EVOLVING ENTERPRISE SECURITY OPERATIONS

For Adaptive Visibility, Focus, and Action

In recent years, the roles of enterprise information security leaders—Chief Information Security Officers (CISOs)—have seen a fundamental shift in their focus. As organizations of all sizes face rapidly increasing frequency and sophistication of cyber attacks, these threats have taken an expanding toll on network security, compliance, performance, and availability—and many have resulted in the theft or exposure of sensitive data.

Enterprises that have sustained breaches can testify to the catastrophic impacts they have had on their organizations' viability. The fallout can have lasting impacts on a company's brand, with negative, long-term effects on customer trust and loyalty. Many of these organizations have also experienced collateral damages such as fines, lawsuits, credit problems, and decreased stock prices. The public exposure that comes with a breach reaches well beyond the IT realm, touching every line of business within the organization.

SECURITY AND RISK MANAGEMENT CHALLENGES

You are tasked with delivering greater visibility and tighter controls over current and future risks. Establishing a new, inclusive approach to securing enterprises at a strategic level is no small feat with the many dynamic environmental complexities:

- A rapidly expanding threat landscape
- A shortage of skilled cybersecurity personnel
- A lack of integrated security and risk-management tools
- Difficulties in complying with regulatory standards
- Challenges of managing the global information assets
- Limited cross-organization collaboration (including network and security operations centers)

FORTINET SECURITY OPERATIONS SOLUTION OVERVIEW

Fortinet has taken an architectural approach to security, integrating its solutions with a single operating system across a collaborative Security Fabric. The Fortinet Security Fabric was designed to connect security solutions into a unified framework, allowing organizations to dynamically adapt to their evolving IT Infrastructure and defend a rapidly changing attack surface.

Fortinet's Security Operations solution extends the Security Fabric by bringing in context from network elements beyond the Fortinet family of products. This provides organizations with a comprehensive solution that covers both IT and security risk management across the entire enterprise, including pre-existing infrastructure. Our solution is comprised of FortiSIEM, FortiAnalyzer, and FortiManager, as well as FortiGuard threat intelligence data.

FORTISIEM

FortiSIEM provides a comprehensive, holistic, and scalable solution for managing security, performance, and compliance from IoT to the cloud—delivered through a single-pane-of-glass view of the organization. It encompasses not only Fortinet solutions, but also non-Fortinet sources within the infrastructure.

FortiSIEM reduces complexity and accelerates threat detection capabilities while providing greater control and visibility of the security and functionality of the network.

- **Audit Trails of User Activity**—tracks user context in real time via audit trails of IP addresses, user identity changes, and physical/geo-mapped location data context
- **Role-based Access Controls**—for restricting access to GUI and data at various levels
- **Cross-security Platform Integration**—through continual self-discovery, provides organizations with an integrated view of the network-attached elements (including non-Fortinet products) to improve visibility, focus, and adaptive awareness from IoT to the cloud
- **Automated Device and Configuration Discovery**—intelligent infrastructure and application discovery engine that can find and map topologies of physical and virtual infrastructure, on-premises, and public/private clouds simply using credentials

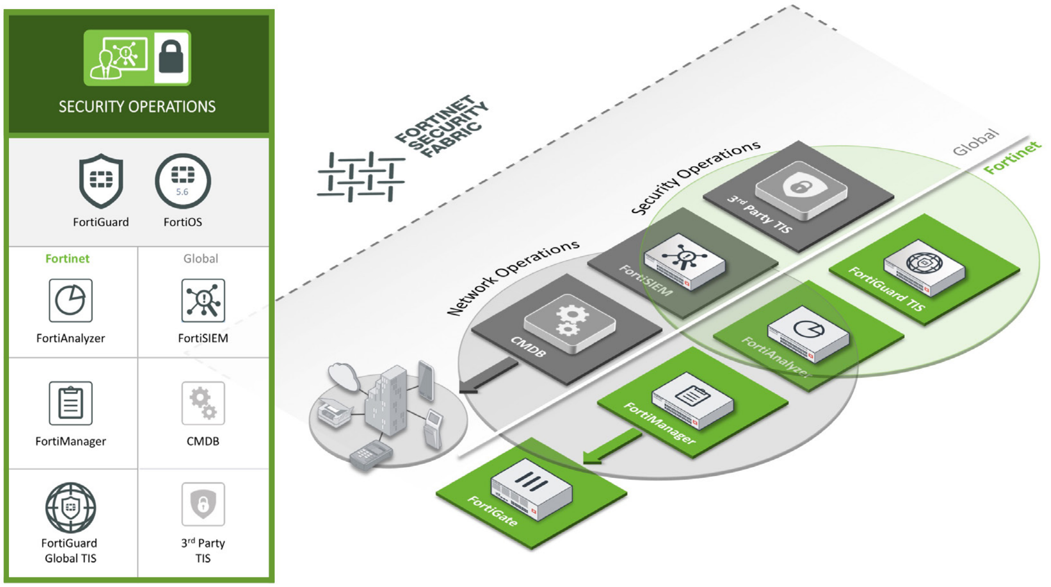
SECURITY OPERATIONS REQUIREMENTS

- Visibility across an expanding threat landscape
- Integration of mounting information from disparate systems
- More skilled cybersecurity personnel

FORTINET SECURITY OPERATIONS SOLUTION

- FortiSIEM
- FortiAnalyzer
- FortiManager
- FortiGuard Threat Intelligence Services

- **Real-time Correlation of SOC and NOC Analytics**—brings together, in real time, cross-correlated threat data traditionally monitored in separate systems providing a more holistic view of the organization to speed detection



FORTIANALYZER + FORTIGUARD INDICATORS OF COMPROMISE (IOC)

FortiAnalyzer collects, analyzes, and correlates log data from a distributed network of Fortinet enterprise firewalls for increased visibility and robust security alert information. When combined with a subscription to the **FortiGuard Indicator of Compromise (IOC)** service, it also provides a prioritized list for compromised hosts to allow for rapid action. IOC features include:

- Scans FortiGate security logs to identify suspicious traffic patterns
- Automates a breach defense system that continuously monitors the network for attacks
- Presents a prioritized list of hosts that are compromised and require further action
- Improves security posture and helps safeguard organizations through accurate detection of advanced threats

FORTIMANAGER

FortiManager provides single-pane-of-glass management across the entire extended enterprise for insight into network-wide traffic and threats. It includes enterprise-class features for containing advanced threats, as well as industry-leading scalability to manage up to 10,000 Fortinet devices.

FORTIGUARD THREAT INTELLIGENCE SERVICES

The Fortinet Security Operations solution also includes access to advanced threat intelligence, such as:

- **FortiSIEM Threat Intelligence Feed**—cyber threat intelligence delivered via the Fortinet Developers Network
- **Cyber Threat Intelligence Feed**—threat data available to all customers, including malicious IP addresses, malicious URLs, and phishing URLs
- **Weekly Threat Brief**—an email overview of the most prevalent threats that FortiGuard Labs collected for that week

SUMMARY

The Fortinet Security Operations solution reduces the complexity in managing security, performance, and compliance with a comprehensive, single-pane-of-glass approach that provides enterprises and CISOs with greater visibility and control over their current and desired risk posture. The adaptive, scalable, and holistic view of the threat landscape and global threat intelligence, along with real-time, cross-correlated NOC and SOC analytics, enables enterprises to more rapidly detect and respond to threats and focus on remediation efforts.

FORTINET

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
905 rue Albert Einstein
06560 Valbonne
France
Tel: +33.4.8987.0500

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA HEADQUARTERS
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
Tel: +1.954.368.9990

November 23, 2016