



Enterprise Vault Whitepaper

Enterprise Vault in Hosted Environments

This whitepaper will discuss the different options available for Enterprise Vault in hosted environments. This whitepaper will mainly discuss Enterprise Vault solutions and briefly describe EV.Cloud offerings.

If you have any feedback or questions about this document please email them to EV-TFE-Feedback@symantec.com stating the document title.

This document applies to the following version(s) of Enterprise Vault:
9 & 10

This document is provided for informational purposes only. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice. Copyright © 2012 Symantec Corporation. All rights reserved. Symantec, the Symantec logo and Enterprise Vault 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

Document Control

Contributors

Who	Contribution
Evan Barrett	Author/Contributor
Christopher Moreau	Author/Contributor

Revision History

Version	Date	Changes
1.0	March 2012	Initial Release

Related Documents

Version	Date	Title

Table of Contents

Introduction	1
Deployment Models	1
Private or Dedicated Cloud	1
Hybrid Cloud	2
Community Cloud	4
Public Cloud	4
Managed Service Providers	6
Remote Management	6
Off-premise Hosting	7
Hosted Software as a Service (SaaS) for File System Archiving	7
Hosting Configurations	7
Single Tenant Hosting	7
Configuration Overview	8
Benefits	9
Cautions	9
Multi-Tenant Hosting	9

Introduction

Many customers today have the need to reduce costs associated with maintaining electronic communications, file storage, and eDiscovery. Symantec offers industry-leading solutions to help manage these costs with archiving and effective eDiscovery. These solutions can be used in a wide range of deployment models.

Customers may want to outsource all operations associated with messaging and eDiscovery to third parties, while others may need to manage all operations onsite. Managed Service Providers (MSP) provide solutions that incorporate Enterprise Vault and EV.Cloud for archiving and eDiscovery in offsite or a mixed onsite/offsite environments helping to reduce costs.

The main intent of this whitepaper is to discuss the options available to customers regardless of the deployment model (Private Cloud, Hybrid Cloud, or Public Cloud) when it comes to archiving content. Although cloud solutions for Enterprise Vault will mainly be discussed, EV.Cloud options will also be presented.

Deployment Models

There are four main deployment models that will be discussed: Private Cloud, Hybrid Cloud, Community Cloud, and Public Cloud. The deployment method to use will depend on the end goal of the customer. Use cases will be provided for each deployment model.

Private or Dedicated Cloud

The Private Cloud model utilizes Managed Service Providers (MSP) or hosting providers who manage all aspects of an Enterprise Vault environment including deployment. The Enterprise Vault environment can be either on-premise or off-premise. On-premise installations are managed remotely by an MSP. The MSP or hosting provider in which all archived data is maintained securely hosts off-premise installations.

Customers who require a Private Cloud deployment model on premise will generally have one or more of the following requirements:

- Mandate to keep all archived data on-premise
- Support for content beyond electronic communications
 - Files
 - Databases
 - SharePoint
 - Other content
- Tightly integrated end user experience
 - End user access to archived content from many sources

- Offline access to archived content and mobile search
- Robust eDiscovery capabilities
 - Collection of desktops/laptops and content outside the archive
 - eDiscovery of files, SharePoint, Databases and other information

In the event a company wishes to leverage a hosting provider to provide a dedicated Private cloud model the customer may require all data and infrastructure to be separate from any other customer's infrastructure, but does not have a requirement to maintain the solution on their premise. Most often, this is due to the desire to reduce on premise data center resource costs.

Hybrid Cloud

Hybrid Cloud solutions offer a mix of on-premise and off-premise hardware, software, and storage.

Starting with Enterprise Vault 10, less-accessed archived content can be migrated to the Cloud. Symantec has recently announced several partnerships with the leading cloud storage vendors: Nirvanix™, Amazon S3, Backspace, and AT&T Synaptic. The customer can configure storage migration on a per Vault Store Partition basis. The Enterprise Vault product can be configured to send data to the cloud storage based on time. This is done generally for less frequently accessed information, for example mailbox archive or file system archive data that is older than 3 – 6 months. The information can still be accessed via shortcuts. Data can be sent to these cloud vendors directly from Enterprise Vault solution to the cloud based storage solution maintaining all capabilities including retrieval, retention and eDiscovery capabilities.

Migrating content to the Cloud requires that migrations be enabled at the Vault Store partition level. Once data has been migrated to the cloud, there is less data locally which reduces storage requirements and backup windows and requirements. For more information on enabling migrations on Vault Store partitions, please read the *Enterprise Vault Installing and Configuring Guide*.

Migrating data will not affect searches against the Enterprise Vault index as the indexes remain on premise. Any item that would need to be accessed (such as a user recalling an archived email that is not in Vault Cache, using Browser Search, rebuilding an index, or exporting data from Discovery Accelerator) would initiate a call to the archived item in the cloud. It is generally not recommended to migrate archived email content to the cloud if eDiscovery is consistently used as this can slow down the discovery process.

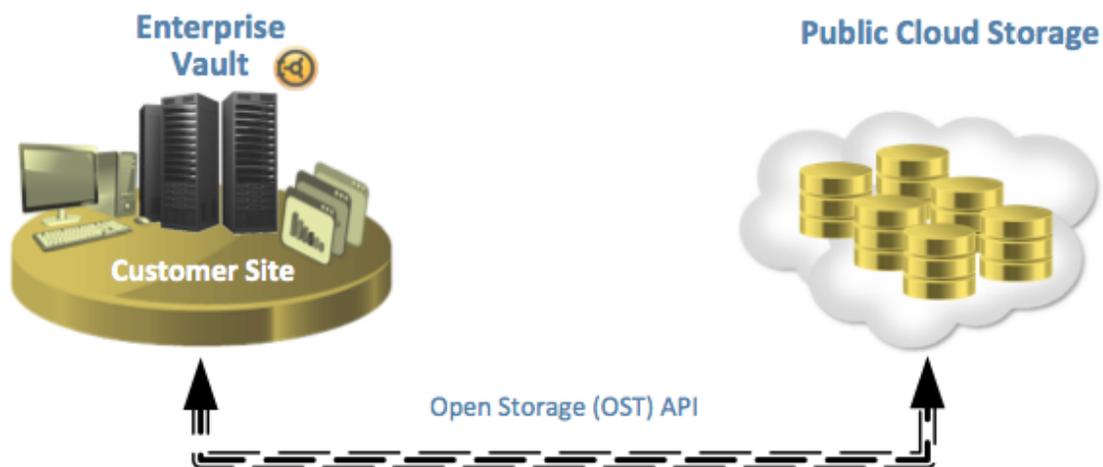


Figure 1 – Cloud Storage Configuration

Another Hybrid Cloud solution includes Enterprise Vault hosted on-premise while having email hosted by providers such as Microsoft, Google, and Lotus Live. This offers the ability to keep archives on-premise for eDiscovery and Compliance purposes. Having an on-premise Enterprise Vault server also allows the archiving of other on-premise source content such as files, SharePoint, and databases.

Archiving email solutions such as Microsoft Office 365 fall under the Hybrid Cloud solution. The email server would remain offsite where the archived content would be store on-premise in a customer's datacenter. For more information on Enterprise Vault integration with Microsoft Office 365, please visit: <http://www.symantec.com/business/support/index?page=content&id=TECH169342>.

Archiving of social media content also falls under the Hybrid Cloud model. Enterprise Vault, in conjunction with Symantec Partner solutions, can archive content from sources such as public web pages, Facebook, LinkedIn, and Twitter.

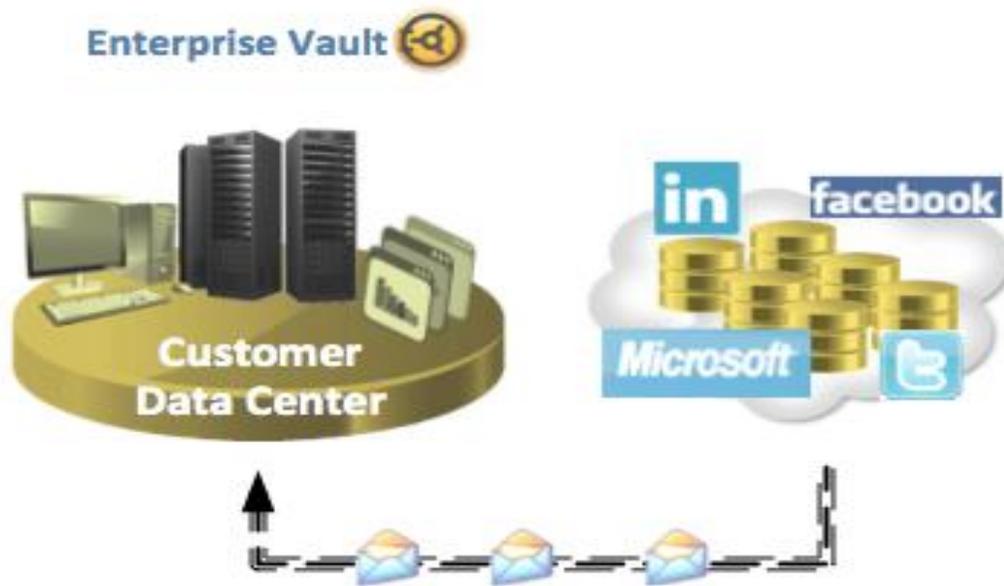


Figure 2 - Hybrid Cloud Configuration with Electronic Communications

Community Cloud

The Community Cloud deployment model provides for a shared cloud environment for a particular community such as government-based agencies. These cloud environments are multi-tenanted, but not public. The solution would be maintained by a Managed Service Provider (MSP) or hosting provider leveraging dedicated infrastructure and storage for the designated community. This solution is achieved by leveraging dedicated images of Enterprise Vault for each member of the Community to separate data and indexed information, thus allowing the Community to leverage the resources dedicated to them while maintaining separate instances for each member of the community.

Public Cloud

Customers may have one or more reasons to use Public Cloud-based archiving solutions:

- A mandate to move the Cloud
- Requirement to reduce resource footprint (such as costs associated with datacenter, staff, maintenance, or upgrades)
- Archiving and eDiscovery against electronic communications only
- A solution that is simple to acquire and easy to deploy
- Customer lacks high-availability for email and is looking to have a solution for email continuity

If an organization is looking at a purely electronic communications off-premise archiving solution, EV.Cloud may be the answer. EV.Cloud has the following features:

- Purely Hosted
 - No hardware, software, or plug-ins to install and maintain
 - Low upfront investment and total cost of ownership (TCO)
 - Flat fee per mailbox per month which includes service upgrades
- Unlimited Storage and Rapid Search
 - Unlimited email storage and retention
 - Rapid search results from scalable grid architecture
 - No mailbox size limits for end users
- Enterprise-class Infrastructure and Security
 - Redundant, scalable, Tier 4 datacenters
 - Data encrypted in transit and at rest
 - 24/7/365 support included in cost of service

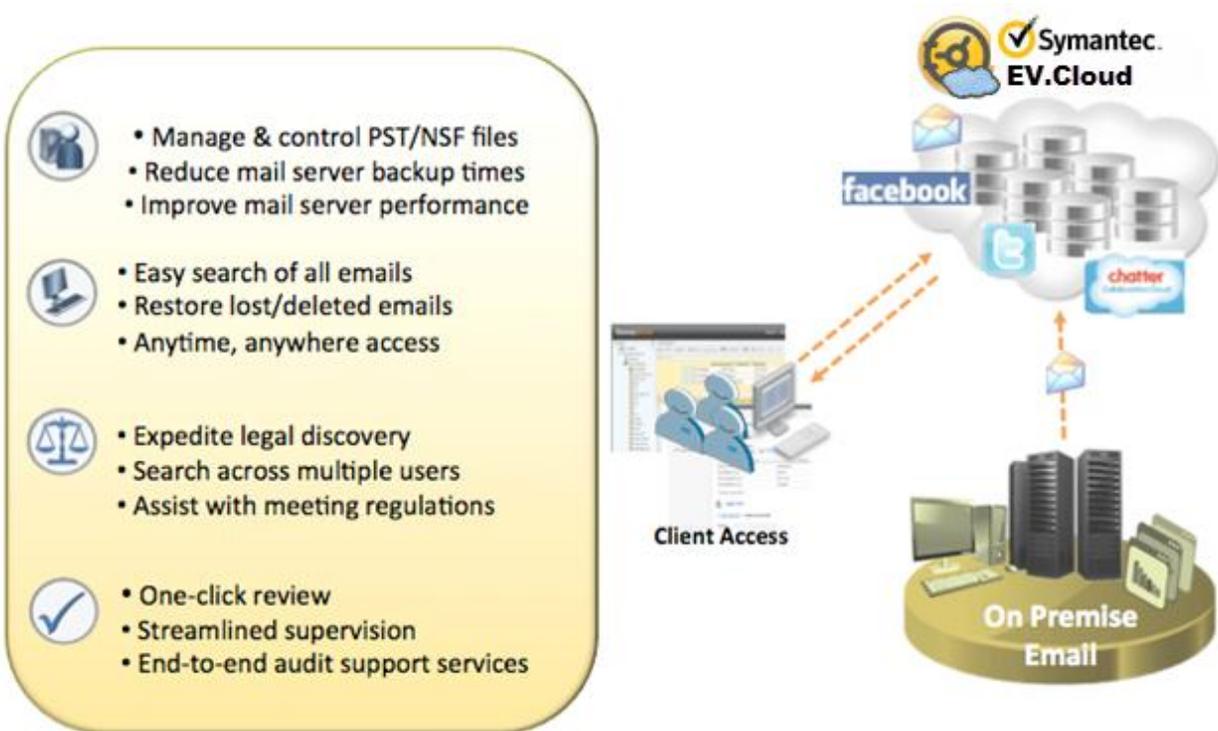


Figure 3 - EV.Cloud Overview

For more information on EV.Cloud visit <http://www.symantec.com/enterprise-vault-cloud>.

Managed Service Providers

Managed Service Providers (MSP) provide a wide range of services including remote management of on-premise Enterprise Vault installations and hosting Enterprise Vault installations off-premise.

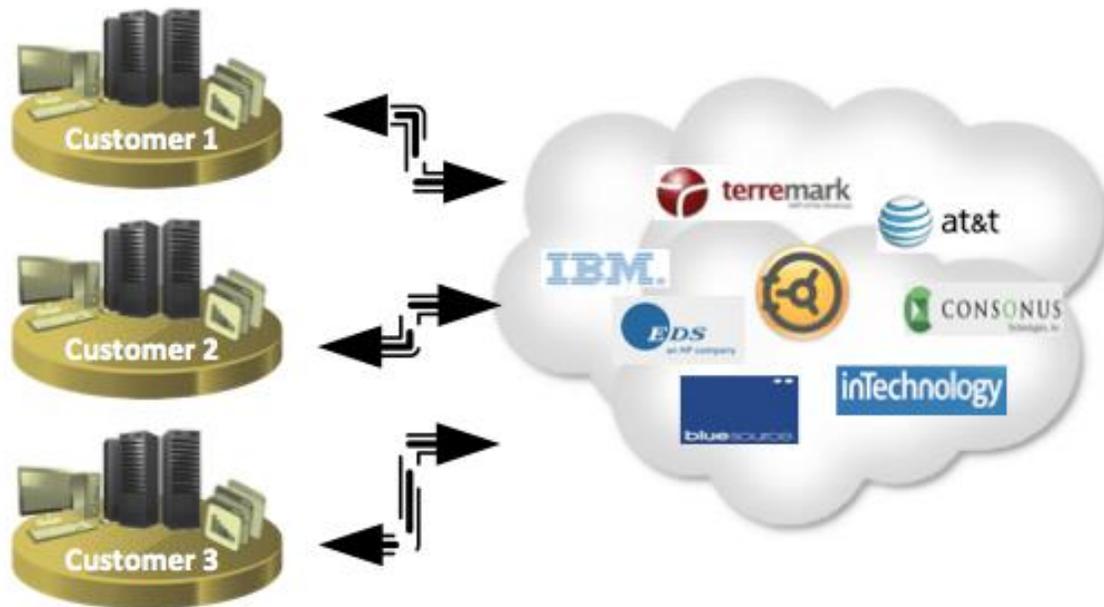


Figure 4 - Managed Service Provider Overview

Remote Management

Customers may want consider remote management and monitoring of Enterprise Vault by MSPs for the following reasons:

- A requirement to maintain all archived content on-premise
- Looking to reduce costs associated with administration of Enterprise Vault
- Lacks personnel who have the skills necessary to manage Enterprise Vault

Managed Service Providers who currently offer remote management for Enterprise Vault include:

- BlueSource (<http://www.bluesource.co.uk> or <http://www.bluesource.net>)
- EDS (<http://www8.hp.com/us/en/business-services/index.html>)
- Globanet (<http://www.globanet.com>)
- Terremark (<http://www.terremark.com>)

In Remote Management configurations, the Enterprise Vault environment remains on-premise with all management and monitoring of Enterprise Vault performed by the MSP. If remote management is not desired, the MSP may offer an onsite resource or consultant to manage the Enterprise Vault environment.

Off-premise Hosting

Customers may want the fully functionality that Enterprise Vault offers for archiving but may not want to or have the ability to maintain Enterprise Vault onsite. Off-premise solutions offer the following benefits:

- Dedicated Service Level Agreements (SLA) around Enterprise Vault
- Hardware and software managed and maintained by MSP
- Customer is not required to have personnel on staff who are knowledgeable with Enterprise Vault

In off-premise solutions, each customer's Enterprise Vault deployment is maintained separately and securely from other customers' Enterprise Vault deployments. An MSP will typically provision one or more virtual servers (using virtualization technology such as VMware ESX) or have dedicated physical hardware for each customer's environment. A dedicated virtual private network (VPN) may be configured to establish a secured connection between the customer's network and the MSP in order to perform archiving operations. For Active Directory synchronization, a replicated domain controller for the customer's environment may also be housed at the MSP's datacenter.

Partners who currently offer off-premise solutions for Enterprise Vault:

- AT&T (<http://www.att.com>)
- Consonus (<http://www.consonus.com>)
- EDS (<http://www8.hp.com/us/en/business-services/index.html>)
- Terremark (<http://www.terremark.com>)
- InTechnology (<http://www.intechnology.co.uk>)

Hosted Software as a Service (SaaS) for File System Archiving

This solution is targeted at new customers who are looking to move to a cloud-based solution only and require a basic solution for eDiscovery and Compliance for file systems. These partners currently provide these services:

- Consonus (<http://www.consonus.com>)
- InTechnology (<http://www.intechnology.co.uk>)

Hosting Configurations

This section will describe two different hosting methods, single tenant and multi-tenant, and provide pros and cons for each type of configuration.

Single Tenant Hosting

Single tenant hosting is a configuration where a hosted Enterprise Vault environment is installed on hardware that is dedicated to a single customer and managed by a Managed Service Provider (MSP).

The hardware that is used for the environment can be dedicated physical hardware or run in a virtual environment such as VMware ESX. The EV/DA environment is completely isolated from other customer configurations for maximum security of archived content.

Configuration Overview

All components of archiving and eDiscovery (Microsoft SQL Server, Enterprise Vault, and Discovery Accelerator) are located at the MSP datacenter. The Microsoft Exchange environment, Domino mail server environment, file servers, SharePoint servers, or other archiving targets remain on-premise in the customer's environment. Figure 5 provides a sample configuration for single tenant hosting.

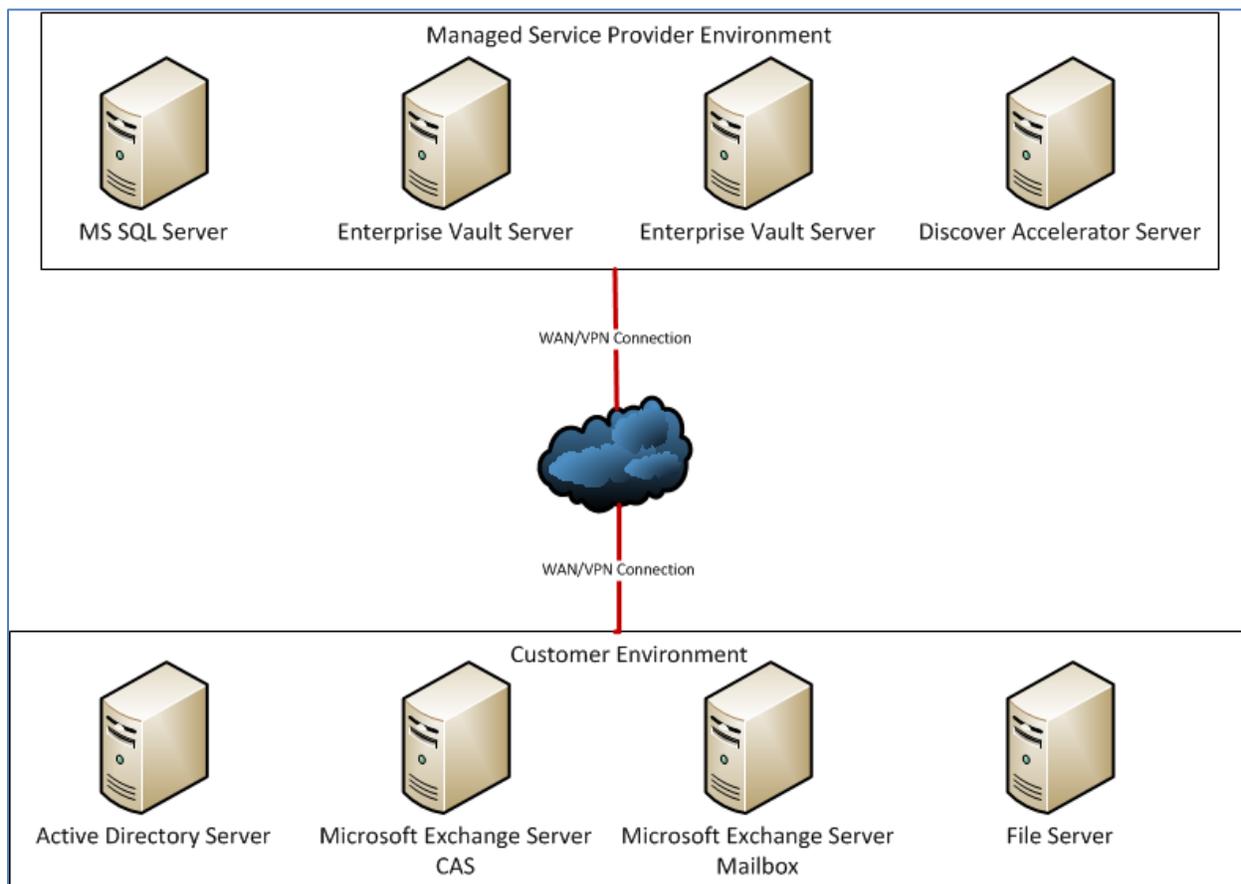


Figure 5 - Single Tenant Hosting Example

A network connection will be required between the MSP datacenter and the customer's network. This can be a dedicated WAN link or a virtual private network (VPN) connection. This network connection will allow the archiving of content in the customer's datacenter to the hosted environment. This will allow for the customer to retrieve or search against archived content. Sufficient bandwidth will be required in order to provide for timely archiving of targets and Vault Cache synchronization (where applicable). WAN/VPN

bandwidth size will vary depending on a number of factors such as the amount of data on the archiving target, archiving policies, archiving window, and number of Vault Cache users.

For Exchange archiving, an Active Directory server can be installed in the MSP datacenter. This will reduced the amount of Active Directory calls generated by Enterprise Vault and Discovery Accelerator across the WAN.

Benefits

A single tenant hosting model provides the following benefits:

- The management of all Enterprise Vault and Discovery Accelerator components is performed by the MSP
- Archived data is stored securely and separately from other customer environments

Cautions

A single tenant hosting model has the following caution:

- Higher costs due to dedicated environment for archiving

Multi-Tenant Hosting

The EV.Cloud solution is a full multi-tenant platform designed to host multiple customers on a multi-tenant platform. The traditional Enterprise Vault platform can be leveraged to provide a dedicated instance to a single tenant and some solution providers do offer this deployment model, but those looking to leverage a multi-tenant infrastructure often look to a solution such as EV.Cloud to accomplish this task. The solution leverages the Journaling capabilities of the email system to send all data to the cloud for a given customer which is then separated and associated with each user at the given customer to allow the user to access his or her individual messages. For more information on EV.Cloud see the following:

For more information on EV.Cloud visit <http://www.symantec.com/enterprise-vault-cloud>.

About Symantec:

Symantec is a global leader in providing storage, security and systems management solutions to help consumers and organizations secure and manage their information-driven world.

Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored.

For specific country offices and contact numbers, please visit our Web site: **www.symantec.com**

Symantec Corporation
World Headquarters
350 Ellis Street
Mountain View, CA 94043 USA
+1 (650) 527 8000
+1 (800) 721 3934

Copyright © 2012 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.