

## DATA SHEET

# FortiCloud SOC-as-a-Service™

Available in:



Cloud

## FortiCloud SOCaaS

This managed service provides scalable security operations designed to help you maintain continuous Cyber Awareness and Control of your Fortinet Security Fabric network.



### FORTINET SOC ANALYSTS MONITOR CUSTOMER'S NETWORK FOR SECURITY EVENTS, TRIAGE ALERTS AND ESCALATE THREATS



#### Detect

- 7×24×365 Security Operation
- Compromised Hosts
- Malware Detection
- Unauthorized Access
- Policy Violation
- Command & Control & Botnet



#### Investigate

- Automated Correlation, Analysis and Context Enrichment using SOAR Playbooks
- Alert Triage on Incident Types
- Incident Analysis, Validation & Severity Ranking



#### Respond

- End-to-End Workflow
- SOP & Playbooks
- Incident & Ticket Management
- Communication & Escalation Path SLA
- Remediation Recommendation



#### Monitoring

- FortiGuard Threat Intelligence
- Cyber Kill Chain Tracing
- Indicators of Compromise
- Suspicious Activities
- Privileged Access Monitoring
- Policy Violation & Misconfiguration
- Vulnerability Monitoring



#### Management & Tuning

- SOC Portal (Device Onboarding, Device Tuning Advisory, Change Request, Ticket Status)
- Incident Severity Definition Correlated with Asset Classification
- Device Health Monitoring
- Device Hardening
- Device Performance Tuning
- Fabric Posture Improvement

## Why Fortinet

- Security focused skill staff with technical expertise on Fabric Devices and Incident Response (IR) best practices
- Orchestration, Automation & Response with pre-built threat Use Cases and Playbooks
- Best of Breed Fabric based SOC Platform
- Global SOC locations

### 7×24×365 Monitoring by Expert Analysts around the Globe

# HIGHLIGHTS

## How Does It Work

Two Deployment Options

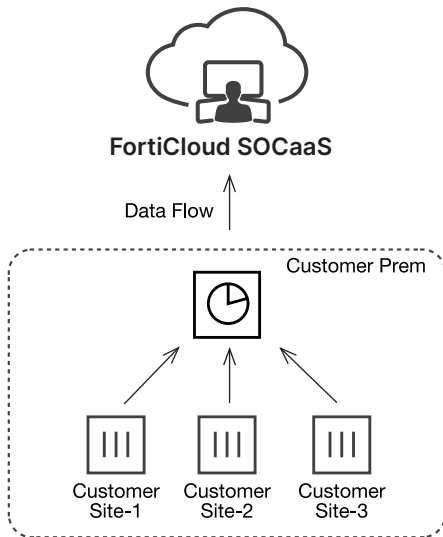
**Customer On-Prem FAZ**

**Subscription**

- Subscribe to FortiCloud SOCaaS per FortiGate License

**Monitoring**

- Customer FGT logging to On-Prem FAZ
- On-Prem FAZ forwards logs to FortiCloud SOCaaS for Security Orchestration, Automation and Incident Response



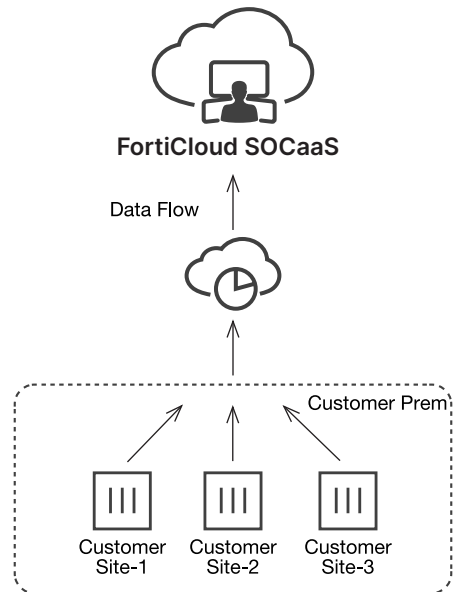
**Customer FAZ Cloud**

**Subscription**

- Subscribe to FortiCloud SOCaaS per FortiGate License

**Monitoring**

- Customer FGT logging to FAZ Cloud
- FAZ Cloud sends alerts to FortiCloud SOCaaS for Security Orchestration, Automation and Incident Response



## Value to Customers

Full Cyber Kill Chain Lifecycle SOC Use Cases

SOC USE CASES	ATTACK KILL CHAIN REFERENCE	FORTIGATE MODULES AND LICENSE REQUIREMENTS	SOC DELIVERABLES
<b>Fabric Device Monitoring (Logging &amp; Security)</b>	Attack Prevention & Detection Across all Kill Chain Phases	FortiAnalyzer (Firmware License)	FortiGate Logging to FAZ
<b>Fabric Device Tuning &amp; Reports</b>			
<b>Policy Violation Detection</b>	Recon Activity	App Control (Firmware License) Traffic Log Analysis (Firmware License)	FortiGate System Security Event Monitoring
<b>Initial Compromise Detection</b>	Weaponizing & Delivery	Web Filtering (UTP License Required) Spam Filtering (UTP License Required)	Daily \ Weekly SOC Reports:
<b>Malware Detection</b>	Exploitation & Installation	Antivirus (ATP License Required) Outbreak Prevention (License Required) Sandbox Cloud (License Required)	<ul style="list-style-type: none"> <li>• Asset Visibility</li> <li>• Policy Violations</li> <li>• UTM Tuning</li> </ul>
<b>Intrusion Detection</b>		Intrusion Prevention (ATP License Required) Industrial DB (License Required) WAF (License Required)	Threat Detection & Analysis - Alert Triage
<b>C&amp;C &amp; Botnet Detection (Compromised Host)</b>	Command & Control	Intrusion Prevention (ATP License Required) FortiAnalyzer (IOC License Required)	SOC Portal Access
<b>Recon Activity &amp; Lateral Movement Detection</b>	Action on Objectives	Anomaly Detection (Firmware License) Traffic Log Analysis (Firmware License)	



## BENEFITS

### Actionable Alerts

- Customer's network is monitored by Fortinet SOC analysts
- Customers don't have to deal with overwhelming alerts and false positives

### Simplified Operations & Predictable Costs

- Customers have a predictable cost for their security operations
- Reduced operational complexity
- Reduced operational cost

### Gain Expert Insights

- Customer gain expert insight into their log data and misconfigured security controls
- Real-time incident alerting
- Fast incident response and remediation
- 24x7 access to expert SOC analysts

## Global SOC Locations



## ORDER INFORMATION

Each FortiGate unit to be monitored must have one of the following subscriptions:

SKU	Description
<b>FC-10-XXXXX-841-02-DD</b> <i>XXXXX is defined by the FortiGate appliance code</i>	360 Protection (FMG/FAZ Cloud, FortiCloud SOCaaS, IPS, AMP, App Ctrl, Web & Video Filtering, AS, Security Rating, IoT Detection, Industrial Security, SD-WAN Orchestrator, SD-WAN Cloud Monitoring, FortiConverter Svc, and ASE FortiCare)
<b>FC-10-FG[X]VM-842-02-DD</b> <i>X refers to different FG VM models - # of CPUs</i>	360 Protection for FortiGate-VM with X CPU (FMG/FAZ Cloud, FortiCloud SOCaaS, IPS, AMP, App Ctrl, Web & Video Filtering, AS, Security Rating, IoT Detection, Industrial Security, SD-WAN Orchestrator, SD-WAN Cloud Monitoring, FortiConverter Svc, and ASE FortiCare)
<b>FCx-10-FGVVS-843-02-DD</b> <i>X refers to different FortiGate VM subscription licences</i>	Subscriptions license for FortiGate-VM with 360 Protection Bundle included
<b>FC-10-XXXXX-464-02-DD</b> <i>XXXXX is defined by the FortiGate appliance code</i>	FortiAnalyzer Cloud SOCaaS: Cloud-based Log Monitoring (PaaS), including IOC Service and FortiCloud SOCaaS



[www.fortinet.com](http://www.fortinet.com)

Copyright © 2021 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 General Counsel, 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.