Research Highlight

Market Guide for Network Sandboxing
Analyst: Lawrence Orans and Jeremy D'Hoinne
Research Date: March 2, 2015

Gartner Summary:

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.

Cisco-specific Footnote:

Because AMP Threat Grid does not compare directly with a network sandbox, but Lawrence felt compelled to include it in the report, the following footnote was added:

"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."

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:

- 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.

Additional Observations:

- The report recommends is readers are budget-constrained or looking for a quick path to add sandboxing, they should 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.
- Critical capabilities of a sandboxing solution cited in the report are:
    - The ability to analyze a broad range of suspicious objects
    - Static analysis and other prefiltering techniques
    - Comprehensive operating system and application stack
    - Anti-evasion technologies
    - The rate at which objects can be analyzed in the sandbox
    - A combination of virtualization-based and emulation-based

sandboxing analysis
- Contextual information about the malware or targeted attack
- Integration with forensics tools

Upcoming activity related to this report:
We have a Strategic Advisory Session coming up with Lawrence on March 31.

Accessing the report:
Access to the full report is available only to Gartner seat-holders. If you have a seat, you can download or view this report by clicking here.
If you do not have a seat and would like to purchase one, you can do so via the SRE tool.

Please feel free to reach out to me with any questions about this Research Highlight.

Best,
Trevor Bratton
Senior Global Analyst Relations Manager
Security
trbratto@cisco.com
@trevorsecurity
949.823.1212