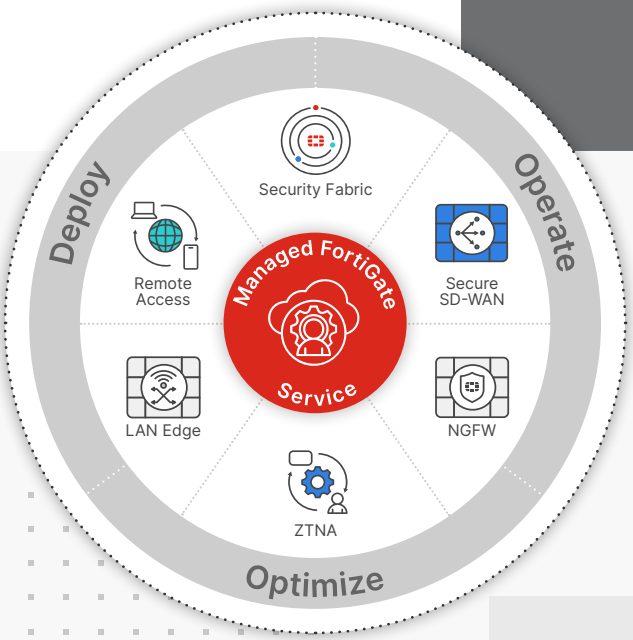
Managed FortiGate Service ™



Highlights

- **Deploy Quickly** according to Fortinet best practices.
- **Operate Securely** via Structured, ITIL™ aligned change management process.
- **Optimize Continuously** to enhance your security posture and meet evolving regulations.
- **Scale Effectively** across diverse environments and security scenarios.

Securely Accelerate Your Digital Journey with Vendor Expertise

Discover peace of mind with **Managed FortiGate Service (MFGS)** - your trusted, cloud-based network security solution, available around the clock. MFGS enhances your security experience by making deployments faster, daily operations simpler, and your overall protection stronger.

Whether you're a partner or a customer, MFGS is designed to help scaling your operations efficiently without the usual headaches. You can focus on your core business, knowing our friendly team of Fortinet experts is always here to:

- **Deploy your FortiGate devices quickly**, so you're up and running in no time.
- **Keep your network safe** with proven, structured processes based on ITIL and Fortinet's best practices.
- **Maintain compliance with ease**.

Key Features

Vulnerability Management

- Easily identify FortiOS versions impacted by PSIRT vulnerabilities within a detailed report.
- Automatically trigger patching for vulnerabilities with a severity rating of medium or higher.

Security Posture Assessment

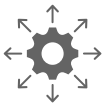
Audit onboarded FortiGates against Fortinet security guidelines to uncover misconfigurations and security gaps.

Incident Containment

Benefit of a comprehensive incident management solution by combining MFGS with SOCaaS.

Firmware Upgrade

Let MFGS experts handle your firmware upgrades to maximize effectiveness and minimize risk.



Deploy

- Ensure FortiGates, FortiAPs, FortiSwitches and FortiExtenders are quickly and correctly deployed, configured to best practices, and aligned with business requirements.



Operate

- Continuous management of firewall rules, threat prevention settings, and security posture to block evolving threats.



Optimize

- Easily identify and remediate FortiGate devices affected by PSIRT Vulnerabilities
- Audit onboarded FortiGates against Fortinet security guidelines to enhance your overall security posture.
- Rapidly contain escalated SOCaaS alerts to minimize response time
- Leverage Fortinet experts to assess and execute firmware upgrades using risk-reducing best practices.

ACTIVITY	AVAILABILITY
Service Onboarding	
MSSP (Service Providers who manage FortiGate devices for clients)	✓
Regular Customer (Customers who manage their FortiGate devices)	✓
Deploy	
NGFW	✓
Security Fabric	✓
Secure SD-WAN	✓
Remote Access	✓
LAN Edge	✓
Operate	
ITIL Framework	✓
Separation of roles for change initiator/approver	✓
Four Eyes Principle	✓
Revision History	✓
Change Schedule Calendar	✓
Modification/Deletion of existing config objects	✓
Addition of new config objects	In accordance with the service catalog
Device Monitoring	*
Optimize	
FortiGuard SOCaaS Incident containment	Requires FortiGuard SOCaaS subscription
Vulnerability Management	✓
Security Posture Assessment	Requires attack surface security service subscription
Firmware Upgrade	✓
Operations and Integrations	
Dedicated Service Portal	✓
Integration with FortiCloud	✓
Access to Central Management	✓

* Real-time device monitoring available via the Service Portal. Proactive service requests are automatically generated if the management tunnel between FortiManager Cloud and FortiGate remains down for 10 minutes or longer.

Service Catalog Use Cases

CATEGORY	TITLE	JOURNEY
 NGFW	Networking Fundamentals	Recommended
	System Hardening	Recommended
	High Availability	Optional
	Application Control	Recommended
	DoS Policy	Recommended
	Intrusion Prevention	Recommended
	Email Filter	Recommended
	DNS Filter	Recommended
	Web Filter	Recommended
	Logging Best Practices	Recommended
	Dual Internet Connections	Optional
	Traffic Shaping	Optional
	Antivirus	Recommended
	Automated Certificate Management	Optional
	Server Load Balancing	Optional
	Network Segmentation with VDOMs	Optional
	Policy Based Routing	Optional
	Static Virtual IP	Optional
	Local-inPolicies	Optional
	FortiGate and LAN Edge monitoring via SNMP	Optional
	FortiGate Local Admin User	Recommended
	Generating daily security report on a FortiGate	Optional
 Security Fabric	Automation Stitches	Recommended
	Automated endpoint quarantine using Forticlient EMS	Optional
 LAN Edge	FortiAP Deployment	Optional
	FortiSwitch Deployment	Optional
	Deploy FortiExtender as WAN Extension	Optional
	Guest WiFi- Captive Portal	Optional
 Secure SD-WAN	Static Application Steering	Recommended
	Dynamic Application Steering	Recommended
	Direct Internet Access	Recommended
	Single Datacenter	Optional
	Multiple Datacenters	Optional
 Remote Access	Dialup IPSec VPN Server with FortiClient	Optional
	Site-to-site IPSec VPN	Optional
	Redundant site-to-site IPSec VPN	Optional
	SSL-VPN tunnel	Optional
	SSL-VPN to IPSec VPN Migration	Optional
 ZTNA	HTTPS Access Proxy	Optional
	TCP Forwarding Access proxy	Optional

For a detailed description of use cases, please visit https://docs.fortinet.com/product/managed-fortigate-service

Simplified Service Commencement



Purchase a Managed FortiGate Service subscription license.

Register your contract code in your FortiCloud account, then associate it to the FortiGate unit you want to include in the service.

Access the Managed FortiGate Service portal and submit your onboarding request using the wizard.

Benefits

Augmented Operations
Rely on people, processes and tools available 24/7.

Reduced Costs
Optimized service cost with predictable forecast.

Peace of Mind
Focus on your core business needs.

Certified Security
SOC2 Type II & ISO27001 certified

24×7 Global Coverage
- North America
- EMEA
- APAC

Strategic Data Centers Locations
- Burnaby, Canada
- Dallas, USA
- Frankfurt, Germany
- Tokyo, Japan

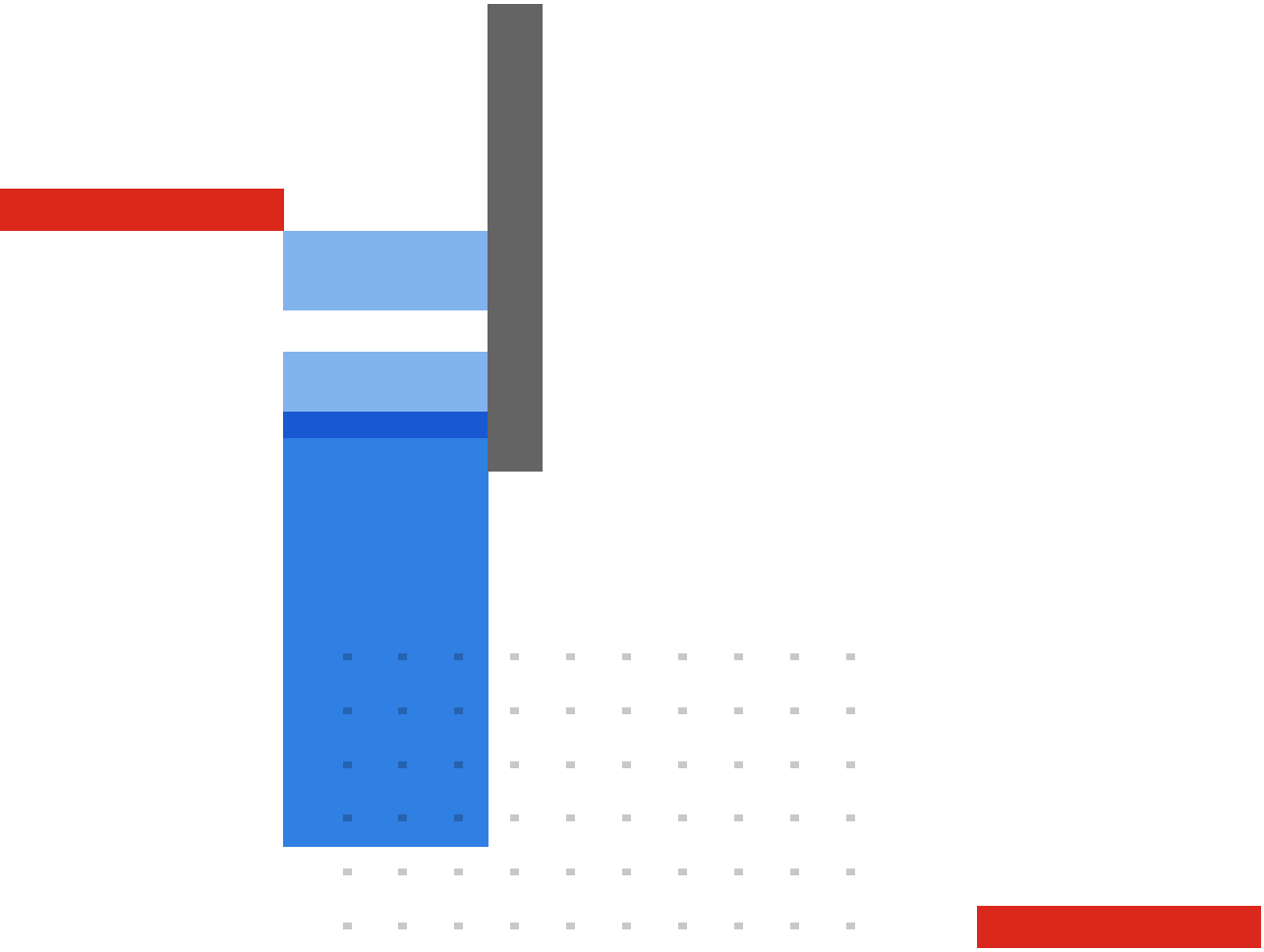
Ordering Information

Service	SKU	Description
Managed FortiGate Service	FC-10-[FortiGate Model Code]- 660-02-DD	Managed FortiGate service, available 24×7, with Fortinet NOC experts performing device setup, network, and policy change management

Visit https://www.fortinet.com/resources/ordering-guides for related ordering guides.

Fortinet Corporate Social Responsibility Policy

Fortinet is committed to driving progress and sustainability for all through cybersecurity, with respect for human rights and ethical business practices, making possible a digital world you can always trust. You represent and warrant to Fortinet that you will not use Fortinet's products and services to engage in, or support in any way, violations or abuses of human rights, including those involving illegal censorship, surveillance, detention, or excessive use of force. Users of Fortinet products are required to comply with the Fortinet EULA and report any suspected violations of the EULA via the procedures outlined in the Fortinet Whistleblower Policy.



FORTINET

www.fortinet.com

Copyright © 2025 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's SVP Legal and above, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

October 10, 2025

MFGS-DAT-R07-20251009