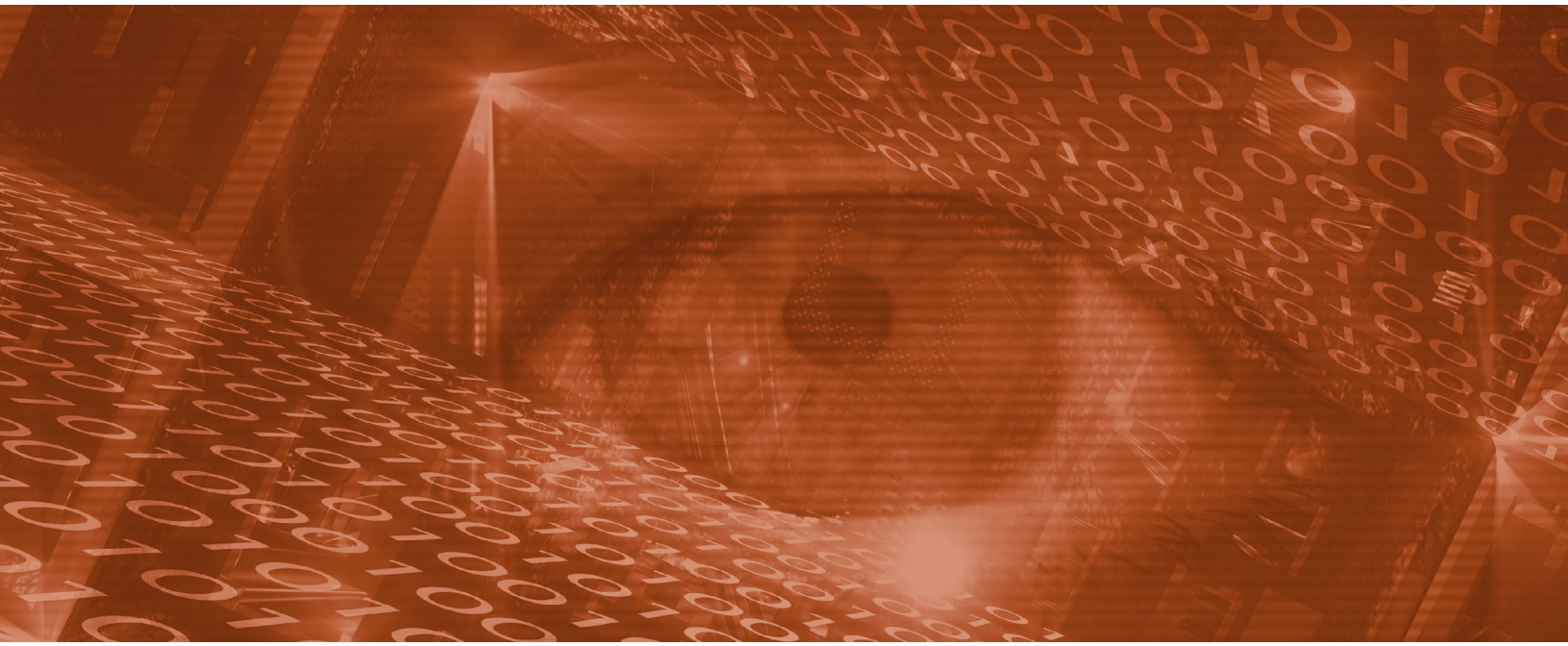
MAPPING THE REQUIREMENTS OF NEXT-GENERATION SANDBOXING TO ADDRESS THE ADVANCED THREAT LANDSCAPE



EXECUTIVE SUMMARY

As network infrastructures expand to include new technologies and services for greater business agility, security must also evolve to anticipate ever-increasing vulnerability to new, undiscovered threats. Sandboxing is a critical part of the security architecture for detecting and preventing threats before they can impact a business. But many sandbox solutions—old and new—aren't well-suited to the current demands of modern networks. When adding or replacing a sandbox, organizations should focus on solutions that offer a few specific next-generation features and capabilities.

WHAT TO SEEK IN A SANDBOXING SOLUTION

Driven by the digital transformation (DX) of network infrastructures, a rapidly changing threat landscape, and new business requirements, sandboxing technologies have had to evolve and provide next-generation capabilities to keep pace. But there are still many outdated solutions on the market that don't self-identify as "first generation" or that have incomplete functionality for addressing the requirements of the evolving threat landscape. It's incumbent on buyers to know what they need from a sandbox to fully complement their present and future security architecture.

For organizations that are evaluating their current sandboxing solution, the following are some of the key next-generation sandboxing attributes they need to ensure are included to truly address the advanced threat landscape:

1. Integration and Automation

Many sandboxing technologies reside in their own silos as isolated "point" devices—which means that they can't share threat intelligence with other security elements across your organization or benefit from that kind of information in return.

This is problematic because sophisticated threats often target a broad attack surface when trying to breach an organization's network. Or they may be so new that they're missing from third-party evaluation tests. To help foil these kinds of assaults, a sandbox that connects with the broader security architecture is required. Specifically, integration enables your solution to share zero-day intelligence out to all inline security controls that apply appropriate protections automatically. This helps eliminate manual processes, shrinks response windows, and reduces management burden—especially for organizations facing a shortage of skilled security staff.

Seamless "plug-and-play" integration also enables transparent visibility and simplified security management as well as fast and easy sandbox deployment. Avoid devices that must be connected through TAP network components, which creates lengthy deployment cycles and incurs ongoing management time whenever network ports or virtual local area networks (VLANs) change.

2. Detection and Prevention

Many sandboxing solutions only offer detection capabilities. But the inclusion of advanced threat prevention (ATP) is critical for minimizing your organization's exposure to threats. According to third-party test provider NSS Labs, when it comes to breach prevention systems, the windows for threat detection and breach prevention are intertwined. Per the latest NSS Labs breach prevention system report, "The ability of the product to block and report on successful infections in a timely manner is critical to maintaining the security and functionality of the monitored network. Infection and transmission of malware should be reported quickly and accurately, giving administrators the opportunity to contain the infection and minimize impact on the network."[1]

To ensure that the sandbox solution you're evaluating has true detection and prevention capabilities, you should vet them through third-party certifications and current recommended ratings from trusted, outside testing organizations. Areas of evaluation should include total cost of ownership (TCO), time to detect, evasions, and security effectiveness in both breach detection and breach prevention. Avoid solutions that receive warnings or other non-recommended ratings and are missing from breach detection system or breach prevention system tests altogether.

3. SSL/TLS Inspection

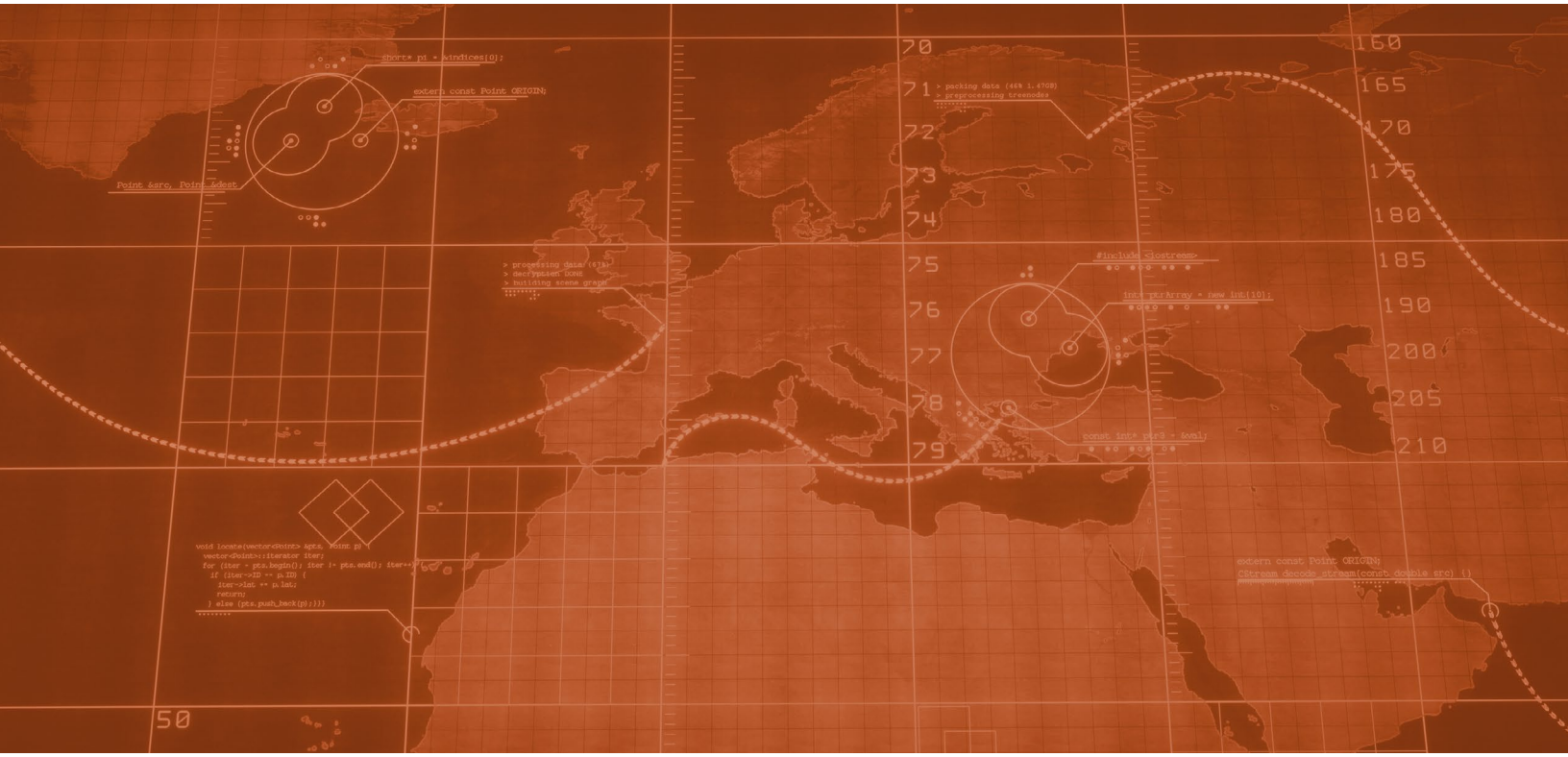
To comply with industry regulations, many enterprises are required to protect certain types of sensitive data using secure sockets layer (SSL) or transport layer security (TLS) encryption. Encrypted content accounts for as much as 60% of network traffic today, and that volume continues to grow annually.[2] But cyber criminals can also use encryption to conceal malware and ransomware from traditional enterprise security solutions.

But this is where many sandboxing solutions on the market run into problems. Rather, they are dependent on additional third-party appliances to inspect encrypted data. In this instance, security and network leaders should look for a sandbox that can access robust encryption inspection capabilities via integration with existing security controls, such as next-generation firewalls.

4. Scalability

Anticipating growth of your infrastructure is another aspect of how a sandbox fits into the broader security architecture. An ideal solution should support high throughput and scalability for potential or planned additions to the business in the future.

In terms of scalability, a high number of nodes per cluster helps future-proof the sandbox to handle changes that may increase security demands over time. For example, enterprises are now looking to extend sandboxing capabilities into the cloud to take advantage of cloud elasticity. It's a critical requirement for solutions to both scale and offer high availability as enterprise networks naturally expand in the current DX era.



5. Original Technologies

Many sandboxing providers license generic technologies from larger original equipment manufacturers (OEMs) that are used within their products. Since these companies don't own or originate all the contributing hardware and/or software, they remain at the mercy of licensors to keep the product updated, patched, and effective. If the solution provider's third-party license expires or changes before your product reaches its end of life, you could be completely out of luck in maximizing your sandbox investment. Even more troubling, some sandboxes are based on open-source technology—to which malware authors have open and equal access for ease of exploitation.

Look for providers that base their solution designs on original, in-house-developed technologies. Security and network leaders want solutions that are up to date, fully patched, and armed with the latest and best features for the current state of the threat landscape. Solutions that were developed by the provider in-house typically means that you're getting products that will receive continuous advancements, knowledgeable support and training resources, and (most importantly) timely bug and security fixes.

6. Form Factor

Look for a sandbox that comes in multiple form factors. As virtualization and cloud adoption grows, on-premises sandbox solutions will no longer be sufficient for many organizations. In the DX era, organizations need the flexibility to leverage sandboxes across multiple form factors—on-premises, as a virtual machine (VM), and/or in the cloud.

An SMB with a hosted cloud may not want to manage an on-premises sandbox. Having multiple form-factor options also provides a seamless experience when transitioning from one environment to another. For example, an enterprise may be planning to move to the cloud in phases over a three-year period as part of a DX initiative to move internal and external applications and services from the data center to the cloud. In the meantime, they still need to secure assets in their current data center. An on-premises solution can protect their existing infrastructure while supporting a seamless migration into the cloud as needed with consistent protection, configuration, and licenses.

7. Lower your TCO

A modern sandbox should be a unified solution that connects into the broader security architecture. Look for one device, one subscription that will integrate with the other components in your security architecture to cover the entire attack surface (network, endpoints, web, email, and cloud) without additional licenses or costs. Avoid sandboxing that requires multiple devices, licenses, and/or threat intelligence subscriptions.

Compare the price-performance ratio (cost per protected Mbps) of solutions, as calculated in third-party testing. This not only accounts for a sandbox's purchasing and licensing but also operational costs such as staff time spent on solution management, maintenance, logs, and reports.

LOOK FOR "SANDBOX: THE NEXT GENERATION"

There are many outdated or otherwise limited products on the market to avoid. But knowing which features to look for will help you navigate the pitfalls and find the best sandbox for sifting malware and other malicious threats out of your network traffic.

While it might not be explicitly labeled a next-generation solution, a sandbox that's ready to serve the needs of modern networks will include:

- Prevention of advanced threats
- Detection of emerging threats based on proactive threat research/intelligence
- Third-party certifications and testing recommendations
- Encryption inspection support (SSL/TLS)
- A high number of nodes per cluster for scalability
- Original technologies designed by the provider
- Multiple form-factor options
- One device, one license, one subscription

[1] William Dean Freeman and Jessica Williams, "Breach Prevention Systems Test Report: Fortinet Advanced Threat Protection," NSS Labs, December 13, 2017.
[2] See, e.g., J. Michael Butler, "SANS Institute InfoSec Reading Room: Finding Hidden Threats by Decrypting SSL," November 2013; Johnnie Konstantas, "SSL Encryption: Keep Your Head in the Game," SecurityWeek, March 15, 2016.

June 13, 2018 12:37 PM