DETERMINING IF YOU'VE OUTGROWN YOUR FIRST-GEN SANDBOX

SANDBOXING IS A REQUISITE PART OF ADVANCED THREAT PROTECTION

In a recent report, cyber crime was shown to cost the annual global economy over $450 billion, with over two billion personal records stolen worldwide and over 100 million medical records taken from United States citizens alone.[1] With external threat actors responsible for more than 90% of security incidents,[2] it is time to rethink how a sandbox solution should function within a larger defensive architecture designed for today's networking environments.

There are more than 700 million malware files in existence today.[3] One of the latest trends includes the adoption of Malware-as-a-Service and artificial intelligence (AI) to automate extremely effective attacks. These are some of the primary reasons why automated defenses enabled by sandboxing capabilities are gaining steam as a countermeasure. The global network security sandbox market is expected to reach $40.48 billion by 2025.[4]

In addition to the accelerating threat landscape, networks themselves are undergoing a period of radical digital transformation. The widespread deployment of cloud technologies, for example, has created a need for integrated security solutions that share intelligence from end to end across distributed networks. Cloud adoption places increasing bandwidth constraints on the edges of networks. As companies add more cloud services and environments to their increasingly distributed network infrastructures, they also need to be able to scale security (such as sandboxing) into these environments to cover newly exposed vulnerabilities.

There are more than 700 million malware files in existence today.[3]

Each of these factors, along with the declining purchase prices of sandbox devices combined with a rise in organizations wanting to prevent data breaches (rather than just detecting them), indicates that the time is right 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can keep pace with today's demands—especially first-generation or "traditional" sandboxes with limited performance and outdated capabilities (such as the ability to integrate into a broader security architecture, or advanced threat prevention capabilities). The following four main problem areas of traditional sandboxing solutions suggest what to look out for when adding or upgrading a sandbox in an enterprise.

SECURITY EFFECTIVENESS

Many popular sandboxing solutions are falling behind in security effectiveness in an era when it's 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.[5]

In this case, evaluation of a solution should be based on not only its effective threat detection rate but also the time-to-detect metrics that directly impact ROI for enterprises.[6] Faster identification of threats and containment of breaches yield lower recovery costs.

Organizations are often forced to choose between security's ability to keep the network safe from all forms of attack 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] 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. Additional capabilities that affect a sandbox's effectiveness include:

- **Integration.** Avoid standalone, "point-only" products that can't be flexibly integrated into a broader security architecture for better visibility and manageability. Malware is designed to detect the presence of a virtual sandbox and evade discovery—rendering first-generation sandbox technologies obsolete. Some IT managers try to avoid this problem by deploying multiple sandboxing technologies. But this, in turn, greatly increases configuration complexity, administrative overhead, and costs.[8]
- **Threat Intelligence.** As an extension of integration, sandboxes need access to real-time intelligence backed by a solid threat research team (not just third-party threat feeds) to be aware of the very latest emerging problems worldwide. The sandbox should work as a zero-day hub, sharing the latest information out to other security tools and elements across the architecture for coordinated, automated responses to broad attacks. When the different solutions in the security architecture are integrated and share information, they become greater than the sum of their parts.[9]
- **Detection + Prevention.** Detecting an effective malware intrusion should happen quickly and accurately to help administrators contain the infection and minimize impact on the network.[10] 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. A sandbox's preventative ability to block and report potential threats in a timely manner is critical. Here, organizations need to look for a solution that supports breach prevention (sometimes referred to as Advanced Threat Prevention or ATP) as well as detection capabilities.
- **Homegrown Technology.** Avoid sandboxes designed on commodity-grade technologies licensed by OEMs to multiple vendors. In the event that a contract expires or a licensor is slow to update their original code, organizations may be left with an ineffective product and little recourse to resolve the situation. 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.

ADMINISTRATION OVERHEAD

IT security teams typically face tight budgetary constraints and a worldwide shortage of available skilled staff. For example, 45% of organizations claim to have a problematic shortage of cybersecurity skills.[11] 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. Following are key considerations:

- **Simplify Security Management.** Look for a sandbox that can share zero-day intelligence out to all in-line security controls that apply appropriate protections automatically across the network. In addition to an improved security posture, this helps eliminate manual processes and reduces management burden.

Security teams are stretched and they need to improve productivity.

45% of organizations claim to have a problematic shortage of cybersecurity skills.[11]

- **Deployment and Form Factors.** Ease of integration is the second most important consideration for U.S. enterprises during security product purchase decisions (after cost).[12] 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 TAP network components) can significantly increase the time and cost to deploy sandboxing across an organization.

SCALABILITY

Many traditional sandboxes also struggle with scaling to accommodate increasing traffic or infrastructural changes resulting from digital transformation initiatives (such as expansion into different cloud environments). Lacking the latest technical capabilities may require the purchase of additional devices, which adds cost and complexity to scaling a sandbox solution. Insufficient performance capacity, prohibitive licensing, and physical deployment limits are also common scalability concerns.

- **Licensing.** In addition to the physical problems of outdated connectors and limited form factors, prohibitively complicated and expensive licensing models can impact a solution's ability to affordably deploy as needed across an expanding environment.
- **Nodes per Cluster.** Look for a sandbox that supports a high number of nodes per cluster to anticipate network growth, increased traffic, and expanding security needs into the future.

COST

Implementation of sandboxing can be complex, with numerous factors impacting the overall cost of deployment, maintenance, and upkeep.[13] Many sandbox solutions require multiple devices and/or subscriptions, which leads to a high total cost of ownership (TCO). Following are key areas of consideration:

- **Attack Surface.** Whether evaluating an existing solution, looking to upgrade, or adding a sandbox for the first time, consider the completeness of the solution and all related expenditures. Questions to ask include: Does the sandbox cover the entire attack surface (network, endpoints, web, email, and cloud) without additional licenses and costs? Does it anticipate increasingly important 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.

MOVING BEYOND TRADITIONAL, FIRST-GENERATION SANDBOXING

Previous-generation sandboxes can't keep up with the speed and sophistication of today's threat landscape, or transformative changes to network infrastructures brought on by increasing digitalization. At the same time, sandboxing remains a critical need within an integrated security architecture.

[1] "The Hiscox Cyber Readiness Report 2017," Hiscox Insurance Company Inc., accessed March 21, 2018.
[2] "2017 Verizon Data Breach Investigations Report (DBIR) from the Perspective of Exterior Security Perimeter," Verizon, July 26, 2017.
[3] "Malware," AV-TEST, April 9, 2018.
[4] "Network Security Sandbox Market Analysis By Solution, By Services (Professional Consulting,Maintenance, Subscription), By Application, By Region, And Segment Forecasts, 2014 – 2025," Grand View Research, November 2017.
[5] "Breach Prevention Systems Test Report," NSS Labs, December 13, 2017.
[6] "NSS Labs Announces 2017 Breach Detection Systems Group Test Results," NSS Labs, October 19, 2017.
[7] "Breach Prevention Systems Report," NSS Labs, December 13, 2017.
[8] "Nick Ismail, "Is your sandbox strategy keeping you safe?" Information Age, July 6, 2017.
[9] Jason Pappalexis, "Breach Prevention Systems and the Importance of Interoperability," NSS Labs, February 6, 2018.
[10] William Dean Freeman and Jessica Williams, "Breach Prevention Systems Test Report," NSS Labs, December 13, 2017.
[11] Jon Oltsik, "Cybersecurity skills shortage creating recruitment chaos," CSO, November 28, 2017.
[12] Jason Pappalexis, "Breach Prevention Systems and the Importance of Interoperability," NSS Labs, February 6, 2018.
[13] "Breach Prevention Systems Test Report," NSS Labs, December 13, 2017.

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
905 rue Albert Einstein
06560 Valbonne
France
Tel: +33.4.8987.0500

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA HEADQUARTERS
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
Tel: +1.954.368.9990

April 26, 2018 8:23 PM