SOC as a Service

Always-on protection with 24/7 threat monitoring and incident response, without operational complexity

Available Globally



Highlights

- 24×7×365 security monitoring and threat detection
- Integrated MDR, Incident Response, and Digital Forensics services
- Global SOC locations enabling always-on managed services
- Highly skilled security analysts with deep Fortinet expertise
- Dedicated Service Delivery representatives supporting customer success
- Advanced Fortinet SOC platform with AI and machine learning
- Built-in security orchestration, automation, and response with pre-built use cases and playbooks
- Integrated FortiGuard Threat Intelligence for enhanced threat detection and response

Always-on Security Operations as a Service

Maintaining effective security operations requires specialized expertise, continuous monitoring, and significant operational resources; challenges many organizations face as threats continue to evolve. Fortinet SOC-as-a-Service (SOCaaS) provides always-on protection through 24×7 threat monitoring, intelligent alert triage, and expert-guided incident response. Delivered by Fortinet's global SOC team and powered by FortiGuard Threat Intelligence, SOCaaS helps organizations detect threats earlier, respond faster, and strengthen their security posture. By offloading operational complexity, SOCaaS enables security teams to focus on strategic priorities while maintaining continuous protection across their environments.

Cybersecurity breaches can instantly disrupt operations and erode stakeholder trust. Even enterprises and service providers with substantial security investments remain vulnerable to misconfigurations, vulnerabilities and a sophisticated threat landscape.

Fortinet SOCaaS compliments your incident response team with 24/7 Monitoring and Triage of Alerts, expert analysis and recommendations, and provides a flexible and scalable solution accelerating response for your network threat monitoring.

Key Capabilities

24/7 Monitoring and SOC Experts Access

24×7 monitoring and incident response guidance across all time zones in global Security Operations Center (SOC). Customers benefit from continuous access to certified SOC analysts who provide expert-level support for escalated security alerts.

FortiCloud Built-in Portal

Customer Portal provides centralized visibility into SOC operations including monitored assets, alerts, reports, dashboards, service requests, settings and more.

Integration with FortiCloud Central Management features such as IAM, IDP, API, Organizations enable customers and partners to control access to SOC data. Native integration with other FortiCloud services and streamlined processes ensures productivity across all managed services.

AI-driven Automated Triage

SOAR automation playbooks enable SOC team to extract insights from different data sources and enrich alerts. AI-driven alert triage capabilities trained over years enable SOC Team with fast decision making.

Seamless integration with FortiGuard Labs' threat intelligence enhances alert triage quality with the latest indicators of compromise, signatures and outbreak alerts service. Alerts are automatically enriched by CMDB meta data as well as historical activities of affected assets which lead to more accurate triage and additional context in incidents.

Incident Response Guidance

Following initial triage, SOC provides an analysis, verdict, severity and Incident Response guidance to contain and mitigate ongoing threats. Source of detection, Indicators of compromise, affected users and entities, triage reports with historical data and sample logs are made available to facilitate incident response.

Risk score system calculates risk for different entities including users, endpoints, indicators, security events and alerts. Automated Risk Adjusted Alerts enables more effective impact assessment and prioritizing incident response.

Feedback channels are available to reduce noise and False-positive alerts. Requests can be made to tune detection rules, define exceptions and exclusions. Requests for threat hunting and further investigations into incidents can be made. Reports would be made ready and shared upon request.

Fortinet SOCaaS is a cost-effective solution that supports data collection and monitoring across Fortinet Security Fabric devices, FortiCloud services, and third-party data sources, helping organizations build a top-tier security response capability.

Integration with Fortinet Managed Services

SOCaaS works in close coordination with other subscribed Managed Services, securely sharing relevant artifacts and associated data. This integration enables timely and effective actions to contain incidents and improve security posture. Streamlined collaboration across services ensures that customers benefit from a cohesive incident response life cycle, enabling faster resolution and informed planning to mitigate future risks.

SOC alerts shared with Managed FortiGate, FortiClient, FortiEndpoint Services could lead to containment actions and tightening security controls. SOC data sharing with MDR service would enhance XDR capability and threat detection while sharing data with Fortiguard Forensics and Incident Response services would facilitate incident investigation, remediation and recovery.

Multi-Tenancy & Partner Enablement

Fortinet Partners and service providers can augment their managed security services with SOCaaS. Multi-tenancy is in the core of SOCaaS design and meets ISO and SOC2 compliance requirements. While data boundary is maintained, SOC single pane visibility is available from the multi-tenant customer portal. Partners can choose to grant access to their clients.

FortiCloud Organizations facilitates multi-tenancy by allowing partners manage multiple accounts centrally. FortiCloud IAM, IDP and API users facilitates portal access and integration with partner portals or Incident management solutions. Moreover, Fabric devices set up for multi-tenancy using FortiGate VDOMs or FortiClient EMS Sites could be assigned to multiple tenants and then monitored separately for each tenant.

Customer Success

Our dedicated Service Delivery Managers (SDMs) provide guidance through your SOCaaS journey, helping to ensure that your service is delivered efficiently and aligned with your strategic business goals. On-demand service reviews are available to assess performance, answer questions, and provide guidance for refining your SOC strategy for a Customized experience.

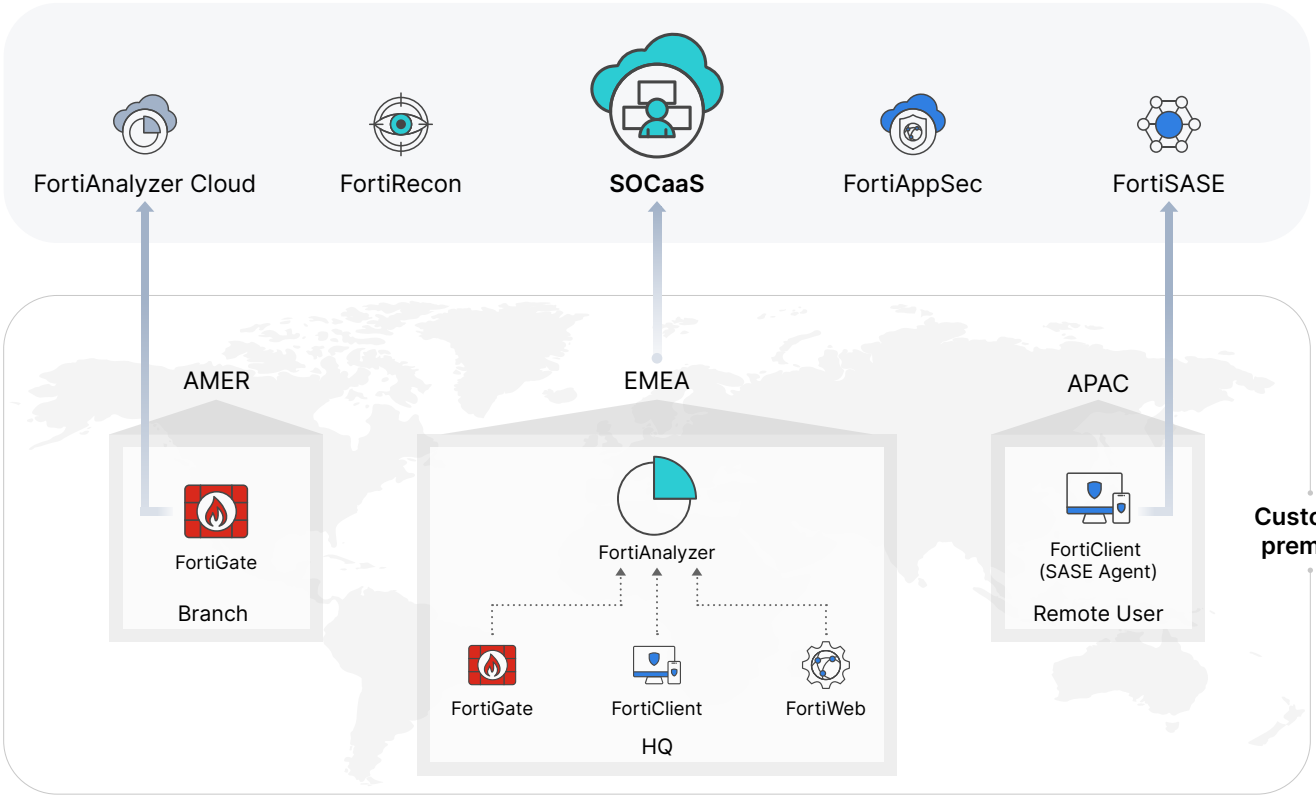
Threat Detection

SOCaaS threat detection capabilities are based on two data collection and analytics models:

Fortinet Fabric Monitoring

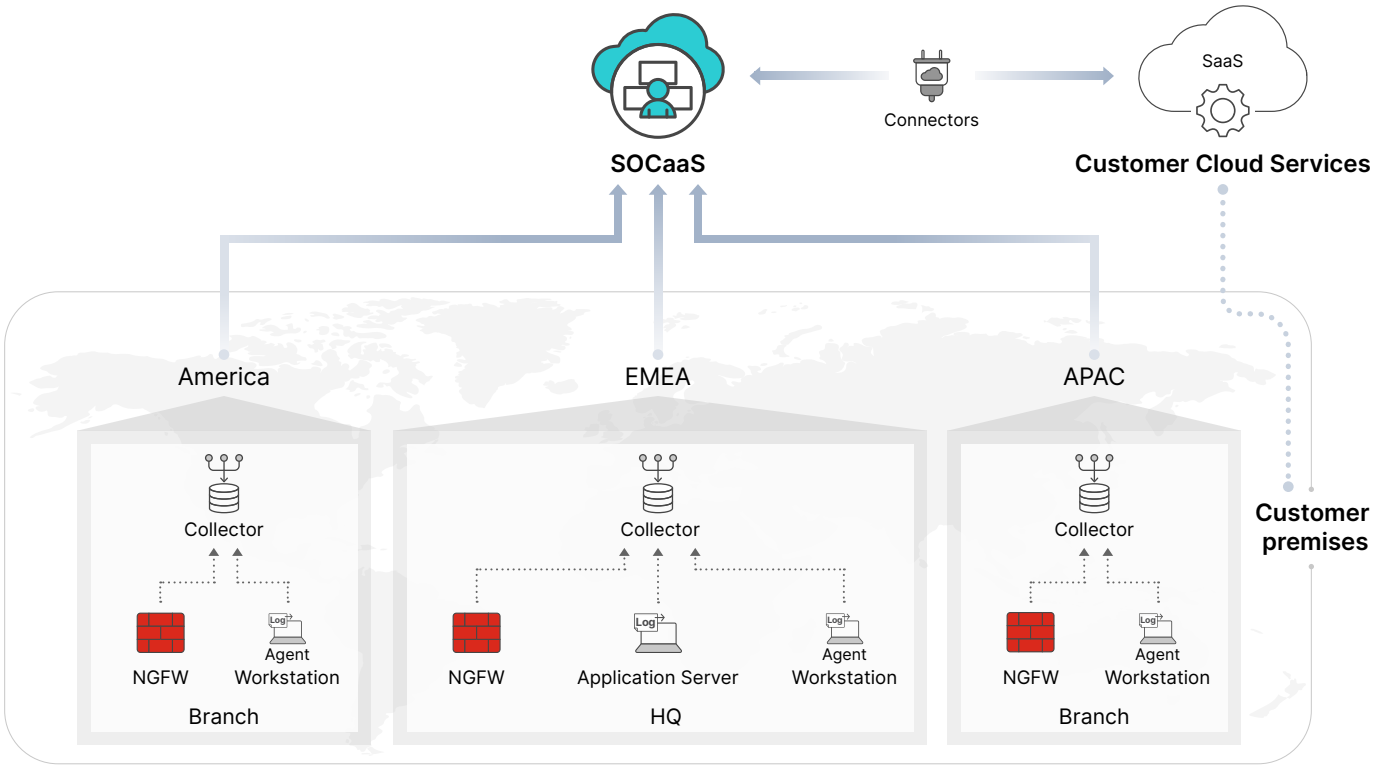
Network traffic and endpoint activity can be monitored when supported Fortinet Security Fabric devices, such as FortiGate or FortiClient/FortiEndpoint, are onboarded to SOCaaS. Onboarding typically takes only a few days. FortiAnalyzer serves as the primary analytics platform to collect, process, and forward logs to the SOC for monitoring and analysis.

A complete list of supported threat detections is available in the SOCaaS Threat Detection Guide.



Multi-Vendor Monitoring Model

A wide range of assets including applications, network devices such as firewalls, and cloud services from Fortinet and third-party vendors can be monitored under this model. Onboarding additional data sources may take several weeks depending on the type of system being integrated. Deployment of on-premises or cloud-based log collectors, as well as agent installation, may be required.

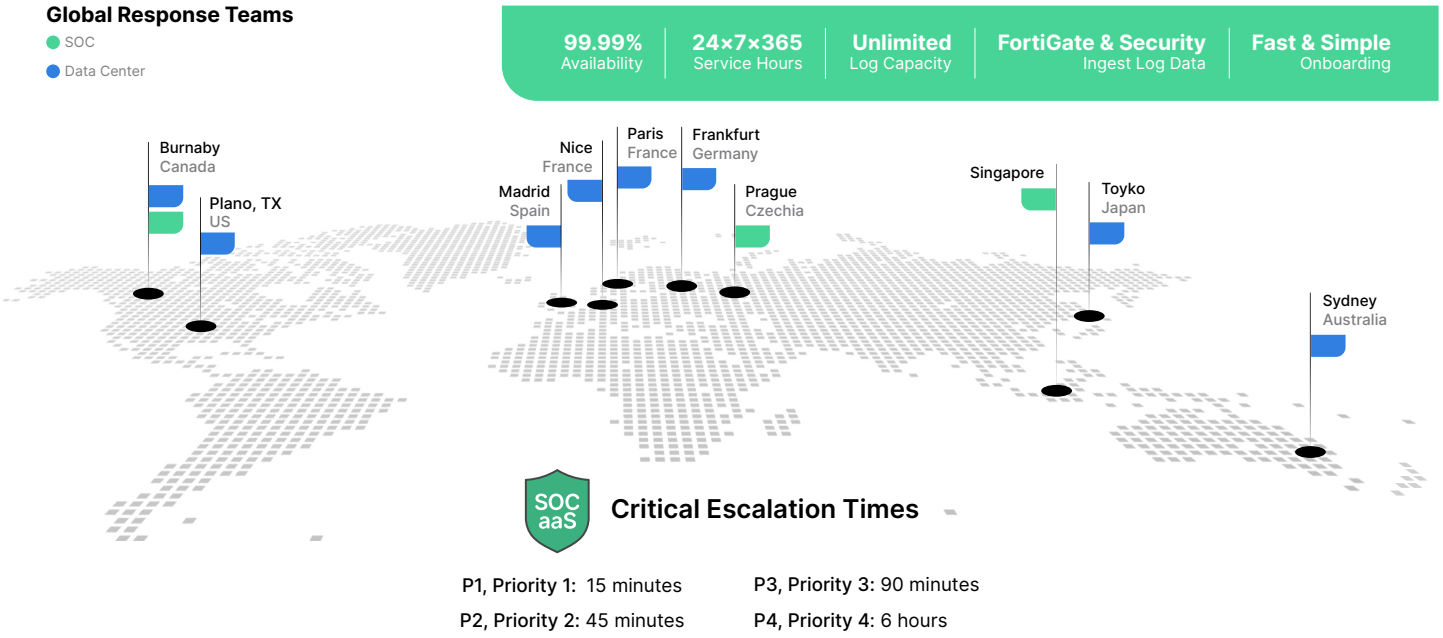


FortiSIEM serves as the primary security analytics platform for this monitoring model within the Fortinet SOC. As a result, all data sources and connectors supported by FortiSIEM are available for integration. A complete list of supported data sources is available in this FortiSIEM Guide.

Managed FortiAnalyzer Service

Managed FortiAnalyzer Service (MFAZ) provides 24×7 monitoring of system logs on G-series FortiAnalyzer appliances to ensure platform health, availability, and proper functionality. The service also includes device management tasks such as firmware upgrades, configuration updates, user management, capacity monitoring, and related operational activities.

The 24×7 monitoring scope is limited to the FortiAnalyzer system and its local logs. Threat monitoring and analysis of data collected from external sources require a separate license, depending on the specific data sources being monitored.



Subscriptions and Bundles

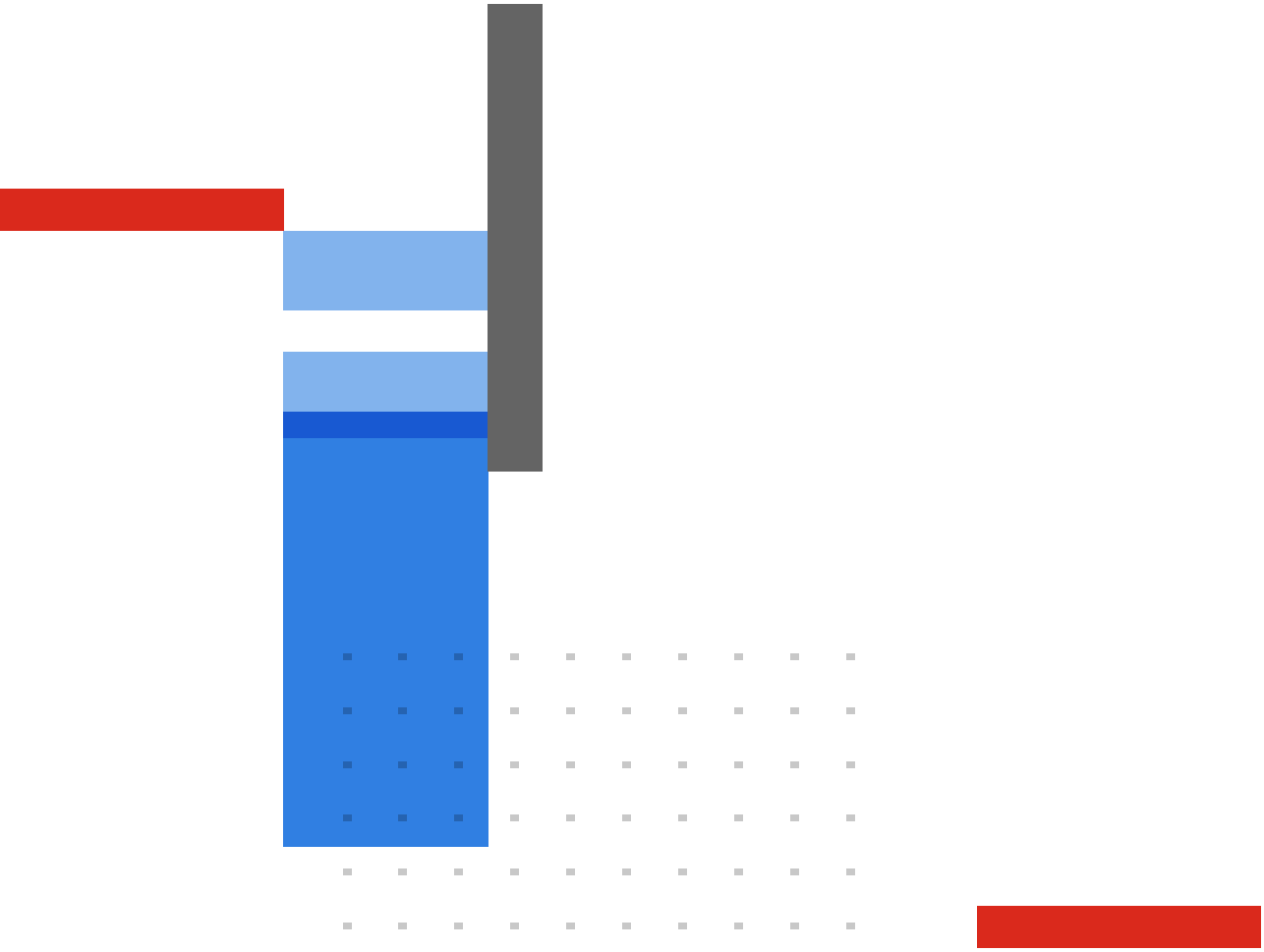
SOCaaS Fabric Monitoring is available as an add-on license for select Fortinet Security Fabric products or included with certain product plans and subscriptions. The service can also monitor a broad range of Fortinet Fabric and third-party data sources, providing flexible coverage across diverse environments.

For more information on licenses, please refer to SOCaaS Ordering Guide.

Service	Description
SOCaaS Multi-Vendor Monitoring	Subscription for 24×7 SOCaaS monitoring: 1 GB/day of logs, covering both Fortinet and third-party sources. FortiCare Premium included.
SOCaaS Fabric Monitoring	SOCaaS 24×7 cloud-based managed log monitoring, incident triage and SOC escalation service.
	FortiGate: Add-on to any FortiGate HW\VM. Includes a complimentary instance of FortiAnalyzer Cloud with limited features and storage.
	FortiSASE: Included with FortiSASE Advanced or Comprehensive Subscriptions.
	FortiWeb: Add-on to FortiAppSec Cloud WAF Standard and Advanced plans. Included with Enterprise plan.
	FortiAppSec Cloud: Included with FortiAppSec Standard or Premium subscription.
	FortiEndpoint: Included with all Managed options and select DIY FortiEndpoint subscriptions.
	FortiClient: Incldued with FortiGuard Forensics Subscriptions..
	FortiEDR: Included with XDR and Managed XDR options.
SOCaaS Managed FortiAnalyzer Service	24×7 SOCaaS expert-delivered monitoring and management service for FortiAnalyzer G series appliances.

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

Copyright © 2026 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 SVP Legal and above, 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.

March 11, 2026

SOC-DAT-R15-20260311