Security for Retailers

A Changing Threat Landscape for the Retail Industry

What to do about Targeted Attacks, Web Applications, PCI DSS 2.0

White Paper

WatchGuard® Technologies, Inc.
Published: February 2011

Retailers Are Under Attack

The recent, unprecedented upsurge in attacks on retail businesses makes it clear that cyber criminals have now turned more of their attention – and formidable skills – to cashing in on the sector's rich cache of confidential data.

According to MessageLabs, the number of attacks that specifically targeted the retail sector jumped to 516 in just one month during Q4 2010, compared to the earlier average of 7 attacks per month for much of that same year.[1] It also marked the first time in recent years that the retail sector became the focus of a major targeted attack campaign.

It's All about the Data

Cyber criminals follow the money. Credit card numbers and other forms of personal data make the retail industry a particularly lucrative target. Harvesting customer information, of course, is not new to the industry. The infamous 2007 hack of TJX Companies Inc. resulted in the theft of 45.7 million credit and debit card numbers, with an estimated cost to the company of $216 million. What started as a poorly secured wireless connection eventually opened the door to complete access to the TJX databases.

The graph below shows how retail has compared to other industries over the last few years, based on the percentage of records/people affected by a data breach. At 31%, retail trails financial services only slightly (33%) for the highest number of people affected by data breaches. (Source: KPMG's Data Loss Barometer http://www.datalossbarometer.com/index.html)

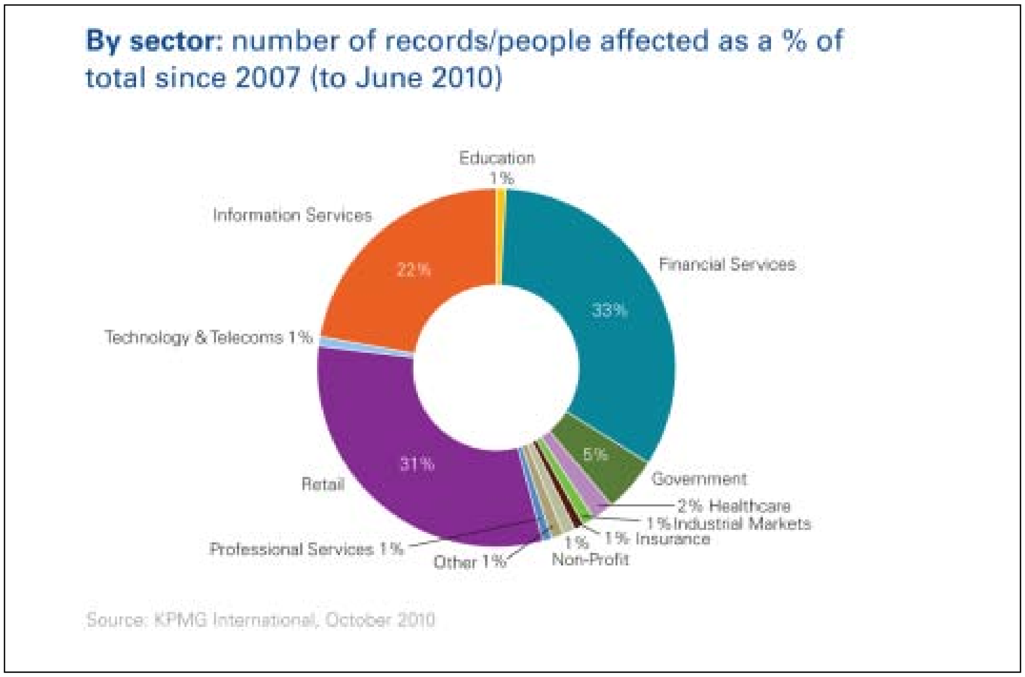


Figure 1. Retail is Second in the Number of Records/People Affected

[1] MessageLabs Intelligence Report, October 2010, http://www.messagelabs.com/resources/press/61775

Recent Attacks Show Increasing Sophistication

One of the most disturbing trends for the retail sector is what's known as the "targeted attack." In the past, most attacks involving email were widely distributed, using indiscriminate mass mailings to cast the broadest net. Targeted attacks, on the other hand, are characterized by low-volume distribution. Organizations are selected and researched before highly sophisticated social engineering scams are executed to gain access to sensitive data.

Spear Phishing

One targeted attack strategy involves a technique called "spear phishing." Simple "phishing" exploits are impersonal spam emails aimed at tricking victims into giving up sensitive data. However, spear phishing is much more refined and carefully crafted, using some form of personalized information in the email to make the recipient think the message is from a reputable and trusted source. More important, spear phishing is targeted towards a specific organization or individual. Spear phishers typically target "whales," which are high-level individuals at an organization – for instance, C-level executives.

How do scammers get the personal information for the attack? There is a great deal of data available on the web that criminals can use. Personal info is easily harvested these days from blogs, social networking sites such as Facebook and Twitter, or from a business's web site itself. It's as uncomplicated as searching for blog postings about buying certain products, monitoring LinkedIn for people who work for a particular organization, or capturing the names of friends on Facebook pages. One report revealed that 324 spear phishing attacks against 88 employees of the same company appeared to come from their senior executive email addresses – addresses most likely gleaned from professional networking sites. [3]

BLEEDING EDGE TARGETED ATTACKS

Advanced Persistent Threats (APTs) are the new high-end of targeted attacks. There is no single, standard definition of APTs, but they do have these things in common:

- **APTs apply the most advanced** attack, infection, and malware propagation techniques known.
- **They are designed to stay hidden** within a victim network or host for a long period of time – typically hiding behind strong rootkit technology, cleaning logs, and slow, quiet Command and Control channels.
- **They tend to have a specific, targeted goal** in mind. For instance, they might be designed to slowly steal intellectual property from a specific business or quietly take control of a retailer's network admin privileges. [2]

The following example of a targeted spear phishing attack highlights the growing menace posed by exploits involving retail. It relied on the much-talked about Zeus botnet. "Zeus" is actually a family of malware designed to steal data. At one time it was used mostly to target online banking sites, but by mid-2010 it was reported that up to 88 percent of Fortune 500 companies showed Zeus botnet activity. [4]

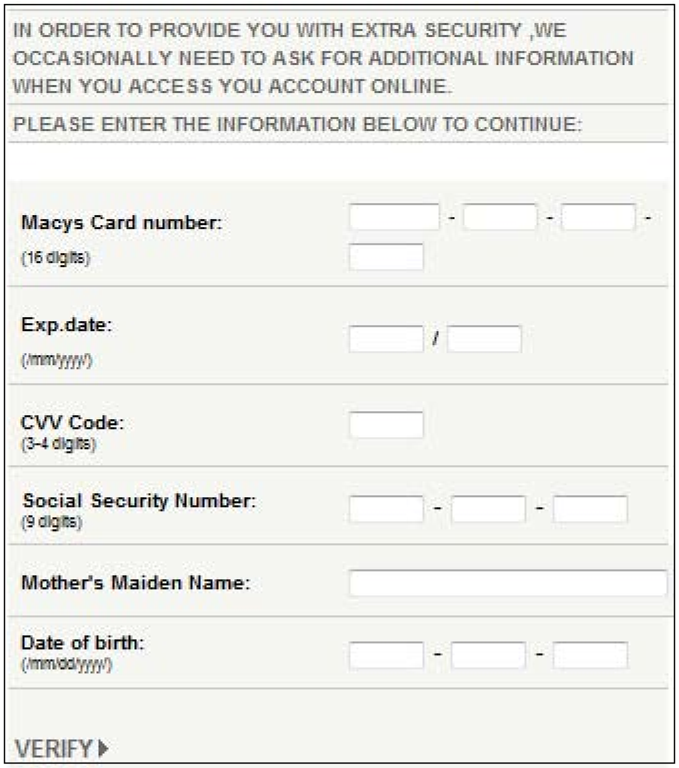
[2] WatchGuard 2011 Network Security Predictions, www.watchguard.com/docs/brochure/wg_2011_security_predictions.pdf

[3] Zeus botnet targeting Macy's, Nordstrom account holders, SC Magazine, December 09, 2010, http://www.scmagazineus.com/zeus-botnet-targeting-macys-nordstrom-account-holders/article/192509/

[4] CNET News, April 14, 2010, http://news.cnet.com/8301-27080_3-20002425-245.html#ixzz1A6sCBtC4

In late 2010, researchers discovered a Zeus botnet that was targeting credit card accounts of major retailers, including Macy's and Nordstrom. Although other versions of Zeus have been known since 2007, this attack used a Zeus 2.1.0.8 botnet – the most sophisticated version of Zeus to date, in an exploit specifically crafted to steal credit card information at the retailer's gateway.

The attack relied on a social engineering scheme that took advantage of the trust relationship between customer and merchant. The victim would receive a highly plausible email that appeared to come from the retailer, containing a link to the merchant's web site – www.macys.com, for example. When the unsuspecting victim connected to the web site, Zeus malware would inject a legitimate-looking, man-in-the-middle pop-up (see Figure 2) that requested personally identifiable information. Attackers use forms such as this to gather additional personal information along with the customer's credit card number. This not only opens the door to identify theft, it gives attackers what they need to bypass fraud detection measures that could be used by the merchant to investigate suspicious transactions. (Source: Help Net Security, December 2010)



IN ORDER TO PROVIDE YOU WITH EXTRA SECURITY ,WE OCCASIONALLY NEED TO ASK FOR ADDITIONAL INFORMATION WHEN YOU ACCESS YOU ACCOUNT ONLINE.

PLEASE ENTER THE INFORMATION BELOW TO CONTINUE:

Macys Card number: (16 digits)

Exp.date: (/mm/yyyy/)

CVV Code: (3-4 digits)

Social Security Number: (9 digits)

Mother's Maiden Name:

Date of birth: (/mm/dd/yyyy/)

Figure 2: **Fraudulent pop-up window from Zeus botnet/phishing exploit.**

At the same time that Zeus was collecting personal data via a retail-oriented spear phishing exploit, massive cyber attacks were hitting other retail/hospitality organizations as large as McDonalds and Walgreens, forcing them to notify customers that their personal information may have been compromised. [5]

[5] Retailers Come Under Cyber Attacks, December 21, 2010, http://vsr.edgl.com/reseller-stories/Retailers-Come-Under-Cyber-Attack57164

Customers Expect a Great Deal from You

In the world of retail it's no longer enough to provide a pleasant customer experience. Retailers need to extend the concept of customer service to looking after a customer's personal data after the transaction is completed. There's more at stake than just PCI compliance. Security and trust have been described as the backbone of doing business over the Internet. Customers need to feel that they can rely on the merchants they do business with to have stringent security measures in place to prevent data theft.

There are more than 57,000 illegitimate web sites created each week.[6] Most of these malicious sites mimic prominent web sites in an attempt to fool the web-browsing public. Perhaps more worrisome to retailers are the number of legitimate web sites that have been infected with malware, making them possible distribution centers of malware for customers, employees, and partners. In other words, your retail business web site, unbeknownst to you, could become infected – or may even be infected now – with malware that can, in turn, infect your stakeholders' computers as well as steal their data.

WHO'S SPOOFING YOUR DOMAIN?

Has your business's online reputation been compromised? Check your reputation score on the WatchGuard Reputation Enabled Defense web page.

Reputation Enabled Defense is the powerful cloud-based engine that gathers data from millions of global sources and deployed systems worldwide to identify and block spam, malware, and malicious threats in real-time.

By cross-referencing and analyzing data from global feeds across multiple protocols, this technology provides an all-encompassing view of the IP address behavior and URL threat risk level.

Reputation Enabled Defense technology is integrated into WatchGuard security solutions. Read more on page 8.

How Safe Are You?

The size of your retail business doesn't matter. Any data you collect is big business. In 2010, credit card information was the most commonly advertised item for sale on underground black-market servers, accounting for 23 percent of all goods and services.[7] Every merchant that connects to the Internet is a potential target of cyber crime.

Unfortunately, there is nothing you can do if customers fall victim to scams that fraudulently present your business's name to gain their trust. That falls in the area of your customers' own security measures and the safeguards they employ. But there are plenty of ways that retail businesses can ensure their web sites and data are protected. Cyber criminals target weak network configurations, vulnerabilities in software applications (particularly Web 2.0 apps), unencrypted data in motion, and gaps in network security deployments; these are all areas where you can ensure you have strong protection.

Today's businesses are becoming more concerned and better informed about the cyber threat landscape, and are increasingly seeking security solutions that better protect their own and their customers' data.

[6] "The Criminal in Your Browser Is Real," Help Net Security, December 2010 , http://www.net-security.org/article.php?id=1549&p=3

[7] 2010 Annual Security Report, MessageLabs, http://www.messagelabs.com/globalthreats

How WatchGuard Keeps Your Retail Business Protected

The key to security is multi-layered, multifaceted defenses. Below are five steps to better security you can't afford to ignore on your network – from application control to data loss prevention – to ensure your retail business stays in business.

1. Control Applications on Your Network

Employees in all industries are turning more and more to the web to communicate, share files, interact with blogs, etc. Retail businesses are no exception. Facebook, Twitter, Hotmail, YouTube, MSN Messenger – there are hundreds and hundreds of these web applications. While some are useful, many are non-productive and all of them can potentially carry threats. Web apps pose unique security problems for your network because they allow users to interact and exchange data via online tools that bypass traditional network controls. To a conventional firewall, it just looks like regular web traffic.

You Need Granular Control That Is Easy to Manage

Outright blocking of every web application is possible, but problematic. True, these apps are notoriously unsecure – but there are concrete business reasons to allow some types of access.

For example, your business may maintain a presence on Facebook, which has over 500 million active users worldwide,[8] as a way to reach out to customers. The sheer size of the social network makes it an attractive, low-cost marketing vehicle. You can't completely block Facebook on your network if you need to maintain a Facebook page. What you require is a solution that allows fine-grained control over which applications your employees can access. With WatchGuard Application Control[9] protecting your network you can easily define by domain, group, or individual user who may use Facebook.

WatchGuard Application Control extends this granular control over more than 1,800 web and business applications, managed from an easy-to-use centralized console that organizes applications by categories and

IS IT SAFE FOR RETAIL TO SKYPE?

Around 37 percent of businesses use Skype to communicate and conduct video conferences.[10] It's free, feature-rich, and easily accessible. But Is it safe for your employees to use?

- Instant messaging with Skype can be a source of malware and spam
- File transfer could be a source of infection from viruses
- File transfer could be used to transfer sensitive data outside the organization
- Idle chat and calls could become major productivity issues

To block or not to block – that's the business owner's dilemma.

WatchGuard Application Control lets you move beyond the restrictive "on or off" option. It allows you to actually control Skype on your network to take advantage of the technology when it makes good business sense and disallow it when it doesn't.

[8] Facebook: Facts & Figures For 2010, March 22, 2010, DigitalBuzz blog, http://www.digitalbuzzblog.com/facebook-statistics-facts-figures-for-2010/

[9] For more information about WatchGuard Application Control read "Take Back Control: Increase Security, Empower Employees, Protect the Business" at https://www.watchguard.com/tips-resources/whitepapers/application-control.asp?t=freg

[10] "Skype By the Numbers" Gigaom, April 20, 2010, http://gigaom.com/2010/04/20/skype-q4-2009-number/

subcategories for simple setup and quick configuration changes as your usage policies are refined.

For the Facebook example above, your IT administrator could easily drill down with a few clicks in the Application Control "social media" category, select Facebook and grant access only to the marketing team, but disallow the use of time-wasting Facebook games and chat with just a few more clicks into the subcategories. With steps as simple as these, you can finally begin to take back control of your network.

2. Keep the Bad Guys Out of Your Inbox

When it comes to spam the sheer volume is staggering, with billions of emails per day, accounting for 89 percent of all email sent worldwide.[11] Some think of spam as a vast nuisance that clogs networks and wastes time, but a far greater problem is the pervasive risk of attack.

As a delivery mechanism, spam is utilized by attackers several ways.

- **Malware can be contained within the message itself.** For example, an email might include an attachment that, if opened, launches a network intrusion, or a malicious program might be initiated simply by opening an HTML email message.
- **Spam messages can be free of malware but contain embedded URLs.** Clicking these links takes unsuspecting users to malicious web sites where drive-by downloads await.

What's a Drive-by Download?

"Drive-by downloads" are triggered by visiting an infected web site where malicious software automatically downloads and installs on the victim's computer. This happens in the background without the victim's knowledge. The infected computer then becomes host to malware that might be designed to steal data, log keystrokes, or even launch more spam attacks via the victim's network.

The Solution

If you can prevent malicious messages from entering your network in the first place, then you never have to deal with the serious consequences of a successful exploit.

WatchGuard provides exceptionally strong anti-spam technology to keep the ceaseless barrage of messages at bay. WatchGuard products have tools that block nearly 100 percent of unwanted emails, recognizing and stopping spam regardless of the language, format, or content of the message – even image-based spam that other anti-spam products often miss. This takes the heat off your email servers by stopping spam and email-borne threats at the perimeter of the network. It provides the solid protection your business needs, while saving you from the burden of processing massive amounts of unwanted email.

EMAIL STATS AT A GLANCE

Tallied at the close of 2010, these statistics show why email has so much appeal for cyber crooks.

- **294 billion** – Average number of email messages sent per day
- **262 billion** – The number of spam emails per day
- **1.88 billion** – The number of email users worldwide
- **480 million** – New email users since the year before
- **2.9 billion** – The number of email accounts worldwide
- **25 percent** – Share of email accounts that are corporate

(Source: Venture Beat Jan 2011)

[11] "2010: the year in internet stats," Venture Beat, January 12, 2011, http://venturebeat.com/2011/01/12/2010-the-year-in-internet-stats/

Why Reputation Matters

One of the highly effective tools that WatchGuard uses to stop spam is its Reputation Enabled Defense. Reputation Enabled Defense gathers data from millions of global sources and deployed systems worldwide, including major anti-virus engines, to identify spam in real time. Its sophisticated next-generation technology analyzes the risk level of incoming email, blocking upwards of 95 percent of spam before it enters the network.

This innovative "in the cloud" anti-spam engine examines sender information and content, including attachments and embedded URLs. It automatically conducts contextual analysis of message traffic to determine the message's safety score for highly intelligent protection.

Bad emails are detected and blocked immediately. Suspect mail is directed to a secure spam quarantine where users can manage their quarantined messages, safe lists, and block lists from an easy-to-use interface for maximum flexibility.

Reputation Enabled Defense is a "connection level" block. Many anti-spam solutions that don't have a dynamic reputation authority like WatchGuard's have to let your email server receive and start processing the spam email before the solution can analyze it and decide whether or not it's spam. While these solutions may eventually block the unwanted messages, your email server still has to use resources for partially processing that email. Reputation Enabled Defense blocks spammer addresses at the FIRST packet, before an email connection is even complete. That means that not only is spam stopped, but your email server does not need to waste resources processing spam.

3. Tighten Web Security

There are more than 255 million web sites now with 21.4 million added just last year.[12] The number of malicious web sites has increased 111.4 percent, with 79.9 percent of the infected web sites identified as legitimate sites that have been compromised.[13] The web has become the primary attack vector for distributing malicious code. This is a precarious situation for merchants attempting to do business in an online environment. Good web security is a must.

"Web security" is actually a blanket term that includes a variety of network defenses. After all, the web is a big place; good web security has to cover a lot of territory. Below are three important security capabilities that retail businesses should layer on to have the level of web protection they need.

- **URL Filtering**
  Unlimited web access can greatly impact productivity in the workplace, and inappropriate web surfing can violate acceptable use policies and lead to lawsuits. Above all, unfettered web access opens the network to attack. Keep in mind, there's a strong correlation between sketchy web

[12] Venture Beat http://venturebeat.com/2011/01/12/2010-the-year-in-internet-stats/

[13] State of Internet Security, http://community.websense.com/blogs/websense-features/archive/2010/02/04/websense-security-labs-report-state-of-internet-security-q3-q4-2009.aspx

content and risk. For instance, researchers have repeatedly found that sites with sexually explicit content are the number one web site category most likely to include malware.[14]

WatchGuard makes it easy to block whole categories of unacceptable content types. With a few clicks of the mouse IT administrators can choose from a menu of web categories to select the type of content they deem inappropriate or unsafe. Behind the easy-to-use interface is a continually updated database of tens of millions of global sites so your network has far-reaching coverage.

- **Incoming Web Content Filtering – Help from "The Cloud"**
  The same powerful cloud-based engine that WatchGuard uses to stop spam also protects users from malicious web pages, with the added bonus of dramatically reducing web processing overhead. WatchGuard's Reputation Enabled Defense provides real-time, dynamic web protection, scanning web pages for hostile content, and harnessing millions of continuous updates to the global web reputation database to keep your network safe.

  Because bad web traffic is identified and stopped at the network perimeter, your retail business not only has stronger web security but faster web performance as well. The typical savings in web processing overhead can be 30 to 50 percent, resulting in faster browsing times and greater throughput at the gateway.

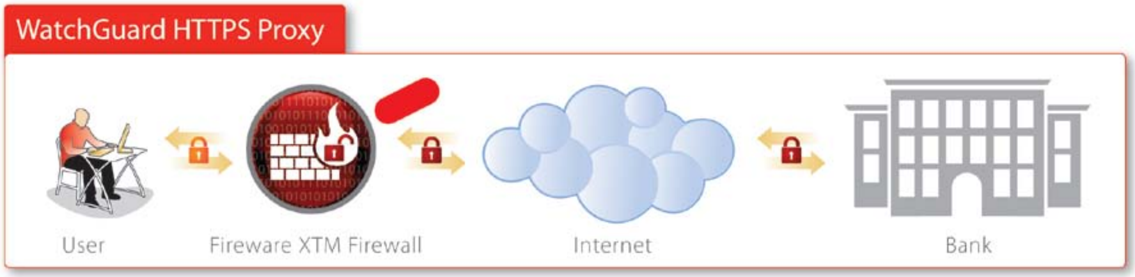
- **HTTPS Inspection**
  Regular web traffic flows over HTTP. Attackers have learned to hide their activities by cloaking them in HTTPS, which is the encrypted form of web traffic.[15] Most firewalls can inspect regular HTTP traffic, but strong web security demands HTTPS inspection as well.

  When a user behind a typical firewall requests encrypted data from an HTTPS web site, that data – whether it's safe or dangerous – is returned to the user's network fully encrypted. Because the firewall cannot see what's inside this encrypted traffic, it enters the network regardless of its payload. That's what cyber criminals are counting on.

  WatchGuard firewalls have full HTTPS inspection via HTTPS proxy technology. That means HTTPS traffic is briefly decrypted once it enters the firewall and inspected for anomalies. If anything compromising is discovered the traffic is immediately dropped. If it passes the security inspection it is re-encrypted and passed to the user. The user's communication remains confidential, while the network has an additional layer of protection from encrypted threats.

[14] Help Net Security http://www.net-security.org/secworld.php?id=10438&utm_source=feedburner&utm_medium=email&utm_campaign=Feed%3A+HelpNetSecurity+%28Help+Net+Security%29

[15] HTTPS is a combination of regular Hypertext Transfer Protocol (HTTP) with the SSL/TLS protocol to provide encrypted communication and secure identification of a network web server. HTTPS connections are often used for payment transactions on the web and for sensitive transactions in corporate information systems. http://en.wikipedia.org/wiki/HTTPS



F

Figure 3: HTTPS traffic flowing between a banking establishment and a user through a WatchGuard firewall, where encrypted traffic is decrypted to scan for malware.

The figure above shows the path of HTTPS traffic with a WatchGuard firewall. Its HTTPS inspection works on both incoming and outgoing traffic, and inspects not only packet headers but also payload (body content). The firewall can also be configured to apply additional gateway anti-virus and intrusion prevention services against the HTTPS traffic once it has been decrypted for even greater levels of protection.

4. Protect Your Data in Motion

Retail businesses must be on constant guard against customer data being lost or stolen. When PCI DSS was first mandated, merchants were mainly concerned about shielding their data from outside attacks, but today a thorough defensive strategy includes protecting data from the inside, as it attempts to leave the network.

Sensitive information enters and exits retail networks every day and in more ways than you might realize. It's not just about what travels via corporate email accounts anymore. Employees may be using popmail accounts such as Hotmail and Gmail, which allow them to communicate directly with the web. They may access file sharing and social networking sites, wikis, and blogs where sensitive data, whether accidentally or maliciously, can be posted.

WatchGuard provides in-depth data loss prevention (DLP) to prevent unauthorized confidential data from exiting the network. This DLP solution can comprehensively monitor all web and email traffic – including what is being sent, to whom, and where – to ensure outgoing communications are in strict accordance with your business's policies. This includes scanning attachments.

WatchGuard's XCS product line has next-generation DLP technology that enables tight policy management, while automating monitoring and remediation actions. You can efficiently set policies on the data that is allowed to cross network boundaries, using pre-defined policies – including a PCI DSS dictionary – that are easily customized to reflect your specific business requirements. You can also specify the action to be taken if a policy violation is detected, including block, allow, blind copy, quarantine, and encrypt.

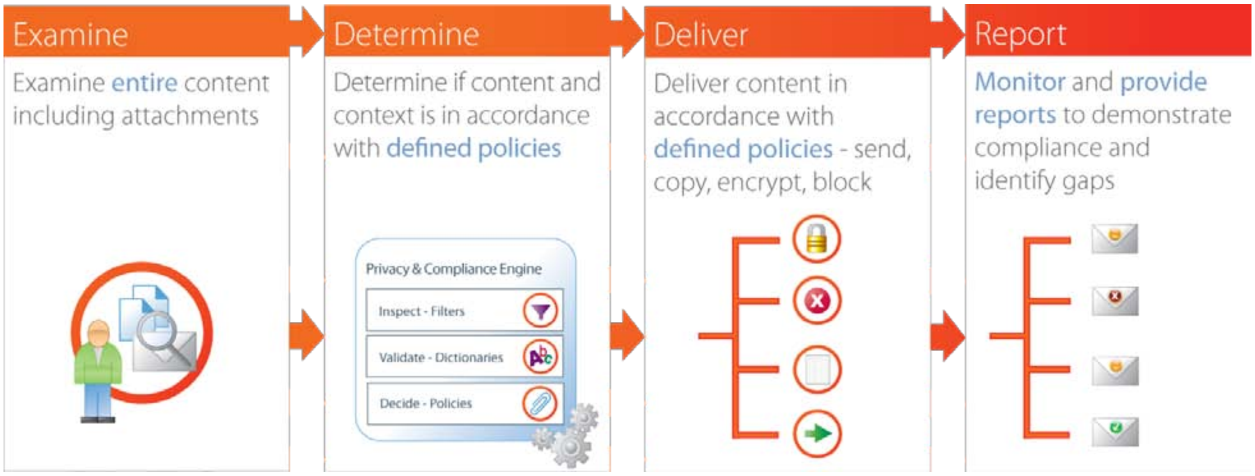

Examine
Examine entire content including attachments
Determine
Determine if content and context is in accordance with defined policies
Privacy & Compliance Engine
Inspect - Filters
Validate - Dictionaries
Decide - Policies
Deliver
Deliver content in accordance with defined policies - send, copy, encrypt, block
Report
Monitor and provide reports to demonstrate compliance and identify gaps

Figure 4. Integrated Process for Privacy and Compliance Protection

For example, you could set a policy that only your finance department can send credit card information out of the network, and further stipulate that if the credit card information has not already been encrypted, the WatchGuard solution will encrypt it automatically before sending. The same policy can be applied to both email and web traffic for efficient company-wide policy management and comprehensive data loss prevention.

5. Stay Up to Date with New PCI DSS 2.0 Regulations

The retail sector has come a long way since the major credit card companies mandated PCI DSS compliance back in 2004. Not all merchants have been in agreement over the regulations, but the fact remains – PCI DSS is here to stay and partial compliance is not an option. Being a successful merchant in today's world goes hand-in-hand with aligning your business to PCI DSS.PCI DSS was designed to protect consumers, credit card companies, and web site owners who host online payment services from credit card fraud, but it also helps set the standard for a solid security posture to ensure business continuity for the retail organizations themselves. PCI DSS 2.0 should be viewed as a continuation of industry efforts to make the Internet a safe place to do business.

Overview of PCI DSS

The Payment Card Industry describes the PCI Data Security Standards as "…a set of comprehensive requirements for enhancing payment account

CAN CUSTOMERS TELL IF YOUR RETAIL BUSINESS IS PCI COMPLIANT?

PCI compliance is mandatory for any business worldwide that accepts credit card payments from American Express, JCB International, Discover Financial Services, Visa Inc. or MasterCard Worldwide.

Compliance, therefore, is an assumption that your customers make every time they are given the option to use credit cards on your site. If your web site accepts credit cards it means – or is supposed to mean – that you have met the requirements.* This is an implicit trust relationship between consumer and retailer that a savvy merchant would never want to jeopardize.

*If you weren't compliant, you would be sending customers to a third-party processing service such as PayPal to complete the actual transaction.

data security." PCI DSS was developed by the founding payment brands of the PCI Security Standards Council: American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc. International. The goal was to help facilitate the broad adoption of consistent data security measures on a global basis.

PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design, and other critical protective measures. This comprehensive standard is intended to help organizations proactively protect customer account data. Anyone who accepts a credit card as payment is referred to as a "merchant" in PCI parlance, and is subject to all PCI rules.

Basic PCI DSS Requirements

PCI DSS comprises 12 requirements for "minimum" security measures
to protect against electronic and paper theft of cardholder data. The requirements are organized below into six main control objectives, mapped to the components associated with network security.

1. **Build and Maintain a Secure Network**
   - Requirement 1: Install and maintain a firewall configuration to protect cardholder data
   - Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters
2. **Protect Cardholder Data**
   - Requirement 3: Protect stored cardholder data
   - Requirement 4: Encrypt transmission of cardholder data across open, public networks
3. **Maintain a Vulnerability Management Program**
   - Requirement 5: Use and regularly update anti-virus software
   - Requirement 6: Develop and maintain secure systems and applications
4. **Implement Strong Access Control Measures**
   - Requirement 7: Restrict access to cardholder data by business need-to-know
   - Requirement 8: Assign a unique ID to each person with computer access
   - Requirement 9: Restrict physical access to cardholder data
5. **Regularly Monitor and Test Networks**
   - Requirement 10: Track and monitor all access to network resources and cardholder data
   - Requirement 11: Regularly test security systems and processes
6. **Maintain an Information Security Policy**
   - Requirement 12: Maintain a policy that addresses information security

There's No Such Thing as "Certified PCI DSS Compliant"

Where firewalls are concerned, there is no product that is going to be "certified PCI DSS compliant." It's just a myth. Any network firewall, and by extension a next-generation firewall or unified threat management (UTM) appliance that combines a network firewall with other features (such as anti-virus and intrusion prevention services), can be a part of *becoming* compliant, but it's only going to cover a certain portion of the compliance requirements.

Maintaining the PCI Zone

For companies seeking PCI DSS compliance, it is important to design a network with appropriate physical and logical boundaries to segregate the PCI-compliant operating environment; what the requirements have described as the "PCI Zone." This is a separate network zone or VLAN separating and protecting systems that store, transmit, or process cardholder data.

To this end, the strong segregation capability available with multiple, port independent interfaces of the WatchGuard® XTM family of appliances is ideally suited to meeting these requirements.

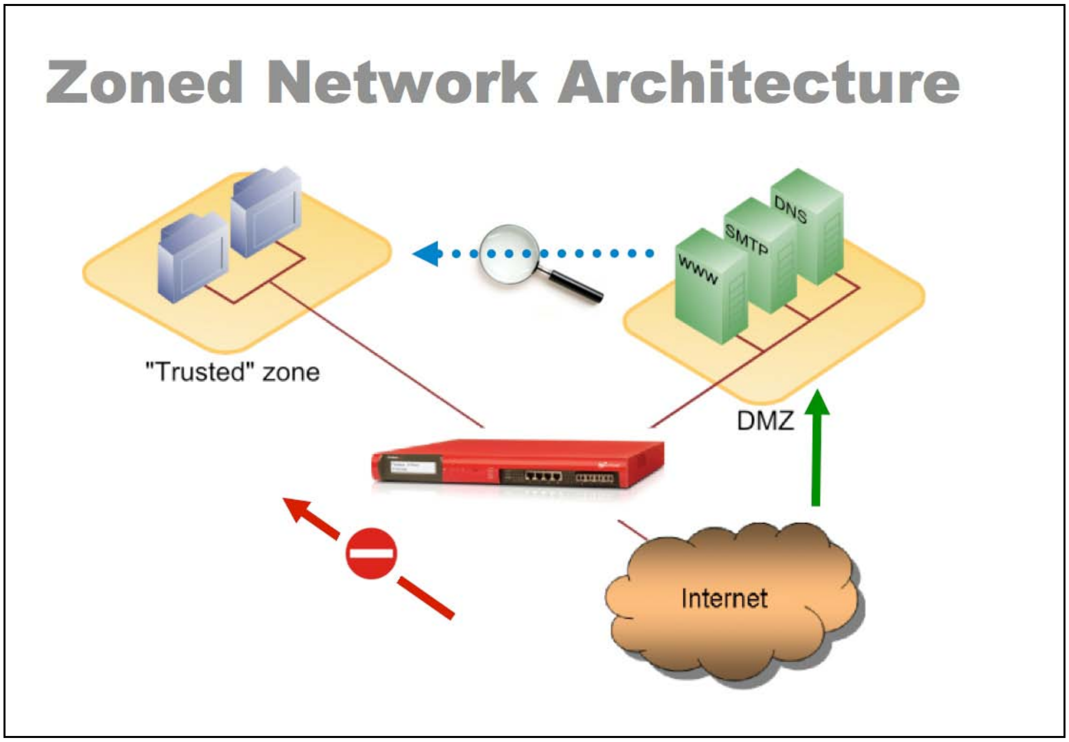


Figure 5: WatchGuard XTM Zoned Network Architecture

All WatchGuard XTM appliances support the zoned network architecture for creating a Demilitarized Zone (DMZ), as required by PCI DSS. In this architecture, only the servers contained within the DMZ are accessible from the Internet, and the cardholder data is contained within the Trusted network zone.

WatchGuard application proxy technology provides detailed control over the traffic that passes between zones, which is also required by PCI DSS. This enables administrators to block all traffic by default and to define which traffic is allowed to pass from one zone to the next, including protocols, ports, and content type. Via this architecture, communication between the Trusted zone and the Internet can be completely prohibited, and those between the Trusted and DMZ zones can be strictly limited to traffic that meets PCI DSS and corporate communication requirements.

For instance, WatchGuard XTM 5 Series appliances have seven independent ports. This allows IT administrators to segment six different internal networks (the seventh would be the Internet). In addition, WatchGuard supports VLAN tagging, which further helps segment your network beyond the physical interfaces.

Besides supporting the required network architectures, there are strong logging, monitoring, and auditing components required by PCI DSS, all of which are supported by WatchGuard XTM appliances. In addition, the security subscriptions available for XTM appliances – including Application Control, Reputation Enabled Defense, Gateway AntiVirus, Intrusion Protection Service, WebBlocker, and spamBlocker – are a perfect complement to PCI DSS standards.

Data Loss Prevention and Remediation

It is well-documented how compliance violations, unauthorized data losses, and privacy leaks cost merchants time and money. With WatchGuard XCS, your organization can protect data-in-motion losses and leaks with powerful data loss prevention capabilities integrated into all WatchGuard XCS appliances.

WatchGuard XCS is positioned on the corporate network in front of the corporate email server(s). Messages are forwarded from the email system to the WatchGuard platform for inspection and processing before leaving the organizational boundary. When specified data patterns or filtering rules are triggered, messages can be automatically encrypted, blocked, or quarantined, without user intervention.

WatchGuard XCS includes several regulatory-specific, customizable dictionaries (or lexicons), including one for PCI, that specifies commonly encountered cardholder data patterns. Filters can be customized to trigger actions based on message attributes such as recipient, sender, or subject. The policies are highly flexible, allowing the merchant to weight certain words, and to create specific policies with thresholds that, when exceeded, will trigger a variety of actions. In addition, policies can be tied to groups of users.

For example, a policy can be created that dictates that no Excel attachments can be sent out of the organization, except by Finance users. When a Finance user sends an Excel file it will automatically be encrypted if it contains sensitive information such as social security numbers or cardholder information.

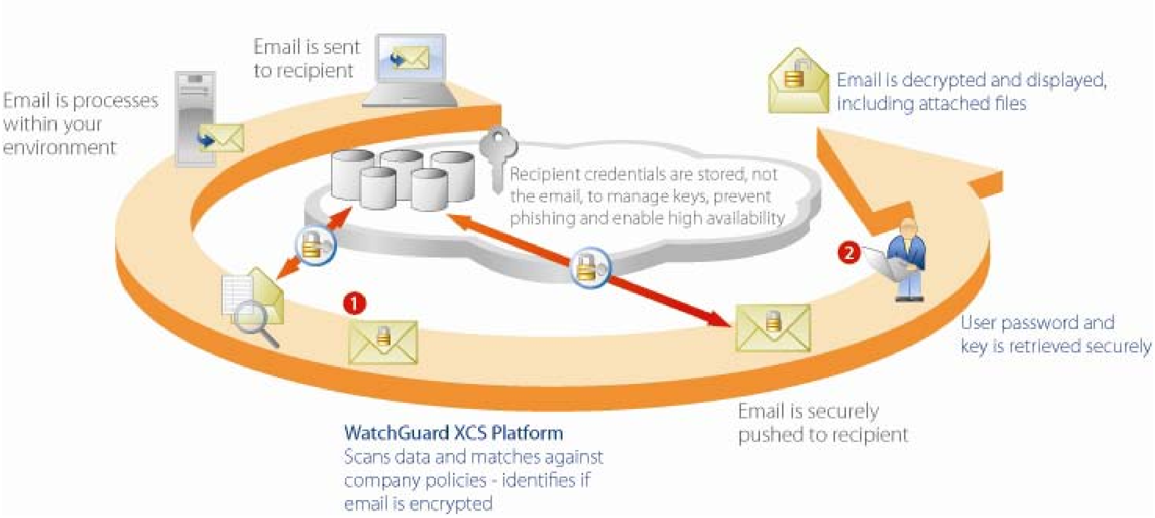

Email is processes within your environment
Email is sent to recipient
Email is decrypted and displayed, including attached files
Recipient credentials are stored, not the email, to manage keys, prevent phishing and enable high availability
1
2
User password and key is retrieved securely
Email is securely pushed to recipient
WatchGuard XCS Platform
Scans data and matches against company policies - identifies if email is encrypted

Figure 6: Process Flow for the WatchGuard XCS Encryption Function

What's New in PCI DSS 2.0

As of January 1, 2011, all merchants worldwide that process credit card transactions are expected to be compliant with PCI DSS 2.0.

A 2010 year-end survey of 1,500 retailers with 50 or more stores revealed that over 63 percent of respondents were partially or even completely unaware of the specifics of the new requirements.[16] This may be because, as expected, 2.0 is mostly a clarification of the existing standards.

As the PCI DSS Security Standards Council explains, modifications in 2.0 are relatively straightforward and do not introduce significant change. This, they say, reflects the growing maturity of the standards as a strong framework for protecting cardholder data.[17]

Whether the changes are small or not, as a merchant you are still responsible for implementing all PCI requirements. If you haven't already aligned your security programs with the new 2.0 standards, you are at risk of incurring fines, potentially hurting your brand and losing the confidence of your customers.

WatchGuard can help your retail business meet the latest PCI standards in several ways.

11.1 Detect Unauthorized Wireless Access Points

This change, which the PCI Security Standards Council refers to as "additional guidance" clarifies that a process should be in place to "detect unauthorized wireless access points on a quarterly basis."

[16] "Lack of awareness for PCI DSS 2.0," Help Net Security, December 15, 2010 http://www.net-security.org/secworld.php?id=10314
[17] PCI Security Standards Council, https://www.pcisecuritystandards.org/

WatchGuard’s line of XTM 2 Series wireless appliances include a wireless radio that can be set to scan for unauthorized access points within range and report on them. Because the appliance can generate logs, alerts, and reports based on the scan, you have the information you need to show compliance with the 11.1 requirement.

11.4 IPS Enhancement

Although not new to PCI, requirement 11.4 clarifies that intrusion detection /intrusion prevention systems (IDS/IPS) monitor traffic at the perimeter and at key points inside the cardholder data environment (CDE), rather than all traffic in the CDE.

This means that an organization must now have IDS/IPS between internal subnets, which is something that all WatchGuard XTM appliances are capable of. As part of the zoned network architecture described on page 13, WatchGuard solutions provide this level of security between any of our port-independent subnets. For example, if you segment your engineering network from your accounting network using different interfaces, you can also apply WatchGuard IPS to traffic between those two internal networks, not just to Internet-based traffic.

5.4 Audit Logs

This requirement clarified that anti-virus mechanisms should be generating audit logs, rather than just being “capable of generating” such logs.

All WatchGuard XTM appliances offer centralized logging, and log all IPS and anti-virus events to the same log file. IT administrators can have one log of activities no matter how many appliances are included in the deployment. Since all our security services log to the same place, you can easily find/audit all security events using one convenient, searchable, and filterable tool. What’s more, WatchGuard’s proprietary logging channel is TCP-based for reliability, and encrypted for security.

This section on PCI DSS is only a brief look at the objectives and top line requirements of the PCI DSS mandates. For specific details on how you can achieve PCI compliance with WatchGuard network security solutions, download these free white papers[18] from the WatchGuard web site:

PCI Requirements Mapping WatchGuard XCS Secure Content & Threat Management

Meeting PCI DSS Merchant Requirements with WatchGuard® XTM

CONCLUSION

Retail businesses don’t have to let the latest web applications put their network s in danger, allow web surfing to squander work hours, lose confidential data, or permit malware to enter the network via spam. WatchGuard offers network security solutions that control applications, filter URLs, block spam, prevent data loss and more to keep your business safe and in compliance with PCI DSS mandates.

[18] These white papers and more are at www.watchguard.com/whitepapers

Find out more about WatchGuard network security solutions at www.watchguard.com, or contact your local reseller, or call WatchGuard directly at 1.800.734.9905 (U.S. Sales) or +1.206.613.0895 (International Sales).

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

WEB:
www.watchguard.com

U.S. 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.

No express or implied warranties are provided for herein. All specifications are subject to change and any expected future products, features, or functionality will be provided on an if and when available basis. Part No. WGCE66727_022511