ORDERING GUIDE

Managed Security Services

Product Offerings

Fortinet offers managed Security Operations services to complement and enhance Enterprise security operations center (SOC) capabilities through integration, technology automation, and security experts. This includes:

- **FortiCloud SOCaaS**: 24×7 log-based monitoring, triage, and incident escalation service
- **Managed FortiClient**: cloud-based endpoint management and provisioning includes setup of Zero Trust Network Access for secure remote application access while reducing attack surface, VPN for secure remote work, real-time vulnerability detection, and autopatching for further reduced attack surface, endpoint security for protection against ransomware and advanced threats, web security to protect against malicious and phishing sites, and Fortinet Security Fabric integration for end-to-end visibility and control.
  - **Managed FortiClient plus Forensics Analysis Service**: above plus on-demand escalation to a specialized forensics team to perform deeper investigation of requested endpoints. Forensics Analysis Service is coming in Q2. Check the pricelist for availability.
- **Managed EDR**: 24×7 experts to monitor, hunt, analyze, and respond to malicious activity detected from your endpoints.
  - **Managed XDR**: above plus extended detection and response capabilities of the FortiXDR platform

	LOG-BASED	ENDPOINT ATTACK SURFACE		ENDPOINT SECURITY	
	SOC-AS-A-SERVICE	MANAGED FORTICLIENT	MANAGED FORTICLIENT + FORENSICS (COMING SOON)	MANAGED EDR	MANAGED EDR + XDR
Security Event Coverage	Log-based analysis and incident response	Endpoint remote access and attack surface management		Endpoint behavior and AI-based security	
Incident Management	24×7 monitoring, triage, and escalation by dedicated analysts	Automated incident detection and escalation		24×7 monitoring, triage, and escalation by dedicated analysts	
Onboarding	On-demand via self-service portal	On-demand via self-service portal		On-demand	
Configuration and Tuning	System hardening, use case-based logging and policy tuning	Best practice consultation, use case-based policy configuration, and Fortinet Security Fabric integration included		Best practice consultation, use case-based policy configuration, and Fortinet Security Fabric integration included	
SOC Integration Points	Threat intelligence and IoC ingestion plus out-of-the-box incident detection, investigation, and notifications	Endpoint vulnerability and EPP monitoring and reporting	Endpoint vulnerability and EPP monitoring and reporting, plus on-demand endpoint forensic analysis	Asset discovery and protection, and behavior-based analysis and response	Asset discovery and protection, and behavior-based analysis and response, including advanced cross-Fortinet Security Fabric correlation and automated response

MANAGED LOG-BASED DETECTION AND RESPONSE

FortiCloud SOCaaS connects the Security Fabric eco-system to a central, automated, managed platform that monitors logs, detects events, engages security experts, and finally escalates critical incidents to customers. This service is delivered by a global team of 24×7 incident response analysts, leveraging real-time security expertise and a shared SOAR platform to integate seamlessly with cusotmer SOC operations.

The following table highlights the key components of this service (refer to the datasheet for full details):

	FORTICLOUD SOCAAS
Device Hardening Best Practices	
Logging Best Practices	✓
Health Monitoring	✓
Tuning Recommendations	✓
Security Rating	✓
Threat Use Cases	
FortiGate Network Security	✓
Endpoint Security*	✓
SOC Operations and Integration	
FortiGuard Global Threat Intelligence	✓
IOC Ingestion and Search	✓
Alert Triage	✓
24×7 Notification	✓
Self-service Portal	✓
SOAR Platform	✓
Log Storage	3 months, add-on long-term storage
Additional Services	
24×7 support	Included
Quarterly Business Review	Included
Alert Detection and Escalation Tuning	Included
Reports	Included

* FortiClient use cases have already been added to Endpoint Security use cases for detection. If a customer has already been onboarded via an on-premise FortiAnalyzer, SOC can take all supported Security Fabric logs, including FortiEDR logs. More use cases are constantly being added.

ORDER INFORMATION

Note that SOCaaS is a simple add-on to any FortiGate model (hardware or virtual). Logs may be forwarded directly to SOCaaS, but are typically forwarded from the attached FortiAnalyzer (cloud, virtual or hardware).

SOLUTION BUNDLE		FORTICLOUD SOCAAS
FortiAnalyzer SOCaaS Subscriptions	**FortiAnalyzer Cloud SOCaaS**	FC-10–[FortiGate Model]-464-02-DD

SEE ALSO

For more information about log collection, reporting and compliance, refer to the FortiAnalyzer Ordering Guide.

MANAGED ENDPOINTS

Managed FortiClient enables organizations to rapidly adopt a managed remote user/device deployment, including Remote Access (IPsec or SSL VPN or ZTNA) for work from anywhere, plus vulnerability management with autopatching to reduce attack surface, web security against malicious and phishing attacks, and endpoint protection against ransomware and advanced threats. After onboarding, this service provides full access to the Endpoint Management System (SaaS platform) for granular controls to NOC/SOC teams.

Managed FortiClient + Forensic Analysis adds access to the dedicated FortiGuard Forensics team, enabling customers to isolate and submit suspicious endpionts for detailed scanning and analysis. Forensics Analysis Service is coming in Q2. Check the pricelist for availability.

The following table highlights the key components of these services (refer to the datasheet for full details):

	MANAGED VULNERABILITY AND EPP	MANAGED VULNERABILITY AND EPP + FORENSICS
Device Hardening Best Practices		
Logging Best Practices	✓	✓
Tuning Recommendations	✓	✓
Threat Use Cases		
Endpoint Security	Pre-attack	Pre- and post-attack
Managed Endpoint		
Endpoint Onboarding	✓	✓
Initial Provisioning	✓	✓
Security Fabric Setup/Integration	✓	✓
Vulnerability Monitoring	✓	✓
Endpoint Security Monitoring	✓	✓
Automated Scan of All Suspicious Endpoints		✓
Forensics Triage and Investigation		✓
Incident Readiness		
Post or Active Breach Investigation		✓
Compromised Device/User Identification		✓
Containment and Remediation (Strategy and Execution)		✓
Patient 0 Identification		✓
Exfiltration Identification		✓
Future Recommendations and Final Report		✓
Additional Services		
Self-service Portal	✓	✓
24×7 Support	Included	Included

ORDER INFORMATION

ORDERING OPTIONS		MANAGED VULNERABILITY AND EPP	MANAGED VULNERABILITY AND EPP + FORENSICS
Per-Endpoint	**25-pack**	FC1-10-EMS05-485-01-DD	FC1-10-EMS05-539-01-DD
	500-pack	FC2-10-EMS05-485-01-DD	FC2-10-EMS05-539-01-DD
	2,000-pack	FC3-10-EMS05-485-01-DD	FC3-10-EMS05-539-01-DD
	10,000-pack	FC4-10-EMS05-485-01-DD	FC4-10-EMS05-539-01-DD

MANAGED ENDPOINT BEHAVIOR AND RESPONSE

Managed EDR leverages all telemetry data from the FortiEDR platform, which our dedicated team of security experts use to monitor, hunt, analyze, and respond to malicious activity on your endpoints 24×7. In addition, the team provides guidance and next steps to incident responders and IT administrators as needed.

Managed XDR expands your attack surface coverage, leveraging extended context inputs to correlate incidents across a wider domain. The Managed XDR service also provides SOAR playbooks and guidance for integration with customer SOC workflows.

The following table highlights the key components of these services (refer to the datasheet for full details):

	MANAGED EDR	MANAGED XDR
Policy Tuning and Review	✓	✓
Environment Tuning	✓	✓
Daily Health Checks	✓	✓
Customized Onboarding	✓	✓
Guided Recommendations and Best Practices	✓	✓
Threat Use Cases		
Endpoint Security	Pre- and post-attack	Pre- and post-attack
SOC Operations and Integration		
FortiGuard Global Threat Intelligence	✓	✓
24×7 Threat Detection and Analysis	✓	✓
Notifications with Human Context	✓	✓
Containment and Remediation	✓	✓
Forensic Escalation Requests	✓	✓
Quarterly Situational Awareness Reports	✓	✓
Advanced Forensics Investigation	✓	✓
Threat Hunting - Emerging Threats	✓	✓
Quarterly Threat Briefings (by Request)	✓	✓
SOAR Playbooks	✓	✓
Extended Threat Analysis		✓

ORDER INFORMATION

SOLUTION BUNDLE		MANAGED EDR	MANAGED XDR
Per-Endpoint	**25-pack**	FC1-10-FEDR1-349-01-DD	FC1-10-FEDR1-396-01-DD
	500-pack	FC2-10-FEDR1-349-01-DD	FC2-10-FEDR1-396-01-DD
	2,000-pack	FC3-10-FEDR1-349-01-DD	FC3-10-FEDR1-396-01-DD
	10,000-pack	FC4-10-FEDR1-349-01-DD	FC4-10-FEDR1-396-01-DD

FORTINET

www.fortinet.com

SOC-OG-R4-20221202