WHITE PAPER: ENDPOINT PROTECTION.CLOUD - TECHNICAL PRODUCT OVERVIEW

# Symantec Endpoint Protection.cloud

## Technical Product Overview

*Employing cloud-based technologies to address security risks to endpoint systems*

Symantec.cloud

# Symantec Endpoint Protection.cloud

## Technical Product Overview

**Contents**

## Overview

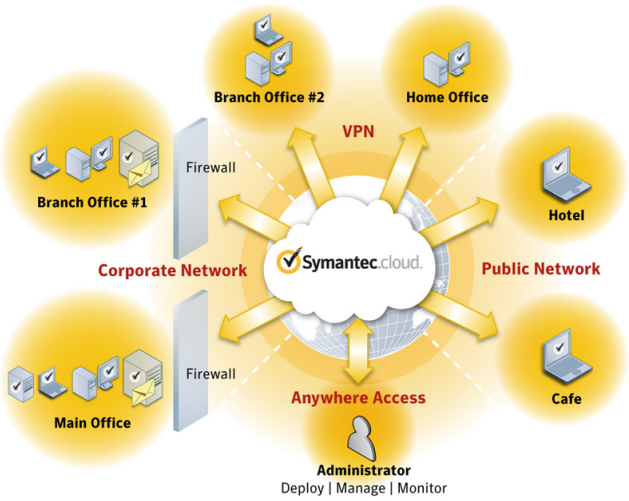
Today's IT managers are faced with the challenge of navigating an increasingly complex threat landscape . This challenge is compounded by the fact that employees are increasingly working in remote and distributed configurations. As a result, IT departments are demanding highly accurate security solutions that are easy to set up and maintain regardless of administrator or user location. These requirements are important to businesses of all sizes, but especially so to small and medium-sized businesses (SMBs) that have limited resources to help stay current with changing security requirements while managing numerous additional IT responsibilities.

Symantec Endpoint Protection.cloud offers a way for IT managers of SMBs to manage endpoint security for end users within and outside of the corporate network. The hosted service delivers advanced technologies that help protect customers' Windows-based systems without requiring additional hardware, management software, or dedicated IT staffing.

Endpoint Protection.cloud combines Symantec's 18 years of experience developing technology for endpoint protection with MessageLab's 10-plus years of software-as-a-service leadership to deliver and manage protection for computers connected anywhere. The solution offers antivirus, antispyware, firewall, and host intrusion prevention, all managed from a single web-based console.  It aids IT Managers in addressing security risks by helping to contain malware, eliminate infections, prevent data loss associated with corrupt machines and reduce unwanted applications such as media file sharing.

This white paper describes how the solution works, what protections it provides, and how the network-wide deployment of agents helps to keep security levels and policies current. It will also illustrate how the service is deployed and administered to aid in keeping computer systems protected.

## How the Service Works




- The administrator logs on to the Web-based management console and deploys the agent to individual endpoint systems or can use a remote management server to silently push the agent to the organization's computers.
- Upon installation, preconfigured policies are enabled for the agent to include antivirus, antispyware, firewall, and host intrusion prevention.
- After the install, the agent proactively refreshes the latest security definitions and updates.
- Administrators can use the management console to set custom policies and push to all endpoints in the network.
- The management console is also used for ongoing maintenance including deploying new endpoints, viewing status and managing remote clients.

## Successful Service Delivery

Successful service delivery relies on three core components: the cloud-based service infrastructure, which is the core service intelligence, the web-based management console, which provides the administrative interface, and the local agents which reside on selected endpoint systems.

The service infrastructure is the combination of technologies managed by Symantec.cloud that allows delivery of hosted services that include security policies, updated protection levels, alerts and messages.

The Web-based management console is the tool used by the administrator to deploy and manage the service.

The agent delivers services to a selected endpoint (laptop, desktop, or file server); it communicates information about system health, threats, and security policies with the management console. The agent receives protection updates via the service infrastructure. Agents are deployed via standard download or email invitation. They can also be deployed to an organization's computers using a redistributable package.

Once installed on the selected endpoint systems, the agent is in position to help defend customer computer systems against a myriad of risks and threats.

### Comprehensive Global Threat Intelligence for Endpoint Defense

The large number of Symantec customers around the world provides the business with visibility into a tremendous volume of security threats. Symantec is able to feed that information back into its research and development teams. The data collected during the Endpoint Protection.cloud threat management process is reported to Symantec's research groups and aggregated with data from Symantec customers around the globe. Symantec research groups – including

Symantec Global Intelligence Network and MessageLabs Intelligence are recognized by industry analysts as key to improving product efficacy.[1]

Symantec Global Intelligence Network processes over 8 billion email messages daily and gathers malicious code intelligence from more than 133 million desktop, server, and gateway antivirus installations that allow malware, spyware and adware to be captured and transmitted back to Symantec Security Response centers for analysis. Symantec virus definitions updated 3 times a day and for every major outbreak. All this allows Symantec to provide customers with comprehensive protection in an evolving threat landscape and greatly improve the ability of customers to protect their businesses with the most current information available.

## Protection for Desktops and Laptops

### Cloud-Based Reputation Database

Nearly every threat today is unique in some way and is designed to evade detection - putting pressure on the traditional signature-based approach. Attackers often create threats that quickly appear and disappear. By the time a signature file is created for a particular malware variant, it has already changed itself – rendering the signature ineffective. Symantec Endpoint Protection.cloud integrates proven antivirus and antispyware technologies to provide traditional, signature-based protection in combination with behavior-based, proactive protection capable of defending against variations of known threats as well as new and emerging threats.

It uses a cloud-based reputation database to examine downloads to your desktops and laptops for malware. Since its inception in 2007 more than 175 million endpoints around the globe have contributed information to the reputation database.

This database possesses data on millions of applications and individual files that have been statistically evaluated to determine a reputation for each one. This innovative approach offers improved protection for users by using Symantec's deep threat knowledge base to help determine how likely an unknown executable under evaluation is to carry some form of malware.

### Intelligent Scanning Technologies

Endpoint Protection.cloud uses the reputation database to check applications already installed on end user laptops and desktops. Most users run "good" applications of known origin, developed by known publishers which carry a number common attributes which indicate their legitimacy. Conversely, suspect applications have very few users, an unknown publisher, and other attributes that give it a poor reputation making it suspect. This data allows Symantec to calculate a reputation safety score for each application. Without ever having to ask the user, Symantec can statistically infer with an extremely high degree of accuracy the likelihood of an unknown application being good or bad.

The reputation database also assists with more efficient scanning. The service will prioritize scanning of suspicious executables and applications first - thereby maximizing protection while minimizing impact on systems performance.

## Endpoint Perimeter Defenses

### Antivirus

Virus and security risk protection features provide comprehensive virus prevention and security risk detection for desktop and laptop systems. Known viruses are automatically detected and repaired. Instant messenger attachments, email message attachments, Internet downloads, and other files are scanned for viruses and other potential risks. In addition, regular definition updates help keep users prepared for the latest security risks.

### Antispyware

Symantec Endpoint Protection.cloud Antispyware is designed to detect these major categories of spyware: Security risk, hack tool, spyware, trackware, dialer, remote access, adware, joke programs, security assessment tools and misleading applications.

### Advanced rootkit detection and removal

Rootkits attack the Windows file system and as a result they can conceal themselves within existing processes. Traditional anti-malware tools rely on the Windows file system APIs to list, scan, and delete files, often preventing effective detection and removal of rootkits.

Endpoint Protection.cloud provides rootkit detection and removal using the VERITAS Mapping Service which enables thorough analysis and repair with access below the operating system. VERITAS Mapping Services is able to parse the raw data on the disk to determine the location and content of files through direct examination of disk sectors even if the Windows file system functions have been attacked by a rootkit. By detecting and removing the most difficult rootkits, the service helps to save time, money and lost productivity associated with having to re-image infected machines.

### Firewall security

Defends against hackers with a quiet two-way firewall. The Smart Firewall monitors the communications between protected user desktops and laptops and other systems on the Internet.

It also protects customer endpoints and alerts administrators to such common security problems as:

- Improper connection attempts from other computers and of attempts by programs on protected endpoints to connect to other computers.
- Intrusions by detecting and blocking malicious traffic and other attempts by outside users to attack protected systems.

The firewall is referred to as a “smart firewall” because it does a pre-check on a network application against its application database and can force a virus scan before an application can fully launch.  If the application being launched passed the initial start up checks but doesn’t have any firewall rules associated with it, the smart firewall will automatically create access rules for the application.

A firewall blocks hackers and other unauthorized traffic, while it allows authorized traffic to pass. The service provides a configurable option which allows a local endpoint system user to override the firewall configuration for a certain period of time in order to permit an installation or other administrative function.

### Host Intrusion Protection

Helps guard against malware attacks that exploit vulnerabilities in applications that interact over the internet. Intrusion Prevention scans all the network traffic that enters and exits selected endpoint systems and compares this information against a set of attack signatures. Attack signatures contain the information that identifies an attacker's attempt to exploit a known operating system or program vulnerability. Intrusion Prevention protects customer computers against most common Internet attacks.

If the information matches an attack signature, Intrusion Prevention automatically discards the packet and breaks the connection with the computer that sent the data. This action protects systems from being affected. Intrusion Prevention relies on an extensive list of attack signatures to detect and block suspicious network activity. Administrators should run regular definition updates to ensure that the list of attack signatures is up to date.

### Web Security Features

Analyzes the security levels of the Web sites end users visit and identifies unsafe and dangerous websites right in the search results. This service lets users know if websites are deemed safe to visit and alerts them to known unsafe and malicious websites, including phishing sites that could steal personal information. Web security features can also help to protect your Web browser against drive-by downloads from malicious Web sites, proactively blocking new or unknown malware programs before they attack endpoint systems. This secures sensitive company information and prevents the attackers from controlling endpoint system remotely. Administrators should check browser requirements to make sure that they can utilize web services.

### Regular Security Updates

Protection levels for all desktop and laptop security services are kept current with regular “pulse” updates that occur every 5 – 15 minutes for up to the minute protection. The service agents are not chatty. Agents send the system a heartbeat twice a minute and check for updates every five minutes. Updates to the software and the agent itself are delivered using the Symantec’s LiveUpdate technology and can vary in size.

### File Server Defenses

Symantec Endpoint Protection.cloud offers advanced antivirus/antispyware for Windows-based file Servers. This service protects file servers by blocking viruses, spyware, Trojan horses, worms, bots, and rootkits using traditional signature-based technologies.

File server protection services also include Symantec TruScan™ Proactive Threat Scan,. TrueScan is a feature that is currently targeted to detect Trojans, Worms and Key logger categories of threats, but may also be able to detect other threats which exhibit similar characteristics. The advantage of the TrueScan heuristic feature is the ability to detect/ mitigate threats without the need of a specific threat signature. TrueScan works by first enumerating all active processes on the file server and processes behavioral data associated with the application. Then, TrueScan uses hundreds of

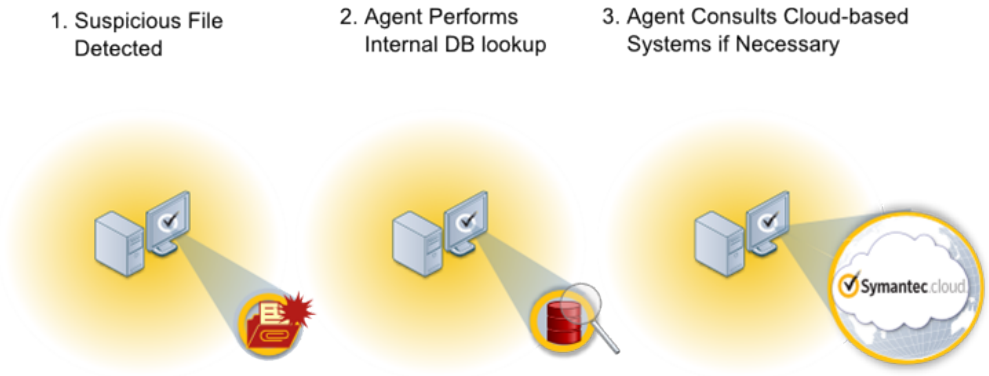
detection modules (valid and malicious) to correlate the process with behavioral data to determine if it exhibits a particular behavioral attribute.

TrueScan uses a set of advanced algorithms to determine if an application should be deemed malicious based on its behavioural attributes. TrueScan also looks for known good attributes (Pro-Valid detection Modules) in an effort to minimize false positives.

And, like the security services for desktops and laptops, our file server defenses benefit from Symantec's security infrastructure, the Symantec Global Intelligence Network, that provides unparalleled insight into today's threats.

## Using and Configuring the Service

The agent's defense mechanisms detect the threat and evaluate it using the agent's local database. The local database is a cache of recent queries and responses from the cloud-based reputation database. By referencing the local database first, the service provides better performance for scanning because it can go directly to the cache rather than requiring internet access for each query. If a threat cannot be evaluated locally, the agent contacts the cloud-based reputation database for a conviction.




When the agent identifies a suspicious file as a known threat or risk, it isolates it to quarantine state. When the endpoint is safe, it reports the incident to the service. The administrator is alerted whenever an event pierces the alerting threshold configured by the administrator.

Administrators have the ability to view alerts in the management console, they can also customize delivery via email or SMS text. Alerting thresholds can be set by alert type (general, policy, detected risk) and severity.

Administrators can use the management console to view information about and take action on quarantined threats. For example, administrators can view quarantined threats by machine, search by threat name or type and delete threats, or restore a selected quarantine item to the computer.

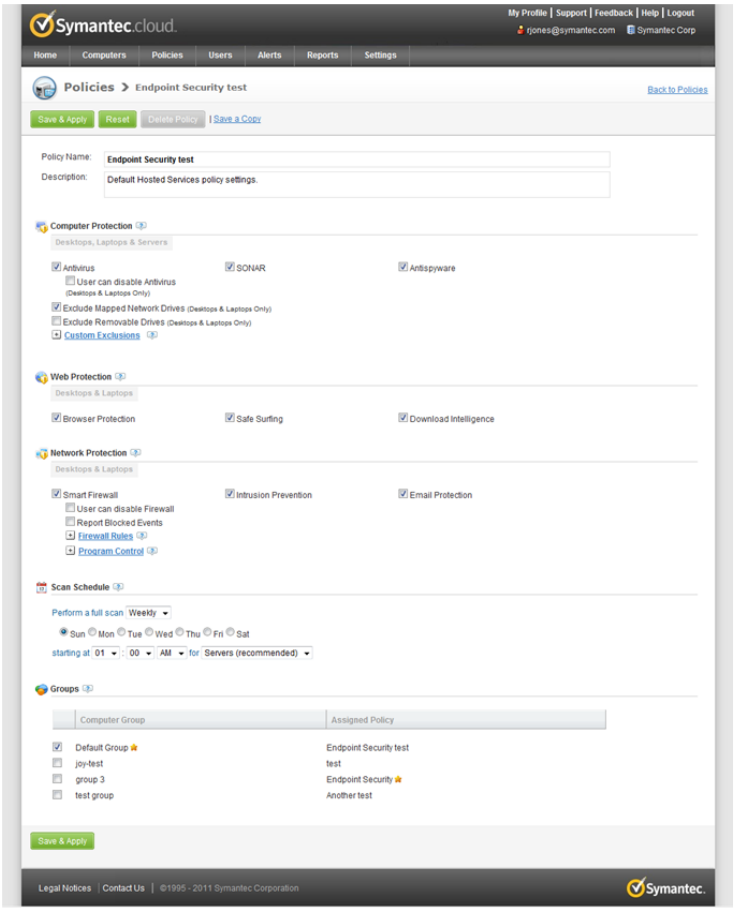
## Management and Administration

*Web-based Management Console*

Administrators can manage their service from a single Web-based management console accessible via an internet connection. The management console enables an administrator to: invite users to install the agent, manage computers, create and modify company policies, create/manage additional users to manage the console, set up alerting and schedule/run reports. It provides multiple system health and threat indicators that together offer a comprehensive view of company-wide security. Administrators can easily drill down into any indicator for more information.

Policies allow an organization to uniformly apply security policies across a group of computers. Symantec Endpoint Protection.cloud offers businesses a default selection of pre-defined security policies. The use of pre-defined policies accelerates set up and requires less customization on the part of the administrator. Upon installation of the agent, pre-configured security policies for antivirus, anti-spyware, firewall, and host intrusion prevention are automatically applied to new users. The protection settings available within a policy are dependent upon whether the policy is being applied to a laptop or desktop agent or to a file server agent.

*Endpoint Protection.cloud: Policies – Summary View*



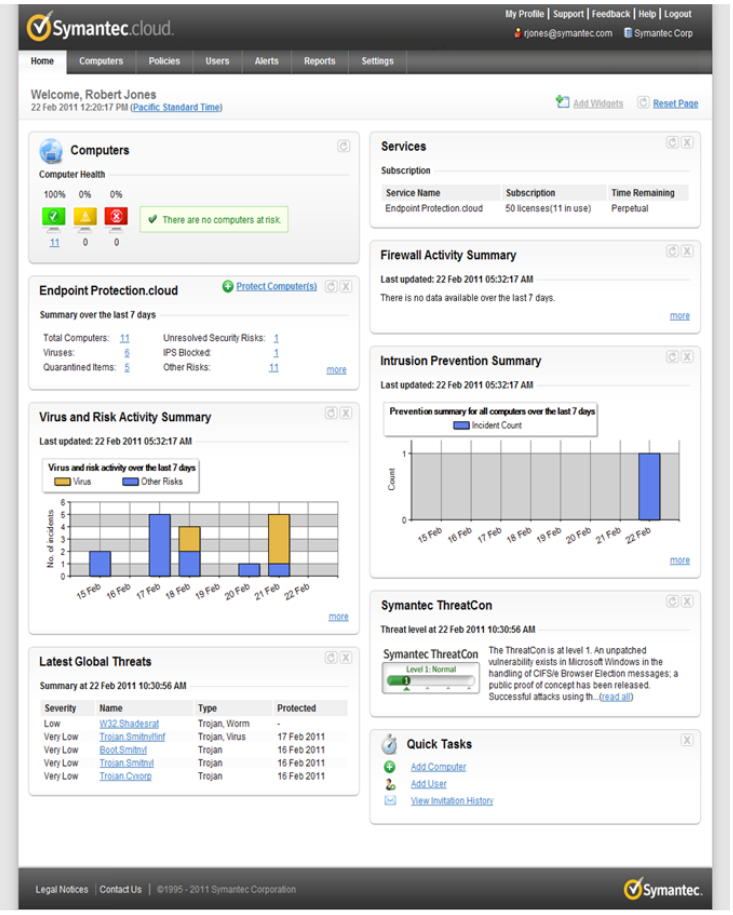

Symantec Endpoint Protection.cloud offers businesses pre-defined, configurable security policies. Administrators may use management console to set custom policies and push to all endpoints or a group of endpoints in the network.

Using the management console, administrators can make logical groups for the computers within their organization and decide which default policies are best for each group. The administrator can then apply those policies to specific groups.

Because the Endpoint Protection.cloud agent connects directly to the cloud-based service infrastructure, all security definitions and end user security policies are automatically updated via the internet whether the endpoint is on the corporate network or roaming.

Upon logging onto the management console, administrators are presented with an at-a-glance summary of network protection levels. Administrators can also use management settings to receive alerts on system health via email or SMS without requiring logging onto the console. When responding to an alert, an administrator will access the management console to take any number of actions – for example, they may issue a command to delete the malicious files held in quarantine by the agent; or might proactively scan groups of computers.

*Endpoint Protection.cloud: Home – Summary View*




Administrators can manage their service from a single Web-based management console accessible via an Internet connection.

Endpoint Protection.cloud offers a number of other configurable options to administrators. For example administrators can configure firewall settings for desktops and laptops through the management console. They can allow, block, or monitor network services destined for specific ports on the machines. Administrators can also use these settings to allow or block specific applications running on the desktop, report on blocked events, and allow or block file and printer sharing.

This level of granularity provides administrators with greater control over security settings and protection levels that are better tuned to their business needs as a result.

Administrators also have the ability to take group action support and lock user rights. Group action support capabilities ease administration by allowing administrators to centrally trigger group actions such as virus definition updates and scanning action for multiple online computers that belong to one or more groups. The lock user rights feature can be used to ensure that AV protections stay in place by preventing users from manually turning off the AV service on their computers (desktops and laptops).

## Reporting and Alerts

The management console is also used for running, setting distribution preferences, and viewing reports. Endpoint Protection.cloud provides five configurable reports to help customers analyze data and manage their systems.

**Alert history** – Shows the history of alerts for any group of computer systems the administrator selects.

**Security audit** – Provides a summary of user-generated events, including logons, jobs run and modifications made.

**Firewall history** – Summarizes firewall events for one or more computers.

**Risk detection** – Details the numerous types of risks detected in one or more computer systems.

**Security overview** – Provides threat summary information that includes: Top Ten threats, Firewall activity, Top Ten Network Intrusion attacks, and Phishing attacks.

The reports can be run in the default configuration or tailored using a report wizard tool. They can be formatted as: PDF, HTML and XML and can be delivered to multiple users as an email attachment or simply be posted in the management console when data is available.

## Service Level Agreement

Symantec Endpoint Protection.cloud is backed by a Service Level Agreement that targets 100% availability of the service portal is not met. In addition, customers benefit from strict support levels to guarantee service and support when required.

### Part of the Symantec.cloud Portfolio

Customers benefit from advanced protection from the endpoint to the gateway when they use Symantec Endpoint Protection.cloud with Symantec.cloud offerings for email, Web, and instant messaging (IM) security.

These solutions for hosted email, web, and IM security help protect systems from threats in the cloud that could enter your network through the corporate gateway. Endpoint Protection.cloud provides security on the machine itself. When used together, administrators can breathe easier, knowing that their users are protected from threats that can enter their environment through any number of entry points inside and outside the corporate network.

## Summary

Symantec Endpoint Proteciton.cloud helps protect Windows-based desktops, laptops, and file servers with advanced technologies for antivirus, antispyware, firewall, and host intrusion prevention - all managed from a single Web-based management console.

With Symantec Endpoint Protection.cloud, automatic security updates occur transparently over an Internet connection, enabling employee systems to stay current whether workers are in the office or on the road.

At Symantec, we understand that our customers face many demands, and that today it is more difficult than ever for IT Managers to stay current on evolving security requirements alongside the day to day responsibilities. Symantec Endpoint Protection.cloud provides the protections our customers expect, is simple to use, and allows our customers to get back to running their businesses.

**Begin a free trial of Symantec Endpoint Protection.cloud**

**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

Symantec helps organizations secure and manage their information-driven world with **managed services**, **exchange spam filter**, **managed security services**, and **email antivirus**.


4/2011 21182051