



Successful Security Strategies for Retailers in a Challenging Economy

*Driving productivity and profitability with
robust network security.*

CONTENTS

Economic Environment as a Challenge for Retailers.	2
- Gaining a Competitive Edge	
- Meeting Retail Challenges	
Conquering Threats with Increased Network Security	3
- Requirements for PCI Compliance	
What it Takes to Survive and Thrive in Today's Retail World	4
SonicWALL Retail Solutions	
- Network Security/ UTM	
- Secure Wireless	
- Secure Remote Access	
- Anti-Spam/ Email Security	
- Backup and Recovery	
- Global Management and Reporting	
Conclusion	5

Abstract

Today's economic environment has been challenging for many retailers. With increased unemployment and fewer customers, retailers have had to look for new ways to meet financial goals. At the same time, rising incidences of security breaches, credit card fraud, and identity theft are making retailers more aware of the need for tighter network security. Fortunately, by using creative methods to meet changing demands and bolstering consumer confidence with increased network security, many savvy retailers view this as a unique opportunity to gain a competitive advantage. By deploying a robust network security solution that helps deliver productivity and profitability while ensuring data remains protected, retailers can drive excellence throughout the organization—and set themselves apart from competitors.

Gaining a Competitive Edge in a Complex Climate

A variety of economic factors is creating a challenging environment for retailers and consumers. The mortgage crisis, bank closures, and rising credit-card fraud and identity theft are contributing to lowered consumer confidence and reduced spending. At the same time, the retail marketplace is becoming more competitive than ever, with traditional storefronts, kiosks and online shopping all competing for the same consumers' dollars.

While some retail businesses are finding it difficult to balance economic and security needs, many others are thriving as they adapt to this rapidly changing business landscape. For example, department store retailer Kohl's has assumed 31 Mervyns stores to gain a presence in "under-penetrated" markets. OfficeMax is opening four stores in the first half of 2009 to support the launch of its wellness retail concept. And Target is opening 45 new general-merchandise stores to rival Wal-Mart's Supercenters.¹ To increase efficiency and bolster data security, retailers, such as Palm Beach Tan, are realizing savings and increased productivity by deploying a point-of-sale (POS) and reporting solution that reduces time spent implementing remote franchise computers by 50 percent while securing their network against data breaches.

These examples illustrate that companies that react swiftly to a changing business environment are succeeding. By taking proactive steps, including increased collaboration, support for a flexible, mobile workforce, and the introduction of new applications to networks, retailers can survive the current downturn and continue to prosper. While these innovations can improve productivity and reduce costs, they also increase the potential for cyber attacks and other costly network security breaches. To meet this threat, retailers need a security solution that protects sensitive data from emerging threats and unforeseen disasters and streamlines network security management to improve productivity and profitability.

Meeting Retail Challenges in the New Economy

The key to getting ahead in today's economic climate revolves around a retailer's ability to offer an enticing, safe shopping environment—whether on- or offline. A critical component to success is addressing the security challenges that can overwhelm even the best-run operations. Gone are the days when data breaches are solely a concern for e-retailers—now all retailers with networked operations must worry about the vulnerabilities of their data and infrastructure.

Forward-thinking retailers recognize that retail operations make convenient targets. That's because each store and channel is typically connected in multiple ways to corporate databases. These connections offer a way for intruders to infiltrate the network and access all the information stored in the corporate data center. In addition, the potential for large-scale fraud has risen as more credit card numbers are stored

¹ Retail Info Systems News, *Beating the Odds: 10 Retailers Rack up Big Gains Heading into 2009*, 1/6/2009

electronically. Higher incidences of credit card fraud and data breaches lower consumer confidence, which is the last thing that retailers need.

Conquering Threats to Retail Success with Increased Network Security

To address heightened consumer awareness of data breaches and protect consumer credit card information, a consortium of most credit card issuers has implemented the PCI (Payment Card Industry) Data Security Standard (DSS). Managed by the PCI Security Standard Council, the standards are intended to help organizations that process card payments prevent credit card fraud, hacking, and other security vulnerabilities and threats. Any retailer processing, storing or transmitting cardholder data must be PCI DSS-compliant. To ensure that PCI requirements are met, retailers need centralized management of security rules and policies across a distributed environment, real-time monitoring and logging services, and historical compliance reporting for deployments of all sizes. Without these safeguards, they risk losing their ability to process credit card payments and could be audited and fined.

Key requirements for PCI compliance include:

- Maintaining a secure network, systems and applications
- Protecting cardholder data
- Preventing breaches via wireless and POS networks
- Using and regularly updating anti-virus software

More than Reputation is at Stake

With reputations and revenues at risk, organizations that wish to gain a competitive advantage cannot afford to relax data-security standards. Consider the class-action lawsuit against TJX Companies, Inc. in the wake of the massive data breach disclosed by the company in early 2007². The result of this unauthorized intrusion was the theft of customer data, which put customers at risk for identity theft. While the resulting legal fees and damages soared into the hundreds of millions of dollars, the overall cost to the retailer in terms of reputation and resulting loss of business was incalculable.

Retailers of all sizes would be well served to shore up protection of their networks and data. After all, cyber threats do not discriminate when it comes to the networks they target. Nor are insider attacks confined to big brand name retailers. On top of that, small retailers tend to invest less in stringent security measures and IT resources, making their networks more susceptible to breaches.

Companies that fail to protect their infrastructure and electronic data clearly face significant losses, both in terms of business and customer trust. According to a survey by Javelin Strategy & Research, the majority of consumers polled said they would stop shopping at stores that suffer data breaches³. Considering that it costs 6 to 10 times more to acquire a new customer than to retain existing ones⁴, it only makes sense that retailers take the necessary measures to prevent network attacks and downtime. These measures start with the deployment of an effective network security solution. In fact, companies that do invest in a robust network security solution will net a critical advantage in a challenging marketplace.

² InfoWorld, *Retailer TJX reports massive data breach*, January 17, 2007

³ Information Week, *Three of Four Say They Will Stop Shopping at Stores that Suffer Data Breaches*, April 12, 2007

⁴ Frederick Reichheld, *Loyalty Rules*. Harvard Business School Press, Bain & Co. 2001.

What It Takes to Survive and Thrive in Today's Retail World

As retailers consider their options, they need to recognize that it takes more than protecting credit card data to maintain an inviting and trustworthy shopping environment. To survive, they must maintain high productivity despite tighter budgets, all while adapting to more stringent regulations, an increasingly part-time and mobile workforce, and broader collaboration. As they deploy new applications to support these efforts, retailers are facing a new set of emerging threats. In response, they need to bolster their networks and systems against the variety of threats and vulnerabilities that can compromise business operations. Such measures not only help mitigate security threats, they can help retailers prosper in a challenging economy.

Unfortunately, traditional endpoint approaches are inadequate in addressing these needs. While some retailers rely upon a single end-point security solution to protect the network from incoming threats, others install a myriad of non-integrated security solutions that must be individually managed. Either way, the network is still vulnerable to the variety of existing and new threats that find their way into retail environments every day.

Rather than viewing secure technology as simply another line-item expense, successful retailers are adopting a holistic approach to their network security, seeing it as an integral investment underlying all their business initiatives. Holistic network security encompasses a range of measures that helps protect systems, applications, and data from compromise. Such an approach can actually enhance profitability by effectively protecting the network and customer data in an integrated manner. As a result, retailers can reduce overhead and operational costs, exploit new or expanded revenue streams, and comply with industry and government regulations.

SonicWALL Retail Solutions

SonicWALL® offers a scalable portfolio of security solutions for retailers that enable a holistic security approach designed to ensure uptime and mitigate security risks. This approach enables organizations to reduce costs associated with multi-consoles and stress on IT resources with an easy-to-manage, single view into the entire security system. In addition, an advanced range of Web, voice, wireless, and remote access technologies supports e-commerce and cross-channel sales initiatives for retailers of all sizes. By enabling retailers to provide more purchase options and better service, these solutions help drive customer satisfaction and revenues.

Network Security/Unified Threat Management/Network Security Appliance

The SonicWALL E-Class Network Security Appliance (NSA) and TZ Series are next-generation solutions that enable retailers to protect Internet, extranet and internal networks. By integrating multiple security services—including anti-virus, anti-spyware, intrusion prevention protection and application control—the appliances offer multi-threat protection. Delivered at gigabit speeds, this protection helps safeguard against all application-layer and content-based attacks without compromising performance.

Secure Wireless

SonicWALL SonicPoints in conjunction with E-Class NSA, NSA and TZ appliances empower cutting-edge initiatives in secure mobile POS, inventory tracking and interactive marketing, to protect against broadband connection failure the NSA and TZ products offer 3G connectivity providing WAN failover. These solutions provide anywhere, anytime access over cellular networks to ensure that retailers can securely access inventory systems and POS applications.

Secure Remote Access

The SonicWALL Secure Remote Access Solutions extend secure access beyond remote offices and corporate-controlled laptops out to network environments and external computers that are not controlled and managed by the corporate IT department. Remote support is also easy to implement using SonicWALL Virtual Assist, a clientless tool that enables a technician to assume control of a customer's PC or laptop in order to provide assistance.

Anti-Spam/Email Security

SonicWALL Anti-Spam/Email Security solutions ensure uninterrupted retail business communications while preventing inappropriate content entering or leaving the network. The award-winning SonicWALL Email Security Series offloads IT by automating anti-spam updates and by delegating costly and time-consuming inbox administration tasks to the end-user. With powerful and flexible controls, retailers can easily fine-tune the solution to best protect their organization against spam, viruses, phishing attacks, information leaks, and compliance violations.

Backup and Recovery

Retailers need to protect not only their data, but also the systems that access that data, such as Exchange, SQL Server and Active Directory. They also need the performance to backup and restore rapidly expanding volumes of data while meeting stricter regulatory compliance for data archiving – and should disaster strike, they need the flexibility to immediately recover the most current data to new locations or computer platforms. SonicWALL Continuous Data Protection (CDP) offers SMBs end-to-end disk-based backup and flexible disaster recovery options. Low-touch CDP transparently and automatically protects data and applications, while enabling self-directed restoration of files.

Global Management and Reporting

Without centralized management, unified policy enforcement, and active monitoring and reporting, organizations are more likely to experience network attacks, outages and security vulnerabilities. SonicWALL Global Management System eases administration and helps meet regulatory compliance by providing flexible, powerful and intuitive tools to manage from a few up to thousands of remote SonicWALL network security appliances, all from a central location. Through a simple Web interface, IT administrators can access centralized security, policy and network management; real-time monitoring and alerting; and robust reporting functionality. SonicWALL ViewPoint delivers a breadth of summary and drill-down reports that exhibit detailed network activity inside a company's network.

Conclusion

Smart, well-managed retailers seem to thrive in the face of any challenge—whether tougher competition or new network threats and vulnerabilities. Increasingly, decision makers are differentiating their retail environments by adopting a strategy that ensures their entire network is secure. After all, they recognize that traditional security approaches—such as individual end point solutions and non-integrated security products—are no longer adequate to the task at hand.

To achieve this level of security, retailers must adopt a holistic view that protects systems, applications and data from cyber threats. This integrated approach also helps retailers thrive in a challenging economy by streamlining security management to reduce operational costs, enhance productivity, comply with regulations and allow for new retail revenue streams.

SonicWALL, a leading provider of security solutions, enables retailers to adopt a holistic approach to security that can ensure a competitive advantage. Through a scalable portfolio of security solutions featuring an advanced range of Web security, voice, wireless, and remote access technologies, SonicWALL helps retailers protect the complex retail environment, accelerate customer loyalty, and remain productive and profitable.

For more information on how SonicWALL can help your organization succeed in a challenging retail economy visit www.sonicwall.com.

©2009 SonicWALL, Inc. is a registered trademark of SonicWALL, Inc. Other product names mentioned herein may be trademarks and/or registered trademarks of their respective companies. Specifications and descriptions subject to change without notice.