SOLUTION BRIEF

Stop Zero-Day and Previously Unknown Threats with the FortiGuard Inline Sandbox Service

Executive Summary

Sandboxing solutions have traditionally been used to address zero-day and previously unknown file-based threats. However, in the name of performance, they are configured to let potentially infected files into the network before the file is completely analyzed. This poses risk and requires security teams to chase down malicious files.

Given the nature of today's threat landscape, this approach is no longer viable. Sandboxing solutions need to evolve and adapt to protect the ever-growing attack surface. Instead of forcing a choice between security and performance, FortiGuard Inline Sandbox solutions hold suspicious files until they are found to be safe, without any performance impact.

This approach is not new. It has been already implemented in high-risk access points such as email and endpoints. Providing the same level of security for the network is a natural extension of that security control.

FortiGuard Labs saw nearly a 100% increase in ransomware variants in just the first half of 2022.[1]

FortiGuard Inline Sandbox Overview

The FortiGuard Inline Sandbox Service enables organizations of all sizes to move from a detection approach to a protection approach. It not only detects but also prevents unknown and zero-day malware from entering the network by holding the suspicious file until a verdict is reached. The inline sandbox, unlike a traditional sandbox, 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 inline sandbox 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:** Machine learning 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 until the verdict is rendered by the inline sandbox.

5. **Perform dynamic analysis:** This includes code emulation and is performed in a contained environment to uncover the full attack lifecycle. 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 inline sandbox 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.
   - The inline sandbox generates new preventions and shares them with the Fortinet Security Fabric and ecosystem to harden security across the cyber kill chain for this newly discovered threat.

Using AI-powered inline sandboxing is your best option to protect against sophisticated ransomware and wiper malware threats.[2]

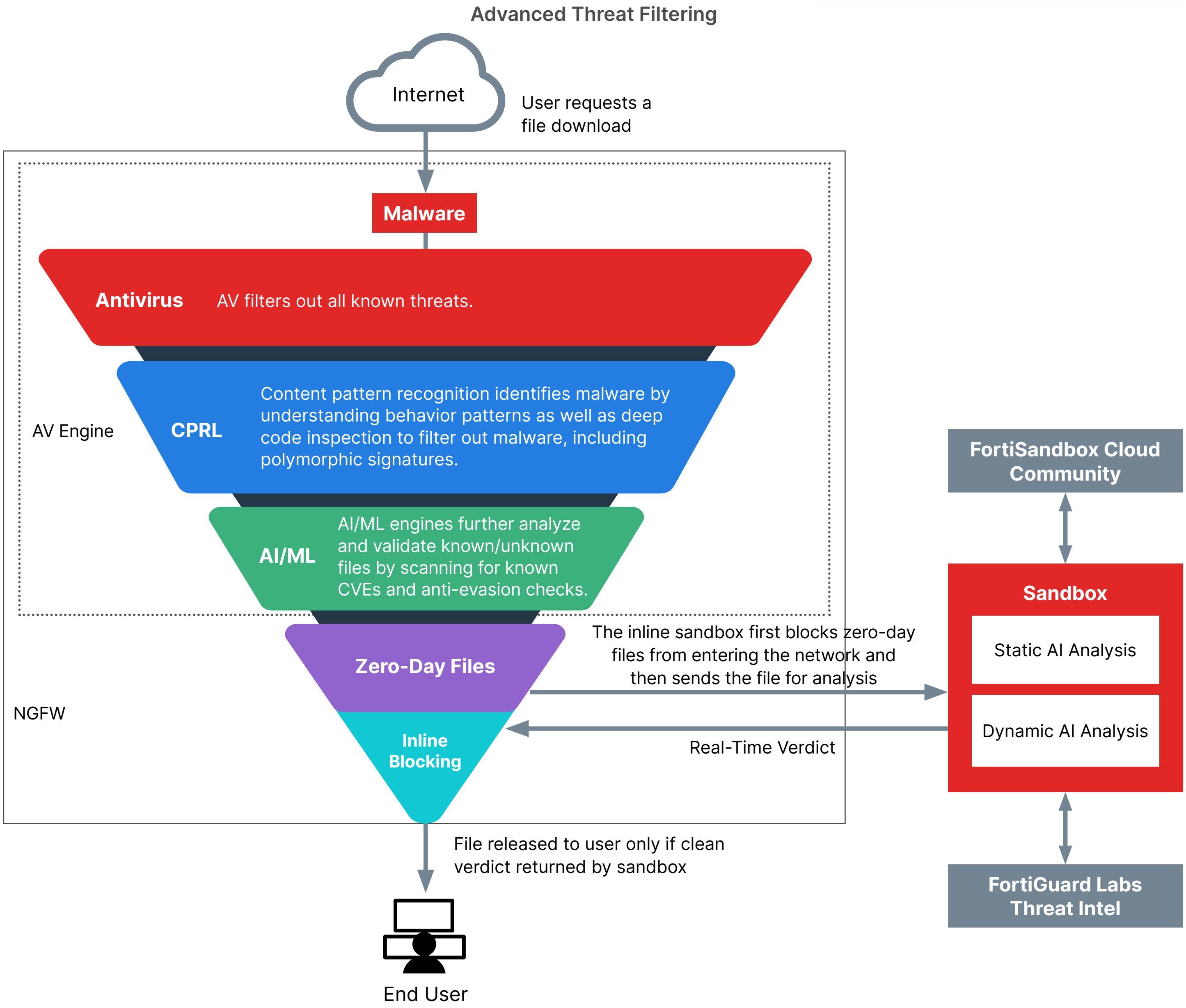
Advanced Threat Filtering
Internet
User requests a file download
Malware
Antivirus
AV filters out all known threats.
AV Engine
CPRL
Content pattern recognition identifies malware by understanding behavior patterns as well as deep code inspection to filter out malware, including polymorphic signatures.
AI/ML
AI/ML engines further analyze and validate known/unknown files by scanning for known CVEs and anti-evasion checks.
Zero-Day Files
The inline sandbox first blocks zero-day files from entering the network and then sends the file for analysis
NGFW
Inline Blocking
Real-Time Verdict
FortiSandbox Cloud Community
Sandbox
Static AI Analysis
Dynamic AI Analysis
FortiGuard Labs Threat Intel
File released to user only if clean verdict returned by sandbox
End User

Figure 1: Fortinet Inline Sandbox process

Key Features

- AI enables proactive and predictive identification and classification of threats.
- Real-time analysis ensures only clean files are released (without traffic impact).
- Holding files reduces risk and time spent chasing down malware.
- 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 inline sandbox provides protection across both information technology (IT) and operational technology (OT) environments and can be deployed at multiple locations, including cloud, data center, branch, campus, email, and endpoints. Because the inline sandbox is fully integrated with other security products, it helps to close the gaps in your attack surface.

The inline sandbox is available as an a la carte offering for NGFW* or as a feature within FortiSandbox** in the following configurations:

Product/Services	Deployment	Available for
FortiGuard Inline Sandbox 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 Inline Sandbox Service Addresses Today's Security Challenges

The FortiGuard Inline Sandbox Service takes a better approach to stopping unknown file-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.

[1] "Global Threat Landscape Report," FortiGuard Labs, August 2022.

[2] Derek Manky, "What CISOs Need to Know About the Threat Landscape in 2023 and Beyond," Fortinet, November 16, 2022.

Copyright © 2022 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 General Counsel, 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.

January 12, 2023 9:02 AM