Has Your Network Outgrown Its First-generation Sandbox?
Executive Overview

Digital innovations are introducing new network vulnerabilities, while the threat landscape simultaneously expands and evolves. As a result, the average number of security breaches has increased by 67% over the last five years. The latest generation of sandboxing solutions can provide broad protection through advanced capabilities, native integration of in-line security controls, and accelerated responses to advanced threats. But many outdated sandboxes are still on the market—ones that lack the latest features for protecting evolving networks (such as artificial intelligence [AI]) or that require multiple devices, licenses, or subscriptions to address key functions (such as automated breach prevention).

Sandboxing Is a Requisite Part of Breach Prevention

There are more than 975 million malware files in existence today. Many advanced threats are now multivector, concurrently targeting different points on the expanded network attack surface in coordination. All at once, they can attack a full spectrum of endpoint devices and applications across on-premises and cloud environments. Some exploits have become “living organisms” that employ polymorphic malware to circumvent the latest signatures and patches. Most malware now employs some form of polymorphism—and next-generation polymorphic malware built around AI can spontaneously create entirely new, customized attacks. Botnet swarms can be transformed into compute nodes for creating new malware variants at machine speed and are especially effective when coupled with Malware-as-a-Service (MaaS) threat campaigns that help sustain automated attacks.

In addition to the accelerating threat landscape, networks themselves are undergoing a period of radical digital transformation (DX). Almost 80% of organizations are introducing digitally fueled innovation faster than their ability to secure it against cyberattacks. In response, security architects often resort to covering individual risk exposures with an assortment of point security products from different vendors. As a result of having various security solutions deployed, security architects face the burden of having to learn multiple nonstandard security languages. This solution complexity also introduces disparate threat-intelligence streams that can hinder the security team’s ability to effectively apply protections across the dynamic attack surface. And this directly increases the likelihood of a security incident or a breach.

Breach frequency has grown by 67% over the last five years—and the total cost of cybercrime per company increased by 72% over that same period to reach a new average high of $13 million. With outsiders responsible for more than 69% of successful breaches, it is time to rethink how a sandbox solution should function within a larger security architecture designed for digitally transforming networking environments. Automated defenses enabled by sandboxing capabilities are gaining steam as a countermeasure. At a moment when most organizations want to prevent data breaches (rather than just detecting them after the fact), the time has come for a robust sandbox renaissance.
Four Core Challenges of Traditional Sandboxing Solutions

Unfortunately, not all sandboxing solutions can keep pace with today's demands—especially first-generation or "traditional" sandboxes with limited performance and outdated capabilities (such as the ability to integrate into a broader security architecture, or breach prevention capabilities). The following four main problem areas of traditional sandboxing solutions suggest what security architects need to look out for when adding or upgrading a sandbox in an enterprise.

1. Security Effectiveness

Many popular sandboxing solutions are falling behind in security effectiveness in an era when it is even more critical to shrink detection and intrusion windows. The response times to any security event must be instantaneous to minimize risk exposure. A product'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.11

Organizations are often forced to choose between a security solution's ability to keep the network safe from all forms of attack, and the network's ability to support high-performance throughput of traffic. Traditional sandbox solutions can impact both network performance and security effectiveness due some critical shortcomings:

- **Lack of integration.** Malware is designed to detect the presence of a virtual sandbox and evade discovery—rendering first-generation sandbox technologies obsolete. Some security architects try to avoid this problem by deploying multiple stand-alone sandboxing technologies. This approach, however, greatly increases configuration complexity, administrative overhead, and capital expenditure (CapEx) costs. Most importantly, stand-alone, "point-only" security products cannot be flexibly integrated into a broader security architecture—which inhibits both visibility and manageability.

- **Lack of artificial intelligence.** First- and second-generation sandboxes are typically lacking when it comes to the latest tools for exposing previously unknown threats—such as AI and machine learning (ML). Outdated sandboxing solutions lack true AI capabilities—including both static analysis and behavioral analysis of indicators during malware execution to spot known threats and learn to spot new ones.

- **Detection + prevention.** Detecting an effective malware intrusion should happen quickly and accurately to help administrators contain the infection and minimize impact on the network.14 Once a threat is detected, organizations need to automate breach protection responses to address both the security operations talent shortage and also to shrink the window of exposure where sensitive data may be exfiltrated post-breach. While all sandboxing solutions include some kind of threat detection, sandboxes also should help prevent attacks before they reach the network interior and sensitive data. Here, a sandbox's preventative ability to block and report potential threats in a timely manner is critical.

- **Legacy technologies.** Many traditional sandboxes were designed on commodity-grade technologies licensed by OEMs to multiple vendors. In the event that a contract expires or licensor is slow to update their original code, organizations may be left with an ineffective product and little recourse to resolve the situation.

---

Up to 40% of new malware detected on a given day is now zero day or previously unknown.10

More than half (54%) of security architects report challenges defending against zero-day and unknown threats.12

Automation, artificial intelligence, and machine learning are only being taken up by 38% of organizations. This not only represents a lost opportunity but it exposes organizations to advanced threats that traditional security models cannot address—or keep up with.13
2. Administration Overhead

Cybersecurity teams typically face tight budgetary constraints and a worldwide shortage of available skilled staff. Security teams are stretched and they need to improve productivity wherever possible. Many outdated sandboxing products require manual administration, which adds to the strain on human resources. In fact, 57% of CISOs named “too many manual processes” as one of their top challenges—followed by “missed malware and attacks.” Following are key considerations:

- **Manual security management.** Outdated sandboxes that lack integration cannot share zero-day intelligence to other in-line security controls that enables them to automatically apply protection across the network. This lack of robust security automation means that manual processes must be used to perform these controls, which increases the burden on human staff.

- **Manual malware reporting processes.** Disaggregated security that relies on multiple point solutions creates complexity in terms of multiple, nonstandard languages in use for malware reporting. This creates a burden on security teams having to learn the various solution languages, increases manual workflows, and distracts staff from other critical security tasks.

3. Scalability

Many traditional sandboxes also struggle with scaling to accommodate increasing traffic or infrastructural changes resulting from DX initiatives. Lacking the latest technical capabilities may require the purchase of additional devices, which adds CapEx costs, along with infrastructural complexity that increases operating expense (OpEx) and cyber risk to the process of sandbox scaling. Insufficient performance capacity, architectural limitations, and physical deployment limits are also common scalability concerns for many sandboxing solutions.

- **Clustering.** A sandbox that lacks a sufficient number of nodes per cluster limits the solution’s ability to support network growth, which increases traffic demands and expands security needs in the future. And many sandbox solutions on the market do not have an architectural foundation to support any clustering capabilities at all.

- **Form factors.** Ease of integration is the second most important consideration for U.S. enterprises during security product purchase decisions (after cost). Outdated solutions with “on-premises only” form factors may limit the options of where and how sandboxing can be used. Also, solutions that use physical connectors—such as test access point (TAP) network components—can significantly increase the time and cost to deploy sandboxing across an organization.

4. Total Cost of Ownership (TCO)

Implementation of sandboxing can be complex, with numerous factors impacting the overall cost of deployment, maintenance, and upkeep. Many sandbox solutions require multiple devices and/or subscriptions, which leads to a high TCO. Following are key areas of consideration:

- **Attack surface.** Many previous-generation sandboxes cannot cover the entire attack surface (network, endpoints, web, email, and cloud) without additional licenses and costs. They also may lack integrated access to other important security solution functions, such as secure sockets layer (SSL) and transport layer security (TLS) encryption inspection.

- **Cost per protected Mbps.** Organizations should look for replacement sandboxes that reduce cost per protected Mbps (as measured by third-party testing organizations like NSS Labs) and eliminate supplemental subscription costs.
To Avoid Sandbox Problems, Choose a Next-generation Solution

Previous-generation sandboxes cannot keep up with the speed and sophistication of today’s threat landscape, as well as the transformative changes to network infrastructures brought on by increasing digitalization. At the same time, sandboxing remains a critical need within an integrated security architecture. When evaluating an existing sandbox, security leaders should consider security effectiveness, administrative overhead, scalability, and cost of the solution as factors for upgrading to a more fully featured, third-generation solution.

2 Ibid.
10 According to internal data from FortiGuard Labs.
17 “Strategies for Building and Growing Strong Cybersecurity Teams: (ISC)² Cybersecurity Workforce Study 2019,” (ISC)², October 2019.