PRODUCT BRIEF

# Symantec® Malware Analysis Service

## CLOUD-BASED MALWARE PROTECTION

- A flexible subscription-based cloud service for combating malware and advanced threats
- Highly available, inline operation with active blocking capabilities to prevent threats from entering the enterprise
- Protection for remote and roaming users going direct-to-net to access websites and apps

## MULTIPLE LINES OF DEFENSE

- Accurate, real-time threat data from the world's largest civilian threat intelligence network
- Proxy-based architecture, including SSL traffic inspection, to filter web threats and orchestrate detailed analysis
- Customizable allow/deny list files and Symantec antimalware engine
- Predictive file analysis
- Identify and block zero-day threats
- Unknown file analysis and hold for verdict in your cloud Secure Web Gateway
- Dual detonation techniques (virtual/emulation) and custom virtual machines to defeat sophisticated attacks
- Behavioral and static (YARA) analysis: Interact with malware during detonation and design custom risk scoring

## Evolving Threat Landscape

Determined hackers coupled with the expanding adoption of cloud applications and the explosion of mobile workforce devices means that enterprises must find new ways to protect themselves from increasingly sophisticated, malicious attacks. It is a daunting challenge that raises tough questions for enterprises such as the following:

- How can we accurately identify and block all of the rapidly emerging known threats attacking our business without over-blocking our users and impacting their ability to do their jobs?
- How can we protect mobile and remote users effectively and efficiently?
- How can we protect ourselves from the sorts of zero-day threats which are increasingly finding their way into our environment?

Given their scarcity of resources, organizations need capabilities that will address these issues not only with enterprise-class capabilities, but with speed, simplicity and efficiency—terms synonymous with the cloud.

## Cloud-Based Malware Analysis

Broadcom has developed a cloud-based multi-tiered solution that includes advanced analysis techniques to identify and neutralize malware designed to evade detection technology. These techniques block known threats, analyze anything new and unknown, and combat evolved attacks. The entire system is designed to make sure that you get enterprise-class protection while ensuring that false positives remain extremely low, ensuring that precious security and incident response personnel are not wasting time chasing false alarms.

This service is delivered via the Symantec® SASE Network, providing swift and scalable access to critical security services.

## Multi-tiered Threat Defense

Symantec Malware Analysis Service works in concert with Symantec Cloud Secure Web Gateway (Cloud SWG) and the Global Intelligence Network (GIN) to give organizations the enterprise-class advanced threat protection they require.

### Symantec GIN

- The world's largest civilian threat intelligence network
- Quickly identifies known-bads from across the globe and provides real time updates to your system
- Classifies URLs into 80 over content categories and nine risk-related security categories to filter threats

### Symantec Cloud SWG

- Decrypts SSL encrypted traffic for deep content inspection
- Multi-layered antivirus and heuristic analysis combines to block sophisticated malware
- Customizable allow/deny list capabilities and file-reputation analysis tailored to your business

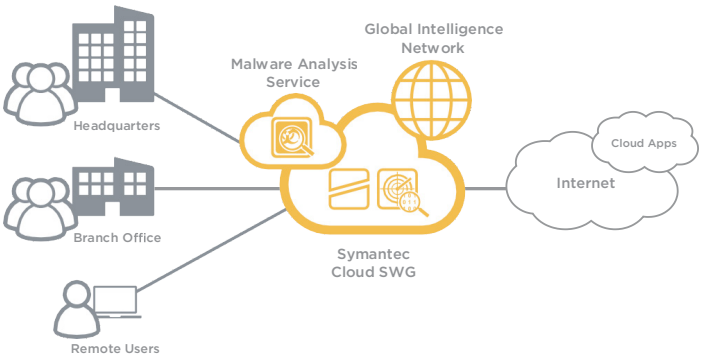
### Symantec Malware Analysis Service

- Provides advanced analysis (static code, YARA rules, behavioral) as well as in-line real-time file blocking
- Utilizes sandboxing to detonate suspicious samples; virtual and emulated environments are available
- Coordinates with the Cloud SWG to delay file delivery until all analysis is complete

## How It Works

This approach provides a highly efficient and scalable solution architecture for advanced analysis and incident resolution. Here is an example of how it functions:

1. A user downloads content from the web and the traffic passes through the Symantec Cloud Secure Web Gateway, which has content analysis capabilities to check the file in real time against the known-good-file allow list database hosted in the GIN. If it's listed there, the file is delivered and processing is finished.
2. If the file is not allowed, it is scanned by the antivirus (AV) engine in the Cloud SWG. If the file is known-bad, it is blocked and its URL is added to the GIN.
3. If the file is neither known-good nor known-bad, it is sent to the Symantec Malware Analysis Service for advanced inspection. When sandbox analysis is complete, the result goes to the Cloud SWG. If the file is malicious, the system updates its file hash database and tells the proxy component of the service to block all subsequent requests to the same object. It also updates the GIN with the object's URL, file hash, timestamp, and filename.




## Symantec Malware Analysis Service

To complement the capabilities of the Symantec Cloud SWG, we give enterprises a flexible subscription model to add malware and threat prevention service through two licensing approaches: Malware Analysis Service Standard Service and Malware Analysis Advanced Service—which adds broader file type support, mobile platform sandboxing, and more detailed reporting to the Malware Analysis Standard Service offering.

| Key Capabilities | Standard | Advanced |
|---|---|---|
| Static Code Analysis | • | • |
| Behavioral Analysis | • | • |
| YARA Rule Analysis | • | • |
| Inline, Real-Time Blocking | • | • |
| File and URL Reputation | • | • |
| Windows Emulation | • | • |
| EXE and DLL Support | • | • |
| Virtual Sandbox Support for Office and PDF Files | • | • *+ JAVA, MSI, RTF, ZIP* |
| Full Windows OS Detonation | | • |
| Full Detonation Report | | • |

### STRENGTH IN NUMBERS: SYMANTEC GIN

The Symantec Cloud SWG taps into the Symantec GIN, the world's largest civilian cyber-defense threat intelligence services. Fed by threat information from over 15,000 enterprises, 175 million consumer and enterprise endpoints, and over 1000 researchers and engineers, the solution categorizes and analyzes the threats posed by over a billion previously unseen and uncategorized websites each day and over 2 billion daily emails sent/received by our customers. Unique expertise minimizes false positives and you benefit from the network effect of joining thousands of Broadcom customers, giving you access to the world's most powerful analytical threat engine that will keep you a step ahead of fast-changing security threats.

BROADCOM®
connecting everything®

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


SYM-MAS-PB100 January 21, 2025