

Symantec MessageLabs Web Security.cloud

Analyst View

“Malware has successfully infiltrated nearly two-thirds of corporate networks through simple Web surfing”

Osterman Research, Messaging and Web Security Market Trends 2010-2013, August 2010

The Symantec.cloud Difference

- Threat Intelligence gathered across email, Web and IM protocols for enhanced accuracy
- Global Infrastructure is redundant and load-balanced for high availability
- Aggressive Service Level Agreement
- Single management console for email, Web, and IM services for increased visibility, and control

Service Level Agreement

MessageLabs Web Security.cloud is backed by a Service Level Agreement with money-back or other remedies if the following performance levels are not met:

- **Web AntiVirus Protection**
- 100% protection against known viruses
- **Latency** - Average scanning time of Web content within 100 milliseconds
- **Service Availability** - 100% uptime

The Growing Challenge of Secure and Productive Web Use

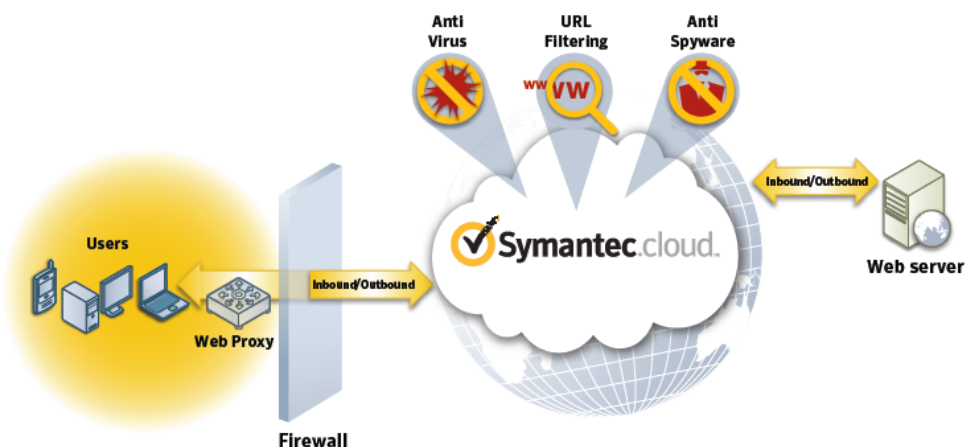
The Internet has become an indispensable business tool, yet browsing the Web has never been more dangerous. Attackers now utilise the Web as the primary vector for delivering viruses and spyware. Users who visit sites that have been compromised can unwittingly download malware that can harm your business.

Other factors associated with employee Web-usage and access have the potential to expose businesses to risk as well. The growing popularity of social networking and micro-blogging websites introduces the potential for malware risk and Web misuse by company employees. Organisations are realizing that Web acceptable use policies need to be defined and enforced in order to maximize productivity, limit data loss, and minimize legal risk. Also, as workers access the web from a growing number of locations, businesses need to take care to secure interactions and enforce proper usage for remote and roaming employees.

IT departments must determine how to best empower employees to safely and productively use the Internet to conduct business without burdening IT resources or impacting network performance.

MessageLabs Web Security.cloud helps protect your organization from Web-borne threats and enables the control, monitoring and enforcement of Web acceptable use policies with minimal latency. Anti-malware layers block threats safely away from your network while URL filtering policies and Web traffic quota limits reduce Web misuse and help you protect company bandwidth.

Help Secure Your Web Traffic and Enforce Proper Web Use



MessageLabs Web Security.cloud is delivered through our global network of highly available, load-balanced data centers enabling fast, efficient, always-on protection without impacting the productivity of your users.

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

About Symantec.cloud

Symantec.cloud is the world's leading provider of hosted services for securing and managing email, Web, and IM traffic (or communications).

Over 32,000 organizations and over 10 million end users in 99 countries employ Symantec Hosted Services to protect against viruses, spam, phishing, inappropriate Internet use, spyware and other organisation-damaging threats.

Taking Your Web Security to the Cloud

Comprehensive defences – Multiple commercial and proprietary anti-spyware and anti-virus engines scan Web content for malware before delivery to your network. Commercial engines are continually updated by Symantec Hosted Services, ensuring accurate detection of known threats and reducing maintenance and management burdens for your staff. Our proprietary Skeptic™ heuristic technology guards against zero hour threats.

Skeptic automatically shares knowledge when it is gained in one protocol with all other protocols enabling us to detect threats, which target more than one delivery method.

URL filtering and Web policy engine - All Web requests are checked against a policy engine and URL categorization database to ensure appropriate content remains accessible while restricted content is controlled. The policy engine allows administrators to create custom rules for select users, groups, specific blocks of time or by bandwidth consumption levels. To help administrators configure the service more easily, the URL Filtering feature contains default best practices rules for commonly blocked categories and a URL lookup tool to assist in the creation of custom policies. Our URL categorization database supports multiple categories within a single URL to help create policies for sites with dynamic content such as portals and Web 2.0 sites.

Predictable costs and simplified management: A regular subscription fee replaces large upfront expenses with affordable, predictable costs. Easy to set up and use, the service is efficiently managed from a central Web-based management console. Upgrades occur automatically to reduce administrative burden and help your staff be more productive.

Feature	Benefit
Multi-layered protection	<ul style="list-style-type: none">• Skeptic™ predictive technologies, combined with multiple commercial scanners help defend your organisation from zero-hour and known web-borne threats, addressing them safely away from your network
URL Filtering and Web Policy Enforcement	<ul style="list-style-type: none">• Enables administrators to create and enforce a Web Acceptable Use policy with rules based on content types and website categories.• Supports multiple categories for a single website URL.• Helps protect corporate bandwidth and productivity by blocking or restricting downloads of certain file types and placing time and volume limits on Internet consumption.
Minimal Latency	<ul style="list-style-type: none">• Average scan time of Web content occurs within 100 milliseconds and is backed by an SLA to provide confidence and set performance expectations• Globally distributed, redundant, and scalable architecture enables a consistent, secure browsing experience while minimizing delay to end users
Comprehensive Reporting	<ul style="list-style-type: none">• Dashboard, Summary, Detailed and Scheduled Reporting provide visibility, accountability and confidence in the service's effectiveness• Monitor compliance with your Web Use policies and Internet consumption levels using detailed reporting options for browse time, bandwidth use by URL category or individual websites