SERVICE BRIEF

Comprehensive Protection with FortiGuard AI-Powered Security Services and Bundles for FortiGate

Executive Overview

Many IT teams are struggling to keep up with an ever-expanding attack surface and an increase in sophisticated cybersecurity threats. FortiGuard AI-Powered Security Services for FortiGate Next-Generation Firewalls (NGFWs) provides market-leading security capabilities to protect organizations against network-, web-, application-, file- and web-based threats. Tightly integrated into FortiGate solutions, FortiGuard AI-Powered Security Services is designed to address major use cases associated with protecting branch, campus, cloud, and data center environments.

FortiGuard Labs

FortiGate NGFWs and NGFW-based solutions include FortiGuard AI-Powered Security Services. These services are developed and continuously enriched with the latest threat intelligence from FortiGuard Labs, the elite Fortinet threat research team.

Protect against Known and Unknown Threats

As IT teams work to support business objectives, the attack surface continues to expand. At the same time, the sophistication and volume of today's 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 AI-driven threat intelligence integrated with critical 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.

FortiGuard Labs maintains AI-powered analysis environments that span solution databases to help ensure that all products have the same up-to-the-minute data. Each solution has access to all the security intelligence related to its function and location across the attack surface, so security is deployed consistently and enforced cohesively. The AI-based analysis and local machine learning (ML) capabilities, in some cases, operate behind the scenes to provide full-spectrum detection and mitigation of known and unknown threats.

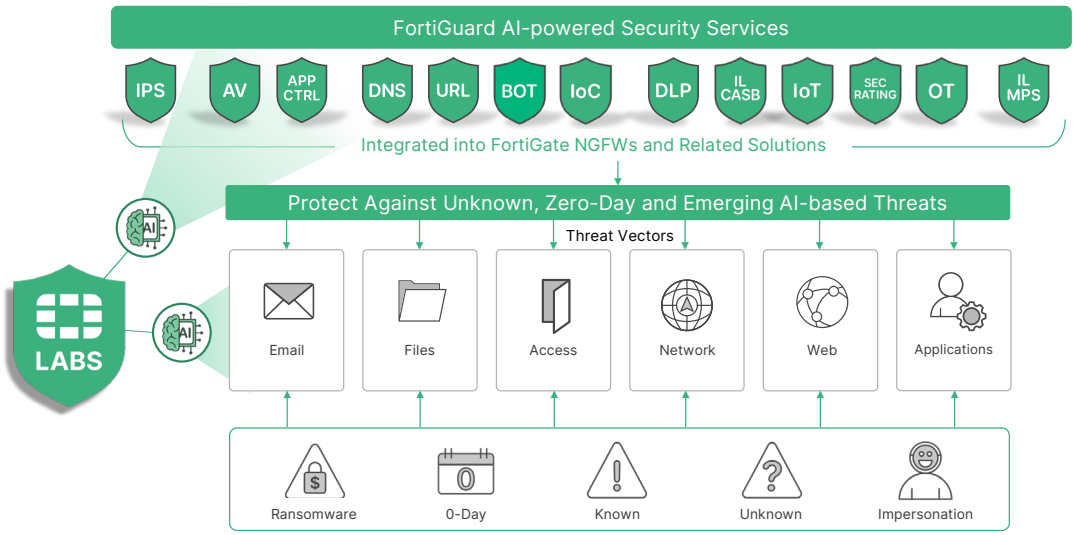

Figure 1: FortiGuard AI-Powered Services utilizes FortiGuard Labs real-time threat intelligence.

FortiGuard AI-Powered Security Services

FortiGuard AI-Powered Security Services provides real-time defense against the latest attacks and is natively integrated into the Fortinet Security Fabric to deliver coordinated detection and enforcement across the entire attack surface. The following services are available.

Network and file security

The FortiGuard IPS Service blocks the latest stealthy network-level threats and network intrusions. It uses a comprehensive IPS library with thousands of signatures, backed by FortiGuard research, credited with over 1,000 zero-day threat discoveries. Natively embedded in the context-aware policies, IPS enables full control of attack detection methods to address complex security applications and resist evasion techniques. Dedicated IPS includes end-to-end updates for IPS administration, including support for finance and other regulated deployments.

The FortiGuard Antivirus Service delivers automated updates that protect against the latest polymorphing attack components, including ransomware, viruses, spyware, and other content-level threats. It uses advanced detection engines to prevent new and evolving threats from gaining a foothold inside the network, endpoint, and clouds and accessing valuable resources.

The FortiGuard Application Control Service lets you quickly create policies to allow, deny, or restrict access to applications or entire categories of applications. Application control helps keep malicious, risky, and unwanted applications out of the network through control points at the perimeter, in the data center, and internally between 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

The FortiGuard AI-based Inline Malware Prevention Service (IL MPS) combines AI/ML-powered detection and threat filtering, detecting and remediating threats that traditional approaches miss. Static and dynamic analysis of suspicious files results in sub-second malware detection and verdicts. If the file is clean, the 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.

AI-Powered Security Bundles

FortiGuard AI-Powered Security Bundles for FortiGate helps IT and security teams scale to meet the challenges posed by today's cyberthreats. The bundles heighten prevention, reduce mean time to detect threats and mean time to respond to incidents, and help automate and accelerate security operations.

You can choose strategically curated bundles tailored to your organization's unique business requirements or customize your security strategy by ordering individual services.

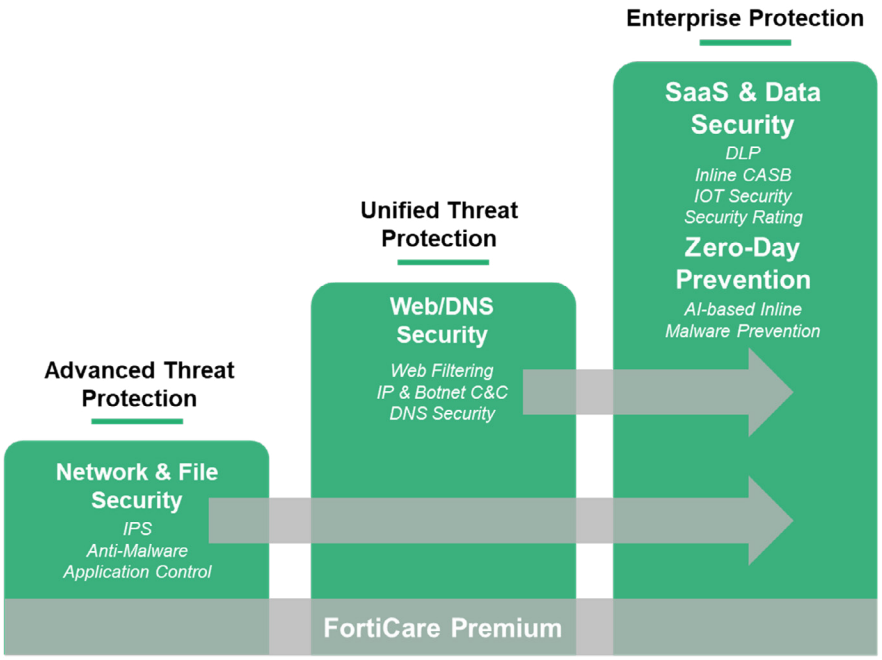

Figure 2: FortiGuard AI-Powered Security Bundles for FortiGate

Advanced Threat Protection

The Advanced Threat Protection Bundle delivers AI-powered protection against network- and file-based threats and is appropriate for:

Data centers

- Edge: North-south protection to protect against traffic into and out of the data center
- Segmentation: East-west protection to protect workloads and applications

Intrusion prevention system (IPS) replacement

- For optimized deep packet inspection of encrypted network traffic

The bundle addresses network and file security through the following FortiGuard AI-Powered Security Services:

- FortiGuard IPS Service
- FortiGuard Antivirus Service
- FortiSandbox SaaS Service
- FortiGuard Application Control Service
- FortiGuard CASB Service (Inline)

Unified Threat Protection

The Unified Threat Protection (UTP) Bundle builds on the ATP bundle with advanced web/DNS security services to protect organizations against web-borne threats, including sophisticated DNS-based threats. It is appropriate for:

Distributed firewalls

- Edge firewalls with direct internet access

Secure connectivity

- Secure, simple-to-manage architecture with centralized management and configuration

SD-WAN

- Scalable and flexible SD-WAN for delivering a secure and optimal user experience

Guest Wi-Fi security

The bundle addresses web/DNS security through the following FortiGuard AI-Powered Security Services:

- FortiGuard DNS Filtering Service
- FortiGuard URL Filtering Service
- FortiGuard Anti-Botnet and C2 Service

Enterprise Protection

The Enterprise Protection (ENT) Bundle provides several key features over the Unified Threat Protection Bundle that help NOC and SOC teams further mature and heighten the organization's security posture. It is appropriate for:

Secure enterprise networks

- Comprehensive security for complex enterprise HQ, branch, and campus environments

Hybrid work

- Enterprise-grade security for remote access and work from anywhere

Supply chain risk

- Protection against unauthorized access to systems, data, and lateral movement

Cyber-physical security

The bundle addresses SaaS and data security and zero-day prevention through the following FortiGuard AI-Powered Security Services:

- FortiGuard Attack Surface Security Service
- FortiGuard Data Loss Prevention Service

Zero-day prevention

- FortiGuard AI-based Inline Malware Prevention Service (IL MPS)

Additional Available Services

The FortiGuard OT Security Service features more than 3,000 OT-specific vulnerability and application signatures to identify and police over 70 ICS/SCADA protocols and industrial equipment for granular visibility and control. Other capabilities, such as device and OS detection and IoT hardware MAC address vendor mapping updates, provide additional protection. Device detection and protection services for OT devices include vulnerability correlation and virtual patching.

The FortiGuard IOC and Outbreak Detection Service is available with FortiAnalyzer. It helps SOC teams search for and detect an existing breach of their environment by searching for Indicators of Compromise collected by Fortinet. The service gives threat hunters further resources to detect and stop an ongoing attack that may already be present within the environment. In addition, the service provides SOC teams with the latest insights and guidance for remediation of major vulnerabilities and areas of risk identified by FortiGuard Labs.

	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		
Protection	**Data Centers Segmentation**	**Distributed Firewalls Secure Connectivity SD-WAN Guest Wi-Fi**	**Secure Enterprise Networks Hybrid Work (SASE) Supply Chain Risk Cyber-Physical Security***
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.

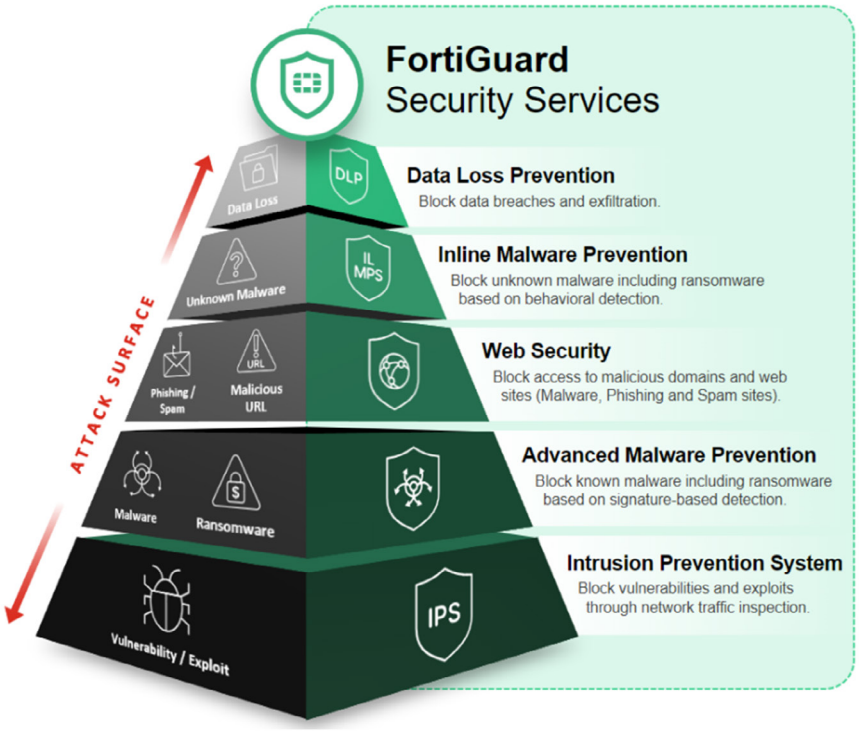

Figure 3: Building a strong security foundation and moving up the pyramid

Talk to a Fortinet Expert Now

Finding the right blend of security capabilities to complement your FortiGate NGFW or Fortinet NGFW-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.

If you need more detailed information on what is in each bundle or how to order a solution from Fortinet, please refer to the ordering guide.

February 15, 2024 2:48 PM
2421758-A-0-EN