ENJOY SAFER TECHNOLOGY™

Cloud Security Sandboxing:

A DYNAMIC APPROACH TO THREAT PROTECTION

Security teams, users, and organizations gain efficiencies and improved threat protection with cloud-based security sandboxing.

Computers, routers, Wi-Fi networks, collaboration tools, and cloud-based applications have all become major attack targets since the global coronavirus pandemic started.

"The pandemic created a fertile environment for a whole range of cyber actors to take advantage," says Tonya Ugoretz, deputy assistant director of the FBI Cybersecurity Division.

Adversaries are launching sophisticated attacks to identify security weaknesses in endpoints accessing the enterprise network. This trend has exposed limitations in appliance-based sandboxing technologies that many organizations use to protect against endpoint threats.

Traditional sandboxing—an isolated environment to test an application or its components—is limited to on-premises devices and doesn't scale to meet the requirements of a widely distributed workforce. It focuses primarily on known threats, so it's not always strong enough against ever-evolving attacks and malware hidden in Secure Sockets Layer/Transport Layer Security (SSL/TLS) traffic.

Also, traditional sandboxing typically operates in Terminal Access Point mode, so it monitors only traffic passing through the network. Although it analyzes suspicious files and sends alerts, these notifications may arrive after the malware has hit the device—at which point the damage may already have been done.

Cloud-based sandboxing offers multiple security benefits

Cloud sandboxing offers multiple benefits compared to traditional appliance-based sandboxing, starting with the protection of end users and their devices. The cloud sandboxes sit between endpoint devices and the internet, inspecting traffic for malware and suspicious files—regardless of whether users are on-premises or in remote locations.

A cloud-based security sandbox also offers a virtual environment where a suspicious program can be safely executed and its behavior can be analyzed and reported in an automated fashion.

> "The pandemic created a fertile environment for a whole range of cyber actors to take advantage."
>
> — **Tonya Ugoretz, deputy assistant director of the FBI Cybersecurity Division.**

In such an environment, security teams can analyze ransomware, zero-day malware, and other threats in real time, without the malicious code having to touch a computer or network device. A cloud sandbox is typically integrated into the solution provider's threat intelligence platform and/or endpoint protection platform, so there is increased protection against zero-day malware and previously unknown threats.

CSO FROM IDG

For example, mature cloud sandbox providers apply artificial intelligence (AI) technology and machine learning (ML) models to inspect online traffic for malware and signs of anomalous behavior. The result is a more granular examination of threats and better reporting on security issues. In addition, the processing power required to do this sort of analysis and reporting is often unavailable—or too expensive to implement—on appliance-based sandboxes.

Another benefit: Cloud-based sandboxes provide an environment where developers can test applications and software for security issues before distributing them to users. Plus, they free IT security teams from routine, time-consuming appliance-based sandboxing tasks such as ongoing maintenance and updates.

Evaluation criteria for cloud-based security sandboxing

There is a difference in the quality and experience of solution providers in the cloud security sandboxing space. Here are some factors to consider and questions to ask:

File types and web objects that the cloud sandbox can analyze. Hackers use a variety of file types such as Word documents, PDFs, scripts, installers, and executable files to conceal malware. Consequently, the degree to which your organization is protected against online threats depends to a large extent on the ability of the cloud sandbox to inspect and analyze a wide range of files.

Your organization's tech stack. Consider your operating system environment and application stacks. If your organization has a heterogeneous IT landscape, you'll need a sandboxing solution that has the flexibility to protect users across all of these scenarios. Many threats can lurk in virtual environments and encrypted traffic. Can the cloud sandbox detect these threats without slowing things down?

Technical requirements. Many modern ransomware tools can infect and encrypt entire networks in a matter of hours. Bandwidth requirements and the speed with which the cloud sandboxing solution can analyze files are critical. Ask:

- How quickly can the cloud sandbox detect malicious files?
- How quickly can it quarantine your network?
- How quickly will the file classification occur?
- What level of file analyzation reporting will we receive?

Also, evaluate whether the solution provider's classification of files is sufficiently granular and relevant to support good decision-making. For example, does the vendor's definition of a "highly suspicious" file meet your organization's definition? Speed matters when it comes to decisions that can make the difference between keeping your business running and experiencing catastrophic disruption.

Total-cost-of-ownership considerations. Examine the cost-effectiveness of the cloud sandboxing solution and how flexible its licensing options are. Also, if the sandboxing technology has a steep learning curve, evaluate whether the benefits the technology offers are worth the investment in time and effort.

Finally, the partnership matters. Cloud sandboxing providers should be progressive in terms of their investments in automation, AI, and ML. At the end of the day, find out whether human expertise is involved or the provider is relying purely on automated analysis to classify files.

The bottom line

The rapidly changing threat landscape and the large-scale shift to remote work are driving the need for a better approach to sandboxing. Cloud sandboxes offer a cost-effective, scalable way to extend protection to distributed workforces, with few of the cost, maintenance, upgrading, and staffing issues tied to appliance-based approaches.