

Solidify Your Retail POS Devices



Retail Industry Trends

The retail industry is being revolutionized by the movement in consumer perception of shopping exemplified by “Shopping is Theater”. Increasingly, consumers are expecting shopping to be a highly interactive and rewarding experience. This has been driving the need for reduced time to market of newer retailing ideas, and the use of advances in hardware and software technologies to create a richer experience, while keeping the total costs of ownership low.

Two trends in retailing technology have gained prominence as a result of this. The first is the increased use of standard operating systems such as Microsoft Windows XP, Windows XP Embedded, WEPOS, and Linux. The second trend is that retail devices are becoming increasingly interconnected. These trends have come about due to a variety of factors including:

- A desire to reduce the cost of development of hardware and software for retail devices
- Need to use standardized interfaces such as UPOS, etc.; and need to support newer software and hardware on existing hardware
- A desire to leverage the large development community behind the third party operating systems

Retail Industry Challenges

The retail industry computing infrastructure includes point of sale and point of service devices such as POS checkout terminals, self check units, cash drawers, information/web kiosks, PCs, and back office servers. The shift towards standard operating systems and increased network connectivity has given flexibility to the industry, but at the cost of ‘control challenges’. Retail devices typically flow through a multi-

party distribution channel from the device manufacturer, to the system integrator or dealer, and finally get deployed at the retail site. Owing to the existence of multiple parties involved in the distribution channel, it often becomes difficult to control the state and availability of the retail device when in production. This leads to several business level challenges such as:

- How to keep support costs of retail POS devices low?
- How to increase revenue?
- How to help device manufacturers, system integrators, and dealers to meet the retailers’ requirements?

Operational Challenges

The following sections describe the key operational challenges faced by the retail device industry.

Multi-stage, multi-party distribution channel

- Who owns the end state of the retail device in production?
- Who decides the change policy (what, when, who) for software updates?
- What software should be allowed to run on the retail devices?
- What software and hardware peripherals can be attached to the retail device?

In a typical distribution channel for retail devices, at the head of the channel is the device manufacturer, who assembles the initial retail device from hardware and software of their choosing. The retail device then passes through the hands of one or more system integrators, dealers, distributors, and/or value added resellers (VARs), before being delivered to the retailer. Each VAR may choose to add applications or peripheral hardware (with the corresponding software)

before passing the device further down the channel. Eventually, the device ends up in the hands of a retailer who is expected (but may or may not) to use the device without further modification.

In such a situation, it often becomes difficult to enforce a validated golden base image, approved and certified by the retail device manufacturer. The device manufacturers face the challenge of how to control what level of flexibility to give to their distribution channel to change the base image, as it gets deployed; which directly translates into which peripheral devices and corresponding software can be installed on the retail device. Also, on an ongoing basis, which software updates can be installed on the deployed retail devices in production (and which should not be installed), is an issue over which the device manufacturer has no enforceable control today, other than honor code or warranty violations.

Ability to control maintenance schedules

- How to enforce a change policy of what changes can be made, when?

In addition to the above challenge of controlling what software can be updated, is the challenge of controlling when the software can be updated on the deployed retail devices and in what order, given the existence of multiple parties in the distribution channel. Today, the device manufacturer has no control over when the changes are made or whether only approved and certified changes are made by authorized support personnel.

Support Challenges

Increased In-field breakage due to security attacks

- Are your retail POS devices secure against existing and zero day security threats?

Retail devices present an **increased attack surface** today as compared to similar devices in the past, due to:

- being part of increasingly inter connected retail networks,
- running commercial operating systems and commercial applications, and
- using industry standard interfaces for peripherals and retail applications.

Due to the increased attack surface area, retail devices are vulnerable to existing and zero day security threats in a manner similar to a white box PC. Worms, viruses, malware can compromise and spread on these retail devices just like on a Windows system. This is one of the key causes of in-field breakage or unavailability of retail devices. One popular method used to protect them against security threats is the use of anti-virus software; however, this is not sufficient to defend against zero day threats and also has a negative impact on the performance of the device.

Test & validate every patch, monthly patching cycle, dedicated test team?

- Can the device manufacturer or channel afford to validate every software update and patch to be applied to all the models of retail devices in production, in every geographic location?

Often device manufacturers and other software providers in the retail distribution channel have to spend significant amount of time validating and testing any new software update (operating system updates, application updates, firmware updates, etc.) before rolling them out on the deployed retail devices.

Many of the retailers have become very security conscious and have chosen patching as the way to be compliant with the security standards. Scans of devices connected to the network are fairly common and the devices found need to be at the right patch level. This introduces a very difficult problem for the device manufacturers: consider a Windows based device; Microsoft releases a patch, and the retailer does a network scan and figures out that a Windows-based retail device does not have the patch. The retailer's security policy dictates that since this is a high priority patch it should be deployed within 24 hours otherwise it shows red on the dashboard. Microsoft could not have tested the patch with the specification of the embedded device. If the retailer deploys the patch, it may break the device. This puts additional pressure on the device manufacturer to test all Microsoft patches coming out. This can be very time consuming and a huge resource drain – and borders on being infeasible.

In addition, the above problem is complicated if there is a channel involved: Company A produces a retail device which is resold by a reseller. The reseller may be installing some value added software to the device - for example, monitoring or anti-virus software. Now, if a patch comes out, every party in the channel has to test it with their software on the device – making it very difficult to meet the retailer's mandated standard for patching in 24 hours or 48 hours.

Not only is this expensive but also not scalable given the complex matrix of operating system flavors, application flavors, and number of retail models deployed. It often forces the device manufacturers to have a dedicated team that is responsible for validating and certifying patches in time, or play catch-up when the deployed retail devices get updated by any party in the distribution channel.

Who pays for the in-field breakage?

This is a question that often haunts the retail distribution channel. When the retail devices in production go through changes, some authorized, some unauthorized or uncertified, then the rate of breakage in the field increases. In such cases, it is often difficult to decide which software updates made to the retail device led to the breakage of device functionality, who made these updates, and hence who should pay for the break-fix cost? Should it be the retailer who applied

the software updates to protect against the latest virus outbreak, or is it the channel providing the support who also sneaked in some unapproved and untested software updates during the last scheduled maintenance cycle?

Increased supports costs to replace and fix returned devices

Often, the device manufacturer's or channel's support team is required to fix an unavailable retail device, either remotely or via on-site analysis. If the device cannot be fixed on site, the quickest option for the support personnel is either to replace its parts, or else to replace the device and get back the original device for maintenance. This is an expensive support process and not feasible for small or distant retail stores where the device manufacturer wants the retail device to perform as expected all the time.

Increased support costs to break-fix devices with customer data

To add to the break-fix support costs, if the unavailable retail device or its corresponding back office system has retail customer data on it, then there are extra steps to backup and clean the data for recovery and privacy reasons before shipping the device or back office system to the manufacturer.

Violating regulations: Are the retail devices still compliant?

Many devices are accessed by on-site support personnel with administrative privileges for applying software updates and for break-fix support. Often, the support personnel are contracted from 3rd party support services or other professional services companies and not necessarily from the device manufacturer or the channel.

In such a scenario, how can the retailer be sure that only the authorized and certified changes/updates have been applied and the known policies and procedures have been followed? This lack of control directly translates to uncertainty as to whether the device is still compliant with mandatory regulatory standards such as PCI. Is there an audit log of all the software updates made to prove compliance of the retail device/infrastructure?

Centralized software distribution model does not suit all the retail stores

It is often the case that when the size of individual retailers is small and/or geographical location of the retailers is remote, the centralized software distribution model doesn't work, and support personnel have to provide on-site support.

Increasingly interconnected & highly configurable

Complex network topologies exist between device manufacturer and dealers, system integrators, and the system integrators and the retail store networks. The rate of change of software and configuration on these retail devices, running commercial operating systems and applications, is high. As a result, the party in the distribution channel

providing ongoing support is forced to have an expensive support SWAT team available for handling change while keeping the retail devices up and functional.

Revenue Stream Challenges

How to increase revenue?

Several retail device manufacturers have a revenue stream via professional services and certifications. They charge for adding or certifying that a new hardware/application/software/version is compatible and can be installed on the retail device deployed in production. However, the device manufacturers do not have a way to enforce this other than owning the entire professional services and support role of the distribution channel.

Meeting Retailer Requirements

How to empower device manufacturers, system integrators, and dealers to meet retailer requirements?

The retailers often have demands for one or more of these: low TCO, high SLA on availability, compliance (e.g. PCI) , manageability, performance, security etc. It is often difficult for the device manufacturers to meet all of the above requirements without any additional software.

Solution Characteristics

The following section describes the key characteristics of a solution to address the above challenges. The solution must be able to give flexibility and help retain control while keeping the support costs low.

- **Provide Control over Deployed Devices:** have better control over the state of the deployed POS devices and back-office servers; control what's installed and running on them. Reduce in-field breakage with this control as the retail device passes through multiple dealers in its multi-stage manufacturing process and while in-production. Enforce that only the software authorized by device manufacturer gets installed.
- **Improve Security and Reduce Patching:** reduce security risks, reduce the overhead from frequent patching and maintenance of deployed POS devices and back-office servers, reduce the number of touch points and rate of change on the devices in production
- **Low touch:** provide a solution that works out of the box and requires little or no training of large and distributed dealer network, (that provide ongoing operational and maintenance support services for the deployed POS devices and back-office servers at the retail site). Also, the solution must not impact retailer requirements of low footprint, performance, and availability.

Solidcore's S3 Control - Embedded

Solidcore's *S3 Control - Embedded* helps address the above challenges of providing device control and enhanced zero day threat protection, thereby reducing support costs and making devices compliance ready for the retail industry. It integrates with manufacturer/channel or retailer's manufacturing, provisioning, monitoring, change management and in-field maintenance processes while keeping total costs of ownership low. It is a low footprint, low overhead control and security solution that can be setup quickly with very low initial and ongoing operational overhead.

S3 Control for Embedded has three key features described below.



- **Device Control**

The Device Control module helps enforce the device manufacturer's change control policy in two distinct workflows: as the device flows through its multi-stage manufacturing lifecycle as multiple channel vendors install their own software and value added services; and secondly during in-production operational maintenance as the device owner or the multiple channel vendors issue software updates for their software and hardware. This module is flexible, and allows several modes of operation. For example: It can enforce that only the software certified by the device owner can be applied to the device during manufacturing and in-production and none other. It can also allow selective

channel partners to be able to make updates to the device and log the updates made for use in forensics.

- **Device Security**

The Device Security module helps provide protection against existing as well as zero day polymorphic threats via malware such as worms, viruses, Trojans and buffer-overflow threats, etc.; thereby ensuring that the device is secure and cannot be compromised in production. It also helps eliminate emergency patching, reduces the number and frequency of patching cycles, and enables more time for testing before patching. It reduces any security risk on difficult to patch devices, for example, devices that are remote and distributed, in areas with little or no local support. The Device Security module helps reduce costs of operations by reducing both planned patching and unplanned recovery downtime, thereby increasing device availability. It reduces the support costs by reducing number of touch points needed. This turns out to be an ideal solution for lower end devices or for devices in small or distant retail stores.

- **Compliance Enabler**

The Compliance Enabler module is a by-product of the above two, and enforces that the control requirements for PCI, and other regulatory standards are met, and necessary tamperproof audit logs are present to prove that regulatory controls are in place.

Conclusions

This white paper outlined some of the considerations that adopters of control and security solutions for retail POS devices have used to evaluate and compare different solutions.

Solidcore offers a unique combination of control and security solution that can help the device manufacturers or the system integrators, dealers, VARs, and professional services groups in significantly reducing their ongoing support costs. S3 Control helps reduce the number of in-field breakage incidents due to unauthorized changes and security threats by adding enhanced control and security to retail POS devices.

About Solidcore Systems

Solidcore is a leading provider of change control for embedded systems and enterprise change management. Solidcore is used by major manufacturers of ATMs, point-of-sale terminals, thin-clients, storage appliances and other devices to securely leverage open systems while controlling support costs. Solidcore also adds control to enterprise change management with real-time change auditing and the industry's first and only solution to automate the enforcement of change management policies. Customers trust Solidcore to improve service availability, implement ITIL initiatives, and lower costs related to Sarbanes-Oxley compliance. Solidcore is headquartered in Palo Alto, California. For more information, visit www.solidcore.com.

solidcore®

Solidcore Systems, Inc.
3408 Hillview Avenue, Suite#180
Palo Alto, CA 94304

Email: sales@solidcore.com
Web: <http://www.solidcore.com>
Tel: 888.210.6530