PRODUCT BRIEF

Symantec® Cloud Sandbox

Comprehensive solution for protection against unknown, advanced, and evasive malware

KEY BENEFITS

- Protects organizations against new, advanced, evolving, and targeted attacks
- Accelerates incident response and augments threat analysis
- Delivers greater detection and more accurate and relevant analysis
- Transforms malware exposure into continuous security improvement
- Provides exceptional performance to meet the most stringent security requirements
- Runs on Google Cloud to give customers comprehensive, fully scalable, enterprise-class malware detonation in highly realistic sandbox environments
- Combines contextual, static, emulation, and dynamic analysis techniques for more thorough malware analysis
- Executes malware in an environment that makes malware believe it's not being analyzed
- Presents detailed forensics and leverages shared threat intelligence gathered from all Symantec products and our global customer base
- Seamlessly integrates with the Symantec portfolio of security products
- Easy to enable with existing on-premises, cloud, or hybrid Symantec solutions

Introduction

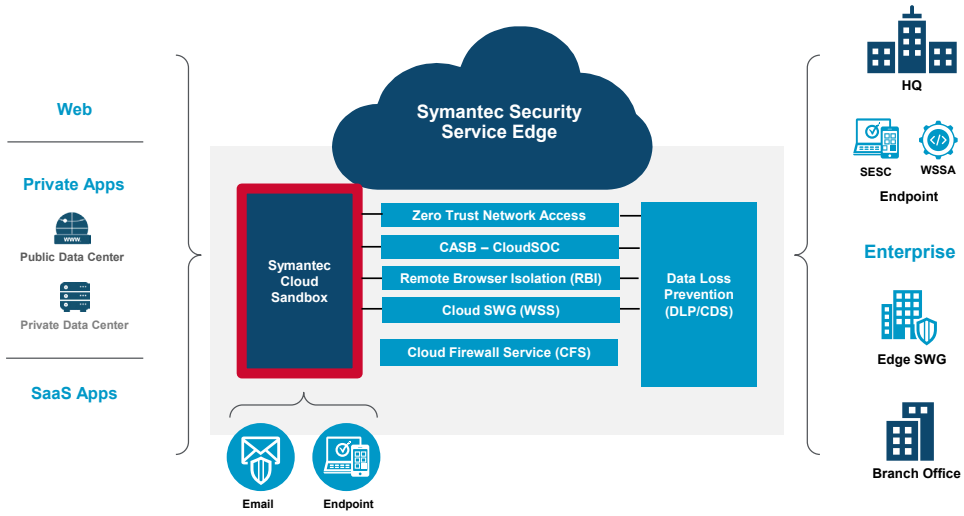
In the ever-evolving threat landscape, malicious actors are increasing the capabilities and resources available to produce new and advanced malware. To ensure that malware is detected and sufficient metadata is provided to aid threat-hunting and correlation capabilities, Symantec® Cloud Sandbox provides a leading platform for in-depth malware analysis. Over decades, Broadcom has invested in building technology to accurately identify malicious files at scale, and with the Symantec Cloud Sandbox, we deliver the full analytical power of Symantec solutions directly to your organization.

Symantec Cloud Sandbox is a fully managed service that provides detonation and analysis capabilities with little to no customer effort. This service makes it possible to scale as required to ensure significant resources are available to perform in-depth analysis and detect any new and evolving threats.

Solution Overview

Broadcom has a well-established track record, providing highly available, fully-managed cloud services with over two decades of enterprise-level performance, such as Cloud Secure Web Gateway and Email Security. Symantec Cloud Sandbox provides a highly scalable, geo-redundant, multitenanted, integrated, and effective sandboxing solution that is updated multiple times a day with new detection capabilities. As a cloud-based solution, Symantec Cloud Sandbox provides cloud-hosted analysis capabilities for both on-premise and cloud-based security products in the Symantec security product portfolio. In addition to the traditional sandbox providing behavioral analysis, Symantec Cloud Sandbox also provides new detection techniques and features not yet available on the endpoint or regular cloud analysis security products.

Figure 1: Integrated Symantec Cloud Sandbox Protection



KEY FEATURES

- Available to use with three data residency options (US, Europe, and Global), which allows customers to choose where the detonation happens.
- Reviews file metadata using Symantec Global Intelligence Network to eliminate known threats and benign traffic.
- Uses the file content, age, frequency, and other factors to identify threats that would otherwise be missed.
- Detects known and ever-evolving threats through Advanced Machine Learning.
- Conducts static scanning, disassembly, statistical/entropy analysis, emulation, and multi-level embedded/encoded artifact extraction for static analysis, to name a few.
- Executes potential malware in a controlled sandbox environment, where techniques like human presence and randomization allow malware to exhibit all possible features and expose itself for proper identification.
- Numerous new and leading-edge threat protection technologies are applied to the sample with additional resources that are only available in the Symantec Cloud Sandbox.
- Symantec URL categorization service uses the Global Intelligence Network to identify threats, threat artifacts, and malicious network activity.
- In addition to post-detonation, behavioral, network, and artifact analysis, the Symantec Cloud Sandbox also performs an active inline evaluation of the sample during detonation, which provides a richer, context-aware malware analysis.

Symantec Cloud Sandbox is hosted in the cloud and scales on demand to meet the needs of the many integrated services that support detection and analysis use cases. This allows the sandbox to not only effectively handle the ever-changing threat landscape and volatile traffic patterns effortlessly, but also ensures that the sandboxing solution is always available, delivering optimal performance.

Detect New and Advanced Threats

The Symantec Cloud Sandbox detects malicious code and suspicious behavior by using a proprietary conviction engine to inspect files using the vast array of prevention and detection technologies created over decades of research and development. This conviction engine arrives at either a clean or malicious verdict based on analyzing the file in the context of data from our comprehensive cyber-intelligence and sensor network.

To ensure accurate malware detection, the Symantec Cloud Sandbox execution environment leverages various behavioral tracing technologies, monitoring both user-mode and kernel-mode hooks. It observes not only the operating system and applications, but also the network activity through application monitoring and packet capture.

The behavioral tracing technology, which provides visibility into actual activity if malware is triggered, is also extremely valuable for analytics and threat-hunting purposes. When it comes to evasive malware, a growing trend is for malicious files to detect and identify the execution environments themselves, so they can either avoid detection or exhibit completely different behaviors in the hope of throwing security solutions off their scent. Symantec Cloud Sandbox actively works to mitigate these evasion techniques so malware can be accurately detected by creating a detonation environment that includes common applications and configurations that mimic a Windows desktop configuration. It can detect advanced threats that are looking to bypass analysis and further inspection. Such threats will be met with a busy Windows session that makes the malware believe it is running in a real user environment with documents and activity history.

Use Cases

Threat Protection: Polymorphic Downloaders

Attackers use a variety of downloaders and delivery techniques like documents (PDFs, Word) that entice users to execute malicious commands. Hiding or repackaging the downloader within these benign-looking documents often leads to the endpoint device receiving the malware being downloaded, leading to a compromised endpoint and potentially the start of a greater attack. Symantec Cloud Sandbox provides great protection against such threats, as the various obfuscations and static analysis evasion tactics do not deter the sandbox. The extra inspection techniques and resources available in Symantec Cloud Sandbox detect these threats before they reach the customer network.

SEIM Integration: Incident Analytics and Forensics

Analyzed samples from the Symantec Cloud Sandbox deliver evidence of suspicious activity that a customer's SIEM might use to correlate with telemetry from their endpoint solutions. This allows the ability to hunt down incidents where malicious actors might have found a new, unprotected vector to penetrate the organization's infrastructure.

On-Premises Security: Cloud Detonation and Inspection

On-premises network traffic analysis appliances installed with Symantec Content Analysis can be configured to perform detonations in the Symantec Cloud Sandbox. With cloud detonation configured, integration and scaling of on-premises appliances is simplified and the overhead of local sandbox provisioning and management is removed.

Product Integration: Symantec Email Security.cloud

Email has always been a key attack vector used by malicious actors to target businesses and public sector organizations. Email Security.cloud customers can enable Symantec Cloud Sandbox to deliver inline protection from new and rapidly evolving threats that work hard to bypass the static/emulation layers.

Product Integration: Cloud Secure Web Gateway (formerly WSS)

In addition to on-premises or hybrid content analysis solutions, customers with Symantec Cloud Secure Web Gateway (SWG) can enable the Cloud Sandbox feature to analyze suspicious files. Cloud SWG customers can benefit from aggressive protection features built into the Cloud Sandbox.

Product Integration: Symantec Endpoint Security Complete (SESC)

With Symantec Endpoint Security Complete, customers can evaluate breach assessments, conduct advanced threat hunting, and deliver incident analytics to correlate metadata for analyzed samples from the Symantec Cloud Sandbox.

Product Integration: Symantec Zero Trust Network Access (ZTNA)

Symantec ZTNA enables secure and granular access to any corporate resource, hosted on-premises or in the cloud, without the need for a VPN. Symantec Cloud Sandbox inspects suspicious files traveling over a ZTNA connection for potential malicious content.

BROADCOM®
connecting everything®

For more information, visit our website at: www.broadcom.com

SYM-Cloud-Sandbox-PB100 February 26, 2025