ThreatTrack SECURITY

Malware Analysis Sandboxing: Is Open Source or Commercial Right for You?

Summary

Many enterprises evaluating sandboxing products find themselves considering both products from commercial vendors and open source projects.

This comparison of Cuckoo Sandbox and ThreatAnalyzer, two leading dynamic malware analysis solutions, will help you determine which approach is the best fit for you.

Sandboxing: What is the Best Fit for You?

In the war against cybercriminals and hackers, dynamic malware analysis technology has emerged as one of the most valuable weapons for information security teams. "Sandboxing" products help security professionals identify unknown malware, respond more quickly to Zero-day attacks, thwart APTs and other advanced attacks, and perform forensic examinations of breaches.

Many enterprises evaluating sandboxing products find themselves considering both products from commercial vendors and open source projects. The commercial solutions are more mature and feature-rich, and are supported by the vendors; the open source alternatives are "free" and make source code available for modification.

What is the best fit for you? Do the additional features and predictable support of the commercial products justify the extra up-front cost?

This white paper will help you answer those questions by comparing two dynamic malware analysis solutions: ThreatAnalyzer from ThreatTrack Security, and Cuckoo Sandbox from the Cuckoo project.

We will discuss:

1. "Generic" advantages that often differentiate open source and commercial alternatives.
2. What advantages actually apply to sandboxing solutions.
3. Three feature areas that are particularly important for dynamic malware analysis:
   - *Defeating VM-aware malware.*
   - *Providing customized environments and detection rules.*
   - *Accelerating malware analysis and reporting.*

Generic Advantages of Open Source and Commercial Solutions

Through many debates in the IT industry press, advocates of open source and commercial software have presented what might be called the generic advantages of each approach. These are "generic" because they apply in many

Open Source Software	Commercial Products
No licensing fees	Lower ongoing management costs
Source code is available for modification	Vendor supports enhancements
Freedom from lock-in to a commercial vendor	Dedicated, paid developers and support staff
Many "eyes on the code" to find vulnerabilities	Cybercriminals cannot access source code
Potentially unlimited number of contributors	Mature software with more features

Table 1: Generic Advantages of Open Source and Commercial Solutions

areas of software technology, but not all. Those most commonly cited are shown in **Table 1**.

Open source software is available through a "general public license" that offers the software at no cost, provided users follow a few rules (such as not selling products that include any of the licensed code). Commercial vendors pay more attention to minimizing installation and ongoing management costs. They provide installation wizards, user-friendly interfaces and other features that reduce administrative costs.

Open source licenses include the right to modify source code, so users can fix bugs, enhance the software, and even "fork" the code to create a completely customized version. Commercial vendors support enhancements, so users do not need to worry about maintaining modified source code.

Open source users are not locked into a single vendor, and in fact can begin supporting their own version of the source code at any time. Commercial products are backed by dedicated, paid development teams and support staffs; customers are not reliant on volunteer contributors who might lose interest, move to another open source project, or neglect support.

Open source communities encourage many contributors to review source code to find and fix security vulnerabilities. Commercial vendors prevent cybercriminals and hackers from reviewing source code to find and exploit security vulnerabilities.

Open source communities have the potential to harness the efforts of thousands of contributors, and have done so for projects such as Apache, Linux, Eclipse and OpenOffice. However, in most areas of software technology, commercial products have been around longer and are more mature, reliable and feature-rich.

What Advantages Apply for Sandboxing Solutions?

Not all of the generic advantages of open source software apply to every project, and not every generic advantage of commercial products is relevant to every vendor's solution. Let's look at which factors are relevant in the area of dynamic malware analysis, and specifically for Cuckoo Sandbox and ThreatAnalyzer.

Table 2 shows some basic facts about Cuckoo Sandbox and ThreatAnalyzer.

Cuckoo Sandbox	ThreatAnalyzer
The Software	
Cuckoo Sandbox is a dynamic malware analysis "sandboxing" product. It is available through a GNU General Public License.	ThreatAnalyzer is a dynamic malware analysis "sandboxing" product. It is available through a commercial license.
The Organization	
The Cuckoo Foundation is a non-profit organization incorporated in the Netherlands. Currently it has 4 active developers. Since the beginning of the project 13 additional contributors have made 5 or more contributions to the code base, and 29 individuals who have made 1-4 contributions.	ThreatTrack Security is a venture-backed cybersecurity firm based in the USA. Its offerings include the ThreatAnalyzer sandbox, the ThreatSecure advanced threat detection and remediation platform, the ThreatIQ real-time threat intelligence service, and VIPRE antivirus endpoint protection. ThreatTrack Security products currently protect over 10 million endpoints. Its solutions, trusted by U.S. federal and civilian agencies, play a key role in U.S. cybersecurity defense.
Release History	
Cuckoo Sandbox was started in 2010 as a student project. The 1.0 release was published in January 2014. The most recent release is 1.1, published in April 2014.	ThreatAnalyzer was first released in 2005 under the name of CWSandbox. The most recent release is 5.1, published in June 2014.

Table 2: Facts about Cuckoo Sandbox and ThreatAnalyzer
Source: CuckooSandbox.org and ThreatTrack.com, as of September 2014

So which of the generic advantages of open source software actually apply to Cuckoo Sandbox?

The absence of licensing fees is a factor in favor of Cuckoo Sandbox for enterprises that have very tight capital budgets. However, this is partially offset by the fact that the Sandbox clients still require Microsoft Windows and Office licenses.

Because users have the right to modify source code, Cuckoo Sandbox is a good option for organizations that need to make custom modifications to meet unique requirements for malware analysis.

The freedom from lock-in to a commercial vendor is offset by dependence on a relatively small community of volunteers (4 active developers and a relatively small number of occasional contributors). The number of "eyes on the code" is not large enough to provide an advantage of security. Although the contributing community could grow, at its current size it is not likely to produce enhancements faster than commercial vendors like ThreatTrack Security.

Which of the generic advantages for commercial projects are significant for ThreatAnalyzer? ThreatAnalyzer is much easier and less expensive to manage than Cuckoo Sandbox. Typical of many open source products, Cuckoo Sandbox expects administrators to have a high knowledge level and to devote significant time to mastering the product and the requirements for installation and management.

"Cuckoo is a great resource, but setup is not exactly 'user-friendly'... [I]t helps to have a good understanding of things like Linux, virtualization software (VIrtualBox, VMware, etc), virtual networking, and the Python programming language...Take plenty of time setting up the sandbox and make sure you understand the configuration. If it's not making sense, read through the documentation repeatedly until you understand the basics."

Joshua Cannell, Automating Malware Analysis with Cuckoo Sandbox

For example, independent consultant Joshua Cannell, who sees many advantages in Cuckoo, nevertheless reports that setup "is not exactly user-friendly" and requires a good understanding of Linux, virtualization software, virtual networking and Python.

The Cuckoo developers themselves state that their software is "not a technology meant to be accessible to just anyone." They are also pretty clear about their views on customer support: "[I]f a problem occurs you have to make sure that you did everything you could before asking for time and effort from our developers and users. We just can't help everyone..."

"Cuckoo stumbles and produces some error I don't understand. Cuckoo is a young and still evolving project, it's possible that you encounter some problems while running it, but before you rush into sending emails to everyone make sure you read what follows.

Cuckoo is not meant to be a point-and-click tool: it's designed to be a highly customizable and configurable solution for somewhat experienced users and malware analysts.

It requires you to have a decent understanding of your operating systems, Python, the concepts behind virtualization and sandboxing. We try to make it as easy to use as possible, but you have to keep in mind that it's not a technology meant to be accessible to just anyone.

That being said, if a problem occurs you have to make sure that you did everything you could before asking for time and effort from our developers and users. We just can't help everyone, we have limited time and it has to be dedicated to the development and fixing of actual bugs."

Excerpt from the Troubleshooting section on the Cuckoo Sandbox documentation web site FAQ page

In contrast, ThreatAnalyzer includes intuitive interfaces and management tools that make it much easier and less costly to deploy and manage.

Another factor to consider is that ThreatTrack Security enhances and supports ThreatAnalyzer, so customers do not need to staff their organization with developers to customize and support the solution. In addition, ThreatTrack Security has full-time customer support personnel to help with installation, configuration, best practices and other topics.

The final major advantage of ThreatAnalyzer is its maturity and feature-richness, particularly in three areas that are crucial to the effectiveness of dynamic malware analysis:

- Defeating VM-aware malware.
- Providing customized environments and detection rules.
- Providing tools that simplify and speed up malware analysis and reporting.

These topics will be addressed in the next three sections of this paper.

Table 3 duplicates Table 1, but shows which of the "generic" advantages of open source and commercial projects actually apply to Cuckoo Sandbox and ThreatAnalyzer (highlighted in green).

Open Source Software	Commercial Products
No licensing fees	Lower ongoing management costs
Source code is available for modification	Vendor supports enhancements
Freedom from lock-in to a commercial vendor	Developers and support staff are paid
Many "eyes on the code" to find vulnerabilities	Cybercriminals cannot access source code
Potentially unlimited number of contributors	Mature software with more features

Table 3: Generic advantages relevant to a comparison of Cuckoo Sandbox and ThreatAnalyzer (in green)

ThreatAnalyzer: Defeating VM-Aware Malware

VM-Aware Malware

Many sandboxing solutions run only on virtual machines, and some use hooks into the hypervisor to perform malware monitoring functions. This approach promotes performance and efficiency, because multiple analyses can be conducted simultaneously on one physical system. Also, when an analysis is complete it is easy to shut down a VM and fire up a new one.

Unfortunately, hackers have identified virtual machines as an Achilles heel in many dynamic malware analysis products, both open source and commercial. They have designed malware to stay hidden in virtual environments, and "detonate" only on physical systems.

Techniques to evade VM-based sandboxing products include:

- Using one of several methods to detect the presence of a hypervisor.
- Waiting for human interaction, such as a mouse click on a license dialog box.
- "Sleeping" for an extended time, in order to outwait the usual duration of a sandbox test.
- Waiting for a reboot, which occurs on physical machines but not in VM sandbox environments.

Defeating VM-Aware Malware

With almost a decade in full production use by hundreds of customers, ThreatAnalyzer has built up a set of features and functions beyond those available in a relatively new product like Cuckoo Sandbox. Some of the most important lie in the area of defeating VM-aware malware.

For example, ThreatAnalyzer can:

- Simulate a range of human interactions, including clicks on license and installation dialog boxes and application prompts.
- Monitor and accelerate sleep calls, to prevent the malware from outwaiting the sandbox test period.
- Simulate a reboot on a virtual machine.

In addition, ThreatAnalyzer software can be run on a native (physical) machine, to make certain that malware will not detect any evidence of a virtual environment.

"It's also important to note that like us, Cuckoo isn't perfect. In certain cases, submitted analyses will fail. This can happen for a variety of reasons. For example, some of the malware today is designed to check if it's inside a virtual environment or sandbox, and may not execute properly if detected."

Joshua Cannell, Automating Malware Analysis with Cuckoo Sandbox

ThreatAnalyzer: Providing Customized Environments and Detection Rules

Why malware writers target specific software

Another tactic increasingly used by malware writers is to check for a specific product version before detonating. Malware writers use this tactic to:

- Exploit vulnerabilities in a specific version or versions of a product (say a given release of Internet Explorer or Adobe Reader).
- Prevent detonation and analysis in sandbox environments that don't include that particular version.
- Target environments that cannot be included in standard sandbox configurations, such as enterprise applications, POS (point of sale) terminals, and industrial SCADA (supervisory control and data acquisition) systems.

Detecting targeted attacks: Groups of custom environments

ThreatAnalyzer includes features to detect targeted attacks. The first of these is the ability to submit a malware sample to a group of customized environments in one step, and to compare the results immediately.

For example, a suspect file in PDF format can be submitted to a group of clients running different versions of Adobe Reader **(Figure 1a)**. In less than two minutes, ThreatAnalyzer would provide a report showing which clients were at risk and which were not **(Figure 1b)**.

Many ThreatAnalyzer users create clients that replicate all of the typical corporate desktops in their environment, including enterprise and custom applications. By submitting samples to the members of this group, they can detect all malware targeting those desktops. Not only does this help identify application-specific malware, it prevents analysts from wasting time responding to alerts about malware that is malicious but does not threaten the enterprise.

Detecting targeted attacks: Malware Determination Rules

ThreatAnalyzer also includes a "Malware Determination Engine" that tests samples against Malware Determination Rules (MDRs). These rules identify specific traits and activities associated with malware, for example attempts to edit specific registry keys, calls to specific files, and efforts to access certain types of resources (say POS terminals or SCADA systems). Rules can also look for characteristics on non-executable files that would be ignored by most sandboxing solutions.

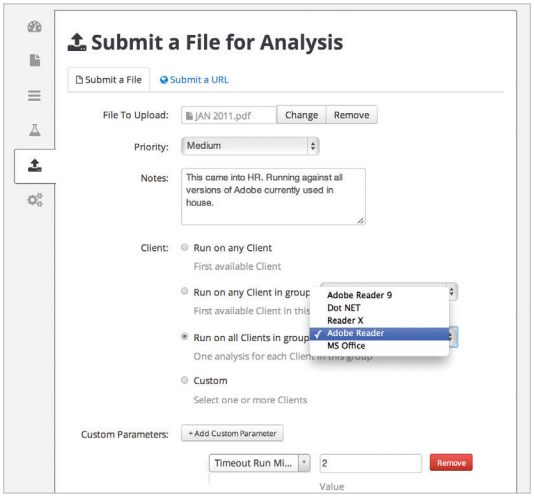

Figure 1a: Submit a file to a group of clients

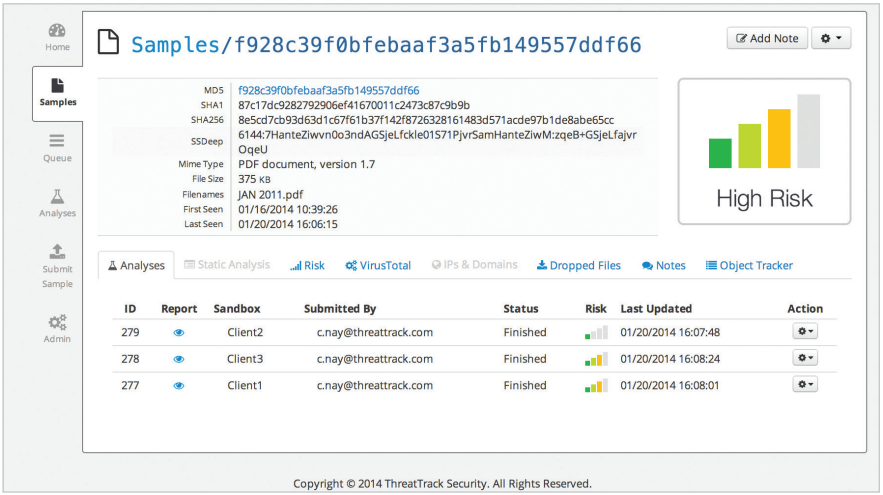

Figure 1b: A report shows which clients are at risk

ThreatTrack SECURITY

ThreatAnalyzer comes with a comprehensive standard rule set. The rule set is continuously improved and extended by a dedicated research team that monitors 200,000 malware samples a day and delivers enhancements through ThreatTrack's ThreatIQ service.

"Cuckoo Sandbox [is] NOT a drop in replacement for commercial solutions at this point. No automated malware identification or loading."

Presentation at Defcon Groups DC214 meeting: Automating Malware Analysis: A Look at Cuckoo Sandbox

In addition, customers can add custom rules to protect their most sensitive data and systems.

Cuckoo Sandbox, in its most recent release, added the capability to create custom sandbox environments. However, malware samples have to be loaded individually into each environment, and any comparison reporting needs to be done manually. Also, Cuckoo Sandbox has no equivalent of ThreatAnalyzer's Malware Determination Rules or ThreatIQ service.

ThreatAnalyzer: Speeding up Malware Analysis and Reporting

Speed is of the essence

For incident responders and security analysts, faster threat analysis and reporting mean:

- More malware samples can be tested.
- Analyses can be more thorough and informative.
- Incidents can be resolved faster.
- Defenses against newly emerged threats can be put in place sooner.

Over time the developers of ThreatAnalyzer have added many features and functions that accelerate malware analysis and reporting. Some of the most useful include:

- The ability to pull samples periodically from a directory, so they can be submitted automatically by next-generation firewalls, SIEM systems and other security devices.
- Centralized management of multiple virtual machines and physical systems, so malware samples can be analyzed in parallel on multiple systems.
- A GUI that allows analysts to submit a malware sample in one step to a single client, to a pre-established group of clients, or to a group of clients selected on demand.
- A GUI that allows analysts to select a wide variety of parameters without having to modify the sandbox clients manually, for example, to fake a reboot, to click buttons displayed by the file, to extend the default runtime for analysis, to start an external application after a delay, or to force sleep operations from malware to last only one millisecond.
- Support for multiple analysts, including different access roles and audit trails for security and regulatory compliance.
- A threat dashboard showing actionable information such as top IPs and domains associated with a malware sample, top malicious behaviors identified in recent malware tests, the number of samples by risk level (low, medium and high), and a list of high risk samples recently analyzed.
- A searchable archive of analysis reports, so analysts can quickly find past analyses with information related to a current one.

"Cuckoo is still a very young solution, sometimes problems occur, especially when it comes to generating report containing some foreign language characters – it drops number of errors and fails, at least in my environment. When Cuckoo doesn't behave as expected, it's good to have something else..."

Hubert Kromer, blog post: Choosing the best Sandbox for malware analysis

ThreatTrack Security also offers a cloud-based threat intelligence service called ThreatIQ. This service regularly updates ThreatAnalyzer with newly detected malicious URLs and IP addresses and phishing links, as well as signatures of suspected malicious files. ThreatIQ helps ThreatAnalyzer users stay ahead of advanced threats as they emerge.

Cuckoo Sandbox does not yet provide a user-oriented GUI or the productivity features described above. Its primary use case is a single expert user, submitting one malware sample at a time for analysis.

Conclusions

Enterprises comparing open source and commercial solutions typically look at a variety of trade-offs:

- No licensing fees, versus lower ongoing management costs
- Available source code, versus vendor support for enhancements
- Freedom from vendor lock-in, versus paid developers and support staff
- Many "eyes on the code," versus preventing bad guys from analyzing the code
- Potentially unlimited contributors, versus mature, reliable software with more features

In the area of dynamic malware analysis technology, some of those factors are more important than others. For example, Cuckoo Sandbox has no licensing fees and can be freely modified by users, but other generic advantages of open source projects are less relevant, because the development and support of Cuckoo Sandbox depend on a very small community of contributors.

ThreatAnalyzer has distinct advantages over products like Cuckoo in low management costs and reliable customer support. It also includes critical features for:

- Defeating VM-aware malware, through techniques like simulating user behavior, cutting short sleep calls, and simulating reboots.
- Defeating VM-aware malware by providing an option to run tests on physical (native) systems as well as virtual machines.
- Detecting targeted attacks by making it easy to test samples against multiple customized environments.
- Detecting targeted attacks by executing custom Malware Determination Rules.
- Accelerating malware analysis and reporting, for example through tools to allow multiple analysts to work together, to give analysts more control over when and how tests are run, and to allow users to search archives of past analyses.

For these reasons ThreatAnalyzer is a better choice for security groups who are concerned about VM-aware malware, who may be subject to version-specific and targeted attacks, who have multiple incident responders and analysts, and who place a premium on completing analyses and reports quickly.

For more information on ThreatAnalyzer from ThreatTrack Security, please visit http://www.threattracksecurity.com/enterprise-security/sandbox-software.aspx or contact us at Sales@ThreatTrack.com.

About ThreatTrack Security

ThreatTrack Security specializes in helping organizations identify and stop Advanced Persistent Threats (APTs), targeted attacks and other sophisticated malware designed to evade the traditional cyber defenses deployed by enterprises and government agencies around the world. With more than 300 employees worldwide and backed by Insight Venture Partners and Bessemer Venture Partners, the company develops advanced cybersecurity solutions that Expose, Analyze and Eliminate the latest malicious threats, including its ThreatSecure advanced threat detection and remediation platform, ThreatAnalyzer malware behavioral analysis sandbox, ThreatIQ real-time threat intelligence service, and VIPRE business antivirus endpoint protection.

Learn more at www.ThreatTrackSecurity.com.

To learn more about ThreatTrack Security
call **+1-855-885-5566** or visit **www.ThreatTrackSecurity.com.**

ThreatTrack SECURITY