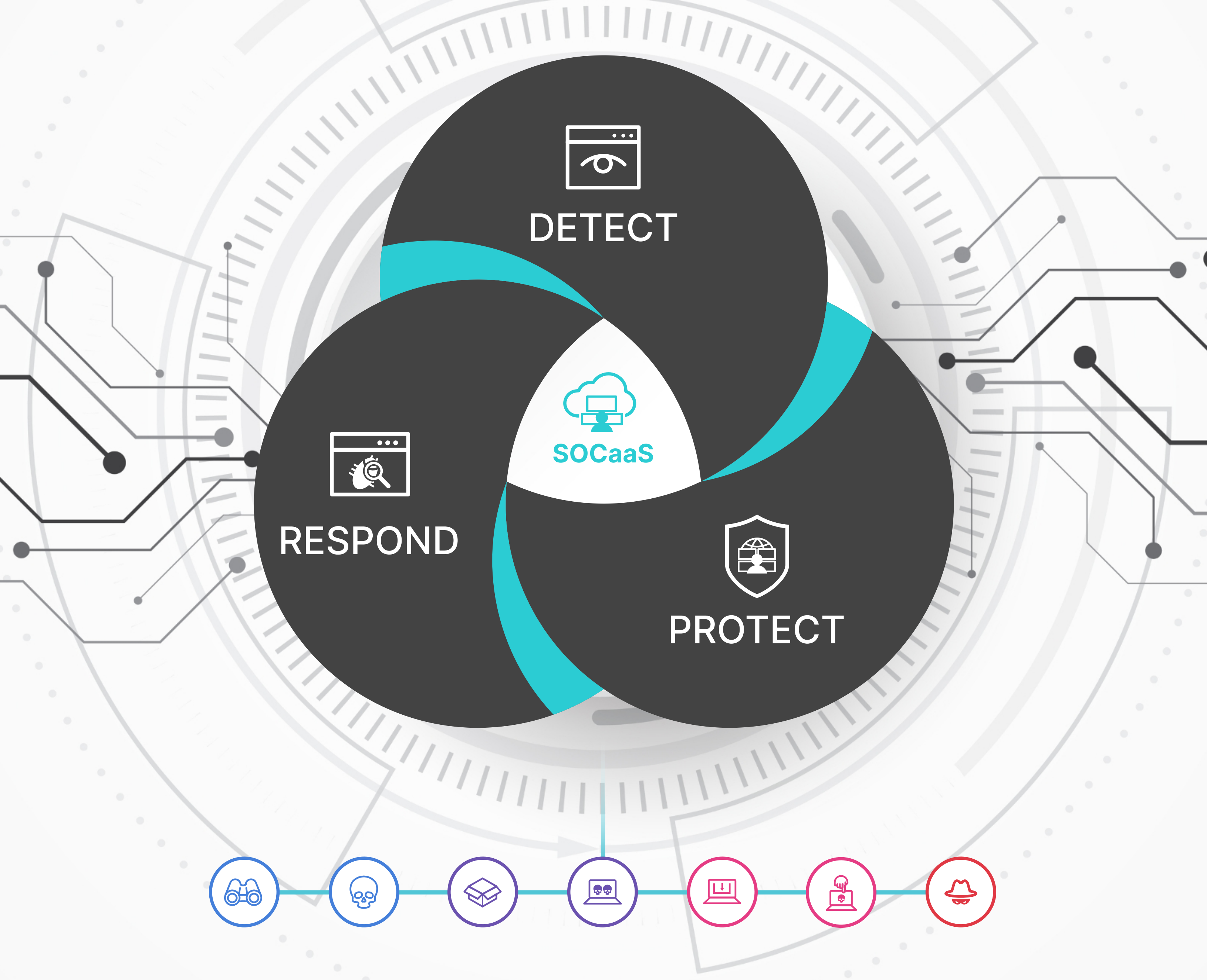
SECURITY OPERATIONS CENTER AS A SERVICE PARTNER GUIDE

Fast-Track your managed SOC offering with Fortinet SOCaaS



Q4/2023

Service at a Glance

Use Case Coverage

- Compromised Hosts
- Malware Detection
- Unauthorized Access
- Policy Violation
- Botnet / C&C
- Lateral Movement

Operations & Integration

- 24×7 Monitoring & Triage
- Cloud Service Portal
- Reports
- Quarterly Business Review
- Integrated with FortiSASE
- Integrated with Managed FortiGate Service
- Integrated with FortiClient Forensic Service
- Powered by FortiGuard & SOAR
- Driven by Security Experts

Hardening Best Practices

- Logging Best Practices
- Health Monitoring
- Security Posture Review

Information Security Management ISO 27001 Certified

SOC 2 TYPE II COMPLIANT

What is SOCaaS ?

Today many small and mid-sized organizations lack the necessary cybersecurity expertise and personnel to establish and sustain a **24/7** security operations center (SOC). As a result, they are increasingly turning to managed service providers (MSPs) and managed security service providers (MSSPs) for assistance in managing their security needs.

Fortinet Security Operations Center-as-a-Service (SOCaaS) offers a cloud-based security monitoring service that enables Fortinet Partners to efficiently and flexibly deliver a managed SOC service to their end customers in a cost-effective manner. This solution serves as a streamlined approach to rapidly deploy and operate a SOC, ensuring operational efficiency and adaptability for Fortinet's partners.

How does it work?

Subscribe

To **subscribe** to SOCaaS, simply purchase the FortiGate subscription license through a licensed reseller and register it to FortiCloud.

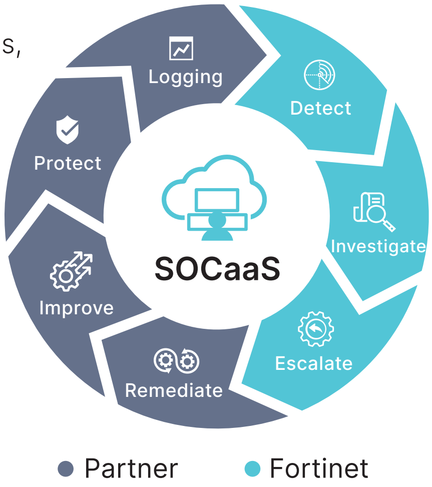
Onboard

Fortinet security experts work with you to onboard your entitled devices into the SOCaaS. During the onboarding phase, a review takes place to assess and address any security gaps that may exist. This is crucial for ensuring effective incident detection and response.

Incident Response

After the devices are successfully onboarded, the SOC team works round the clock, 24×7×365, to collect and analyze incoming logs. Their main goal is to identify any confirmed or suspicious activity. Initially, the SOC analyst triages these activities, determining their level of priority. Once confirmed, the incidents are escalated back to the customer's SOC team for further action.

When combined with Managed FortiGate Service, partners gain the valuable expertise of a trusted security advisor who can help enhance their SOC and NOC capabilities.



Use Cases

Fortinet Partners can boost their service revenue while improving operational efficiencies with SOCaaS. There are a variety ways that Fortinet Partners can take advantage of this service:

Sell-Through

Partner simply resells Fortinet SOCaaS to their clients.

Fortinet Partners can leverage SOCaaS to either sell through to grow their revenue, or they can start to immediately offer it as a new service. When combined with Fortinet Managed FortiGate Service, partners will be able to deliver a comprehensive NOC and SOC offering with a trusted network security advisor.

Managed CPE

Partner is the interface of Fortinet SOCaaS to their end customer.

Partners who have customer premises equipment (CPE) can enhance their services by offering managed CPE service. This includes valuable offerings like policy creation and optimization for Next-Generation Firewalls (NGFW), setting up Security Fabric, managing Secure SD-WAN, ZTNA, and complementing them with SOCaaS. Additionally, for partners already providing SOCaaS, they can further optimize their resources by entrusting operational tasks to Fortinet, freeing up their valuable time and expertise.

Clean Pipe Services

Partner is the interface of Fortinet SOCaaS to their end customer; and partner hosts multiple tenants on devices using VDOM.

Partners require a rapid and scalable solution to onboard Clean Pipes for the organizations whose networks they oversee. By leveraging SOCaaS, partners can efficiently expand their teams and operations, facilitating seamless scalability.

Partially Managed

Partner collects end customer logs and forward to Fortinet SOCaaS. End customer devices are registered in their own accounts.

Partners can capitalize on the benefits of SOCaaS by leveraging the expertise of Fortinet professionals to effectively manage the network security requirements of their end customers. By entrusting Fortinet experts to act on their behalf, partners can ensure comprehensive and efficient management of their customers' network security needs. This collaboration allows partners to focus on their core business while benefiting from the specialized knowledge and capabilities of Fortinet in safeguarding their customers' networks.

Fully Build Up MSSPs

MSSPs who have invested in the Fortinet technology stack, running a fully built-up managed security service offering today.

MSSPs can maximize the advantages of SOCaaS by leveraging Fortinet's infrastructure, security experts, and industry best practices to effectively scale their operations. Furthermore, MSSPs can benefit from Service portal APIs, allowing them to automate and seamlessly integrate customer onboarding and incident management into their existing workflow and service portal. This integration enhances efficiency and streamlines their overall service delivery.

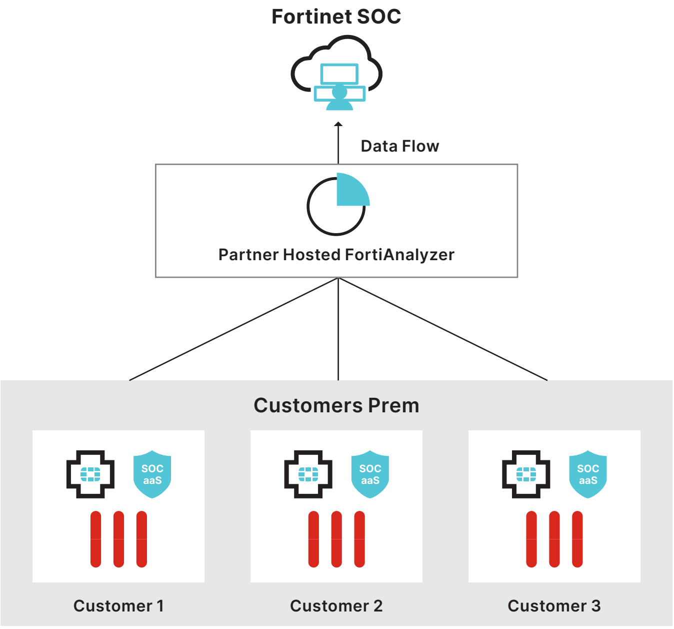
Internal Use

Partner uses Fortinet SOCaaS for their corporate assets monitoring.

Fortinet Partners can leverage SOCaaS to monitor their corporate network while simultaneously offering services like clean pipe services and web security. By doing so, they can free up valuable resources, leading to improved operational efficiency and enhanced customer satisfaction.

With Fortinet SOCaaS taking care of network security monitoring, partners can focus on delivering high-quality services to their customers, resulting in a more streamlined and effective operation.

Typical Deployment



Subscription

Subscribe to FortiGuard SOCaaS per FortiGate License.

Monitoring

- Customer FortiGate logs are sent to on-premises Partner hosted FortiAnalyzer.
- Partner hosted on-premises FortiAnalyzer forwards logs to SOCaaS.
- Alerts are sent to SOCaaS SOAR platform for Security Orchestration, Automation and Incident response.

Other deployments such as customer on-premise FortiAnalyzer or hosted FortiAnalyzer Cloud are also supported.

Service Onboarding Details

Service Onboarding Stage		Alert Escalation	Reporting	Service Requests
STAGE 1 Device Onboarding	**STAGE 2** Log Collection & Preparation	**STAGE 3** Service Commencement	Alerts & Reports	Change Requests
• Onboarding Partner customer devices and logs to Fortinet SOCaaS.	• SOCaaS collects logs for minium 3 days. • SOCaaS generates and escalates an alert to Partner SOC if no logs received in an 8hr period.	• SOCaaS starts to escalate alerts to the Partner. • SLA is measured according to the service description.	• Partner reviews escalated alerts. • Send comments to SOCaaS for additional information. • Update alert status. • Review weekly reports. • Review asset license and onboarded status.	• Partner can submit a service request. • Update service scope. • Update asset criticality. • Modify grouping. • Update escalation or point of contact. • Submit meeting request and other business service requests.

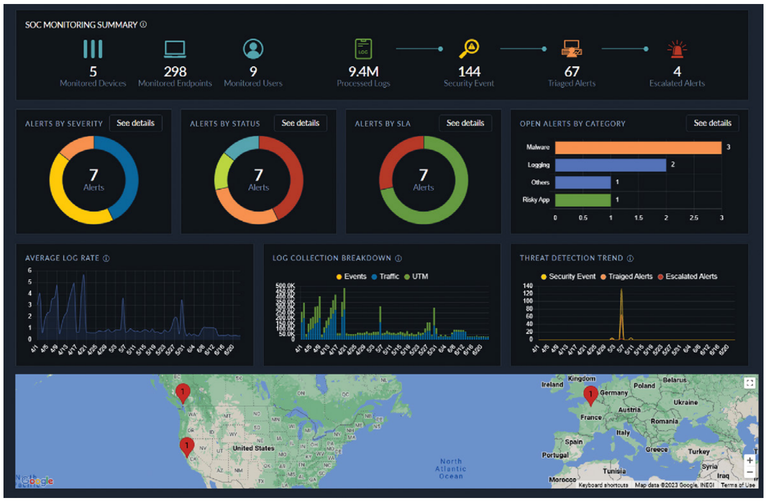
Device Registration and Alert Escalation Details

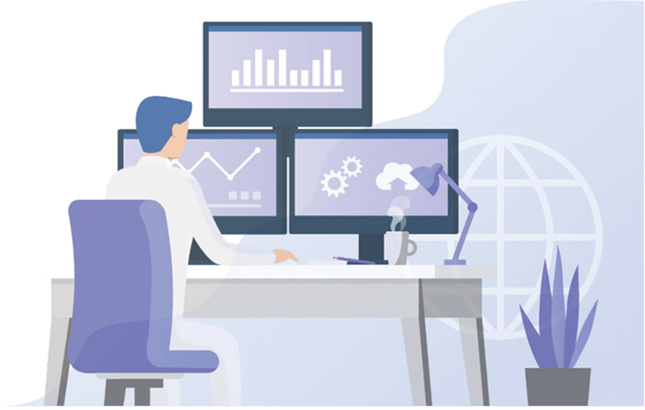
Partner Use Case	Device Registration	Onboarding	Alert Escalation	SOCaaS Portal Access	Status
Sell-through	End Customer FortiCare Account	End Customer	End Customer	End Customer	Supported
Managed CPE	Partner FortiCare Account	Partner	Partner	Partner	Supported
Clean Pipe Services	Partner FortiCare Account	Partner	Partner	Partner	Supported
Partially Managed	End Customer FortiCare Account	Partner	Partner	Partner	Supported
Internal Use	Partner FortiCare Account	Partner	Partner	Partner	Supported

How does Partner SOC integrate with SOCaaS?

Fortinet SOCaaS detections are investigated **24×7**, and qualified incidents will be escalated to the Partner SOC contact points.
Alerts can be received via Email or phone call, and all details are provided within the SOCaaS Portal:

- SOCaaS alert notification is sent to Partner through the SOC Portal.
- Partner manages alert and communications with their end customer.





Threat Focus Areas

Preparation Attacker can enter the network, perform malicious transfers, and go undetected due to mis-configuration.

Reconnaissance Attacker probes the victim's infrastructure and gains insights into vulnerable access points.

Initial Access Attacker gains initial foot hold of the victim's network through successful spear-phishing attacks.

Execution Attacker is able to execute commands or scripts on a local server.

Persistence Attacker is able to maintain a foothold on a victim vulnerable server by replacing legitimate code or adding start-up code.

Privilege Escalation Attacker is able to exploit weaknesses on the Victim's network to gain access to root or admin account.

Defense Evasion Attacker is able to hide or disguise their presence by disabling security software or encrypting sessions.

Credential Access Attacker has obtained username and passwords for the accounts associated with members of senior management.

Discovery Attacker has obtained full control of the victim's server and has gained significant information regarding infrastructure assets and privileged accounts.

Lateral Movement Attackers is able to move through the network from system to system by using legitimate credentials or installing remote access code.

Collection Attacker has gained access to local files or database stores and is gathering confidential data.

Command and Control Attacker has full remote control over a victim's asset.

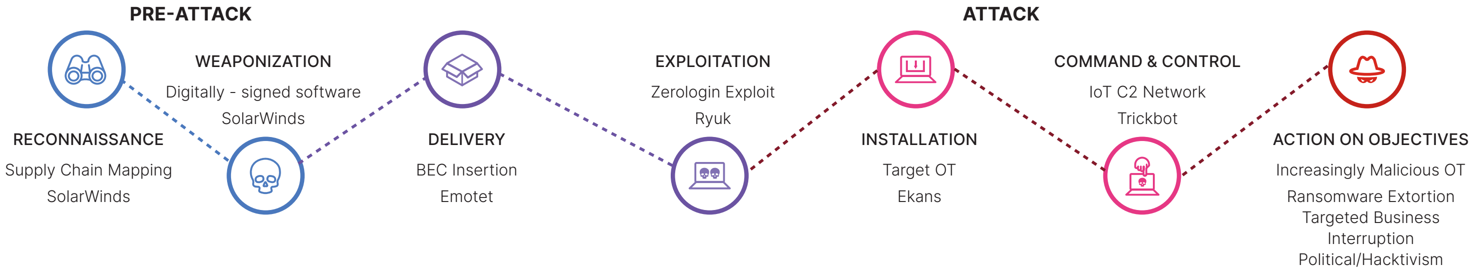
Exfiltration Attacker is using stealth techniques to remove confidential data form the victim's network.

Impact Attacker is using disruptive or stealth techniques to hide their presence and data exfiltration exploits.

Order Information

Product	Description	Managed Service SKU
	FortiGate SOCaaS Subscription	FC-10-[FortiGate Model]-464-02-DD
	Managed FortiGate Service	FC-10-[FortiGate Model]-660-02-DD
	FortiSASE + Forensics + SOCaaS	FC2-10-EMS05-676-01-DD
		FC5-10-EMS05-759-01-DD
	FortiGuard Forensics + SOCaaS	FCx-10-EMS05-537-01-DD
		FCx-10-EMS05-538-01-DD
		FCx-10-EMS05-539-01-DD

Cyber Kill Chain



PRE-ATTACK

RECONNAISSANCE
Supply Chain Mapping
SolarWinds

WEAPONIZATION
Digitally - signed software
SolarWinds

DELIVERY
BEC Insertion
Emotet

EXPLOITATION
Zerologin Exploit
Ryuk

ATTACK

INSTALLATION
Target OT
Ekans

COMMAND & CONTROL
IoT C2 Network
Trickbot

ACTION ON OBJECTIVES
Increasingly Malicious OT
Ransomware Extortion
Targeted Business
Interruption
Political/Hacktivism

SOC Use Cases for IT

SOCaaS IT Monitoring Use Cases are powered through the enablement of FortiGuard Security Services on the FortiGate. The FortiGate must have a valid FortiGuard Security Services Licenses and corresponding security profiles are used in a policy.

- The minimum requirement is the FortiGuard ATP Bundle (IPS, Anti-Malware, Application Control Protection)
- In order to take advantage of SOCaaS out-of-the box monitoring capabilities, it is highly recommended to use the FortiGuard UTP bundle (ATP + Web Filtering, IP & Botnet C&C, DNS Security).

PREPARATION

FortiGate Best Practices

Use cases which detect misconfigurations, gaps in visibility & detection, and logging problems.

Monitoring Use Case	Fabric Device	Protection Features and Log Sources	Availability
Device Logging Problems	FortiGate | FortiSASE	Not applicable	✓
Device misconfigurations (Tuning Preventive Controls)	FortiGate | FortiSASE	UTM logs	✓

RECONNAISSANCE

Reconnaissance

Use cases which detect techniques actively or passively gathering information.

MITRE ID	Monitoring Use Case	Fabric Device	Protection Features and Log Sources	Availability
T1595	Active Scanning	FortiGate | FortiSASE	Traffic, IPS	✓

SOC Use Cases for IT

DELIVERY

Initial Access

Use cases which detect compromised websites, applications, remote access, services or phishing attacks.

MITRE ID	Monitoring Use Case	Fabric Device	Protection Features and Log Sources	Availability
T1133	External Remote Services	FortiGate | FortiSASE	IPS, Traffic, VPN	✓
T1189	Drive-by Compromise	FortiGate | FortiSASE	Traffic, Web Filtering, DNS Filtering, IPS	✓
T1190	Exploit Public-Facing Application	FortiGate | FortiSASE	IPS	✓
T1566	Phishing	FortiGate + FortiSandbox	AV, Sandbox, DNS and Web Filtering	✓

EXPLOITATION

Execution

Use cases which detect when unauthorized code or software is enabled on a system.

MITRE ID	Monitoring Use Case	Fabric Device	Protection Features and Log Sources	Availability
T1072	Software Deployment Tools	FortiGate | FortiSASE	Application Control, Traffic	✓
T1059	Command and Scripting Interpreter	FortiGate | FortiSASE	Application Control, Web and DNS filtering, Traffic	✓
		FortiClient + MS Windows	MS Windows Application events	✓
T1203	Exploitation for Client Execution	FortiGate | FortiSASE	IPS	✓

SOC Use Cases for IT

EXPLOITATION

Credential Access

Use cases which detect attempts to steal credentials such as keyloggers or credential dumping attacks.

MITRE ID	Monitoring Use Case	Fabric Device	Protection Features and Log Sources	Availability
T1083	File and Directory Discovery	FortiGate | FortiSASE	IPS, Traffic	✓
T1110	Brute Force	FortiGate | FortiSASE	IPS, Traffic	✓

Discovery

Use cases which detect when attackers are attempting to gain knowledge about system and internal networks.

MITRE ID	Monitoring Use Case	Fabric Device	Protection Features and Log Sources	Availability
T1018	Remote System Discovery	FortiGate | FortiSASE	IPS, Traffic	✓
T1046	Network Service Scanning	FortiGate | FortiSASE	IPS, Traffic	✓
T1083	File and Directory Discovery	FortiGate | FortiSASE	IPS, Traffic	✓
T1087	Account Discover	FortiClient	MS Windows Application Events	✓
T1135	Network Share Discovery	FortiGate | FortiSASE	IPS, Traffic	✓

SOC Use Cases for IT

EXPLOITATION

Defense Evasion

Use cases which detect when attackers are attempting to circumvent protection controls.

MITRE ID	Monitoring Use Case	Fabric Device	Protection Features and Log Sources	Availability
T1070	Indicator Removal on Host	FortiClient + MS Windows	MS Windows Application Events	✓
T1211	Exploitation for Defense Evasion	FortiGate | FortiSASE	IPS	✓
		FortiClient	FortiShield & Anti Exploit	✓
T1212	Exploitation for Credential Access	FortiClient	MS Windows Application Events	✓
T1497	Virtualization / Sandbox Evasion	FortiClient + FortiSandbox	Malware Execution	✓
T1548	Abuse Elevation Control Mechanism	FortiClient + MS Windows	MS Windows Application Events	✓
T1562	Impair Defenses	FortiClient + MS Windows	FortiShield + MS Windows Application Events	✓

Privilege Escalation

Use cases which detect attempts to gain higher-level permissions on a system or network.

MITRE ID	Monitoring Use Case	Fabric Device	Protection Features and Log Sources	Availability
T1078	Valid Accounts	FortiClient + MS Windows	MS Windows Application Events	✓
T1548	Abuse Elevation Control Mechanism	FortiClient + MS Windows	MS Windows Application Events	✓

SOC Use Cases for IT

INSTALLATION

Lateral Movement

Use cases which detect attempts to gain unauthorized access to systems on a network from a presumably trusted source on the same network.

MITRE ID	Monitoring Use Case	Fabric Device	Protection Features and Log Sources	Availability
T1021	Remote Services	FortiGate | FortiSASE	Traffic	✓
		FortiClient + MS Windows	MS Windows Application Events	✓
T1072	Software Deployment Tools	FortiGate | FortiSASE	Application Control, Traffic	✓
T1210	Exploitation of Remote Services	FortiGate | FortiSASE	IPS	✓
T1534	Internal Spearphishing	FortiGate + FortiSandbox	Anti-Virus, Web Filtering	✓
T1570	Lateral Tool Transfer	FortiGate + FortiSandbox	IPS, Anti-Virus, Traffic	✓

Persistence

Use cases which detect attempts to keep access to systems across restarts, changed credentials, and other interruptions that could cut off adversary access.

MITRE ID	Monitoring Use Case	Fabric Device	Protection Features and Log Sources	Availability
T1176	Browser Extensions	FortiGate | FortiSASE	Traffic	✓
T1133	External Remote Services	FortiGate | FortiSASE	IPS, Traffic, VPN	✓
T1136	Create Account	FortiClient + MS Windows	MS Windows Application Events	✓

SOC Use Cases for IT

COMMAND & CONTROL

Collection

Use cases which detect techniques used by attackers to gather information for the purpose of exfiltration.

MITRE ID	Monitoring Use Case	Fabric Device	Protection Features and Log Sources	Availability
T1602	Data from Configuration Repository	FortiGate | FortiSASE	Traffic, IPS	✓

Command & Control

Use cases which detect suspicious traffic originating from internal system to external destinations.

MITRE ID	Monitoring Use Case	Fabric Device	Protection Features and Log Sources	Availability
T1001	Data Obfuscation	FortiGate | FortiSASE	IPS, Web and DNS Filtering, Traffic	✓
T1008	Fallback Channels	FortiGate | FortiSASE	IPS, Web and DNS Filtering, Traffic	✓
T1071	Application Layer Protocol	FortiGate | FortiSASE	IPS, Web and DNS Filtering, Traffic	✓
T1092	Communication Through Removable Media	FortiClient	USB Device Control	✓
T1095	Non-Application Layer Protocol	FortiGate | FortiSASE	IPS, Web and DNS Filtering, Traffic	✓
T1104	Multi-Stage Channels	FortiGate | FortiSASE	IPS, Web and DNS Filtering, Traffic	✓
T1105	Ingress Tool Transfer	FortiGate + FortiSandbox	IPS, AV, Traffic	✓
		FortiClient + FortiSandbox	Anti-Virus	✓
T1132	Data Encoding	FortiGate | FortiSASE	IPS, Web and DNS Filtering, Traffic	✓
		FortiClient + MS Windows	MS Windows Application Events	✓
T1219	Remote Access Software	FortiGate | FortiSASE	Traffic & Application Control	✓
T1568	Dynamic Resolution	FortiGate | FortiSASE	IPS, Web and DNS Filtering, Traffic	✓
T1571	Non-Standard Port	FortiGate | FortiSASE	IPS, Web and DNS Filtering, Traffic	✓
T1573	Encrypted Channel	FortiGate | FortiSASE	IPS, Web and DNS Filtering, Traffic	✓

SOC Use Cases for IT

ACTIONS ON OBJECTS

Exfiltration

Use cases which detect techniques that adversaries may use to steal data and avoiding detection while removing it.

MITRE ID	Monitoring Use Case	Fabric Device	Protection Features and Log Sources	Availability
T1041	Exfiltration Over C2 Channel	FortiGate | FortiSASE	IPS, Web and DNS Filtering, Traffic	✓
T1048	Exfiltration Over Alternative Protocol	FortiGate | FortiSASE	Traffic	✓
T1052	Exfiltration Over Physical Medium	FortiClient	USB Device Control	✓
T1537	Transfer Data to Cloud Account	FortiGate | FortiSASE	Traffic, Application Control, Web Filtering	✓
T1567	Exfiltration Over Web Service	FortiGate | FortiSASE	Traffic, Application Control, Web Filtering	✓
		FortiClient	Web Filter	✓

Impact

Use cases which detect techniques that adversaries may use to disrupt availability or compromise integrity by manipulating business and operational processes.

MITRE ID	Monitoring Use Case	Fabric Device	Protection Features and Log Sources	Availability
T1486	Data Encrypted for Impact	FortiClient	Ransonware Protection	✓
T1498	Network Denial of Service	FortiGate | FortiSASE	IPS	✓

SOC Use Cases for OT

The FortiGuard Operational Technology (OT) Security Service includes both application control and Intrusion Prevention Signatures (IPS) for industrial applications and protocols. The OT signatures are only updated if the FortiGate has a valid FortiGuard OT Security license. IPS and application security profiles should also be used on policies. In addition to OT Monitoring Use Cases, IT Use Cases are also applicable to OT networks.

DELIVERY

Initial Access

Use cases which detect compromised websites, applications, remote access, services or phishing attacks.

MITRE ID	Monitoring Use Case	Fabric Device	Protection Features and Log Sources	Availability
T0819	Exploit Public-Facing Applications	FortiGate | FortiSASE	IPS (OT Signatures)	✓
T0866	Exploitation of Remote Service	FortiGate | FortiSASE	IPS (OT Signatures)	✓
T0886	Remote Services	FortiGate | FortiSASE	Traffic and Application Control	✓

EXPLOITATION

Discovery

Use cases which detect when attackers are attempting to gain knowledge about system and internal networks.

MITRE ID	Monitoring Use Case	Fabric Device	Protection Features and Log Sources	Availability
T0846	Remote System Discovery	FortiGate | FortiSASE	Traffic and Application Control	✓

SOC Use Cases for OT

INSTALLATION

Lateral Movement

Use cases which detect attempts to gain unauthorized access to systems on a network from a presumably trusted source on the same network.

MITRE ID	Monitoring Use Case	Fabric Device	Protection Features and Log Sources	Availability
T0866	Exploitation of Remote Service	FortiGate | FortiSASE	IPS (OT Signatures)	✓
T0891	Hardcoded Credentials	FortiGate | FortiSASE	Traffic and Webfilter	✓
T0886	Remote Services	FortiGate | FortiSASE	Traffic and Application Control	✓

Persistence

Use cases which detect attempts to keep access to systems across restarts, changed credentials, and other interruptions that could cut off adversary access.

MITRE ID	Monitoring Use Case	Fabric Device	Protection Features and Log Sources	Availability
T0891	Hardcoded Credentials	FortiGate | FortiSASE	Traffic and Webfilter	✓

ACTIONS ON OBJECTS

Inhibit Response Function

Use cases which detect techniques that adversaries may use to alter security controls in place.

MITRE ID	Monitoring Use Case	Fabric Device	Protection Features and Log Sources	Availability
T0814	Denial of Service	FortiGate | FortiSASE	IPS DOS Policy	✓

The Fortinet Security Fabric

The Fortinet Security Fabric is at the heart of the Fortinet security strategy. It is a platform organically built around a common operating system and management framework to enable broad visibility, seamless integration and interoperability between critical security elements, and granular control and automation.

Broad

visibility and protection of the entire digital attack surface to better manage risk.

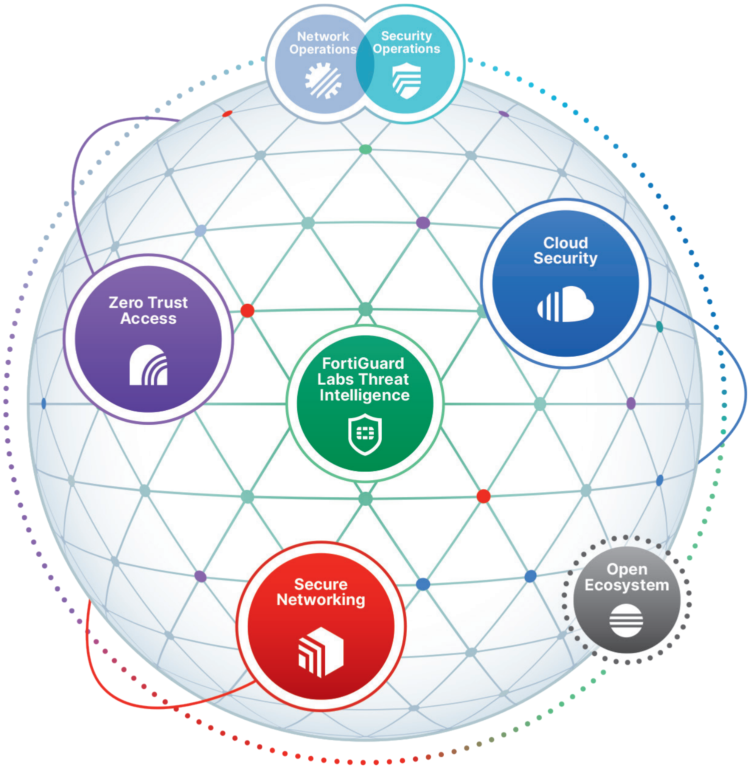
Integrated

solution that reduces management complexity and shares threat intelligence.

Automated

self-healing networks with AI-driven security for fast and efficient operations.

Learn more at www.fortinet.com/corporate/about-us



Broad Portfolio of Solutions to Protect Your Digital Attack Surface

Zero Trust Access

- ZTNA Agent
- Authentication
- MFA/Token
- SASE

Secure Networking

- Network Firewall
- SD-WAN
- SD-Branch
- Web Proxy
- Wi-Fi
- Switching
- 5G/LTE
- Network Access Control
- And More...

Cloud Security

- Cloud-Native Protection
- DevSecOps
- Cloud Firewall
- SD-WAN for Multi-cloud
- WAF
- Email Security
- ADC/GSLB
- Anti-DDoS
- CASB

Network Operations

- Network Management
- Network Orchestration
- Network Monitoring
- Cloud Management
- Digital Experienc Monitoring

Security Operations

- Endpoint (EDR XDR)
- Automation: SIEM/SOAR
- Managed SOC & MDR
- DRPS, EASM
- Deception

Open Ecosystem

- Fabric Connectors
- Fabric API
- Fabric DevOps
- Extended Ecosystem
- 490+ Open Ecosystem
- Integrations

Visit Fortinet.com for more details.

November 29, 2023