Symantec MessageLabs Web Security.cloud

Analyst View

"The Web has become the new threat vector of choice by hackers and cyber criminals to distribute malware and perpetrate identity theft, financial fraud, and corporate espionage."

IDC Worldwide IT Security Software, Hardware, and Services 2009–2012 Forecast and 2007 Vendor Shares: The Big Picture

The Symantec.cloud Difference

- Advanced architecture, providing unparalleled protection with minimal latency
- Industry-leading Service Level Agreement with money back remedies if performance levels are not met
- Single management console and shared threat intelligence shared across email, Web, and IM services for increased protection, visibility, and control
- Complimentary global 24/7 support is provided in 10 languages and delivered by SaaS specialists

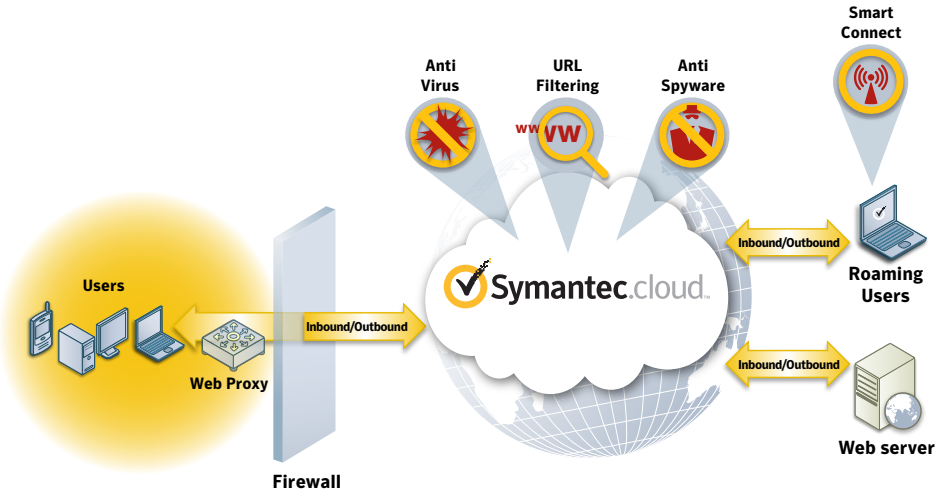
How Do You Monitor And Secure Web Traffic In Your Organization?

The Internet has become a fundamental business tool, yet browsing the Web has never been more dangerous. Attackers now leverage the Web as the primary vector for delivering viruses and spyware. Users who visit sites that have been compromised can unwittingly download malware that seeks to steal confidential information.

Organizations are also realizing that Web acceptable use policies need to be defined and enforced in order to maximize productivity, limit data loss, and minimize legal risk. The potential for Web misuse continues to increase as the use of Web 2.0 and social media sites is becoming more prevalent.

Symantec MessageLabs Web Security.cloud blocks web-borne virus, spyware and phishing threats and controls web traffic through URL filtering, enabling enforcement of Web acceptable use policies. Operating at the Internet level, Web Security.cloud blocks threats before they reach your network and uses URL filtering to restrict Web access by category, user, time of day, URL, or file type. Support for roaming users extends protection and policy enforcement to employees who access the Internet from outside the corporate network.

Web Security And Control



Web Security.cloud is delivered with minimal latency through our global network of highly available, load balanced data centers enabling fast, efficient, always-on protection without impacting the productivity of your users. Our solution is easy to deploy, easy to manage, backed by the strongest Service Level Agreement in the industry, and comes with complimentary 24/7 global support delivered by SaaS specialists in 10 languages.

Symantec.cloud

How The Service Works

- Web traffic requests are routed through Symantec. cloud and checked against your acceptable use policy
- If no policy rule is triggered, the request passes through
- If a policy rule is triggered, the request is either logged and allowed to pass or access to the Web page is denied
- Web page requests are retrieved by Symantec.cloud before delivery to your network and are scanned for known and emerging Web threats
- New and converged malware threats are identified by Skeptic™, while known threats are identified by multiple malware signature engines
- When a threat is identified, access to the requested Web page is denied
- If no threat is identified, the page is delivered to the user with no noticeable delay

Service Level Agreement

Web Security.cloud is backed by the following Service Level Agreement (SLA) performance levels:

- Web Anti-Virus Protection - 100% protection against known viruses
- Latency - Average scanning time of web content within 100 milliseconds
- Service Availability - 100% uptime
- Technical Support - response times for critical, major, and minor calls

Next Steps

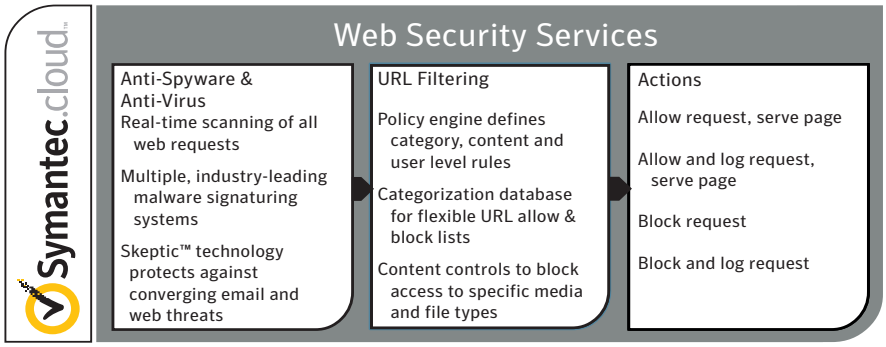
Contact a product specialist:
US: 866 460 0000
info@messagelabs.com

Web Security.cloud consists of two core components:

Multi-layer Security – Multiple commercial anti-spyware and anti-virus engines scan Web content for malware. These engines are continually updated by MessageLabs, ensuring accurate detection of known threats. Additionally, Symantec.cloud proprietary Skeptic™ heuristic technology guards against new and converging threats, which can target web users via other protocols such as email and instant messaging.

URL Filtering - All Web requests are checked against a sophisticated policy engine and URL categorization database to ensure appropriate content remains accessible while restricted content is carefully controlled. The policy engine is highly flexible and intuitive, enabling organizations to create policies and monitor behavior for specific users and groups.

Symantec.cloud offers a single, integrated management console for email, Web, and Instant Messaging, simplifying administration and lowering total cost of ownership while providing increased visibility into user behavior. Threat intelligence is shared across communication protocols for increased protection.



Feature	Benefit
Multi-layered anti-virus and anti-spyware defenses operating at the Internet level	Blocks viruses and spyware before they reach your network
Skeptic ™ heuristic technology	Protects against new and converging malware threats that span email, Web, and Instant Messaging
Distributed global architecture supporting minimal latency	Enables secure browsing without noticeable delay
Intuitive URL filtering policy-building engine	Enables organizations to quickly create Web use policies and prevent misuse by restricting access to undesirable sites and content
Highly configurable Web Policy Enforcement	Helps protect corporate bandwidth by restricting downloading of certain file types and allowing time or volume-based Internet consumption limits
Roaming user support	Extends protection and policy enforcement to employees outside the corporate network
Dashboard, summary, detailed and scheduled reporting	Provides visibility, accountability and confidence in the service's effectiveness