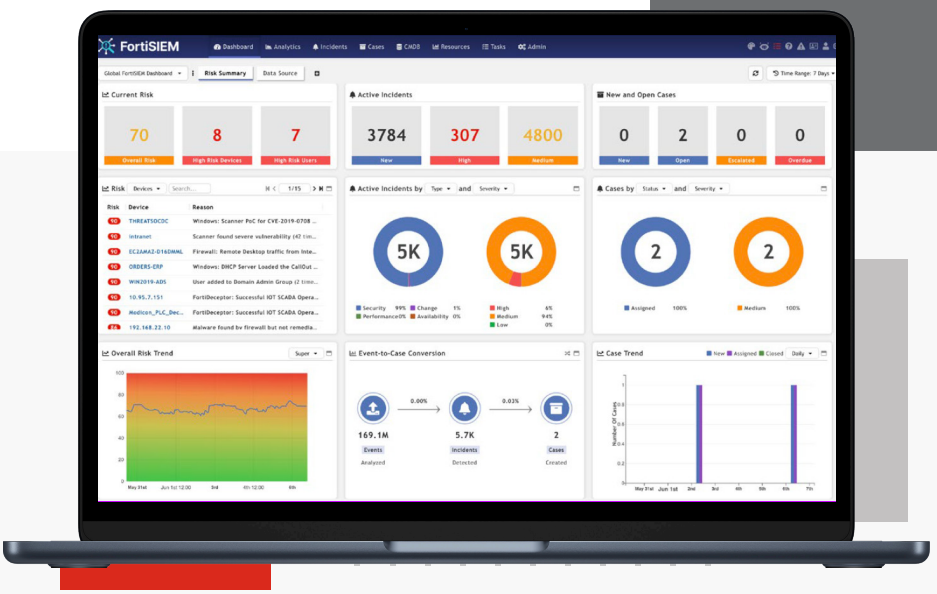
FortiSIEM®

Available in:

Appliance | Virtual Machine | Cloud | Hosted

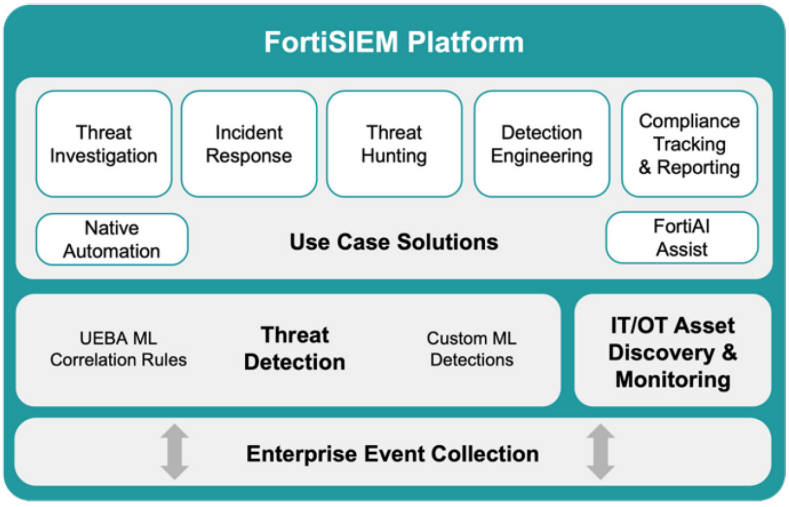


Highlights

- Universal event collection
- IT/OT asset CMDB with discovery and monitoring
- Advanced behavioral threat detection using AI
- Realtime detection and risk scoring
- Rich investigation and response features
- FortiAI-Assist GenAI
- Built in SOAR automation
- Compliance reporting
- Distributed processing and massive scalability
- Multitenancy and other MSSP-focused features
- Simple management and exceptional TCO
- Deploy on-prem, in cloud, or a SaaS global service

Delivering on the promise of next-gen SIEM security

FortiSIEM is designed to be the backbone of your security operations team and attack protection. It provides a unique, high-performance IT/OT SIEM feature set built on advanced analytics, inbuilt configuration management database (CMDB), native SOAR automation, and the latest in GenAI assistance. Delivering out-of-the-box value, complete flexibility, and ultimate scale, it's the right solution for organizations and MSSPs of any size.



Highlights

Universal event collection

FortiSIEM collects, correlates, and normalizes events/alerts from hundreds of IT/OT multivendor sources across any cloud or on-prem environment. FortiSIEM Generic API integrations and inbound webhook allows for customize support of API and SaaS based services. FortiSIEM flexible agent technology supports high speed ingestion and can filter and tag events at the source. Advanced Endpoint Agents can be used to directly collect detailed information such as file integrity monitoring and support built-in Osquery for advanced threat hunting and investigations.

IT/OT asset CMDB with discovery and monitoring

FortiSIEM supports a built-in Configuration Management Database (CMDB) that provides automatic asset identification and categorization, as well as the collection, monitoring, and threshold alerting of essential asset health metrics. Active polling employs a range of methods to collect metrics, including availability, performance, resource utilization, and configuration changes. CMDB information and asset categorization are also helpful during the incident investigation, providing insights into affected assets and simplifying analyst search queries.

Advanced behavioral threat detection using AI

FortiSIEM uniquely detects attacks using a wide variety of methods and a distributed processing architecture. Tunable UEBA ML and over 2800 IT/OT correlation rules that are updated and powered by the latest threat available threat intelligence. Customers can import additional rules from the open-source SIGMA library and create or customize their own rules. Additionally, the inbuilt ML workbench, designed for ease of use, makes it straightforward for customers to build, train, and deploy their ML-based detections, all within FortiSIEM.

FortiGuard threat intelligence and more

FortiGuard Threat Intelligence integrated within FortiSIEM expands and improves incident detection. FortiSIEM can import threat intelligence feeds from a wide variety of independent sources to power threat detection, incident enrichment, and threat hunting. FortiGuard intelligence value-added features include Outbreak Detections, which provide intelligence, detection rules, and threat hunting procedures on for newly discovered security attacks.

Realtime risk-based threat scoring

FortiSIEM provides a clear view of incidents, prioritized through severity ratings while dynamically scoring the associated users and hosts. FortiSIEM risk scoring considers asset criticality, the type and volume of associated incidents and vulnerabilities. With a comprehensive approach to identify the severity and risk, security teams can more effectively manage and mitigate risks.

Rich investigation, response, and agent features

FortiSIEM offers a robust incident investigation experience, starting with the auto-enrichment of incidents and automatic risk evaluation. Events are grouped into incidents, and a visual display graphs their relationship. Common investigation and response actions are available as built-in scripts or pre-built automation playbooks. Complete case management and features are also supported.

Detailed endpoint investigation is accomplished using FortiSIEM Agents, which provide event collection, File Integrity Monitoring (FIM), and built-in native support for Osquery to deliver forensic-level details on the endpoint state. FortiSIEM can also periodically perform Osquery queries, which then enter the data pipeline, rules engine and data lake to expand detection and investigation capabilities.

Highlights

FortiAI-Assist GenAI

The FortiAI-Assist function is natively built into common FortiSIEM workflows to guide, simplify, and automate analyst activities, including event analysis, incident management tasks, query building and guidance. FortiAI-Assist for FortiSIEM offers the choice of the latest OpenAI and Microsoft Azure OpenAI LLMs, utilizing a standard Response Augmentation Generation method to augment, shape, and ensure the accuracy of responses or actions. FortiSIEM can mask sensitive data before submission and help maintain privacy without compromising efficiency.

Built in SOAR automation

Rich, built-in SOAR automation is available to turbocharge investigation and response, as well as any analyst workflow or task. A pre-built playbook library provides common use cases that can be used directly or customized, and new playbooks are added continuously. Based on FortiSOAR technology, the intuitive playbook builder supports playbooks of any complexity and provides access to the entire library of FortiSOAR connectors.

Compliance reporting

FortiSIEM provides over 1300 out-of-the box compliance reports including coverage for CIS, COBIT, FISMA, GLBA, GPR13, HIPAA, ISO 27001, ITIL, NERC, NESA UAE, NIST800-53/171, PCI, SOX, SANS Critical Control, and KSA ECC. To meet GDPR requirements, Personally Identifiable Information (PII) can be obscured based on the user role.

Distributed processing and massive scalability

FortiSIEM is based on a 3-tier architecture of Supervisors, Workers, and Collectors. Supervisor nodes provide core functionality and user interactions and can act as an all-in-one instance for smaller deployments. Worker nodes handle event processing, correlation, and reporting using a distributed processing model to support large workloads. Collectors ingest, parse and filter, events before uploading to the FortiSIEM cluster. High availability, disruption handling, and distributed deployment across cloud and on-prem environments is supported.

Multitenancy and MSSP-focused features

FortiSIEM supports a centrally controlled multi-tenant architecture allowing for the flexible creation of individual end customer tenants. Unique reports, rules, and dashboards can easily be built for each tenant, and deployed across 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 tenants/ customers. For large MSSPs, Collectors can be configured as multi-tenant to reduce the overall deployment footprint.

Simple management and exceptional TCO

For self-managed deployments, the efficient FortiSIEM architecture featuring distributed processing, 10x data compression, and flexible storage configurations simplify system management and assure a minimum TCO. These same attributes contribute to a highly affordable FortiSIEM SaaS offering as well.

Deploy on-prem, in cloud, or a SaaS global service

FortiSIEM supports a complete range of deployment models. A Fortinet-managed SaaS offering is available in 19 AWS locations worldwide. Customers can also choose to deploy FortiSIEM software (VM) on-premises via their own infrastructure or via a choice of dedicated FortiSIEM hardware appliances. Finally, FortiSIEM can also be deployed directly in AWS, GCP, Oracle, Aure and other cloud providers that support KVM.

Features

Real-Time Operational Context for Rapid Security Analytics

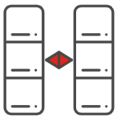
- Continually updated and accurate device context — configuration, installed software and patches, running services
- System and application performance analytics along with contextual inter-relationship data for rapid triaging of security issues
- Detect unauthorized network devices, applications, and configuration changes

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



Availability Monitoring

- System up/ down monitoring — via Ping, SNMP, WMI, Uptime Analysis, Critical Interface, Critical Process and Service, network 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

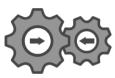
- Search events in real time— without the need for indexing
- Keyword and event-based searches
- Search historical events — SQL-like queries with Boolean filter conditions, group by relevant aggregations, time-of-day filters, regular expression matches, calculated expressions — GUI and API
- Use discovered 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

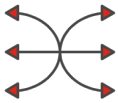
- Integration with any external web site for IP address lookup
- API-based integration for external threat feed intelligence sources
- API-based two-way integration with help desk systems — seamless, out-of-the box support for ServiceNow, ConnectWise, and Remedy
- API-based two-way integration with external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

Features



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

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

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
- Trigger on complex event patterns in real time
- Incident Explorer — dynamically linking incidents to hosts, IPs and user to understand all related incidents quickly

FortiSIEM Automation Service

- Expand FortiSIEM automation capabilities with FortiSIEM Automation Service, a SaaS based SOAR service integrated directly within FortiSIEM
- Create and run playbooks natively within FortiSIEM
- Streamlines incident response workflows by integrating playbook management directly into FortiSIEM
- Allows direct execution of playbooks from an incident or via an Automation Policy
- Features role-based access control for managing playbook creation, editing, and execution
- Playbooks connector actions are executed by Automation Agents on Supervisor and Collector nodes
- Check for availability in Q3 2025

Rich Customizable Dashboards

- Configurable real-time dashboards, with “Slide-Show” scrolling for showcasing KPIs
- Sharable reports and analytics across organizations and users
- 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

- APIs for integrating external threat feed intelligence — Malware domains, IPs, URLs, hashes, Tor nodes
- Built-in integration for popular threat intelligence sources — FortiGuard, FortiSOAR, 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

Features

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

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
- To meet high availability requirements, data replication and HA clustering of Supervisor nodes

Agent Features

	AGENTLESS	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 provides subscription and perpetual licenses.

The Devices + EPS license is available on software/virtual and hardware appliance deployments in subscription and perpetual terms. A Device license supports data capture and correlation, alerting and alarming, reports, analytics, search, and includes 10 EPS (events per second). EPS is a performance measurement that defines how many messages or events each device generates in a second. Additional EPS can be purchased separately from the Device license.

FortiSIEM GB per day is available as a subscription license on software deployments. FortiSIEM measures the GB per day storage of uncompressed event data. Please check GB per day licensing support for availability in FortiSIEM 7.2.x release notes. FortiSIEM GB per day licensing is supported with the ClickHouse event database only.

FortiSIEM Cloud

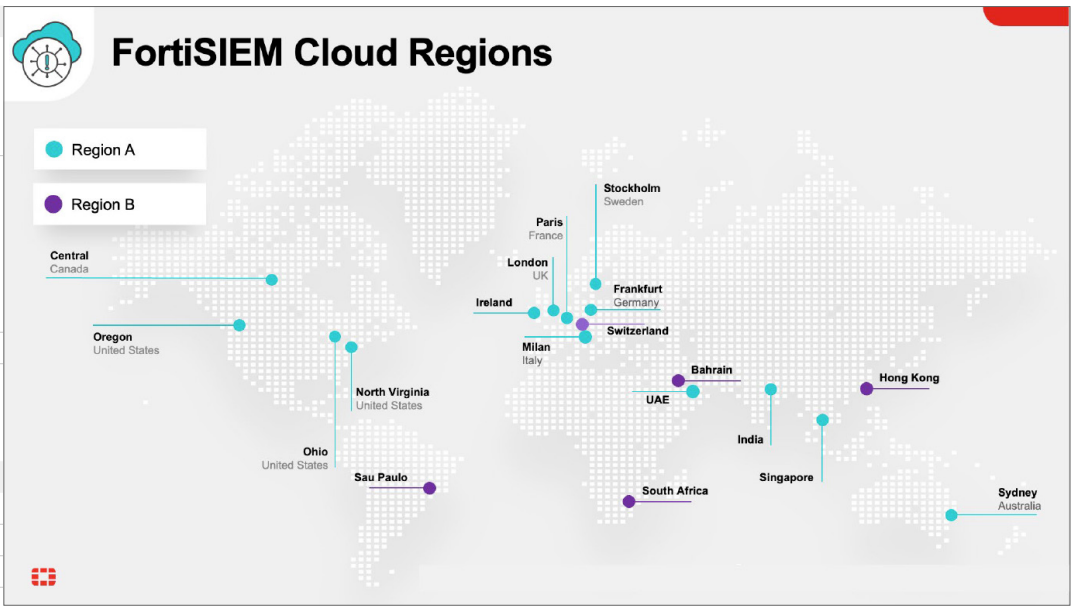
FortiSIEM Cloud unifies all licensed components that are available with VA and HW licensing within the FortiSIEM Compute Units (FCU). Every 10 FCU provides a licensed daily average of 1K EPS. FortiSIEM Cloud is licensed on FCU, Online storage [maximum quantity 120 (60 TB)], and Archive storage and depending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

Security Automation Service

FortiSIEM Automation Service provides a cloud-based automation service within FortiSIEM deployments and is licensed based on the number of concurrent playbook executions. FortiSIEM requires internet connectivity to FortiSIEM Automation Service, supported FortiSIEM version 7.4.0 or later, and is available from the FortiCloud USA region.

FortiSIEM Cloud is available in the following regions:

REGION A	
North America	Canada Central
	USA East - Northern Virginia
	USA East - Ohio
	USA West - Oregon
Europe	France - Paris
	Germany - Frankfurt
	Ireland
	Italy - Milan
	UK - London
	Sweden - Stockholm
Middle East	United Arab Emirates
Asia Pacific	Australia - Sydney
	India - Mumbai
	Singapore
REGION B	
South America	Brazil - São Paulo
Africa	South Africa
Europe	Zurich
Middle East	Bahrain
Asia Pacific	Hong Kong



Appliance Specifications

	FortiSIEM 500G "Collector"	FortiSIEM 2200G "Supervisor or Worker"	FortiSIEM 3600G "Supervisor or Worker"
Hardware Specifications			
CPU	Intel Xeon E-2226GE 6C6T 3.40GHz	2 x Intel Xeon Silver 4210R 10C20T 2.4GHz	2x Intel Xeon Gold 6226R 16C32T 2.90GHz
Memory	DDR4 16GB (2× 8GB)	DDR4 128GB (16GB x 8 ECC RDIMM)	DDR4 128GB (16GB x 8 ECC REG Memory)
Network Interfaces	4x GbE RJ45	4× 1GE RJ45 ports 2× 25GE SFP28 ports	2× 1GE RJ45 ports 2× 10GE SFP+ ports 2× 25GE SFP28 ports
Console Port	DB9	DB9	DB9
USB Ports	2x USB, 2x USB 3.0	2x USB 3.0 ports	2x USB 3.0 ports
Storage Capacity	4TB (1× 4TB)	8× 3.5 in. hot-swappable 4TB HDDs (32TB) 4× 2.5 in. hot-swappable 1.92TB SSDs (7.68TB)	12× 3.5 in. hot-swappable 8TB HDDs (96TB) 4× 2.5 in. hot-swappable 3.84TB SSDs (15.36TB)
Usable Event Data Storage	—	Hot/SSD = ~5.2 TB Warm/HDD = ~21 TB	Hot/SSD = ~11 TB Warm/HDD = ~65 TB
Performance Benchmark	8K EPS. 500 SNMP, 200 WMI for Performance/ 100 WMI for Logs	20K EPS with Collectors	50K EPS with Collectors
Recommended Max. UEBA users	—	10 000	10 000
Dimensions			
Height x Width x Length (inches)	1.73 × 17.32 × 21.26	3.46 × 17.32 × 29.33	5.25 × 17.2 × 24.4
Height x Width x Length (mm)	44 × 440 × 540	88 × 440 × 745	132 × 438 × 621
Weight	16.76 lbs (7.6 kg)	57.64 lbs (26.145 kg)	63.89 lbs (28.98 kg)
Form Factor	1 RU	2 RU	3 RU
Environment			
AC Power Supply	350W single PSU	100-240 VAC, 60-50 H	100-240 VAC, 60-50 H
Power Consumption (Average / Maximum)	93.87 W / 114.73 W	610 W / 744 W	695 W
Heat Dissipation	425.58 (BTU/h)	2537 BTU/h	2370 BTU/h
Operating Temperature	32°F ~ 104°F (0°C ~ 40°C)	32°F to 104°F (0°C to 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)	-4°F to 167°F (-20°C to 75°C)
Humidity	5% to 95% (non-condensing)	5% ~ 95% relative humidity, non-operating, non-condensing	5% ~ 95% relative humidity, non-operating, non-condensing
Forced Airflow	Front to Back	Front to Back	Front to Back
Operating Altitude	—	10 000 feet (3048 meter)	10 000 feet (3048 meter)
Compliance			
Compliance	FCC, ISED, CE, RCM, VCCI, BSMI, UL/cUL, CB		

Ordering Information

PRODUCT	SKU	DESCRIPTION
Device + EPS Licensing		
FortiSIEM Hardware Product		
FortiSIEM 500G	FSM-500G	FortiSIEM Collector Hardware Appliance FSM-500G. Supports up to 5000 EPS.
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 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-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-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 and Linux) Perpetual License	FSM-AGT-ADV-XX-UG	XX Advanced Agents for Perpetual License.
FortiSIEM Advanced Agent (WIndows and 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	24×7 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 GB Per Day Licensing		
FortiSIEM GB Subscription License	FC[1-6]-10-SMGS1-1026-02-DD	FortiSIEM Subscription license for XXGB - YYGB Logs per day. Increments of additional 1GB Logs per day. Includes HA Super, FortiCare Premium support.
FortiSIEM GB UEBA Subscription License	FC[1-3]-10-SMGS1-334-02-DD	Per UEBA Agent based telemetry Subscription License for XX - YYY Agents.
FortiSIEM GB Advanced Agent Subscription License	FC[1-3]-10-SMGS1-182-02-DD	Per Advanced Agent Subscription License for XX - YYY Agents. Providing File Integrity Monitoring (Windows, Linux), advanced monitoring and forensics.
FortiSIEM GB Indicators of Compromise (IOC) Service	FC[1-L]-10-SMGS1-149-02-DD	FortiGuard Indicators of Compromise (IOC) Service (for XX - YYGB/Day of Logs).

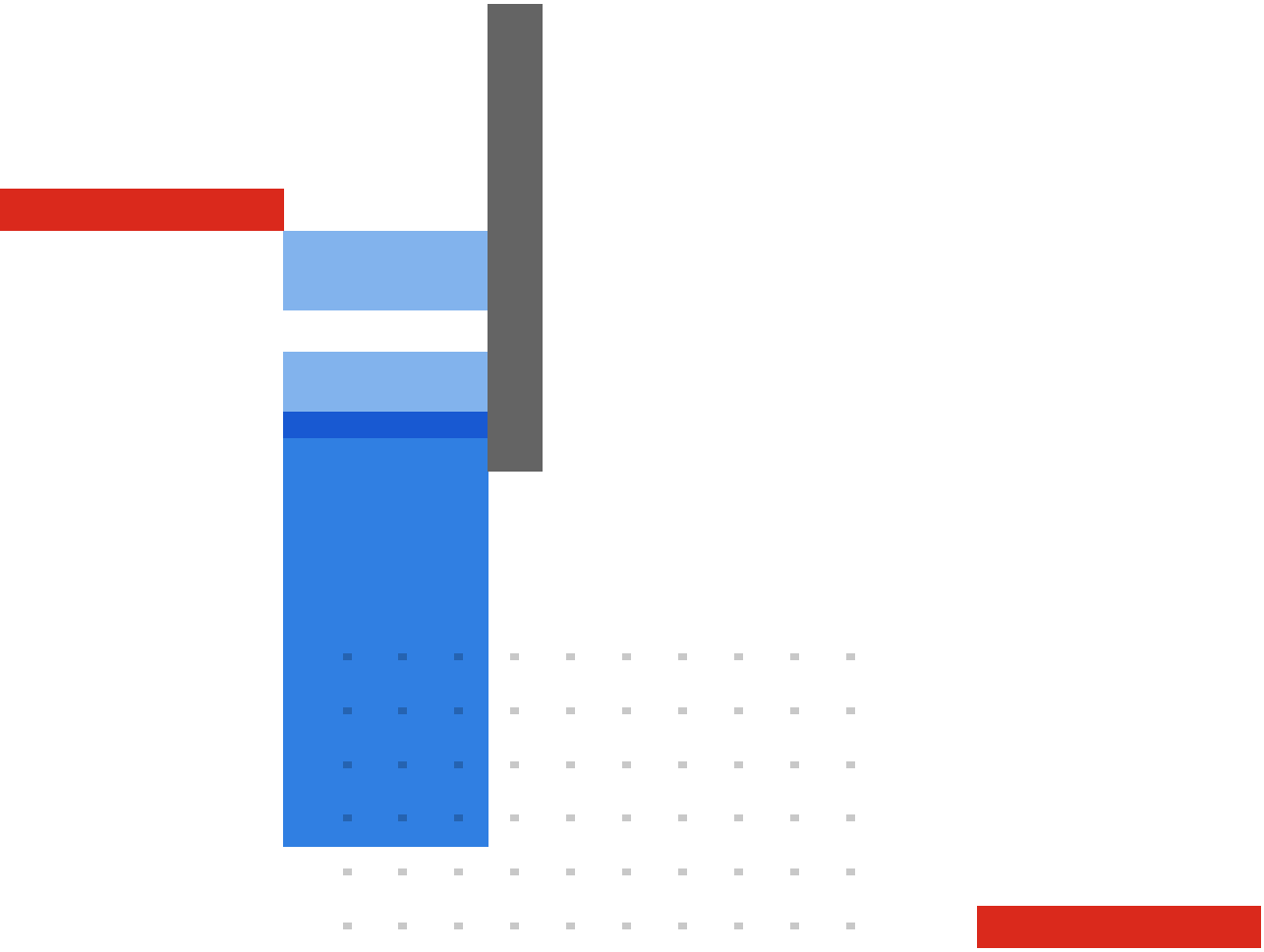
Ordering Information

PRODUCT	SKU	DESCRIPTION
FortiSIEM Cloud		
Region A		
	FC2-10-SMCLD-543-02-DD	10 FortiSIEM Compute Units (FCU). Quantity 1 only. Deployment regions A, refer to datasheet for region locations. Annual Subscription. Includes FortiCare Premium Support.
	FC3-10-SMCLD-543-02-DD	10 FortiSIEM Compute Units (FCU). Minimum quantity of 2 and maximum 4. Deployment regions A, refer to datasheet for region locations. Region A Annual Subscription. Includes FortiCare Premium Support.
	FC4-10-SMCLD-543-02-DD	10 FortiSIEM Compute Units (FCU). Minimum quantity of 5 and maximum 60. Deployment regions A, refer to datasheet for region locations. Annual Subscription. Includes FortiCare Premium Support.
	FC-10-SMCLD-541-02-DD	500GB Online storage. Deployment regions A, refer to datasheet for region locations. Requires minimum quantity of 1 with initial FortiSIEM Compute Unit order. Annual Subscription.
	FC-10-SMCLD-542-02-DD	Optional Archive storage. 500GB of Archive storage per unit. Deployment regions A, refer to datasheet for region locations. Annual Subscription.
Region B		
	FC2-10-SMCLB-543-02-DD	10 FortiSIEM Compute Units (FCU). Deployment regions B, refer to datasheet for region locations. Quantity 1 only. Annual Subscription. Includes FortiCare Premium Support.
	FC3-10-SMCLB-543-02-DD	10 FortiSIEM Compute Units (FCU). Deployment regions B, refer to datasheet for region locations. Minimum quantity of 2 and maximum 4. Annual Subscription. Includes FortiCare Premium Support.
	FC4-10-SMCLB-543-02-DD	10 FortiSIEM Compute Units (FCU). Deployment regions B, refer to datasheet for region locations. Minimum quantity of 5 and maximum 60. Annual Subscription. Includes FortiCare Premium Support.
	FC-10-SMCLB-541-02-DD	500GB online storage. Deployment regions B, refer to datasheet for region locations. Requires minimum quantity of 1 with initial FortiSIEM Compute Unit order. Annual Subscription.
	FC-10-SMCLB-542-02-DD	Archive 500GB storage. Deployment regions B, refer to datasheet for region locations. Annual Subscription.
FortiSIEM Automation Service		
FortiSIEM Automation Service	FC1-10-SIMPC-1055-02-DD	FortiSIEM Automation Service providing one concurrent playbook execution capacity. Increase quantity to enable additional concurrent playbook processing. Maximum quantity of 10.

Visit https://www.fortinet.com/resources/ordering-guides for related ordering guides.

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.



FORTINET

www.fortinet.com

August 15, 2025

FSIEM-DAT-R41-20250815