# Make your Retail Systems Market Ready: Faster, Better & More Secure

## Industry Trends

Every industry is being revolutionized by technology: Retail, Healthcare, Finance, Restaurant, Travel and Government. The trend is to create a rewarding and interactive customer experience. This has been driving the need for reduced time to market of newer store ideas, and the use of advances in hardware and software technologies based on industry standards, to create a richer customer experience, while keeping the total costs of ownership low.

Two technology trends have gained prominence. The first is the increased use of commercial and open operating systems such as Microsoft Windows XP, Windows XP Retail, WEPOS, and Linux. Secondly, that the retail systems are becoming increasingly interconnected. These trends have given flexibility to the retail system manufacturers to stay competitive in this low margin business.

## Solidcore's learning from its customers

The above trends have definitely given flexibility to the retail system ( kiosks, point of sale etc) manufacturers but at the expense of control, security and compliance challenges. The most asked question while architecting a Kiosk or putting a point of service system in production is *how to lockdown and secure them, how to make them work in the field as shipped?*

The following sections highlight some of the challenges that Solidcore has learnt from its customers shipping retail systems.

### Business Challenges

Business challenges faced by retail system manufacturers, system integrators and the channel that service them:

- How to keep maintenance and support costs of retail systems low?
- How to increase margins and revenue?
- How to help retail system manufacturers, system integrators, and dealers meet their customers' requirements?

### Operational Challenges

MULTI-STAGE, MULTI-PARTY DISTRIBUTION CHANNEL

- Who owns the end state of the retail system in the field?

> *"We identified uncontrolled change as the primary cause of POS unavailability issues and maintenance costs for our POS devices. Embedding Solidcore into our POS systems gives us complete control and certainty over what changes on each device. The added control enables us to drastically reduce our support costs by preventing all out-of-policy changes and eliminating emergency patching procedures."*
>
> - Hiroshi Komura
> General Manager
> i-Appliance division, NEC Infrontia

- Who decides the change policy (what, when, who) for software updates and the maintenance schedules?
- What software should be allowed to run on the retail systems in the field?
- What software and hardware peripherals can be attached to the retail system in the field?

Many retail systems typically flow through a multi-party distribution channel. The retail system may pass through the hands of one or more system integrators, dealers, distributors, and/or value added resellers (VARs), before being delivered to say a retailer. Each VAR may choose to add applications or peripheral hardware (with the corresponding software) before passing the system further down the channel.

In such a situation, it often becomes difficult to enforce a validated golden base image, approved and certified by the retail system manufacturer. The latter 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 what software can be installed on the retail system. Also, on an ongoing basis, which software updates can be installed on the deployed retail systems in production (and which should not be installed), is an issue over which the retail system manufacturer has no enforceable control today, other than honor code or warranty violations.

### Support Challenges

INCREASED IN-FIELD BREAKAGE DUE TO SECURITY ATTACKS

- Are your retail systems secure against existing and zero day security attacks?

Retail systems present an increased attack surface today and are vulnerable to existing and zero day polymorphic security threats via worms, viruses, malware, buffer over flow attacks, rootkits etc. This is one of the key causes of in-field breakage or unavailability of retail systems. One popular method used to protect them against security threats is system hardening and the use of anti-virus software; however, the latter is not sufficient to defend against zero day threats and also has a negative impact on the performance of the retail system.

### TEST & VALIDATE EVERY PATCH, MONTHLY PATCHING CYCLE, DEDICATED TEST TEAM?

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

Often retail system 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 systems.

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 retail system manufacturers to have a dedicated team that is responsible for validating and certifying patches in time, or play catch-up when the deployed retail systems get updated by any party in the distribution channel.

### WHO PAYS FOR THE IN-FIELD BREAKAGE, RETURNED SYSTEMS?

This is a question that often haunts the distribution channel. When the retail systems 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 do root-cause analysis and figure out what led to the breakage of retail system 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 that also sneaked in some unapproved and untested software updates during the last scheduled maintenance cycle?

### VIOLATING REGULATIONS: ARE THE RETAIL SYSTEMS STILL COMPLIANT?

Many systems are accessed by on-site support personnel with administrative privileges for applying software updates and for break-fix support. Key challenge is whether they stay compliant after every support procedure?

### CENTRALIZED SOFTWARE DISTRIBUTION MODEL DOES NOT SUITE ALL 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 onsite support. How to ensure same updates are applied in every scenario?

## Revenue Stream Challenges

### HOW TO INCREASE REVENUE?

Several retail system 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 system deployed in production. However, the system manufacturers do not have a way to enforce this other than owning the entire professional services and support role of the distribution channel.

## Meeting End-Customer Requirements

### HOW TO EMPOWER MANUFACTURERS, SYSTEM INTEGRATORS AND DEALERS TO MEET RETAILER REQUIREMENT?

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 retail system manufacturers to meet all of the above requirements without any additional software.

# Solidcore's S3 Control for Retail - Benefits

## Faster, Better and more Secure

Solidcore's *S3 Control for Retail* addresses the above challenges. It helps accelerate time to market by providing a quick to deploy software solution that provides out of box security, lockdown, software change control and compliance, the essentials of a production ready retail system.

- Out of box Security: protect against existing and zero day threats including worms, viruses, Trojans, malware, buffer overflow attacks, rootkits etc.

- Enables Software Change Control: Enforce system manufacturer's software change policies. Control what software gets installed and runs during retail system's lifecycle. Ensure only software authorized by system manufacturer gets installed and run on in-field systems.

- Reduced Support Costs: reduce in-field breakage by preventing any unauthorized changes. Lockdown hard to service systems in remote locations.

- Control over Patching: gain increased time for testing of patches, reduce the overhead from frequent emergency patching required to stay secure

- Low touch: works out of the box; requires little or no training and overhead; does not impact requirements of low footprint, performance, and availability.

- **Compliance Ready:** control the state of the retail system with audit logs of every authorized change or unauthorized attempt.

- **Integration ready:** Integrates with manufacturer/channel or retailer's manufacturing, provisioning, monitoring, change management and in-field maintenance processes.

## Solidcore's S3 Control: Feature Overview

The following section describes the key features that enable S3 Control to provide the above benefits to retail systems:


*Solidcore's S3 Control – Reduces time to market for Retail Systems*

- RUNTIME CONTROL

  *Helps control what software can run*

  The Runtime Control module helps control what software can run from disk and in memory, preventing execution of any unauthorized code. It provides protection against existing as well as zero day polymorphic threats via malware such as worms, viruses, Trojans , rootkits, 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 Runtime control 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 remote retail stores.

- CHANGE CONTROL :

  *Helps control what software can change, how, by whom, when*

  The Change Control module helps control what software changes can be made, by whom, when and how, via authorized updaters, authorized change control windows and secure signed updates. It enforces 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 or audit.

- CHANNEL FRIENDLY:

  *Quick and Simple Setup*

  The software solution is very easy and quick to setup, doesnot require any ongoing configuration or signature updates to be effective. It has very small footprint and low performance overhead.

  *Flexible Operational Integration*

  S3 Control is flexible to support common mechanisms of making software updates to production systems. It empowers service channel to control changes without changing their existing software update workflows.

- COMPLIANCE READY

  S3 Control helps enable compliance ready retail systems. It helps meet requirements for PCI DSS, HIPAA and other regulatory standards, and generates necessary tamperproof audit logs to prove regulatory controls are in place.

## Summary

Solidcore offers a unique combination of control and security solution that can be deployed very quickly and enhance any retail offering for kiosks , point of sale systems or ATMs. It can give a competitive edge in reducing OEM support costs by controlling production changes and reducing support incidents over a known and predictable system state. It helps lower end customer's total cost of ownership by enabling patching only once a year and obviating the need for ineffective antivirus solutions. Lastly, it helps meet end customer requirements of compliance.

### About Solidcore Systems

Solidcore is a leading provider of change control for retail 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 is headquartered in Palo Alto, California.