybersecurity within the SOC.

As the time from initial compromise to attack execution decreases, accelerating the mean time to detect and contain is imperative for cyber-survival. Implementing a security operations approach where disruption of attacks occurs in near-real time limits risk quickly, buying time for deeper analysis to be completed. Current operating models are simply not scalable enough to accomplish this acceleration, making transformation and platform retooling a key priority for security leaders.

Enterprise Strategy Group recommends that security leaders look to integrated security solution providers like Fortinet to help transform the security operations function, accelerating threat detection and response, increasing operational efficiency, fulfilling regulatory compliance requirements, and improving overall security posture.

About Enterprise Strategy Group
TechTarget's Enterprise Strategy Group provides focused and actionable market intelligence, demand-side research, analyst advisory services, GTM strategy guidance, solution validations, and custom content supporting enterprise technology buying and selling.

contact@esg-global.com
www.esg-global.com