White Paper

Retail Security: Protect Customer Data While Saving Money and Time

What You Will Learn

Retail IT environments face an unprecedented level of technological change. Stores have more requirements, and customers expect both performance and security when using in-store services. Retail organizations also face organized and well-funded hackers that prey on any weakness in networks and point-of-sale (POS) systems. The unfortunate result of many attacks is the theft of credit card and other customer data.

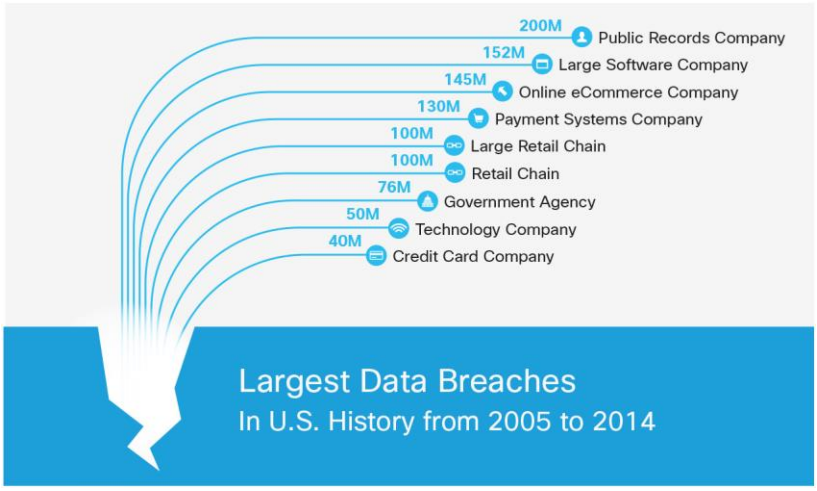
This white paper summarizes the challenges that retail networks are confronting and describes a Cisco® security solution that provides effective, up-to-date, dependable protection: Cisco Cloud Web Security (CWS).

Threats to Retail IT Environments Increasing

Bringing in-store networks up to the required performance and security capabilities is not a trivial task. From simple control over in-store Internet access to the complex compliance requirements of the Payment Card Industry Data Security Standard (PCI DSS), retail organizations must think proactively about how to control network traffic. An effective security solution must provide network control at the same time that it adapts to the accelerating velocity of change for in-store networks. Most importantly, it must adapt to the increasing complexity of the threat landscape.

The rate of high-profile attacks and breaches in retail IT environments continues to increase despite the efforts of industry and security professionals. Victims range from Fortune 10 retailers to global franchise restaurants (Figure 1). Attackers consistently target payment systems. These breaches have resulted in damage to company brands and customer confidence along with mitigation and restitution efforts that sometimes total hundreds of millions of dollars.

Figure 1. The Largest Data Breaches in U.S. History (Based on Cost of Attacks)



Sources: Bloomberg, Privacy Rights Clearinghouse, Breach Level Index

In-store guest Wi-Fi and interactive mobile shopping experiences have led to an increase in new offerings such as shopping apps and in-store network access. Although these in-store services can provide demonstrable customer value, they also increase the complexity of store networks and add more pressure to existing IT resources. The online services expand the attack surface, leaving businesses more exposed to those who search for and prey on network vulnerabilities. It is therefore important for retailers to invest in protecting customer data both within stores and at headquarters.

Another IT trend that retailers must manage is the Internet of Things (IoT). The IoT represents a network of physical objects connecting to the Internet through embedded technology, interacting with both the internal network and the external environment. For example, a retailer could push relevant real-time information about products to the mobile devices of interested consumers based on contextual customer information gathered from merchandise within the store.

Other IoT business applications include tracking inbound inventory in real time by using RF tags or providing supply-chain vendor access to internal systems and data in order to expedite operations. The wide range of devices in the IoT will increase the number of critical technologies within the store itself. In many cases, security is not built into these devices, and it might be added only as an afterthought.

Given the challenging profit margins across the retail industry, organizations face the harsh reality of tackling the ever-evolving threat landscape while at the same time providing innovative, personalized shopping experiences to customers. It is increasingly necessary to upgrade POS systems or to invest in security technologies to control the risk of data loss. In response to the growing threat environment, the retail industry is not standing idle. Organizations have recently banded together to develop the Retail Cyber Intelligence Sharing Center (R-CISC) initiative.

The Retail Weak Spot

In 2013, retail organizations and restaurants were the second most attacked industry, according to the 2013 Verizon Data Breach Investigations Report. Even if customers do continue shopping at a retailer that has been breached, a report by Retail News Insider in 2014 suggests they might begin to use cash instead of credit, which leads to a decrease in spending.

According to a 2014 report by Interactions Consumer Experience Marketing, evidence shows that attackers are not that creative when targeting retail organizations. “Compared to other industries, attackers used relatively few methods to get the data when attacking retail organizations,” the group found. In retail attacks, 97 percent involved payment system tampering.

Retail organizations face a large challenge in detecting security breaches. Typically, malicious malware sits in the retail IT environment until a third party (typically law enforcement or fraud detection) finds indicators of unusual activity. According to a three-year study by Verizon Enterprise Solutions quoted in a 2014 Bloomberg Business week article, companies discover breaches through their own monitoring on average only 31 percent of the time. For retailers, it’s 5 percent.

Table 1 shows four examples of the largest breaches reported in 2014, along with how much time the malware sat in the IT environment before discovery.

Table 1. Characteristics of the Largest 2014 Network Breaches

Attack	Length of Time	Attack Method	Point of Failure
U.S. liquor store	17 months	"Low-and-slow malware"	Technology
U.S. and Canadian craft store chain	8-9 months	Modified POS systems	Process
U.S. and Canadian home store chain	6 months	Custom malware designed to evade detection and attack registers	Security not a priority; unused product features
Online retail exchange	3 months	Hacked database	People and technology

Sources: Sophos, Bank Information Security, Krebs on Security, Bloomberg News, Private WiFi.com, and the Huffington Post

Capabilities and Functional IT Requirements Increasing

Retail IT network environments are becoming more complex. And they are becoming more complex to manage. In the IT industry, a growing skills shortage compounds the difficulty of dealing with these in-store Internet-connected environments. To combat the scarcity, especially in cybersecurity, IT groups centralize the management and operation of the retail IT environment.

One of the most challenging areas of complexity exists within in-store networks initially used to connect point-of-sale (POS) terminals to back-end servers and the corporate WAN. These in-store networks, intended to handle little traffic, now serve many other applications, including marketing, intranet and Internet access for employees, IoT use cases, alarm and video surveillance systems, and guest Wi-Fi.

More compelling technology will constantly come online for retailers, providing incredible value for customers and making them "must-haves" for retailers to deploy in their stores. At the same time, these solutions will consume more bandwidth and require more data processing. Further complicating matters is the difficulty in predicting bandwidth requirements that vary from facility to facility. These requirements not only depend on the size of each store but also on the use of various technologies.

The security model of most in-store networks was initially built to protect internal network traffic. Stores now support communications outside the home network, including connections to business partners, vendors, and the Internet.

Providing adequate security will require that organizations deploy new preventive and detective controls on in-store networks that can provide more sophisticated network-level segregation of devices and users, advanced network-use controls, and acceptable-use policy enforcement. Given the kinds of malware and attacks being seen in the retail industry, it is understood that all the devices connected to retail networks run in a hostile environment.

How can the threat environment be defined? Primarily, attackers target the path of least resistance to gain a foothold in an environment. This typically includes a focus on POS terminals. Unfortunately, many of the leading POS systems are built with commodity hardware, operating systems, and software components that are easily compromised using unsophisticated attacks. Even if the POS vendors properly patch the systems, the operational cost of patching hundreds of thousands of devices is significant and typically requires manual updates.

The traditional connections of POS systems to the public Internet invite risk. Such a setup makes remote operations possible, where the POS back-end systems are located in a different facility and where remote support can be provided. However, operational groups must choose between streamlining management of the devices and reducing the risk of network-based attacks. This is not a fair or necessary trade-off.

Traditional web security gateways require the installation of a centralized gateway in the head office. Each store or branch forwards all traffic to the central aggregation point for inspection before going out to the Internet. Given the increased traffic (both inbound and outbound) at stores, this approach consumes large amounts of the limited bandwidth. Compliance is also a significant factor to consider, as retail IT remains within the scope of the PCI DSS. To comply with the regulation and pass annual assessments, organizations need to implement proactive network controls to protect connections and help ensure the ongoing security of systems that process cardholder data.

In summary, in-store networks have commonly been built with the singular purpose of connecting POS systems to the corporate WAN. These solutions were typically deployed inside the security perimeter of the organization. Recent security breaches in retail organizations involving POS systems suggest that this network architecture is no longer viable for building or operating in-store networks.

Common Gaps in IT Environments

Due to the time-critical pressures on retailers to address security issues, retail organizations commonly assume that a point solution will protect important assets. However, a cohesive security model must provide more than a point solution and must implement sufficient network security controls to meet both today's problems and tomorrow's requirements.

The difference between a point solution and a comprehensive security solution is exemplified by the deployment of direct Internet connectivity to the stores. When a direct Internet connection is deployed, a new firewall is added to protect the store network. The firewall is deployed in one of two models.

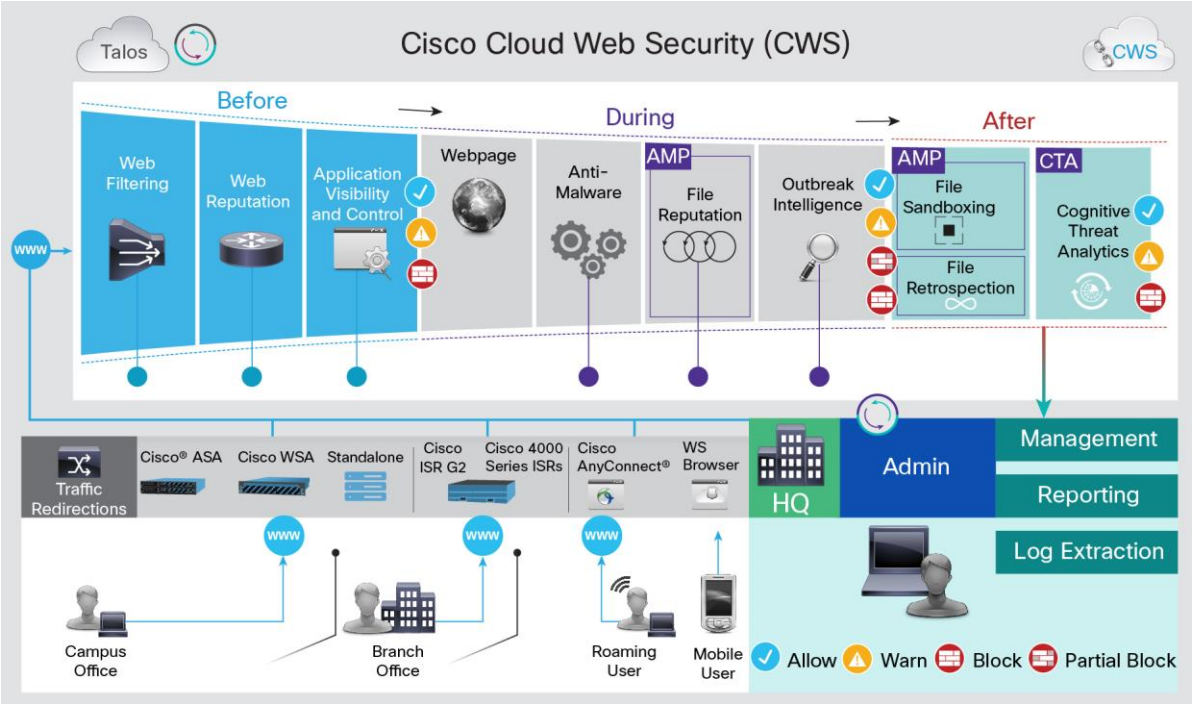
1. Rules can be set in the WAN router to transfer Internet-bound traffic to the new firewall.
2. The in-store network-connected devices can use the firewall as the default gateway, thus removing control or monitoring of the network. When deploying in-store Wi-Fi connectivity, if the traffic is not routed correctly to an inspection point, there is no way to ensure corporate data does not leak to the Internet. Furthermore, there is no assurance that acceptable-use policies are followed continuously.

Overall, a patchwork of point products creates a situation where the real risk to the organization is not easily controlled, seen, or managed.

Threats to retailers have been making headlines for years, such as a major retail breach in 2006 that compromised the data of up to one million credit cards. Hackers exploited weak controls within the stores to gain access to credit card and other customer information. Once they find a vulnerability, attackers move laterally through corporate networks, further compromising private data.

Given the ability of hackers to share attack tactics and automate their attacks, they target large corporations through the weakest link in the chain, which often means a retail location with subpar controls.

Figure 2. How Cisco Cloud Web Security Works



Flexible Protection and Control

Cisco has developed a set of products and capabilities that address the security and networking needs of retail IT environments. These solutions range from wireless access points, routing, and switching to cloud-based advanced security services.

The market-leading Cisco Web Security Appliance (WSA) and Cisco Cloud Web Security (CWS) products offer flexible deployment models, providing both on-premises and cloud-delivered content security. Selecting Cisco WSA for network-level protection at headquarters while choosing Cisco CWS for branches satisfies IT security requirements while largely removing the need to buy new hardware for all the branches to increase protection. Integrating directly with in-store technologies, including Cisco Adaptive Security Appliance (ASA) firewalls,

Cisco Integrated Services Routers (ISRs), and the Cisco AnyConnect® client, Cisco CWS lets you use existing investments and operational support processes to gain increased protection and more efficient operational support.

Cisco moves the protection of Internet connections down to the store level without requiring any additional hardware and backhauling traffic only when dictated by policy. Low-risk traffic goes directly to the Internet, while other traffic is sent to the central location for further inspection.

To protect against both known and emerging threats, Cisco CWS looks for attacks using a variety of techniques, including traditional malware signatures as well as file and site reputation filters and outbreak filters. Additionally, Cisco CWS integrates with the Cisco Collective Security Intelligence (CSI), Cisco's industry-leading threat intelligence capability, which includes the Talos security intelligence and research group. Cisco CSI and Talos help ensure that customers benefit from the tens of thousands of customers using Cisco technology.

Cisco CWS offers reporting detail that includes traditional information security data, as well as a detailed analysis of bandwidth consumption and use. In bandwidth-constrained environments, this visibility is a critical tool toward achieving efficiencies. Another advanced reporting feature details guest Wi-Fi browsing habits, providing visibility into and protection against comparison shopping and price checking with online retailers, as well as the viewing of offensive content. Cisco CWS reporting capabilities thus have value not only for the IT security team but also for the overall retail organization.

Perhaps most importantly, as a cloud solution, Cisco CWS (Figure 2) provides easy scaling and optimization of bandwidth capabilities for any organization. This means direct, quantifiable cost savings and dramatic improvements in the effectiveness of an organization's in-store threat management capabilities. These savings are achieved by offloading all processing for traffic management and control from local hardware to cloud-based systems. Furthermore, by using a software-as-a-service (SaaS) model for delivering policy-based decisions on traffic, Cisco CWS significantly reduces the load on the in-store network hardware.

How Cisco CWS Can Help a Retail Organization

This real-world example shows how Cisco CWS can protect a retail organization from today's threat landscape: An IT security manager has been charged with protecting a 1,500-store chain that is rolling out in-store technology to provide Internet access for customers along with a variety of additional services. The security manager is aware of the recent spate of advanced malware attacks being used to compromise in-store systems (including POS devices) and wants these attacks to be detected quickly and remediated effectively. Compounding the challenges, many of the stores have limited bandwidth, and the solution must optimize network connections to each store.

The security manager deploys Cisco ISR edge routers in each store. These devices support Cisco Intelligent WAN (IWAN) capabilities to both protect and optimize the bandwidth at each store. IWAN can help manage bandwidth by using lower-cost Internet connections as opposed to more expensive private network links. The product also offers a graceful migration path so the organization can migrate from the private network links at its own pace. To make sure that mobile devices connect to the correct network in each store, the Cisco Identity Services Engine (ISE) protects the in-store systems, determining which users and devices can access which parts of store networks.

To protect web traffic, the organization will use Cisco CWS Premium for Direct Internet Access, which can be deployed through the Cisco ISR edge routers, requiring no additional hardware. Cisco CWS Premium contains Cisco Advanced Malware Protection (AMP) and Cognitive Threat Analytics (CTA) to protect all users through advanced threat defense capabilities. CTA is a near real-time network behavior analysis system that uses machine learning and advanced statistics to identify unusual activity on a network to detect possible attacks. AMP uses a combination of file reputation, file sandboxing, and retrospective file analysis to identify and stop threats that are already present in the network.

Using these Cisco security products, the 1,500-store chain can now manage its bandwidth usage, user access levels, threat defense, and content security. This is only one possible combination of Cisco security products. In this case, the IT security manager satisfies the business's network and security goals for its distributed retail network.

Cisco CWS Benefits

An organization using the integrated Cisco solution to protect its networks can enforce a common policy, detect advanced attacks, and optimize bandwidth use on the WAN. Cisco CWS Premium, integrated with the Cisco ISR edge routers, also makes botnet tracking possible. This helps ensure that POS devices are not compromised and can safely transfer data to headquarters. Additionally the organization will be able to increase its savings by bundling the solutions.

The organization doesn't need to worry about integrating the individual elements of the solution because all of the capabilities are designed to work together. The result is a savings to the IT staff that Cisco estimates can equal up to 40 percent of its time spent in reduced configuration and implementation support. The organization also benefits from a high, consistent level of security on its network worldwide, so it can continue to grow and focus on its business instead of worrying about attackers seeking to penetrate in-store networks.

Conclusion

Retailers can significantly decrease the operational load of monitoring, managing, and maintaining their networks using cloud-enabled tools like Cisco CWS. Working easily with Cisco ASA and Cisco ISR products, CWS intelligently offloads the need for local security policy enforcement, reducing the bandwidth requirements of each individual store. Acknowledged as a leader in the market by Gartner, Cisco CWS offers a smart way to add the most effective security capabilities to in-store networks without adding operational complexity.

For More Information

For more information, visit http://cisco.com/go/cws.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C11-733817-02 03/16