FortiCloud SOC-as-a-Service™

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

**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

**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

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

How Does It Work
Two Deployment Options

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

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

<table>
<thead>
<tr>
<th>SOC USE CASES</th>
<th>ATTACK KILL CHAIN REFERENCE</th>
<th>FORTIGATE MODULES AND LICENSE REQUIREMENTS</th>
<th>SOC DELIVERABLES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fabric Device Monitoring (Logging &amp; Security)</td>
<td>Attack Prevention &amp; Detection Across all Kill Chain Phases</td>
<td>FortiAnalyzer (Firmware License)</td>
<td>FortiGate Logging to FAZ</td>
</tr>
<tr>
<td>Fabric Device Tuning &amp; Reports</td>
<td>Recon Activity</td>
<td>App Control (Firmware License)</td>
<td>FortiGate System Security Event Monitoring</td>
</tr>
<tr>
<td>Policy Violation Detection</td>
<td>Weaponizing &amp; Delivery</td>
<td>Traffic Log Analysis (Firmware License)</td>
<td>Daily \ Weekly SOC Reports:</td>
</tr>
<tr>
<td>Initial Compromise Detection</td>
<td>Exploitation &amp; Installation</td>
<td>Web Filtering (UTP License Required)</td>
<td>- Asset Visibility</td>
</tr>
<tr>
<td>Malware Detection</td>
<td>Intrusion Detection</td>
<td>Spam Filtering (UTP License Required)</td>
<td>- Policy Violations</td>
</tr>
<tr>
<td>Intrusion Detection</td>
<td></td>
<td>Antivirus (ATP License Required)</td>
<td>- UTM Tuning</td>
</tr>
<tr>
<td>C&amp;C &amp; Botnet Detection (Compromised Host)</td>
<td>Command &amp; Control</td>
<td>Intrusion Prevention (ATP License Required)</td>
<td>Threat Detection &amp; Analysis - Alert Triage</td>
</tr>
<tr>
<td>Recon Activity &amp; Lateral Movement Detection</td>
<td>Action on Objectives</td>
<td>Intrusion Prevention (IOC License Required)</td>
<td>SOC Portal Access</td>
</tr>
</tbody>
</table>
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

- **BURNABY (CANADA)**
- **Ottawa (CANADA)**
- **Prague (CZECH)**
- **SINGAPORE**
### ORDER INFORMATION

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

<table>
<thead>
<tr>
<th>SKU</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FC-10-FG[XX]-842-02-DD</td>
<td>360 Protection for FortiGate-VM with X CPU (FMG/FAZ Cloud, FortiCloud SOCaaS, IPS, AMP, App Ctrl, Web &amp; Video Filtering, AS, Security Rating, IoT Detection, Industrial Security, SD-WAN Orchestrator, SD-WAN Cloud Monitoring, FortiConverter Svc, and ASE FortiCare)</td>
</tr>
<tr>
<td>FCx-10-FG[XX]-843-02-DD</td>
<td>Subscriptions license for FortiGate-VM with 360 Protection Bundle included</td>
</tr>
<tr>
<td>FC-10-XXXXX-464-02-DD</td>
<td>FortiAnalyzer Cloud SOCaaS: Cloud-based Log Monitoring (PaaS), including IOC Service and FortiCloud SOCaaS</td>
</tr>
</tbody>
</table>

XXX is defined by the FortiGate appliance code