Advanced Malware Sandbox Market Analysis
“Must Have” Security Technology Reaches Mass Adoption

Report Excerpt
Key Findings

- Advanced malware utilizes sophisticated evasion detection techniques such as polymorphism (modifying code to defeat signature-based tools) or obfuscation (programming to hide evidence of malicious activities) to bypass traditional security models.
- Advanced malware now threatens businesses of all sizes, thereby necessitating a new approach to detection and mitigation.
- An advanced malware sandbox (AMS) is an analysis environment (often virtualized) in which a suspicious program is executed and the behavior of the program is observed, noted, and then analyzed in an automated manner.
  - This approach is more effective than traditional security models because it returns a verdict based on what the malware does rather than how it appears.
- The advanced malware sandbox market has grown rapidly in a short time frame, reaching nearly a billion dollars in revenue in 2015. By 2020, the market will grow to $3.3 billion as it gains greater adoption in new geographic and vertical markets.
- The market is dominated by a handful of early entrants and is expanding as new vendors outfit existing product lines with AMS functionality or add cloud-based services.

Source: Frost & Sullivan
Advanced Malware Sandbox—Market Overview

AMS Offers Unique Benefits

• The goal of sandboxing is to create an analysis environment in which a suspicious program can be executed and observed for malicious actions or evidence of malicious intent.
  
  o This approach is more effective than just looking at the appearance of the executable, because sandboxing goes beyond just the mere appearance of the binary, and observes what the binary does.
  
  o Binaries that perform decidedly “bad” actions are considered malware. Therefore, AMS is much more conclusive in determining if an executable is malicious, returns higher fidelity results, and alerts on the most important issues.
  
  o This approach has multiple benefits compared to traditional security techniques:
    ▪ More conclusive verdicts and evidence of malicious actions or intent has the benefit of reducing false negatives.
    ▪ Higher fidelity results helps to reduce false positives.
    ▪ It alerts on the most important issues, thereby helping to prioritize security response efforts.

Source: Frost & Sullivan
AMS Origins

- The concept for malware sandboxes descends from traditional malware analysis techniques, wherein antivirus companies would analyze suspicious files in test environments to determine the intentions of the binary.

- However, the successful emergence of production-ready AMS solutions and subsequent widespread adoption is enabled by:
  - Technological advancements needed to make this a near real-time process (cloud computing, virtualization, machine learning, and advanced analytics).
  - Strategic efforts to make this a user-friendly product (integrations, pre-filtering, user interfaces, and multiple deployment models).

- The AMS market is now full of solutions with widely varying origins from vendors with equally varied backgrounds and corporate “DNA.” Some solutions are purpose-built and some trace their roots back to security testing tools. AMS vendors include security specialists with expertise in firewalls, content security, or endpoint security, as well as companies with ties to government, defense, and higher education institutions.
AMS Going Forward

• AMS analysis techniques are a valuable capability. However, the market continues to face a number of challenges.

  o The nature of advanced malware continues to evolve. Threat actors now attempt to evade detection, as research labs have identified malware that attempts to defeat AMS analysis using a number of techniques such as:

    ▪ Determining the authenticity of the computing environment prior to executing malicious code. For example, malware may check for user actions that appear authentic.

    ▪ “Waiting out” the sandbox analysis by staying dormant or performing only benign actions until a certain programmed event or until a set amount of time has passed.

  o Networking and IT technologies and practices continue to evolve. Currently, most businesses focus on securing Web and email threat vectors but future versions of AMS solutions will have to support mobile devices and cloud services.
Key Characteristics of an Advanced Malware Sandbox Solution

Threat Analysis

• Advanced malware sandbox solutions utilize dynamic analysis (also called behavioral analysis). Dynamic/behavioral analysis is the process of executing code to monitor for suspicious behavior, artifacts, or other indicators of compromise (IOCs) that indicate the presence of malicious programming.
  o Suspicious behavior includes actions such as injecting code, contacting known command and control systems, dropping malware, and disabling security systems.
  o Artifacts and IOCs are any signs that are left behind by malware such as modified registry keys, unusual files, or new programs in the Startup folder.
• AMS solutions may utilize additional techniques such as statistical analysis and static analysis to identify threats, often as part of the pre-filtering process described in the following slide.
  o Static analysis scans the file for any signs of malicious code. It is not looking for an exact signature but can be useful to identify libraries or reused pieces of code that are known to be malicious.
  o Statistical analysis uses algorithms and machine learning to determine patterns that are similar to known threats in order to detect the newest threats that have never been identified before.

Source: Frost & Sullivan
Pre-Filtering

• AMS analysis requires more time compared to other threat detection systems. Therefore, pre-filtering is an important process to avoid wasting AMS resources on “known good” and “known bad” files.
  o This step is important. Sandbox analysis can require minutes compared to seconds (or fractions of a second) for an AV or IPS inspection. Customers must be selective and send only suspicious or previously unseen files for AMS analysis.

• Currently, AMS vendors utilize a mix of security techniques including IPS inspection, content analysis, black listing, and other capabilities to filter out “known malware.” To perform some of these pre-filtering inspections, the solution will require either “baked-in” capabilities or integration with related security tools.
  o Customers should ensure that the AMS solution that they are evaluating can support their existing security investments.

• AMS solutions may also utilize special rules that pre-classify or pre-filter files based on characteristics such as file type or contents of a file.

• This competitive factor is important as it has an impact on both the performance of the network and the accuracy of the solution.

Source: Frost & Sullivan
Time to Detection

• AMS solutions require extensive time for analysis. Many AMS solutions leverage the cloud for computing power.
  o This allows the on-premises solutions to focus on simply performing the deep packet inspection necessary to extract the file and submit the file to the sandbox for analysis.
  o This actual traffic inspection and file extraction process takes only milliseconds.
• Unfortunately, even the best malware sandboxing solutions may potentially require several minutes to return a verdict.
• To mitigate this user impact, most solutions offer the option to permit the file to pass while it is being utilized.
  o This is a potential risk for infection, with some vendors attempting to balance this option with the ability to follow the trajectory of a file throughout an organization, past the inspection point. This may require integration within the broader IT environment (such as endpoint visibility) or network infrastructure (such as switches and firewalls).
• Essentially, vendors take a wide range of approaches to mitigate the long analysis times required for a sandbox inspection.
Key Characteristics of an Advanced Malware Sandbox Solution (continued)

**Reporting**

- The ability of the sandbox solution to communicate its results to administrators is of underestimated importance.
  - An advanced malware sandbox is simply a tool. The most accurate tool in the world is incomplete if it is unable to communicate its results to human users.
  - Whether a breach is due to technical failings of a product or human error, either end result is unacceptable.
- Sandbox solutions vary in terms of their reporting and user interface.
- Though the largest enterprise organizations may have dedicated, skilled experts that are familiar with command-line interfaces and manual processes, the fact is that every user would benefit from graphical representations of findings and results.
  - Solutions that deliver the most critical and useful information in visually intuitive interfaces enable security analysts to prioritize threats in a more effective and efficient manner.
- As AMS solutions become more prevalent among smaller enterprise organizations or the less technically sophisticated, the importance of reporting and user interfaces increases in magnitude.

Source: Frost & Sullivan
Key Characteristics of an Advanced Malware Sandbox Solution (continued)

Automation

• Sandbox solutions must be able to answer the question of “why” files have been flagged as malicious (or suspicious). It is not enough for an AMS solution to simply return a “malicious or not” verdict.

• AMS solutions should provide detailed reports that indicate the malicious actions that the malware performs so that incident response teams and security professionals can take investigative and corrective action.

• Ideally, AMS solutions will be able to integrate with network security and endpoint controls that allow it to automatically initiate a quarantine or corrective action for newly discovered threats.
  o For example, integration with network monitoring tools and endpoint agents can be used to track which endpoints the malware infected, and also to identify the changes made on an endpoint, and to undo the actions done by the malware.
  o These automation capabilities will require integration between security vendors and are in development by leading AMS vendors now.

Source: Frost & Sullivan
Key Characteristics of an Advanced Malware Sandbox Solution (continued)

Roadmap

- Vendors vary greatly in terms of roadmap.
  - The newness of the technology challenges multiple vendors that are now moving quickly to add customer-requested features.
  - Established vendors with mature products continue to pour in millions of dollars in research and development to stay ahead of threat actors.
- Across the board, vendors are challenged to add new threat detection capabilities and to adapt their solutions to detect the latest evasion techniques.
- Additionally, all AMS vendors are working to speed up analysis processes and to integrate with customers’ networking and security ecosystems.

Source: Frost & Sullivan
Advanced Malware Sandbox in the Context of Advanced Threat Protection

Advanced Malware Sandbox is a Component of Advanced Threat Protection

- Advanced malware sandbox solutions are often confused with the broader concept of advanced threat protection.

- An AMS is just one component (albeit, a very important component) of an advanced threat protection strategy.
  - Advanced threat protection is not comprised of any one security technology. Instead, advanced threat protection requires a framework of security tools, intelligence, analytics, and expertise.

- The need for advanced threat protection has become widespread because cyber threats became too sophisticated for traditional security tools to defend against.
  - Now, an AMS solution is necessary to identify advanced malware. However, advanced malware is just one component of advanced persistent threats.

Source: Frost & Sullivan
**Advanced Malware in the Context of Advanced Persistent Threats**

**Advanced Malware is a Component of Advanced Persistent Threats**

- Nation-states with tremendous resources and strong motivations developed advanced malware that could evade detection by existing security tools of the time. This malware was unleashed against political, national, and ideological rivals in campaigns of sabotage, espionage, and theft.

- Soon, businesses around the world began to report similar attacks, as cyber criminals learned and then employed similar advanced techniques. The evolution of APTs is charted in the following slide.

- The term “Advanced Persistent Threat” (APT) was coined in reference to this new threat.
  - Technically, the term APT refers to the threat actor and/or their attack campaign.

- Unfortunately, the term APT has been used loosely, and may refer to the advanced malware that threat actors utilize such as Stuxnet, Flame, and Duqu.
  - It is important to note that APTs often utilize a number of techniques such as social engineering, zero-day vulnerabilities, or stolen credentials, in addition to advanced malware.
  - The distinction is important: an AMS solution may not detect an attack if the attack does not feature malware.
An advanced persistent threat is defined as follows:
- Targets or focuses on specific individuals or organizations.
- Looks to penetrate and persist in an environment (network or endpoint).
- Utilizes advanced malware, zero-day vulnerabilities, and sophisticated techniques.
- Evades signature-based detection techniques.
- Is planned, launched, and supported by an organized group (with specific objectives such as for monetary or intellectual property gains).

Advanced persistent threats have three key attributes:
- Targeted
- Persistent
- Advanced

These attributes are explained in-depth in the following slides.

Source: Frost & Sullivan
Advanced Malware in the Context of Advanced Persistent Threats (continued)

**APT Targeted Attribute**

- APTs target specific individuals or organizations.
- Organizations with valuable intellectual property, state secrets, or sensitive customer information are targets for APTs.
- Threat actors save the most sophisticated and new attacks for high value targets to maximize return on investment.

Source: Frost & Sullivan
Advanced Malware in the Context of Advanced Persistent Threats (continued)

**APT Persistent Attribute**

- Threat actors are persistent in their approach to cyber attacks.
  - They have a profit motive and are looking for a return on investment.
  - They are well organized, funded, and managed.
  - They invest time—from development of new phishing techniques and malware to the processes of research, recon, testing and penetrating defenses, delivering payloads, moving laterally through the target network, and data exfiltration.
  - Threat actors will use multiple phishing techniques, malware samples, and attack vectors. If defeated once, they will modify their strategies and attempt to leverage new or different tactics in follow-up attacks.

- The malware is persistent.
  - The malware looks to remain in the network for a long period of time.
  - The malware is quiet, only performing actions that do not trigger alerts, draw attention to its activity, or alert security analysts to its presence.
  - The malware may obfuscate evidence of its activity or existence, hiding or destroying logs and artifacts, or tampering with or disabling security tools.

*Source: Frost & Sullivan*
Advanced Malware in the Context of Advanced Persistent Threats (continued)

APT Advanced Attribute

• Early cyber attacks were executed using rudimentary and standard malicious binaries, often referred to as viruses.
  
  o Defense against these malicious binaries was effectively accomplished by signature-based antivirus, IPS, and Web and email content security platforms. These tools would rely on an actual pattern or static image of the binary.
  
• To defeat these security systems, threat actors developed malware that could automatically modify or alter its appearance while continuing to deliver its malicious payload. This feature is called polymorphism.
  
  o If the code of the binary looks different, the signature for the code will also be different, rendering signature-based defenses, such as those often included in antivirus solutions, insufficient.
  
  o As a result, this advanced malware is capable of avoiding detection by traditional network and endpoint security solutions.

Source: Frost & Sullivan
Focus on Advanced Malware to Defend Against Advanced Persistent Threats

- The idea to focus on the advanced malware used in APT attacks is a natural conclusion: advanced malware is one of the most important tools used by these threat actors.
- Considering the characteristics of “targeted, persistent, and advanced,” a behavioral approach is required to detect APTs.
  - Instead of trying to detect malware based on what it is (signature-based), behavioral detection relies on what the binary does.
  - For example, if the first action taken by an executable file is to disable logs or antivirus, security analysts can safely assume that the executable is a malicious binary.
    - The malicious executable should then be quarantined, and security personnel notified.
  - If the executable does an action such as changing registry keys, this may be considered an indicator that it is malware.
    - Multiple indicators of compromise can be compiled and analyzed to prove that a file is malicious with a high degree of certainty.
- AMS solutions have proven capable of performing this behavioral analysis with a high degree of fidelity and insight into malware activities. As a result, AMS solutions have proven to be valuable tools within advanced threat protection portfolios.

Source: Frost & Sullivan
• Ultimately, the effectiveness of an AMS solution within a broader advanced threat protection strategy is based on several factors:
  o Intelligence—visibility, knowledge, and correlation of security incidents across the entire IT environment, as well as an understanding of relevant threat trends.
  o Technical expertise—the ability to use the full features of the solution in correct, timely, and consistent fashion.
  o Available resources—IT staff, administrators, security analysts, and the time needed to investigate security incidents.

Source: Frost & Sullivan
Competitive Landscape

FireEye remains the clear market leader despite intensifying competition.

Competitive Landscape
Total Advanced Malware Sandbox Market: Global, 2015

Source: Frost & Sullivan
FireEye is dominant in terms of market share.

**Total Advanced Malware Sandbox Market: Percent Revenue by Vendor, Global, 2015**

- **FireEye**: 56%
- **Company A**: 13%
- **Company B**: 10%
- **Company C**: 8%
- **Company D**: 4%
- **Company E**: 3%
- **Company F**: 2%
- **All Others***: 4%

* A list of companies included in “Others” can be found in the appendix.

Note: All figures are rounded. The base year is 2015. Source: Frost & Sullivan.
Predictions

1. Advanced Malware Sandbox technology will become a fundamental component of the security architecture with some form of the functionality becoming as ubiquitous as firewalls.

2. AMS technology will increasingly be integrated into existing security platforms such as NGFWs and SWGs in order to enhance value and security efficacy. This factor will be advantageous for security vendors with broad portfolios.

3. However, the AMS will remain in a period of rapid technological advancement as vendors adjust to new threats. The high level of technological change will ensure the need for pure-play competitors in the market.

Source: Frost & Sullivan
Recommendations

1. AMS solutions require visibility. Solutions are more effective when they are able to analyze more files across more attack vectors. Integration is key to ensure that the AMS provides the greatest level of detection across the entire IT environment both in terms of visibility and response.

2. An AMS is just one tool needed to defend against APTs. AMS must be considered in the context of broader advanced threat protection goals.

3. Despite the high level of demand and enthusiasm for AMS, the reality is that businesses of all sizes are already stretched thin in terms of resources, time, and budgets. Competitive factors such as value, flexibility, ease-of-use, and support for existing tools and processes should not be overlooked.
Legal Disclaimer

Frost & Sullivan takes no responsibility for any incorrect information supplied to us by manufacturers or users. Quantitative market information is based primarily on interviews and therefore is subject to fluctuation. Frost & Sullivan research services are limited publications containing valuable market information provided to a select group of customers. Our customers acknowledge, when ordering or downloading, that Frost & Sullivan research services are for customers’ internal use and not for general publication or disclosure to third parties. No part of this research service may be given, lent, resold or disclosed to noncustomers without written permission. Furthermore, no part may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the permission of the publisher.

For information regarding permission, write to:

Frost & Sullivan
331 E. Evelyn Ave. Suite 100
Mountain View, CA 94041

Source: Frost & Sullivan
One of Frost & Sullivan’s core deliverables is its Market Engineering studies. They are based on our proprietary Market Engineering Methodology. This approach, developed across the 50 years of experience assessing global markets, applies engineering rigor to the often nebulous art of market forecasting and interpretation.

A detailed description of the methodology can be found [here](#).