SOLUTION BRIEF

Eliminate SaaS-based Sandboxing Limitations with FortiSandbox Cloud

Executive Overview

There are a number of reasons for adopting Software-as-a-Service (SaaS)-based sandboxing—from securing new digital innovations, to protecting widely distributed environments, to compensating for a lack of security staff. Unfortunately, many SaaS sandboxing solutions cannot handle the fast-paced nature of the evolving threat landscape. This is because these offerings are based on shared infrastructure, creating limitations such as slower threat responses, capped submissions, and limited integration options. The Fortinet FortiSandbox Cloud Platform-as-a-Service (PaaS) solution eliminates these deficiencies by offering a dedicated instance of a sandbox in the cloud. This allows organizations to reap the many feature benefits of the on-premises FortiSandbox solution without the hassle of deploying and provisioning a physical device.

Adopting SaaS-based Sandboxing

Seven out of every ten breaches last year were caused by external actors—including an uptick in ransomware incidents.[1] In addition to a rising volume of sophisticated threats, organizations face expanded risk exposure due to increasing numbers of employees using remote access, advanced malware, and targeted attacks per business sector.

While virtual security controls can offer advantages over on-premises counterparts—from a reduced footprint, to improved performance, to simplified management—many of these solutions cannot offer sufficient protection in addition to these operational conveniences. The key reasons for adopting an effective cloud-hosted sandbox solution include:

Digital Transformation

Two-thirds of organizations that have embraced digital transformation have either already moved their data, services, and applications to the cloud or are in the process of doing so.[2] Leaving their on-premises security infrastructures (including sandboxing) behind, however, has created security gaps due to a lack of visibility as well as inferior detection and responses to threats.

Distributed Locations

Organizations with distributed environments (for example, retailers, gas stations, schools, embassies) that require ubiquitous protection find it challenging to deploy physical sandbox hardware in every location due to cost and complexity. At the same time, many organizations have recognized the benefits of software-defined wide-area networking (SD-WAN) for branch deployments, leading to its expanded adoption.[3] Under these conditions, protecting WAN links against unknown threats becomes even more critical because of increased risk exposure and an expanded attack surface.

Lean IT/Security Teams

A majority (68%) of organizations are understaffed and IT teams typically wear multiple hats in addition to managing security.[4] As a result, these organizations often stay away from time-consuming and resource-intensive investment in on-premises sandboxing. But because they still need the functionality of a sandbox to aid in their threat analysis and investigation efforts, they opt for a SaaS-based solution.

But with traditional SaaS-based sandboxing, a fair use algorithm is instituted for sharing the sandboxing resources across users—which provides greatly inferior performance in comparison to their physical sandbox counterparts. Many SaaS-based solution vendors have also introduced a cap on the number of submissions allowed for sandboxing. Moreover, organizations cannot expect their security infrastructure to fully integrate with SaaS-based sandboxing due to the complexity of vendor back-end management. This limits visibility and reporting of zero-day attacks, which eliminates the possibility of automated zero-day protection across the organization.

Evolving Beyond SaaS Sandboxing with PaaS Sandboxing

FortiSandbox Cloud is a step above SaaS-based sandboxing. Our solution provides organizations with their own dedicated instance of a sandbox in a cloud-hosted environment using a Platform-as-a-Service (PaaS) approach. FortiSandbox Cloud supports critical capabilities of an on-premises sandboxing solution without the hassle of deploying and managing a physical device. Its key solution benefits include:

FortiSandbox Cloud can easily analyze up to 72,000 files per day as it supports up to 200 sandbox VMs.

Fast and effective zero-day detection

In this evolving threat landscape, the FortiGuard Labs threat research team has noted a number of opportunistic attacks—including targeted threats seeking to exploit the COVID-19 pandemic,[5] and U.S. tax season,[6] as well as advanced ransomware attacks.[7]

To reduce the success of these attacks and potential damage caused by a breach, a sandbox's performance via the service-level agreement (SLA) is critical. Artificial intelligence (AI)-powered FortiSandbox Cloud leverages two machine learning (ML) models to power sandbox analysis—returning verdicts in mere minutes rather than hours. Furthermore, FortiSandbox is a proven effective solution as testified by customers, industry peers, and independent, third-party testing.[8,9]

Scalability

Traditional SaaS-based sandboxing solutions limit the number of suspicious objects that can be submitted for analysis. Once the limit is reached and the queue is full, these samples are discarded after a certain period—allowing potential threats to slip through. This not only creates undue exposure to risk but also hinders security's ability to keep pace with business growth over time.

As an organization's needs grow due to additional integrated security controls or increased traffic, users, and applications, FortiSandbox Cloud provides the flexibility to scale beyond initial sandboxing capacity through the addition of dedicated sandbox virtual machines (VMs).

Simple and Broad Integration

Perhaps the biggest drawback of a traditional SaaS sandbox is that it typically connects to only one or two native security products—leaving an organization blind to other threat vectors and the inability to apply sandbox protections across the broader security infrastructure.

FortiSandbox Cloud ensures zero-day threat visibility by integrating with both Fortinet solutions (via single-click configuration) as well as third-party solutions (via JSON application programming interfaces [APIs]). As seen in Figure 1, this broad integration helps organizations protect themselves against zero-day attacks hiding in both encrypted and nonencrypted network traffic.

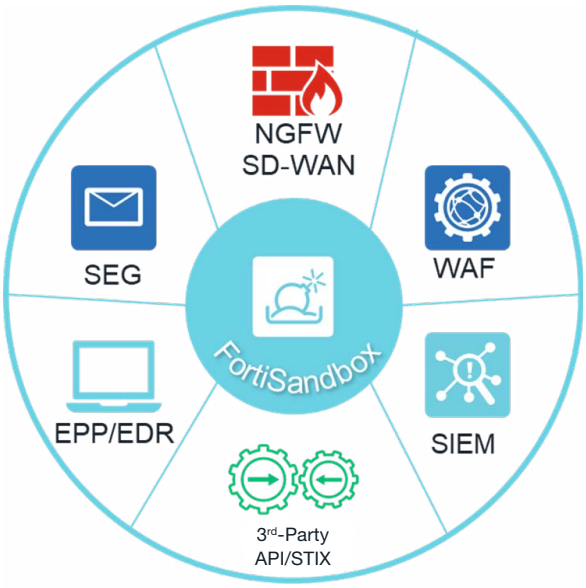

Figure 1: FortiSandbox offers broad integration across the network security infrastructure.

Automated Breach Protection

With the well-documented shortage of skilled cybersecurity talent worldwide, increased use of automation becomes an obvious priority to help balance resource allocation across IT support, network, security, compliance, and ongoing tool management demands. Yet only 38% of organizations are currently taking effective advantage of automation, artificial intelligence, and machine learning.[10]

FortiSandbox Cloud automates breach protection by providing threat intelligence in real time so policies can be instantly enforced. FortiSandbox integration with a next-generation firewall (NGFW) can automate blocking of malicious domains, IPs, or objects traversing the network. In combination with a secure email gateway (SEG) solution, FortiSandbox helps automatically block phishing attempts with malicious attachments or URLs. With an endpoint protection (EPP)/endpoint detection and response (EDR) solution, FortiSandbox helps quarantine malicious processes and objects or isolate a suspicious endpoint device without involving human staff. This greatly reduces threat response time and allows security teams to focus attention on higher-function tasks.

Centralized Reporting

When a threat campaign is waged against an organization, it can sometimes be difficult to discern an attacker's main objective in a timely manner. The broadness of some attacks creates a barrier to building a holistic mitigation plan due to the siloed and basic reporting capabilities offered by traditional SaaS-based sandboxes.

FortiSandbox Cloud acts as a centralized zero-day intelligence hub—gathering threats from every security control and presenting them in a single console. This in turn provides the ability to correlate attacks and determine if something is an isolated threat or part of a coordinated attack. With standards-based MITRE ATT&CK reporting built in, FortiSandbox Cloud helps accelerate threat investigation and accelerates proper mitigation actions being put in place.

Advanced SaaS-based Sandboxing Requires a Platform Approach

Organizations are concerned about the risk of business disruption due to the quickly evolving threat landscape. They need sandboxing that combines cloud-based convenience with the more robust protection offered by physical sandbox devices. Unlike existing SaaS-based sandboxing, FortiSandbox Cloud makes this possible by offering a dedicated sandbox in the cloud via its PaaS approach. This gives organizations superior sandbox performance, eliminates submission limits, provides scalability for business growth, and most importantly, integrates with the broader security infrastructure to automate protection against known and unknown threats.

[1] "2020 Data Breach Investigations Report," Verizon, May 2020.

[2] "The CISO and Cybersecurity: A Report on Current Priorities and Challenges," Fortinet, April 26, 2019.

[3] R. Brooks Borcherding, "4 Trends Driving Accelerated SD-WAN Adoption," Network Computing, February 5, 2019.

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

[5] Val Saengphaibul and Fred Gutierrez, "Attackers Taking Advantage of the Coronavirus/COVID-19 Media Frenzy," Fortinet, March 4, 2020.

[6] Xiaopeng Zhang, "NetWire RAT Targeting Taxpayers is Spreading via Legacy Microsoft Excel 4.0 Macro," Fortinet, April 14, 2020.

[7] Udi Yavo, "Update: Curveball Exploit (CVE-2020-0601) Starts Making the Rounds," Fortinet, January 21, 2020.

[8] "FortiSandbox Reviews," Gartner Peer Insights, accessed August 27, 2020.

[9] "FortiSandbox Certifications," Fortinet, accessed August 27, 2020.

[10] Kelly Bissell, et al., "Ninth Annual Cost of Cybercrime Study," Accenture and Ponemon, March 6, 2019.

September 5, 2020 6:04 AM

766366-0-0-EN

D:\Fortinet\Solution Brief\Teal Solution Brief\FortiSandbox Cloud\sb-FA-eliminate-saas-based-sandboxing-limitations-with-fortisandbox-cloud-952020