FortiGuard SOC as a Service

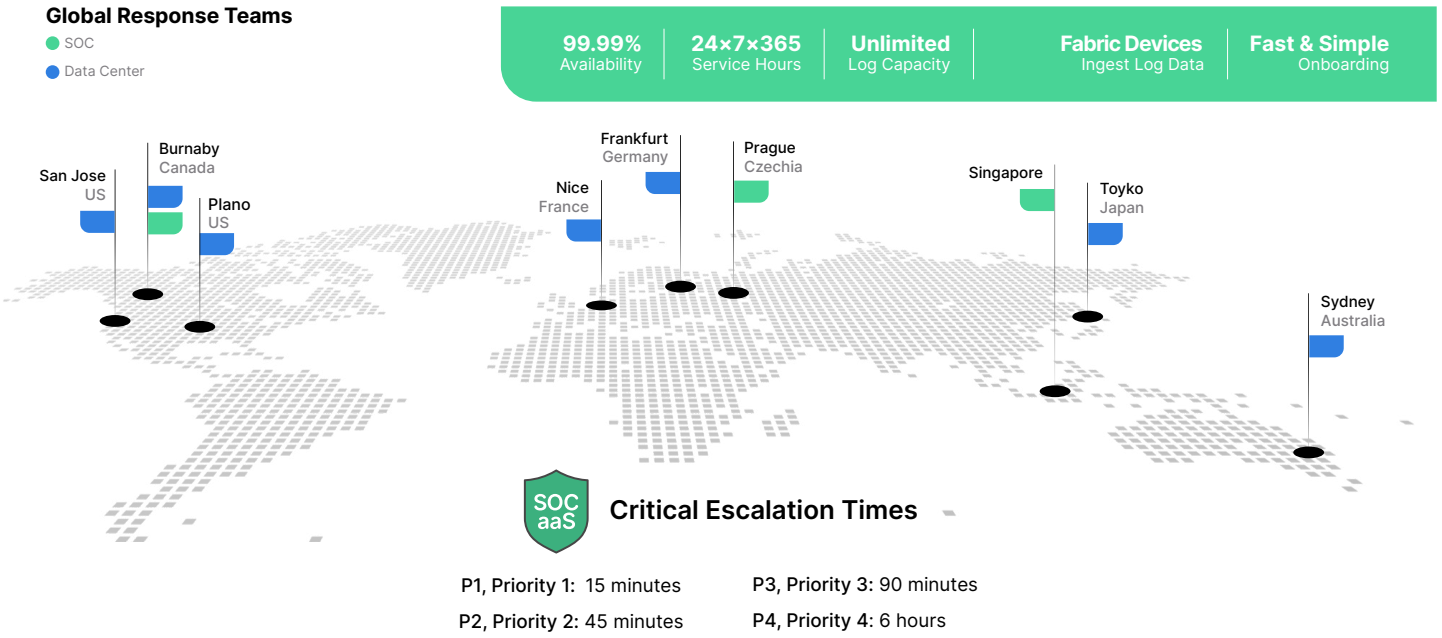
Highlights

- SOC 2 Type II and ISO27001 certified service
- 24×7×365 monitoring services enabled through Global SOC locations
- Security skilled staff with Fortinet product technical expertise
- Dedicated Service Delivery representatives to foster business relationships and customer success
- Best of breed Fortinet SOC platform, including AI and Machine Learning capabilities, Security Orchestration, Automation and Response with pre-built SOC Use Cases, Playbooks and integration with FortiGuard Threat Intelligence Services

Augment Your SOC With FortiGuard SOCaaS

Take advantage of Fortinet's turn-key Security Operations Center as a service, a cloud based managed service providing you visibility on security threats in your network. A simple Fabric Device add-on offering that is designed to help you fast-track your SOC, detect and respond to threats, and improve security posture by providing continuous Cyber Awareness, Visibility, and Control over your Security Fabric network.

- FortiGuard SOCaaS connects the Security Fabric eco-system to a central, automated, managed platform that monitors logs, detects threats, engages Fortinet security experts, and escalates critical incidents to customers
- Delivered by a global team of 24×7×365 Fortinet Security Analysts and leveraging FortiGuard Threat Intelligence Services
- Single-Pane FortiCloud Portal for SOCaaS and other integrated managed services, including Managed FortiGate Service, FortiGuard Forensics, and FortiSASE



SOC Monitoring Use Cases

SOCaaS provides 24×7 coverage of Network and Endpoint use cases mapped to the Cyber-kill Chain.

Network Security Use Cases

FortiGate and FortiSASE security monitoring.

Powered through FortiGuard Security Services activation, the service actively monitors and detects network threats against customer network assets.

- 24/7 log monitoring, incident triage, and alert escalation
- Weekly SOC and Alert escalation reports

FortiWeb and FortiWeb Cloud Integration for Web Application and API Security.

Actively monitor and detect threats against critical web applications and APIs. New integration with FortiWeb enabled with the Threat Analytics service license will evaluate thousands of alerts and group them into incidents based on the patterns identified.

- Real-time security monitoring and detection of dynamic attacks like DoS, SQL injections, XSS, and other OWASP Top 10 Web Application Security Risks
- Differentiate significant threats from informational alerts and false positives
- Alert triage reports providing incident details to support timely incident handling
- Weekly executive summary, threat protection, and security tuning reports providing stakeholders actionable steps to strengthen their security posture and optimize operations

Endpoint Protection Use Cases

FortiEndpoint Integration

FortiEndpoint is an all-in-one single-agent solution offering centralized management of endpoints and advanced endpoint protection benefit.

- FortiEndpoint XDR + SOC license provides 24/7 endpoint threat monitoring and detection, and alert escalation
- Escalations will be coordinated between the SOCaaS team and the Managed FortiEndpoint Services team for customers subscribed to both Managed services
- FortiGuard Forensic. Request a comprehensive endpoint Forensic analysis directly from the SOCaaS Portal. This feature is available with a FortiEndpoint or FortiSASE license

FortiEDR Threat Detection.

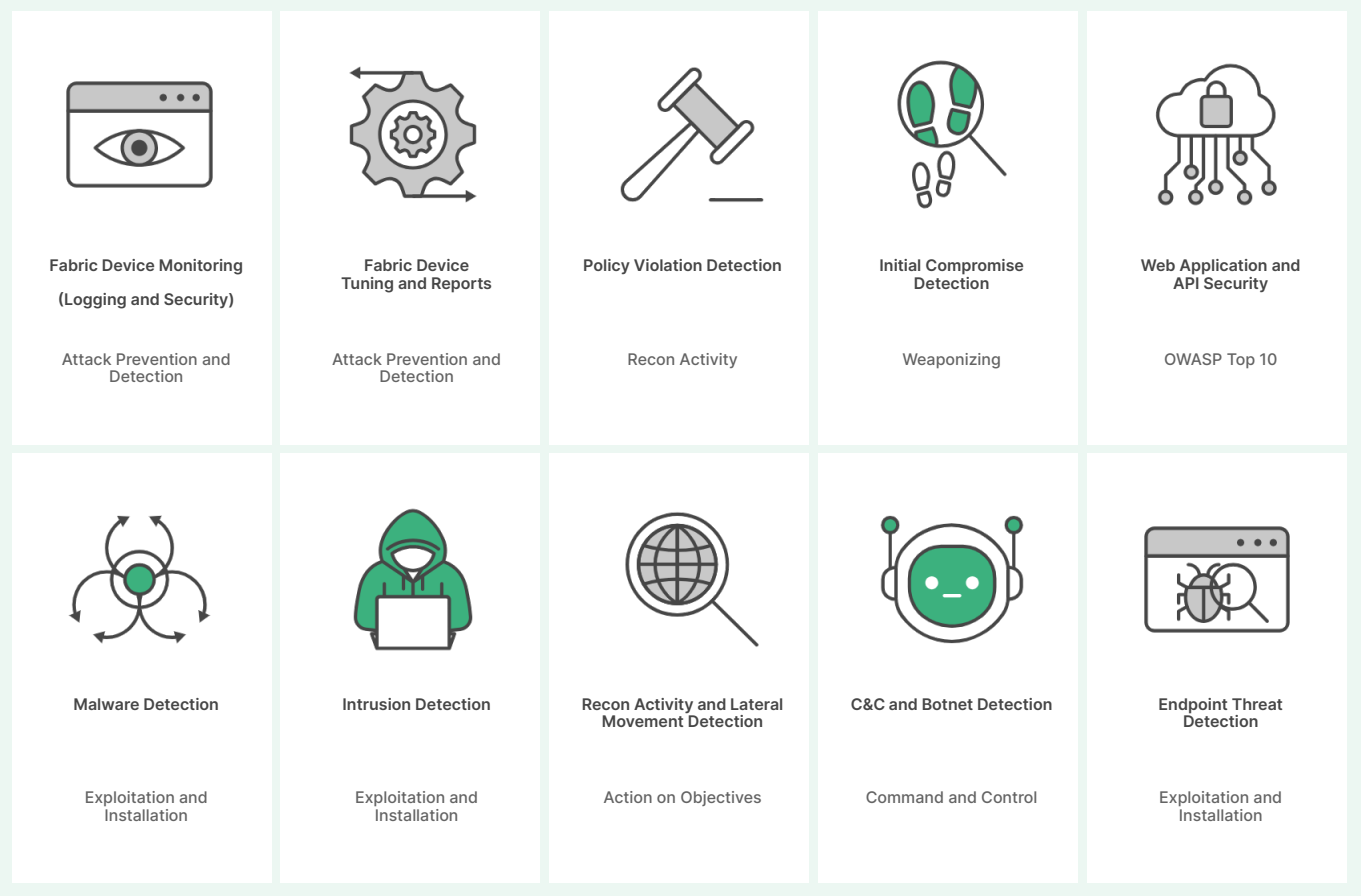
FortiEDR monitoring and detection correlation with FortiGate or FortiSASE logs.

- 24/7 monitoring of FortiEDR detection logs
- Enrichment of use cases resulting in faster detections
- Incident escalation with detailed remediation steps

Capabilities

Use Case Coverage

- SOC Detection Cyber Kill Chain coverage for Network and Web Application use cases across IT and OT environments



Cloud Service Portal

- Maintain visibility in multiple languages for onboarded Fabric devices, monitor assets, manage SOC escalated alerts, interact with SOC security analysts, review weekly SOC reports, submit service request, request forensics analysis, and more

Monitor and Detect

- 24×7×365 security operations monitor logs and events for pre-defined detection use cases
- 24×7×365 FortiEDR Threat Detection and Monitoring
- 24×7×365 FortiWeb Attack logs and Threat Analytics monitoring
- 24×7×365 access to SOC analysts for technical support from SOC portal

Investigate and Escalate

- Alert triage including analysis and validation of threat signatures, indicators, and anomalies
- Flexible escalations in different severities and SLAs as short as 15 minutes including alert details, correlations, and reports

Service Delivery

- Connect with a dedicated service delivery representative for on-demand service reviews
- Review security posture, tuning and improvement options, integration possibilities, and get the most from your entitlements

Benefits

Resource Savings

- Eliminate tedious manual work
- Eliminate technology, playbooks, and talent maintenance
- Experience reduced and predictable costs
- Experience simplified threat detection

Effective Detection

- Eliminate missing threats
- Detect incidents in early stage
- Gain expert insights and guidance
- Gain access to threat intelligence

Maximized Investment

- Access service delivery managers
- Improve security posture
- Experience SOC maturity through fabric integrations

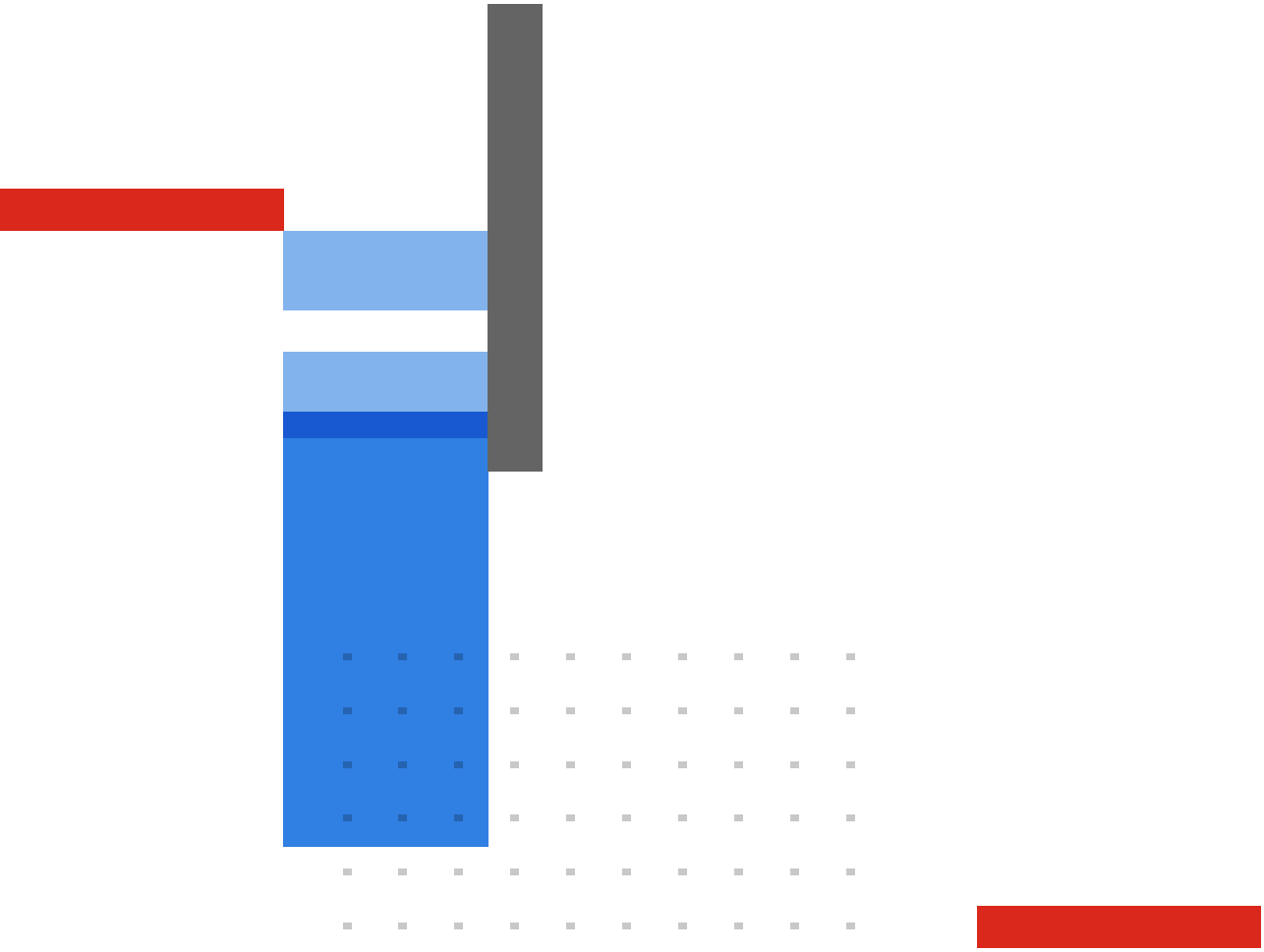
Ordering Information

SERVICE	DESCRIPTION
Network Security Use Cases	
FortiGate + SOCaaS	A simple add-on to any FortiGate Hardware or VM. SOCaaS: 24×7 cloud-based monitoring, incident triage and SOC escalation service.
FortiSASE + Forensics + SOCaaS	SOCaaS coverage with FortiSASE Advanced or Comprehensive Subscription plus FortiGuard Forensics.
FortiWeb + Threat Analytics + SOCaaS	A Simple add-on to an FortiWeb Hardware, VM or FortiWeb Cloud. SOCaaS: 24×7 cloud-based managed log monitoring, incident triage and SOC escalation service. Must purchase Advanced or Enterprise bundle.
Endpoint Protection Use Cases	
FortiEDR XDR + SOCaaS	SOCaaS coverage with FortiEDR Protect and Respond and XDR Cloud Subscription and FortiCare Premium.
FortiEndpoint (DIY) XDR + SOCaaS	XDR + SOC Subscription (Discover, Protect and Respond) with XDR-AI, ZTNA/VPN and Advanced EPP, plus FortiGuard Forensics and SOCaaS integration.
FortiEndpoint (DIY) PREVENT + SOCaaS	Advanced EPP (with ZTNA/VPN) plus FortiGuard Forensics and SOCaaS integration, including FortiAnalyzer Cloud and FortiCare Premium.
FortiEndpoint (Managed) PREVENT + SOCaaS	Advanced EPP (with ZTNA/VPN) plus FortiGuard Forensics and SOCaaS integration, including FortiAnalyzer Cloud and FortiCare Premium.
FortiEndpoint (Managed) EDR ESSENTIAL + SOCaaS	EDR Essentials Subscription (Discover, Protect and Respond) with ZTNA/VPN and Advanced EPP, plus FortiGuard Forensics and SOCaaS integration.
FortiEndpoint (Managed) XDR + SOCaaS	XDR + SOC Subscription (Discover, Protect and Respond) with XDR-AI, ZTNA/VPN and Advanced EPP, plus FortiGuard Forensics and SOCaaS integration.

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

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 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.

October 31, 2024

FSOC-DAT-R9-20241031