Malware Sandboxing: Your Deployment Options

Cloud, On-Premise, Managed Service or a Mix of All?

Malware sandboxes play a key role in advanced threat detection and incident response. To derive maximum value from your investment in sandboxing technology, make sure you allow enough time to evaluate the different deployment options available to you, and carefully consider their resource implications, such as implementation time, implementation cost, as well as staff resources needed to manage and maintain the sandboxing solution.

There are four main deployment models: managed in-house by your own security staff as an on-premise solution, managed in-house by your own security staff as a cloud-based solution, outsourced to a Managed Security Service Provider (MSSP), and lastly, a hybrid approach combining different elements of the above. **Each scenario has its pros and cons, so be sure you fully understand how they will work in your existing environment.**

Deployment Option 1: On-Premise

Pros: On-premise sandboxes investigate potential threats without any data leaving the organization's network. It is therefore the preferred option of organizations that are required to keep sensitive data within their own environment for compliance reasons. On-premise sandboxing solutions usually allow a somewhat higher degree of customization, such as the use of the organization's Golden Images or the modification of advanced settings.

Cons: Cost of hardware (sandbox appliance or server hardware), time and cost of initial implementation and ongoing maintenance. TCO can become problematic in appliance-based sandboxes due to potential scalability issues.

Keep in mind: A very important decision criterion for or against an in-house solution is the organization's ability to recruit, train, and retain the highly specialised security experts that are needed to deal with threat analysis and incident response. Depending on the security needs of the organization, the team would have to be large enough to provide 24x7x365 coverage. It goes beyond cost considerations - the cybersecurity skills gap is the true challenge.

Deployment Option 2: Cloud-Based

Pros: Cloud-based deployment offers faster time-to-value (no hardware to purchase, no implementation nor maintenance efforts required). They are easier to scale up and offer more flexibility in terms of regional coverage – at some point in time, you might want to move from a centralized sandbox to geographically dispersed sandboxes that are managed by regional teams.

Deployment Models Explained

- **On-Premise**
  Refers to solutions that are operated at the organization's premises by the organization's own staff.
- **Cloud-Based**
  Refers to solutions that are operated in a cloud environment by the organization's own staff.
- **Managed Service**
  Refers to solutions operated by a Managed Security Service Provider (MSSP), either at the provider's premises or in the cloud.
- **Hybrid Model**
  Refers to solutions that contain a mix of in-house and outsourced (MSSP) elements.

Cons: As data will be processed outside the organization's network environment, cloud-based solutions might not be an option for some highly security-sensitive organizations. As with on-premise deployments, in-house security specialists are needed to operate the sandbox.

Keep in mind: Regulated sectors such as health care, finance, and government are required by compliance regulations to have control over where their data resides. Before committing to any cloud-based solution, ask your shortlisted vendors what data center locations they can offer, if their cloud-offering allows the creation of completely isolated environments for each customer, if there are any open-source tools and services involved, and if their solutions conform with data protection regulations, such as GDPR.

Deployment Option 3: Managed Service

Pros: For smaller organizations, using a security-specialized service provider is often the easiest way to strengthen their cyber resilience quickly. The days are gone in which IT personnel could take care of cybersecurity alongside the job of running the systems. With managed services, they can leverage the expertise that is already out there.

Cons: Managed Security Service Providers (MSSP) have access to very sensitive business information, and this must be considered when outsourcing security operations. When using an external provider, you should audit them regularly, which includes visits to the facilities. Look beyond the impressive screens on the wall, ensure that your compliance and data privacy requirements are met and that you receive the level of security service needed to keep your organization safe.

Keep in mind: You cannot outsource responsibility.

Deployment Option 4: Hybrid Model

Pros: Hybrid deployment scenarios offer the highest level of flexibility. You can combine an on-premise sandbox, to retain critical data in-house, with a self-managed cloud-sandbox for better scale, or use any of the two in-house options together with managed services to provide 24x7x365 coverage for defined use cases. Some organizations decide to kick-start their project with managed services to obtain the much-needed malware detection and incident response capabilities quickly, then move to a hybrid model and build up own expertise along the way, and maybe after a couple of years move to full in-house operations.

Cons: You need to spend some time on the design of a well-structured hybrid model. The mix of different deployment options adds complexity to the system.

Keep in mind: Done right, you can get the best of both worlds with a minimum of drawbacks.

Recommendations

Choose the deployment model that best supports your organization now and also in the years to come. This will future-proof the investment. Shortlist and evaluate only vendors that can offer the full range of deployment choices because you might need the additional flexibility when your organization's structure changes. Regardless of the deployment model you decide on, always choose a sandboxing solution with superior detection, reporting and automation capabilities. Alert fatigue and low-quality analysis results impact in-house security teams and MSSP teams alike.

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.