

FortiSIEM®

Available in:



Appliance



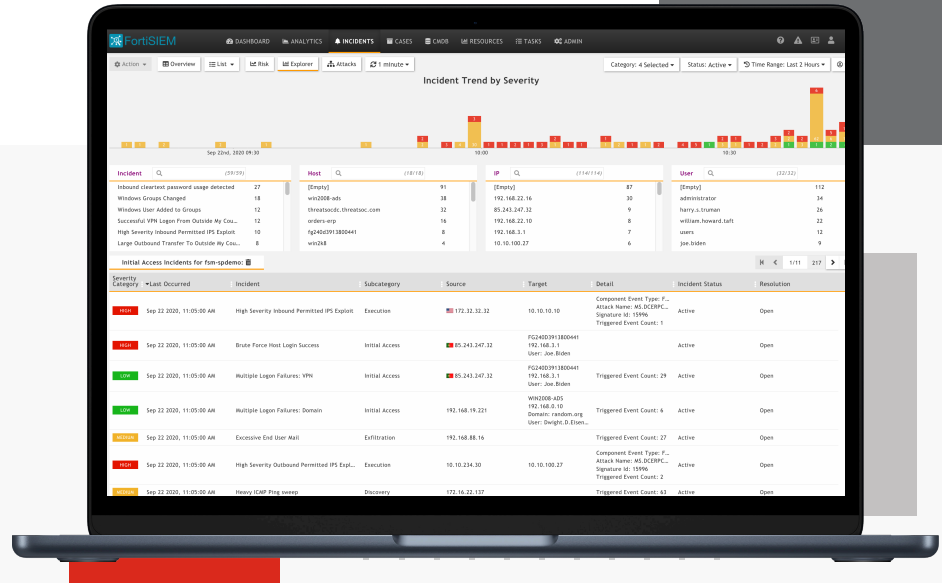
Virtual Machine



Cloud



Hosted



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

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 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.

Highlights



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.



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 method makes it possible to create policies or perform investigations based on user identity instead of IP addresses—allowing for rapid problem resolution.

Highlights



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 and firewall logs. 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.



Business Services Dashboard — Transforms System to Service Views

Traditionally, SIEM's 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.



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



UEBA

- FortiSIEM Agent-based UEBA telemetry allows for the collection of high fidelity user-based activity that includes User, Process, Device, Resource, and Behavior. Using an agent-based approach allows for the collection of telemetry when the endpoint is on and off the corporate network, providing a more complete view of user activity. UEBA telemetry allows for the identification of unknown bad activities that can be alerted and acted upon

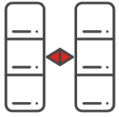


Performance Monitoring

- Monitor basic system/ common metrics
- System level via SNMP, WMI, and PowerShell
- Application level via JMX, WMI, and PowerShell
- Virtualization monitoring for VMware, Hyper-V — guest, host, resource pool, and cluster level
- Specialized application performance monitoring
- Databases — Oracle, MS SQL, MySQL via JDBC
- VoIP infrastructure via IPSLA, SNMP, and CDR/CMR
- Flow analysis and application performance — Netflow, SFlow, Cisco AVC, NBAR, and IPFix
- Ability to add custom metrics
- Baseline metrics and detect significant deviations



Features



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



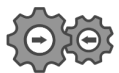
Powerful and Scalable Analytics

- 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 and 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

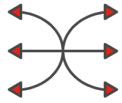


External Technology Integrations

- Integration with any external web site for IP address lookup
- API-based integration for external threat feed intelligence sources
- API-based two-way integration with help desk systems — seamless, out-of-the box support for ServiceNow, ConnectWise, and Remedy
- API-based two-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



Features



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
- 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



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

FortiSIEM Cloud is available in the following regions:

North America	Europe	Asia Pacific	Australia
Canada Central	Ireland	India - Mumbai	Sydney
USA West - Oregon	UK - London	Singapore	
USA East - Ohio	France - Paris		
USA East - Northern Virginia	Sweden - Stockholm		
	Germany - Frankfurt		

Features



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



Automation 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 Case Management 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, IPs 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

Features



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 — FortiGuard, Dragos WorldView, ThreatStream, ThreatConnect
- Technology for handling large threat feeds — incremental download and sharing within cluster, real-time pattern matching with network traffic. STIX and TAXII support



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 and event loss
- Policy-based archiving
- Hashing of logs in real time for non-repudiation and 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 (AWS), Microsoft Azure and Google Cloud Platform (GCP)
- 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

Features

	AGENTLESS TECHNOLOGY	ADVANCED WINDOWS AGENT	ADVANCED LINUX AGENT
Agentless			
Discovery	☑	—	—
Performance Monitoring	☑	—	—
(Low Performance) Collect System, App and Security Logs	☑	—	—
Agents			
(High Performance) Collect System, App and 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	—	☑	—
Central Management and Upgrades of Agent	—	☑	☑
Osquery Support	—	☑	—

Licensing Scheme

FortiSIEM Virtual Appliance (VA) and Hardware Appliance (HW)

FortiSIEM licenses provide the core functionality for cross-correlated analytic network device discovery. Devices include switches, routers, firewalls, and servers. 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.

FortiSIEM Cloud

FortiSIEM Cloud unifies all licensed components that are available with VA and HW licensing within the FortiSIEM Compute Units (FCU). Every 10 FCU provides a licensed daily average of 1K EPS. FortiSIEM Cloud is licensed on FCU, Online storage [maximum quantity 120 (60 TB)], and Archive storage and depending on the performance requirements additional FCU or storage can be added. FCU are licensed with increments of 10 FCU with a minimum quantity of 10 (recommended >=20) and a maximum of 600 FCU. A minimum of 500GB on online storage is required.



Specifications



	FortiSIEM 500F "Collector"	FortiSIEM 500G "Collector"
Hardware Specifications		
CPU	Intel Xeon E3-1225V3 4C4T 3.20 GHz	Intel Xeon E-2226GE 6C6T 3.40GHz
Memory	DDR3 16 GB (2× 8 GB)	DDR4 16GB (2× 8GB)
Network Interfaces	4x GE RJ45 ports	4x GbE RJ45
Console Port	DB9	DB9
USB Ports	2x USB 2.0; 2x USB 3.0	2x USB, 2x USB 3.0
Storage Capacity	3 TB (1× 3 TB)	4TB (1× 4TB)
Usable Event Data Storage	—	—
Performance Benchmark	8K EPS, 500 SNMP, 200 WMI for Performance/ 100 WMI for Logs	8K EPS, 500 SNMP, 200 WMI for Performance/ 100 WMI for Logs
Dimensions		
Height x Width x Length (inches)	1.7 × 17.2 × 19.8	1.73 × 17.32 × 21.26
Height x Width x Length (mm)	43 × 437 × 503	44 × 440 × 540
Weight	31 lbs (14 kg)	16.76 lbs (7.6 kg)
Form Factor	1 RU	1 RU
Environment		
AC Power Supply	100~240V AC, 60~50 Hz	350W single PSU
Power Consumption (Average / Maximum)	132.3 W / 150.3 W	93.87 W / 114.73 W
Heat Dissipation	546.95 BTU/h	425.58 (BTU/h)
Operating Temperature	50°F to 95°F (10°C to 35°C)	32°F ~ 104°F (0°C ~ 40°C)
Storage Temperature	-40°F to 158°F (-40°C to 70°C)	-4°F ~ 167°F (-20°C ~ 75°C)
Humidity	8% to 90% (non-condensing)	5% to 95% (non-condensing)
Compliance		
Compliance	FCC, ISED, CE, RCM, VCCI, BSMI, UL/cUL, CB	FCC, ISED, CE, RCM, VCCI, BSMI, UL/cUL, CB

Specifications



	FortiSIEM 2000G "Supervisor or Worker"	FortiSIEM 2200G "Supervisor or Worker"
Hardware Specifications		
CPU	2x Intel Xeon Silver 4210R, 10C20T, 2.40GHz, C621 (total 40T)	2 x Intel Xeon Silver 4210R 10C20T 2.4GHz
Memory	DDR4 128GB (16GB x 8 ECC REG Memory)	DDR4 128GB (16GB x 8 ECC RDIMM)
Network Interfaces	4x GbE RJ45 ports 2x 25GbE SFP28	4x 1GE RJ45 ports 2x 25GE SFP28 ports
Console Port	DB9	DB9
USB Ports	2x USB 3.0	2x USB 3.0 ports
Storage Capacity	32TB (3.5 in. SAS 4TB x 8) + 4TB (2.5 in. NVMe 1TB x4)	8x 3.5 in. hot-swappable 4TB HDDs (32TB) 4x 2.5 in. hot-swappable 1.92TB SSDs (7.68TB)
Usable Event Data Storage	~19TB	Hot/SSD = ~5.2 TB Warm/HDD = ~21 TB
Performance Benchmark	20K EPS with Collectors	20K EPS with Collectors
Recommended Max. UEBA users	10 000	10 000
Dimensions		
Height x Width x Length (inches)	3.46 × 17.32 × 29.33	3.46 × 17.32 × 29.33
Height x Width x Length (mm)	88 × 440 × 745	88 × 440 × 745
Weight	55.78 lbs (25.3 kg)	57.64 lbs (26.145 kg)
Form Factor	2 RU	2 RU
Environment		
AC Power Supply	100–240V AC, 60–50 Hz	100-240 VAC, 60-50 H
Power Consumption (Average / Maximum)	593.1 W / 724.9 W	610 W / 744 W
Heat Dissipation	2507.48 BTU/h	2537 BTU/h
Operating Temperature	32°F ~ 104°F (0°C ~ 40°C)	32°F to 104°F (0°C to 40°C)
Storage Temperature	-4°F ~ 167°F (-20°C ~ 75°C)	-4°F to 167°F (-20°C to 75°C)
Humidity	5% to 95% (non-condensing)	5% ~ 95% relative humidity, non-operating, non-condensing
Compliance		
Compliance	FCC, ISED, CE, RCM, VCCI, BSMI, UL/cUL, CB	FCC, ISED, CE, RCM, VCCI, BSMI, UL/cUL, CB

Specifications



	FortiSIEM 3500G "Supervisor or Worker"	FortiSIEM 3600G "Supervisor or Worker"
Hardware Specifications		
CPU	2x Intel Xeon Gold 5118 12C24T 2.30GHz	2x Intel Xeon Gold 6226R 16C32T 2.90GHz
Memory	DDR4 128GB (16GB x 8 ECC REG Memory)	DDR4 128GB (16GB x 8 ECC REG Memory)
Network Interfaces	2x GbE RJ45 ports 2x GbE SFP ports 2x 25GbE SFP28	2x 1GE RJ45 ports 2x 10GE SFP+ ports 2x 25GE SFP28 ports
Console Port	DB9	DB9
USB Ports	6x USB 3.0	2x USB 3.0 ports
Storage Capacity	96 TB (4TB x 24)	12x 3.5 in. hot-swappable 8TB HDDs (96TB) 4x 2.5 in. hot-swappable 3.84TB SSDs (15.36TB)
Usable Event Data Storage	~75 TB	Hot/SSD = ~11 TB Warm/HDD = ~65 TB
Performance Benchmark	40K EPS with Collectors	50K EPS with Collectors
Recommended Max. UEBA users	10 000	10 000
Dimensions		
Height x Width x Length (inches)	7 x 17.2 x 26	5.25 x 17.2 x 24.4
Height x Width x Length (mm)	178 x 437 x 660	132 x 438 x 621
Weight	90.75 lbs (41.2 kg)	63.89 lbs (28.98 kg)
Form Factor	4 RU	3 RU
Environment		
AC Power Supply	100–240V AC, 60–50 Hz	100-240 VAC, 60-50 H
Power Consumption (Average / Maximum)	645.10 W / 696.02 W	695 W
Heat Dissipation	2408.94 BTU/h	2370 BTU/h
Operating Temperature	50°F to 95°F (10°C to 35°C)	32°F to 104°F (0°C to 40°C)
Storage Temperature	-40°F to 158°F (-40°C to 70°C)	-4°F to 167°F (-20°C to 75°C)
Humidity	90% (non-condensing)	5% ~ 95% relative humidity, non-operating, non-condensing
Compliance		
Compliance	FCC, ISED, CE, RCM, VCCI, UL/cUL, CB	FCC, ISED, CE, RCM, VCCI, BSMI, UL/cUL, CB

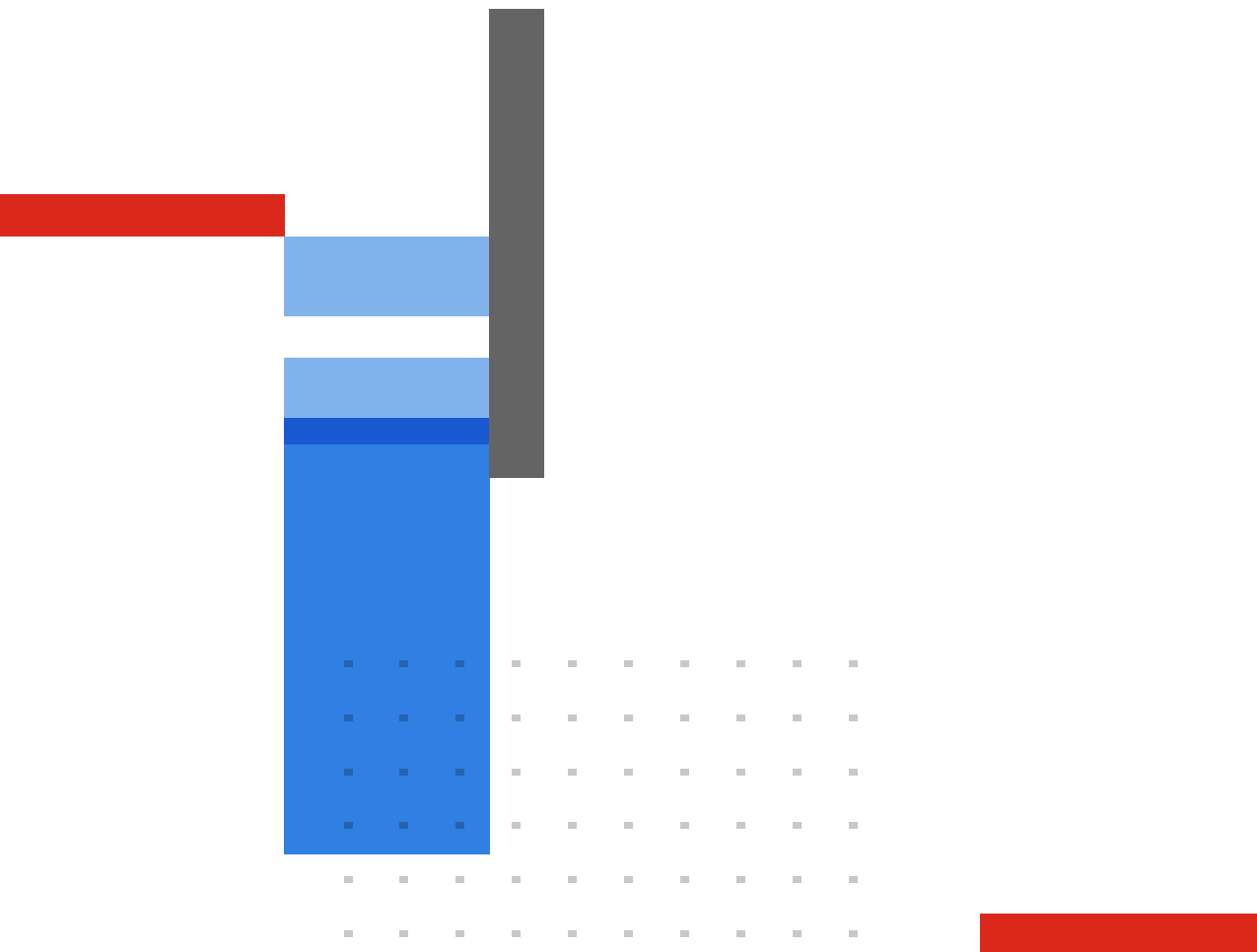
Ordering Information

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 500G	FSM-500G	FortiSIEM Collector Hardware Appliance FSM-500G. Supports up to 5000 EPS.
FortiSIEM 2000G	FSM-2000G	FortiSIEM All-in-one Hardware Appliance FSM-2000G supports up to 20K EPS using Collectors, (all features turned on). Does not include any device or EPS licenses which must be purchased separately.
FortiSIEM 2200G	FSM-2200G	FortiSIEM All-in-one Hardware Appliance FSM-2200G supports up to 20K EPS using Collectors, (all features turned on). Does not include any device or EPS licenses which must be purchased separately.
FortiSIEM 3500G	FSM-3500G	FortiSIEM All-in-one Hardware Appliance FSM-3500G supports up to 40K EPS using Collectors, (all features turned on). Does not include any device or EPS licenses which must be purchased separately.
FortiSIEM 3600G	FSM-3600G	All-in-one Hardware Appliance FSM-3600G. Does not include any device or EPS licenses and 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-2000	FSM-AIO-2000-BASE	100 devices and 1000 EPS All-in-one Perpetual License for FortiSIEM FSM-2000. Does not include Maintenance & Support.
FortiSIEM All-In-One Perpetual License for FSM-2200	FSM-AIO-2200-BASE	100 devices and 1000 EPS All-in-one Perpetual License for FortiSIEM FSM-2200. Does not include Maintenance & Support.
FortiSIEM All-In-One Perpetual License for FSM-3500	FSM-AIO-3500-BASE	500 devices and 5000 EPS All-in-one Perpetual License for FortiSIEM FSM-3500G. Does not include Maintenance & Support.
FortiSIEM All-In-One Perpetual License for FSM-3600	FSM-AIO-3600-BASE	500 devices and 5000 EPS all-in-one perpetual license for FortiSIEM FSM-3600G. Does not include Maintenance & Support
FortiSIEM All-In-One Subscription License	FC1-8-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 - Log & FIM" or 10 "Advanced Agents - UEBA Telemetry" equals 1 point.
FortiSIEM-UEBA Agent Perpetual License	FSM-UEBA-XX-UG	Advanced Agents - UEBA Telemetry Perpetual Licenses. Does not include Maintenance & Support.
FortiSIEM-UEBA Subscription License	FC[1/4/9]-10-FSM98-334-02-DD	Per Advanced Agent - UEBA Telemetry Subscription License, a minimum of 25 Agents. Does not include Maintenance & Support.
FortiSIEM Manager	FC1-10-SMMGR-574-02-DD	Subscription license for FortiSIEM Manager providing centralised incident, management and status of independent FortiSIEM instances. Requires a Minimum Qty. of 5 to monitor 5 separate FortiSIEM Instances, max of 50 Instances. Includes Maintenance and Support.
FortiSIEM High Availability Super	FC[1-Y]-10-FSM98-593-02-DD	FortiSIEM High Availability Supervisor Cluster Subscription.
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 - Log & FIM" or 10 "Advanced Agents - UEBA Telemetry" equals 1 point.
FortiCare Support for Hardware Appliance	FC-10-FSM[XX]-247-02-DD	FortiCare Premium Support - Hardware Appliance only - product support required separately.
FortiSIEM Cloud		
FortiSIEM Compute Units	FC-10-SMCLD-543-02-12	FortiSIEM Compute Units (FCU). Minimum quantity of 10 FCU. Annual Subscription. Includes FortiCare Support.
FortiSIEM Cloud Online Storage	FC-10-SMCLD-541-02-12	Additional 500GB online storage. Requires minimum quantity of 1 with initial FortiSIEM Compute Unit order. Annual Subscription.
FortiSIEM Cloud Archive Storage	FC-10-SMCLD-542-02-12	Archive 500GB storage. Annual Subscription.



Fortinet Corporate Social Responsibility Policy

Fortinet is committed to driving progress and sustainability for all through cybersecurity, with respect for human rights and ethical business practices, making possible a digital world you can always trust. You represent and warrant to Fortinet that you will not use Fortinet's products and services to engage in, or support in any way, violations or abuses of human rights, including those involving illegal censorship, surveillance, detention, or excessive use of force. Users of Fortinet products are required to comply with the [Fortinet EULA](#) and report any suspected violations of the EULA via the procedures outlined in the [Fortinet Whistleblower Policy](#).



www.fortinet.com

Copyright © 2024 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 Chief Legal Officer, 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.