SERVICE BRIEF

Stop Zero-Day and AI-Driven Threats with the FortiGuard AI-Based Inline Malware Prevention Service

Executive Summary

Sandboxing solutions have traditionally been used to address malware, ransomware, zero-day, and previously unknown file-based threats. However, to ensure performance lags do not slow down productivity, these offline solutions are configured to let potentially infected files into the network before the file is completely analyzed. This poses a risk because in the case of a malicious verdict, the security team must chase down the file and mitigate the threat before it can do damage.

Given the nature of today's AI-driven threat landscape and increasing attack surface, this approach is no longer viable or recommended. Instead of forcing a choice between security and performance, the FortiGuard AI-Based Inline Malware Prevention Service blocks unknown files including zero-days and AI-driven threats inline and in real time. The service does not allow them into the network until they are found to be safe, and there is no performance impact.



In 2025, FortiGuard Labs disrupted 3.8 trillion vulnerability exploitation attempts, preventing 2.71 billion malware deliveries, and blocking 257 million newly seen malware variants worldwide.[1]

Overview

The FortiGuard AI-Based Inline Malware Prevention Service enables organizations of all sizes to move from a reactive detection approach to a proactive protection approach. It not only detects but also prevents unknown, zero-day malware (including polymorphic and AI-driven threats) from entering the network by holding the suspicious file until a verdict is reached. The service analyzes and resolves every potential unknown threat in real time. It also generates new preventions across the Fortinet Security Fabric without affecting enterprise traffic or business productivity. It is available directly on FortiGate Next-Generation Firewalls (NGFWs), on FortiSandbox, or as-a-Service.

Multiple Technologies and Multistage Analysis Reduce Risk

Leveraging artificial intelligence (AI), machine learning (ML), and other technologies on top of contextual databases for both dynamic and static analysis enables the AI-based inline malware prevention service to identify, classify, and protect against all types of malicious threats in record time.

Because not all unknown files are equally dangerous, multistage analysis is performed so the sandbox can focus only on the ones that truly pose a risk. The stages are:

1. **Block all known threats:** Threat evaluation is based on 20+ years of threat data from FortiGuard Labs and ecosystem partners.
2. **Address polymorphic and code reuse:** Content pattern recognition language (CPRL) and antivirus (AV) scans eliminate known threats as they filter out malware by understanding behavior patterns and applying deep code inspection.
3. **Perform static analysis:** ML further filters out known/unknown threats and performs anti-evasion checks.
4. **Hold unknown content:** The inline blocking within the firewall holds any unknown content, including AI-driven threats until the verdict is rendered by the service.
5. **Perform dynamic analysis:** This includes code emulation and is performed in a contained environment to uncover the full attack life cycle. It takes advantage of behavior-based ML that is constantly learning new malware techniques and automatically adapting malware behavioral indicators. Use of deep neural networks enables sub-second malware detection.

The AI-based service:

- Continually applies these deep-learning methodologies to detect any anomalies within the code base of malicious files. Once a file has been cleared, it is allowed into the network without any impact on performance or security.
- Generates new preventions and shares them with the Fortinet Security Fabric and ecosystem so that customers are protected against the newly discovered threat.

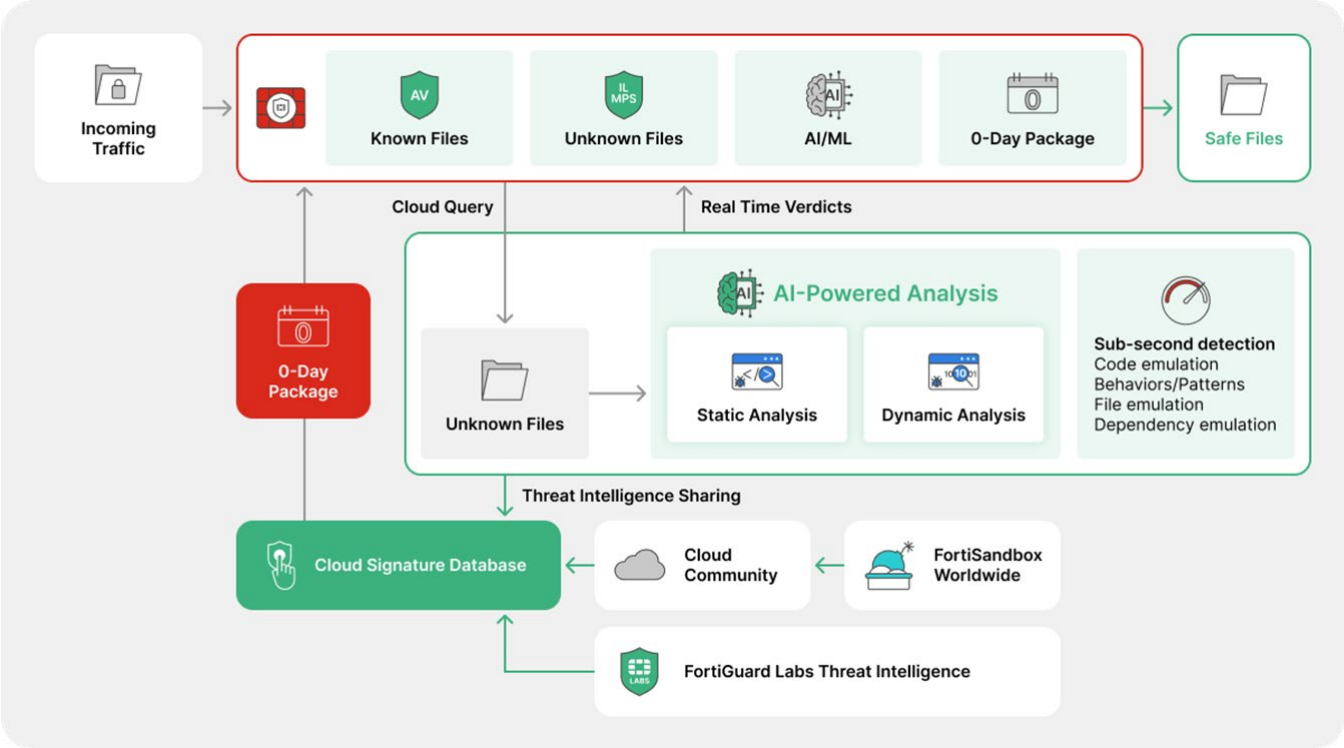


Figure 1: FortiGuard AI-Based Inline Malware Prevention Service flow

How the Inline Malware Prevention Service Works

When a user requests a file download, runs an application, or clicks on a URL, the file is first analyzed by the AV engine using CPRL and AI/ML. This analysis filters out known, unknown, polymorphic, and behavior-based signatures. The result of this analysis is one of three classifications: known good, known bad, or malicious/unknown. If the file is known good, it is allowed in. Malicious files are blocked and quarantined. If the file is unknown, the service holds the file and sends it to a sandbox for further analysis.

Unknown signatures are subjected to a cloud query to check if we have seen this signature before and follows the same logic of known good, known bad, and unknown. Unknown files are further analyzed using static and dynamic AI/ML analysis until a verdict is reached. This generally happens in seconds and this verdict is communicated to the firewall so that only clean files are allowed in. When this analysis is complete, the threat intelligence is shared with the FortiGuard threat intelligence ecosystem and the cloud signature database is updated. To enable fast protection and threat intelligence sharing across the Fortinet Security Fabric, signatures are updated and shared every two minutes.

Key features

- AI enables proactive and predictive identification and classification of threats.
- Files sent to the FortiGuard Inline Malware Prevention Service are analyzed before other files.
- Verdicts are rendered in less than one second.
- Real-time analysis ensures only clean files are released (without traffic impact).

- Holding files reduces risk and time spent chasing down threats.
- Flexible deployment options and full integration remove security gaps.
- Scalability makes it ideal for any sized organization.

Flexible Deployment Options Across the Fortinet Security Fabric

The FortiGuard AI-Based Inline Malware Prevention Service provides protection across information technology (IT) and operational technology (OT) environments. It can be deployed at multiple locations, including cloud, data center, branch, campus, email, and endpoints. Because the service is fully integrated with other Security Fabric products, it helps to close security gaps across the entire attack surface in real time.

The FortiGuard Inline Malware Prevention Service is available as part of the Enterprise (ENT) Bundle or a la carte for FortiGate,* or as a feature within FortiSandbox** in the following configurations:

Product/Services	Deployment	Available for
FortiGuard AI-Based Inline Malware Prevention Service	ENT Bundle Subscription	FortiGate
FortiGuard AI-Based Inline Malware Prevention Service	SaaS Subscription	FortiGate
FortiSandbox Hosted	PaaS Subscription	FortiGate, FortiClient, and FortiMail
FortiSandbox Virtual Appliance	VM Subscription	FortiGate, FortiClient, FortiMail, FortiWeb. FortiProxy, and FortiADC
FortiSandbox Hardware	HW + Licenses	FortiGate, FortiClient, FortiMail, FortiWeb. FortiProxy, and FortiADC

*Must be running FortiOS 7.2 or later

**Version 4.2 or higher

The FortiGuard AI-Based Inline Malware Prevention Service Addresses Today's Security Challenges

The FortiGuard AI-Based Inline Malware Prevention Service takes a better approach to protecting against the modern threat landscape including malware, ransomware, evasive, unknown, and AI-based threats. It is automated, integrated, and intelligent. The ultimate combination of AI-/ML-powered detection and proactive mitigation enables files to be fully verified before being let into the network. Further, coordinated advanced detection (to prevent multistep/multihop attacks), dynamic antivirus scanning, threat scanning, web filtering, and threat intelligence combine to detect threats that traditional approaches miss. The service is a key security control for the modern enterprise.

[1] Outbreak Alerts Annual Report 2025, Fortinet, March 2026. https://global.fortinet.com/lp-en-ap-outbreakalerts-report25

Copyright © 2026 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.

March 25, 2026 10:51 AM / MKTG-3142-0-0-EN