DATA SHEET

FortiSIEM®

Unified event correlation and risk management for modern networks

Uptime is a mandate for today's digital business and end users do not care if their application's problems are performance or security-related. That's where FortiSIEM comes in.

Unified NOC and SOC Analytics (Patented)

Fortinet has developed an architecture that enables unified data collection and analytics from diverse information sources including logs, performance metrics, SNMP Traps, security alerts and configuration changes. FortiSIEM essentially takes the analytics traditionally monitored in separate silos — SOC and NOC — and brings that data together for a comprehensive view of the security and availability of the business. Every piece of information is converted into an event which is first parsed and then fed into an event-based analytics engine for monitoring real-time searches, rules, dashboards and ad-hoc queries.

Machine Learning/UEBA

FortiSIEM uses Machine Learning to detect unusual user and entity behavior (UEBA) without requiring the Administrator to write complex rules. FortiSIEM helps identify insider and incoming threats that would pass traditional defenses. High fidelity alerts help prioritize which threats need immediate attention.

User and Device Risk Scoring

FortiSIEM build a risk scores of Users and Devices that can augment UEBA rules and other analysis. Risk scores are calculated by combining several datapoints regarding the user and device. The User and Device risk scores are displayed in a unified entity risk dashboard.

Highlights

- Cross Correlation of SOC and NOC Analytics
- Real-Time Network Analytics
- Security and Compliance out-of-the-box
- Single IT Pane of Glass
- Cloud Scale Architecture
- Self Learning Asset Inventory (CMDB)
- Multi-tenancy
- MSP/MSSP Ready
- Available as a virtual or physical appliance

Highlights

Distributed Real-Time Event Correlation (Patented)

Distributed event correlation is a difficult problem, as multiple nodes have to share their partial states in real time to trigger a rule. While many SIEM vendors have distributed data collection and distributed search capabilities, Fortinet is the only vendor with a distributed real-time event correlation engine. Complex event patterns can be detected in real time. This patented algorithm enables FortiSIEM to handle a large number of rules in real time at high event rates for accelerated detection timeframes.

Real-Time, Automated Infrastructure Discovery and Application Discovery Engine (CMDB)

Rapid problem resolution requires infrastructure context. Most log analysis and SIEM vendors require administrators to provide the context manually, which quickly becomes stale, and is highly prone to human error. Fortinet has developed an intelligent infrastructure and application discovery engine that is able to discover both physical and virtual infrastructure, on-premises and in public/private clouds, simply using credentials without any prior knowledge of what the devices or applications are.

An up-to-date CMDB (Centralized Management Database) enables sophisticated context aware event analytics using CMDB Objects in search conditions.

Dynamic User Identity Mapping

Crucial context for log analysis is connecting network identity (IP address, MAC Address) to user identity (log name, full name, organization role). This information is constantly changing as users obtain new addresses via DHCP or VPN.

Fortinet has developed a dynamic user identity mapping methodology. Users and their roles are discovered from on-premises or Cloud SSO repositories. Network identity is identified from important network events. Then geo-identity is added to form a dynamic user identity audit trail. This makes it possible to create policies or perform investigations based on user identity instead of IP addresses — allowing for rapid problem resolution.

Flexible and Fast Custom Log Parsing Framework (Patented)

Effective log parsing requires custom scripts but those can be slow to execute, especially for high volume logs like Active Directory, firewall logs, etc. Compiled code on the other hand, is fast to execute but is not flexible since it needs new software releases. Fortinet has developed an XML-based event parsing language that is functional like high level programming languages and easy to modify yet can be compiled during run-time to be highly efficient. All FortiSIEM parsers go beyond most competitor's offerings using this patented solution and can be parsed at beyond 10K EPS per node.

Business Services Dashboard — Transforms System to Service Views

Traditionally, SIEMS monitor individual components — servers, applications, databases and so forth — but what most organizations really care about is the services those systems power. FortiSIEM now offers the ability to associate individual components with the end user experience that they deliver together providing a powerful view into the true availability of the business.

Automated Incident Mitigation

When an Incident is triggered, an automated script can be run to mitigate or eliminate the threat. Built-in scripts support a variety of devices including Fortinet, Cisco, Palo Alto and Window/Linux servers. Built-in scripts can execute a wide range of actions including disabling a user's Active Directory account, disabling a switch port, blocking an IP address on a Firewall, deauthenticating a user on a WLAN Access Point, and more. Scripts leverage the credentials FortiSIEM already has in the CMDB. Administrators can easily extend the actions available by creating their own scripts.

Infusion of Security Intelligence

FortiGuard Threat Intelligence and Indicators of Compromise (IOC) and Threat Intelligence (TI) feeds from commercial, open source and custom data sources integrate easily into the security TI framework. This grand unification of diverse sources of data enables organizations to rapidly identify root causes of threats, and take the steps necessary to remediate and prevent them in the future. Steps can often be automated with new Threat Mitigation Libraries for many Fortinet products.

Highlights

Large Enterprise and Managed Service Provider Ready — "Multi-Tenant Architecture"

Fortinet has developed a highly customizable, multi-tenant architecture that enables enterprises and service providers to manage a large number of physical/logical domains and over-lapping systems and networks from a single console. In this environment it is very easy to cross-correlate information across physical and logical domains, and individual customer networks. Unique reports, rules and dashboards can easily be built for each, with the ability to deploy them across a wide set of reporting domains, and customers. Event archiving policies can also be deployed on a per domain or customer basis. Granular RBAC controls allow varying levels of access to Administrators and Tenants/Customers. For large MSSPs, Collectors can be configured as multi-tenant to reduce the overall deployment footprint.

Features

Real-Time Operational Context for Rapid Security Analytics

- Continually updated and accurate device context — configuration, installed software and patches, running services
- System and application performance analytics along with contextual inter-relationship data for rapid triaging of security issues
- User context, in real-time, with audit trails of IP addresses, user identity changes, physical and geo-mapped location
- Detect unauthorized network devices, applications, and configuration changes

Out-of-the-Box Compliance Reports

- Out-of-the-box pre-defined 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, NIST800-53, NIST800-171, NESA
- To meet GDPR requirements, Personally Identifiable Information (PII) can be obscured based on an administrator's Role

Performance Monitoring

- Monitor basic system/common metrics
- System level via SNMP, WMI, PowerShell
- Application level via JMX, WMI, PowerShell
- Virtualization monitoring for VMware, Hyper-V — guest, host, resource pool and cluster level
- Storage usage, performance monitoring — EMC, NetApp, Isilon, Nutanix, Nimble, Data Domain
- 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 — Netflow, SFlow, Cisco AVC, NBAR, IPFix
- Ability to add custom metrics
- Baseline metrics and detect significant deviations

Availability Monitoring

- System up/down monitoring — via Ping, SNMP, WMI, Uptime Analysis, Critical Interface, Critical Process and Service, BGP/OSPF/EIGRP status change, Storage port up/down
- Service availability modeling via Synthetic Transaction Monitoring — Ping, HTTP, HTTPS, DNS, LDAP, SSH, SMTP, IMAP, POP, FTP, JDBC, ICMP, trace route and for generic TCP/UDP ports
- Maintenance calendar for scheduling maintenance windows
- SLA calculation — "normal" business hours and after-hours considerations

Features

Powerful and Scalable Analytics

- Search events in real time— without the need for indexing
- Keyword and event-based searches
- Search historical events — SQL-like queries with Boolean filter conditions, group by relevant aggregations, time-of-day filters, regular expression matches, calculated expressions — GUI & API
- Use discovered CMDB objects, user/identity and location data in searches and rules
- Schedule reports and deliver results via email to key stakeholders
- Search events across the entire organization, or down to a physical or logical reporting domain
- Dynamic watch lists for keeping track of critical violators — with the ability to use watch lists in any reporting rule
- Scale analytics feeds by adding Worker nodes without downtime

Baselining and Statistical Anomaly Detection

- Baseline endpoint/server/user behavior — hour of day and weekday/weekend granularity
- Highly flexible — any set of keys and metrics can be “baselined”
- Built-in and customizable triggers on statistical anomalies

External Technology Integrations

- Integration with any external web site for IP address lookup
- API-based integration for external threat feed intelligence sources
- API-based 2-way integration with help desk systems — seamless, out-of-the box support for ServiceNow, ConnectWise and Remedy
- API-based 2-way integration with external CMDB — 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 — Windows and Linux — who and what details
- Automated detection of changes from an approved configuration file
- Automated detection of windows registry changes via FortiSIEM windows agent

Device and Application Context

- Network Devices including Switches, Routers, Wireless LAN
- Security devices — Firewalls, Network IPS, Web/Email Gateways, Malware Protection, Vulnerability Scanners
- Servers including Windows, Linux, AIX, HP UX
- Infrastructure Services including DNS, DHCP, DFS, AAA, Domain Controllers, VoIP
- User-facing Applications including Web Servers, App Servers, Mail, Databases
- Storage devices including NetApp, EMC, Isilon, Nutanix, Data Domain
- Cloud Apps including AWS, Box.com, Okta, Salesforce.com
- Cloud infrastructure including AWS
- Environmental devices including UPS, HVAC, Device Hardware
- Virtualization infrastructure including VMware ESX, Microsoft Hyper-V Scalable and Flexible Log Collection

Scalable and Flexible Log Collection

- Collect, Parse, Normalize, Index and Store security logs at very high speeds
- Out-of-the-box support for a wide variety of security systems and vendor APIs — both on-premises and cloud
- Windows Agents provide highly scalable and rich event collection including file integrity monitoring, installed software changes and registry change monitoring
- Linux Agents provide file integrity monitoring, syslog monitoring and custom log file monitoring
- Modify parsers from within the GUI and redeploy on a running system without downtime and event loss
- Create new parsers (XML templates) via integrated parser development environment and share among users via export/import function
- Securely and reliably collect events for users and devices located anywhere

Features

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 — ServiceNow, ConnectWise, and Remedy
- Built-in ticketing system
- 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, IP's and user to understand all related incidents quickly

Rich Customizable Dashboards

- Configurable real-time dashboards, with "Slide-Show" scrolling for showcasing KPIs
- Sharable reports and analytics across organizations and users
- Color-coded for rapidly identifying critical issues
- Fast — updated via in-memory computation
- Specialized layered dashboards for business services, virtualized infrastructure, event logging status dashboard, and specialized apps

External Threat Intelligence Integrations

- API's for integrating external threat feed intelligence — Malware domains, IPs, URLs, hashes, Tor nodes
- Built-in integration for popular threat intelligence sources — ThreatStream, 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 & TAXII feeds are supported

Simple and Flexible Administration

- Web-based GUI
- Rich Role-based Access Control for restricting access to GUI and data at various levels
- All inter-module communication protected by HTTPS
- Full audit trail of FortiSIEM user activity
- Easy software upgrade with minimal downtime & event loss
- Policy-based archiving
- Hashing of logs in real time for non-repudiation & integrity verification
- Flexible user authentication — local, external via Microsoft AD and OpenLDAP, Cloud SSO/SAML via Okta, Duo, RADIUS
- Ability to log into remote server behind a collector from FortiSIEM GUI via remote SSH tunnel

Easy Scale Out Architecture

- Available as Virtual Machines for on-premises and public/private cloud deployments on the following hypervisors — VMware ESX, Microsoft Hyper-V, KVM, Amazon Web Services AMI, and Azure
- Multiple physical appliance models with varying levels of performance to provide a variety of deployment options
- Scale data collection by deploying multiple Collectors
- Collectors can buffer events when connection to FortiSIEM Supervisor is not available
- Scale analytics by deploying multiple Workers
- Built-in load balanced architecture for collecting events from remote sites via collectors
- Log storage can be either the FortiSIEM proprietary NoSQL database, or Elasticsearch which provides the ultimate in scalability
- To meet high availability requirements, the Supervisor can be configured with Active/Passive instances

FortiSIEM Advanced Agents

Fortinet has developed a highly efficient agentless technology for collecting information. However some information, such as file integrity monitoring data, is expensive to collect remotely. FortiSIEM has combined its agentless technology with high performance agents for Windows and Linux to significantly bolster its data collection.

Features

	AGENTLESS TECHNOLOGY	ADVANCED WINDOWS AGENT	ADVANCED LINUX AGENT
Agentless			
Discovery	✓		
Performance Monitoring	✓		
(Low Performance) Collect System, App & Security Logs	✓		
Agents			
(High Performance) Collect System, App & Security Logs		✓	✓
Collect DNS, DHCP, DFS, IIS Logs		✓	
Local Parsing and Time Normalization		✓	
Installed Software Detection		✓	
Registry Change Monitoring		✓	
File Integrity Monitoring		✓	✓
Customer Log File Monitoring		✓	✓
WMI Command Output Monitoring		✓	
PowerShell Command Output Monitoring		✓	

Specifications

	FORTISIEM 500F "COLLECTOR"	FORTISIEM 2000F "SUPERVISOR OR WORKER"	FORTISIEM 3500F "SUPERVISOR OR WORKER"
Hardware Specifications			
CPU	Intel Xeon E3-1225V3 4C4T 3.20 GHz	Intel Xeon E5-2620V3 6C12T 2.40 GHz	2x Intel Xeon E5-2680V2 10C20T 2.80 GHz
Memory	DDR3 16 GB (2x 8 GB)	DDR4 32 GB (4x 8 GB)	DDR3 64 GB (8x 8 GB)
Network Interfaces	4x GE RJ45 ports	4x GE RJ45 ports	2x GE RJ45 ports, 2x SFP ports
Console Port	DB9	DB9	DB9
USB Ports	2x USB 2.0; 2x USB 3.0	2x USB 2.0; 2x USB 3.0	4x USB 2.0
Storage Capacity	3 TB (1x 3 TB)	36 TB (12x 3 TB)	72 TB (24x 3 TB)
Usable Event Data Storage		23.4 TB	55.7 TB
Dimensions			
Height x Width x Length (inches)	1.7 x 17.2 x 19.8	3.5 x 17.2 x 25.6	7 x 17.2 x 26
Height x Width x Length (mm)	43 x 437 x 503	89 x 437 x 648	178 x 437 x 660
Weight	31 lbs (14 kg)	58 lbs (26.3 kg)	93.74 lbs (42.5 kg)
Form Factor	1 RU	2 RU	4 RU
Environment			
AC Power Supply	100–240V AC, 60–50 Hz	100–240V AC, 60–50 Hz	100–240V AC, 60–50 Hz
Power Consumption (Average / Maximum)	132.3 W / 150.3 W	285.7 W / 310.5 W	528 W / 586.6 W
Heat Dissipation	546.95 BTU/h	1093.55 BTU/h	2035.60 BTU/h
Operating Temperature	50–95°F (10–35°C)	50–95°F (10–35°C)	41–95°F (5–35°C)
Storage Temperature	-40–158°F (-40–70°C)	-40–158°F (-40–70°C)	-40–140°F (-40–60°C)
Humidity	8–90% (non-condensing)	8–90% (non-condensing)	8–90% (non-condensing)
Compliance			
Safety Certifications	FCC Part 15 Class A, C-Tick, VCCI, CE, UL/cUL, CB	FCC Part 15 Class A, C-Tick, VCCI, CE, UL/cUL, CB	FCC Part 15 Class A, C-Tick, VCCI, CE, UL/cUL, CB

Order Information

Licensing Scheme

FortiSIEM licenses provide the core functionality for cross-correlated analytic network device discovery. Devices include switches, routers, firewalls, servers, etc. Each device that is to be monitored requires a license. Each license supports data capture and correlation, alerting and alarming, reports, analytics, search and optimized data repository and includes 10 EPS (Events Per Second). “EPS” is a performance measurement that defines how many messages or events are generated by each device in a second. Additional EPS can be purchased separately as needed. Licenses are available in either a “Subscription” or “Perpetual” version.

PRODUCT	SKU	DESCRIPTION
FortiSIEM Hardware Product		
FortiSIEM 500F	FSM-500F	FortiSIEM Collector Hardware Appliance FSM-500 supports up to 5K EPS, 500 SNMP, 200 WMI for Performance/100 WMI for Logs.
FortiSIEM 2000F	FSM-2000F	FortiSIEM All-in-one Hardware Appliance FSM-2000F supports up to 15K EPS (all features turned on). Does not include any device or EPS licenses which must be purchased separately.
FortiSIEM 3500F	FSM-3500F	FortiSIEM All-in-one Hardware Appliance FSM-3500F supports up to 30K EPS (all features turned on). Does not include any device or EPS licenses which must be purchased separately.
FortiSIEM Base Product		
FortiSIEM All-In-One Perpetual License	FSM-AIO-BASE	Base All-in-one Perpetual License for 50 devices and 500 EPS.
	FSM-AIO-XX-UG	Add XX devices and EPS/device All-in-one Perpetual License.
FortiSIEM All-In-One Perpetual License for FSM-2000F	FSM-AIO-2000-BASE	100 devices and 1000 EPS All-in-one Perpetual License for FortiSIEM FSM-2000F. Does not include Maintenance & Support.
FortiSIEM All-In-One Perpetual License for FSM-3500F	FSM-AIO-3500-BASE	500 devices and 5000 EPS All-in-one Perpetual License for FortiSIEM FSM-3500F. Does not include Maintenance & Support.
FortiSIEM All-In-One Subscription License	FC1-10-FSM98-180-02-DD	Per Device Subscription License that manages minimum XX devices, 10 EPS/device.
FortiSIEM Additional Products		
FortiSIEM End-Point Device Perpetual License	FSM-EPD-XX-UG	Add XX End-Points and 2 EPS/End-Point for All-in-one Perpetual License
FortiSIEM End-Point Device Subscription License	FC[1-8]-10-FSM98-184-02-DD	Per End-Point Subscription License for minimum XX End-Points, 2 EPS/End-Point
Add 1 EPS Perpetual License	FSM-EPS-100-UG	Add 1 EPS Perpetual
Add 1 EPS Subscription License	FC[1-10]-FSM98-183-02-DD	Add 1 EPS Subscription
FortiSIEM Advanced Agent (Windows & Linux) Perpetual License	FSM-AGT-ADV-XX-UG	XX Advanced Agents for Perpetual License
FortiSIEM Advanced Agent (WIndows & Linux) Subscription License	FC[1-8]-10-FSM98-182-02-DD	Per Agent Subscription License for minimum XX Advanced Agents
IOC Service Subscription License	FC[1-G]-10-FSM98-149-02-DD	(X Points) FortiSIEM Indicators of Compromise (IOC) Service. 1 device or 2 End-Points or 3 Advanced Agents equals 1 point.
FortiSIEM Support		
FortiCare Support for FortiSIEM	FC[1-G]-10-FSM97-248-02-DD	24x7 FortiCare Contract (X Points). 1 device or 2 End-Points or 3 Advanced Agents equals 1 point.
	FC-10-FSM04-311-02-DD	8x5 FortiCare Contract
	FC-10-FSM04-247-02-DD	24x7 FortiCare Contract