



## Retail: Securing the Competitive Edge with Technology

*A comprehensive approach to securing retail  
technology from sophisticated threats.*

### CONTENTS

Gaining Advantages of Retail Technology	2
- Gaining a technology edge in cost reduction	
- Gaining a technology edge in revenues	
- Gaining a technology edge in customer relationships	
Securing the Competitive Edge	3
- PCI Compliance	
- Unified Threat Management	
- Clean VPN	
The SonicWALL Solution	6
Conclusion	7

## Abstract

In today's global marketplace, retail is more competitive than ever. The effective application of technology can cut the costs of doing business, open revenue opportunities, enhance customer service and widen profit margins, giving retailers a significant edge over their competition. However, if unsecured, this same technology can potentially expose retailers to loss of data, customers, revenues and reputation. A comprehensive approach to securing retail technology would enforce centrally-managed, policy-based controls over the entire retail network, including intranet, extranet and Internet traffic. Optimally, a retail security solution should cost-effectively protect retail transactions, supply chain processes, business data integration, intellectual property and mission-critical resources, thereby freeing retailers to safely leverage technology for optimal profitability.

# Competitive Advantages of Retail Technology

Retailers who take the greatest advantage of evolving technology stand to gain an edge over their competition through cutting costs, increasing revenue opportunities and being more responsive to their customers' needs.

## Gaining a technology edge in cost reduction

Emerging technologies have transformed inventory and supply chain automation. For example, radio-frequency identification (RFID) has revolutionized warehouse management and store replenishment by eliminating errors, reducing labor costs, and streamlining processes. In a recent study conducted at the University of Arkansas<sup>1</sup>, the retail application of RFID technology resulted in a 30% reduction in out-of-stocks. High-frequency RFID is extensively replacing barcode technology for tracking such items as jewelry, books, apparel and pharmaceuticals, while ultra-high frequency RFID is being applied to tracking case, pallet and shipping container information to enhance warehouse and transport management.

Similarly, supply intelligence technology, such as supply chain management software (SCMS) integrated over virtual private networks (VPNs), has greatly improved the cost-efficient transfer of goods by enabling analytical supply chain data to be shared over the Internet between producers, wholesalers, distributors and retailers. Such collaborative data helps produce more accurate sales and replenishments forecasts, resulting in significantly reduced inventory costs.

The ease of deploying, using and managing these new technologies also contribute significantly to overall cost reduction by optimizing the utilization of workforce resources to enhance productivity.

## Gaining a technology edge in revenues

Going forward, retailers will increasingly require the centralization and integration of demand intelligence technology<sup>2</sup> in order to forecast demand accurately and maintain an appropriate category mix. The effective gathering and sharing of demand intelligence information will continue to be largely dependent upon point-of-sale (POS) data retrieval and systems integration. Formidable retailers such as Ace Hardware make use of virtual private networks (VPNs) over the Internet to connect all the members of their cooperative. However, as POS becomes further virtualized both in the store and on the Web, evolving technology will be critical in leveraging new methods of gathering and sharing demand intelligence to improve revenues.

---

<sup>1</sup> B.C. Hardgrave, M. Waller, R. Miller, *RFID's Impact on Out of Stocks: A Sales Velocity Analysis*, University of Arkansas (2006), Ref. No. ITRI-WP068-0606

<sup>2</sup> *Worldwide Retail Industry 2008 Top 10 Predictions*, Doc. No. GRI210285, Global Retail Insights, an IDC company.

Retailers will also find competitive advantage in revenue generation through applying VPN technology to collaborative merchandising by integrating with partner and sales channel information systems. Planning for global capacity in technology infrastructures will also be a necessary strategy.<sup>3</sup> VPNs enable retailers to extend resource pools and expand their markets globally using more broadly-distributed business models, as well as over the Internet.

## Gaining a technology edge in customer relationships

While it is often said that it costs five times more to acquire a new customer than to retain an existing one, building and maintaining solid customer relationships offer more than just cost reduction. A mere 5% improvement in customer retention can cause an increase in profitability of between 25% and 85% in terms of net present value depending on the industry.<sup>4</sup>

Interactive Web 2.0 technology is changing the face of B2B and B2C customer relations. According to IDC, "The online social community revolution will target traditional retailers hard." (*Ibid.*) Web e-commerce, Voice over Internet Protocol (VoIP) commerce, personalized portals, and mobile and remote POS technologies offer customers more purchase options. E-mail, instant messaging/chat, VPNs and VoIP provide new channels for customer support and feedback. Savvy retailers are using these new technologies to drive online branding and segmented online store offerings. Successful "e-tailers" like Amazon.com apply adaptive promotions based on Web shopping habits. Brick-and-mortar retailers are introducing in-store displays and shopping carts that directly interact with customers as they buy using wireless-based technology and sophisticated back-end databases.

To retain market share today, retailers must also be responsive to their customers' social and cultural concerns as well, including such issues as identity and confidential data protection, workplace policy and practices and responsible energy consumption. IDC projects that "corporate social responsibility" and "green retail" will be among the top five priorities facing retailers (*Ibid.*).

## Securing the Competitive Edge

None of these advantages in savings, revenues or customer retention can be effectively attained without securing the underlying technologies which provide them. Despite their advantages, emerging technologies tend to be prone to vulnerabilities that can be readily exploited by professional attackers. No longer individuals out for the prestige of showing they could compromise a system, today's exploit developers are backed by profit-driven criminal organizations that seek to gather login credentials to financial sites for financial theft, identity theft and pump-and-dump stock schemes. In response to skyrocketing increases in malicious attacks, industry and government regulators require ever-tighter security in order for IT to meet compliance or else face stiff penalties.

## PCI compliance

- Identity fraud has reached epidemic proportions. Theft of identity information has outpaced traditional robbery to become a multibillion-dollar phenomenon, widely perpetrated by professional criminals. According to a report by the Federal Trade Commission<sup>5</sup>, the annual total loss to organizations and individual victims for all types of reported identity theft, including both new account and existing account

---

<sup>3</sup> *Ibid.*

<sup>4</sup> Reichheld, F. and Sasser, W., *Zero defects: quality comes to services*, Harvard Business Review, Sept-Oct, 1990, pp 105-111

<sup>5</sup> *Identify Theft Survey Report*, Federal Trade Commission (2003)

fraud, runs upwards of \$53 billion annually. This same study revealed that one in four U.S. households has been a victim of identity theft in the past five years.

- The Payment Card Industry Data Security Standard<sup>6</sup> (commonly referred to simply as PCI) was designed to provide the baseline requirements for how vendors should protect cardholder data to ensure it is not stolen or compromised. Depending upon a retail organization's transaction volume, payment channels and potential exposure, PCI classifies merchants into four levels of required compliance verification:
  - Level 1: These are merchants processing over 6 million transactions per year or compromised in the past year, regardless of acceptance channel. To comply with PCI, Level 1 merchants are required to conduct annual onsite review by a Qualified Data Security Company (CDSC) or internal audit; as well as quarterly network scans by a qualified independent scan vendor.
  - Level 2: These are merchants processing 1-6 million transactions per year, regardless of acceptance channel. To comply with PCI, Level 2 merchants are required to conduct annual self-validated assessment questionnaires, as well as quarterly network scans by a qualified independent scan vendor.
  - Level 3: These are merchants processing 20,000 to 1 million transactions per year. To comply with PCI, Level 3 merchants are also required to conduct annual self-assessment questionnaires, as well as quarterly network scans by a qualified independent scan vendor.
  - Level 4: These are merchants processing under 20,000 e-commerce transactions per year, and all other merchants processing up to 1 million transactions per year. To comply with PCI, Level 4 merchants are also required to conduct annual self-assessments and an annual network scan.

Merchant Level	Annual Criteria	Audit by Qualified Security Assessor	Annual Self-Assessment Questionnaire	External Scans
1	6M+ transactions OR security breach	x		x
2	150K-6M transactions		x	x
3	20K-150K transactions		x	x
4	<20K transactions		x	x

---

<sup>6</sup> *Payment Card Industry Data Security Standard 1.1*

The PCI standard is broken down into twelve fundamental requirements that are designed to be relatively intuitive to follow:

1. Install and maintain a firewall configuration to protect cardholder data
2. Do not use vendor-supplied defaults for system passwords and other security parameters
3. Protect stored data and do not store card and transaction data unnecessarily
4. Encrypt transmission of cardholder data and sensitive information across public networks
5. Use and regularly maintain secure systems and applications
6. Develop and maintain secure systems and applications
7. Restrict access to data by business need-to-know
8. Assign a unique ID to each person with computer access
9. Restrict physical access to cardholder data
10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes
12. Establish and maintain high level security principles and procedures

These standard principles and mandated requirements offer an overall guideline for security best practices that should be applied not only to credit card information, but as part of any retail organization's entire business data security program. Best practices warrant a defense-in-depth approach utilizing multiple layers for thorough protection, such as Unified Threat Management and Clean VPN.

## **Unified Threat Management**

In the past, retailers have had to settle for esoteric security solutions targeting single-point threats like viruses, spam and intrusions as they arose, often adding complexity and expense without corresponding value.

Today, security technology has evolved, and retailers demand simpler, well-engineered and cost-effective solutions. Unified Threat Management (UTM) firewall technology combines multiple security features into a single platform that can be easier and more cost effective to deploy and manage.

While malicious attacks can penetrate stateful packet inspection firewalls, early attempts at deep packet inspection with UTM often resulted in significant performance reduction. Advanced UTM solutions, such as those recently engineered by SonicWALL®, apply patented innovative technology to break through these earlier restrictions.

## **Clean VPN**

With the evolution of ecommerce, traditional retail boundaries are disappearing and "the store" is no longer limited to any specific physical location. Retail boundaries are blurring, with "outside" partners, vendors and consultants playing an increasingly vital a role in daily operations, often collaborating in cross-functional teams requiring secure access to "inside" application resources from "outside" devices, traversing internal and external firewalls. Increased access has increased productivity. However, it has also increased the number of access points, devices and network environments that are outside of the enterprise's direct control. It is more important than ever to monitor and secure both the traffic flowing through the network perimeter and the endpoints beyond the perimeter.

A "clean VPN" approach integrates a layer of intelligent remote access technology such as a Secure Sockets Layer virtual private network (SSL VPN) to secure users and devices beyond the perimeter, with layer of intelligent firewall technology such as Unified Threat Management (UTM) to secure data traffic

penetrating the perimeter. To be practically effective, an integrated clean VPN should be able to comprehensively detect the integrity of all endpoints, users and data traffic; protect resources against unauthorized access and malware attacks; and connect authorized users easily to mission-critical resources in real time.

## The SonicWALL Solution

SonicWALL streamlines the complexity out of retail security, allowing retailers of all sizes to leverage the Internet and their networks to enhance productivity, while maintaining the confidentiality, integrity and availability of their information assets. SonicWALL helps retail break free from premium-priced, complex legacy systems with easy, affordable solutions that are robust enough to support the needs of any organization. By relentlessly innovating to drive the costs and complexity out of building and running high-performance secure infrastructure, SonicWALL offers organizations exceptional value in:

- **Affordable acquisition** by standardizing to commercially available hardware, maximizing supply chain efficiencies and leveraging SonicWALL's leading-edge software development across the entire product line to drive down costs of high-performance network security for organizations of all sizes.
- **Ease-of-deployment** by delivering elegant, simplified solutions that are fast and easy to set up, even in the most demanding network infrastructures
- **Streamlined management** and operations by providing globally-managed, centrally-administered products and dynamic security services that deliver real-time threat and data protection

SonicWALL streamlines retail security, freeing resources to increase productivity and profitability, by integrating dynamically intelligent services, software and hardware into a comprehensive offering of high-performance security solutions, including:

- **Network Security Appliances** that apply a multi-tiered proactive security defense for wired and wireless retail networks, featuring ultra high-performance multi-core platforms and a patented Reassembly-Free Deep Packet Inspection (RFDPI) technology (U.S. Patent 7310815) to deliver real-time detection and protection through a suite of Unified Threat Management services including gateway anti-virus, anti-spyware, intrusion prevention, anti-spam and content filtering.
- **Secure Remote Access** featuring SonicWALL SSL VPN and award-winning SonicWALL Aventail E-Class SSL VPN technology, which enables remote and mobile employees, partners and customers to access mission-critical resources with granular policy control, endpoint interrogation, clientless Web deployment and unified policy management.
- **E-mail Security and Anti-Spam** providing inbound protection against spam, viruses, phishing and other e-mail threats as well as outbound protection from confidential information leaks.
- **Continuous Data Protection (CDP)** offering automatic, real-time tape-free data backup and recovery for network servers, laptops and POS PCs.
- **Global Management System (GMS)** enabling IT to manage a few or thousands of SonicWALL appliances from a central location, along with real-time ViewPoint reporting.

Additionally, all SonicWALL appliances running SonicOS Standard/Enhanced firmware are backed and **approved by an independent PCI Qualified Security Assessor**, ensuring their capacity to serve as technological control components in any network striving to achieve PCI compliance.

## Conclusion

Retailers stand to gain more competitive advantages in the marketplace from technology than ever before, with corresponding gains in cost reduction, revenue opportunities and customer satisfaction. To secure this competitive edge, however, retailers must take a comprehensive approach to protecting their technology from increasingly sophisticated threats.

SonicWALL is committed to providing retailers of all size with solutions of greater security value than the competition, at a significantly lower total cost of ownership, through purpose-built solutions designed to address retail's unique security requirements.