Corporate Armor
sales@corporatearmor.com
877.449.0458

FORTINET

SOLUTION BRIEF

Fully Automate Threat Detection, Investigation, and Response with FortiXDR

Executive Summary

For years, organizations have added new cybersecurity products to address new cybersecurity threats. While individually effective in many cases, they have become overwhelming as a whole to be managed, monitored, and acted upon by overburdened security teams. As a result, organizations run an increased risk of missing potentially damaging cyberattacks that slip through the cracks, get lost in the noise, or are otherwise missed. Today, most organizations are engaged in or planning for vendor consolidation hoping to improve security and operational efficiency. However, to successfully realize those outcomes, consolidation must lead to an integrated, effective, and efficient overall security solution, rather than a collection of independent products from a single vendor. That's where FortiXDR can help, building on the broad, integrated, and automated Fortinet Security Fabric with fully automated threat detection, investigation, and response. This helps organizations improve their security posture and operational efficiency, easing the burden on security teams.

Consolidation Based on Extended Detection and Response (XDR)

According to Gartner, 80% of organizations are either currently or planning in the next two to three years to consolidate security vendors.[1] Rather than consolidating based on procurement simplicity (through a suite or enterprise license purchase), many organizations prefer to consolidate based on a security architecture like XDR. FortiXDR converts your Fortinet Security Fabric into an XDR solution. The broad range of Fortinet security controls deployed across your organization feed information into a centralized normalization layer. From there, analytics are applied to detect potential high-risk incidents and kick off investigation/classification. Finally, response actions can be predefined to handle the appropriate remediation and response. This process can be fully automated, detecting and mitigating attacks that might otherwise be lost in the volume of alerts and easing the burden on security staff.

Broad Security Controls

The Fortinet Security Fabric covers the entire digital organization including:

- Endpoints and users with endpoint protection (EPP) and identity and access management (IAM)
- The network and access layer with wired switches, wireless access points, and enterprise firewalls
- The cloud with cloud access security brokers (CASBs), web application firewalls (WAFs), and secure email gateways (SEGs)

All of the products are integrated and send telemetry to a single, central analytics platform.

Detection Analytics

A constantly increasing set of advanced analytics designed to identify early indicators of potential cyberattacks are developed by the experts of FortiGuard Labs and applied to that centralized, normalized, correlated telemetry. These detections start the next stage of incident investigation.

Artificial Intelligence (AI)-powered Investigation

Based on the type of initial detection, an automated process of investigation is dynamically followed by an AI-powered decision engine, replicating the expert actions a human security analyst would generally take. The decision engine is able to call a wide range of micro-services that provide enrichment and further analysis. A few representative examples include threat intelligence from FortiGuard Labs and third parties, file analysis such as static Yara rules or dynamic sandbox evaluation, community reputation, or user behavior baselines. But there are many more that lead to a final classification.

Predefined Response Framework

Organizations have the option to set policies in advance that will define actions to be taken based on classification, user group, risk exposure, and other criteria. This speeds the ultimate remediation and response.

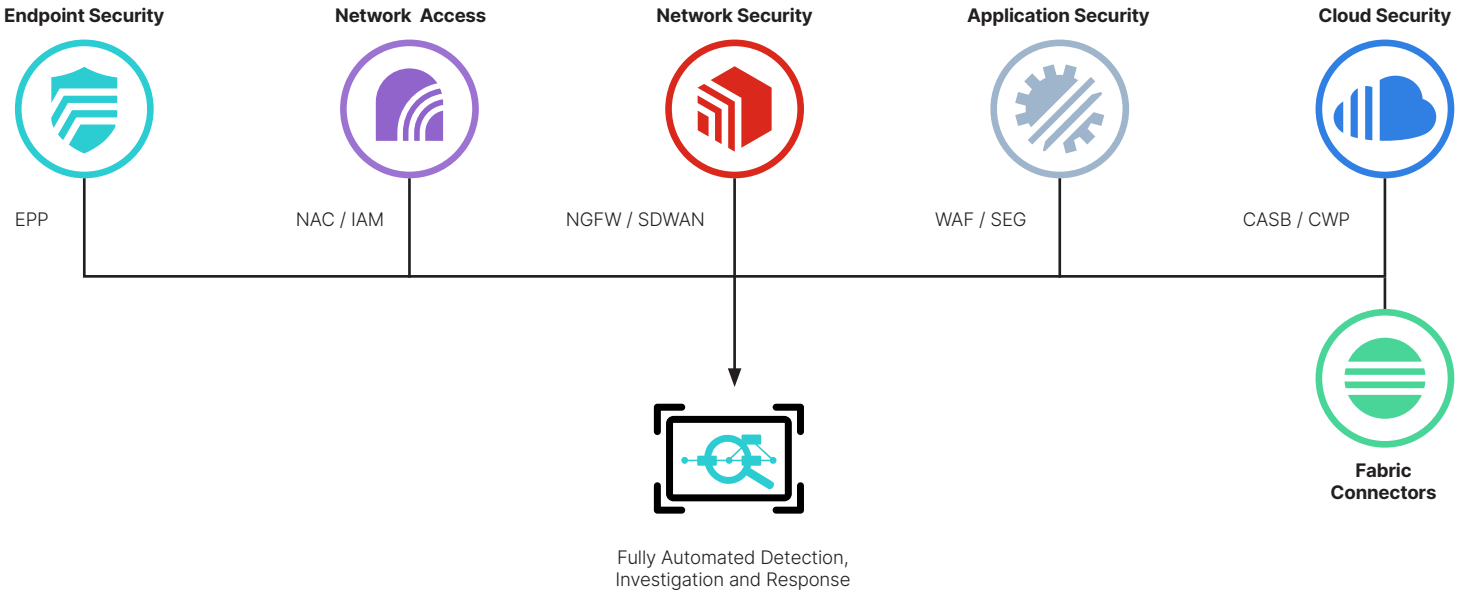

Figure 1: FortiXDR and the Fortinet Security Fabric.

The FortiXDR Difference

XDR is an early-stage concept and hot topic in the industry. However, it is in perfect alignment of our established Security Fabric vision, giving our solution a number of natural advantages. These advantages include breadth of coverage, effectiveness of individual components, and degree of automation. As a result, organizations are more likely to realize the benefits of vendor consolidation.

Breadth of Coverage

The further one can "extend" the XDR solution, the more information becomes available for analysis, enrichment, and ultimately classification. While network and endpoint components are foundational, the ability to also cover access, email, web applications, and cloud set FortiXDR apart. Similarly, while applying analysis to critical, middle Cyber Kill Chain stages of cyberattack delivery, exploit, installation, and communication is essential. The ability to extend telemetry both earlier and later to cover the entire Cyber Kill Chain is a significant advantage. Of note, insight from deception technology aids in reconnaissance detection and is complemented by late-stage data monitoring by our agent-based user and entity behavior analytics (UEBA).

On average, FortiXDR converts 100 high-value individual alerts into 10 high-fidelity incident detections for further investigation and response.

Effectiveness of Components

Organizations need not worry that deploying Fortinet security controls and XDR to consolidate vendors will result in substandard components. All Fortinet security products that feed into FortiXDR consistently receive top marks in independent testing. They demonstrate industry-leading performance in testing conducted by third parties like AV-Comparatives, ICSA Labs, NSS Labs, Virus Bulletin, and more. In fact, the Fortinet portfolio is the most independently certified in the industry.

Degree of Automation

It is certainly important to detect threats that would otherwise go unnoticed, causing great harm to the organization. However, the last thing most security teams need are more alerts. Whereas some vendors have taken the approach of correlating and presenting more security information in one place, admittedly with some nice visualizations, Fortinet has gone well beyond that. FortiXDR enables full automation of not only data normalization/correlation and detection analytics, but also the incident investigation, classification, and remediation process. As a result, it offloads rather than creates work for security teams—while increasing cybersecurity posture.

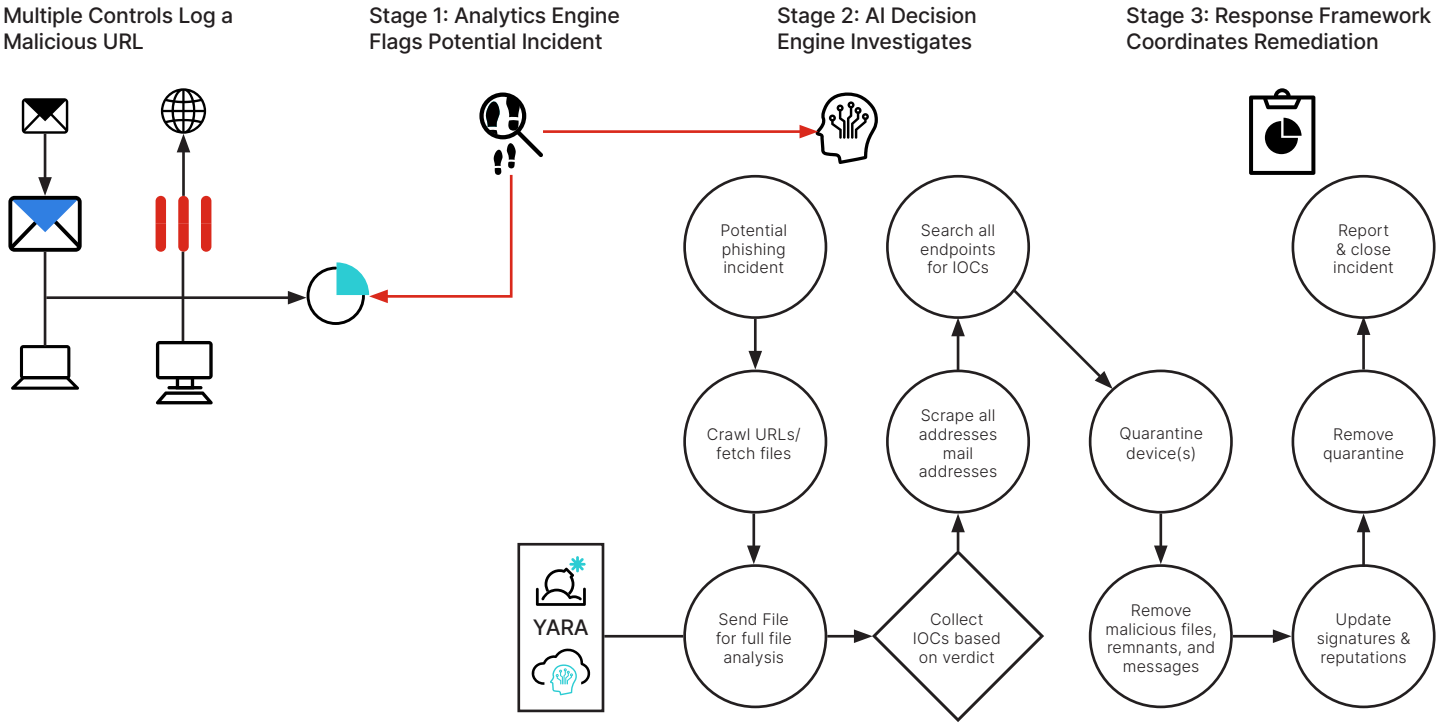

Figure 2: Phishing detection, investigation, and response.

Increase Security Posture and Operational Efficiency with FortiXDR

Given the increasing volume, sophistication, and speed of today's threat landscape, security teams are more challenged than ever—at a time that cybersecurity staff and skills remain in short supply. With so many individual (often "best-of-breed") security products to manage, security information to analyze, and potential incidents to investigate, a fundamentally different approach to enterprise security is needed. That's why so many organizations are pursuing vendor consolidation and why new solutions like XDR are so promising. FortiXDR takes a unique approach in fully automating the process of detection, investigation, and response. This increases the likelihood of identifying cyberattacks in progress (before they turn into data breaches or successful ransomware incidents). Further, it eases the burden on security teams, reserving them for higher-value strategic activities.

[1] John Watts and Peter Firstbrook, "Security Vendor Consolidation Trends: Should You Pursue a Consolidation Strategy?" Gartner, July 30, 2020.

FORTINET

www.fortinet.com

April 21, 2021 10:57 AM
sb-FA-fully-automate-threat-detection-investigation-and-response-w-FortiXDR-042021
859551-A-0-EN