SOLUTION BRIEF

FortiSIEM for Network Visibility, Event Correlation, and Risk Management

Satisfying NSA CSfC Requirements for Continuous Monitoring of Data Transit

Executive Summary

The National Security Agency's (NSA) Commercial Solutions for Classified (CSfC) program knows architecting and deploying layered, secure networks with best-in-class COTS products for mission-critical data isn't enough. Unrelenting bad actors and sophisticated threats can find ways to circumvent protections and exploit any network if left unchecked. Every host, network device, and network segment can present just the right vulnerability and opportunity for an attacker to avoid detection and move to the next phase in their campaign.

Because of this, the NSA CSfC released guidance for Continuous Monitoring (CM) of data in transit. The guidance provides a baseline of expected network and system behavior, detection of misconfigurations in solution products, and analysis of system audit logs to detect unauthorized activity. In order to meet the guidance, CSfC customers will have to enable audit logging in key components of the network and consolidate them into a single tool.

The Fortinet FortiSIEM multivendor security incident and event management (SIEM) solution provides the visibility, correlation, automated response, and remediation in a single, scalable solution.

FortiSIEM combines a broad feature set, easy-to-use interface, and massive scalability into a fully featured SIEM platform appropriate for deployment into any size organization from a few devices to large multi-tenant networks.

FortiSIEM for Network Visibility, Event Correlation, and Risk Management

FortiSIEM offers an affordable and all-inclusive solution, delivering continuous monitoring for various CSfC capability packages, whether cross-domain environments or a standalone system. Fortinet's patented architecture in FortiSIEM enables unified data correlation and analytics from diverse sources, which includes logs, KPI metrics, SNMP traps, important security alerts, and configuration changes made to the devices, providing a comprehensive view of the security posture for networks large or small, such as flyaway kits and on-premises static devices.

The breadth of features offered by FortiSIEM allows for massively scalable architecture, supporting a wide variety of IT products and making it an attractive choice for any environment that requires visibility and actionable intelligence when implementing continuous monitoring as part of a holistic risk management and defense-in-depth information security strategy integrated into CSfC architectures.

CSfC CM capabilities are designed with a multilayer approach to complement the functional architecture of a CSfC solution. CSfC CM solutions provide high visibility across the monitored network, allowing analysts to validate the operational status of encryption components by observing network activity both before and after encryption points and within management networks and at eight distinct but strategic monitoring points within the CSfC architecture. FortiSIEM can meet CM needs by implementing its collectors and workers at monitoring points, collecting data for analysis and notifying system activities to the FortiSIEM supervisor, which runs all the core services and manages other nodes in the cluster. FortiSIEM is a powerful and feature-rich monitoring and analytics solution with many use cases across the enterprise.

FortiSIEM is designed to provide comprehensive data collection with rapid-scale architecture as required and data aggregation from each MP into centralized monitoring SIEM systems. FortiSIEM offers security administrators the collective dataset to monitor the security posture of the CSfC solution and report on security-relevant events within the infrastructure. FortiSIEM accomplishes distributed event

correlation through a defined set of automated notification capabilities and dashboards built to identify targeted information of interest. Some of the key innovative and powerful technologies included in the FortiSIEM solution:

- Distributed event correlation
- Distributed querying and reporting
- A high-performance, optimized NoSQL event database

Pre-deployment planning is an essential step to ensuring a successful implementation that will meet CSfC requirements. Before embarking on a deployment, performing detailed design and planning focused on visibility, performance, efficiency, and resiliency is recommended.

Design for CSfC Use Case

FortiSIEM can be used for many applications across the enterprise; however, for CSfC CM use, the following can be included per the Continuous Monitoring Annex:

- Log ingestion and storage
- SOC analytics and incident response
- Performance monitoring
- Compliance reporting
- Management reporting

FortiSIEM Architectures

FortiSIEM is a flexible solution that can be deployed in different ways to meet different performance, scalability, and topological requirements. The main deployment enclaves are remote, enterprise, and service provider. Small enclave would be the focus for CSfC deployment, which is most applicable since remote deployments are typically smaller and can consist of an all-in-one or a small distributed solution (see Figure 1).

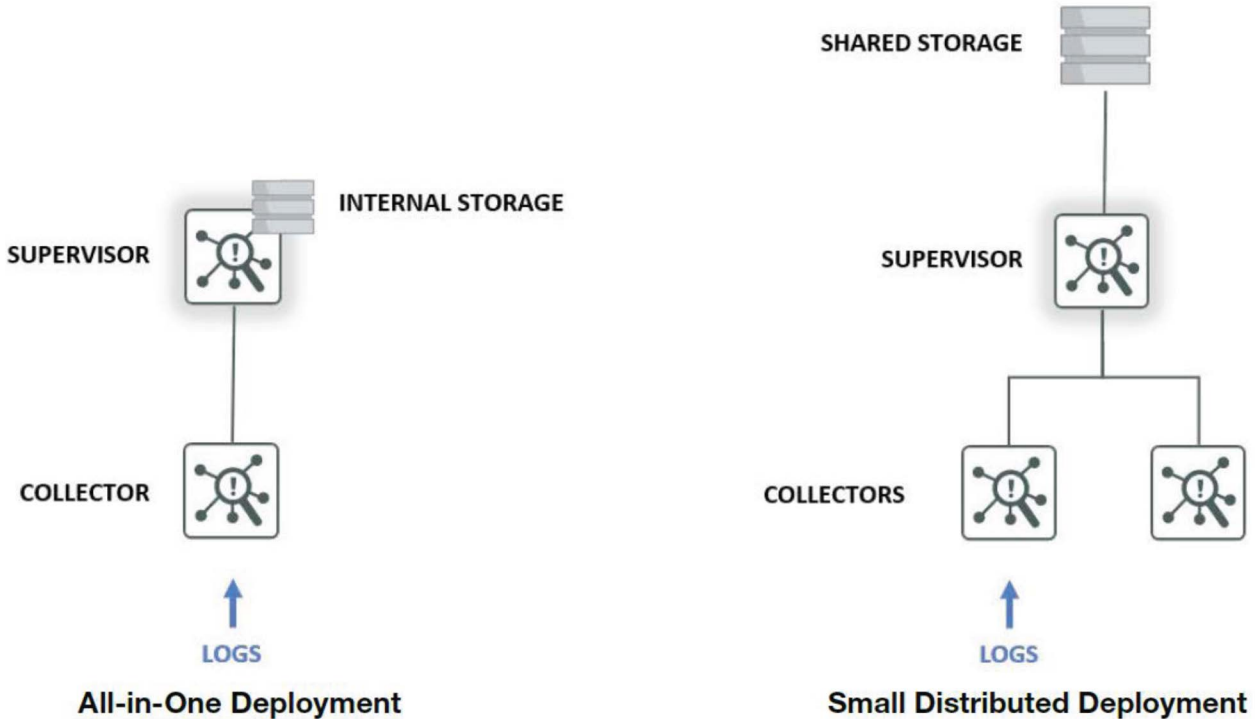

Figure 1: FortiSIEM architecture diagram.

The FortiSIEM all-in-one architecture is an easy-to-deploy, self-contained, single-server solution that is suitable for smaller deployments. It uses a local disk on the virtual appliance, or the in-built hardware appliance storage, for event storage. It is limited in scalability due to the local storage and does not support the Rapid Scale Architecture because worker nodes cannot be added to an all-in-one deployment.

While a single all-in-one node delivers a functional system, most organizations should plan to also deploy at least one collector to assist with log collection, and to support FortiSIEM server agents. Enclaves requiring additional scalability to meet current or future capacity and performance requirements should use a distributed solution with shared storage.

FortiSIEM Database Structure

- FortiSIEM uses multiple databases presented in a single GUI.
- In a multi-node deployment, the event database is moved to external storage for scalability.
- NFS or elastic search is supported.

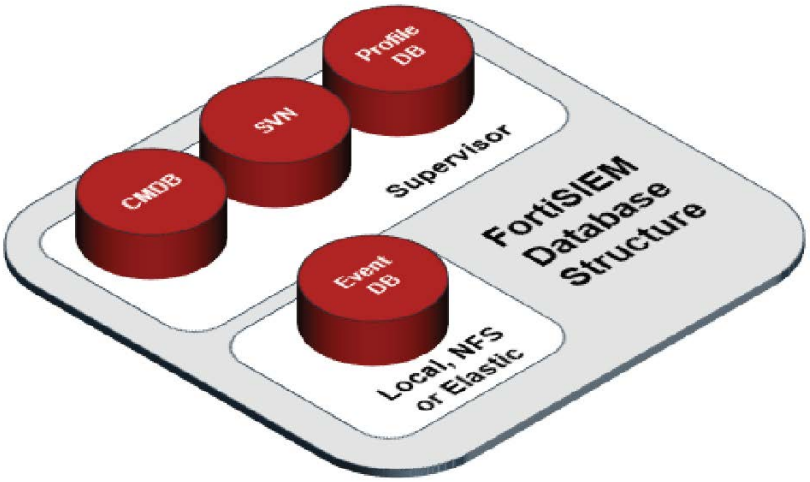

Figure 2: FortiSIEM database structure diagram.

The Life of an Event in FortiSIEM

Fortinet offers a virtual appliance architecture using a three-tier structure to provide an easily scalable solution that can start as a small single-node deployment, and rapidly scale to a large, high-performance system as needed.

- The supervisor node provides core functionality, and in a smaller solution, it can deliver an all-in-one system specifically applicable to a CSfC solution use case.
- Worker nodes are used in conjunction with the supervisor node to scale event processing and report which may or may not be needed depending on deployment size and use case.
- Collectors can be used to provide remote site log collection, and to offload log collection from the supervisor or worker nodes for increased scalability.

FortiSIEM Features

Real-time Operational Security Analytics

- Continually update on security events and provide accurate device context configuration, installed software and patches, running services
- FortiSIEM offers system and application performance analytics along with contextual interrelationship data for rapid triaging of security issues
- User context, in real time, with audit trails of IP addresses, user identity changes, physical and geomapped location
- Detect unauthorized network devices, applications, and configuration changes
- Out-of-the-box predefined reports supporting a wide range of compliance auditing and management needs including PCI DSS, HIPAA, SOX, NERC, FISMA, ISO, GLBA, GPG13, SANS Critical Controls, COBIT, ITIL, ISO 27001, NERC, NIST 800-53, NIST 800-171, NESA Performance Monitoring

Performance Monitoring

- Monitor basic system/common metrics
- System level via SNMP, WMI, PowerShell
- Application level via JMX, WMI, PowerShell
- Virtualization monitoring for VMware, HyperV—guest, host, resource pool, and cluster level
- Storage usage, performance monitoring for EMC, NetApp, Isilon, Nutanix, Nimble, Data Domain environments
- Specialized application performance monitoring
- Microsoft Active Directory and Exchange via WMI and PowerShell
- Databases—Oracle, MS SQL, MySQL via JDBC
- VoIP infrastructure via IPSLA, SNMP, CDR/CMR
- Flow analysis and application performance for NetFlow, S-Flow, Cisco AVC, NBAR, IPFix environments
- Ability to add custom metrics
- Baseline metrics and detect significant deviations

External Technology Integrations

- Integration with any external website for IP address lookup
- API-based integration for external threat feed intelligence sources
- API-based two-way integration with help desk systems, including seamless, out-of-the-box support for ServiceNow, ConnectWise, and Remedy
- API-based two-way integration with external CMDB, including out-of-the-box support for ServiceNow, ConnectWise, Jira, and Salesforce
- Kafka support for integration with enhanced Analytics Reporting (i.e., ELK, Tableau, and Hadoop)
- API for easy integration with provisioning systems
- API for adding organizations, creating credentials, triggering discovery, modifying monitoring events

Real-time Configuration Change Monitoring

- Collect network configuration files, stored in a versioned repository
- Collect installed software versions, stored in a versioned repository
- Automated detection of changes in network configuration and installed software
- Automated detection of file/folder changes, including Windows and Linux, and who and what details
- Automated detection of changes from an approved configuration file
- Automated detection of windows registry changes via FortiSIEM Windows Agent

Notification and Incident Management

- Policy-based incident notification framework
- Ability to trigger a remediation script when a specified incident occurs
- API-based integration to external ticketing systems, including for ServiceNow, ConnectWise, and Remedy
- Incident reports can be structured to provide the highest priority to critical business services and applications
- Trigger on complex event patterns in real time
- Incident Explorer, dynamically linking incidents to hosts, IPs, and user to understand all related incidents quickly

External Threat Intelligence Integrations

- APIs for integrating external threat feed intelligence, malware domains, IPs, URLs, hashes, Tor nodes
- Built-in integration for popular threat intelligence sources, including Threat-Stream, CyberArk, SANS, Zeus, ThreatConnect
- Technology for handling large threat feeds, incremental download and sharing within cluster, real-time pattern matching with network traffic. All STIX and TAXII feeds are supported.

Summary

To defend against adversaries in modern cyber warfare, CSfC customers need maximum visibility into multi-enclave network activity of their users, devices, and data. They must also have automated correlation and remediation of audit logs to ensure that mitigations are effective in minimizing or altogether preventing the infiltration of malicious actors and extraction of classified data.

FortiSIEM is the ideal solution to provide industry-leading speed in data correlation and insights into complex, seemingly unrelated activity to accurately identify attempts to compromise the network. For more information on the Fortinet Continuous Monitoring solution, please go to https://www.fortinet.com/products/siem/fortisiem or contact us at federalsales@fortinet.com.

Copyright © 2020 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

July 9, 2020 6:07 AM

712912-0-0-EN

D:\Fortinet\Solution Briefs\Teal Solution Brief\Federal CFSC Asset\sb-FA-fortisiem-for-network-visibility-event-correlation-and-risk-mgmt-792020