

FortiGuard IPS Service Brief

Executive Summary

The AI/ML-powered FortiGuard IPS Service from Fortinet combines near-real-time intelligence with thousands of intrusion prevention rules to detect and block known and suspicious threats before they ever reach your devices.

Natively integrated into the Fortinet Security Fabric, the FortiGuard IPS Service combines rich IPS capabilities, such as deep packet inspection (DPI) and virtual patching, with industry-leading performance and flexible deployment options to detect and block malicious traffic and coordinate a networkwide response to threats. It is also available as a standalone system.

Regardless of where or how it is deployed, the innovative FortiGuard IPS Service leverages a modern, efficient architecture to make performance in even the largest data centers reliably consistent.

What Is the FortiGuard IPS Service?

Fortinet's powerful intrusion prevention system (IPS) security solution is designed to protect organizations by actively detecting and blocking cyberthreats. Using real-time analysis and advanced AI/ML capabilities, Fortinet IPS fortifies organizations' cybersecurity posture by detecting and preventing intrusion attempts, malware infections, and zero-day attacks.

Key features and benefits include:

Focus Area	Benefits
 Signature Clustering	Consolidates and manages multiple signatures associated with a specific vulnerability or threat. Rather than using numerous individual signatures of unique attack patterns, all targeting the same vulnerability, signature clustering groups similar signatures into a single group. This approach enhances threat detection accuracy, addresses multiple attack variants efficiently, and frees up processor bandwidth.
 Real-Time Threat Intelligence	FortiGuard IPS uses signature-based and behavior-based techniques powered by AI/ML to identify known and unknown threats in real time. And by monitoring global threat intelligence feeds, FortiGuard IPS continuously updates its knowledge base to detect and mitigate emerging threats.
 Zero-Day Protection	It analyzes behavioral patterns and anomalies to proactively detect and defend against unknown and zero-day attacks.
 Virtual Patching	FortiGuard IPS enables virtual patching to ensure timely protection against vulnerabilities before they are officially patched by vendors.
 Customizable Policies	Organizations can create tailored security policies for granular control over their network traffic and security rules.
 High Performance	Fortinet's advanced architecture and patented ASICs ensure optimal network performance and minimal latency for even the most processor-intensive actions, whether deployed as a virtual device, cloud-based service, or appliance.

FortiGuard IPS is powered by FortiGuard Labs, Fortinet's threat intelligence and research organization that develops, innovates, and maintains one of the industry's most advanced AI and ML systems. We use this technology to deliver proven protection, unparalleled visibility, and robust business continuity across the Fortinet Security Fabric. We consistently protect organizations against today's rapidly evolving and increasingly sophisticated threats targeting IT and OT environments.

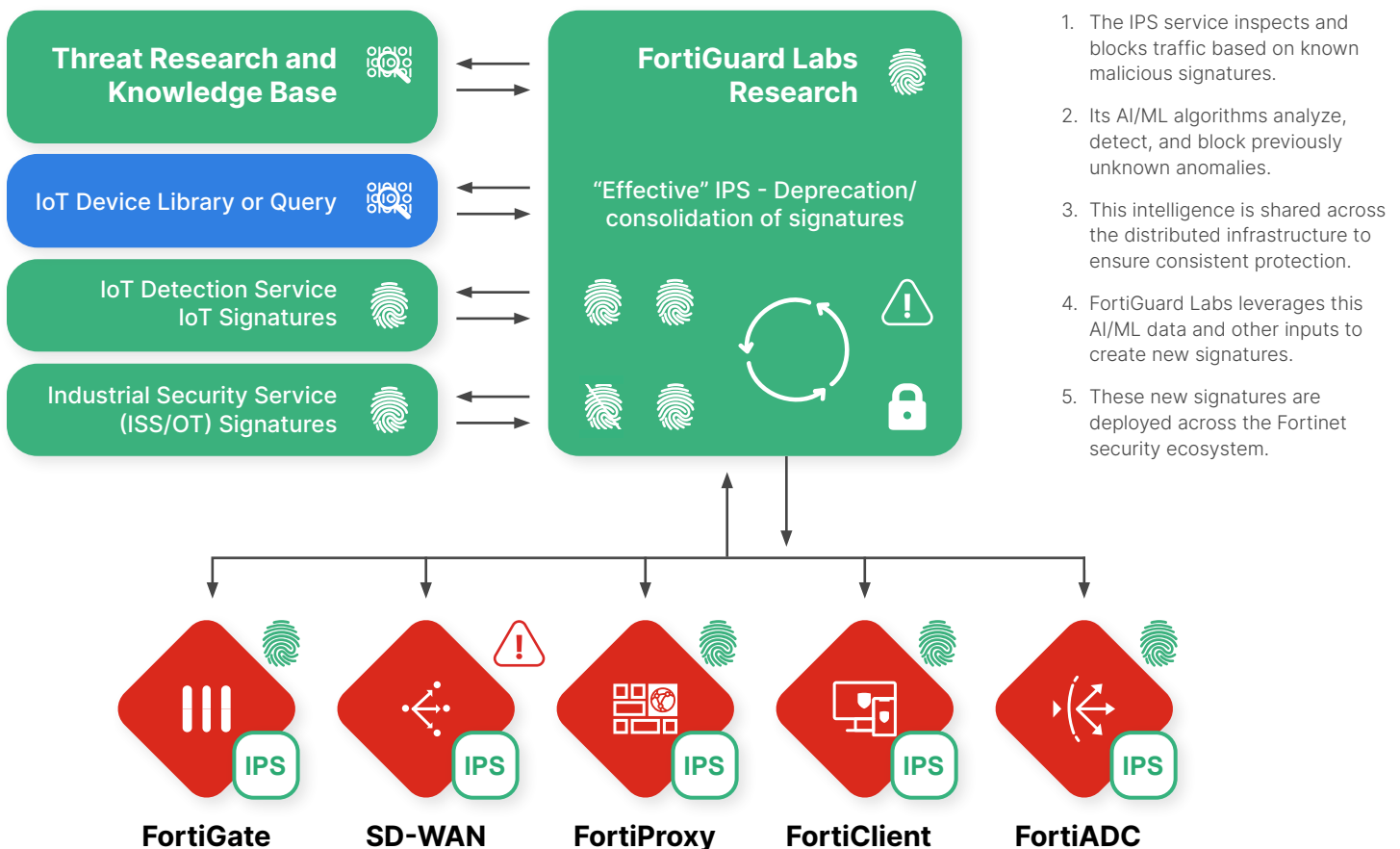
Key Fabric Integrations

FortiGuard IPS is tightly integrated with FortiGate Next-Generation Firewalls and various Fortinet Security Fabric products to enable a comprehensive platform approach to security. Key integrations include:

- FortiGate
- Secure SD-WAN
- Fortinet Secure Web Gateway
- FortiClient
- FortiADC
- FortiProxy

Integrating products and services creates a unified Fortinet Security Fabric platform that can be deployed anywhere across the network, allowing organizations to deploy dozens of critical services and still have them function as a single, expansive solution. Intrusion prevention system policies can be managed centrally through a single console to better correlate threat data and initiate and automate coordinated responses.

How the FortiGuard IPS Service works



FortiGuard IPS uses a combination of traffic inspection, signature-based detection, behavior analysis, and anomaly detection to identify potential threats. It continuously monitors network traffic using deep packet inspection, analyzing packets for known threats based on signatures and behavioral patterns. And its AI/ML algorithms can also detect and prevent emerging and unknown threats that lack traditional signatures.

Once a potential threat is detected, Fortinet IPS shares this information with FortiGuard Labs. It creates a new signature or consolidates multiple signatures targeting the same vulnerability or attack pattern, classifying them as part of a similar vulnerability through its signature clustering technique. These signatures are then shared with other Fabric products.

FortiGuard automated IPS updates provide the latest defenses against network intrusions, arming organizations with the latest defenses against stealthy network-level threats. In addition to updated signatures, FortiGuard Labs also provides a comprehensive IPS library with thousands of signatures, flexible policies that enable complete control of attack detection methods to suit complex security applications, advanced resistance to evasion techniques, and an IPS signature lookup service.

With the FortiGuard IPS Service integrated into the broader security infrastructure, Fortinet can analyze and deploy new intrusion prevention signatures in near real time for coordinated network response.

FortiGuard IPS Service Benefits

- Zero-day threat protection
- Over 13,500 vulnerability and exploit signatures
- Threat intelligence in near real time to stop the latest threats combined with daily updates to IPS signatures
- Insight into threats anywhere in the world through a global network of more than 3 million sensors
- Fast and comprehensive intelligence across the Security Fabric via automated and advanced analytics (such as ML) combined with high-fidelity delivery with mature and rigorous back-end processes
- Proactive threat research to prevent the exploitation of new avenues of attack

FortiGuard IPS Ordering Information

Organizations simply need to add the desired security subscriptions to their existing Fortinet Security Fabric deployment to enjoy the benefits of the intelligence, expertise, and protection delivered by FortiGuard Labs. The FortiGuard IPS Service is available as standalone and bundled subscriptions.

	Standalone	ATP Bundle	UTP Bundle	ENT Bundle
FortiGuard IPS	Yes	Included	Included	Included
SKU	FC-10-0060F-108-02-DD	Refer to price list	Refer to price list	Refer to price list



www.fortinet.com