CHECKLIST

Top 5 Considerations for Choosing a Robust Cloud-based Sandbox

The current threat landscape is rapidly evolving and aggressively opportunistic. Businesses in almost every sector face expanded risk exposure due to high volumes of remote working, advanced malware variants, and targeted attacks. At the same time, adoption of new digital innovations has shifted many services and applications from the data center to the cloud. As a result, organizations with lean IT security teams prefer cloud-based sandboxing to protect their data, users, and applications from zero-day threats in this new dynamic environment.

Five Things To Look for in a Cloud-based Sandbox Solution

☑ 1. Fast performance

A sandbox's security effectiveness should be evaluated within the context of its performance and vice versa.[1] Any sandbox solution needs to be able to keep pace with a rapidly changing threat landscape—both unknown malware as well as new variants of previously seen attacks.

Unfortunately, the current cloud-based service level agreement (SLA) from many sandbox vendors limits the ability to quickly respond to threats. This makes these solutions slower than most dedicated, on-premises sandbox appliances. An effective cloud-hosted sandbox solution should include an SLA that supports the ability to mimic appliance-grade performance.

☑ 2. No submission-rate limitation

Many organizations have been forced to accept limits on how many sandbox submissions are allowed for each integrated security device. This hinders growing security needs—especially as more work transactions happen remotely via the network.

These rate limits create unwanted risk exposure as submissions that exceed parameters are queued and sometimes even dropped if a certain time limit expires. For example, a next-generation firewall (NGFW) sends a suspicious object to the cloud-hosted sandbox for analysis while allowing traffic through. If this submission exceeds the daily limit and ends up being discarded, then potential threats are allowed to slip through.

☑ 3. Broader security architecture integration

Threats have evolved beyond targeting a single vector or using manually controlled tactics. The advent of Malware-as-a-Service allows even unsophisticated attackers to create coordinated threat campaigns that simultaneously target multiple entry points across an organization—all with just a few clicks.

As a result of these threat landscape changes, a cloud-hosted sandbox solution should easily connect to other security controls across the organization—such as firewalls, secure email gateways, endpoint protection platforms, and web application defenses—to enable wider threat visibility.

☑ 4. Automated breach protection

A majority of organizations struggle to recruit, hire, and retain cybersecurity talent. And three-quarters had at least one breach over the past year that could be partially attributed to a gap in cybersecurity skills.[2] Limited human resources leaves security teams underequipped for investigating and mitigating every threat alert they receive.

As a result, security automation has become a critical need. A robust cloud-hosted sandbox must instantly share threat information, not only to the submitting security control to initiate mitigation response but also with an organization's entire security ecosystem to automate breach protection holistically.

☑ 5. Centralized reporting based on security standards

An ideal cloud-hosted sandbox should offer a unified management console and follow standards-based reporting to help accelerate investigation. Instead of reviewing and reporting in different solution consoles, a single console view centralizes threat visibility and helps with correlation to distinguish an isolated threat from a broad and coordinated attack.

This centralized approach also supports reporting in a universal security language. The MITRE ATT&CK security standard describes malware threats by the techniques they use. Analyzing threats in this format within a sandbox report is imperative to help identify the type of threat faced.

[1] Jessica Williams, et al., "Breach Prevention Systems Test Report: Fortinet FortiGate 500E v6.0.3 + FortiClient v6.0.3.6219 + FortiSandbox v3.0.2," NSS Labs, August 7, 2019.

[2] "Fortinet Survey Finds Widespread Impact from Cybersecurity Skills Shortage," Fortinet, May 22, 2020.

August 12, 2020 4:27 AM

749382-0-0-EN

D:\Fortinet\Checklist\739670 - FortiSandbox Cloud\cl-top-5-considerations-for-choosing-a-robust-cloudbased-sandbox-V1-8122020\cl-top-5-considerations-for-choosing-a-robust-cloudbased-sandbox-V1-8122020