

Secure Networks form the Backbone of Profitable Retail Initiatives

Leveraging technology to improve internal operations, dealings with suppliers and customer service.

CONTENTS

Abstract	2
The Case for Connectivity	2
Profits Out of Thin Air	3
From POS to Point-of-Profits	3
PCI Standards on the Path to Profits	4
Security Made Simple	5
SonicWALL Solutions for Retail	6
Summary	7

Abstract:

The retail environment has never been tougher. While competitive pressures hold prices down, there is no corresponding relief for costs. The best path to lowering operating costs is capital investment in IT infrastructure.

Retailers may try to compete on customer service. But infrastructure is increasingly required to keep that promise too. A study by Alliance Data Systems of consumer attitudes shows the top four influencers of shopping preference as: Reasonable prices (86%); Quality merchandise (68%); Handles returns fairly (65%); and "I can always find what I want" (64%). Information systems have a direct influence on each of these criteria. Beyond their effect on pricing, electronic connections allow retailers to more efficiently manage multiple suppliers to assure consistent quality of goods. Access to databases enables smooth handling of returns. And the electronic underpinnings of a supply chain are essential to guard against out-of-stocks.

In short, to increase revenues, retailers must leverage technology to enhance customer service by improving communications and tightening supply chain, while reducing costs by streamlining internal operations.

An information network built on secure infrastructure and maintained securely is the necessary backbone for these capabilities.

The significance of security in the provisioning of data systems has now been underscored by adoption of the Payment Card Industry (PCI) Data Security Standard. This initiative by all major credit card issuers is aimed at reducing the billions of dollars in fraud and theft perpetrated annually. While each member bank will determine the compliance process and penalties for its customers, the potential assessment of damages and dramatically higher fees are a threat to any retailer's bottom line.

The good news is that the same secure systems that satisfy PCI standards are the basis for increasing operational efficiencies and improving customer satisfaction. And those are the keys to profitability.

The Case for Connectivity

It is easier to move information than it is to move goods. The more information you can securely move between locations, warehouses, logistics, suppliers, payment systems and customers, the lower the cost of sales will be...and the easier it will be to make sales.

Consider this case history for one of New Zealand's made-to-order retailer furniture stores. It has achieved 100% growth in the past four years thanks to the company's investment in a highly secure, scalable VPN which connects its 12 nationwide stores to the head office. The financial controller for the company says that as a result of changing the way his employees go about their daily tasks the company has increased productivity, achieved major efficiencies and reduced the overall cost of sales. He believes that, branch by branch, the company is making more money than ever before with an increase in profits of 180%.

Its experience highlights many of the benefits of a secure network:

- More effective management through greater visibility into operations and centralized data resources
- Improved customer satisfaction through faster and more accurate order entry, access to account history regardless of location and simplified order tracking
- Reduced costs through elimination of redundant data entry and automation of administrative tasks
- Improved inventory management through supply chain visibility
- Increased same store sales by reducing the number of out-of-stocks, facilitating cross-location inventory availabilities and enabling execution of promotions
- Increased employee productivity through faster access to customer and order information and quicker transaction processing

- Improved employee effectiveness and reduced training costs by simplifying inventory look-up, transaction processing, and order entry and tracking

These benefits are multiplied for chain stores and multiple unit ownership (MUO) operations. Not only does this make it easier to expand but it lowers the cost of sales, store by store and overall.

Profits Out of Thin Air

When you think of a secure network, you might not think of the wireless component. But the wireless segment can be secured as tightly as a wire line. But without those wires, whole new categories of cost savings and improved customer satisfaction are possible.

Of course, the obvious savings from a wireless network are decreased wiring costs. New locations can be built out quickly and less expensively. Reconfigurations can also be performed faster.

With a wireless hand-held bar code scanner as the input device, shipping and receiving can process orders faster and more accurately. Inventory can be conducted the same way, virtually eliminating the sales lost when you are closed for the process. In the hands of sales staff, the scanners can increase customer service and loyalty by instantly getting pricing information or checking inventory for alternative colors or sizes.

With the arrival of radio frequency identification (RFID), wireless inventory management is becoming faster and easier. RFID virtually eliminates the need to manually scan a SKU or even a pallet. And it gives real-time accuracy of inventory status, dramatically lowering the related costs. Because RFID is, by its nature, a wireless technology, the sooner retailers build out the wireless segment of their network, the better able they will be to compete.

By cutting costs, improving customer service and enabling more precise and better informed management, a secure wireless implementation can have a positive and considerable impact on profits.

From POS to Point-of-Profit

Perhaps the biggest transformation in retailing has been the concept of the point-of-sale. The POS long ago evolved from a cash register into the most critical information input device in the store.

Product mix, inventory, cash flow, customer identities, promotional performance and more are captured in hard numbers at the POS. But to take full advantage of this crucial information, retailers need to connect POS systems to all their other information systems such as financials and logistics. This has been made relatively easy and inexpensive using conventional broadband connections to the Internet. In fact, formidable retailers such as Ace Hardware make use of Virtual Private Networks (VPNs) over the Internet to connect all the members of their cooperative. Secure broadband and VPNs offer a number of benefits, including:

- Reduced infrastructure costs while increasing bandwidth
- Centralized management of credit card transactions for a significant reduction in fees and speed through checkout lines
- Increased revenue with gift card and loyalty programs
- Reduced deployment costs

The lower costs of networking solutions like this—in combination with the increased efficiency and operational control they provide—translate directly into greater profitability and help level the competitive playing field.

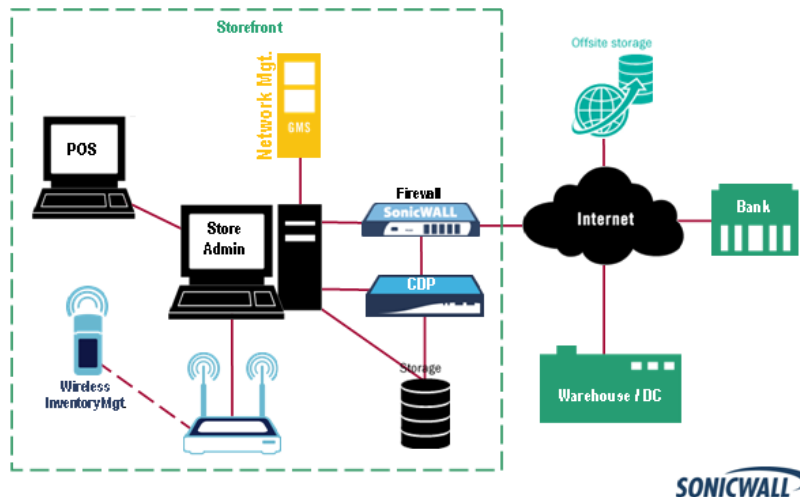


Figure 1. A Typical Retail Implementation

PCI Standards on the Path to Profits

It is estimated that credit card fraud costs issuing banks several billion dollars each year; the exact numbers are a sensitive and closely held secret. As more credit card numbers are stored in data systems, the potential for large-scale fraud has increased. To address this vulnerability, a consortium of virtually all credit card issuers has implemented the PCI (Payment Card Industry) Data Security Standard for the processing, storage and transmission of cardholder information.

The elements of the standard are practical and straightforward:

- Build and maintain a secure network
 - Install and maintain a firewall configuration to protect data
 - Do not use vendor-supplied defaults for system passwords and other security parameters
- Protect cardholder data
 - Protect stored data from theft
 - Encrypt transmission of cardholder data and sensitive information across public networks
- Maintain a vulnerability management program
 - Use and regularly update anti-virus software
 - Develop and maintain secure systems and applications
- Implement strong access control measures
 - Restrict access to data by business need-to-know
 - Assign a unique ID to each person with computer access
 - Restrict physical access to cardholder information
- Regularly monitor and test networks
 - Track and monitor all access to network resources and cardholder data
 - Regularly test security systems and processes

- Maintain an information security policy
 - Maintain a policy that addresses information security

Target dates for compliance have been set according to the size of the merchant; larger merchants must comply sooner than smaller ones. PCI does not penalize merchants for non-compliance. Instead, they can levy charges of up to \$500,000 against the issuers (banks) in the event of the loss of cardholder data. The issuers, in turn, must deal with the retailers with whom they hold the merchant account. While each bank is free to set its own penalty structure as it deems appropriate, potential fines on the order of \$100,000 are not uncommon. In the event of the loss of cardholder data, it is also possible for a merchant to lose their ability to process credit cards altogether. The impact this could have on profits is obvious.

Fortunately, many of the technical requirements of PCI can be satisfied by properly maintained secure network equipment with standard management tools and anti-virus/anti-spyware subscriptions.

Security Made Simple

While new technology such as wireless and broadband increase revenue opportunities, they open the door to new and more sophisticated threats. Network security is not an additional issue in building out a network. Instead of viewing secure technology as simply just another line item expense, retailers must recognize it as an integral investment in ongoing profitability, underlying all their business initiatives.

Given the high turnover of retail staff and minimal training time available, network security must account for users of all kinds—technologically sophisticated and not. It must be able to securely protect, transport and backup two categories of information: shared information like inventory and customer orders and protected information like customer account details and business financial data. SonicWALL engineers solutions that drive the cost and complexity out of running secure high-performance retail networks, freeing resources to increase productivity and enhance customer satisfaction.

Global Management

The award-winning SonicWALL® Global Management System (GMS) provides retailers, distributed stores and POS branches with a flexible, powerful and intuitive solution to centrally manage and rapidly deploy SonicWALL appliances and security policy configurations. SonicWALL GMS™ also provides centralized real-time monitoring, comprehensive policy and compliance reporting across all MUO and retailer environments.

Unified Threat Management (UTM)

Between front office, back office or beyond, a retailer needs connectivity to be efficient, and that connectivity must be secured to protect the information and keep customer data safe and secure. SonicWALL offers retail environments real-time detection and protection through a suite of Unified Threat Management (UTM) services, including gateway anti-virus, anti-spyware, intrusion prevention, anti-spam, and content filtering. This solution flushes out both internal and external threats by addressing multiple threat access points and thoroughly scanning all network layers.

Secure Remote Access (SRA)

Secure remote access is how chains or MUOs connect to one another. Customers, partners and suppliers need policy-defined access to your business resources from potentially anywhere. Uncertainties and disasters can threaten network access and disrupt business. Easily deployed over the Web, SonicWALL SSL VPN solutions require no pre-installed client software. SonicWALL SSL VPN solutions have no restrictions on the number of concurrent users, allowing organizations to scale their remote access connectivity as they grow.

Continuous Data Protection (CDP)

Unexpected downtime and lost data can be very costly, even driving retailers out of business. Regulatory and compliance obligations now demand stricter control over service and data availability and security. SonicWALL continuous data protection provides end-to-end data protection for any retailer, including

individual locations in a chain or MUO set-up. The disk-based solution allows administrators to instantly recover data themselves with the touch of a button, so there's no down time or loss of productivity. CDP eases administration by eliminating the need for data to be manually transported to multiple locations.

SonicWALL Solutions for Retail

SonicWALL products and services enable networking with a focus on security. They are not supplemental, but central in a secure, high-speed network. Because of SonicWALL's long-term focus on smaller and medium sized businesses, their price/performance advantages are ideal for most retailers who need to gear up for profitability without crippling capital investments.

Global Management System (GMS)

SonicWALL GMS eases administration and helps meet regulatory compliance by providing flexible, powerful and intuitive tools to manage a few up to thousands of remote SonicWALL network security appliances, all from a central location. GMS provides flexible, powerful and intuitive tools to manage a few up to thousands of remote SonicWALL network security appliances, all from a central location.

TZ Series - Remote Connectivity and Protection

SonicWALL's complete line of integrated wired and wireless solutions makes it easy to add secure wireless into an existing network infrastructure or to create a new wireless network from the ground up.

PRO, NSA and E-Class NSA Series - Central Data Communications Hubs

Designed to increase security by reducing complexity, SonicWALL network security appliances eliminate the cost and complexity of installing and managing separate devices and software packages for comprehensive security.

Gateway Anti-Virus, Anti-Spyware and Intrusion Protection Service

This unique solution features a high-performance deep packet inspection engine that delivers threat protection directly on the security gateway by matching downloaded, e-mailed and compressed files against an extensive signature database.

Content Filtering Service (CFS)

CFS Standard and Premium Editions feature a powerful rating and caching architecture that leverages a database of millions of continuously updated Web sites to eliminate non-productive or even potentially harmful use of the Internet.

SSL VPN and E-Class Aventail SSL VPN

SonicWALL Secure Remote Access solutions for remote access and Virtual Assist clientless remote support extends your marketplace to any location, empowering outsource, affiliate, contract, supplier and channel partnerships, as well as providing business systems continuity during disaster recovery.

Secure Wireless

SonicWALL SonicPoints in conjunction with E-Class NSA, NSA, PRO, and TZ appliances empower leading edge initiatives in mobile POS, inventory tracking, and interactive marketing, while offering the security of 3G failover should standard broadband connections go down.

Anti-Spam/Email Security

SonicWALL Anti-Spam/Email Security solutions keep retail business communications running fluidly and effectively without getting bogged down in spam, and protects against inappropriate content being sent into or out of your organization.

Continuous Data Protection (CDP)

CDP provides data back-up and protection without tapes or disks to manage. It includes simple, centralized administration.

Your information systems solutions provider can help you choose the equipment and services ideal for your business needs, physical location(s) and budget.

Summary

As competitive pressures mount for retailers, profitability can seem like a distant dream. But the arrival of cost-effective, easy-to-manage and easy-to-maintain information networks can level the playing field. Such a network can enable efficiencies across the supply chain, inside operations, and even in service delivery. At the same time, such technology can enable improved customer service. This, in turn, can lift sales.

By cutting costs and improving sales, retailers can bolster profitability from both sides of the equation. Since credit card companies are requiring a comprehensive addressing of information systems, there is no more ideal time to consider how a new or revamped network can serve your larger business goals.

As a relentless innovator in the secure infrastructure market, SonicWALL is committed to improving the performance and productivity of retail businesses by engineering the cost out of building and running secure networks. With cost-effective and practical solutions from SonicWALL, retailers can positively influence their bottom line today and stage themselves for future growth.