ORDERING GUIDE

SOC Augmentation 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 service includes:

INCIDENT DETECTION

FortiGuard SOC-as-a-Serice (SOCaaS)

- 24×7 cloud-based event monitoring, alert triage, and threat escalation by Fortinet SOC experts
- Includes support of MITRE mapped detection and powered by FortiGuard and AI/ML engines
- Customer interface via cloud service portal with quarterly reports and business reviews

Managed EDR/XDR

- 24×7 cloud-managed service delivered by experienced analysts and FortiEDR experts
- Includes monitoring, threat hunting, analysis, and response to endpoint threats
- Integrated with FortiXDR and FortiAnalyzer for automated response capabilities

INCIDENT RESPONSE

Managed FortiClient Forensics

- Built-in forensics components enable FortiGuard experts to investigate suspicious endpoints, retrieve forensics evidence and give recommendations for further remediation
- Includes dedicated cloud portal to interact with FortiGuard experts and discuss the results

Incident Response (IR) Service

- Personalized assistance for cyber incident investigation, analysis, containment, forensics, and remediation
- Can be delivered on-site or remotely by the FortiGuard IR experts

FORTIGUARD SOC-AS-A-SERVICE

FortiGuard SOCaaS connects the Security Fabric ecosystem 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).

	FORTIGUARD 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	three months, add-on long-term storage
Integration	
FortiGate / FortiWiFi	✓
FortiSASE	✓
FortiClient	✓
FortiClient Forensics	✓
Additional Services	
24×7 support	✓
Quarterly Business Review	✓
Alert Detection and Escalation Tuning	✓
Reports	✓

ORDER INFORMATION

Note that FortiGuard 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).

PRODUCT	SOCAAS SUBSCRIPTION	DESCRIPTION
FortiGate	FC-10-[FortiGate Model]-464-02-DD	SOCaaS: 24×7 cloud-based monitoring, incident triage and SOC escalation service.
FortiWiFi	FC-10-[FortiWiFi Model]-464-02-DD	SOCaaS: 24×7 cloud-based monitoring, incident triage and SOC escalation service.
FortiClient	FCx-10-EMS04-537-01-DD FCx-10-EMS05-537-01-DD	FortiClient VPN/ZTNA Agent Subscriptions plus FortiGuard Forensics with FortiCare Premium
	FCx-10-EMS04-538-01-DD FCx-10-EMS05-538-01-DD	FortiClient VPN/ZTNA Agent and EPP/APT Subscriptions plus FortiGuard Forensics with FortiCare Premium
	FCx-10-EMS05-539-01-DD	Managed FortiClient VPN/ZTNA Agent and EPP/APT Subscriptions plus FortiGuard Forensics with FortiCare Premium
FortiSASE	FC2-10-EMS05-676-01-DD	FortiSASE Advanced Subscription including FortiGuard Forensics
	FC5-10-EMS05-759-01-DD	FortiSASE Comprehensive Subscription including FortiGuard Forensics

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 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	QUANTITY	MANAGED EDR	MANAGED XDR
Per-Endpoint	25-pack	FC1-10-FEDR1-392-01-DD	FC1-10-FEDR1-596-01-DD
	500-pack	FC2-10-FEDR1-392-01-DD	FC2-10-FEDR1-596-01-DD
	2000-pack	FC3-10-FEDR1-392-01-DD	FC3-10-FEDR1-596-01-DD
	10 000-pack	FC4-10-FEDR1-392-01-DD	FC4-10-FEDR1-596-01-DD

For more MDR options, please see the FEDR Price List.

MANAGED ENDPOINT FORENSICS

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.

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	✓	✓
SOCaaS Integration		✓

ORDER INFORMATION

ORDERING OPTIONS	QUANTITY	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
	2000-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

FORTIGUARD INCIDENT RESPONSE SERVICE

FortiGuard Incident Response Service combines proactive security services with incident response (IR) support. It assesses, tests, and strengthens your incident response plan before a security incident occurs. In the event of an unexpected cyber incident, it provides analysis, containment, forensic investigation, and remediation support.

The following table highlights the key components of the services.

SERVICE CATEGORY	SERVICE	CONSUMPTION	HOURS
Digital Forensics and Incident Response	Custom IR Services	SOW or Subscription	Scoping Required
Incident Response Playbook Development	Custom Playbook Development	SOW or Subscription	Scoping Required 20+
Penetration Testing	Remote penetration test of one web application or one mobile application	SOW or Subscription	n/a
	Remote penetration test of up to 128 IP addresses	SOW or Subscription	n/a
	Remote penetration test of up to 256 IP addresses	SOW or Subscription	n/a
	Remote penetration test of up to 512 IP addresses	SOW or Subscription	n/a
	Remote penetration test of up to 1024 IP addresses	SOW or Subscription	n/a
Vulernability Assessment	Remote vulnerability assessment of one web application or one mobile application	SOW or Subscription	n/a
	Remote vulnerability assessment of up to 128 IP addresses	SOW or Subscription	n/a
	Remote vulnerability assessment of up to 256 IP addresses	SOW or Subscription	n/a
	Remote vulnerability assessment of up to 512 IP addresses	SOW or Subscription	n/a
	Remote vulnerability assessment of up to 1024 IP addresses	SOW or Subscription	n/a
Assessments	Incident Response Readiness Assessment	SOW or Subscription	52
	Ransomware Readiness Assessment	SOW or Subscription	40
	SOC Assessment	SOW or Subscription	80
	Active Directory Security Assessment	SOW or Subscription	Scoping Required 40+
	Compromise Assessment	SOW or Subscription	Scoping Required 100-1000
Tabletop Exercises	Custom Tabletop Exercise	SOW or Subscription	Scoping Required 30+
Incident Response Plan Development	Custom Incident Response Plan	SOW or Subscription	Scoping Required 40+

ORDER INFORMATION

SERVICE	SKU
Custom Incident Reponse Services	FP-10-IR-FRNSCS
Remote Penetration Test	FP-10-PT0XX-000-00-00
Remote Vulnerability Assessment	FP-10-PT0XX-000-00-00
Assessments, Custom Tabletop Exercise, Custom Playbook Development, Custom Incident Response Plan	FP-10-IR-PROACTIVE
FortiGuard Incident Readiness Subscription Service	FP-10-IR001-709-02-12
Ten Service Points for Readiness Subscription Services	LIC-IR-10

FORTINET

www.fortinet.com