Choosing a network sandboxing solution is challenging due to the wide array of options available from established security vendors and new entrants. This market guide will help network security managers understand the range of sandboxing technology and deployment options.

Key Findings

- The market for network sandboxing consists of three categories: (1) stand-alone (solutions that have no dependencies on existing security infrastructure); (2) sandboxing as a feature of firewalls, intrusion prevention systems (IPSs) and unified threat management (UTM) devices; and (3) sandboxing as a feature of secure Web gateways and/or secure email gateways.

- The number of sandboxing vendors has grown quickly due to low barriers to entry and high demand. Several vendors have licensed sandboxing technology from OEM providers, and some have added very basic sandboxing capabilities.

- The network sandboxing market is far from mature, and solutions vary widely in functionality (for example, the types of objects that can be analyzed), efficacy and pricing.

Recommendations

Security leaders:

- Implement sandboxing technology if you need to improve perimeter-based inbound malware detection capabilities.

- Evaluate sandboxing-as-a-feature options from your strategic security vendors.

- Evaluate one or more network sandboxing solutions in the stand-alone category. These sandboxes are implemented independently of other security products and services.

- Maximize the breadth of sandboxing coverage allowed by your budget by implementing solutions that analyze a broad set of suspicious objects (for example, executables, files and Web objects) and monitor both Web and email channels.
Market Definition

Network-based sandboxing is a proven technique for detecting malware and targeted attacks. Network sandboxes monitor network traffic for suspicious objects and automatically submit them to the sandbox environment, where they are analyzed and assigned malware probability scores and severity ratings. In "Five Styles of Advanced Threat Defense," Gartner referred to network sandboxing as "payload analysis." Here, we use the more popular "sandbox" term.

Sandboxing technology has been used for years by malware researchers at security companies and even in some large enterprises that are highly security conscious. Traditionally, using a sandbox has been an intensive effort requiring advanced skills. The malware researcher manually submits a suspicious object into the sandbox and analyzes it before flagging it as malware or not. By adding automated features to sandboxing technology (automatically submitting suspicious objects and automatically generating alerts), FireEye became instrumental in moving sandboxing from research labs into enterprise datacenters, a transformation that began around 2010.

Today, many vendors sell sandboxing either as a stand-alone product or as a feature of other security solutions. Several vendors of advanced threat defense solutions that use other primary technologies for detecting threats, such as network protocol analysis, network forensics and some endpoint solutions, use sandboxing technology to further enhance the efficacy of their solutions, although they do not sell sandboxing as a separate feature (see Note 1).

Market Direction

The market for network sandboxing consists of these three categories:

**Stand-alone** — These solutions are implemented independently of other security products. No prerequisite products are required.

**Firewall/IPS/UTM** — Sandbox is an optional feature of an existing network security product. It is commonly implemented in the cloud, with customers paying an annual subscription for the sandboxing service. For example, Palo Alto Networks’ fee-based WildFire service charges a 20% premium for each firewall that contributes suspicious objects to the service (it also offers a more limited version free of charge). If the cost of the firewall is $100,000, customers pay $20,000 per year for this firewall to utilize the WildFire service (multiple firewalls can utilize WildFire, but customers must purchase a license for each firewall that submits objects to WildFire). Other vendors in this category have similar pricing models. Check Point is an exception, since its pricing model is based on the number of files submitted to the cloud infrastructure. Some vendors in this category offer on-premises appliances instead of a cloud-based service, primarily to address privacy concerns, and some vendors offer both on-premises and cloud-based options.

**Secure Web Gateway (SWG)/Secure Email Gateway (SEG)** — Sandbox is offered as an optional feature of these content-centric solutions. The pricing models and the deployment options, cloud-based or on-premises solutions, are similar to the category above.
Two factors account for network sandboxing emerging as the most popular "style" (see "Five Styles of Advanced Threat Defense").

- The rapid growth of FireEye — FY14 revenue growth of 163% (see Note 2) — combined with aggressive marketing campaigns, has contributed heavily to the interest in sandboxing solutions. However, FireEye's solutions are expensive, and this has opened the door for many competitors to enter the market. This research identifies nearly 20 vendors offering sandboxing products/services.

- There is a low barrier to entry for traditional security vendors to add sandboxing as a feature to other products and services, because vendors can license technology from an OEM provider (two examples are Joe Security and Lastline) or build their own using open-source code.

To date, most of the challenges to FireEye's dominance have come from the less expensive cloud-based services of the firewall vendors. However, Gartner expects serious challenges from key vendors in the secure Web gateway market in 2015 and 2016, particularly as Blue Coat and Zscaler ramp up their go-to-market plans.

**Market Analysis**

Several factors distinguish sandboxing solutions. The concept of "feeding content to the sandbox" represents an important architectural difference. Figure 1 shows the three main options for feeding suspicious objects to a sandbox.

The integrated sensor approach (Option A) is where the feeding sensor and the sandbox are integrated in one appliance. With this approach, the sandbox "feeds" itself.

The distributed sensor approach is where the feeding sensors are distributed, and they feed a centralized sandbox. Depending on the implementation, the feeding sensors could be firewalls, IPSs, UTM devices, SWGs, SEGs or dedicated sensors. Some solutions enable endpoints to feed suspicious objects to the sandbox. In Option C, the sandbox is in the cloud and is managed by the vendor. An alternative implementation for a centralized sandbox is for an enterprise to implement a local appliance-based sandbox in one of its own data centers. (Option B).
The following sections analyze the three segments of the sandboxing market:

**Stand-Alone**

Stand-alone sandboxes are implemented independently of other security products. Unlike solutions where sandboxing is a feature of other security products (for example, firewall, IPS, UTM, SWG, SEG), no prerequisite products are required to implement a stand-alone sandbox. Stand-alone sandboxes can use an integrated sensor like FireEye or Trend Micro or distributed sensors like Cyphort or Lastline. In both scenarios, the sandboxes are designed to "feed" themselves without dependency on other security products.

A drawback to the stand-alone approach is the requirement to add new equipment, feeding sensors, to the network. The integrated feeding sensor approach is more expensive, especially for distributed enterprises with many Internet egress points, whereas the distributed feeding sensor approach is typically less expensive, because of the centralized sandbox analysis environment.

Sample Vendors: AhnLab; Cyphort; FireEye; HP; Lastline; Trend Micro; Websense
Firewall/IPS/UTM

All solutions in this category utilize the distributed feeding sensor approach. Implementations are usually cost-effective and easy to deploy, particularly when the feeding sensors (firewalls, IPSs or UTM appliances) are already in place. These devices only need to be configured to "feed" the centralized sandbox.

As noted in the Market Direction section, it’s common for vendors to offer sandboxing analysis as a cloud service (for example, Palo Alto WildFire, Check Point Threat Emulation, Fortinet FortiSandbox). These vendors and others also offer an on-premises appliance as an alternative model to a cloud-based service.

The sandboxing features of firewalls, IPSs and UTM appliances focus on file-based analysis. They are less effective in detecting Web-based exploits, which require the analysis of Web objects, such as JavaScript and HTML. Parsing these objects negatively impacts performance on firewalls, IPSs and UTM devices, which is why many customers disable the feature or do limited (headers only) parsing.

Because these solutions use the distributed sensor approach (Figure 1, Options B and C), bandwidth limitations may restrict the number of objects that they can send to a centralized sandbox. By design, they cannot flood a WAN link with a heavy load of suspicious objects, because the extra traffic may negatively impact network performance. This is especially true for small branches with more limited bandwidth than larger locations.

Intellectual property and privacy concerns apply only to cloud-based sandboxes, which are a common offering among firewall, IPS and UTM vendors. Enterprises that are highly security conscious often choose appliance-based sandboxes over cloud-based sandboxes due to confidentiality concerns related to cloud services.

The ability to terminate and decrypt SSL traffic is an advanced capability that is commonly found in firewalls, IPSs and UTM devices. These solutions have an advantage over those stand-alone sandboxing solutions that do not support the termination and inspection of SSL traffic. However, the performance hit from enabling SSL decryption discourages many organizations from enabling this feature (see "Security Leaders Must Address Threats From Rising SSL Traffic").

Sample Vendors: Barracuda Networks; Check Point Software; Palo Alto Networks; Fortinet; Intel Security-McAfee; WatchGuard

Secure Web Gateway/Secure Email Gateway

Similar to the FW/IPS/UTM category, SWG and SEG vendors utilize the distributed feeding sensor approach to submit objects to a centralized sandbox. Many vendors that offer SWGs and SEGs have added sandboxing as an optional feature to both solutions. This is a cost-effective approach that enables malware detection across email and Web channels.

The bandwidth limitation issues and the concerns about intellectual property and privacy that were noted in the FW/IPS/UTM section above also apply to sandboxing as a feature of SWG/SEG.
solutions. Also, many SWGs support SSL termination, thereby enabling greater visibility into network traffic, although the performance impact on the SWG varies widely.

Sample Vendors:

SWG and SEG (shared sandbox approach) — Intel Security-McAfee, Trend Micro; Websense.

SWG — Blue Coat; ContentKeeper Technologies, iboss Network Security; Zscaler.

SEG — Proofpoint.

Note: FireEye offers a sandboxing appliance and a cloud-based service to analyze email attachments, but it does not offer a SEG. HP and Trend Micro also offer a sandboxing appliance to analyze email attachments.

Technical Evaluation Guidelines

The quality of sandboxing solutions varies widely. Critical capabilities include:

- **The ability to analyze a broad range of suspicious objects** — The most basic sandboxes offer a very limited set of file types that can be analyzed (executables, DDL objects, sometimes PDFs). More advanced sandboxes include the ability to analyze other common files such as Microsoft Office documents, Java, Flash and other file types. The most advanced sandboxes are able to detect Web exploits by analyzing more Web objects, such as JavaScript and HTML elements.

- **Static analysis and other prefiltering techniques** — Many technologies use prefiltering techniques to minimize the number of objects that are fed to the sandbox for further analysis. These techniques include static analysis, antivirus engines, reputation feeds and other approaches to identify malware without requiring a sandbox analysis. Suspicious objects that cannot be identified via prefiltering are analyzed in the sandbox. Prefiltering is an important factor in determining the rate of false positives and false negatives.

- **Comprehensive operating system and application stack** — It is important to detect malware that has been fine-tuned to run only in a specific targeted environment. Comprehensive approaches include regional versions of Windows operating systems (for example, a Chinese version), full Microsoft Office software (not just a Word document reader) and a variety of minor and major versions of the software used to open the suspicious files.

- **Anti-evasion technologies** — These are necessary to counter malware that attempts to detect the presence of a sandbox environment. An example is the use of customized hypervisors, which make it more difficult for malware to detect that it is running in a sandbox environment. A common characteristic of advanced malware is to look for the presence of a hypervisor, which may be a signal that the code is executing in a sandbox. Customized hypervisors are harder to detect and, therefore, harder to evade. However, there is a trade-off to customized hypervisors — they may restrict the sandbox to running a generic version of a desktop environment instead of the enterprise’s "gold" desktop image.
The rate at which objects can be analyzed in the sandbox — This is an important indicator of scalability. One way to measure scalability is to compare the number of objects that the sandbox can analyze per hour. Another important aspect to evaluate is how the sandboxing engine behaves when its queue is full.

A combination of virtualization-based and emulation-based sandboxing analysis — In the virtualization-based approach, suspicious objects are analyzed while executing in a virtualized operating system environment. The emulation approach uses a software layer that imitates (part of) an application, OS or hardware platform. An emulator translates, for example, API calls and machine instructions to another platform. Solutions that combine virtualization and emulation sandboxing capture the benefits of both approaches.

Contextual information about the malware or targeted attack — Context is important because it can help incident responders determine whether or not malware represents a targeted attack or consumer-grade malware. Information that reveals if the attack was aimed at a specific industry vertical or the motivation of the threat actors is highly valuable.

Integration with forensics tools — Because sandboxing analyzes malware in a simulated environment, integrating with forensics tools is valuable for confirming the impact to the enterprise’s true environment. Integration with endpoint forensics tools and/or network forensics tools (for example, packet capture) enables security teams to shorten the incident response window.

Market Recommendations

If your organization is budget-constrained or looking for a quick path to add sandboxing, first evaluate adding sandboxing as a feature from one of your current security vendors. Assess the sandboxing capabilities of your firewall, IPS or UTM solutions and do the same for your SWG and SEG. It’s likely that this approach will be the most cost-effective option, because it utilizes existing infrastructure to feed suspicious objects to the sandbox.

If budget permits, or when targeted malware is identified as a high risk, evaluate stand-alone sandboxing solutions. This is likely to be the most expensive option, because it requires the addition of feeding sensors to the network. Stand-alone sandboxes typically include more advanced functionality (more of the critical capabilities outlined in the Market Analysis section) than the sandboxing-as-a-feature capabilities that have been added to firewalls, UTM devices and SWGs, although this is not always the case. The increased cost should come with recognized additional benefits such as higher detection rates and a lower number of false positives.

Gartner Recommended Reading

Some documents may not be available as part of your current Gartner subscription.

"Five Styles of Advanced Threat Defense"
"Designing an Adaptive Security Architecture for Protection From Advanced Attacks"

"Magic Quadrant for Secure Email Gateways"

"Magic Quadrant for Secure Web Gateways"

"Magic Quadrant for Enterprise Network Firewalls"

"Malware Protection Systems for Detecting Malicious Code in the Network"

"Fight Network Security Evasion via Wider Testing, Refined Monitoring and Vigilant Patching"

Note 1 Solutions That Embed Sandboxing Technology
Some solutions use sandboxing technology to complement their primary malware and advanced threat detection techniques. For example, Fidelis Cybersecurity Solutions (Fidelis XPS) and Cisco (Sourcefire Advanced Malware Protection) use this approach. Sandboxing capability is included in the core product offering for both vendors.

Cisco offers a sandbox appliance known as AMP Threat Grid (available since January 2015). Because suspicious objects are not automatically fed to AMP Threat Grid by other Cisco products, it does not meet Gartner's definition of a network sandbox. At the time of this writing, suspicious files must be fed manually to the AMP Threat Grid appliance, but Cisco's road map includes plans to automate the feeding of suspicious objects to the appliance.

Note 2 Factors Contributing to FireEye's Revenue Growth
Network sandboxes are the flagship solutions offered by FireEye, but other products (for example, endpoint security), support services and professional services also contributed to its revenue growth.
GARTNER HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

Regional Headquarters
AUSTRALIA
BRAZIL
JAPAN
UNITED KINGDOM

For a complete list of worldwide locations,
visit http://www.gartner.com/technology/about.jsp

© 2015 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. or its affiliates. This publication may not be reproduced or distributed in any form without Gartner’s prior written permission. If you are authorized to access this publication, your use of it is subject to the Usage Guidelines for Gartner Services posted on gartner.com. The information contained in this publication has been obtained from sources believed to be reliable. Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information and shall have no liability for errors, omissions or inadequacies in such information. This publication consists of the opinions of Gartner’s research organization and should not be construed as statements of fact. The opinions expressed herein are subject to change without notice. Although Gartner research may include a discussion of related legal issues, Gartner does not provide legal advice or services and its research should not be construed or used as such. Gartner is a public company, and its shareholders may include firms and funds that have financial interests in entities covered in Gartner research. Gartner’s Board of Directors may include senior managers of these firms or funds. Gartner research is produced independently by its research organization without input or influence from these firms, funds or their managers. For further information on the independence and integrity of Gartner research, see “Guiding Principles on Independence and Objectivity."