BLUE COAT®

Network
+ Security
+ Cloud

TOP 5 CRITICAL CAPABILITIES FOR YOUR MALWARE SANDBOXING STRATEGY

SECURITY INSIGHT BRIEF

Malware is Evolving. So Should Your Defenses.

Malware authors are clever and persistent. More than 200,000 new malware samples are uncovered every day.[1] And new malware attacks are often successful: According to the 2015 Experian Data Breach Industry Forecast, 73% of companies are expecting a data breach. Layered defenses can block the "known bad," but malware continues to slip through. Today, you must also analyze and defend against "unknown" files and URLs with dynamic sandboxing. It's the only way to methodically unmask zero-day exploits, advanced persistent threats, and advanced targeted attacks. So what should you look for in dynamic sandboxing technology? Here's the short list.

Top 5 Must-Haves for Malware Sandboxing

1 Multiple Detection Methodologies

How do you block the known bad and gain new insights and actionable intelligence about unknown threats? By diversifying your detection methodologies. Ideally you'll need support for dual malware behavioral detection methodologies – both emulation and virtualization – to detect unknown threats and generate actionable intelligence.

Two sandbox environments using different approaches can also expose evasive, virtual-machine-aware (VM-aware) malware through kernel-level event detection and hook-based introspection that is extremely difficult for malware authors to circumvent without advanced proprietary knowledge of the malware analysis testbed. Malware defense-in-depth often rests on the ability to detect "edge cases" that others miss (the incremental percentages of hard-to-spot samples that frequently evade detection) and the dual-detection hybrid sandboxing approach provides a key advantage in the ongoing arms race between attackers and defenders.

2 Customizable and Realistic Virtual Environments

Sophisticated malware can attack the systems, processes, and individuals of a particular company while seeking a specific asset or database. To combat this new scourge, malware analysis sandboxes must be able to closely replicate actual production environments and spot malware seeking to exploit specific configurations. The sandbox should allow you to match nearly any target Windows environment. Profiles should come ready to use out-of-the-box, and you should be able to create your own custom profiles to match corporate standards or account for different configurations across various user groups, including common applications and Web browsers.

[1] Source: Kaspersky Lab

3 Behavior-Based Classification and Custom Risk Scoring

Your sandboxing solution should tell you why a sample file or URL was flagged as malicious, and not simply report a "good or bad" result. It should use behavior-based malware classification patterns, not code-based signatures, to flag events based on potential malicious activity.

The patterns should also provide risk scoring, either out-of-the-box or customizable based on your own criteria, covering everything from generic malicious behavior (e.g. modifying registry keys) to family-specific behavior patterns (e.g. banking Trojans); and they should include anti-VM (virtual machine) detection patterns. These patterns should be completely open and should not attempt to hide why an event is being flagged as a suspicious indicator. The system should report all patterns that "triggered" based on the behavior of a sample during the analysis run, with matching patterns available for post-analysis inspection.

4 Access to Comprehensive Event Data and Analysis Resources

For intelligence to be actionable by security teams, it first has to be accessible to them. Your malware analysis solution should make all event data and analysis resources readily available for inspection. Granular data should be available, including risk scores, pattern group hits, analysis summaries, event details, and full protocol buffers to provide multiple levels of detail for analysts to act upon.

In addition, full packet captures (PCAPs) should be made of all network activity relating to each analysis task. PCAP inspection can help security analysts identify malware calls to command-and-control servers, login credentials or commands used by the malware, URL redirects to malicious websites, subsequent malware downloads, and data that has been

exfiltrated from a victim organization. PCAPs can be post-processed through traditional IDS systems to add further analysis context.

All raw event data should be preserved, meaning that dropped files should be saved even if the files were removed by the malware and no longer exist at the end of the malicious execution cycle. As more tasks are processed, a uniqueness score should be calculated, indicating whether a given event has been seen before, such as a new domain name or a randomly generated polymorphic file name.

Also, look for a solution that can automatically generate screen shots of visible system changes, including multi-step installers. Your solution should provide insight into website interaction and the various online activities performed by malware when connected to remote servers.

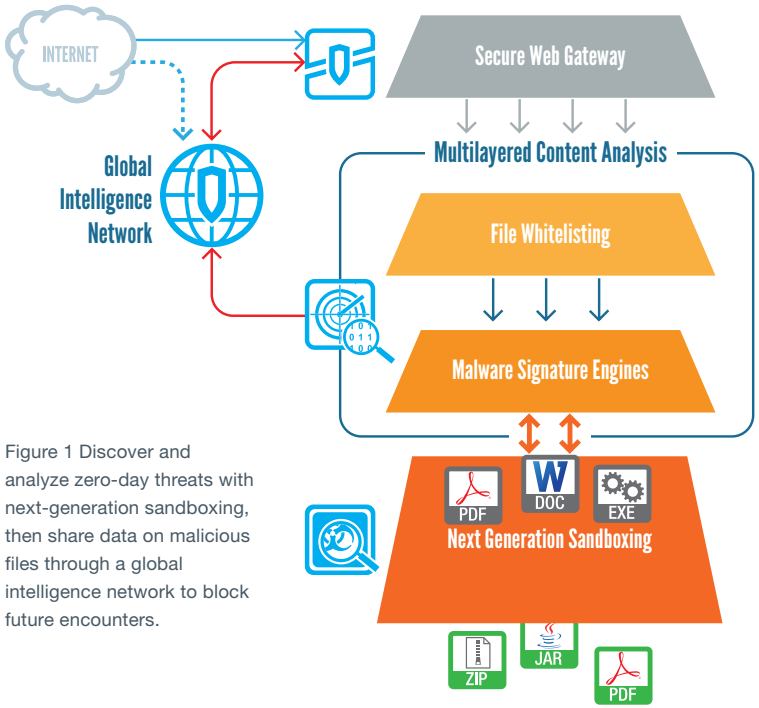

Figure 1 Discover and analyze zero-day threats with next-generation sandboxing, then share data on malicious files through a global intelligence network to block future encounters.

5 Shared Actionable Threat Intelligence

A well-designed sandboxing system provides a focal point for generating threat information, but that intelligence must be shared for the overall solution to be truly effective (see Figure 1). File and URL characteristics must be brought back "upstream" into a global intelligence network so that future attacks can be blocked at their points of origin. This is critical in order to keep up with the proliferation of polymorphic attacks that may originate from a common malicious website yet steadily evolve.

The ability to continuously update white/black lists, security analytics profiles, and content analysis systems all reinforce the organization's identification, forensics, and remediation capabilities. In this way, sandboxing underpins the ability to provide comprehensive defense-in-depth security against today's sophisticated threats.

Get Beyond Limited Solutions – and Empower Your Business

You have many things to consider when evaluating sandboxing solutions for advanced malware protection, and this brief can touch upon only a few. The goal is to help you focus on the most important capabilities your solution should deliver. At the same time, though, keep in mind a few characteristics to look out for.

For example, many products today call themselves "sandboxes," but beware of one-size-fits-all, non-configurable solutions. The generic detection they provide may not be directly relevant to your organization.

Also take care to avoid lightweight implementations that only provide good/bad "verdicts" without generating the actionable intelligence necessary for the organization to continuously improve its comprehensive security posture. And finally, steer clear of closed platforms that are incapable of sharing malware threat intelligence within a comprehensive solution suite.

Learn More

Blue Coat stands ready to assist you with additional evaluation criteria, answers to your specific questions about advanced threat protection, or a demonstration of the capabilities of our Content Analysis System and Malware Analysis Appliances.

Take the next step by learning more about Blue Coat's dynamic malware analysis products and how they can expand your defenses.

Visit www.bluecoat.com/atplifecycle.

BLUE COAT®

Network + Security + Cloud

Blue Coat Systems Inc.
www.bluecoat.com

Corporate Headquarters
Sunnyvale, CA
+1.408.220.2200

EMEA Headquarters
Hampshire, UK
+44.1252.554600

APAC Headquarters
Singapore
+65.6826.7000