Buyer's Guide: Malware Sandbox Solutions

Criteria to Consider and Questions to Ask When Choosing an Advanced Malware Sandbox

A sandbox for automated malware detection and analysis is an essential component of an organization's advanced threat protection strategy. However, investing in a sandboxing solution without first getting a clear picture of the capabilities the sandbox must have to meet expectations, is likely to cause problems down the line. It is a recommended best practice to look beyond technical and performance considerations and evaluate how the new solution can provide value to the security stack that is already in place, to people and processes.

Advanced Threat Protection Defined

There is no single product that can ensure protection from advanced threats. It is the proper mix of threat prevention, detection, response, and mitigation measures, tied together into a multi-layered, cohesive security ecosystem that will achieve the highest possible level of protection. Integration of all technologies across the prevention–detection–response-mitigation process is a key requirement; a collection of individual products and disconnected workflows is bound to fail. The results achieved in one stage will inform the activities in the next stage, and the lessons learned during the mitigation stage will influence future measures in the prevention stage. Implemented correctly, it is a self-reinforcing cycle, and a strong sandboxing solution is an integral part of this cycle.

Must-Have Capabilities of a Strong Sandbox Solution

It is important to do a thorough side-by-side comparison of competing solutions. Do not short-cut the process by limiting the choices to the evaluation of the incumbent technology vendor. Include the following requirements in the selection process to build your short-list.

Requirement #1: Detection and Analysis Accuracy

- **Evasion Resistance**
  Advanced Threats are designed to recognize when they are running in a sandbox and will take evasive measures to avoid detection. Many sandboxes use in-guest monitoring, leaving tell-tale signs within the analysis environment. Look for a sandboxing technology that places the monitoring system outside the analysis environment and looks "from the outside in", so the virtual machines used for analysis can run completely unmodified. It is important that sandboxes replicate in every detail the actual desktop and server systems they are protecting, and allow Golden Images, pseudo-random attributes, different location settings, automated user interactions and automated reboot as part of the analysis environment. Sandboxes need to support all major file formats, scripts, archives, drivers, executables, as well as URLs. To counteract environment-aware malware, the sandbox must be able to detect the malware's environment queries and identify hidden code branches.

Two Key Questions to Start With

- How can we **maximize the value of the current security** stack?
- Which **additional technologies** are needed to fill the gaps?

Questions to Ask When Evaluating the Options

- **What is the impact on the environment –** does it augment or replace existing solutions?
- **What is the impact on team productivity –** does it increase or ease the current workload?
- **What is the impact on current workflows –** does it enable automation or is it a disconnected process?
- **What is the impact on the efficacy of the security program –** which KPIs will be positively influenced?

- **Monitoring and Reporting Quality**
  The sandbox must capture every interaction between the suspicious files or URLs and the system environment, with granularity that extends down to the level of function calls. Deep-dive investigations for incident response, digital forensics and threat hunting require a very high level of detail. Many sandbox solutions deliver analysis results that contain a significant amount of irrelevant background noise. This dilutes and obscures the critical information that analysts rely on to streamline incident response and trigger mitigation actions. Investigations are more time-consuming and Incident Response teams may even draw incorrect conclusions. Choose a sandbox that only captures signals that are relevant to resolving a threat. Analysts must be able to quickly gain insight into malware behavior, and machine-readable analysis results that are shared with other security systems must be reliable and precise. The ability of a sandbox solution to communicate clear analysis results is often underestimated.

Requirement #2: Resource Implications

- **Staff Productivity**
  Automation capabilities are a very important criterion, especially when staff resources are stretched thin and senior-level expertise is in short supply. SOC teams are flooded daily with alerts from different sources and are expected to rapidly spot the "needles in a haystack" – the alerts that signal a real threat. A strong sandbox has the capability to automate the alert submission from source systems such as EDR, SIEM, SOAR and network security technologies, and then validate the alerts, eliminate False Positives, and provide the information that is required for alert triage. The increased efficiency of junior staff frees up senior analysts to focus on advanced challenges, an important point in times of talent shortage and skill gaps.

- **Implementation, Maintenance, Scalability**
  Carefully assess "hidden" success criteria like implementation cost, implementation time, resources required for maintenance and management of the sandbox, deployment options and scalability. They all contribute to the overall success of the sandbox project. Choose a sandbox that offers deployment flexibility (on-prem, Cloud, a mix of both) and can be easily scaled up. The solution must be able to meet your organization's security requirements today and into the future. You might want to switch from a centralized sandbox today to regionally deployed sandboxes in the future, at an affordable cost. Total-cost-of-Ownership (TCO) may become an issue with appliance-based sandboxes due to scalability limitations. It goes without saying that a sandbox must offer a tightly integrated multi-stage analysis engine, combining static and dynamic methods. Known good and known bad files will be quickly discovered and removed from the process by different static methods and only the remaining unknown files will undergo dynamic analysis in the sandbox environment

Requirement #3: Integration Into The Broader Security Environment

- **Technology Stack Integration**
  No security solution can live in a silo. Defending against advanced malware requires significant coordination between the different technologies in the security stack. The solutions need to work together, share information, and correlate events if they are to achieve their full potential. The malware sandbox is no exception. The sandbox should have a wide range of out-of-the-box connectors to make integration

Questions to Ask Your Security Vendors

- How does it help us to **validate and triage alerts**, so we can quickly identify those that need immediate attention?
- Does it help us to prioritize and respond to threats by **providing actionable, contextual intelligence?**
- Does it supply structured insights that **enables junior staff to make informed decisions?**
- Does it automatically **share threat information obtained during the analysis** with the wider security environment?
- Does it help to **create automated malware detection** workflows and processes?
- Does it **protect our existing security** investment by enhancing its resilience?
- Is it **future-proof** by allowing us to **cost-efficiently** expand the deployment?

with the organization's existing security stack easy and offer APIs for custom-integrations. Typical technologies to be integrated are EDR, SIEM, SOAR systems, and Threat Intelligence Platforms (TIP).

- **Generation of In-House Threat Intelligence**
  Many security teams struggle to enrich their third-party threat intelligence data with their own threat intelligence that is based on the unique attacks they are already seeing inside their networks. With the right sandbox solution, the teams will be able to automatically extract highly reliable Indicators of Compromise (IOCs) from data gathered during threat analysis and, through proper integration with the wider ecosystem, have it automatically pushed to security tools that trigger the necessary measures. The quality of the in-house generated IoCs is of paramount importance. Do not invest in a solution that generates IoCs of poor quality, due to high noise levels, which miss out on critical details during analysis, and result in high False Positive rates.

Further Recommendations

Do not rely on third-party validation and vendor-provided information alone; conduct thorough internal testing of the short-listed solutions in your own environment. A solution that might be a perfect fit for another organization is not necessarily the best fit for yours.

Adding a sandboxing technology to the environment should support the following long-term objectives:

- **Move the organization towards a cohesive, synergetic security approach** that leverages integration, automation, and shared threat intelligence
- **Maximize investments** that are already in place today **by closing gaps or mitigating weaknesses** in the current approach

visit **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.