

## Advanced malware is smart:

It has been engineered to evade detection and bypass an organization's cybersecurity measures. This limits the effectiveness of many security defences that are in place today, and despite their investments in security technologies, many organizations still struggle to detect zero-day threats and targeted malware.

This paper examines the role of malware sandboxing in Advanced Threat Protection concepts and discusses the impact on an organization's security posture.

## Just Another Point Solution?

Do we really need a malware sandbox? You will have heard it said or perhaps said it yourself: Your organization has already invested in a multi-layered security environment, and now there is a request for yet another technology. Another point solution for malware protection? Is the additional investment justified?

What does a sandbox provide that an organization does not already get from their Next-Generation Firewall, their Intrusion Prevention and Intrusion Detection Systems (IPS, IDS), their Email Gateway, Web Gateway, or Antivirus? They also provide protection from malware.

In fact, nearly every organization already has technologies in their security stack that can detect malware, but in most cases, it is detection based on static analysis methods, using malware signatures or static heuristics. Very effective against known malware, and partially against variants of known malware, but not against threats that have not been seen before, such as zero-day malware and targeted malware. The problem lies in detecting the "unknown".

## The Challenge of Detecting Unknown Malware

A typical example of static analysis is the signature-based detection used by classic Anti-Virus solutions. These products maintain large, regularly updated libraries of unique identifiers (signatures) of known malware. If no identifiers are available because the malware has not been seen before, or the identifiers no longer match because the malware has disguised or changed its characteristics to evade detection, signature-based methods will not recognize the file for what it really is. There are other static analysis methods besides signatures, but all rely on "a priori" knowledge of known bad characteristics to identify malicious intent. The organization would still be at risk from unknown threats. Sandboxes provide the capabilities that are required to detect these unknown threats.

The operating principle of a sandbox is simple: it is an isolated environment that mimics an end-user system or a server system and allows a suspicious file to execute and perform all its operations (dynamic analysis). The files' interactions with the system environment are recorded and interpreted. Dynamic analysis identifies malware with a very high

## What is Advanced Malware?

- ♦ **Zero-Day Malware**  
Malware that is seen for the first time, with no identification characteristics (e. g., signatures) available yet.
- ♦ **Evasive Malware**  
Malware that uses sophisticated techniques to conceal its nature and recognizable characteristics, and thus evade detection.
- ♦ **Targeted Malware**  
Highly complex malware, designed to compromise the systems of a specific target-organization or industry sector. Remains inactive on non-target systems.

degree of confidence based on direct observation of the file's activities, without the need for signatures or reputation data. Malware sandboxes close the "unknown" gap in an organization's security stack.

## Malware Analysis Methods

### Is the Investment Justified?

To assess the business value of a best-of-breed sandboxing solution, consider the following aspects:

**Risk reduction** - The addition of advanced threat detection capabilities considerably reduces cyber risk. Risk has a quantifiable cost – loss of intellectual property, cost of incident response and disaster recovery, fines for non-compliance with data protection regulations, plus the intangible cost of long-term reputation loss. The Return on Investment is the prevention of disaster; the value is in cost avoidance.

**Efficiency gains** – The lack of connected workflows takes a heavy toll on the productivity of SOC and Incident Response teams. A sandboxing solution with strong process automation capabilities contributes to the creation of automation playbooks and increases the operational efficiency of the SOC as well as the speed and accuracy of Incident Response.

**Maximizing existing investments** – The integration of strong sandboxing technology into an organization's existing security fabric augments the resilience and efficacy of the entire system. The precise, actionable threat intelligence produced during the analysis process will be automatically shared across the ecosystem to catch threats that would otherwise be missed.

- ♦ **Static Malware Analysis**  
Performs detection by inspecting the file binary without executing it. It is essentially an analysis of text, looking for characteristics of known malware, for code anomalies or other tell-tale signs that indicate malicious intent.
- ♦ **Dynamic Malware Analysis**  
Performs detection by running the suspicious file in an isolated environment (sandbox) and observing its behavior. Delivers in-depth insight into malware behaviour. Essential for advanced threat detection.

#### Additional Benefits of Sandboxing



- ♦ **Automation of malware detection** workflows
- ♦ **Alert triage** and **alert validation**
- ♦ **Mitigation of skills shortage**, enablement of junior staff
- ♦ **Prevention of alert fatigue** and productivity loss
- ♦ Generation of **in-house threat intelligence**
- ♦ **Faster, more accurate** Incident Response
- ♦ **Reduction of Attacker Dwell Time**


#### Key Features of a Best-of-Breed Sandbox



- ♦ **High resistance** against sandbox evasion
- ♦ **Full visibility** into malware behaviour
- ♦ **Noise-free reporting** and actionable analysis results
- ♦ **Out-of-the-box connectors** for environment integration
- ♦ **Strong process automation** capabilities

## Conclusion

Malware sandboxing offers the opportunity to deepen the lines of defence and close the gaps while leveraging the security solutions that are already in place. But not all sandboxes are equal. Isolated, basic sandboxes used as tactical tools can only bring limited benefits to the organization's overall security posture. The addition of advanced sandboxing technology with strong automation, integration, and reporting capabilities will move the organization's security approach forward.

 visit [vmray.com](https://vmray.com) to learn about VMRay Analyzer, the Gold Standard for dynamic malware analysis.

## About VMRay

VMRay brings leading threat detection and analysis technologies to enterprises, government agencies and research institutions worldwide. VMRay's unique monitoring approach has overcome the detection issues of common sandboxing architectures – a breakthrough in automated malware analysis. Effective threat protection starts with effective threat detection.

