FORTINET

Third-generation Sandboxing Delivers AI-based Breach Prevention

Table of Contents

FORTINET

Executive Overview

As a result of a rapidly evolving threat landscape, breach frequency has grown by two-thirds while the total cost of cyber crime per company increased by 72% over the last five years.[1] Malware now employs advanced tactics like polymorphism and artificial intelligence (AI) to avoid detection by outdated security tools—such as previous-generation sandbox devices. In order to prevent data breaches resulting from unknown threats, organizations must reevaluate their approach to sandboxing. The answer is third-generation sandbox solutions, which can support automated defenses across an organization through security integration, real-time threat-intelligence sharing, advanced AI capabilities featuring static and behavior analysis, as well as a common security language that simplifies management and reporting functions.

Outdated Sandboxes Leave Organizations Vulnerable to Breaches

Each day, the threat landscape expands in terms of the number of unique attacks and the sophistication with which they execute their objectives. As evidence, the average cost of a data breach last year grew to $3.92 million. This was due in no small part to the fact that it takes an average of 279 days to identify and contain a successful attack.[2] Today's latest generation of polymorphic malware utilizes AI to spontaneously create new, customized attacks.[3] On any given day, up to 40% of new malware is now zero day or previously unknown,[4] making it that much harder for security systems to detect and repel attacks.

The limitations of outdated security solutions (including first- and even second-generation sandboxing devices) to cover every new risk have forced many security architects to patch defenses with an assortment of point security products from different vendors. As a result, security teams must learn multiple nonstandard security languages and adopt manual workflows for management and reporting functions—not to mention manage multiple security consoles. This complexity typically lacks comprehensive threat-intelligence sharing, which inhibits real-time, automated responses to threats across the organization.

When this is coupled with the fact that security architects must take measures to thwart zero-day and other unknown attacks to prevent breaches before they occur, the challenge becomes even greater. In that pursuit, security architects should implement a third-generation sandbox solution that delivers advanced AI capabilities as well as integration with their organization's broader security architecture.

Sandbox Evolution

- **First-generation sandboxes** were stand-alone physical devices used to identify advanced threats.
- **Second-generation sandboxes** integrate with other devices across the broader security architecture to detect advanced threats across an organization.
- **Third-generation sandboxes** now also include robust AI capabilities that can perform both static and behavior analysis.

What Makes for a Third-generation Sandbox?

Despite the fact that their protections may be out of date and extremely limited, there is still a wide variety of first- and second-generation sandboxes on the market. It can be very difficult for security architects to tell the difference. In essence, an effective third-generation sandboxing solution must include three critical capabilities:

- It must address the evolving threat landscape by leveraging **AI that performs both static and dynamic analysis** to improve detection efficacy of zero-day threats even further.
- It must utilize a standardized framework that categorizes all malware techniques in an easy-to-read matrix as part of the reporting in a **universal security language** (such as the MITRE ATT&CK framework).
- It must be able to **share threat intelligence across a fully integrated security architecture** and offer automated breach-protection responses—a requisite for combating zero-day threats in real time.

Beyond those third-generation qualifiers, security architects should evaluate the effectiveness of a sandboxing solution in five areas.

Security Effectiveness

A sandbox's response time to any security event must be instantaneous in order to minimize risk exposure. In this case, evaluation of a solution should be based not only on its effective threat-detection rate but also on the time-to-detect metrics that directly impact return on investment (ROI) for enterprises.[5] Faster identification of threats and containment of breaches yield lower recovery costs.

A sandbox's ability to block and report on successful infections in a timely manner is critical to maintaining the security and functionality of the monitored network.[6]

Far too often, organizations must choose between a security solution's ability to keep the network safe and the network's ability to support high-performance throughput of traffic. But a balance of both is necessary for today's evolving infrastructure. A sandbox's security effectiveness should be evaluated within the context of its performance and vice versa.[7] It also needs to apply threat intelligence from global research, locally shared contextual awareness, and (most importantly) its own AI-enabled analytical tools to expose unknown threats.

With all this in mind, organizations need to look for sandboxes with recommended ratings from third-party testing organizations (e.g., NSS Labs) for security effectiveness and time to detect. As such, to gauge the effectiveness of a potential sandbox acquisition, security architects should consider:

- **Integration.** The sandbox should be connected to other security solutions across the organization's broader defensive architecture for better visibility and manageability. Sandbox integration also unlocks its ability to instantly share threat information in support of automated threat-mitigation responses across the organization's extended security ecosystem. This in turn can help prevent breaches from occurring.
- **Advanced AI analysis.** Most sandboxes on the market today lack any AI capabilities at all. Even in cases where a sandbox may claim to use AI, it may only be able to perform static analysis. But an effective, truly AI-enabled sandboxing solution must be able to apply both static and dynamic analysis to expose indicators of compromise (IOCs) during malware execution to spot both known and new behaviors. And as a new behavior appears with greater frequency, AI analysis can automatically track and promote its relevancy as a critical security concern.
- **Detection + prevention.** Detecting an effective malware intrusion should happen quickly and accurately to help administrators contain the infection and minimize impact on the network.[8] But security architects need to look for a sandbox that supports breach prevention as well as detection capabilities. Previous-generation sandboxing solutions provide threat detection. But to help reduce the number and cost of breaches, sandboxes must also now help prevent breaches before they occur. A sandbox's preventative ability to block and report potential threats in a timely manner is now critical.
- **Homegrown technologies.** The most effective sandboxing solutions available tend to be based on original technologies developed in-house. These companies typically keep their products up to date, fully patched, and armed with the latest and best features for the current state of the threat landscape.

Simplified Operations

More than half (57%) of CISOs named "too many manual processes" as a top challenge—followed by "missed malware and attacks."[9] Previous-generation sandboxes typically require more manual administration, which adds to the strain on limited security team resources. However, at the same time, a majority (65%) of organizations report a shortage of cybersecurity staff.[10] Beyond the ongoing skills shortage, security leaders also typically face tight budgetary constraints, which limits their ability to scale resources as needed.

- **Automated security management.** An integrated sandbox that shares zero-day intelligence to other in-line security controls enables automatic protection across the network. This robust security automation helps to eliminate manual processes—which eases the burden on human staff while improving security and reducing operating expenses (OpEx).
- **Automated malware reporting.** An integrated approach to sandboxing supports reporting in a universal security language by using a unified framework for categorizing all malware techniques in an easy-to-read matrix. This simplifies security management while obviating the need for manual processes—namely, investigation and translation of alerts and contextual information surrounding an incident into actionable threat-mitigation processes. One such universal language is the MITRE ATT&CK—a globally accessible knowledge base of adversary tactics and techniques based on real-world observations with broad adoption in the private sector, in government, and in the cybersecurity product and service community.[11]

CISOs name "too many manual processes" and "missed malware attacks" as their top security challenges.

38%

of organizations are currently taking effective advantage of automation, artificial intelligence, and machine learning—which exposes them to advanced threats that traditional security models cannot address.[12]

Scalability

A third-generation sandbox should support scaling to accommodate increasing traffic and infrastructural changes that result from digital innovation adoption. It should offer ample performance capacity, flexible licensing, and multiple deployment options. Core capabilities include:

- **Clustering.** Security architects should look for a solution that supports clustering—including a sufficient number of nodes per cluster to support network growth, increasing traffic demands, and expanding security needs in the future.
- **Deployment.** Sandboxing solutions that go beyond "on-premises only" form factors—including virtual machine (VM) and cloud-based options—provide flexibility for where and how sandboxing can be deployed. For example, a cloud-based sandbox form factor can leverage the elastic nature of Infrastructure-as-a-Service (IaaS) for greater operational scalability across distributed infrastructures.

Cost Controls

Many sandbox solutions require multiple devices and/or subscriptions, which lead to a high total cost of ownership (TCO). Following are key areas of consideration:

- **Consolidated protection.** A third-generation sandbox should cover the entire attack surface (network, endpoints, web, email, and cloud) without additional licenses and costs. It also should be able to integrate with other critical solutions across the security ecosystem—such as a next-generation firewall (NGFW)—to uncover attacks that may be hiding in secure sockets layer (SSL)/transport layer security (TLS) encrypted traffic. Sandboxes without this sort of security integration may require the purchase of separate devices for encryption/decryption capabilities—increasing capital expenses (CapEx) and operational complexity.
- **Cost per protected Mbps.** Cost remains a concern for most organizations, and sandboxes need to reduce cost per protected Mbps (as measured by third-party testing organizations like NSS Labs) and eliminate supplemental subscription costs.

Implementation of sandboxing can be complex, with numerous factors impacting the overall cost of deployment, maintenance, and upkeep.[13]

AI-based Security Designed for the Evolving Threat Landscape

As sophisticated AI-based malware variants continue to multiply and the risk of zero-day threats increases the likelihood of a breach, organizations must consider replacing outdated sandboxes with a solution designed for today's threat landscape. An integrated, third-generation sandbox offers security leaders the ability to both detect and prevent breaches through better 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] "2019 Cost of a Data Breach Report," Ponemon Institute and IBM Security, July 2019.

[3] "AI-driven Cyber Crime Brings New Challenges to CISOs: Too Fast, Too Agile, Too Dangerous for Traditional Security Approaches," Fortinet, June 21, 2019.

[4] According to internal data from FortiGuard Labs.

[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] Ibid.

[8] Ibid.

[9] "The CISO and Cybersecurity: A Report on Current Priorities and Challenges," Fortinet, April 26, 2019.

[10] "Strategies for Building and Growing Strong Cybersecurity Teams: (ISC)^2 Cybersecurity Workforce Study, 2019," (ISC)^2, 2019.

[11] "MITRE ATT&CK," MITRE, accessed November 25, 2019.

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

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

www.fortinet.com

483924-0-0-EN

December 4, 2019 4:23 AM

eb-third-generation-sandboxing-delivers-ai-based-breach-prevention-v1.2