

# **Symantec MessageLabs Web Security.cloud**

## Technical Product Overview



# Symantec MessageLabs Web Security.cloud

## Technical Product Overview

### Contents

<b>Overview</b> .....	<b>1</b>
<b>Global Infrastructure</b> .....	<b>2</b>
<b>Connecting to the Service</b> .....	<b>2</b>
<b>Web URL Filtering</b> .....	<b>4</b>
<b>Policy Stack and Processing</b> .....	<b>6</b>
<b>Web AntiVirus and AntiSpyware</b> .....	<b>8</b>
<b>Skeptic™ Heuristic Technology</b> .....	<b>8</b>
<b>Smart Connect Roaming User Agent</b> .....	<b>9</b>
<b>Key Reporting Capabilities</b> .....	<b>10</b>
<b>A Comprehensive Service Level Agreement</b> .....	<b>11</b>
<b>Summary</b> .....	<b>11</b>
<b>Contact Information</b> .....	<b>12</b>

## Overview

IT departments of all sizes are facing greater security and management challenges as Web 2.0 and collaborative Web-based applications are becoming an increasing part of the workplace. Administrators are facing mounting pressure to open their networks to these Internet-based applications while also protecting endpoints from malware intrusion and preventing employee Web-misuse.

Attackers are adding to these challenges through the use of Web-borne threats that quickly appear and disappear and frequently leverage compromised legitimate websites. These sites rely on the trust of users who visit what they believe to be a 'safe' website to deliver malicious payloads or to redirect them to malicious content. This is done by using multiple media types which pull, or are fed information from sources such as scripts, plug-ins, databases, other sites and servers. Consequently, administrators are under greater demands to monitor their defenses and maintain accurate URL and Website content examination to prevent access to these sites. This can often be difficult given the global nature of threats, the need for timely updates and around-the-clock management to keep up with them.

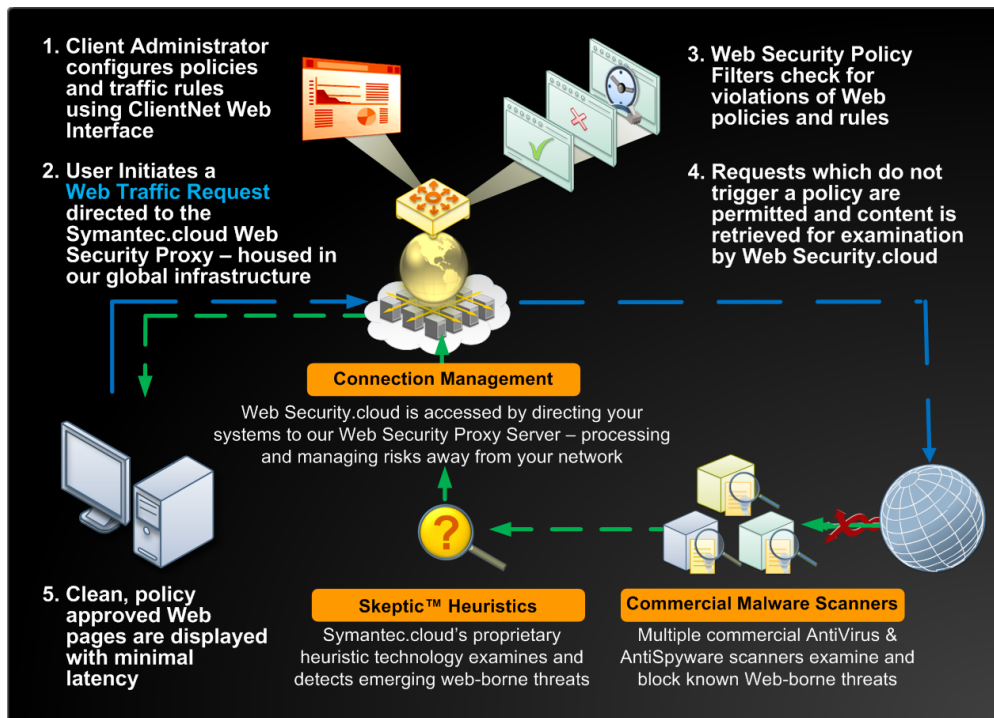
Web policy enforcement is equally important and must not hinder access to business-related resources while at the same time accurately help to avoid productivity losses, prevent data leaks and protect bandwidth. However, the changing nature of workplace Internet use can make measuring policy accuracy a moving target for IT. Permitting select users with access to certain restricted sites, limiting lunch-time use for non-business related activity and keeping Web content filters accurate for sites that have dynamic content can be especially challenging.

Symantec MessageLabs Web Security.cloud allows corporate administrators to create, monitor and enforce Web Acceptable Use Policies that facilitate more productive and safe use of the Internet within their organization. Our extensive URL filtering capabilities enable IT administrators to monitor and control user Web traffic requests while removing the technology management and maintenance hurdles that can be found in other solutions.

Web Security.cloud also uses a multi-layer approach to block Web-borne virus, spyware and phishing threats. This is done by blocking malicious content found on requested website destinations from being returned to your systems, filtering Web traffic requests to potentially dangerous sites, and inspecting all Web content downloads. Operating at the Internet level, Web Security.cloud helps block threats before they reach your network providing an additional layer of protection that resides outside of your corporate system resources. This also aids in optimizing your network bandwidth by processing only secure, filtered Web traffic. Organizations with roaming users who wish to extend their policies and security can also benefit from our optional roaming agent, known as Smart Connect.

This white paper outlines the technical approach used to deliver Web Security.cloud and the Smart Connect roaming agent. It will help illustrate how the service is accessed and administered to help our clients safely and productively use the Web in their organization.

*Web Security.cloud - How it Works:*



### Global Infrastructure

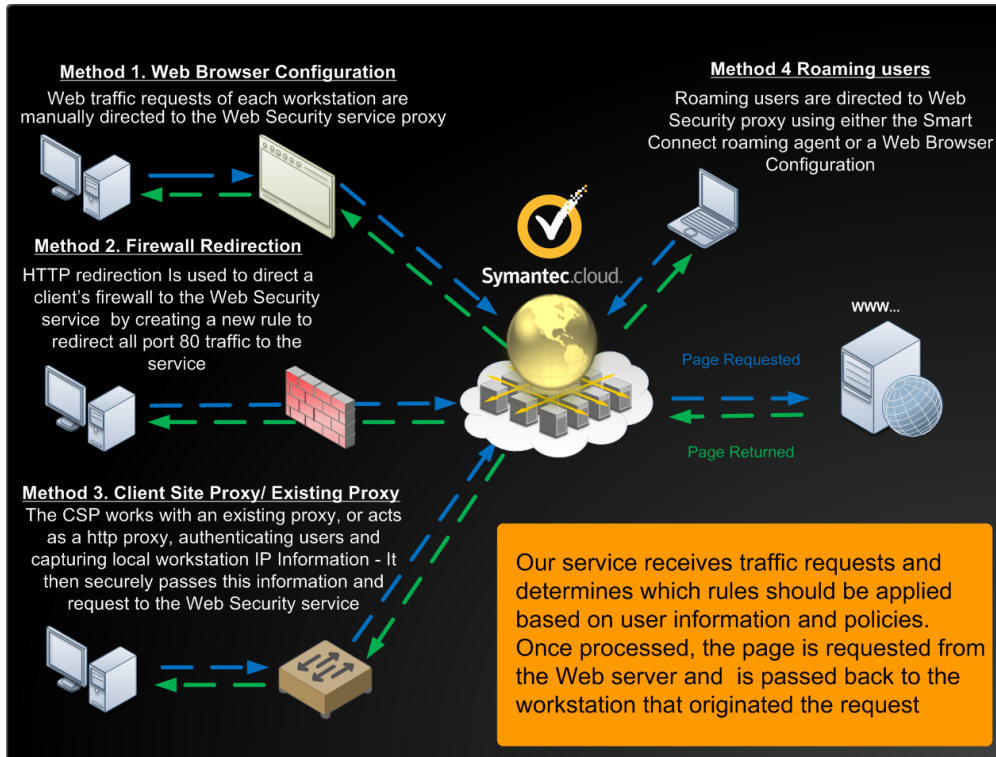
Web Security.cloud is delivered through a global infrastructure of 15 highly available data centers located across 5 continents. These data centers are load-balanced and housed in secure, well-established telecommunications centers located at major Internet exchange points. All data centers are compliant with best practice standards for security (SAS 70 Type II in the US or ISO 27001: 2005 in Europe). As such, our data center facilities feature extensive physical security controls, including 24–7 video surveillance, on-premise guards, biometric scans and mantraps designed with the highest levels of physical security and controlled access. As such, physical, keycard-only and fingerprint access to Symantec.cloud equipment is restricted to authorized personnel.

Because the data centers are load-balanced, Symantec.cloud is able to offer redundancy and handle spikes in traffic. This allows us to offer a Service Level Agreement target of 100% service uptime. We manage our servers to run at an average of 40 percent of their available capacity, providing ample headroom to handle any unexpected spikes in traffic or failure conditions.

### Connecting to the Service

Web Security.cloud customers use the service by directing Web traffic requests to the Symantec.cloud Web security servers for examination, rather than passing a user directly to the Web site or performing scanning within a client's infrastructure.

Configurations that can be used to direct requests to our service:



### Using a Direct Browser Connection

This type of connection allows customers to manually direct the Web traffic requests of each workstation to the Web security service proxy by configuring proxy settings within the browser itself. To make this process easier for administrators, the browser's proxy settings can also be configured Proxy Auto-Configuration (PAC) file if desired.

### Firewall Port Redirection

Customers can use firewall redirection as a means of configuring the Web Security.cloud service as well. Firewall redirection involves configuring the client's firewall to support HTTP redirection to the Web Security.cloud service infrastructure. This is done by creating a firewall rule that redirects all port 80 traffic to the Web security service on port 3128. By using firewall redirection, customers are able to keep their network protected with their existing firewall solution and to integrate its use with the Web Security service.

### Using the Client Site Proxy

Customers who wish to make use of the Group and User level configuration and reporting functions in the service may use a tool known as the Client Site Proxy (CSP). The CSP is a light weight proxy that authenticates individual user requests and provides the user information to the Web Security.cloud Web proxy system infrastructure.

The CSP performs the task of capturing the end user IP address, Windows domain and login ID of any users who request information. As such, the CSP acts as an authenticated Web proxy for internal computer workstations configured to use the CSP as their http proxy server. When a Web page is requested, the CSP authenticates the user against the local domain and captures the local IP information of the requesting computer, as well as the domain and user name. It then encrypts the information with the original request and passes this information and the original request to the Web security service. The service then evaluates which rules should be applied to the request based on this additional information. This information is compared against user and group information configured within the Web Security.cloud service infrastructure to apply policies specific to the user.

A Group Synchronization Tool is provided to clients to automate the synchronization of their directory-based user groups with the Web Security.cloud service. Once the rules have been processed, the page is requested from the Web server and is passed back to the end user workstation that originated the request. This is performed as one way synchronization initiated by the client to ensure that their directory always remains the master version. The synchronization is carried out over a secure SSL connection to Symantec.cloud with all of the customer's user data encrypted. This allows our clients to safely synchronize with the Web Security.cloud service without the risks of opening their directory to unwanted viewers.

In order to maintain the most accurate data for our service, Group Synchronization is equipped with the option for automated synchronization. This also helps to reduce any burden placed on an administrator to maintain this information.

The CSP can either integrate with Microsoft Internet Security and Acceleration (ISA) or Forefront Threat Management Gateway (TMG) server as a Web plugin. It is also offered in a standalone version for clients without a proxy server currently in place. It is easy to download and eliminates the need to install or update software on each workstation. The CSP also enables full directory-based user level reporting, alerting and configuration when used in conjunction with the Group Synchronization Tool.

### **Using the Smart Connect Roaming Agent**

Highly mobile users who connect to the internet away from the corporate LAN can still receive the benefits of Web Security.cloud by connecting to the service using our Smart Connect roaming agent. More information on how Smart Connect works and connects to the Web Security.cloud service can be found later in this document.

### **Web URL Filtering**

Web URL Filtering is the feature of Web Security.cloud that enables clients to set up policy rules for Web traffic requests to adhere to. Policy rules define actions to be taken when the administrator defined conditions match a user's Web request. There are currently 82 URL categories to select from when creating rules. A URL Categorization Look-up tool is available on the ClientNet administrator portal to aid in the accurate and rapid creation of policies.

Web URL Filtering is also supported by a database of approximately 70 million URLs. Every website URL is assigned at least one category although many have multiple categories assigned if the content spans more than a single category. Policy processing allows for execution of a rule action when either of these categories are matched, as well as handling situations where both categories match but have different rule actions. For example a customer may wish to allow Social Networking but block Blog sites.

The multiple category listing support and flexible rule action helps to address the challenges of large portal sites with diverse content, as well as dynamic user generated sites, particularly Web 2.0 sites. This means that your policies will be consistently enforced and users protected from sites that may one day contain acceptable content but the next introduce content that should be blocked.

Rules are configured using the Symantec.cloud user interface portal, known as ClientNet. ClientNet is an online portal which enables Symantec.cloud customers to configure, monitor and obtain reports about their services. Using ClientNet, rules can be configured for select users, groups, categories, individual websites, content/file types, restricted to specific periods of time/days of the week, as well as to control overall browse time usage or bandwidth consumption levels.

The ability to block or control usage of certain file types can be particularly useful to aid in protecting corporate bandwidth and productivity. Files such as streaming media that tend to be large or consuming can be blocked completely or limited to a daily bandwidth quota level.

Using the configuration options that Web URL filtering provides administrators of the service can create rules to address specific challenges. For example, a rule could be created that restricts access to sites such as Facebook or other social media sites during working hours while permitting employees to access them during lunch hours while on a break. This could also be done in a variety of geographic regions and with specific sites or categories as desired.

Web Security.cloud is also equipped with default best practices rules that can be used to block traffic to Web pages with URLs that are known to contain content in multiple categories. Examples of the categories you can use include: Adult/Sexually Explicit, Criminal Activity, Spam URLs, and Spyware.

Web URL Filtering rules are made up of a defined set of conditions that must be met in order to trigger the rule and its corresponding actions. The list of available conditions for setting Web URL Filtering Policies are:

**Time** - An administrator may select periods, days or blocks of time in which the rule should be observed and enforced. Multiple periods can be joined within a day (for example 9:00 am-12 pm and 1:00 pm - 5:00 pm)

**Groups** - Select user groups may be specified within a rule. This allows for granular rules to be created based on Active Directory groups or custom groups defined by the client.

**Quotas** - Quotas can be used to select daily browse time or bandwidth allowances that reset at 00:00 in the time zone(s) they are configured for. Quotas can be set by days of the week, selected hours of the day and applied to specific users or groups of users.

**URL Categories** - These consist of several choices that filter out commonly visited sites which are inappropriate for work use, viewing in the workplace environment or which impact user productivity. Examples include: Sports, Adult/Sexually Explicit, Social Networking, Shopping, and Webmail.

**Specific URLs** - Specific sites can be blocked which are deemed inappropriate or are not in keeping with the organization's Acceptable Use Policy or allowed as per a Client's needs. An example of this would be the Travel URL Category being blocked, but a client's corporate travel agency's Website being allowed.

**Content Types** - This is a useful way of preventing streaming media and larger file types from being downloaded or accessed in order to protect bandwidth, storage and productive Web use. Rules can be configured for specific MIME types and categories as well as custom file types and categories.

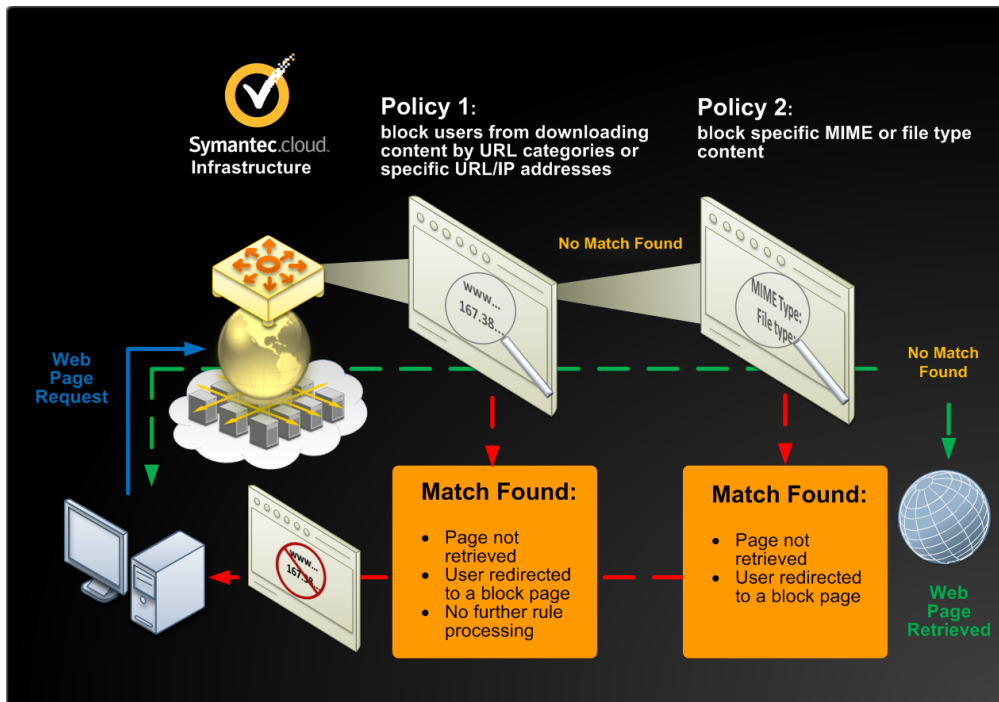
**Action** - Administrators are able to define the action that is performed when a Web request meets the conditions of a rule. Available actions include: allow, block, allow and log, block and log, quota, quota and log.

- Allow: The requested Web target is served to the user.
- Block: The request is halted and the Web target is not passed to the user
- Allow and log: Requested Web target is served and an entry is created to log the activity for administrator awareness and reporting purposes.
- Block and log: The request is halted/not served and an entry is created logging the event for administrator awareness and reporting.
- Quota: Bandwidth is accumulated against all downloaded content. Traffic is not permitted to pass once it reaches the administrator defined threshold. (Note: Only completed downloads count towards bandwidth.)
- Quota and Log: Same process as the above but with the additional step of an entry created to log the event for administrator awareness and reporting.

## **Policy Stack and Processing**

Once rules have been created using ClientNet, each policy rule is placed into a rule "stack" which is then evaluated in order from top to bottom. When the Web Security.cloud service proxy receives a request, it will pass the request to the policy engine for processing and validation.

Example of the Policy Engine Process:



In order for a rule to be executed, the criteria of each rule above it must be examined first. For example, organizations may have one policy that blocks users from downloading content by URL categories or specific URL/IP addresses and a second policy that blocks specific MIME or file type content. In this case, the policy engine will first check if the requested IP/URL matches any rules which block that specific destination. This could be based on URL name or upon the category it belongs to. If a match is found, the page will not be retrieved and the user will be redirected to a block page notifying them of the action taken by the service and no further rule processing will occur. If no match is found on the first rule, the second rule that filters MIME or File type content will be executed where the requested objects would be then checked individually for all content on the requested web page and would be either be allowed or blocked based on the second MIME content type rule filters.

### Processing Downloaded Files

When a file is requested for download by a user, the file is first evaluated against the policies associated with that user. If the file does not match a Web policy that requires it to be blocked (such as file type limitations or quota limits,) it is retrieved by our infrastructure where it is downloaded and scanned simultaneously for vulnerabilities or exploits. Once the scan is completed and the file is found to be clear of threats, it will be released and passed back to the user who requested the file.

Smaller files ( approximately 512 KB or less) are blocked until they have been scanned and users will not receive the HTTP response headers until the file has been scanned. Large files ( greater than 512 KB in size ) are streamed back to the user during scanning. This is visually represented to users by a progress bar that will display the status of the Web traffic scanning process.

The Web Security.cloud service is particularly adept at minimizing disruption to users when a requested file is larger in nature. This is mainly due to the large processing power our infrastructure is able to call upon to expediently download files and process them.

## **Web AntiVirus and AntiSpyware**

Once a Web traffic request has passed through Web URL filtering and on to the requested website, the content response is processed by the Web AntiSpyware and AntiVirus services for analysis. Web Security.cloud enables threats to be detected at the Internet level in order to identify and block inappropriate or malware bearing Web traffic safely away from our customer's systems.

The service begins by identifying known Web-borne threats and routing Web traffic responses through multiple malware scanning engines in parallel. Items passed through the service are scanned for malicious content including viruses, trojans, spyware and adware .

The scanners examine content responses for known threats that match virus signature files as well as some heuristics-based pattern matches for malicious code. If any single scanner response is unknown in terms of identifying the content as malicious or not, the process will wait until the second scanner indicates that the content is malware-free to be forwarded to the end user. However, if any one of the two content malware scanning engines indicates that the content is malicious, the response will be immediately blocked regardless of the status returned by the other scanning engine. This approach of parallel scanning and blocking on a single match provides a high level of detection accuracy for known malicious code.

Once a Web page or file are identified by Web AntiVirus or Web AntiSpyware as containing a potential threat, it is blocked and not delivered to the user. The user will then receive a block alert page indicating why the content is being blocked based on a customized message that is configured by the company administrator.

The scanners are kept up to date through automatic signature updates performed by Symantec.cloud so that the latest virus definitions can be used.

## **Skeptic™ Heuristic Technology**

Although signature-based scanners are effective in identifying many viruses, new or previously unknown threats may not be detected by commercial scanning engines. In order to detect new, 'zero hour' threats, Web Security.cloud uses predictive heuristic technologies built into a proprietary defense layer called Skeptic.

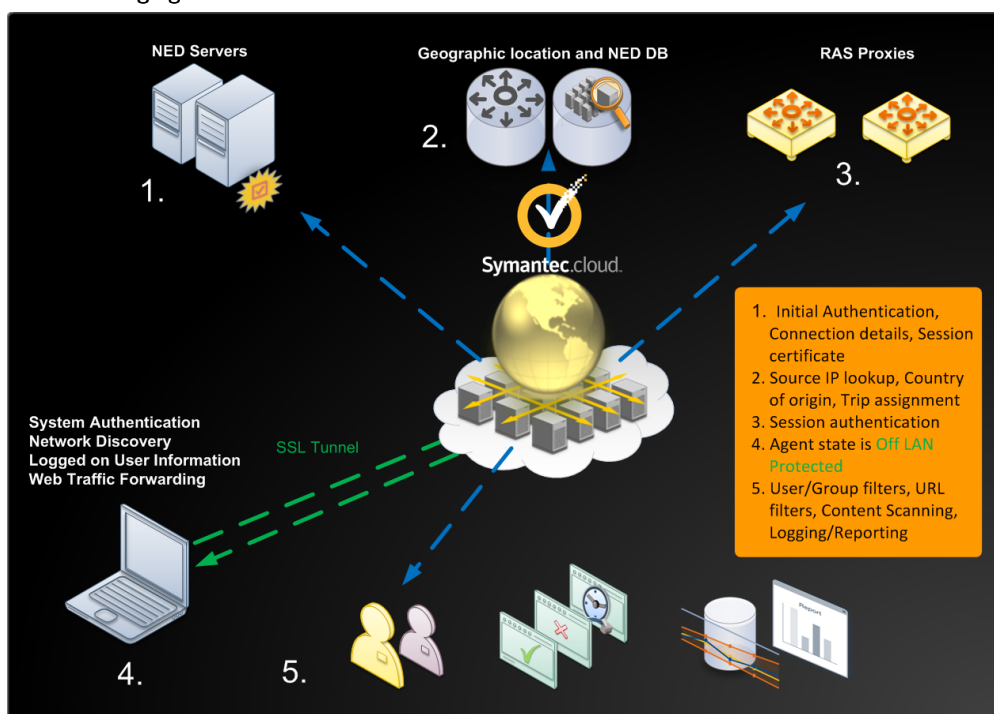
Skeptic employs heuristic technologies to help determine if the requested Web traffic contains any components of malicious code. Skeptic's multiple patented technologies and thousands of rules are applied to analyze and detect unknown threats. To provide enhanced performance, when a new item of malware is identified by Skeptic, a signature is created to enable rapid identification of the item in future instances of the threat. Unlike most commercial antivirus scanning engines, Skeptic cannot be downloaded and tested by cyber-criminals for ways of evading detection.

Skeptic also has access to information shared by the Email Security.cloud and Instant Messaging Security.cloud services to assist in the detection of converging threats (threats that leverage more than a single protocol). This aids in Web Security.cloud's ability to address the evolving nature of threats which frequently leverage multiple protocols. For example, threats that use URLs which link to malware and are sent within emails, but are executed using the Web.

### Smart Connect Roaming User Agent

To help meet the challenge of the increasingly distributed workforce, Web Security.cloud has an optional roaming user agent capability, known as Smart Connect, that helps administrators enforce their organization's policies and protect users who are outside the corporate network.

#### Smart Connect Roaming Agent - How it Works:



Smart Connect uses a locally installed agent-based technology that works in conjunction with the Web Security.cloud service infrastructure to protect roaming Web users.

The agent draws from the following capabilities to protect users and enforce policies without noticeable delay:

- **Network Environment Discovery** Smart Connect understands differences in end user networking environments and adjusts its behavior accordingly. For example, the agent forwards traffic in a passive state when in a captive portal where broader Internet access is not available initially, such as a Wi-Fi hot-spot, to allow payment authorization. Once the payment process is complete, the agent automatically switches to an active state by redirecting the user Web traffic to the Symantec Hosted Services infrastructure.
- **Location awareness** – Smart Connect uses a geographic location capability to identify a user's location and then connect them to the recommended infrastructure Point of Presence within the Symantec.cloud global infrastructure. This helps to ensure the best possible performance can be provided.

- **End user transparency** – Smart Connect provides a consistent sign-on experience regardless of whether the user is roaming off-LAN or connecting through a Web gateway within the corporate LAN environment.
- **Added security** – Smart Connect protects Web browsing via a Secure Sockets Layer (SSL) channel that is established between the agent and Symantec.cloud infrastructure. All communication occurs once both agent and infrastructure have mutually authenticated using X.509 digital certificates.

Smart Connect provides protection against Web-borne malware when users are outside of the corporate network, reducing the risk of a system becoming compromised and bringing malware back into the network upon the user returning to the office.

## Key Reporting Capabilities

Web Security.cloud includes several reporting options to inform administrators of the service's effectiveness and actions. Reports are configured and obtained using the service's ClientNet Web-based portal. Dashboard, summary, detailed and scheduled reporting options are included and are configurable to provide visibility, accountability and confidence in the effectiveness of the service.

**The Dashboard** provides an at a glance view of the current service performance levels and notable activities.

Dashboard graphs and charts show statistics for selected periods of time and include a summary of the volume of Web usage volume, blocked requests, filtered requests and top five blocked categories. Available timeline views range from 24 hours up to 12 months of service activities.

**Summary reports** provide status updates and metrics in a convenient PDF format. The summary report contains graphs, tables, and key statistics on Web volume, user activity, blocked threats and blocked Web page requests which violated the organization's policy. These reports can be customized to reflect a fixed or custom date range, and data for these reports is available from the previous day to the last 12 months of the use of the service.

**Detailed reports** are useful for in-depth service data analysis. Data can be downloaded in the Common Separated Values (CSV) format providing detailed service statistics. These CSV files can also be exported for more detailed analysis and to create custom reports.

Data in the detailed reports includes information on the performance of individual aspects of the service (Web AntiVirus and AntiSpyware performance, Web URL Filtering performance, User browse time by URL category, User browse time by individual URL, User bandwidth usage by URL category, User bandwidth usage by individual URL, the number of URLs visited by specific users, Total browse time or Total bandwidth by URL category or individual websites).

Detailed reports can also be customized by specific users, groups, IP (or IP range) date ranges and domains. The time intervals and date ranges available include the last 60 minutes, 12 hours, previous day, last 7 or 30 days.

**Audit reports** enable you to view detailed information on individual users and are provided in a PDF format. Audit reports include the same customization filters that are available with the detailed reporting option, however It is also possible to specify additional report criteria for more granular data, such as filtering activity by specific URL categories, Policy rules triggered, or destination website URLs)

**Scheduled reports** are available to supply regularly updated information about the activities of the service. These reports can be made available for download to ClientNet users in the reporting section of the service portal or emailed to other company personnel who may not have access to the ClientNet portal. The scheduled reports can be any combination of the summary, detailed, and audit reports mentioned. The frequency of the report can be customized and scheduled to occur on a daily, weekly, or monthly basis at a specified time and reporting interval.

### **A Comprehensive Service Level Agreement**

Web Security.cloud is backed by an aggressive and comprehensive Service Level Agreement (SLA) that includes money back remedies if the following performance levels are not met:

- Antivirus Effectiveness – 100% protection against known Web viruses
- Latency – average Web content scanning time within 100 milliseconds
- Availability - 100% service up-time
- Technical Support - specific response times for critical, major, and minor calls.

### **Summary**

Web Security.cloud helps clients defend against Web-borne threats and enforce Web Acceptable Use Policies (AUPs). Our service helps to block viruses and spyware at the Internet level away from our customer's network. Our Web Security services help to protect organizations from Web misuse and help to prevent wasted bandwidth and productivity loss.

The key advantages of our service offering include our extensive investment in providing protection against new and emerging threats, our comprehensive URL filtering capabilities, our global infrastructure footprint and a broad and flexible set of service reporting options. We also provide an intelligent roaming agent for mobile users to extend your protection, policies and reporting while providing a seamless experience for your users.

Delivered as a hosted service, our solution is scalable to fit your needs as they grow and does not require the upfront investment and hardware costs found in other solutions. By using Web Security.cloud you can spend less time managing your defenses and policies and more time on the projects that enable and drive your business.

### **Next Steps**

**Begin a [free trial of Web Security.cloud today!](#)**

## Contact Information

### AMERICAS

#### UNITED STATES

512 Seventh Avenue  
6th Floor  
New York, NY 10018  
USA  
Toll-free +1 866 460 0000

#### CANADA

170 University Avenue  
Toronto, ON M5H 3B3  
Canada  
Toll-free :1 866 460 0000

### EUROPE

#### HEADQUARTERS

1270 Lansdowne Court  
Gloucester Business Park  
Gloucester, GL3 4AB  
United Kingdom  
Tel +44 (0) 1452 627 627  
Fax +44 (0) 1452 627 628  
Freephone 0800 917 7733

#### LONDON

3rd Floor  
40 Whitfield Street  
London, W1T 2RH  
United Kingdom  
Tel +44 (0) 203 009 6500  
Fax +44 (0) 203 009 6552  
Support +44 (0) 1452 627 766

### NETHERLANDS

WTC Amsterdam  
Zuidplein 36/H-Tower  
NL-1077 XV  
Amsterdam  
Netherlands  
Tel +31 (0) 20 799 7929  
Fax +31 (0) 20 799 7801

### BELGIUM/LUXEMBOURG

Symantec Belgium  
Astrid Business Center  
Is. Meyskensstraat 224  
1780 Wommel,  
Belgium  
Tel: +32 2 531 11 40  
Fax: +32 531 11 41

### DACH

Humboldtstrasse 6  
Gewerbegebiet Dornach  
85609 Aschheim  
Deutschland  
Tel +49 (0) 89 94320 120  
Support :+44 (0)870 850 3014

### NORDICS

St. Kongensgade 128  
1264 Copenhagen K  
Danmark  
Tel +45 33 32 37 18  
Fax +45 33 32 37 06  
Support +44 (0)870 850 3014

### ASIA PACIFIC

#### HONG KONG

Room 3006, Central Plaza  
18 Harbour Road  
Tower II  
Wanchai  
Hong Kong  
Main: +852 2528 6206  
Fax: +852 2526 2646  
Support: + 852 6902 1130

#### AUSTRALIA

Level 13  
207 Kent Street,  
Sydney NSW 2000  
Main: +61 2 8220 7000  
Fax: +61 2 8220 7075  
Support: 1 800 088 099

#### SINGAPORE

6 Temasek Boulevard  
#11-01 Suntec Tower 4  
Singapore 038986  
Main: +65 6333 6366  
Fax: +65 6235 8885  
Support: 800 120 4415

#### JAPAN

Akasaka Intercity  
1-11-44 Akasaka  
Minato-ku, Tokyo 107-0052  
Main: + 81 3 5114 4540  
Fax: + 81 3 5114 4020  
Support: + 852 6902 1130



## About Symantec.cloud

More than 31,000 organizations ranging from small businesses to the Fortune 500 across 100 countries use Symantec.cloud to administer, monitor, and protect their information resources more effectively. Organizations can choose from 14 pre-integrated applications to help secure and manage their business even as new technologies and devices are introduced and traditional boundaries of the workplace disappear. Services are delivered on a highly scalable, reliable and energy-efficient global infrastructure built on fourteen datacenters around the globe. A division within Symantec Corporation, Symantec.cloud offers customers the ability to work more productively in a connected world.

For specific country offices and contact numbers, please visit our website.

Symantec World Headquarters  
350 Ellis St. Mountain View,  
CA 94043 USA +1 (650) 527  
8000 1 (800) 721 3934  
[www.symantec.com](http://www.symantec.com)

Symantec helps organizations secure and manage their information-driven world with [managed services](#), [exchange spam filter](#), [managed security services](#), and [email antivirus](#).

Copyright © 2011 Symantec Corporation. All rights reserved. Symantec and the Symantec Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.  
3/2011 21170376