POINT OF VIEW

Shift from Detection to Real-Time Protection with Inline Sandboxing

Executive Summary

Traditional sandboxing solutions have been used to address attacks that are predominantly content based, including ransomware. Operating offline, they allow all files into the network, which means that security teams need to chase down the files that have been deemed malicious after analysis is completed. This reactionary approach, combined with threats that are continually increasing in volume and sophistication, is not enough. A proactive approach that allows only safe content into the network is needed, such as inline sandboxing.

Traditional Sandboxes

Traditional sandboxes are offline solutions that are designed to detect, identify, and classify unknown threats. They are configured to let files into the network while they are being analyzed offline to avoid a slow-down of enterprise traffic. This means that the analysis does not happen within the file exchange process, deferring security and potentially compromising the organization.

This creates a challenge for security teams in cases where files are found to be malicious. The team must now track down the file in the network. Further, the file may have already caused damage, such as encrypting files for ransom, or affected other networks through lateral movement. Security teams end up playing hide and seek with the file, wasting time and increasing risk.

Traditional sandboxing solutions are effective in detecting threats, but they:

- Are configured to allow all files into the network
- Perform offline analysis on files to render malicious or clean verdict
- Create additional work for security organizations

FortiGuard Labs saw 10,666 ransomware variants in the first half of 2022, compared to just 5,400 in the previous six months. That's almost 2x growth in ransomware variants in half a year.[1]

"Threat actors exploited more zero-day vulnerabilities in 2021 than any prior year."[2]

Inline Sandboxing Delivers Real-Time Threat Protection

Sandboxing solutions need to evolve and adapt to the changing, broad attack surface and sophisticated artificial intelligence (AI)- and machine learning (ML)-driven attack tactics. A solution is needed that does not let suspicious files enter the network until analysis is completed and a clean verdict is determined. This needs to happen in real time without affecting enterprise security and productivity. An inline sandbox is such a solution.

An inline sandbox takes a coordinated, holistic approach that includes antivirus (AV), content pattern recognition language (CPRL), AI, ML, and comprehensive threat intelligence. Artificial intelligence, dynamic analysis, and deep neural networks enable sub-second proactive and predictive identification and verdict determination of threats without disruption to network traffic or delays.

When inline sandboxing is integrated into a high-performance architecture, dangerous zero-day malware threats will not be allowed into the network and end-to-end automation can be enabled. Inline sandboxing can be deployed across IT and OT networks, including the data center, branch, campus, clouds, and endpoints.

> “Zero-day attacks are increasing at an unprecedented rate and threaten to disrupt businesses worldwide.”[3]

How an Inline Sandbox Works

An inline sandbox follows a number of steps to ensure protection once a user requests a file from the internet:

1. Advanced filtering narrows down the number of file-based threats to eliminate false positives and reduce workload on the sandbox. This filtering catches polymorphic signatures.
2. The inline sandbox stops unknown threats from entering the network until a clean verdict is obtained.
3. The inline sandbox uses deep neural networks and ML methodologies to detect any anomalies within the code base of malicious files and issues verdicts in real time.
4. If a clean verdict is obtained, the file is released to the user. If not, it remains blocked.
5. The inline sandbox will generate new preventions and share them with other products in the ecosystem to harden security across the cyber kill chain for this newly discovered threat.

Protection for Today’s Zero-Day Threats Requires a Better Approach

With inline sandboxing, you can get real-time analysis and protection from threats without impacting network performance. Threats can be identified across the network, email, and endpoints. The right solution will let you stop malicious files without compromising security and wasting time searching for malicious files.

[1] “FortiGuard Labs Global Threat Landscape Report 1H 2022,” Fortinet, August 2022.

[2] Ji Vijayan, “Zero-Day Exploit Use Exploded in 2021,” Dark Reading, April 21, 2022.

[3] Shira Landau, “7 Highly Effective Ways to Prevent Those Unexpected Zero-Day Attacks,” eLearning Industry, January 8, 2022.

FORTINET

www.fortinet.com