FORTINET

WHITE PAPER

# Purpose-built Integrated NOC-SOC Management and Analytics

## Fortinet Security Fabric Bridges the Network and Security Architecture Gap

## Executive Summary

**Security with high performance shouldn't be an oxymoron for enterprise networks. But it can often seem that way to those working within siloed network operations centers (NOCs) and security operations centers (SOCs). Security architects have an opportunity to break down those silos, or at least bridge the gap between them, and the Fortinet Management and Analytics solution offers them the means for doing so. As a core component of the Fortinet Security Fabric, Fortinet Management and Analytics is a purpose-built NOC-SOC solution that integrates operational visibility, provides continuous quantified security assessments, and delivers workflow automation across NOC, SOC, and IT service management (ITSM) functions.**

## Aligned Security and Operations Visibility

NOC and SOC teams have common objectives. Both must continually improve their ability to monitor events on the network, escalate issues, and triage incidents.[1] But their perspectives differ, and so do their tools. While the NOC team is at home with Simple Network Management Protocol (SNMP)/syslog-based network monitoring, ticketing, and reporting systems, the SOC team focuses on security information and event management (SIEM) systems that can pinpoint compromised users and servers, guide incident response and remediation, and offer tools for risk management and mitigation.

Without requiring forklift upgrades or organizational restructuring, the Fortinet Management and Analytics solution provides a consolidated view of operations and security, enabling NOC and SOC staff to pursue their various goals, but in alignment with one another. Because the solution integrates and cross-correlates NOC and SOC data, neither team needs to spend time sharing or interpreting the other's data. Thus, detection, response, and recovery can happen in minutes rather than days or weeks. This is important not only because cybersecurity resources are limited but also because of the acceleration of cyber crime: with highly automated attacks and swarm technology, volumes of exploits and the number of malware variants are exploding. Earlier this year, threat intelligence research revealed 7,230 unique exploit detections and 23,945 unique malware variants during a single quarter.[2]

### Key Solution Features and Components

The Fortinet Management and Analytics solution is based on the core elements of the Fortinet Security Fabric: **FortiManager** device and policy management, **FortiAnalyzer** reporting and analytics, and **FortiGate** next-generation firewalls (NGFWs). The number, form factors, and types of NGFWs (edge, data center, internal segmentation, branch) are completely adaptable to the organization's needs, as is its management. The solution also incorporates the latest capabilities of the **FortiSIEM** security information and event management system, with its full configuration management database (CMDB).

The **Fabric View** dashboard in FortiManager 6.0 provides a unified perspective for both SOC and NOC teams. (See Figure 1.) Through this dashboard, administrators can obtain accurate, up-to-theminute status on every device in the organization's Security Fabric. In particular, SOC teams can use the feed of operational data from the FortiSIEM CMDB to accurately assess the scope of security alerts and issues. This is a more efficient approach than using standalone SIEM products that generate their own alerts, which must then be manually cross-referenced with NOC data.

While security analysts work to identify and evaluate the business impact of potential incoming threats, the operations team can also refer to the Fabric View dashboard to immediately see if any of the performance degradations or irregularities they are experiencing are the result of a security incident. With this insight, the operations team is more likely to understand and readily consent to security team requests to reconfigure or quarantine network assets.

The fabric topology of the Fortinet Management and Analytics solution ensures real-time dissemination of alerts and responses among all the devices in the network. This, combined with a real-time global intelligence feed from **FortiGuard Labs,** enables security teams to identify even new and sophisticated threats, thus stopping all threats in their tracks.

Because most organizations operate in multi-cloud (public, private, and hybrid) environments, Fortinet provides both appliances and virtual versions of its NOC-SOC solution components. Virtualized offerings are available for VMware NSX, Amazon Web Services, Microsoft Azure, Cisco ACI, and Nuage.

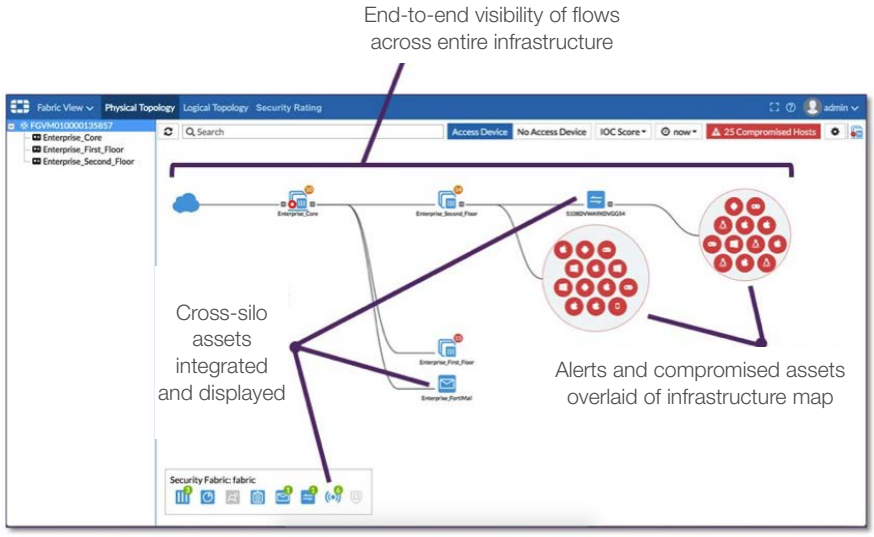


Figure 1: FortiGate and FortiAnalyzer provide a real-time alert feed into FortiManager 6.0, which represents the real-time status of all security fabric devices, including endpoint and user information. This helps security teams to quickly pinpoint risks and respond judiciouusly.

## Automation Across Silos

An integrated perspective enables a faster and more informed response to threats. Yet, with the accelerating pace of threats, human teamwork is not enough. Security architects need to beat cyber criminals at their own game—by leveraging automation and artificial intelligence (AI) technologies to scale protection throughout the enterprise.

### Streamlining Incident Management

Security incident management typically involves multiple steps and touchpoints: the security analyst in the SOC, the internal or external ITSM team, and finally the NOC staff. To minimize response times, the Fortinet NOC-SOC solution automates nearly every routine part of the workflow.

One part of the workflow is ITSM. Fortinet is working with various ITSM vendors to create seamless integrations between their software and the Fortinet management consoles, enhancing the efficiency of ITSM users within the organization or at a service provider. Because this is an integration rather than an add-on or replacement product, organizations avoid the deployment, administration, and training costs that might be associated with a new ITSM product deployment.

For example, enterprises that choose the Fortinet solution can leverage their existing ServiceNow ITSM subscriptions to create automated workflows in which security incidents created in FortiAnalyzer or FortiSIEM are automatically passed to ServiceNow Security Incident Response. Analysts working from the ServiceNow platform can determine how to resolve the incident and choose from a catalog of responses. Responses that require changes to device configuration are automatically implemented through FortiManager. These capabilities reduce response times to minutes rather than days and enable limited staff to focus on expert-level decisionmaking rather than monitoring and information routing.

### Intelligence Enables Perspective and Retrospective Analysis

While automation makes known processes happen faster, AI can help revise those processes based on new patterns of cyber-criminal behavior. For the past six years, Fortinet's FortiGuard Labs has been developing and training its FortiGuard AI self-evolving threat-detection system using supervised machine learning techniques. FortiGuard AI autonomously collects, analyzes, and classifies threats, and subsequently develops highly accurate defensive signatures to block them in rapid succession. It then disseminates the signatures throughout the Fortinet Security Fabric. This includes the ability to define the differences between clean and infected files and to develop signatures that catch zero-day threats before they are even written.

Predictive analysis is not enough, however, as many malicious servers are discovered after they have already caused harm somewhere in the world. The **FortiGuard Indicators of Compromise (IOC)** service helps security analysts identify risky devices and users based on a collection of artifacts that are known to indicate a high probability of a computer intrusion. The IOC service consists of a package of approximately 500,000 IOCs gleaned from a variety of sources around the globe, which is delivered daily to FortiAnalyzer and FortiSIEM devices. Armed with this global threat intelligence, security analysts can scan their NOC's weblogs to identify past communications with servers that are now known to be malicious. They can then work with the operations team to mitigate the impact of such communications.

## Quantifiable Security For Better Decision-Making

Even if security architects make great strides in bridging the NOCSOC gap, they must also be able to demonstrate the results. They may need to respond to demands for proof of compliance or to executive requests for clear information on security posture. And nearly every executive wants to know "How secure are we?"

The Security Rating feature in FortiAnalyzer helps security architects answer this question more competently and efficiently than they could in the past. Fortinet has leveraged its deep experience in the security industry to develop a series of tests, based on the most important security best practices, which run repeatedly on the deployed FortiGate NGFWs. The results are presented as a cumulative companywide score, called a Security Rating, as well as a prioritized list of issues to be resolved. (See Figure 2.)

Security Ratings can be tracked over time to indicate trends and show the return on investment of various security initiatives. Also, because every organization must balance the need for security controls with the network performance demands of the business, the Security Rating provides two forms of context to support risk tolerance analysis.

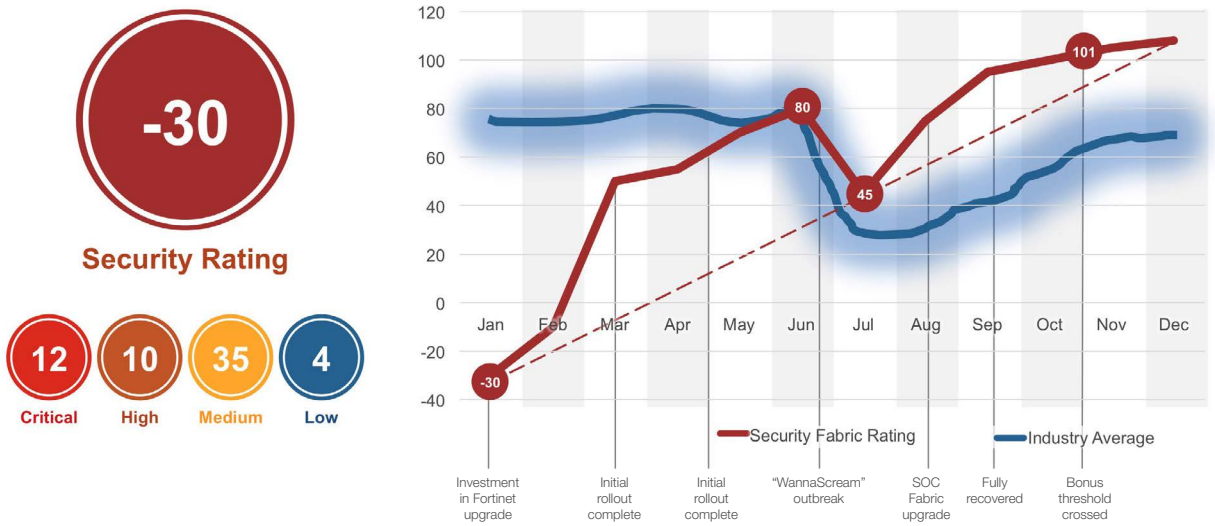


Figure 2: The security rating feature provides both point-in-time and trend analysis, as well as a comparison with industry averages.

**First**, the Security Ratings trendline (the red line in Figure 2) can be plotted on a timeline of known threats, which demonstrates due diligence in protecting against those threats. **Second**, the trendline can be compared with an appropriate industry average trendline (the blue line in Figure 2, delivered through a FortiGuard service). This offers a real-world assessment of the organization's security posture.

## Conclusion

The fully meshed and collaborative approach of a security fabric is the ideal way to enable secure business growth and effective risk management, especially when IT budgets and resources are constrained. And this broad, integrated, and automated solution is available only from Fortinet.

As the world leader in network security, Fortinet has more than 340,000 customers in a wide range of industry sectors around the world. This broad base of industry experience and threat intelligence gives security architects a solid foundation from which to bridge the NOC-SOC gap with confidence.

[1] Nelson Hernandez, "NOC/SOC Integration: Opportunities for Increased Efficiency in Incident Response within Cyber-Security," SANS Institute, January 26, 2018.

[1] "Fortinet Threat Landscape Report Q2 2018," Fortinet, August 2, 2018.

FORTINET

www.fortinet.com



September 14, 2019 12:01 AM

249926-A-A-EN

D:\Fortinet\White Paper\NOC & SOC Management & Analytics\wp-FA-purpose-built-integrated-noc-soc-management-and-analytics