SERVICE BRIEF

# Get Comprehensive, Scalable Protection with FortiGuard AI-Powered Security Services Bundles for FortiGate Next-Generation Firewalls

## 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 AI-driven attacks. FortiGuard AI-Powered Security Services Bundles provide always-on, real-time protection by combining AI, automation, and real-time threat intelligence with deep integration across the Fortinet Security Fabric.

Optimized for FortiGate Next-Generation Firewalls (NGFWs), 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. Along with cutting-edge defenses, the bundles offer simplified licensing and optimal value.

FortiGuard AI-Powered Security Services offers a layered defense for FortiGate NGFWs. 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.

## Modern Threats Require Modern Solutions

Organizations are under siege by evolving AI-powered threats, making it harder than ever to secure data, maintain regulatory compliance, and control sensitive information. The inability to keep up with the volume and sophistication of today's threats is caused by three core, compounding problems.

- **Complex compliance and regulatory overload:** The modern attack surface is vast, fragmented, and poorly understood, leading to significant security blind spots. Compliance in the era of AI is getting more complicated, and organizations suffer from poor visibility into their full attack surface. As a result, critical vulnerabilities and configuration weaknesses often go undetected.
- **The rise of shadow AI and data exfiltration:** The convenience of AI tools is introducing uncontrolled risks to sensitive corporate data. The rise of shadow AI is directly driving up the risk of data exfiltration. The use and misuse of GenAI applications enable employees to intentionally or unintentionally share confidential content and source code with online communities, creating severe, unmonitored data loss vectors.
- **AI-supercharged malware and exploit escalation:** Threat actors are leveraging AI to accelerate attacks, making traditional security defenses struggle to keep pace. We are seeing a major increase in file-based malware supercharged by AI and a rise in sophisticated zero-day exploits. Furthermore, outdated out-of-band inspection methods are slowing down critical business operations.

## Stop Threats across Your Network

The suite of 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. These include AI-powered malware, data security risks arising from the use and misuse of GenAI applications, and shadow AI risks.

The services protect the attack life cycle and across expanding attack surfaces, including IT and OT environments and IoT devices. Fight AI with AI, get visibility across your attack surface, and help meet compliance with comprehensive security from FortiGuard AI-Powered Security Services.

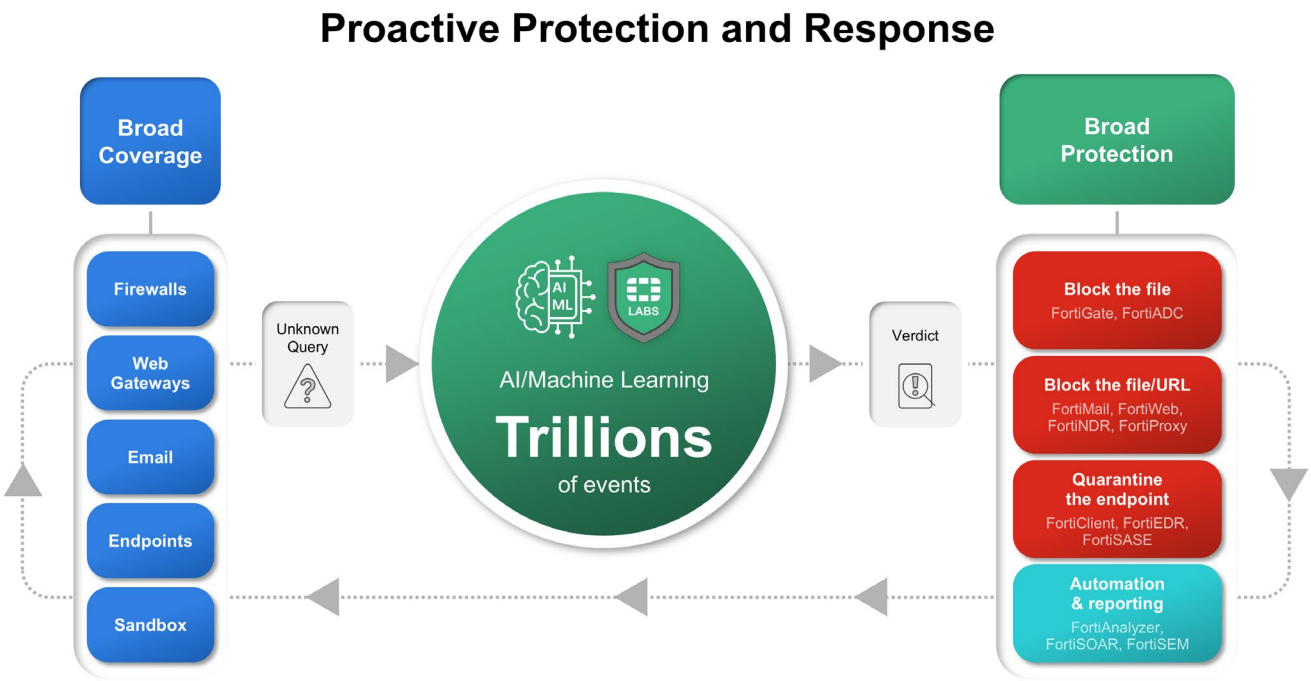



Figure 1: FortiGuard AI-Powered Security Services with real-time threat intelligence from FortiGuard Labs

## Powered by 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 millions of Fortinet devices deployed worldwide, FortiGuard Labs applies AI/ML to analyze trillions of threat events and produce actionable intelligence. This threat intelligence is then shared in real time with Fortinet products, solutions, and services, enabling instant protection against modern, dynamic, and AI-powered threats.

## AI-Powered Security Services

The 20+ FortiGuard AI-Powered Security Services deliver real-time protection against the latest threats, including those accelerated and powered by AI, such as malware, unknown threats, zero-day threats, shadow AI, data loss, and compliance threats. 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 and 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 against 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, allowing logging and blocking for rapid, comprehensive protection and regulatory compliance.

The FortiGuard Anti-Botnet and C2 Service dynamically blocks unauthorized attempts to communicate with compromised remote servers to receive malicious command-and-control information or to send 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 of consistent DLP patterns to solutions across 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 in-use SaaS applications, 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.

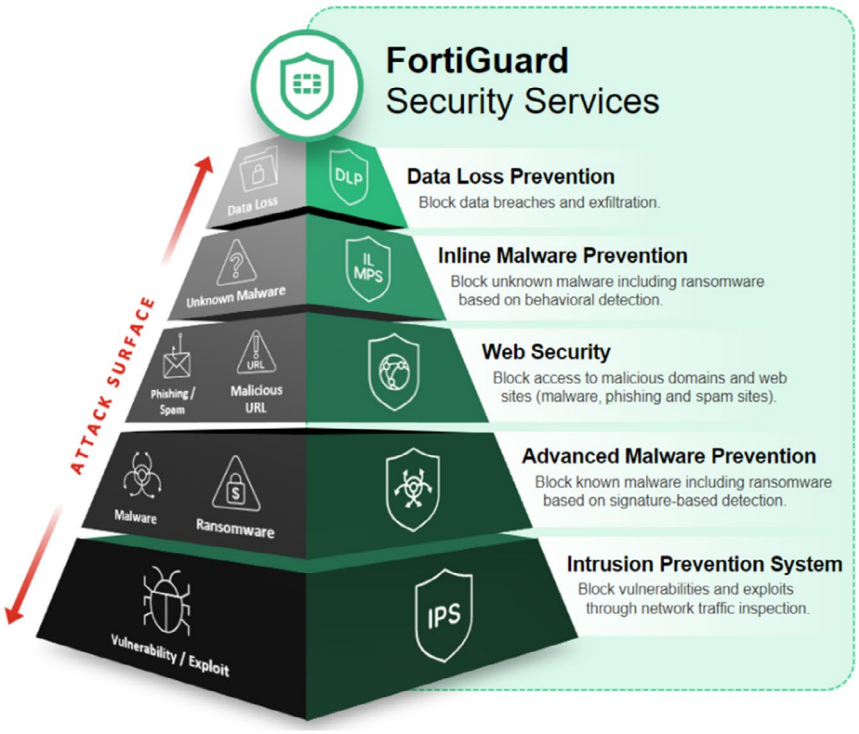



Figure 2: Build a strong security foundation by moving up the pyramid.

### Attack surface monitoring

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 by automating discovery, enabling real-time queries, and implementing segmentation and enforcement for IoT devices.

### Zero-day protection

Static and dynamic analysis of suspicious files results in sub-second malware detection and verdicts. If the file is clean, the FortiGate NGFW 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.

The FortiGuard IL MPS (inline malware prevention service) uses advanced AI and ML to detect and block zero-day threats that traditional methods often miss. Suspicious or unknown files are held at the NGFW 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.

## AI-Powered Security Bundles

FortiGuard AI-Powered Security Services offers the flexibility to tailor protection against modern, critical threats across your entire attack surface. Choose from three curated bundles, each designed to address your needs while delivering maximum value: the Enterprise Protection Bundle (ENT) for comprehensive attack surface security, the Unified Threat Protection (UTP) Bundle for essential web and network defense, and the Advanced Threat Protection (ATP) Bundle as a powerful first line of defense.

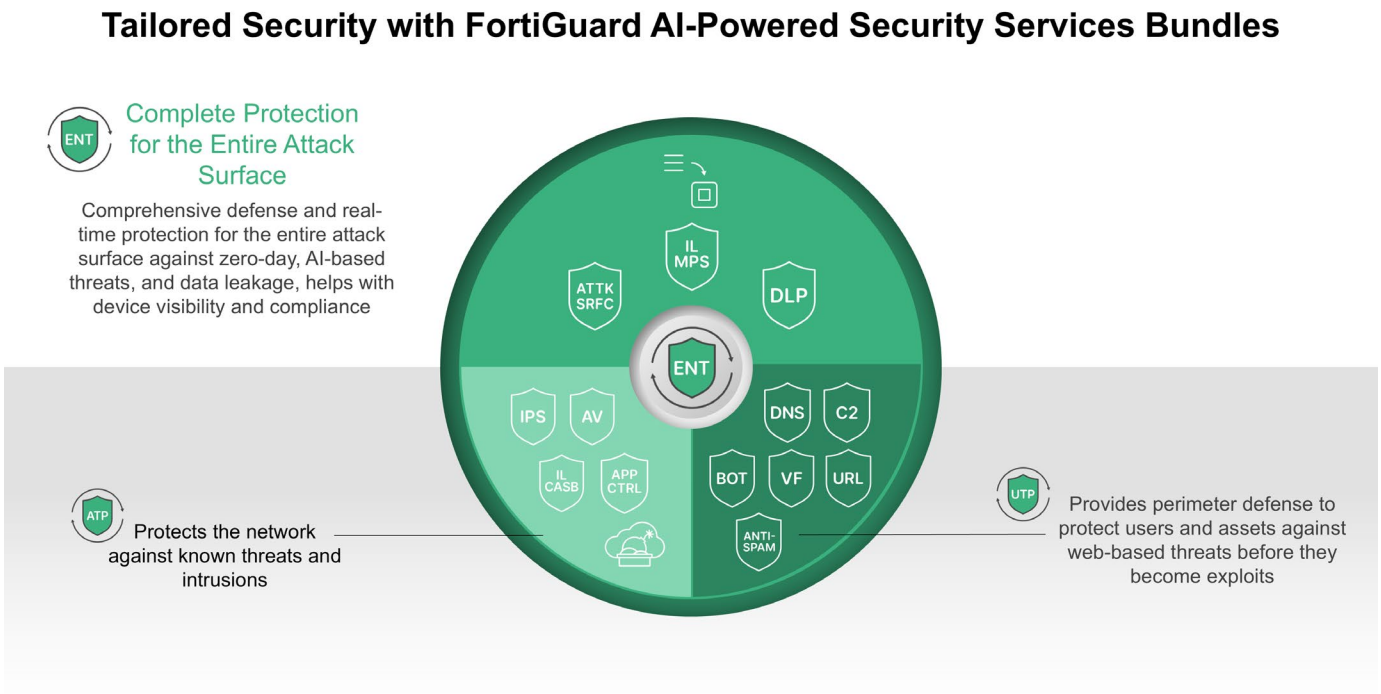



Figure 3: FortiGuard AI-Powered Security Services Bundles for FortiGate NGFWs

### ENT Bundle: comprehensive defense

**What it is:** Ultimate security for your entire attack surface: networks, web, files, SaaS, data, and devices. Includes ATP and UTP.

**Why ENT?** Protect against AI threats, meet compliance, scale, and future-proof security with the lowest cost per service.

**What's included:** All ATP and UTP features, plus DLP, attack surface security monitoring, risk scoring, AI-based inline malware prevention, and IoT detection and vulnerability correlation.

**What's not included:** OT-specific device and protocol recognition. Add the OT Security Service for OT environments.

**UTP Bundle: advanced defense for web and the modern network**

**What it is:** Advanced protection across the network and web. Includes ATP services. Blocks more threat vectors. Included in the ENT Bundle.

**Why UTP?** Protect against the rising tide of web-based threats, intrusions, and malware.

**What's included:** Everything in ATP and URL and DNS filtering, video filtering, and anti-botnet and C2 communication services.

**What's not included:** Advanced DLP, inline malware protection, IoT detection, and attack surface monitoring. Consider the ENT Bundle (above) for comprehensive security.

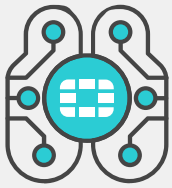
**ATP Bundle: essential first line of defense**

**What it is:** Protection against known network intrusions and malware. Included in the ENT Bundle.

**Why ATP?** Provides core security services necessary to protect your network perimeter and file-based threats.

**What's included:** Foundational security services including: IPS, antivirus, FortiSandbox SaaS, application control, and inline CASB.

**What's not included:** Critical web and DNS security (URL and DNS filtering, anti-botnet and C2), DLP, inline malware prevention service, IoT security, and attack surface monitoring. Consider the ENT Bundle for comprehensive security against the modern threat landscape.



**Fortinet and AI**
Fortinet has been pioneering AI and 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.

## Additional 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 for 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 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.

| | 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) |

Figure 4: FortiCare Premium vs. FortiCare Elite

### Core services available with FortiCare

FortiGuard AI-Powered Security Services Bundles for FortiGate include the following services as part of FortiCare Premium:

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

## Select the Right Services to Meet Your Needs

FortiGuard Labs offers such a comprehensive selection of security offerings to address today's ever-evolving threat landscape that talking to a Fortinet expert, such as your account manager, may be the best way to find the right blend of security capabilities to complement your FortiGate NGFW.

## Why FortiGuard AI-Powered Security Services Bundles?

FortiGuard AI-Powered Security Services Bundles offer the most value and simplify licensing value for comprehensive, scalable protection to complement FortiGate NGFWs. These bundles provide always-on, real-time protection by combining AI, automation, and real-time threat intelligence with deep integration across the Fortinet Security Fabric.

For more information on FortiGuard AI-Powered Security Services, visit fortinet.com. For bundle comparison and a la carte options, refer to the ordering guide.

FORTINET

www.fortinet.com



January 9, 2026 10:44 AM / MKTG-2672-0-0-EN