Product Bulletin

Solidcore/McAfee S3 Control

MB-1215 Issue 4.2b
May 30, 2012

This Issue 4.2 updated the pricing and discount policy. Issue 4.1 updates the PIN description. Issue 4 updated the bulletin in general and changed the licensing process and requirements for the inclusion of Solidcore for ScanMaster and ISS45 stores. Changes of significance for Issue 4 and 4.1 are in red.

StoreNext is pleased to provide Solidcore/McAfee S3 Control for StoreNext ISS45 and ScanMaster POS systems and related StoreNext software. Support, dealer training and professional services packages will maximize dealer and grocer benefit.

No-Frills Summary

Solidcore is available for purchase for ISS45 and ScanMaster systems by Solidcore authorized dealers.

To get Authorized - attend the three S3 webinar classes.

Solidcore has been certified with all StoreNext software.

Solidcore is one of the best ways to handle data breach worries and meet PCI with lower business risk.

Solidcore S3 Control creates a "good list" when installed, and only lets these "good" programs run. This prohibits viruses and un-authorized programs and changes.

S3 installs and inventories the software automatically.

S3 is "deploy and forget" and doesn't need daily downloads.

S3 doesn't use up your CPU like standard anti-virus.

New and existing stores can purchase S3 for $495 list.

Positive change control — prevents breaches, viruses, user blunders, and unauthorized playware, software and system changes from being implemented on any S3 "solidified" machine.

- Deploy-and-forget — Solidcore doesn't need daily downloads from the Internet. Once S3 is installed, everything on that "solidified" machine runs normally.
- PCI Requirements — S3 Control enables your customers to meet some of the key compliance requirements for PCI certification and simplifies meeting some other PCI requirements. Even more important, Solidcore prevents utility-style and purpose-built malware from being installed and breaching sensitive data.
- No performance degradation — standard anti-virus ("A-V") software constantly searches through massive lists of thousands of viruses consuming the CPU. A test at one wholesaler showed their A-V software was locking up 85% of POS terminals' processing capability and slowing down shopper service. Solidcore never uses more than half a percent of runtime CPU resources.
- Change tracking — in real time, S3 Control tracks all software program changes across the store or infrastructure, including the Windows registry and network device configurations. Logs can be read by the Windows Event Viewer and forwarded to such systems as Netcool or MARs.

Solidcore's outstanding combination of system protection, PCI remediation assistance and system control support tools — while bringing back performance without downloads — gives StoreNext dealers a competitive advantage. Plus, StoreNext's S3 version, when operating in a StoreNext POS site, also includes the same full protection for WinEPS, Connected Services, RBO, PocketOffice, Retalix Store and HQ, and is fully compatible with Code Distribution as well as wholesaler utilities and third-party products.

To Your Success,

Antony van Seventer

A HARD SHELL AGAINST THREATS

Software is soft. That's the whole point of software. But that's also the primary risk.

The fundamental value of Solidcore S3 is to reduce and usually eliminate user risk from technology threats. S3 builds a hard shell around your software, so that only authorized users and programs can change the data and update or modify the software. Then S3 tracks all such changes with ultra-secure databases and technology so that whatever took place can always be reviewed for diagnosis and correction.

Threats to software and data come from many sources:

- ***Traditional threats*** — such as viruses, worms, Trojans and spyware
- ***Emerging threats*** — from increasingly sophisticated "malware" such as zero-day attacks, buffer overflows, code injection and exploiting existing applications.
- ***Payment threats*** — Recent breaches exposed how thieves built specific malware to propagate through enterprises and stores and steal card data. These viruses would never be seen by standard-issue A-V, but Solidcore won't even let them install.
- ***Internal threats*** — unauthorized changes, (even well-meaning) internal tampering, auto platform updates that break applications. This includes port and data transmission monitors that can grab credit card numbers.
- ***Business costs and risks*** — due to possible failures of regulatory or financial compliance, security audits, downtime and damage to customer confidence and trust

Who's Using Solidcore – and What Do They Say?

S3 has been proved already in other large and complex commercial application areas:

- **Wells Fargo** uses S3 throughout their entire ATM operation.
- **IBM** implemented S3 across their high-end DB2 applications after their professional hacking team concluding that "no attack against Windows can succeed."
- The **U.S. Navy** needed positive protection in critical areas and employed S3 after a lengthy test where all attacks failed.
- **General Motors** has now tested and deployed S3 on all of its DNS servers world-wide.
- **@Stake**, a business security consulting firm, (1) only authorized code can run, (2) authorized code cannot be modified and (3) authorized code cannot be hijacked.

Independent grocers are even more exposed than most businesses. They are unlikely to have a sophisticated IT staff controlling and protecting systems, and also unlikely to have established and monitored procedures in the stores. But they are likely to have "open" systems and transient, unmonitored staff with just enough knowledge to be dangerous – whether they intend to be or not.

When your independent grocers have risk, you have risk too. Dealers have no choice but to fix a customer's damaged system, but this takes your best support staffers away from installations and other critical business with such unplanned crises. And wholesalers lose sales and competitive members when a grocer's business is compromised, and regulatory compliance issues (Visa/CISP/PCI) trickle *upward* and put the wholesaler's networks and processes at risk.

Solidcore S3 protects grocers — and therefore dealers and wholesalers — by locking down software and data so that only authorized programs and agents can change it.

- Protection from threats
  - Only authorized code can run
  - Authorized processes cannot be hijacked
  - Authorized code is made tamper-proof
- Change control on deployed systems
  - No automated/non-certified/untested operating system updates/downloads
  - Local lockdown of devices and endpoints during deployment

- Lowers operational costs and increases uptime after deployment

➢ Real-time change visibility and audit
- Customers can audit all changes
- Meets PCI change control and A-V (DSS Section 5) requirements

WHY NOT USE PLAIN OLD ANTI-VIRUS?

An updated version of "The Three Little Pigs" might have a house built of traditional A-V products. Like the straw house in the original fable, it looks fine until you get attacked, and then it gets blown away pretty fast.

it's important to really understand this section.

Here are a few of the insurmountable problems that show why "negative" prevention products — the ones that try and keep a black-list — can't handle the big bad wolf in a commercial grocery environment:

➢ ***Daily downloads —*** traditional A-V products operate by continuous monitoring for the digital "signatures" of known viruses and malware. Lack of knowledge, discipline resources, maintenance or updated anti-virus engines all prevent timely downloading of the latest problem data, and that makes the A-V product blind to the latest and most dangerous threats.

➢ ***Virus roulette —*** even if your daily download comes through, will it protect you? The propagation speed of "zero-day" malicious code has increased so that problems race through the Internet faster than A-V products can keep up. It's no longer a question of if your system will be brought down because your A-V was too slow; it's just a question of when.

➢ ***Custom tailored breaches —*** Identity theft is now a well-financed, international criminal business. With profits rivaling traditional underworld trafficking, cost is no object: we're seeing the most sophisticated malware that money can buy. They can get into POS systems in many ways: former and disgruntled employees can be bribed or share the profits. Service providers and technicians can use wireless – and even software upgrade CDs – to penetrate systems, gather data and automatically send it to overseas IP addresses. Standard A-V is totally helpless against these specialized attack programs and benign-looking standard monitoring utilities used by data thieves — they will never be noticed.

➢ ***Slow strangulation —*** the performance degradation of A-V products running in background is getting worse – literally – by the day. As the pile grows — with thousands upon thousands of malicious signatures the A-V has to check — and the threats' ever-increasing sophistication forcing larger and more powerful A-V software, tests showed that up to 85% of the POS' CPU time was consumed by A-V and scanning response time was getting slower and slower. Cashier sign-on took over 12 seconds. Instead of a virus bringing the system to its knees, the anti-virus programs were doing the job almost as effectively.

➢ ***You get an "incomplete" —*** try this: run any up-to-date spyware-prevention tool on your PC and get your machine squeaky clean. Then go to the Web and download a different one. Run it. How many did the new one find? Scary, isn't it. Then download another one. Get the point? No one product finds them all.

➢ ***Fast strangulation —*** make sure you have two or three A-V programs running all the time.

- ***Intel to the rescue? Sorry…*** — the chip makers of course keep making the CPUs faster and better. So can you keep up with the A-V performance drain with new and faster PCs, servers and terminals? Unfortunately, the rate of drain has eclipsed the rate of gain, and Noyce's law gets turned on its head when applied to the resources required to keep up with even simple virus protection. Even the new "dual-core" multi-threaded CPUs that can run simultaneous programs haven't fixed the problem – apparently, the A-V programs now require multiple processes themselves: they completely consume one thread while taking more and more of the remaining core.
- ***Vista to the rescue? Sorry …*** — it'll be great if Vista is perfected, and let's say that includes being hacker and virus-proof. How long will it be before your installed base of POS is all running on Vista machines? Oh yes – and what about all the ***other*** aspects of change and software control, tracking and logging.
- ***There's just no discipline*** — and even the best A-V program can't:
  - Keep store personnel from downloading "funware" during the night-shift
  - Keep dealer support staffers from copying software from infected CDs or USB sticks that the virus-catcher missed
  - Keep the whole unauthorized product, program, testing and update cycle from happening
  - Keep a record of everything that might have changed so you know what to back out.
- ***There's just no knowledge*** — if the A-V system pops up a warning alert and action prompt, how many clerks will coolly evaluate the situation and actually choose the best option under the specific circumstances to delete the data file, quarantine the executable or shut down and reboot the terminal.

And how many will just panic?

THE POSITIVE MODEL WITH DEPLOY-AND-FORGET

Solidcore S3 avoids all these problems due to constant "negative" screening via its unique ***"positive change control"*** model. Instead of frantically searching for malicious code against an ever-growing black-list, S3 instead knows all the right software that should be running on the particular machine, understands its processes and how the applications manage and update data, how its software maintenance is authorized and where that maintenance should be coming from.

ALL THE RIGHT SOFTWARE RUNS EXACTLY AS IT SHOULD.

NOTHING ELSE IS ALLOWED TO RUN.

Once Solidcore is implemented, that machine won't need constant updates. It's ***Deploy-and-Forget.*** Besides the high cost of the A-V software and their requirements for annual subscriptions, the constant requirement for updates is either a serious burden or impossible to fulfill. This has been one of the biggest issues for grocery A-V compliance, since many small grocers don't really know how the A-V system got there in the first place, how it really works, whether they've subscribed to updates, what the account number and password might be, whether they need to download a new testing engine and so forth.

For the grocer, these twin pillars of Positive Change Control and Deploy-and-Forget mean:

- They won't need to install and maintain it
- There's no impact on applications
- There's no impact on performance
- There are no signatures to update

- There are no alerts to review
- The process integration is seamless
- A complete record is maintained in a secure database

SOLIDCORE AND PCI COMPLIANCE

Solidcore helps grocers meet PCI compliance as documented in the PCI Data Security Standards (DSS).

PCI compliance is judged either by the merchant by using the PCI Self-Assessment Questionnaire (SAQ) or by a PCI Qualified System Assessor (QSA). So it's critical to understand that compliance is never a black-and-white issue. Many QSAs have become familiar with Solidcore but sometimes they aren't and need some education before they will agree on exactly what Solidcore has brought to the compliance status of a particular store.

Solidcore has an active program to educate PCI QSAs and their companies to understand the Solidcore S3 Control system and how PCI compliance is positively affected (a slide presentation on Solidcore PCI is available on the StoreNext Dealer Support Web site on the Presentations Page and the Solidcore Page).

There are several areas where Solidcore assists PCI compliance. Solidcore can be implemented with S3 Control at store-level only, but an enterprise-level system is also available from Solidcore directly that reports and manages all endpoints. See the slide presentation for a complete discussion of the DSS as it applies to Solidcore enterprise-wide. However, by implementing only the store-level Solidcore components from StoreNext, some key DSS areas are positively addressed.

One of the most important is DSS Section 5, which calls out the requirements for anti-virus software. Solidcore meets these requirements but also does so with lower "business risk" since some A-V program updates could, as has happened before, incapacitate the POS or other software applications because of incompatibility.

> A word of caution: some QSAs work for companies that have their own A-V or security products, and these QSAs may get commissions or a bonus when their company sells their own products (yes, sometimes the fox gets to watch the henhouse). We've run into occasional "stubborn" QSAs and this seems to be a common scenario. If the QSA is being unreasonable, make sure your grocer knows that there may be a conflict of interest and give them the information below to help them discuss the issue with the QSA.

Here is the full DSS Section 5 (A-V) with a line-by-line analysis.

"5.1 — Deploy anti-virus software on all systems commonly affected by viruses (particularly personal computers and servers)."

- ***This is the basic requirement that must be fulfilled.***

"5.1.1 — Ensure that anti-virus programs are capable of detecting, removing, and protecting against other forms of malicious software, including spyware and adware."

- ***"Detects"*** — Yes: Solidcore detects all viruses, Trojans, spyware, adware, code injections, SQL injections, denial-of-service, buffer overflows, Registry changes etc. It also detects industry-standard logging and monitoring tools that could be used to steal data during transmission. This is because Solidcore detects everything that is not authorized, and viruses etc. are obviously in that category.

- ***"Removes"*** — Yes: Solidcore does not allow any type of malware or any other unauthorized code to load, install, run or regenerate. It constantly monitors all operations and "removes" potential problems in advance before they can do anything. Most PCI auditors recognize this as far preferable to standard product that allow malware to install and only then tries to remove it – if the A-V in fact can even recognize it.
- ***"Protects"*** — Yes: Solidcore protects against all the forms listed, and all other software that's unauthorized. The protection offered is far superior to typical "recognize-and-chase" anti-virus, since these normal A-V products must know in advance that the malware is, indeed, malware. With breaches now being carried out using purpose-built data-theft software and standard PC utilities — neither of which will ever be caught by standard A-V — there are major risk in using A-V software that can only "fight the last war" and offers no protection against zero-day or breach-design code.

"5.2 — Ensure that all anti-virus mechanisms are current, actively running, and capable of generating audit logs."

- "***Current***" — Yes: The Solidcore design does not require daily downloads to keep up. Only the authorized software when the endpoint is "solidified" is allowed to run. Auditors should be reminded that PCs and POS terminals in a many stores seldom if ever get their A-V updated — maybe they are not connected to the Internet, subscriptions run out and no one notices or they're turned off because of performance or interruption problems, etc. This makes Solidcore much stronger in the "currency" requirement than any standard A-V product since it's always current – there's nothing to get out of date.
- ***"Actively running"*** — Yes. Once the endpoint is "solidified," you cannot turn it off, delete it from the tray, stop it with task manager, reboot without it etc. It requires the SYSAD password to stop it or add new software. (Upgrades of existing software using authorized updaters only can be done with a lower-level password.)
- ***"Audit logs"*** — Yes. Solidcore S3 logs all activity, attempted changes, loads and so forth in real time. All software program changes across the store or infrastructure are tracked including the Windows registry and network device configurations. Logs can be read by the Windows Event Viewer and forwarded to such systems as Netcool or MARs, or the Solidcore enterprise product can be purchased from Solidcore.

Regarding Section 6.1 (security updates)

- A strong case can be made that Solidcore provides a compensating control (CC) that significantly reduces a merchant's business risks and temporarily buys time to meet the letter of the DSS with certified and compatible software.
- Keep in mind that CCs always need to be evaluated in the context of the underlying risk in the specific environment, so some QSAs may judge that sometimes it may be a valid CC and sometimes not, and for varying lengths of time.
- Most QSAs balance a merchant's "business risk" against PCI risks. In the case of Windows security updates, it is not possible for software vendors to test the software prior to the automated updates. Even if the updates are not immediately installed, the 30 days provided by the DSS is insufficient time for a vendor to test and release new software, let alone to roll it out.
- Since it's possible that an incompatible O/S update could hobble the store's POS or other systems, QSAs will normally recognize Solidcore's security protection as a CC to temporarily stand in for the security updates. However, QSAs will want to see that the O/S updates actually do get applied within a reasonable time: Solidcore's compensation can delay the implementation but most QSAs will not judge that a CC ***removes*** the requirement.

Regarding Section 8 (passwords)

- As with 6.1 above, most QSAs will recognize Solidcore as a CC for the frequent changing of passwords, lowering the business hassle and cost of PCI-compliant management practices.

Especially for retail stores and the context of electronic payments, meeting Section 5 of the DSS with Solidcore is going to give your customers far better protection and with lower business risk.

If Solidcore is so great, why isn't it used everywhere and on everything?

Solidcore's extremely sophisticated S3 software technology means minimum impact on the installer or user — but it requires a lot more support and testing from StoreNext than a traditional A-V product.

The "positive" deploy-and-forget model means that StoreNext must certify and set up the Solidcore software image prior to installation based on the applications used across a wide variety of stores. That's a lot of effort, testing and certification, and this would be obviously impossible for general A-V's like Norton to manage this across the entire PC market.

Supermarket POS has key differences from "home-use" machines that make S3 practical. Home users are always adding and deleting software, freeware, Internet downloads and updates. Commercial POS users, on the other hand, seldom change their application set significantly after installation. Although software may be updated often, new software programs are seldom added.

This enables StoreNext to provide a Solidcore embedded product that will install quickly and easily when the dealer stages the system. StoreNext can also provide professional services for wholesalers and other application providers to ensure that their products operate properly and map any exceptions accordingly.

Solidcore S3 Implementation and "Solidification"

APPLICABILITY

A POS terminal, PC or Server running Solidcore is called "solidified" when the installation of S3 is complete on that individual piece of hardware. While Solidcore S3 is ***licensed*** on a store-by-store basis, it ***operates*** on a device-by-device basis – S3 is installed on each computer and supports that computer only.

Solidcore from StoreNext will license the complete store, including every PC or server that's in a store meeting the following conditions:

- ISS45 (V7 or V8, Windows components only) or ScanMaster V2 must be the store's POS product. Currently-supported POS versions will all support Solidcore.
- The PC or server in question must be an ISS45 or ScanMaster controller, WinEPS payments controller workstation or POS regardless of what other software is running on that box.

  Solidcore supports many operating systems and databases, but DOS is not among them. Applications such as ScanMaster V1 or ISS45 V7 DOS are not compatible with Solidcore.
- An ancillary machine to any of the above — for example, the U-Scan controller in a customer checkout station or attendant station — that is a controller, workstation or POS terminal will be licensed. Solidcore is controlled by the StoreNext software key – see Page 12.
- Stand-alone machines that are ***not*** controllers, workstations or POS terminals — even if they are attached to the same network – are not eligible under the POS license granted under StoreNext's Solidcore program. Stand-alone wholesaler ordering applications or other application processors would fall into this category. StoreNext now provides a special PIN for a license and key to handle these cases. See the Pricing and Configuration section below.
- Other StoreNext applications running in non-StoreNext POS stores — for example, Retalix Store operating in an IBM POS environment — are not eligil

But it doesn't hurt to ask. We may be able to negotiate exceptions in some cases.

THE SOLIDIFICATION PROCESS

Solidification of a system is a straightforward process. The technical details and methods to solidify a store are fully detailed in the Solidcore 101/102/103 webinar course sequence, the general process goes like this.

- During the staging process, load all the application software that is going to be operated on that machine. If all the software has been Certified, you have a virtual guarantee of no speed-bumps. If there are components, utilities or applications that have ***not*** been Certified, dealers should always test the solidification in advance prior to final staging.
- Load the Solidcore application — this automatically runs the "Scanalyzer" which further checks the machine and builds an inventory of applications with a fully automatic discovery of all software on the machine to be solidified.
  - This assumes that all the application software was loaded onto a clean machine from scratch, and from original or malware-free media. If not, this is where a virus checker should be run first to make sure you don't solidify bad code.
  - Also load the StoreNext Exception Files, which contain special instructions to ensure that Solidcore gracefully handles some specific complex executables and routines.
- Then run the Solidcore solidification routine — this performs a complete pre-computation of system data and establishes automatic code admission control.

These operations create Solidcore's set of system expectations up-front and that's why it has such a tiny footprint at run-time.

- This takes about 20 minutes. Multiple machines can be solidified in parallel.

➢ You now switch S3 into the locked mode – called "enabling" S3. Unless S3 is "disabled" by an authorized person, no new applications or executables will be allowed to run. The existing applications can be updated by the "authorized change agents" – software programs such as code distribution – that are part of the solidification process and therefore authorized to change and update their own applications.

➢ To add a new application later, a technician, manager or other authorized person puts the Solidcore S3 application into an "update" mode where Solid [illegible] new application to be put onto the protected machine.

It takes training, system knowledge and password authorization to run this update mode.

➢ Of course, no viruses or other unauthorized software will be allowed to load and execute with S3 enabled. However, it ***is*** possible that a bad file or an Internet-borne virus could have ended up on the machine. If it's sophisticated enough, such an executable could have been trying to boot up but has been blocked by Solidcore.

- This is why — before you solidify — you should scan the system for viruses using the best and most current anti-virus program you can find. Then, either remove that A-V program or shut it off, and turn Solidcore back on. This way S3 will re-solidify the store from scratch without authorizing any possible lurking malware.

The Solidcore Program from StoreNext

Solidcore is implemented as follows with StoreNext products. See the Solidcore All-In-One Page on the StoreNext Dealer Support Web site.

THE STORENEXT S3 IMAGE

StoreNext has built a Solidcore "StoreNext Image." Creating this image completed all the hard work required to implement S3 in stores with all StoreNext software products. This process required exhaustive testing of all StoreNext software and the creation of the ancillary files required to ensure that dealers can install Solidcore S3 to plug-and-play with any combination of StoreNext systems in the store.

➢ StoreNext will distribute the StoreNext Image on a CD to all dealers in good standing who have been Authorized under StoreNext's training (see Education and Training below). Dealers who have not completed StoreNext training will not receive Solidcore software or have lab, demo or customer keys enabled for the Solidcore license until training is completed. Authorization requires the live training sequence via webinar.

➢ The StoreNext Image is unique and will handle stores with StoreNext ScanMaster and ISS45 systems including additional StoreNext applications (RBO, PocketOffice, U-Scan, ESL etc.) and most third-party software products in that store. The StoreNext Solidcore Image ***will not operate*** in non-StoreNext POS stores, and non-StoreNext S3 images will not operate in StoreNext stores.

➢ The StoreNext Solidcore S3 image requires that Solidcore is authorized on the ISS45 or ScanMaster POS software key. See the Configuring and Ordering section below for licensing and pricing information.

EDUCATION AND TRAINING

StoreNext has prepared and already presented a series of WebEx presentations (Solidcore 101, 102 and 103) specifically for dealers, enabling support personnel to operate Solidcore and manage Solidcore-solidified systems.

The first sets of these courses were provided at no charge. The series of Solidcore 101, 102 and 103 will be repeated to dealers via webinar under StoreNext's course catalog as a professional service pending schedule availability. The fee for the series of courses is $495 per dealership. There will be some lead time required, so please contact Jeff Galing at StoreNext as soon as possible to schedule additional classes.

End-user customers can also receive Solidcore 101, 102 and 103 from StoreNext if requested by the dealer. The customer fee is $995 per customer (company-wide) for the three sessions. Again, please contact Jeff Galing at StoreNext to arrange a schedule for such classes.

TECHNICAL DOCUMENTATION

Solidcore S3 documentation is provided — including installation and operations guides, administrator's manuals and so forth — from the StoreNext Dealer Support Web site.

StoreNext also provides application-specific process documentation and instructions for solidification.

Additional documentation – such as white papers – are also be available to dealers.

Additional technical documentation, including Technical Bulletins, will continue to be provided as appropriate.

SALES MATERIALS

StoreNext provide several presentations, information sheets, press releases, case studies and white papers to assist understanding and sales campaigns with Solidcore.

TECHNICAL SUPPORT

Consistent with POS software, dealers are responsible for Solidcore Level 1 (Help Desk) and Level 2 support. The Solidcore 101, 102 and 103 courses qualify a dealer support person to perform these support levels.

StoreNext takes Level 3 and Level 4 responsibility. Solidcore support will be available from the same StoreNext 800 support line used with all other products.

StoreNext's technical support of Solidcore works as follows:

- StoreNext will provide Level 3/4 support for Solidcore using StoreNext's standard 800 Support line.
- There is no additional software maintenance and support charge to dealers for Solidcore support. Solidcore SMS is provided as part of a dealer's ISS45 and ScanMaster SMS.
- StoreNext Solidcore technical support will take calls from Solidcore-authorized dealer personnel only.
  - Questions from dealer personnel who have not taken StoreNext's Solidcore webinar courses should consult with the authorized personnel at the dealership.
  - Dealerships that do not have any authorized personnel need to take the Solidcore courses (about half a day in total) via webinar from StoreNext. Please contact Jeff Galing at StoreNext to schedule additional classes.
- StoreNext Level 3/4 support will handle questions and issues regarding Solidcore installation, solidification, operation and maintenance related to StoreNext-distributed products on the StoreNext Solidcore S3 image.

There is no additional software maintenance and support charge to dealers for Solidcore support. Solidcore SMS is provided with ISS45 and ScanMaster SMS.

See the current issue of Reference Bulletin 1060 for the definitions of the various levels of support and the services offered.

- Support questions regarding dealer-created utilities and products will be provided by StoreNext Systems Engineers. See the Certification information below.
- Support questions regarding major third-party applications and products — whether certified or not certified — must be referred to the vendor of those products, who must work directly with StoreNext to resolve any issues or receive the necessary Certification. See the Certification information below.

SOLIDCORE CERTIFICATION OF DEALER AND THIRD-PARTY PRODUCTS

- ***Dealer Products —*** Solidcore-authorized Dealers requiring support regarding dealer-created hooks, utilities or applications should call your StoreNext Systems Engineer for assistance. StoreNext will work with the dealer if necessary to ensure the dealer programs will solidify, and will also add the dealer products to the StoreNext S3 Image if required. This assistance from StoreNext Systems Engineers will constitute a Professional Services engagement and standard charges will apply.
- ***Third-Party Products —*** StoreNext wants the benefits of Solidcore to be available to StoreNext grocers regardless of their application selection beyond their use of ISS45 and ScanMaster. Dealers and vendors wishing to operate third-party software applications (for example, BRdata) on a solidified StoreNext platform should contact Heather Blanarik to arrange a formal Certification Program for that product.
  - Certification engagements for third-party software will take place at a StoreNext Lab location, and the product will be thoroughly tested by a combination of StoreNext and vendor personnel to ensure that the product installs and solidify properly.
  - Special exception files will be created if necessary, and the product will be added to the StoreNext Image.
  - The product will receive a formal StoreNext Solidcore Certification which will be logged on the StoreNext Web site for reference. As with other interfaces and utilities, the vendor will thereafter be responsible to ensure ongoing testing of their new releases and updates. The vendor will receive the necessary software, files and keys to carry out all such testing.
  - Certified vendors will work with StoreNext to resolve ongoing questions and issues in the same manner in which these same vendors work with StoreNext today to maintain interfaces and integration consistency.
  - A standard flat Certification fee of $10,000 will apply per application for the above effort, status development and services. Travel costs, if applicable, will use StoreNext's $300 per day flat rate with a minimum of two days.

Most wholesalers have their own applications and application suites that they have created or otherwise sell, recommend, or promote. File maintenance, ordering applications, shelf audit or communications products are common. StoreNext will treat and support these products in the same manner as described here for third-party products, although it is more likely that they will be carried out at the wholesaler site.

Pricing and Configuration

Solidcore S3 is licensed on a store-by-store basis. It can only be licensed in stores with ISS45 or ScanMaster, but it covers all controllers, POS terminals and workstations in the store that are part of the POS system. Stand-alone boxes are not included if they are not an ISS45 or ScanMaster workstation, and can be licensed separately. The "Applicability" section on Page 8 above describes the licenses and limits.

LICENSING

Delivery of software keys to enable Solidcore licenses will continue to be via Authorized dealers only. Dealers who are not yet authorized for Solidcore (by attending the Solidcore webinar classes) can receive software and key upgrades for labs, demos and customers upon completing authorization.

ISS45 and StoreNext ScanMaster stores can be ordered or upgraded to include Solidcore.

- Stores must be on a StoreNext V2 version of ScanMaster. Solidcore is not compatible with ScanMaster V1, and Solidcore will not be Certified or licensed over non-StoreNext ScanMaster loads.
- Solidcore is compatible with currently-supported ISS45 V7 and V8 loads, and currently-supported ScanMaster V2 loads.
- Solidcore is controlled by the ISS45 or ScanMaster software control key (HASP plug). If the key doesn't have Solidcore on it, Solidcore will not install or execute. Solidcore upgrade orders need an accompanying SKIF.
- Solidcore normally installs and operates only on POS system components, including POS terminals, controller/servers, WinEPS machines (if separate) and workstations.
- For standard use with ScanMaster V2 or ISS45 V7 or V8, use PIN SCS3UG below. Use this for either new systems or upgrading existing ScanMaster or ISS45 systems.
- For "stand-alone" PCs or servers in the stores (for example, wholesaler boxes or other application processors) use the SCS3US PIN, which provides a software key that enables S3 to run on a non-system "stand-alone" box. This separate PIN for stand-alone boxes is required where needed for both new and upgrade orders where Solidcore is included.

Solidcore is likely to be compatible with older Windows-compatible versions of ISS45 or ScanMaster too, but these installations are not officially supported and StoreNext cannot provide support on these loads. Dealers are invited to try, but understand that you're on your own.

To add Solidcore to new or existing ISS45 or ScanMaster systems, order:

PIN	Item	Price	Inst	Maint
SCS3UG	Solidcore/McAfee S3 Embedded for ISS45 and StoreNext ScanMaster	$ 495	$ 100	$ 50

The StoreNext Platform Discount applies.

To handle "stand-alone" boxes (not part of the POS system or WinEPS, but used in a site where SCS3UG is ordered on the same P.O.) order one of the following PIN for each stand-alone PC or server to be solidified.

PIN	Item	Price	Inst	Maint
SCS3US	Solidcore S3 Stand-Alone License and Key — one unit when used with Solidcore on POS This PIN may be used only in cases where Solidcore S3 Embedded (SCS3UG) is ordered on the same P.O. for the same site. For use only on -stand-alone- PCs that are not formal components of the ISS45 or ScanMaster POS system (that is, not a POS, Controller or Workstation or WinEPS box). This PIN is to be used in cases where a PC or server in the store may be networked to a POS component (or not) but is not part of the POS system itself. This PIN ships with a software key which enables Solidcore S3 to install and operate on that PC/server only. Order one unit per stand-alone PC or server in the store.	$ 110	$ 35	$ 50

The StoreNext Platform Discount applies.

Where "stand-alone" boxes are to be solidified — but where SCS3UG is ***not*** ordered on the same P.O. — order one of the following PIN for each stand-alone PC or server to be solidified.

PIN	Item	Price	Inst	Maint
SCS3USN	Solidcore S3 Stand-Alone License and Key — one unit This PIN may be used in all cases, including where Solidcore S3 Embedded (SCS3UG) is not ordered on the same P.O. or for the same site. For use only on -stand-alone- PCs that are not formal components of the ISS45 or ScanMaster POS system (that is, not a POS, Controller or Workstation or WinEPS box). This PIN is to be used in cases where a PC or server in the store may be networked to a POS component (or not) but is not part of the POS system itself. This PIN ships with a software key which enables Solidcore S3 to install and operate on that PC/server only. Order one unit per stand-alone PC or server in the store.	$ 225	$ 35	$ 50

The StoreNext Platform Discount applies.

PROFESSIONAL SERVICES

PIN	Item	Price	Inst	Maint
SNPS-PS	Solidcore S3 Certification Engagement for Third-Party Software Applications Flat rate, assumes certification carried out in StoreNext lab with vendor subject matter expert personnel. StoreNext will negotiate traveling to third party location at extra cost for time at $1,750 per day travel time minimum one (1) day and $300 per day flat rate travel expenses with a minimum of two (2) days.	$ 10,000	N/A	N/A
SNPS-PS	Solidcore S3 Certification of Dealer or Customer Systems Per day, travel expenses will be added at $300 flat rate per day with a minimum of two (2) days.	As Quoted	N/A	N/A
SNPS-TNG	Solidcore 101, 102 and 103 Webinar course set for dealer support audience Approximately one-half (½) day cumulative time required	495	N/A	N/A
SNPS-TNG	Solidcore 101, 102 and 103 Webinar course set for customer audience Approximately one-half (½) day cumulative time required	995	N/A	N/A

Discounts do not apply to Professional Services items.

Questions and Answers

BIG-PICTURE QUESTIONS

Is there one place I can go for Solidcore information? — Yes: the Solidcore All-In-One Page on the StoreNext Dealer Support Web site of course!

Why is StoreNext making a big deal of Solidcore? — Malware risk and PCI compliance makes it necessary for grocers to establish system protection and control. Solidcore is by far the best answer, with the greatest benefits. In fact, we think it's so important to the grocery business that we're giving it away on new ISS45 and ScanMaster systems.

How do dealers get paid for providing and supporting it? — Dealers sell Solidcore for new systems and as upgrades to the installed base. Dealers can also charge for Solidcore maintenance.

Is it cheaper for the customer to buy typical anti-virus programs? — No. First, it's typically less expensive to buy a Solidcore license. More important, you don't need to pay the annual subscriptions to the download service, which equal or exceed the acquisition cost. Besides, Solidcore's deploy-and-forget is more secure and far more practical for grocers.

If they already have A-V, how do I convince them they need Solidcore? — Performance, real security and practicality. All that stuff on Page 3.

Why do you call it "change control"? — Solidcore change control goes way, way beyond malware protection. Controlling the software and software changes in a store brings much more than just A-V, since the full logging capability enables dealers to figure out exactly what changes were made in the store and when. This is a critically important diagnostic tool for support.

I'm worried – what happens if suddenly Solidcore won't let one of the applications run? — The solidification process makes this essentially impossible. Besides, of course, you can always switch off S3 in some unforeseen emergency. Solidcore has now run with ISS45 and ScanMaster stores for more than two years without any such difficulties.

Okay, but isn't it just adding a layer of risk? — Completely the opposite! The really big risks are (1) a zero-day threat that beats your A-V to the punch or (2) that your A-V itself downloads an anti-virus change that cripples your application (this has happened to POS).

What does Solidcore have to do with PCI compliance? — Using S3 enables the grocer to meet some of the most important PCI requirements. This is a long topic, but make sure you see the discussion starting on Page 5 of some of the most important aspects of PCI and Solidcore. Also see the Solidcore PCI presentation and PCI white paper that deals with this topic in detail on the StoreNext Web site.

It looks like I have to learn stuff, and do new things. What are the advantages for a dealer? — Solidcore with ScanMaster or ISS45 gives you a huge leg up on your competition: we know of no other POS systems offering Solidcore compatibility or handling these risks. Furthermore, wholesalers and payments processors are demanding PCI compliance and change control protection: your solution is way ahead of anyone else's.

Okay, what else? — Once your customers experience the smooth operation and performance increases of a solidified system, plus the security advantages, dealers will profit by upgrade sales.

More? — Another major advantage is the lock-down of customer sites. You won't have to go out to your stores periodically and clean out all the gunk that shows up on these systems, or diagnose mysterious intermittent problems, or rebuild systems in the middle of the night. Store staff can't add unauthorized software that screws up the system – and if they do, S3's control logging will tell you what, when and where so you can back out the right stuff.

GETTING SOLIDCORE

How do I get authorized? — You attend the Solidcore 101, 102 and 103 webinar courses.

Why do I have to take the class? — Dealers have to be able to perform Level 1 and Level 2 Solidcore support, and that takes a little education.

I missed the classes! How do I get authorized now? — Please contact Jeff Galing at StoreNext to schedule a Solidcore class for you and your dealership.

What about my customers? If I'm not authorized yet, can they get Solidcore with their new ISS45 and ScanMaster systems? — The sooner the dealer is authorized, the sooner the dealer's customers can get Solidcore.

It looks like what you are saying is that until I'm authorized, I'm not going to get software, demo keys or even access for my customers! — That's true.

Once I get authorized, then how do I get my software? — Just ask.

SOFTWARE KEYS

Is Solidcore protected by the ScanMaster or ISS45 software key? — Yes. The StoreNext version of Solidcore won't run without unless the key has been set.

How can that work on the POS terminal since there's no software key on the terminal? — The presence of the software key on the controller is communicated to Solidcore's application running on the terminal. The same is true for workstations – they don't need the key on the box itself, just on the POS system.

What if I have a stand-alone PC that's not connected to the POS in the store. Can I use Solidcore on that box too? — StoreNext's Solidcore protection extends to the controllers, workstations, WinEPS boxes and POS terminals. It won't work on stand-alone boxes in the store, unless…

Unless what? Unless you order the PIN that's been released to handle such stand-alone boxes. See the pricing and configuration section above. This PIN supplies the license and a special key to operate Solidcore S3 on a "non-POS system" box in a store.

Could I plug a key in and solidify the box and then remove the key? — That's clever, but Solidcore checks periodically for the key, and if it's not there it will drive an automated reboot of the PC or server which will then come up normally but without Solidcore running.

CERTIFICATION AND THIRD PARTIES

I'm not quite clear on this Certification thing. Let's say I've got a lot of customers who use the XYZ product on their POS controller: will it be able to run over S3? — Every product should be able to run fine with Solidcore, including XYZ. But XYZ needs to be Certified by XYZ in cooperation with StoreNext to ensure that XYZ will always solidify properly when Solidcore is installed.

What if XYZ isn't Certified? Will it solidify and run? — Maybe it'll run fine, maybe not. Maybe it'll install fine but not run right. To take the risk out of mission-critical applications, it's important to have XYZ and StoreNext Certify them. This will add any special instructions or files to the Solidcore installation program that XYZ needs to solidify and run properly.

If XYZ needs special install instructions, how will they get out to the dealers and customers? — StoreNext will add any special handling for XYZ into the StoreNext Solidcore image and the current image will always be available to dealers on the StoreNext Dealer Support Web site.

It looks like StoreNext is going to make XYZ pay a fee to get Certified. Is that a good deal for XYZ? — It's a great deal for XYZ: their own application will be fully protected by Solidcore without XYZ having to buy any licenses. We're paying the freight.

How will XYZ stay Certified? Will StoreNext make them re-certify every time XYZ comes out with a new version? — StoreNext will provide lab loads and software keys for XYZ so they can check new versions themselves. StoreNext will help XYZ in the future if additional support is required.

What about the wholesaler – they've got an inventory application that runs on the controller. — StoreNext will work with wholesalers the same way StoreNext works with third-party software vendors to make sure all the wholesaler's applications solidify with no problems.

We've got some special utilities and programs we put on every store. Will they solidify right? — Authorized Solidcore dealers should usually be able to test such applications and utilities themselves without a formal certification process from StoreNext. StoreNext's SEs are available to help dealers solidify their own applications as necessary. StoreNext will also add any applications that need special handling to the StoreNext Solidcore image.

THE ENVIRONMENT

What's the point of A-V software if you already have Solidcore? — A good anti-virus scanning program should be used before solidifying a machine. That way you won't solidify malware along with the good stuff.

If the customer already has A-V on the machine, what should you do? — The best advice is to leave it there for occasions where you are adding an application and will be disabling and re-solidifying the machine.

But didn't you say that having anti-virus on the machine would slow it down and consume the CPU? — Yes – leave it on the machine, but turn it off.

It looks to me like network security products such as SonicWall are more complementary than competitive with Solidcore. Should we consider them as part of a solution where an enterprise is being considered? — Yes, this is a good example of a complementary product. Solidcore handles the threats on the machines, prohibits the zero day exploits, protection against known/unknown OS and application vulnerabilities and manages internal threats (hardware-based solutions cannot provide this). Meanwhile, SonicWall provides network security, content management with web filtering, e-mail security, secure remote access and continuous data protection solutions. These are essentially protections of threats in an enterprise network, and are complementary to Solidcore's solutions.

I hear that Microsoft Windows Vista has such great new security features that virus protection won't be needed anymore. So isn't Solidcore just a short-term solution? — With luck, Vista's additional resistance to malware (or with Windows 7) will turn out to work well and be a benefit to us all. But what Vista brings to the table is no substitute for true change control, management and reporting.

Can you be more specific? — If you remember the kinds of threats discussed on the first page of this bulletin, Vista will hopefully make progress against (1) traditional threats and maybe even some (2) emerging threats. But it is very unlikely to bring end-to-end protection against (3) internal threats, zero-day malware, custom malware or resolve (4) the business costs and risks involved.