10 easy steps to secure your retail network

Simple step-by-step IT solutions for small business in retail to leverage advanced protection technology in ways that are affordable, fast and easy

October 2015

Introduction

Every year, network attacks become more widespread, more intelligent and more difficult to detect. Given the public nature of retailers, entry points into the network go beyond employee laptops, desktops and smartphones to include public Wi-Fi, and public-facing ecommerce servers.

As a result, retail networks have two primary challenges. The first is dealing with the complexity of managing many remote locations. The second is being able to provide security protection that mirrors the same threats as those facing large enterprise networks.

In a small retail business, the role of administering network security often falls on the business owner or the default in-house "techie." Typically, neither of these individuals would have the time, resources or expertise to work on complex network security protection deployments and administration. In a distributed retail environment, both the IT department and security department have unique challenges. For IT, it is managing a complex and distributed network (including wireless and switch management). For security, it is deploying consistent policies across the organization.

You can build a secure retail network by taking advantage of modern network security technologies. This e-book examines the ten primary security challenges for your retail network and offers ten proven solutions.

Step 1: Layer your security

Your challenge: Bolster your defense against new threats at every layer

Many of today's attacks are blended attacks which use multiple techniques at different layers to try to infiltrate the network. These attacks can bypass outdated firewalls that lack the power to inspect all traffic, including large files and HTTPS encrypted traffic.

Your solution: Deploy a Unified Threat Management firewall

The best approach for retail network security protection today is Unified Threat Management (UTM). Simply put, UTM firewalls combine the effectiveness of various point defenses to add protection at every networking layer. For a retailer, the value of UTM comes from its combining complex tasks into a single device with a management console. This approach provides a powerful defense against a wide range of security threats. This makes network protection more complete, affordable and easy to manage.

Deploy a Unified Threat Management firewall

Step 2: Secure your gateway

Your challenge: Block threats before they enter your network

E-commerce and Wi-Fi increases the ability for you to reach more potential customers by expanding your network perimeter. However, an expanded perimeter presents more approaches for additional attacks.

Your solution: Inspect the whole file

Deep Packet Inspection technology, when properly deployed at the gateway, can scan the entirety of the data packets that touch your network perimeter. In addition, your UTM firewall also needs to be able to inspect encrypted communication coming from HTTPS traffic in order to catch threats that are hidden inside files, applications and attachments.

No limits on size or type of file

Step 3: Keep it simple

Your challenge: Cut out complexity

Simplicity affects your bottom line. The total cost you pay for security isn't only measured in its list acquisition price. It's also in the cost of installing, using, managing and maintaining your solution.

Your solution: Simplify your technology

High-performance security does not have to be complex. Modern security appliances can make setup and management easy, using features like intuitive web-based interfaces and easy-to-use configuration wizards. For multiple locations, centralized or hosted management can further ease administration and ultimately lower ongoing cost of ownership.

Simplify your technology

Step 4: Keep it affordable

Your challenge: Ensure comprehensive protection on a small budget

Every organization, no matter the size, needs the same protection used by the biggest banks, hospitals, universities and governments. Often to get the best protection means spending beyond the budget.

Your solution: Consolidate your security

Reduce your costs for hardware, set-up, operations and administrative overhead by consolidating multiple security tools in one easily managed, affordable appliance. Optimally, such an appliance should include content filtering, intrusion prevention, anti-spyware, anti-malware and native apps for remote access from any device. To stop today’s threats, consolidated security needs to also include the ability to inspect encrypted files without file size limitations.

Consolidate your security

Step 5: Get rid of bottlenecks

Your challenge: Keep your firewall current with your network build-out

Even if your firewall is only a couple years old, it might be compromising the security and efficiency of your network. You should not have to resort to turning off security features to maintain performance. Scheduled reviews of network improvements must consider the firewall as a key component.

Your solution: Select high-performance hardware and software that is priced for small businesses.

For optimal performance while maintaining maximum security, your solution must deliver throughput that won't bog down performance. Multi-core microprocessor technology allows UTM appliances that are designed for small businesses to gain significant network efficiency.

> Select high-performance hardware and software that is priced for small businesses

Step 6: Keep systems current

Your challenge: Keep track of what is using your network

People use a combination of devices and software to do their work. Many devices and many apps can open windows for cyber-criminals. Controlling what has access to the network, and securing devices, can overwhelm retailer's security systems.

Your solution: Protect your network from suspect devices and applications

At the highest level, a firewall should be able to quarantine guest and employee devices that do not have current anti-virus protection. For even deeper protection, knowing what devices are on the network, and making sure that your guests and employees have the latest software, can reduce exposure to vulnerabilities.

Protect your network from suspect devices and applications

Step 7: Keep your network productive

Your challenge: Weed out non-productive traffic

Today's business networks can be choked by spam, unauthorized web activity and social networking traffic that have nothing to do with getting work done. You may not even know that the person down the hall who is downloading movies is bringing your network to a crawl.

Your solution: Implement content and application management

Insist on a firewall that shows you all network activity of all users in real time. In an environment where you have both employees and guests, you may want to have different usage policies. For employees, it should allow you to easily create rules to restrict the use of non-productive applications and sub-applications (e.g., Facebook may be acceptable for marketing purposes, but the games within Facebook are not). For guests, you may consider restricting activity so as to prohibit users from going to offensive or inappropriate sites.

Implement content and application management

Step 8: Stay compliant

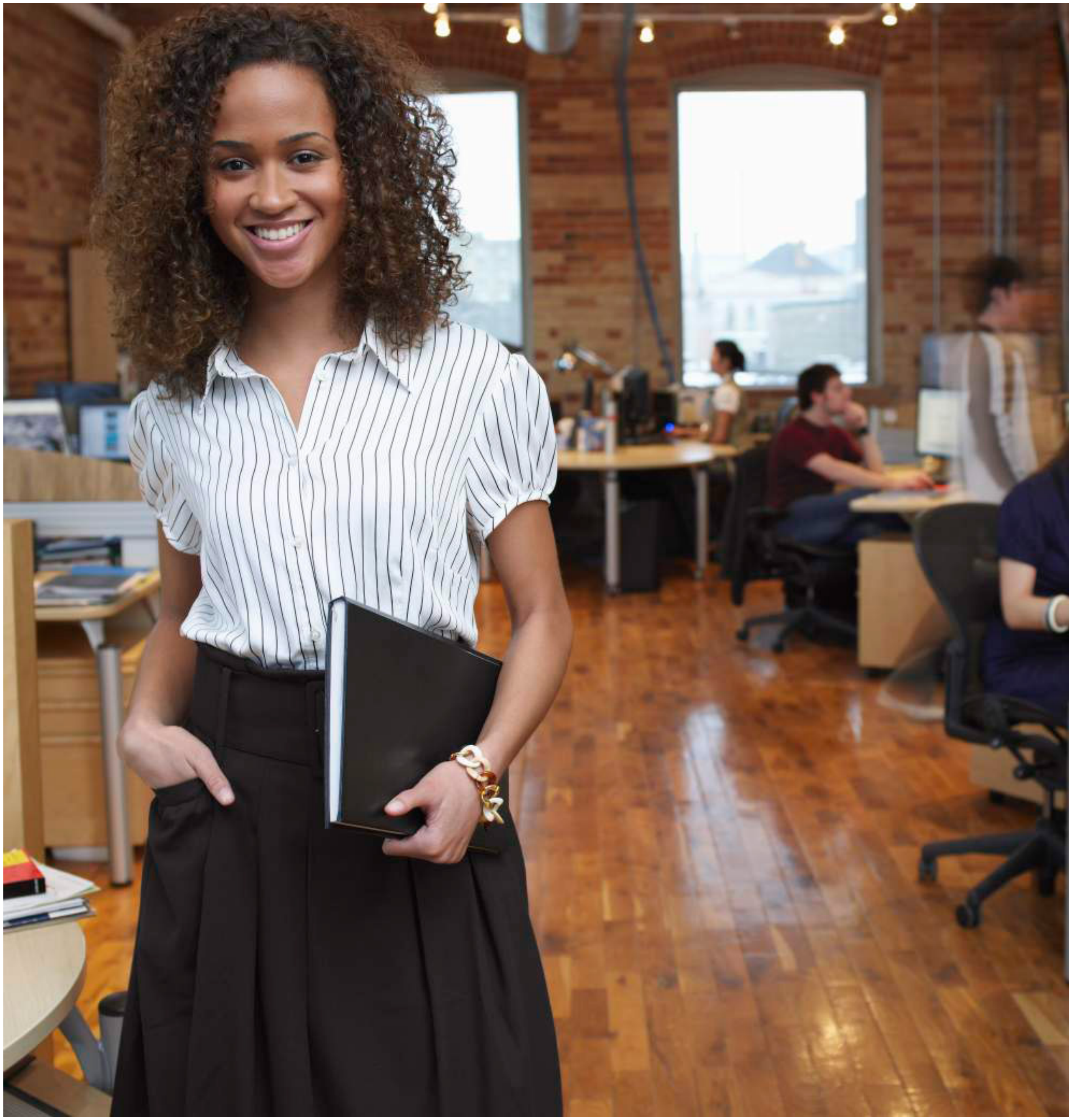
Your challenge: Meet regulations and avoid penalties

Today, there is increased scrutiny on protecting customer credit card data. Maintaining PCI compliance is a great way to cover security basics. PCI compliance starts with installing and maintaining a firewall configuration that protects cardholder data. Changing the default access passwords to the firewall is not just a guideline but a sound business requirement. To avoid costly penalties make sure your business is in compliance, with comprehensive network security and policy enforcement, as well as robust management and reporting.

Your solution: Integrate compliance management

Look for a solution that is easy to implement and starts you on the right track by first requiring you to change the default access. The very first requirement for PCI compliance is to change the default password. Beating defaults is no harder than a simple internet search to identify manufacturer defaults. Make passwords hard to guess and keep them hidden away from prying eyes. The best firewalls will integrate many security features, including malware detection, intrusion prevention and blocking the inclusion of unsanctioned credit card numbers in outbound emails, into a single device.

Integrate compliance management



Step 9: Secure your wireless networks

Your challenge: Prevent wireless-based attacks

Wireless connectivity improves the retail experience. However, it also opens more avenues for attack. On top of that, a wireless security solution often requires adding an expensive controller and another management console.

Your solution: Apply wireless network security

A simple approach would be to bring wireless within the security perimeter. By doing so, the security policies you set can also apply to wireless users. Wireless security should also be able to isolate employees from guests to ensure privacy and confidentiality.

Apply wireless network security

Step 10: Be prepared for the unexpected

Your challenge: Prepare for unplanned disruptions

Even the best UTM-secured network needs a disaster recovery solution. Major disasters have demonstrated how exposed small businesses can be to unexpected events. But it's not only headline-grabbing natural disasters, health pandemics or terrorist attacks that can disrupt a business. For retail businesses, building fires, broken water pipes, power outages, equipment failures, or even lost or stolen laptops can mean disaster. These events can potentially disrupt your operations indefinitely if you are not prepared.

Your solution: Establish a backup plan

Having the ability to restore an individual file or the whole network is within reach of practically every retailer. Backup to a secure secondary business location or third-party site means business systems can be restored and operational even in the primary site is compromised. Bare metal recovery (BMR) technology enables entire operating systems, such as database or file servers, be recovered to new or different hardware platforms if the original device can't be restored.

Establish a backup plan

Conclusion

Retail network security can be a complex issue but, as presented in this e-book, it does not have to be. There are easy ways to start addressing it with IT solutions for small business. Look for a trusted advisor that can help you build a roadmap for small business network security. Insist on no-compromise security that matches performance and protection that fits your budget.

For More Information

The information in this document is provided in connection with Dell products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Dell products. EXCEPT AS SET FORTH IN DELL'S TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, DELL ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL DELL BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF DELL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Dell makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Dell does not make any commitment to update the information contained in this document.

About Dell Software

Dell Software helps customers unlock greater potential through the power of technology — delivering scalable, affordable and simple-to-use solutions that simplify IT and mitigate risk. The Dell Software portfolio addresses five key areas of customer needs: data center and cloud management, information management, mobile workforce management, security and data protection. This software, when combined with Dell hardware and services, drives unmatched efficiency and productivity to accelerate business results. www.dellsoftware.com.

If you have any questions regarding your potential use of this material, contact:

Dell Software
4 Polaris Way
Aliso Viejo, CA 92656
www.dellsoftware.com

Refer to our Web site for regional and international office information.

Ebook-10Steps-SecureRetail Network-US-KS-27124