Cisco Stealthwatch for Retailers

Gain network security, visibility, and analytics

Customer trust is among the most valued asset of retailers. Yet a single cyber attack can send buyers rushing to the competition. According to KPMG, 33 percent won't return for three months, as these attacks draw big headlines and expose consumer credit card information.[1] Furthermore, down time and performance issues can significantly erode brand value and the bottom line.

Adding to retail leaders' concerns are distributed and complex networks with numerous Point-Of-Sale (POS), mobile, and warehouse devices. Multichannel operations intensify cyber risk, as does MPLS traffic that circumvents centralized monitoring.

Yet, deploying specialized security solutions in every store and location can be prohibitively expensive. Moreover, traffic flow and vulnerabilities are expected to increase with the growth of cloud-connected Internet of Things (IoT) technologies, including smart shelves, RFID trackers, and perishable-goods sensors.

Given this complexity, it's no surprise that retailers perceive cyber attacks as their greatest customer relations and revenue risk. Yet only half consider their infrastructure up to date and ready to protect against attacks such as malware, insider threats, Advanced Persistent Threats (APTs), Distributed Denial of Service (DDoS) attacks, and transaction fraud. And, a larger percentage feel ill equipped to maintain full PCI compliance.[2]

[1] "Consumer Loss Barometer Report," KPMG LLC, 2016

[2] Cisco 2017 Annual Cybersecurity Report

Cisco Stealthwatch helps retailers:

- Achieve 24x7 network traffic visibility
- Identify threats on the network
- Protect POS terminal and customer data
- Speed incident response
- Comply with regulations including PCI DSS

Retailer improves threat detection and lowers risk

A global retailer was concerned about visibility gaps in MPLS traffic between hundreds of worldwide locations, and feared an attack could spread before being contained locally. It needed context to identify suspicious activity in remote locations that bypassed centralized network monitoring, but its scale made distributed security prohibitively expensive. The retailer believed its customer data and consumer trust were at risk.

After deploying Cisco Stealthwatch, the company cost-effectively turned its network into a security sensor, using security analytics for early threat detection across the global enterprise. By leveraging its NetFlow-capable infrastructure, the retailer resolved flawed network configurations and bolstered its cybersecurity posture.

Network visibility and insight

Fortunately, security and IT teams in the retail industry can address their technology challenges with the network visibility and analytics provided by Cisco Stealthwatch™ technology and complementary security solutions. Together, these solutions enable a "security everywhere" strategy that leverages the network as a critical sensor and enforcer.

Cisco Stealthwatch provides retailers with the visibility to gain real-time situational awareness of activity across local and global network connections and to every device. Visibility is cost-effectively achieved by collecting NetFlow and other telemetry data from existing network infrastructure devices such as routers, switches, and firewalls.

The solution records and stores NetFlow data, which includes sender and receiver IP addresses, along with the time, date, and size of every network transaction. This insight is critical for obtaining a comprehensive view of network traffic, as well as additional context such as application-level awareness.

With metadata collected directly from retailers' existing infrastructure, Cisco Stealthwatch transforms the network into a powerful security sensor. Visibility scales across thousands of retail locations, points of presence, and e-commerce data centers without relying on expensive probes. And the solution monitors IoT and specialized network devices, in storerooms and shopping carts, that may not be compatible with endpoint-monitoring software.

Additionally, the Stealthwatch Cloud License allows retailers to extend visibility and threat detection to public, private, and hybrid cloud environments by deploying lightweight agents that collect telemetry from distributed locations.

“Stealthwatch gives us visibility into east-west traffic across the core and in the virtual environment ... [It] exposes ... shadow IT [and] misconfigurations.”

Large global retailer

“We have been able to quickly identify users with malware and spyware that could have been sending critical data out to the Internet.”

S&P 500 retailer

Security analytics and incident response

Cisco Stealthwatch transforms the volumes of collected telemetry from network infrastructure devices into actionable intelligence. Through the solution’s powerful analytics, security teams can rapidly identify and counter network attacks to help ensure the uptime of POS, e-commerce, and critical customer services.

With Cisco Stealthwatch, even the most evasive and sophisticated security incidents faced by retailers are quickly identified. And unlike traditional security solutions that may overlook persistent and targeted attacks, the solution does not rely on signatures to detect threats.

Instead, it builds a baseline of expected behavior from each network host and triggers alarms when anomalous activity is observed. If attackers or unauthorized users gain entry and perform unexpected or prohibited activities such as fraudulent transactions, POS, or DDoS attacks, the solution identifies the threat and alerts responders.

PCI compliance and forensic investigation

Cisco Stealthwatch provides continuous monitoring throughout a retailer’s network to help ensure every activity is logged, including all interactions with POS devices. Furthermore, it delivers the comprehensive visibility and analytics necessary to maintain and demonstrate compliance with the Payment Card Industry Data Security Standard (PCI DSS) v3.1, and the Payment Application Data Security Standard (PA-DSS) across physical and virtual networks.

For forensic investigations, the solution uses NetFlow to build a historic audit trail that inspectors can use to quickly uncover the underlying cause of an incident. If a security threat is detected, the operator can identify the point of infection and track its propagation within minutes.

“With Stealthwatch, we’ve had much more visibility into our environment; both ... when investigating an issue, and at a high-level view of overall status.”

S&P 500 large retailer

Advanced endpoint awareness with Cisco ISE

The Cisco® Identity Services Engine (ISE), a complementary security solution, helps address the challenges associated with retailers’ distributed networks through its highly secure network access and endpoint awareness.

When Cisco Stealthwatch is integrated with Cisco ISE, additional endpoint information, such as user, device, credentials, and security policy compliance, is woven into the network audit trail. Investigators can quickly identify the person and device type responsible for suspicious traffic.

Additionally, ISE simplifies a customer’s guest access with automatic registration and access limitations. When needed, ISE can quarantine users and devices from the network after Cisco Stealthwatch identifies a compromised endpoint, leveraging the network as a security enforcer. This capability helps prevent the spread of infection until the issue has been investigated and remediated.

When integrating Cisco ISE and Cisco TrustSec® software-defined segmentation with Cisco Stealthwatch, the combined solution dramatically reduces the network attack surface. Cisco TrustSec assigns a Security Group Tag (SGT) to each user and endpoint based on their role. Administrators can then develop and enforce dynamic and adjustable SGT-based policies to restrict users from accessing unauthorized resources without disrupting network availability.

Learn more

Together, Cisco Stealthwatch, ISE, and TrustSec can help retailers institute more secure and responsive networks that better protect their valuable customer data from today’s advanced threats. For further details on Stealthwatch, visit https://www.cisco.com/go/stealthwatch. To learn more about how to enable your retail network with Cisco, go to https://www.cisco.com/go/retail.

C22-739379-00 08/17