Symantec Malware Analysis Service

At A Glance

Cloud-based Malware Protection

- Utilize a flexible subscription based cloud service for combating malware and advanced threats
- Access highly available, inline operation with active blocking capabilities to prevent threats from entering the enterprise
- Protect roaming and mobile users going direct-to-net to access apps

Multiple Lines of Defense

- Access accurate, real time threat data from the world's largest civilian threat intelligence network
- Leverage proxy-based architecture, including ability to inspect SSL traffic, to filter web threats and orchestrate detailed analysis
- Utilize customizable white/black list files, dual anti-malware engines
- Utilize predictive file analysis

Identify & Block Zero-Day Threats

- Analyze unknown files and hold for verdict in your cloud-based secure web gateway
- Utilize dual detonation techniques (virtual/emulation) and custom virtual machines to defeat sophisticated attacks
- Implement 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's a daunting challenge that raises tough questions for enterprises, such as:

- How can we accurately identify and block all of the rapidly emerging known threats attacking our business without over-blocking our users an 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

Symantec 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 Symantec's distributed global cloud datacenter network, providing local access to critical security services from a certified, redundant, and highly available environment.

Multi-tiered Threat Defense

Symantec's Malware Analysis Service works in concert with Symantec's Web Security Service and Global Intelligence Network to give organizations the enterprise-class advanced threat protection they require.

Global Intelligence Network

- World's largest civilian threat intelligence network
- Quickly identifies "known bads' from across the globe and provides real time updates to your system
- Classifies URL's into 70 content categories and 9 risk-related security categories to filter threats

Web Security Service

- Decrypts SSL encrypted traffic for deep content inspection
- Multi-layered dual anti-virus and heuristic analysis combines to block sophisticated malware
- Customizable White-List/Black-List capabilities and file-reputation analysis tailored to your business

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 Web Security Service to delay file delivery until all analysis is complete

How It Works

Symantec's 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 Web Security Service secure web gateway, which has content analysis capabilities to check the file in real time against the known-good-file whitelist database hosted in the Global Intelligence Network. If it's listed there, the file is delivered and the processing is finished.

2 If the file is not whitelisted, it's scanned by one or two anti-virus (AV) engines in the Symantec Web Security Service. If the file is known bad it is blocked and its URL is added to the Global Intelligence Network.

3 If the file is neither known good or known bad, it is sent to the Symantec Malware Analysis Service for advanced inspection. When sandbox analysis is complete, the result goes to the Web Security Service. 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 Global Intelligence Network with the object's URL, file hash, timestamp and filename.

Symantec Malware Analysis Service

To complement the capabilities of the Symantec Web Security Service, Symantec gives 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.

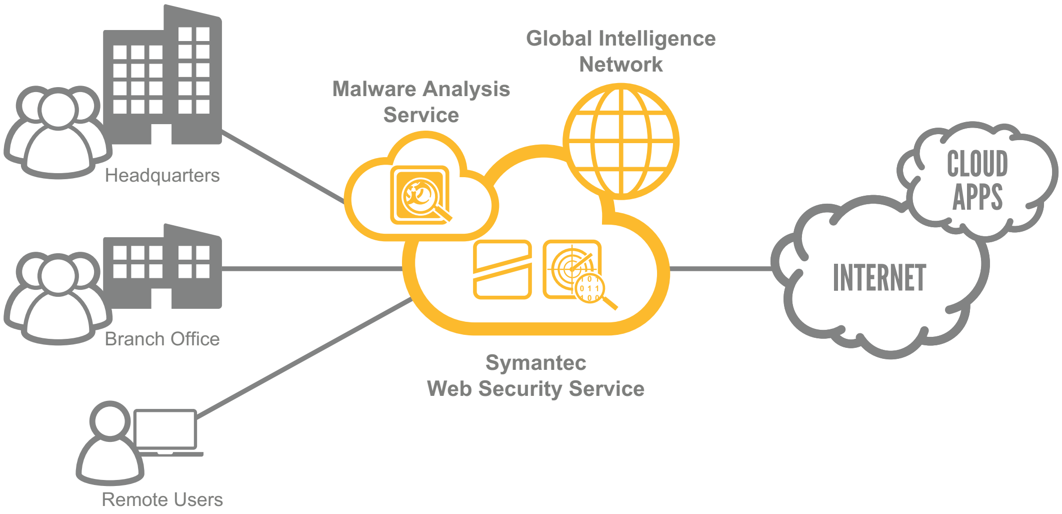
Key Capabilities	Standard	Advanced
Static Code Analysis	✓	✓
Behavioral Analysis	✓	✓
YARA Rule Analysis	✓	✓
Inline, Real-time Blocking	✓	✓
File and URL Reputation	✓	✓
Windows Emulation	✓	✓
EXE and DLL Support	✓	✓
Virtual Sandbox support for Office and PDF files		✓ + JAVA, MSI, RTF, ZIP
Full Windows OS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

Strength in Numbers – Symantec Global Intelligence Network

The Symantec Web Security Service taps into the Symantec Global Intelligence Network, 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 3,000 threat 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. Symantec's unique expertise minimizes false positives and you benefit from the network effect of joining over 90% of the Fortune 500 as a Symantec customer, giving you access to the world's most powerful analytical threat engine that will keep you a step ahead of fast-changing security threats.

About Symantec

Symantec Corporation World Headquarters
350 Ellis Street Mountain View, CA 94043 USA
+1 (650) 527 8000 | 1 (800) 721 3934 | www.symantec.com



Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps businesses, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton suite of products for protection at home and across all of their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit www.symantec.com or connect with us on Facebook, Twitter, and LinkedIn.