Windows Embedded

Securing Your Windows Embedded POSReady 7 Device

Microsoft Corporation
May 2011

Windows® Embedded POSReady 7

Security in retail and hospitality environments is critical. Securing the Point Of Service (POS) means protecting the POS devices and the enterprise networks to which they are connected.

Built on the strengths of the Windows® 7 platform, Windows Embedded POSReady 7 helps strengthen the POS device and the enterprise network.

Contents

Introduction

Securing Point-Of-Service (POS) devices and the enterprise network is critical. Windows Embedded® POSReady 7 enables the protection of POS devices and the enterprise network on which they are connected, building on the strengths of the Windows 7 platform. POSReady 7 readily connects to Windows Server 2008® and industry-standard deployment and management tools while providing embedded enabling features unique to retail and hospitality.

This white paper covers security features provided by POSReady 7, how they relate to PCI-DSS version 2 standards and best practice references. Topics include:

- Securing the POS device through:
  - Safeguarding the operating system.
  - Safeguarding the device system drive's applications and data.
- POSReady 7 and network security.
- POSReady 7 and Payment Card Industry (PCI) security recommendations.
- POSReady 7 solutions for POS devices.

Securing the POS Device

POSReady 7 is uniquely positioned to help secure devices that are used by a variety of users. Unique to the Windows Embedded operating system, OS (operating system) images can be configured with only the components required for the device's function. Components not required are not just disabled; they can be removed from the OS image. Users have no access to components that have been removed.

The result is a reduction in attack surface area at the point of service, and a more reliable and consistent user experience for customers and retailers who use POS devices in environments where IT staff may not be immediately available. POSReady 7 images can be built to exact requirements, increasing confidence while providing the ability to update efficiently as requirements develop over time.

Safeguarding the Operating System

POSReady 7 provides a number of features that help safeguard the operating system of POS devices. These features include:

- **Dialog Box Filter** provides the ability to define default actions to manage pop-up dialogs before the users ever see them.

- **Keyboard Filter** suppresses a single key or combination of keys. For example, an IT administrator could protect the users from closing a POS application with ALT+F4 or restarting the POS devices with CTL+ALT+Delete.
- **Write filters** are unique to POSReady 7 and other select Windows Embedded platforms. Write filters protect the device media using a memory overlay. Writes are redirected to an overlay during normal operation, but are discarded when the device is restarted. Select writes can be persisted, typically to update antivirus, antimalware applications. There are two write filters available:
  - **File-Based Write Filter (FBWF)** protects device media at the file system level.
  - **Enhanced Write Filter (EWF)** protects device media at the volume level.
- **Shell Launcher and custom shell support** enable replacement of the default Windows Explorer shell with a custom shell specific to a retail or hospitality environment. In addition to custom user interface options, the custom shell could prevent switching to non-business related applications, accessing the Control Panel, or accessing the operating system. Shell Launcher handles executing the **Run** and **RunOnce** registry keys, and restarting the custom shell when needed. The **RunOnce** key is especially important for a number of deployment and management scenarios.

Safeguarding the System Drive, Applications and Data

POSReady 7 provides a number of features that help safeguard the applications and data on the POS system drive. Secure drives, applications and data with:

- **Microsoft® BitLocker® Drive Encryption and BitLocker To Go™** help protect data on fixed and removable drives. BitLocker Drive Encryption provides the ability to encrypt drives with a passkey that is effective even if the drive is removed. BitLocker to Go extends BitLocker data protection to removable media such as USB flash drives.
- **Microsoft AppLocker™** enables security and flexibility by managing access to applications, scripts and DLLs through Group Policy. AppLocker helps manage what the customer can access on the POS device, while granting additional access to an IT administrator, for example.
- **Windows® Internet Explorer® 8 and Internet Explorer 9** provides an Internet browser with enhanced security features like phishing filters, adjustable trust settings, and (in the case of Internet Explorer 9) integration with the Microsoft SmartScreen® Filter to help protect from both malware and spyware.
- **Windows® Firewall with Advanced Security** provides host-based, two-way networking traffic filtering for your POS device. This allows the IT administrator to block unauthorized network traffic flowing in and

out of each device. It also works with Network Awareness so that IT can apply security settings appropriate to the types of networks to which the device is connected.

- **Familiar user account controls** allow administrators and users varying levels of POS device access.

POSReady 7 and Network Security

POSReady 7 helps secure mixed network environments that support both corporate and public connectivity through the following:

- **Microsoft System Center Configuration Manager 2007 integration**. POS devices can be managed and maintained through System Center Configuration Manager 2007 similar to PCs and servers.
- **Automated Servicing.** Windows Update can keep security patches current.
- **Network Access Protection (NAP)**. NAP is a feature in Windows Server 2008 that controls access to network resources based on a client computer's identity and compliance with policy. NAP allows network administrators to define levels of network access based on who a client is, the groups to which the client belongs, and the degree to which that client is compliant with policy. If a client is not compliant, NAP provides a mechanism to automatically bring the client into compliance, and then dynamically restore its network access.
- **Full Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6) Support**. POSReady 7 supports IPv6, which increases the address space from 32 to 128 bits, providing for a vast number of network and system connections.
- **Active Directory® Domain Services (AD DS) Support.** POSReady 7 provides support for Group Policy that can be used to manage your POS devices similar to PCs and servers on your enterprise network.

POSReady 7 and PCI-DSS Security Recommendations

The Payment Card Industry Data Security Standard (PCI-DSS) provides a set of industry-recommended standards and requirements that are implemented through people, process and technology. POSReady 7 helps retailers bring their POS environments to PCI-DSS compliance, enabling a secure solution while providing the ability to present a rich, interactive experience to customers.

The following table highlights the PCI-DSS version 2 goals, requirements and recommended solutions to satisfy the requirements. A link to the PCI-DSS document library is provided at the end of this paper.

Table 1: PCI-DSS Goals, Requirements, and Solutions

PCI-DSS version 2 goals	PCI-DSS requirements	Solutions that incorporate POSReady 7
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data. 2. Do not use vendor-supplied defaults for system passwords and other security parameters.	• Enable firewall on POS devices. • Close unused ports on POS devices • Enable Windows Update to keep security patches current. • Allow critical updates through write filters. • Apply User Account Control Best Practices.
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks.	• Enable BitLocker and BitLocker To Go on POS devices. • Enable Keyboard filters to manage access to operating system. • Apply Secure Communications Best Practices.

Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software. 6. Develop and maintain secure systems and applications.	• Enable AppLocker to manage who can access applications and scripts. • Build and deploy POSReady 7 images with only the required OS. components. • Apply Enterprise Security Best Practices.
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need-to-know. 8. Assign a unique ID to each person with computer access. 9. Restrict physical access to cardholder data.	• Use a custom shell. • Centralize image deployment, updates and reporting with System Center. • Apply AD Management Best Practices.
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data. – TFS, event logging 11. Regularly test security systems and processes.	• Monitor POS device event and application logs periodically and purge them regularly. • Leverage all reporting associated with POS applications installed. • Use System Center reporting. • Apply Performance Monitoring Best Practices.
Maintain an Information Security Policy	12. Maintain a policy that addresses information security.	• Follow current government/industry standards and recommendations. • Follow current Microsoft Security Bulletins. • Engage your Microsoft Account Manager.

POSReady 7 Solutions for POS Devices

POSReady 7 devices are commonly found in trusted environments where customers and retailers expect a familiar, rich and interactive experience.

The following sample POSReady 7 device scenarios illustrate some of what's possible:

- **Self-service checkout kiosk**. A next generation UI built on Windows Presentation Foundation delivers the ability for the consumer to get in-depth information on a product or service. Using a common set of Silverlight Expression Blend® generated controls, multiple presentation skin overlays can be applied to the same control suite. For example, a retail application showcasing a "beach" theme and another one with an "alpine" theme can both use the same controls. Using Windows Touch, the application can prompt for language choices, including non-Western language sets such as Kanji and Chinese (Simplified and Traditional). The application is fast and nearly tamper proof as administrators can remove components from the operating system image that are not required.
- **Retail information kiosk**. Monitored by System Center Configuration Manager 2007, an interactive retail information kiosk informs the customer when the store is out of stock of an item being searched on. It prompts the business to send the item directly to the customer's home or notifies the customer when the item will be available at the present store location or another location. A preconfigured web browser provides links to the item manufacturer, providing additional product depth.
- **Gift registry kiosk**. Using a common set of Silverlight Expression Blend generated controls, multiple presentation skin overlays and themes can be presented to customers and gift suggestions that they can use to participate in a gift registry. Deployed worldwide and usable to multinational personas though MUI support. The kiosk runs within a custom application shell with pre-configured dialogs in multiple languages, and is protected with AppLocker and BitLocker. Responses to customer inquiries are fast and efficient after components not needed for the operating system have been stripping from it. Kiosks that run POSReady 7 are Payment Card Industry (PCI) compliant, and equipped with the ability to allow customers to choose the language want to use to operate them.

Conclusion

Windows Embedded POSReady 7 builds on the strengths of the Windows 7 platform to include features unique to retail and hospitality. POSReady 7 readily connects to Windows Server 2008, deployment and management tools, providing additional security, monitoring and maintenance.

POSReady 7 increases confidence in customers and retailers by providing features that help secure the POS device and the enterprise network. The POS environment can be PCI-DSS compliant while delivering rich and interactive experiences that attract and retain customers.

Additional Resources

Additional resources related to this topic include:

- Windows Embedded:
  http://www.microsoft.com/windowsembedded/en-us/windows-embedded.aspx
- POSReady 7: Addressing Common Retail and OEM Scenarios:
  http://www.microsoft.com/presspass/presskits/embedded/pageResources/01-11WEPOS7-white.pdf
- PCI Security Standards Council Document Library
  https://www.pcisecuritystandards.org/security_standards/documents.php
- Securing the Retail Store Series:
  http://msdn.microsoft.com/en-us/library/aa479366.aspx
- Enterprise Security best practices:
  https://www.pcisecuritystandards.org/security_standards/documents.php
- 19 Smart Tips for Securing Active Directory:
  http://technet.microsoft.com/en-us/magazine/2006.05.smarttips.aspx
- Best Practices for Securing Communications:
  http://technet.microsoft.com/en-us/library/bb681065.aspx
- User Account Control in Windows 7 Best Practices:
  http://technet.microsoft.com/en-us/library/ee679793(WS.10).aspx
- Performance Monitoring best practices
  http://technet.microsoft.com/en-us/library/cc728128(WS.10).aspx
- Microsoft Business for Small and Midsize Companies Security:
  http://www.microsoft.com/business/en-us/solutions/security/default.aspx?fbid=o4tcjCpqqVy
- Microsoft Security Bulletin Search:
  http://www.microsoft.com/technet/security/current.aspx
- Windows Update:
  http://www.microsoft.com/windows/downloads/windowsupdate/default.mspx