TECHNICAL BRIEF:
BEST PRACTICES GUIDE FOR PROTECTING
RETAIL POS SYSTEMS

Best Practices for Running Symantec Endpoint Protection 12.1 on Point-of-Sale Devices

Who should read this paper

Customers who are deploying Symantec Endpoint Protection 12.1 in a retail point-of-sale environment.

Best Practices for Running Symantec Endpoint Protection 12.1 on Point-of-Sale Devices

Content

Best Practices for Running Symantec Endpoint Protection 12.1 on Point-of-Sale Devices

Overview

This document describes the recommended configuration for running Symantec™ Endpoint Protection 12.1 on Windows point-of-sale (PoS) devices. Symantec recommends that PoS devices use the following Symantec Endpoint Protection technologies:

1. Antivirus, SONAR, Insight, and an Intrusion Prevention System (IPS).
2. The Application Control policy and System Lockdown to allow only approved applications.
3. The firewall policy to restrict access to specific applications.

Point-of-sale devices may have different operating systems. Symantec Endpoint Protection 12.1 fully supports different Windows operating systems, including Windows Embedded, which is commonly used on PoS devices.

Note: If the PoS device is running a non-Windows operating system, Symantec Critical System Protection may be used as an alternative.

Restricting unapproved applications

One of the most important security practices to implement on a PoS device is to restrict the use of unapproved applications that are allowed to run on the PoS device. You can restrict unapproved applications using Application Control and System Lockdown.

Restricting applications with System Lockdown

System Lockdown enables blacklisting or whitelisting capabilities. The whitelisting mode allows you to tightly control which applications are allowed to run on the PoS device. Approved applications are contained in a list of fingerprints that include checksums and locations of applications that are approved for use.

Implementing System Lockdown is a two-step process. First, you create a fingerprint list, and then you import the list into the Symantec Endpoint Protection Manager (SEPM) for use in the System Lockdown policy.

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 PoS devices, and then use this image to create a file fingerprint list.

For more information on enabling System Lockdown for whitelisting:

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

For more information on excluding Symantec Endpoint Protection definition files:

http://www.symantec.com/docs/TECH207935

Restricting applications with Application Control

Applications can be restricted with Application Control. Application Control must include not only the PoS applications, but also the required operating system applications that the PoS device runs at startup. You configure Application Control to first monitor which applications the device runs, and then create a rule that allows these applications to run. You allow an application by specifying its full path and name.

To restrict an application from running 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 PoS device. Keep the tool running during normal PoS activity to pick up any applications that are short-lived; also, check for startup processes.
2. With a list of all the applications, create an Application Control rule at the highest priority to allow those applications to run. Include the full path and name of the application. This is the first Rule Set.
3. If you are using a software management tool, such as Symantec Endpoint Management or Microsoft System Center, determine which application is used for the software management tool. Create a rule at a lower priority to allow the software management tool to run any application. Enable the **Sub-processes inherit conditions** setting for this rule. This is the second Rule Set.
4. Create a rule at a lower priority to block any application from running. This is the third Rule Set.

Using these three rules will allow only specific known applications to run by file name and path. It will block other applications on the PoS device from running, even if the other applications are valid applications. The advantage of this blocking is that attackers will sometimes use valid applications that are on the PoS device, but are not normally used, to attack the system. As an example, they may use applications like cmd.exe, cscript.exe, or even telnet.exe.

For more information, see Configuring Application and Device Control:

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

Restricting applications with system hardening in Application Control

In addition to fully restricting unapproved applications, you can use Application Control to harden the device. Symantec offers Application Control templates with predefined policies to block behavior known to be malicious. Best practices would include enabling some of these hardening templates on your PoS device to block malicious application behaviors.

To enable system hardening:

1. Download the Application Control hardening policy from the following link:
   http://www.symantec.com/docs/TECH132337
2. Ensure the following application rule sets are enabled:
   a. Block programs from running from removable drives
   b. Block modifications to the hosts file
   c. Block access to scripts
   d. Block access to Autorun.inf
   e. Block File Shares
   f. Prevent changes to Windows shell load points
   g. Prevent changes to system using browser or office products
   h. Prevent vulnerable Windows processes from writing code
   i. Prevent Windows Services from using UNC paths
   j. Block access to lnk and pif files

Restricting applications in the firewall policy

In most PoS devices, there are only few applications that require access to network. These applications need access to specific ports only, either inbound or outbound. As a rule of thumb, you should restrict which applications are allowed to communicate

on the network and what they are allowed to do. When communication is restricted, even if an untrusted application gets on the system, it will not be allowed to send any data from the PoS device.

To restrict applications in the firewall policy:

1. Open the default firewall policy.
2. Disable the following firewall rules:
   a. Allow Local File Sharing to private IP addresses (rule 9)
   b. Allow UPnP Discovery from private addresses (rule 12)
   c. Allow Web Services requests from private IP addresses (rule 14)
   d. Allow LLMNR from private IP addresses (rule 16)
   e. Allow LLMNR from ipv6 traffic (rule 18)
   f. Allow Web Services Discovery from private IP addresses (rule 19)
   g. Allow all applications (rule 24)
   h. Allow VPN (rule 25)
3. Create one rule for each application on your PoS device that sends traffic. Move the rules at the top of the rule set. Edit each of these rules and add in the TCP or UDP ports that are needed for each of these applications. Specify whether the ports are used for inbound or outbound traffic.

For more information on creating and managing the firewall rules:

http://www.symantec.com/docs/HOWTO80775

Configuring anti-malware protection

Restricting which applications are allowed to run can offer enhanced protection. However, Symantec recommends that you also enable anti-malware protection to detect known malware files. This is useful for a number of reasons. First, when Application Control or System Lockdown blocks an application, only the file attributes, such as name, path, and size, are stored. However, if the file is a known malware file, Symantec Endpoint Protection can detect and log the file as malware by using anti-malware technologies. Furthermore, anti-malware technologies block malware other than applications, such as scripts and macros, whereas Application Control and System Lockdown may not be configured to block those scripts or macros.

For advanced anti-malware protection, installing just the antivirus component won't be enough. You should also install SONAR, Insight, and IPS. Symantec Endpoint Protection installs and enables all of these technologies by default.

Note that both Insight and SONAR require Internet access to leverage reputation data from Symantec's Global Intelligence Network. Depending on your policy, it may not be optimal for PoS devices to access the Internet for reputation data. In this case, install and set up Symantec Insight for Private Clouds. Symantec Insight for Private Clouds allows PoS devices to look for reputation data without requiring access to the Internet.

For more information on how to configure Symantec Insight for Private Clouds, see:

http://www.symantec.com/docs/HOWTO84720

Reducing disk space on the PoS device

For PoS devices that have limited disk space, perform the following tasks to reduce the size of the Symantec Endpoint Protection client software, while still installing System Lockdown, Application and Device Control, the firewall, and the IPS, which collectively use less than 150 MB of disk space. This is a good solution for PoS devices with few resources.

Installing the minimal number of features

If space is a concern, install only Application and Device Control (which includes System Lockdown), the firewall, and the IPS.

The antivirus features (including SONAR and Insight) require the most resources. Therefore, depending on the resources available in the PoS device, you may not be able to install the antivirus features. If the PoS is a single-purpose device that does not change often, you can use System Lockdown to create a whitelist for the whole device, thereby reducing the need for the antivirus component. The antivirus component alone requires between 1 to 2 GB of disk space.

To install only Application and Device Control, the firewall, and IPS:

1. In the Symantec Endpoint Protection Manager console, click **Admin**, and then click **Install Packages**.
2. Click **Client Install Feature Set**, and then click **Add Client Install Feature Set**.
3. Add a feature set name, and uncheck all but the following checkboxes, and then click **OK**:
   a. **Application and Device Control**
   b. **Firewall**
   c. **Intrusion Prevention**
4. Click **Client Install Package**, click **Export a Client Install Package**, add the feature set you created in the previous step, and create a client installation package to deploy to the PoS devices.

For more information on how to install a custom client installation package with different features:

https://www-secure.symantec.com/connect/articles/how-do-i-create-and-configure-custom-symantec-endpoint-protection-installation-package-vers

Removing content

The Symantec Endpoint Protection client uses signatures and virus definition files as part of the antivirus engine. These signatures and virus definition files are referred to as content. All content is available on LiveUpdate™ and is periodically updated. If you do not install all of the technologies of the Symantec Endpoint Protection client, you can remove some of the content from the client installation package.

You can remove the largest content files when you export the client package from Symantec Endpoint Protection Manager using the **Basic Content** option on the **Export a Client Install Package** task. In addition, you can remove all content from the client installation package. The client then downloads only the required content when LiveUpdate runs on the PoS device. Since only the required content is downloaded, the client requires less disk space on the PoS device.

To remove all content:

1. Export the client package as a non-EXE file.
2. Open the folder where you exported the client installation package files.

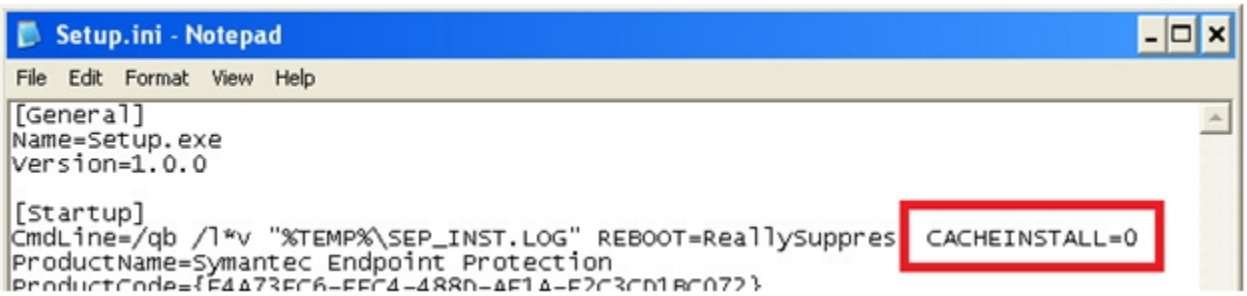
3. Delete the following file file: *Defs.zip

Removing the client installation package in cache

By default, the entire client installation package is cached on the PoS device. To prevent the installer from caching, install the package by changing the setup.ini file. This reduces the client size by more than 100 MB.

To remove the client installation package from the cache:

1. Export the client package as a non-EXE file.
2. Open the folder where the client package files were exported.
3. Edit the setup.ini in Notepad or another text editor.
4. At the end of the line that says “CmdLine=”, type “CACHEINSTALL=0”.



Enabling Write Filters

The Write Filter is a feature of the Windows Embedded client that may be enabled on different PoS devices. It can prevent changes to the disk (or flash) drive to ensure that the device is the same as the last time it started. When the Write Filter is enabled, any changes made are lost when the device restarts. In case an embedded system encounters an issue, you can simply restart the device to reset it.

For details on the Write Filter, see:

http://technet.microsoft.com/en-us/library/bb932158.aspx

Symantec Endpoint Protection 12.1 has the ability to work with the Write Filter, but requires some changes. For more information about how to use the Write Filter with Symantec Endpoint Protection 12.1, see:

http://www.symantec.com/docs/TECH185704

Before building a system image

If you are going to build an embedded image for redeployment, you need to remove some of the duplicate client identifiers. For more information, see:

http://www.symantec.com/docs/HOWTO54706

Supported operating systems for Symantec Endpoint Protection 12.1

The Symantec Endpoint Protection Manager and Symantec Endpoint Protection client support the following standard Windows operating systems:

- Windows 2012 (including R2)
- Windows 2008 (including R2)
- Windows 2003
- Windows 8.1
- Windows 8
- Windows 7
- Windows Vista
- Windows XP

Symantec Endpoint Protection supports the following common embedded systems on both 32-bit and 64-bit operating systems:

- Windows Embedded Point of Service (WEPOS)
- Windows Embedded POSReady 2009
- Windows Embedded POSReady 7
- Windows XP Embedded (XPe)
- Windows Embedded Standard (WES) 2009, 2011, 2012
- Windows Embedded Standard 7 (Windows 7 Embedded)

Legal notice

About Symantec

Symantec protects the world's information, and is a global leader in security, backup, and availability solutions. Our innovative products and services protect people and information in any environment – from the smallest mobile device, to the enterprise data center, to cloud-based systems. Our world-renowned expertise in protecting data, identities, and interactions gives our customers confidence in a connected world. More information is available at www.symantec.com or by connecting with Symantec at go.symantec.com/socialmedia.

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