TECHNICAL BRIEF:
WHITE PAPER: TECHNICAL

Best Practices running Symantec™ Endpoint Protection and Symantec™ Endpoint Protection Manager on the Amazon Web Services Platform

Who should read this paper

Customers who are deploying Symantec™ Endpoint Protection on the Amazon Web Services (AWS) Platform

Best Practices running Symantec™ Endpoint Protection and Symantec™ Endpoint Protection Manager on the Amazon Web Services Platform

Content

Introduction

Amazon WorkSpaces is a managed desktop computing service in the cloud. Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides resizable compute capacity in the cloud. Symantec™ Endpoint Protection (SEP) is certified to run on AWS Virtual Machines (VM). Symantec™ Endpoint Protection can be installed as an application within the AWS Marketplace.

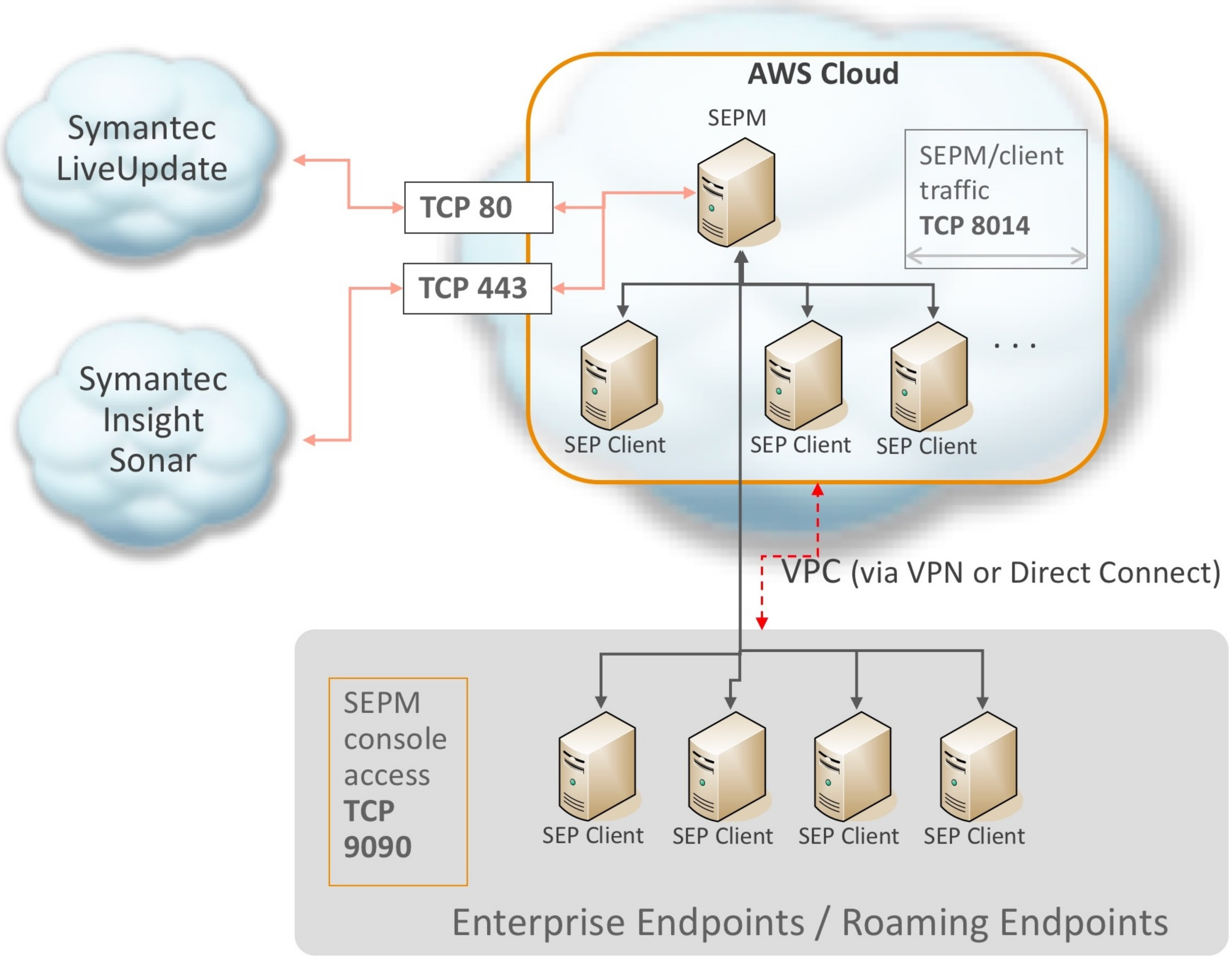
This document describes how to use Symantec™ Endpoint Protection to protect VMs in Amazon Web Services platform. For more information on Amazon Web Services, identity management, roles, and security topics related to the platform, see the Amazon Web Services website.

Overview of Symantec Endpoint Protection on the Amazon Web Services platform

Symantec™ Endpoint Protection goes beyond antivirus to deliver multiple layers of protection for VMs on the Amazon Web Services platform. While our default settings includes virus and spyware technologies, we highly recommend that you also take advantage of other layers of protection for maximum security.

- **Virus and Spyware Protection:** This is a core component of Symantec™ Endpoint Protection and is automatically installed as part of the default setting. It includes signature-based file scanning that detects known threats and threat families.
- **Insight**™: Insight is a cloud-based reputation engine that can accurately identify file reputation upon download. By analyzing key file attributes, Insight provides guidance on whether a file is good, bad or has an unknown reputation. If your VMs can download files through portal applications such as the Internet browser, email and FTP clients, we recommend you turn on the Insight engine.
- **SONAR**™: SONAR monitors suspicious file behaviors to determine whether the files pose a danger to your system. By conducting real-time behavior scanning, SONAR can detect and block never-before-seen threats. We recommend you turn on SONAR to detect advanced threats.
- **Intrusion Prevention System (IPS)**: IPS delivers inbound and outbound network packet scanning for malicious payloads and activity. It may reduce network speed on some high availability servers, so for VM roles running the Windows R2 Datacenter edition, we do not recommend you install IPS.

The above technologies require updates from Symantec. Managed clients receive updates automatically from the Symantec™ Endpoint Protection Manager. Unmanaged clients receive updates from Symantec servers connected to the Internet by running LiveUpdate™. Both Insight™ and SONAR™ require Internet access to leverage reputation data from the Symantec Global Intelligence Network.



The following technologies provide additional protection for your VMs through rule-based policies for system hardening. They do not require updates from Symantec but you do need to enable and configure them.

- **Application Control**: Blocks autorun.inf, file access, registry access, processes from launching, access to removable drives, loading dlls and many additional options. Symantec recommends that you leverage the advanced rule-based protection templates for VMs in an Amazon Web Services environment.
- **System Lockdown**: Defines explicit whitelists or blacklists and that applies to a file fingerprint list. Enable System Lockdown to get the best protection.
- **Firewall:** This is not needed if your VMs are already set up to restrict network traffic using the Windows firewall.
- **Device Control:** Blocks or allows devices by device or class ID. For example, it blocks USB sticks devices except for explicitly allowed models. Device Control is only needed if VMs is connected to removable devices.

If the virtual machine is a Windows server and falls under performance metrics for high availability servers, see the following knowledge base article for specific recommendations:

Best Practices for Installing Symantec™ Endpoint Protection (SEP) on Windows Servers

http://www.symantec.com/business/support/index?page=content&id=TECH92440

Installing a Symantec™ Endpoint Protection client in Amazon WorkSpaces

Contact **Symantec Customer Care** if you need assistance.

Installing an unmanaged client

To install an unmanaged client, download the client installation file from FileConnect to the target virtual machine and double-click setup.exe.

You must license the software by purchasing a copy of Symantec™ Endpoint Protection 12.1 or by installing your existing enterprise license.

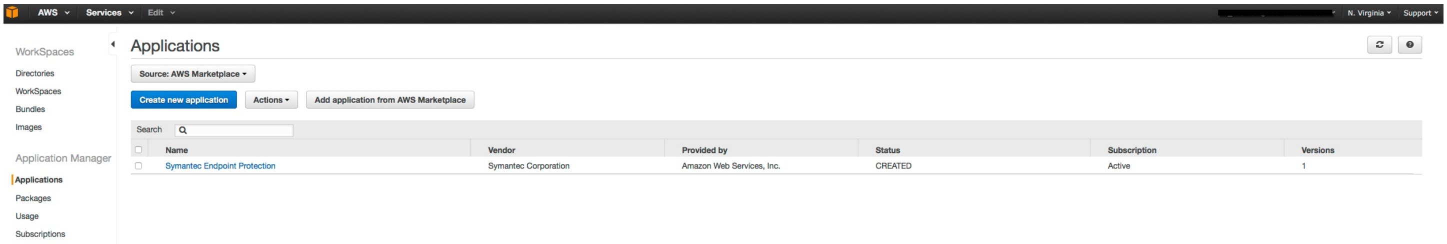
For more information, see the following knowledge base article: Installing an unmanaged Symantec™ Endpoint Protection 12.x client

http://www.symantec.com/docs/TECH104386

Installing Symantec™ Endpoint Protection via AWS Marketplace

Installing a **Symantec™ Endpoint Protection** client on an AWS VM requires access to the Amazon WorkSpaces Application Manager (Amazon WAM).

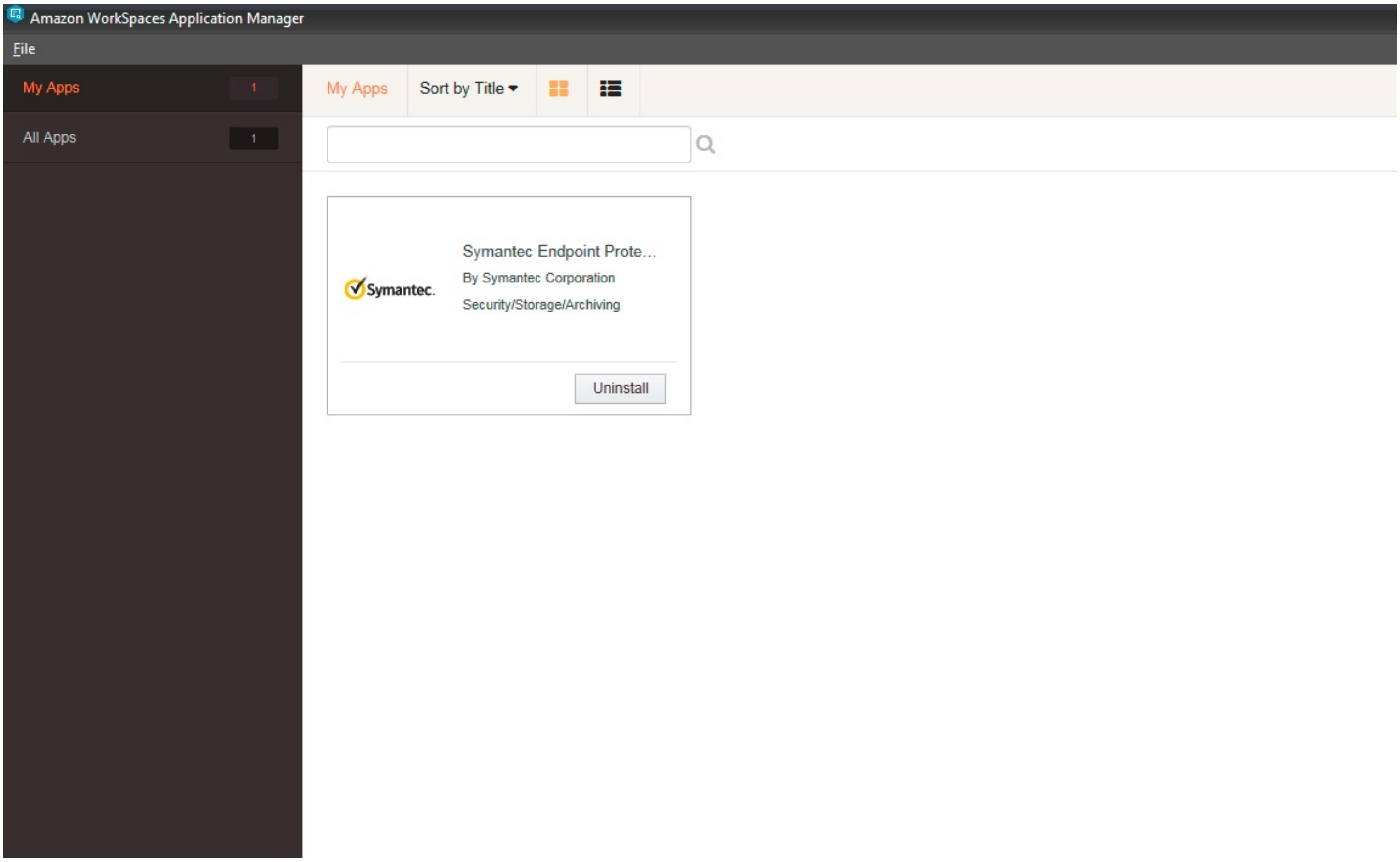
Symantec™ Endpoint Protection listed in the AWS Marketplace. Symantec™ Endpoint Protection Client can be installed by subscribing to Symantec™ Endpoint Protection in the AWS Marketplace for Desktop Apps.



Applications

□	Name	Vendor	Provided by	Status	Subscription	Versions
□	Symantec Endpoint Protection	Symantec Corporation	Amazon Web Services, Inc.	CREATED	Active	1

Administrators can also designate Symantec™ Endpoint Protection as a required application, Symantec™ Endpoint Protection Client will be installed on the EC2 instance automatically.


Amazon WorkSpaces Application Manager
File
My Apps 1
All Apps 1
My Apps
Sort by Title
Symantec.
Symantec Endpoint Prote...
By Symantec Corporation
Security/Storage/Archiving
Uninstall

A subscription is activated and charged the first time a user in launches an application and will renew monthly until access to the application is removed for that user, with a prorated charge for the first month.

The Symantec™ Endpoint Protection security extension is the same code as the client installation file. There are no code changes or alterations to the client itself to support installation on the AWS platform. The security extension is a simple wrapper that passes install parameters for use in the AWS Application Manager.

The default setting of Symantec™ Endpoint Protection when installed from the AWS Marketplace contains Virus and Spyware protection, Intrusion prevention, Insight™ and SONAR™. Default settings require a reboot, the system will automatically reboot at the end of install.

Overview of Symantec Endpoint Protection Manager on the Amazon EC2 platform

Symantec™ Endpoint Protection Manager provides single management console across physical and virtual platforms with granular policy control, remote deployment and client management for Windows, Mac, Linux, virtual machines and embedded systems.

Installing Symantec™ Endpoint Protection Manager on the Amazon EC2 platform

Symantec™ Endpoint Protection Manager is installed by deploying the Symantec™ Endpoint Protection Manager AMI (Amazon Machine Image) from AWS Marketplace. Symantec™ Endpoint Protection Manager AMI can be deployed as a 1-click or via Amazon EC2.

If Symantec™ Endpoint Protection Manager is installed by deploying the AMI via Amazon EC2 an on-premises system, make sure that all ports are available and open for communication between the management console and the Symantec Endpoint Protection clients in AWS.

It is required to configure the following ports in the Security Groups section:

Server port = 8443 TCP

Remote console = 9090 TCP

Client port = 8014 TCP

Server control port = 8765 TCP

Reporting port = 8445 TCP

Web services port = 8444 TCP

RDP = 3389

HTTPS = 443 TCP, Optional for secure communication

FTP port = 21, optional for File transfer

For information on what ports are needed for a managed Symantec™ Endpoint Protection client, see the following knowledge base article:

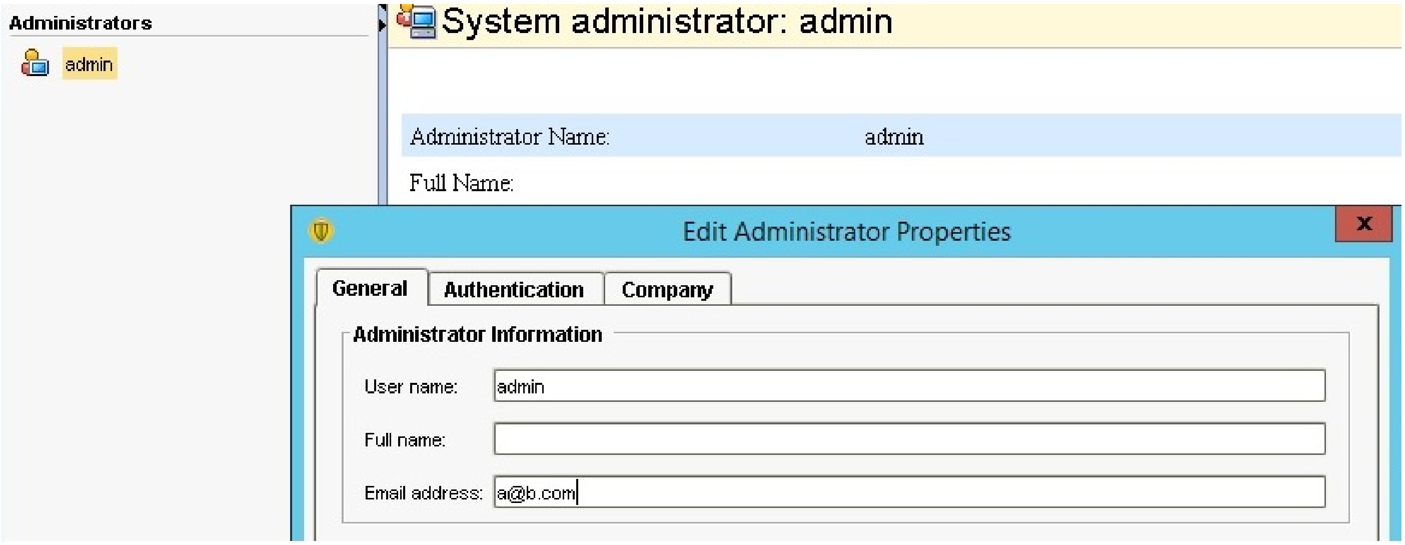
Which communication ports does Symantec™ Endpoint Protection use?

http://www.symantec.com/docs/TECH163787

See the following knowledge base article for the latest system requirements:

http://www.symantec.com/docs/TECH224712

It is recommended to change the default email address on the Symantec™ Endpoint Protection Manager by going to into Admin-> Administrators-> Edit


Administrators
admin
System administrator: admin
Edit Administrator Properties
General
Authentication
Company
Administrator Information

Administrator Name: admin

Full Name:

User name: admin

Full name:

Email address: a@b.com

The recommended configuration is to use embedded database, the Symantec™ Endpoint Protection Manager AMI is pre-installed with an embedded database.

Since Symantec™ Endpoint Protection Manager is pre-installed database replication between sites is not supported.

Symantec™ Endpoint Protection Manager supports 1000 Symantec™ Endpoint Protection instances per AMI.

Running LiveUpdate™ and performance

If you configure the Symantec™ Endpoint Protection clients to run LiveUpdate to get updates, we recommend that you schedule the updates to run when the AWS VM is not running other CPU or disk-intensive activities.

Installing a managed client on the Amazon EC2 platform

To install a managed client, you can create and export a client installation package from the Symantec Endpoint Protection Manager console. You then copy the exported file locally to the target AWS VM.

For more information, see the following knowledge base article:

How to export an install package from the Symantec Endpoint Protection Manager

http://www.symantec.com/docs/TECH181666

Symantec™ Endpoint Protection Manager's push deployment makes use of ICMP ping protocol. The clients need to add the ICMP Echo Request ingress rule in order to be visible on the Client Deployment Wizard. In order for Symantec™ Endpoint Protection Manager to deploy packages you need to enable TCP port 445 on client machines.

Advanced Configuration:

Using Application Control and System Lockdown to restrict applications

If you intend the AWS VM to run specific applications only, you can restrict unapproved applications using Application Control and System Lockdown. You should also use Application Control and System Lockdown for AWS VMs that do not have access to the Internet because the lack of Internet access prevents Insight™ and SONAR™ from protecting these VMs.

Restricting applications with System Lockdown

System lockdown enables whitelisting or blacklisting capabilities. The whitelisting mode allows you to control which applications are allowed to run on the AWS VM. These approved applications are contained in a list of file fingerprints that include the application's checksums and file paths.

Implementing system lockdown is a two-step process. First, create a file fingerprint list and then import the list into Symantec™ Endpoint Protection Manager for use in the system lockdown configuration.

To generate the file fingerprint list, use the checksum tool included in the Symantec™ Endpoint Protection client installation. Symantec recommends that you create a software image that includes all of the applications to whitelist on the AWS VM, and then use this image to create a file fingerprint list.

For more information on configuring system lockdown for whitelisting please visit:

http://www.symantec.com/docs/HOWTO80848

Restricting applications with Application Control

In addition to signature or Symantec-defined rule-based protection, you can also restrict applications from running on the endpoints by creating protection rules that you define. These rules can range from the simple task of blocking access to autorun.inf files on all removable devices, to the more complicated tasks of preventing browser helper objects from being registered, or making USB devices *read only* in a specific location.

Configure Application Control to allow only applications specific to the AWS VM as well as the required operating system applications that the VM runs at startup. To do this you will first monitor which applications the virtual machine runs, and then create a rule that allow these applications.

To restrict applications from running on the VM using Application Control:

1. Run a tool, such as Process Monitor or Process Explorer, to get a list of all applications that run on the AWS virtual machine. Keep the tool running during normal activity to find startup processes and any applications that are short-lived.
2. With a list of all the applications, create an Application Control rule set at the highest priority to allow those applications to run. Include the full path and name of each application.
3. If you are using a software management tool, such as Symantec Endpoint Management or Microsoft System Center, create a second rule set at a lower priority to allow the software management tool to run any application. Enable the **Sub-processes inherit conditions** option for this rule.
4. Create a third rule set at a lower priority to block any application from running.

These rule sets block other applications from running, even if the other applications are valid applications. The advantage of this blocking is that attackers sometimes use valid applications that are on the AWS VM, but that are not normally used to attack the system. For example, attackers may use applications like cmd.exe, cscript.exe, or even telnet.exe.

For more information, see the knowledge base article **About Application and Device Control**

http://www.symantec.com/docs/HOWTO80859

Restricting applications for system hardening

In addition to restricting unapproved applications, use Application Control to harden an AWS VM. Symantec offers predefined rule sets to block behavior known to be malicious. As a best practice, enable the following rule sets to block malicious application behaviors.

To enable system hardening, check the following rule sets in the default Application Control policy to enable them:

1. Block programs from running from removable drives
2. Block modifications to the hosts file
3. Block access to scripts
4. Block access to Autorun.inf
5. Block File Shares
6. Prevent changes to Windows shell load points
7. Prevent changes to system using browser or office products
8. Prevent vulnerable Windows processes from writing code
9. Prevent Windows Services from using UNC paths
10. Block access to lnk and pif files

About Symantec

Symantec Corporation (NASDAQ: SYMC) is the global leader in cybersecurity. Operating one of the world's largest cyber intelligence networks, we see more threats, and protect more customers from the next generation of attacks. We help companies, governments and individuals secure their most important data wherever it lives.

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

1/2016 21363154