FORTINET

WHITE PAPER

FortiSandbox: Third-generation Sandboxing Featuring Dynamic AI Analysis

Executive Summary

As zero-day and unknown attacks continue to grow in numbers and sophistication, successful breaches are taking longer to discover—at a significant cost to businesses. Many first- and even second-generation sandboxing solutions lack key features like robust artificial intelligence (AI) to keep pace with the rapidly evolving threat landscape. A third generation of sandbox devices, however, not only can help detect breaches in a timely manner but also prevent them from happening. FortiSandbox integrates with the broader Fortinet Security Fabric and utilizes the universal MITRE ATT&CK security language for categorizing threat models and methodologies. FortiSandbox applies robust AI capabilities in the form of both static and dynamic behavior analysis to expose previously unseen malware and other threats before a breach can occur.

FortiSandbox AI Capabilities

FortiSandbox applies two robust machine algorithms for static and dynamic threat analysis:

- A patent-pending enhanced random forest with boost tree machine-learning model
- A least squares optimization learning model

Expanding Breach Impacts Require Better Detection and Prevention

A majority (nearly 80%) of organizations report that they are introducing digital innovations faster than their ability to prevent successful cyberattacks.[1] The vast majority (92%) of security architects report experiencing at least one intrusion in the past 12 months.[2] And this problem is compounded by the fact that it typically takes more than nine months (279 days) for an organization to discover a security breach—with an average cost of nearly $4 million in damages per event.[3]

These critical issues beg the question—what can security architects do to improve not only breach detection but prevention as well? For some time now, organizations have successfully relied on sandboxing devices to discover threats (like malware) hidden in network traffic. But over time, cyber criminals have found ways to thwart detection by previous-generation sandboxes—such as encryption, polymorphism, and even their own AI-based codes that give these threats adaptive and intelligent evasion abilities.

Subsequently, a new generation of sandboxes was needed to keep pace with these rapidly evolving threats. FortiSandbox offers a third-generation sandbox designed for detection and prevention of breaches caused by the full spectrum of AI-enabled threats—both known and unknown.

Fortinet Third-generation FortiSandbox Solution

Unlike previous-generation solutions, a third-generation sandbox must do three things:

- It must utilize a universal security language via a standardized reporting framework to categorize malware techniques.
- It must share threat intelligences across a fully integrated security architecture in order to automate breach protection in real time as threats are discovered.
- It must perform both static and dynamic (behavior) AI analysis to detect zero-day threats.

FortiSandbox addresses the problem of multiple, nonstandard security languages for malware reporting through the **MITRE ATT&CK** framework.[4] This broadly adopted knowledge base of adversary tactics and techniques categorizes all malware tactics in an easy-to-read matrix. This, in turn, helps security teams accelerate threat management and response processes.

As an integrated part of the Fortinet Security Fabric architecture, FortiSandbox uses three forms of threat intelligence for automated breach detection and prevention. It uses global intelligence about emerging threats around the world via FortiGuard Labs researchers. Second, it shares local intelligence with both Fortinet and non-Fortinet products across the security infrastructure for real-time situational awareness across the organization. Finally, and most importantly, FortiSandbox applies true AI capabilities—including **both static and behavior analysis**—to improve detection efficacy of zero-day threats.

In addition to the above, FortiSandbox applies AI capabilities throughout the entire sandboxing process. Here, it is important to note that most sandbox vendors have yet to implement any form of AI—and other solutions that claim to use AI techniques may only apply static analysis. But effective AI-based sandboxing requires both static and dynamic operations to successfully spot some types of advanced threats.

AI-driven Security Effectiveness

An effective sandbox should be measured not only in terms of its threat detection rate but also in terms of the time to detect that directly impacts return on investment (ROI).[5] Faster identification of threats and containment of breaches yield lower recovery costs. Following are some of the primary reasons:

Active and passive AI analysis. To address the constantly evolving threat landscape, FortiSandbox applies AI throughout the entire sandboxing process—using both passive and active analysis to adaptively learn new malware behaviors. Unknown objects are submitted to FortiSandbox from Security Fabric-integrated products—both Fortinet and non-Fortinet solutions (with the latter including Fabric-Ready Partners like Carbon Black, SentinelOne, Ziften, and STIX 2.0). FortiSandbox monitors the behavior of an object in a contained environment to uncover the full attack life cycle—including sandbox evasion, registry modifications, outbound connections to malicious IP addresses/URLs, infection of processes, file system modifications, and suspicious network traffic.

FortiSandbox received a Recommended from NSS Labs in its "Breach Prevention System" by achieving an overall security effectiveness of 97.8% while offering the lowest three-year TCO.

Certified performance and protection. NSS Labs' "Breach Prevention Systems" report focuses on both detecting and blocking of exploits, advanced malware, and evasions, which are critical in reducing the risk of breaches. This test helps emphasize the importance in the automation of the advanced threat response cycle of prevent-detect-mitigate across a number of threat vectors including web, email, and endpoint. The different integrated components of breach protection NSS Labs tested from Fortinet included FortiSandbox, FortiGate, and FortiClient. The combination earned a Recommended recognition by achieving an overall security effectiveness of 97.8% while offering the lowest three-year total cost of ownership (TCO).[6]

FortiSandbox has also been validated and recommended in other respected tests such as ICSA Labs' ATD certification[7] and NSS Labs' "Breach Detection Systems" tests.[8]

Automated Detection and Protection Against Zero-day Threats

An integrated sandbox that shares intelligence with other in-line security controls helps to eliminate manual processes via automated responses. This not only improves security but also reduces the burdens on human staff and lowers operating expenses (OpEx). FortiSandbox meets all these requirements:

Accelerated threat awareness. Once a threat is detected in AI-powered analysis, FortiSandbox generates alerts based on an object disposition and shares actionable indicators of compromise (IOCs) intelligence in real time to other in-line controls across the security architecture to block threats in a coordinated fashion. Additionally, integrated seamlessly into FortiSandbox, FortiGuard Labs threat intelligence helps to fortify protection via global anti-malware signatures to both automatically detect and protect against emerging and zero-day threats.

Automation-driven security responses. Security Fabric integration allows FortiSandbox to then unlock an automated prevent-detect-mitigate life cycle across other in-line security controls. Many outdated sandboxing solutions only include threat detection capabilities, which limits an effective real-time threat response (i.e., protection against newly discovered zero-day threats). This effectively slows down security processes by requiring additional manual labor from staff for things like alert analysis, investigation, malware categorization, and reporting in order to ensure coordinated, up-to-date defenses across other parts of the security architecture. This increases both OpEx and exposure windows to a potential breach.

Simplicity, Flexibility, Scalability, and Cost

Complexity is the enemy of security. Security teams that rely on multiple, disaggregated security products from various vendors are typically forced to learn nonstandard security languages. Each solution may have its own unique language to report a potential threat. Alerts describing the same threat must be manually translated and mapped by the security operations (SecOps) team to understand the scope of a problem. This requires the dedicated attention of an experienced SecOps analyst while lengthening the time it takes to investigate and mitigate a potential attack.

And as networks continue to grow and organizations expand adoption of digital innovations, their sandboxing needs must be able to keep pace in terms of performance, scalability, deployment form factors, licensing flexibility, and (perhaps most of all) costs.

Solution simplicity. FortiSandbox addresses the problem of multiple security languages through the adoption of the MITRE ATT&CK framework. This establishes a universal security language for categorizing all malware techniques in an easy-to-read matrix as part of threat mapping and reporting—which helps security architects accelerate threat management and response processes.

FortiSandbox also supports inspection of multiple protocols in a single, unified solution to help simplify infrastructure, centralize reporting, improve threat-hunting capabilities, and reduce costs—capital investment (CapEx) as well as OpEx. Other vendors may require up to four separate sandboxes to provide comparable protection across the extended business infrastructure. Other products may also have limited deployment options that impact the ease of setup and expansion due to business growth.

FortiSandbox uses the same language as the MITRE ATT&CK framework for categorizing malware techniques, which accelerates threat management and response.

Flexible form factors. As FortiSandbox is available in multiple form factors (e.g., on-premises appliance, VM, hosted cloud, public cloud), it supports growth and scalability while covering the entire network attack surface. For example, an organization that purchases a sandbox that only comes in an on-premises form factor will be forced to start over from scratch to extend sandboxing protection into future or current cloud environments (costing time, money, and greater potential risk exposure). And if they want to move to a hybrid sandbox deployment, they have no other alternative.

Scalability and clustering. To handle the scanning of a high number of files concurrently, multiple FortiSandbox devices can be used together in a load-balancing high-availability (HA) cluster.[9] FortiSandbox supports up to 100-node sandbox clusters. Here, clusters can be connected to one another, which means homogenous scale is limitless, enabling FortiSandbox to keep up with high traffic throughput and to remain ahead of potential or planned additions to the business in the future.

Low TCO. Next-generation sandboxing delivers better security for modern networks, as well as better value for new or replacement sandboxing devices. Current testing shows that FortiSandbox provides outstanding performance, value, and investment protection with a low three-year TCO.[10]

Detect and Prevent Breaches with AI-based FortiSandbox

As new malware variants multiply and the risk of zero-day attacks makes breaches an eventuality for organizations of all sizes, security architects should look to replace outdated sandboxing devices with a solution that is designed for current needs. As part of the Fortinet Security Fabric, FortiSandbox provides an integrated, third-generation sandbox that allows security leaders to both detect and prevent breaches through true AI-based security effectiveness, manageability, scalability, and cost.

1 "The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study," Accenture and Ponemon Institute, March 6, 2019.

2 "The Security Architect and Cybersecurity: A Report on Current Priorities and Challenges," Fortinet, November 12, 2019.

3 "2019 Cost of a Data Breach Report," Ponemon Institute and IBM Security, July 2019.

4 "MITRE ATT&CK," MITRE, accessed November 25, 2019.

5 "NSS Labs Announces 2018 Breach Detection Systems Group Test Results," NSS Labs, October 11, 2018.

6 Jessica Williams, et al., "Breach Prevention Systems Test Report," NSS Labs, August 7, 2019.

7 "Q2 2019 Advanced Threat Defense (ATD) Testing Report," ICSA Labs, July 9, 2019.

8 Dipti Ghimire and James Hasty, "Breach Detection Systems Test Report," NSS Labs, October 19, 2017.

9 "Technical Note: FortiSandbox HA-Cluster Explanation and Configuration," Fortinet, accessed November 25, 2019.

10 Jessica Williams, et al., "Breach Prevention Systems Test Report," NSS Labs, August 7, 2019.

FORTINET

www.fortinet.com

December 3, 2019 2:34 PM

483783-0-0-EN

Macintosh HD:Users:bhoulihan:Documents:_Projects:White Paper:wp-third-generation-sandboxing Folder:rounds:wp-third-generation-sandboxing-120319-235pm