PCI DSS

Maintaining Strong Security and PCI DSS Compliance in a Distributed Retail Environment

White Paper

Published: February 2013

Executive Summary

Today's retail environment has become increasingly more complex and sophisticated. IT demands continue to increase due to growing risk management concerns and regulatory compliance requirements. Distributed retail environments are particularly challenging. Each endpoint (store) is an attack vector waiting to be exploited; each store has to meet PCI DSS regulatory requirements.

The PCI DSS requirement affects any merchant who accepts credit card transactions. In a distributed retail environment, this means IT professionals must apply uniform security measurements across all distributed store endpoints. Failure to provide a uniform network security strategy and protective systems deployment can result in substantive penalties, as well as high risk exposure to a variety of data and network threats.

This paper provides business planners with informative details on how to maintain strong security and PCI DSS compliance in a distributed retail environment. Instrumental to this, is a solutions overview of how WatchGuard Technologies keeps applications, data, and networks safe and PCI DSS compliant.

The Distributed Retail Environment

Retail has become one of the most complex IT environments, rivaling the most demanding systems architectures, such as those used in banking and finance. The distributed retail environment presents a multitude of unique IT challenges that stand apart from a more pedestrian single-store infrastructure.

Why is this? Business pressures are forcing retailers to be more agile, more aggressive, and more efficient. To remain competitive, retailers have to invest in IT systems that help retain and nurture customer and brand loyalty, as well as increase sales and, simultaneously, reduce operating costs.

Examples of these technologies include virtual private network (VPN) solutions, which enable secure data communications between individual store locations to back-end IT systems; Voice over IP (VoIP) telephony solutions, which result in toll by-pass telecommunications savings; and Application Control technology, which enables businesses to manage and control what applications traverse their business network.

However, as IT systems become more complex, risks increase. Distributed environments pose additional risks due to the maxim that network security is only as good as the "weakest link."

In a distributed environment, one mistake can have massive repercussions. Example: According to Gartner, 95 percent of firewall breaches are a result of misconfigured firewall--rather than flaws in the firewall—which Gartner believes will continue to hold true through 2018.[1] This means, as IT rolls out firewalls at the branch/retail location – and for a large retailer, this can easily be in the hundreds or thousands – just one firewall misconfiguration can result in a network breach or data loss.

Hackers know this too, which is why a distributed network is particularly enticing to them. Distributed systems mean more points of attack. For retailers, this means strong IPS (intrusion prevention systems)

[1] Gartner, Inc. "One Brand of Firewall Is a Best Practice for Most Enterprises". November 28, 2012.

must be implemented to thwart all sorts of automated network intrusion attacks, such as port scans and distributed denial of service (DDoS) attacks.

In addition to hackers, the Internet itself presents a formidable risk to retailers. Web-based threats continue to rise; the most common of these include viruses and malware variants. Retailers are often targets for spyware, such as keyloggers and botnets, which are optimized to capture financial and credit card data.

Furthermore, as retailers adopt and deploy VoIP systems, they should be cautioned about new and emerging voice over IP threats, such as "vishing," directory harvesting, and other types of VoIP-type attacks that are geared to access network resources.

Lastly, retailers today have aggressively adopted use of social media and other web-based applications for promotion and to attract customers. With this, comes employee use of social media, which can become a systemic drain on IT resources, and can negatively impact productivity.

For these reasons, retail risk management has evolved far beyond the act of deploying a firewall. Many retailers, and, in particular, distributed retailers, turn to vendors, such as WatchGuard, for UTM solutions that incorporate VPN capabilities, firewalling, intrusion prevention, gateway antivirus, and advanced protection against web threats. WatchGuard solutions also include Application Control capabilities, which provide retailers with in-depth, granular controls over users and the applications that traverse their network.

But, if advanced threats were not enough for IT to worry about, today's retailer must also take into account how to best handle regulatory requirements, such as state-by-state privacy and data protection/breach notification laws, as well as industry-driven mandates, such as PCI DSS.

Any merchant who accepts credit cards must abide by PCI DSS version 2.0. This requirement is critical for both consumers and retailers, as it presents a framework that articulates industry best practices for securing cardholder data, as well as general security best practices for applications, networks, and other IT resources.

PCI DSS and Creating a Secure Distributed Retail Ecosystem

According to the nonprofit Privacy Rights Clearinghouse (Aug. 2010), more than 510 million records with sensitive information have been breached since January 2005. And, each day, news breaks on both small and large-scale breaches where consumer credit card data is stolen.

In order to support consumer confidence, as well as to reduce future losses, the five major credit card providers (American Express, Discover, JCB, MasterCard and Visa) created the Payment Card Industry Security Standards Council, whose charter was to develop policies dedicated to the protection of credit card data. From this, all merchants who accepted credit cards for payment could follow a uniform set of requirements to best ensure credit card data is safe and secure.

The overarching result became known as the Payment Card Industry Data Security Standard (PCI DSS) version 1.0, which, at the highest level, outlined 12 requirements that satisfy a variety of security goals.

These goals and general requirements are:

Goal	Requirement
Build and maintain a secure network	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.
Protect cardholder data	3. Protect stored cardholder data. 4. Encrypt transmission of cardholder data across open, public networks.
Maintain a vulnerability management program	5. Use and regularly update antivirus software or programs. 6. Develop and maintain secure systems and applications.
Implement strong access and control measures	7. Restrict access to cardholder data by business need to know. 8. Assign unique IDs to each person with computer access. 9. Restrict physical access to cardholder data.
Regularly monitor and test networks	10. Track and monitor all access to network resources and cardholder data. 11. Regularly test security systems and processes.
Maintain an information security policy	12. Maintain a policy that addresses information security for all personnel.

Additionally, different compliance tiers exist, based on the annual number of credit card transactions. Since the release of PCI DSS version 1.0, the standard has received revisions, clarifications and updates, with the latest version 2.0, having gone into effect January 1, 2011.

PCI DSS version 2.0 does not include any new requirements to the above list; instead, it clarifies requirements in order to help merchants, especially small and midsize retailers, in adhering to the standard.

Furthermore, PCI DSS version 2.0 retains the same penalties for non-compliance. Any retailer found to be non-compliant may face substantive financial penalties, regardless of whether or not a breach has occurred. Typically, fines for non-compliance are levied based on the size of the retailer, but in some cases, a credit card provider reserves the right to expel a retailer from its program, thus effectively cutting off acceptance of that vendor's credit card. Therefore, it is critical that a retailer maintain PCI DSS compliance.

The PCI DSS requirements apply to all "system components," which are defined as any network component, server, or application included in, or connected to, the cardholder data environment. Network components include, but are not limited to, firewalls, switches, routers, wireless access points, network appliances, and other security appliances. Servers include, but are not limited to, web, database, authentication, DNS, mail, proxy, and NTP servers.

Applications include all purchased and custom applications, including internal and external web applications. The cardholder data environment is a combination of all system components that come together to store and provide access to sensitive data.

So, how does WatchGuard help in securing a distributed retail environment?

Build and Maintain a Secure Network

The first requirement of the goal to build and maintain a secure network is to install and maintain a firewall configuration to protect cardholder data.

Here, WatchGuard UTMs provide unparalleled firewall protection to control data traffic in and out of a distributed network. Additionally, WatchGuard UTMs protect against unauthorized access from the Internet and include integrated IPS to prevent hackers from gaining access to internal resources.

Specifically for distributed retail environments, WatchGuard offers RapidDeploy, a unique cloud-based configuration utility that enables uniform, rapid deployment of UTM appliances across a distributed environment. This eliminates the need for IT professionals to pre-configure devices or travel to deployment sites for installation, which significantly reduces total cost of ownership, while also reducing the risk of UTM misconfiguration.

The second requirement under this rubric is to not use vendor-supplied defaults for system passwords and other security parameters.

Here, WatchGuard requires administrators to change default passwords when first configuring appliances. And, with role-based access controls, administrators can effectively manage who can make firewall/UTM changes so that systems are always protected from unauthorized access.

Protect Cardholder Data

The third and fourth requirements call for the protection of stored cardholder data and encrypted transmission of cardholder data across open, public networks.

In general, no cardholder data should ever be stored, but if it need be, the data should be encrypted. While WatchGuard does not provide data storage encryption solutions, it does provide VPN solutions to address the issue of secure data transmission.

Especially suited for distributed retail environments, WatchGuard VPN solutions can create tunnels that provide secure site-to-site connections between networks or distributed store locations. This way, encrypted cardholder data can be securely transmitted and protected from hackers and identity thieves.

Maintain a Vulnerability Management Program

Here, the PCI DSS requirement calls for regular updating of antivirus software or programs.

WatchGuard UTMs offer gateway antivirus to protect against all sorts of viruses, trojans and malware variants. With the security subscription, all WatchGuard UTMs are automatically and seamlessly updated to thwart the latest virus outbreaks. It's worth noting that, with WatchGuard proxies, many "zero-day" attacks can be stopped prior to receiving an antivirus update. And, with WatchGuard's cloud-based Reputation Enabled Defense, dangerous websites and IP traffic can be shunned before it ever reaches a retail branch location.

Implement Strong Access Control Measures

This requirement calls for the restriction of access to cardholder data using business need-to-know policies. To ensure critical data can only be accessed by authorized personnel, systems and processes must be in place to limit access based on job responsibilities.

Here, the best security practice is grounded in the principle of "least privilege," which holds that access to data should be limited to those who need it for legitimate business purposes. With WatchGuard, administrators can enforce granular policies based on individual users or groups, as well as segment network traffic so that access to data is bound by least privilege rights regardless of the user, device, or network.

Regularly Monitor and Test Networks

Under this goal, the requirement calls for tracking and monitoring of all access to network resources and cardholder data.

With WatchGuard, administrators have the most in-depth and feature-rich array of reporting and logging tools, which are included for free with all WatchGuard UTMs. Advanced logging mechanisms support the ability to track individual users, which is critical for forensics and vulnerability management. Moreover, WatchGuard provides easy-access, pre-packaged PCI DSS reports that provide you quick information that helps you stay on top of your compliance landscape.

Additionally, administrators can avail themselves of the Rogue AP scan capabilities of WatchGuard wireless appliances. The scans can help improve WiFi security by detecting and alerting IT to the presence of unknown, potentially unauthorized wireless access points that operate in the same area.

Maintain an Information Security Policy

This goal requires that merchants maintain a policy that addresses information security for all personnel.

Here, WatchGuard helps merchants in a variety of ways. First, every WatchGuard UTM supports extensive policy controls. This way, distributed retailers can maintain and enforce uniform policies across a variety of geographic locations. Second, WatchGuard delivers additional security services via its LiveSecurity service that provides best practices and related security updates for retailers to ensure they are up to speed on the latest security developments.

Conclusion

Today's distributed retail environment architecture is one of the most challenging IT environments, rivaling that of banks and financial institutions. While the distributed retail environment offers substantive business advantages, such as increased sales, improved customer loyalty, and operational efficiencies, it also poses significant challenges. Today's network administrators need not only be mindful of hackers bent on stealing cardholder data, but they must also be fully apprised of legal and industry regulations, such as PCI DSS.

PCI DSS aims to help retailers maintain a secure environment, and to keep cardholder data safe from identity thieves and hackers. WatchGuard arms retailers with a multitude of security and management functions that help in meeting PCI DSS requirements, while providing the backbone functionality to keep networks, applications, and data safe and secure.

For More Information

For more information, visit the WatchGuard website, contact a WatchGuard reseller, or call 1 (800) 734-9905 in the United States and Canada.

ADDRESS:
505 Fifth Avenue South
Suite 500
Seattle, WA 98104

WEB:
www.watchguard.com

NORTH AMERICA SALES:
+1.800.734.9905

INTERNATIONAL SALES:
+1.206.613.0895

ABOUT WATCHGUARD

Since 1996, WatchGuard Technologies has provided reliable, easy to manage security appliances to hundreds of thousands of businesses worldwide. WatchGuard's award-winning extensible threat management (XTM) network security solutions combine firewall, VPN, and security services. The extensible content security (XCS) appliances offer content security across email and web, as well as data loss prevention. Both product lines help you meet regulatory compliance requirements including PCI DSS, HIPAA, SOX and GLBA. More than 15,000 partners represent WatchGuard in 120 countries. WatchGuard is headquartered in Seattle, Washington, with offices in North America, Latin America, Europe, and Asia Pacific. For more information, please visit www.watchguard.com.