FORTINET

SOLUTION BRIEF

Massively Accelerate Time to Detect and Disrupt, Investigate and Remediate with the Fortinet Security Operations Solution

Executive Summary

It's likely no surprise that threat actors often have plenty of time within an organization to accomplish their objectives before detection. According to research, it takes the average security team anywhere from 16 to 204 days to detect a security incident in progress.[1] And 75% of security professionals say the current threat landscape is the most challenging it's been in the past five years.[2]

The Fortinet Security Operations Solution uses AI and advanced analytics to monitor activity across users, devices, networks, emails, applications, files, and logs and detect anomalous or malicious actions that humans may easily overlook. Further, Fortinet Security Fabric native integrations across components enable unique intelligence sharing for automated containment to predict and limit risk. As a result, security teams have more time to conduct a full investigation and remediate each incident in an automated and orchestrated manner, enhancing efficiency and consistency.

On average, customers using the Fortinet Security Operations Solution reduced their time to detect and contain attacks from 180 hours to under an hour (minutes, in most cases) and then to investigate and remediate in 10 to 15 minutes.[3]

Half of organizations say they're investing in AI and ML to detect threats faster, and 44% say they use SIEM and SOAR offerings to enhance response time.[4]

Evolving Threats and an Expanded Attack Surface Mean More Complex (and Costly) Breaches

From a constantly evolving threat landscape and an always-expanding attack surface to a significant shortage of skilled professionals, security teams have many challenges to contend with daily. As a result, even the most well-staffed groups of seasoned practitioners struggle to effectively protect their corporate networks. According to the FortiGuard incident response team—a group frequently called on to investigate cyberattacks—threat actors went undetected on corporate networks for an average of 36 days.[5] And that's much less than the 204 days published in a recent IBM report.[6] In either case, it's clear that threat actors typically have plenty of time to achieve their objectives.

Additionally, successful breaches are becoming increasingly costly to mitigate. According to a recent survey, 84% of organizations experienced one or more breaches in the past 12 months, and 48% suffered cyber incidents that cost $1 million or more to remediate.[7]

The Fortinet Security Operations Solution Accelerates Incident Detection and Response

Accordingly, organizations report that they're prioritizing investment in advanced technologies like AI and ML to detect the signs of intrusion faster, centralized technologies like SIEM and SOAR to speed response to security incidents, and integrated security products to reduce complexity.[8]

This is why the Fortinet Security Operations Solution is critical for enterprise organizations, as it offers:

- The broadest range of behavior-based sensors, deployed within a specific domain or across domains, for early detection and prevention of cyber intrusions
- Centralized security automation to aggregate, enrich, and analyze security information from those and other sensors, as well as to visualize, orchestrate, and automate incident investigation and response
- A set of add-on SOC services to assess and improve the readiness of in-house teams and technologies, augment those teams on an ad hoc or ongoing basis, and assist in the event of crisis incidents
- Built-in Generative AI assistance to inform and speed analyst actions across threat investigation, response strategy, and other key activities

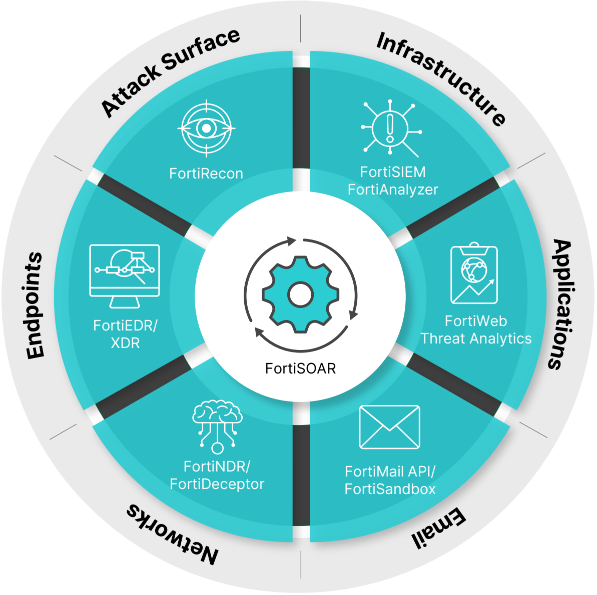

Figure 1: Fortinet Security Operations Solution

Integration Enables Automation with the Fortinet Security Operations Solution

The Fortinet Security Operations Solution is an integrated offering greater than the sum of its parts. While providing effective detection on their own, its components automatically share threat intelligence and take action to move organizations from a reactive to a proactive cyber-defense model. Following are examples of how the Fortinet Security Operations Solution integrates with other Fortinet products and enhances organizational security.

- **FortiEDR:** After making behavior-based detection of suspicious or malicious runtime activity on an endpoint device and blocking high-risk actions like encrypting files or establishing a network connection, the fabric-native integration between FortiEDR and FortiGate NGFWs allows for peer-to-peer, bi-directional sharing of threat intelligence.
- **FortiNDR:** Following a behavior-based detection of suspicious or malicious network activity from a device, FortiNDR can ingest device insight from FortiEDR and even trigger a quarantine of the originating device with its fabric-native integration.
- **FortiRecon:** After assessing external-facing assets, the fabric-native integration of FortiRecon enables it to receive additional assets from FortiGate NGFWs to include in asset inventory and scanning.
- **FortiDeceptor:** After detecting the intrusion of a threat actor, fabric-native integration enables FortiDeceptor to direct FortiGate NGFWs to block access to other devices while returning the expected device replies to continue engaging the unknowing attacker.
- **FortiSandbox:** After making a behavior-based risk rating, FortiSandbox can share that rating with many Fortinet devices, including FortiGate NGFWs and FortiMail, for real-time blocking before delivery.
- **FortiAnalyzer:** A native integration with the breadth of the Fortinet portfolio enables organizations to set event triggers and automation responses.
- **FortiSIEM:** After a rich set of analytics, including those from an ML workbench, make detections, incidents can be handled through remediation actions enabled by more than 300 technology integrations or seamlessly handed off to FortiSOAR for robust orchestration and automation.
- **FortiSOAR:** Once FortiSOAR receives alerts about suspicious activity, automated playbook actions can occur, such as deploying deception tools in the right location to fool and halt the threat actor.

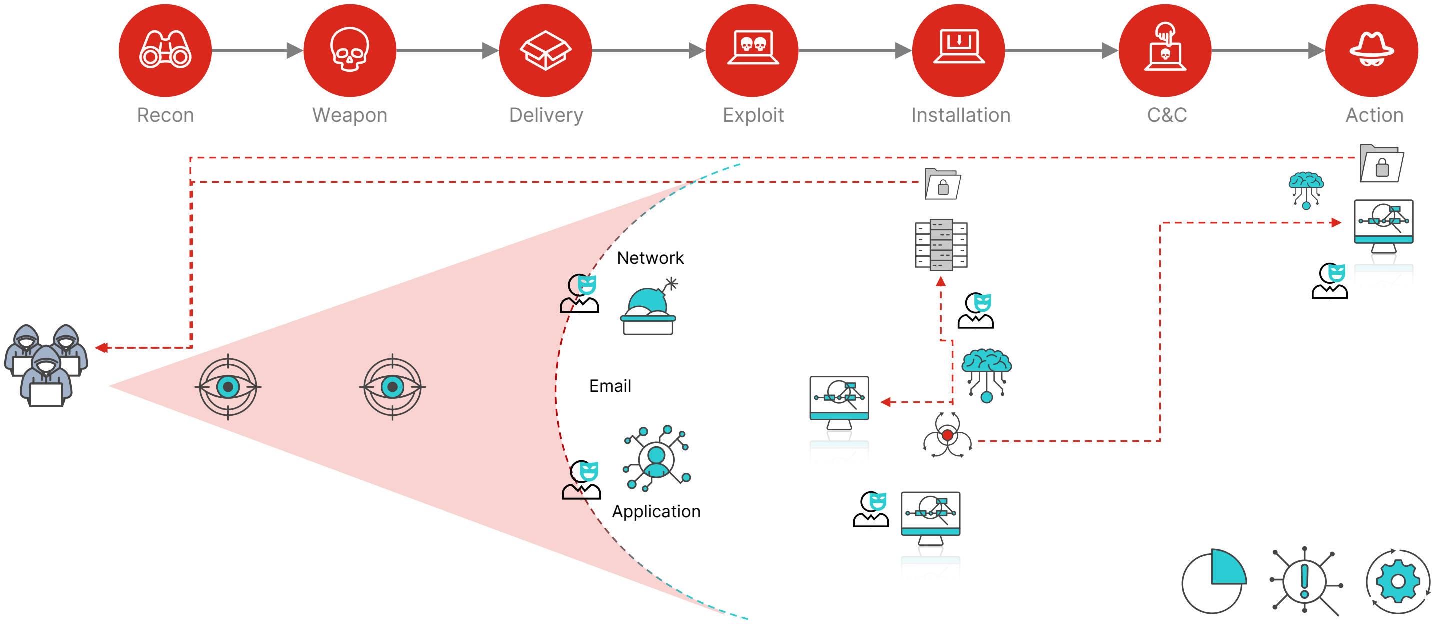

Figure 2: Fortinet Security Operations Solution components applied across the cyber kill chain

Customers Using the Fortinet Security Operations Solution See a 597% Return on Investment[9]

Investing in Fortinet Security Operations Solution components has been proven to reduce dwell time, cyber risk, and security operations effort dramatically. Specifically:

- Before making investments in early detection and prevention sensors, Fortinet customers reported that, on average, it takes their teams 21 days to detect cyber intrusions and another day and a half to contain them.[10] But after deploying products like FortiEDR, FortiNDR, FortiDeceptor, and more, customers reported an ability to detect and contain within an hour (and in minutes for most) threat actor activity.[11]
- Before deploying Fortinet Security Operations Solution components, organizations reported alert investigation and remediation took two to three days.[12] After implementing components, such as FortiAnalyzer, FortiSIEM, FortiSOAR, or others, investigations could be completed in 10–15 minutes.[13]
- Further, customers reported that a team of six (or even three, in one case) could handle the work of 12—a dramatic improvement in operational efficiency.[14]

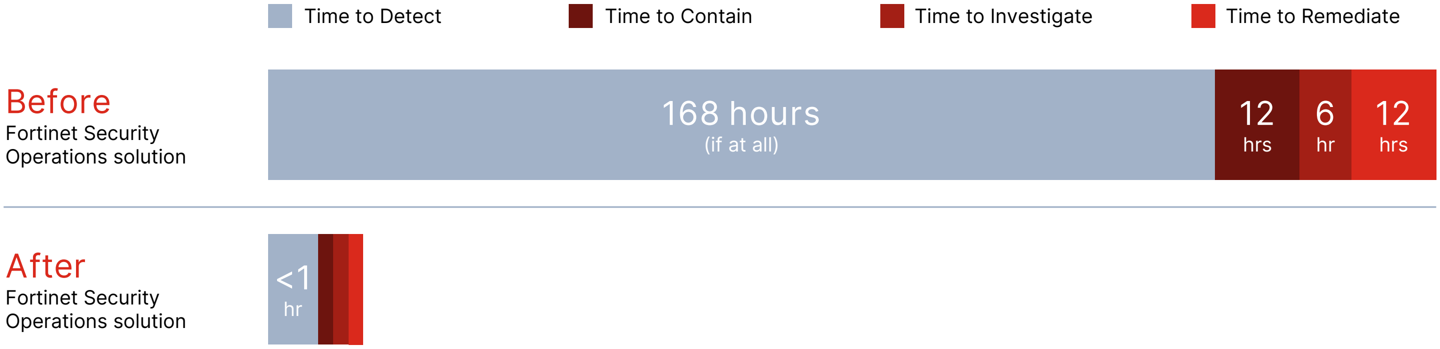

Figure 3: Quatified Benefits of the Implementing Fortinet Security Operations components

ESG Research quantified the value of these improvements concerning risk reduction and expected financial benefits. The research shows that the average organization has nearly a 30% chance of experiencing a breach in a given year, resulting in an expected annual cost of $1.4 million.[15] Combined with the faster time to detect and disrupt, investigate, and remediate, ESG Research calculated an annual $1.39 million in cost savings in terms of reduced expected breach costs by implementing components of the Fortinet Security Operations Solution.[16]

Further as a result of increased productivity after implementing the solution, security teams were projected to save an average of $1.9 million on staffing costs.[17] Ultimately, ESG Research estimates a 597% return on investment for organizations investing in the Fortinet Security Operations Solution, with a payback period of less than two months.[18]

Conclusion

The Fortinet Security Operations Solution enables organizations to introduce powerful, AI-based detection capabilities throughout their digital organization and integrate with existing security controls to dramatically reduce the time it takes to disrupt cyberattacks along the cyber kill chain. The solution also allows security teams to orchestrate, automate, and augment centralized incident investigation and remediation efforts for a faster and more consistent response. Finally, additional expert services are available to assess security operations readiness and assist with security incident response as needed. This breadth of coverage and depth of integration from the Fortinet Security Operations Solution help security teams shift from their time-consuming “detect and respond” approach to a faster “detect and disrupt, then investigate and remediate” paradigm for an active cyber defense.

[1] Cost of a Data Breach Report 2023, IBM, July 24, 2023.

[2] How the Economy, Skills Gap, and Artificial Intelligence are Challenging the Global Cybersecurity Workforce, ISC2, October 31, 2023.

[3] ESG Economic Validation: The Quantified Benefits of Fortinet Security Operations Solutions, Enterprise Strategy Group, August 1, 2023.

[4] 2023 Global Ransomware Report, Fortinet, April 20, 2023.

[5] FortiGuard Labs, accessed November 21, 2023.

[6] Cost of a Data Breach Report 2023, IBM, July 24, 2023.

[7] 2023 Global Cybersecurity Skills Gap Report, Fortinet, March 21, 2023.

[8] 2023 Global Ransomware Report, Fortinet, April 20, 2023.

[9] ESG Economic Validation: The Quantified Benefits of Fortinet Security Operations Solutions, Enterprise Strategy Group, August 1, 2023.

[10] Ibid.

[11] Ibid.

[12] Ibid.

[13] Ibid.

[14] Ibid.

[15] Ibid.

[16] Ibid.

[17] Ibid.

[18] Ibid.

December 5, 2023 11:22 AM

2431037-0-0-EN