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

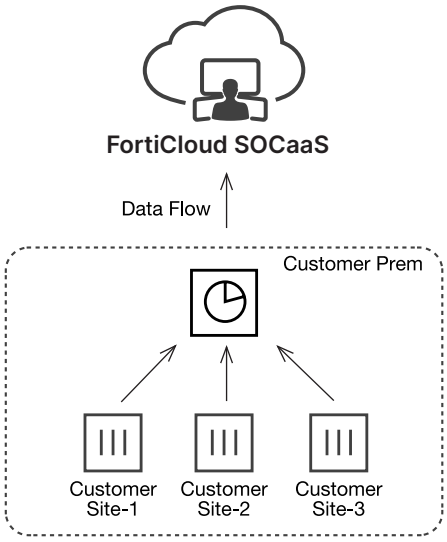
7×24×365 Monitoring by Expert Analysts around the Globe

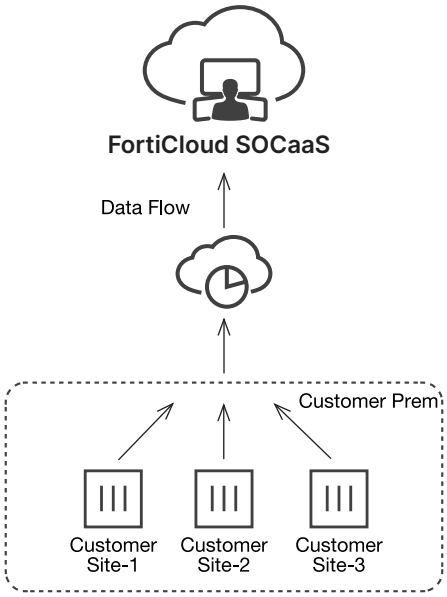
HIGHLIGHTS

How Does It Work

Two Deployment Options

Customer On-Prem FAZ	Customer FAZ Cloud
Subscription ▪ Subscribe to FortiCloud SOCaaS per FortiGate License	**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	**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 REQUIRMENTS	SOC DELIVERABLES
Fabric Device Monitoring (Logging & Security)	Attack Prevention & Detection Across all Kill Chain Phases	FortiAnalyzer (Firmware License)	FortiGate Logging to FAZ FortiGate System Security Event Monitoring Daily \ Weekly SOC Reports: • Asset Visibility • Policy Violations • UTM Tuning Threat Detection & Analysis - Alert Triage SOC Portal Access
Fabric Device Tuning & Reports			
Policy Violation Detection	Recon Activity	App Control (Firmware License) Traffic Log Analysis (Firmware License)	
Initial Compromise Detection	Weaponizing & Delivery	Web Filtering (UTP License Required) Spam Filtering (UTP License Required)	
Malware Detection	Exploitation & Installation	Antivirus (ATP License Required) Outbreak Prevention (License Required) Sandbox Cloud (License Required)	
Intrusion Detection		Intrusion Prevention (ATP License Required) Industrial DB (License Required) WAF (License Required)	
C&C & Botnet Detection (Compromised Host)	Command & Control	Intrusion Prevention (ATP License Required) FortiAnalyzer (IOC License Required)	
Recon Activity & Lateral Movement Detection	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
- 24×7 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
FC-10-XXXXX-841-02-DD *XXXXX is defined by the FortiGate appliance code*	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
FC-10-FG[X]VM-842-02-DD *X refers to different FG VM models - # of CPUs*	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)
FCx-10-FGVVS-843-02-DD *X refers to different FortiGate VM subscription licences*	Subscriptions license for FortiGate-VM with 360 Protection Bundle included
FC-10-XXXXX-464-02-DD *XXXXX is defined by the FortiGate appliance code*	FortiAnalyzer Cloud SOCaaS: Cloud-based Log Monitoring (PaaS), including IOC Service and FortiCloud SOCaaS