SERVICE BRIEF

FortiGuard AI-Powered Security Services Bundles for Fortinet Hybrid Mesh Firewalls

Comprehensive, Flexible, and Scalable Protection

Executive Overview

As the attack surface grows across network, cloud, endpoint, and OT environments, organizations need security solutions that can adapt, scale, and stay ahead of increasingly sophisticated threats—especially those driven by AI. FortiGuard AI-Powered Security Services Bundles provide always-on, real-time protection by combining artificial intelligence (AI), automation, and threat intelligence with deep integration across the Fortinet Security Fabric.

Optimized for FortiGate Hybrid Mesh Firewalls (HMFs), these curated service bundles help security and network teams protect their environments with layered, adaptive defense, whether at the branch, campus, data center, or in the cloud.

FortiGuard AI-Powered Security Services offers a layered defense for FortiGate HMFs and HMF-based solutions. These AI-native services are developed and continuously enriched with real-time threat intelligence from FortiGuard Labs, Fortinet's elite threat research and AI development team.

Protect against Known and Unknown Threats

As security teams work to support business objectives, the attack surface continues to expand. At the same time, the sophistication and volume of today's AI-driven cyberthreats continue to challenge the ability of even the most resourced and capable network operations center (NOC) and security operations center (SOC) teams to keep up.

FortiGuard AI-Powered Security Services delivers a powerful combination of real-time AI-powered threat intelligence integrated with always-on security capabilities to protect organizations against known, unknown, zero-day, and emerging AI-based threats. The services provide protection throughout the attack life cycle and across expanding attack surfaces, including IT and OT environments, as well as coverage for IoT devices. Fight AI with AI with FortiGuard Security Services.

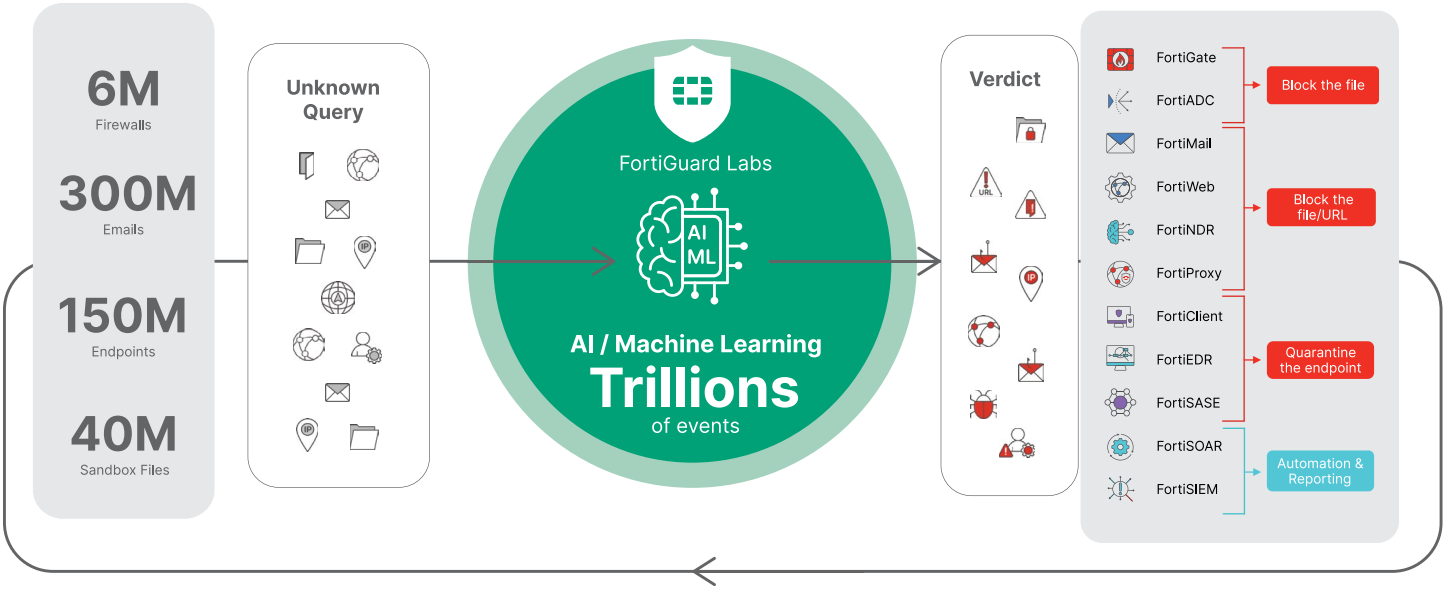
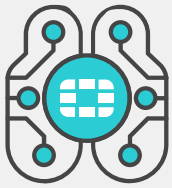


Figure 1: FortiGuard Security Services powered by real-time threat intelligence from FortiGuard Labs

FortiGuard Labs: Real-Time Threat Intelligence

FortiGuard Labs, Fortinet's global threat intelligence and research division, is the engine behind FortiGuard Security Services. Leveraging telemetry from over 10 million Fortinet devices deployed worldwide, FortiGuard Labs applies AI/ML to analyze trillions of threat events and distill actionable intelligence. This data is then shared in real time with Fortinet products, enabling instant protection against both known and unknown threats.



Fortinet and AI

Fortinet has been pioneering AI and machine learning (ML) innovation for over 15 years. Our platforms are built natively with AI-driven capabilities that span ML, deep learning, artificial neural networks, large language models, Generative AI, and agentic AI. These technologies power everything from threat detection to automation, analytics, and advanced decision-making.

AI-Powered Security Services

FortiGuard AI-Powered Security Services delivers real-time protection against the latest threats—including those powered by AI. Natively integrated into the Fortinet Security Fabric, these services provide always-on detection and automated enforcement across the entire attack surface. FortiGuard Security Services Bundles include a broad range of capabilities to support diverse use cases and meet your organization's evolving security needs.

Network and file security

FortiGuard Security Services provides advanced protection against network-based and content-level threats by combining AI-driven detection with deep signature coverage.

FortiGuard Intrusion Prevention System (IPS) blocks stealthy, network-level attacks using a comprehensive library of thousands of signatures backed by FortiGuard Labs research. Natively embedded into context-aware policies, IPS enables precise control over detection methods to address complex threats and resist evasion techniques. An AI engine specifically trained on Cobalt Strike data enhances detection accuracy and helps prevent intrusion attempts using this advanced adversary framework.

FortiGuard Antivirus delivers real-time, automated protection against polymorphic threats—including ransomware, spyware, and viruses—across network, endpoint, and cloud environments. Its advanced detection engines prevent new and evolving malware from gaining a foothold in critical systems.

FortiGuard Application Control allows administrators to create granular policies to allow, deny, or restrict access to specific applications or entire application categories. This helps prevent malicious, high-risk, or unauthorized applications from operating across the perimeter, within the data center, or between internal network segments.

Web/DNS security

The FortiGuard DNS Filtering Service provides consistent protection against sophisticated DNS-based threats, including DNS tunneling, DNS protocol abuse, DNS infiltration, C2 server identification, and domain generation algorithms. DNS filtering provides complete visibility into DNS traffic while blocking high-risk domains, including malicious newly registered domains and parked domains.

The FortiGuard URL Filtering Service provides comprehensive threat protection to address various threats, including ransomware, credential theft, phishing, and other web-borne attacks. It leverages AI-driven behavioral analysis and threat correlation to block unknown malicious URLs with near-zero false negatives immediately. It also provides granular blocking and filtering for web and video categories to allow, log, and block for rapid and comprehensive protection and regulatory compliance.

The FortiGuard Anti-Botnet and C2 Service blocks unauthorized attempts to communicate with compromised remote servers for both receiving malicious command and control information or sending out extracted information. It protects against malicious sources associated with web attacks, phishing activity, web scanning, and scraping.

SaaS and data security

The FortiGuard Data Loss Prevention Service delivers a database with consistent DLP patterns to different solutions within the Fortinet security stack to keep data and users secure and prevent costly data loss incidents.

The FortiGuard CASB Service, our inline CASB service, secures SaaS applications in use, providing broad visibility and granular control over SaaS access, usage, and data. This NGFW and SASE service also integrates with the FortiClient Fabric Agent to enable inline ZTNA traffic inspection and ZTNA posture check.

The FortiGuard Attack Surface Security Service is integrated into FortiGate NGFWs and continuously monitors and assesses the organization's Fortinet Security Fabric infrastructure and controls to provide an overall security posture rating. Unpatched vulnerabilities, misconfigurations, and less-than-optimal settings all play into scoring for each control, which, in turn, influences overall scores for the organization. Visibility across the attack surface, facilitated through the Security Fabric infrastructure, extends to IoT devices connected to the environment. The service reduces the attack surface with automated discovery, real-time query, segmentation, and enforcement for IoT devices.

Zero-day prevention

Static and dynamic analysis of suspicious files results in sub-second malware detection and verdicts. If the file is clean, the FortiGate Hybrid Mesh Firewall (HMF) will release the file to the user. Otherwise, the file will be blocked and quarantined for further action. The service can be deployed on-premises, in the cloud, or as a hosted service to meet enterprise, OT, or SOC needs.

AI-Powered Security Bundles

The FortiGuard IL MPS (inline malware prevention service) uses advanced AI and machine learning to detect and block zero-day threats that traditional methods often miss. Suspicious or unknown files are held at the HMF until a real-time verdict is rendered—allowing, blocking, or quarantining the file as needed.

Combining static and dynamic analysis, IL MPS delivers sub-second detection of malicious content. Clean files are released automatically, while threats are blocked and quarantined to prevent execution and lateral spread. This service can be deployed on-premises, in the cloud, or as a hosted solution, providing flexible protection for enterprise, OT, or SOC environments.

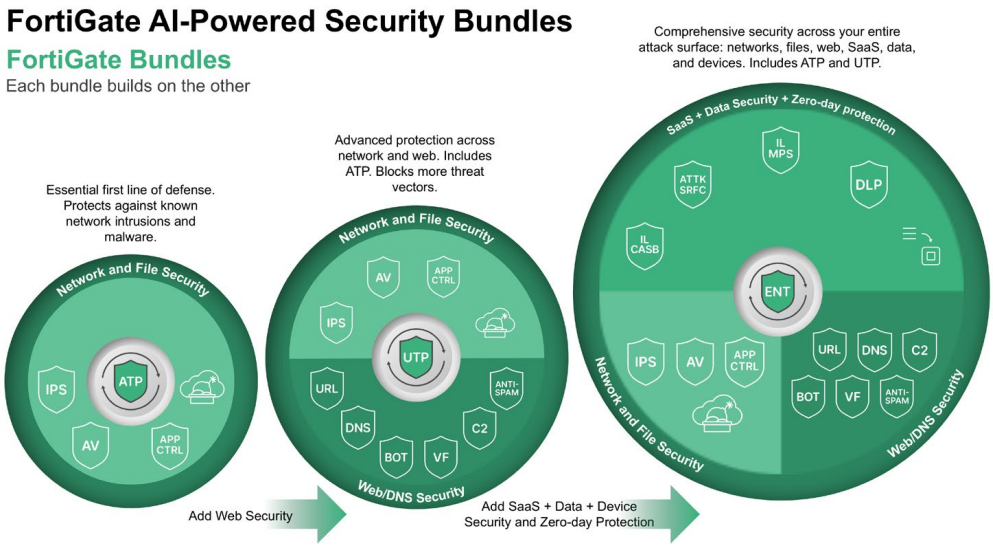


Figure 2: FortiGuard AI-Powered Security Bundles for hybrid mesh firewalls

Advanced Threat Protection (ATP)

Providing essential first-line defense against known threats, ATP protects against common attack vectors like malware and intrusions using Fortinet's foundational security services.

Included services: IPS, antivirus, application control, and FortiSandbox SaaS.

Not included: Web filtering, DNS filtering, anti-botnet, data loss prevention (DLP), CASB, IoT detection, and attack surface monitoring.

Unified Threat Protection (UTP)

UTP extends the power of ATP to deliver deeper protection across web and DNS traffic. It includes advanced threat detection for additional threat vectors such as command-and-control (C2) activity.

Included services: Everything in ATP, plus URL filtering, DNS filtering, video filtering, and anti-botnet protection.

Not included: Advanced data protection (DLP), CASB, IoT detection, and attack surface monitoring (consider the ENT bundle for comprehensive coverage).

Enterprise Protection (ENT)

ENT provides complete protection across the entire attack surface, including network, web, cloud, data, and devices. The ENT Bundle enables proactive risk management and compliance.

Included services: All ATP and UTP features, plus CASB, DLP, IoT detection and vulnerability correlation, attack surface monitoring, and AI-powered IL MPS.

Not included: OT-specific protocol and device recognition (see OT Security Service).

Additional Available Services

In addition to these core bundles, Fortinet offers specialized security services to address OT environments, outbreak response, and incident investigation.

OT Security Service

The FortiGuard OT Security Service includes thousands of signatures for OT vulnerabilities and applications, offering visibility and control over hundreds of ICS/SCADA protocols. Capabilities include device detection, OS identification, MAC address vendor mapping, vulnerability correlation, and virtual patching.

IOC and Outbreak Detection Service

Available through FortiAnalyzer, this service enables SOC teams to proactively search for indicators of compromise (IOCs) and detect hidden breaches. It also provides guidance on remediating major vulnerabilities identified by FortiGuard Labs, helping security teams stay ahead of fast-moving threats.

	FortiCare Premium (Included)	FortiCare Elite
24×7 Support		
Telephone	●	●
Chat	●	●
Web	●	●
Response		
P1 Inquiries	One Hour	15 Minutes
P2 Inquiries	One Hour	15 Minutes
P3 Inquiries	Next Business Day	Two Business Hours
P4 Inquiries	Two Business Days	Four Business Hours
Firmware		
Firmware Upgrades	●	●
Long-Term Supported Firmware		●
Console		
Asset Management Portal	●	●
FortiCare Elite Portal		●
RMA Support (Appliances)		
Return Merchandise Authorization (RMA) Replacement	Advanced Replacement RMA (Eligible for Premium RMA Upgrade)	Advanced Replacement RMA (Eligible for Premium RMA Upgrade)

FortiCare Premium and FortiCare Elite

FortiCare Premium Support Services is included in all available bundles. FortiCare Premium provides 24×7×365 support (phone, chat, and web) with one-hour response times for Priority 1 and Priority 2 inquiries. For most customers, FortiCare Premium provides the right level of support.

For organizations with urgent or acute support needs, FortiCare Elite may be a stronger fit. With FortiCare Elite, customers receive 24×7×365 support with 15-minute response service-level agreements for Priority 1 and Priority 2 inquiries.

Core Services Available with FortiCare

FortiGuard AI-Powered Security Bundles for FortiGate includes the following services as part of FortiCare Premium. The following is included with every bundle:

- Application control
- Inline CASB database
- Internet service (SaaS) database updates
- GeoIP database updates
- Device/OS detection signatures
- Trusted certificate database updates
- DDNS (v4/v6) service

Select the Right Services to Meet Your Needs

To help you determine which bundle or bundles you need, the following table lists a number of potential use cases and protection options.

	Use Cases		
	Data Centers IPS Replacements	Campuses/Branches SD-Branch	Highly Regulated Environments
Protection			
Network and file security Inspect network traffic and files for threats	●	●	●
Web/DNS security Protect against web-based and DNS-based attacks	○	●	●
SaaS and data security Secure applications, data, and usage	○	○	●
Zero-day threat prevention Detect and stop zero-day and emerging threats from getting through	○	○	●
	ATP	**UTP**	**ENT**

*Requires supplemental FortiGuard OT Security Service subscription.

Use the pyramid below, starting from the foundation and moving upward, as a further guide to selecting the right bundle to address your requirements. Organizations should ensure they have enough security to cover their entire attack surfaces, where appropriate.

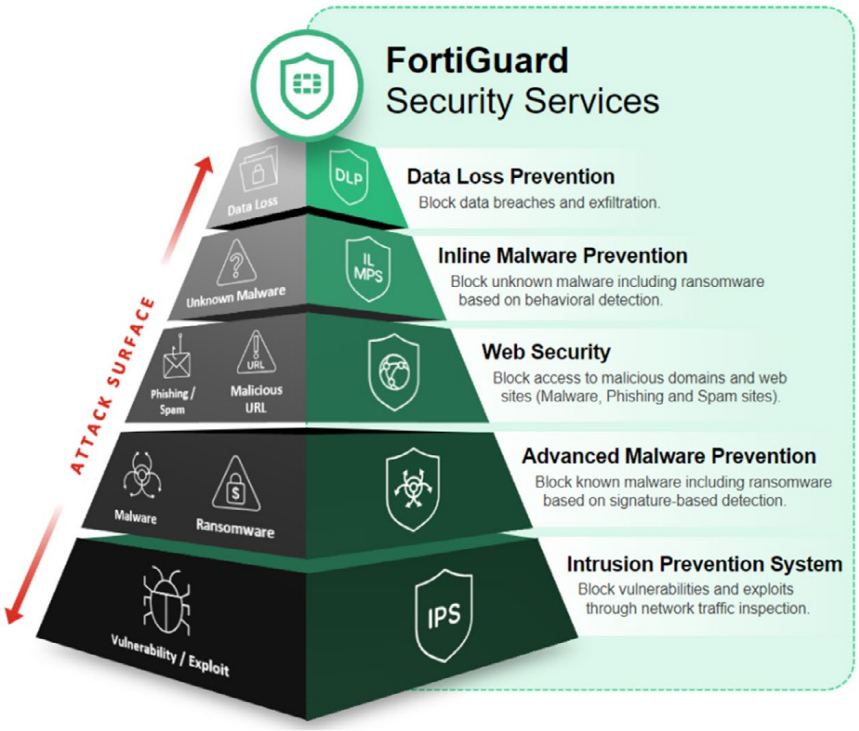


Figure 3: Building a strong security foundation and moving up the pyramid

Talk to a Fortinet Expert Now

Finding the right blend of security capabilities to complement your FortiGate HMF or Fortinet HMF-based solutions like secure SD-WAN and FortiSASE should never be difficult. Your account manager can help you determine the best bundle and a la carte services to meet your organization's requirements.

To better understand FortiGuard AI-Powered Security Services, read the portfolio brief or visit fortinet.com.

For bundle comparison and a la carte options, refer to the ordering guide.

August 26, 2025 10:44 AM / MKTG-1720-0-0-EN