aruba
a Hewlett Packard Enterprise company

AT A GLANCE

MODERNIZING CYBERSECURITY IN RETAIL

Today's shopper is demanding – and willing to shift loyalty to another brand when expectations aren't met. Compacted by evolving shopping methods, retailers are challenged to not only attract customers, but retain customers.

Mobility driven experiences, many enabled through applications on smart phones, are becoming more common-place among small and large retailers alike, helping to attract and retain customers. Additionally, store associates are using smart devices and tablets to deliver exceptional customer service and enabling associates to help customers find the perfect item, answer questions, check inventory and even process and place orders without leaving the customer's side.

IoT is also playing a big part in evolving retail services and efficiencies. Video cameras, people sensors, building technology, and energy systems are transforming stores and in some cases, help to collect increasing amounts of data bout shoppers and their habits. Information about time spent in a store, what products shoppers view and purchase and a variety of other pertinent data can now be collected by wireless networks and IoT and delivered to retailers.

BROAD ATTACK SURFACE

Merchants want to take advantage of the productivity and efficiency benefits of mobility, but above all else, they need to protect their networks and their customers' sensitive credit and debit card data in order to meet compliance demands and safeguard their brand. Digital tools and cloud applications mean more security concerns. Before retailers can deliver experiences and benefit fully from the possibilities of mobility, they need a network that can go beyond connectivity that can securely and seamlessly addresses the needs of associates, smartphone-carrying customers, store operations and payment card industry (PCI)-compliance auditors.

CLOSING THE GAPS

Although retailers are increasing investments in cybersecurity, recent breach statistics suggest there are opportunities for improvement to stay ahead of threats.

Today, one in three retailers lose revenue over cyber-attacks, with 16 percent of companies tallying more than $1 million in losses. And while retailers recognize that they're a frequent target, only 52 percent feel their security infrastructure is up-to-date with the latest threats.

- CyberShark

Let's investigate how modern security solutions from Aruba can help retailers better:

- Gain visibility into everything connected to both wired and wireless networks
- Ensure that the appropriate IT access policies are applied to users and devices
- Ensure PCI compliance compromised insiders

ARUBA SECURE SOLUTIONS FOR RETAIL

Secure Infrastructure

For over 15 years, Aruba has delivered high performance networks that include many built-in security features.

- The newest Wi-Fi certified protocol WPA3™ was co-authored by Aruba experts and delivers a range of security and ease of use features.
- Secure boot delivers anti-tampering features for access points.
- Military grade encryption and VPN ensure traffic is secure.
- The Aruba Policy Enforcement Firewall (PEF) enables user/application visibility and policy enforcement based upon user, role, application, device and location.

ACCESS CONTROLS

Security starts with visibility of who and what is connected to your network and what they are doing on the network at all times.

- **Know What is on the Network**
  Today, many IoT devices are build on standard hardware platforms. That can make it extremely difficult to know exactly what is on your network. For example, a security camera and smart thermostat could both be built on the same Linux platform. ClearPass Device Insight uses machine learning to identify devices based on multiple attributes, traffic destination, and communication frequency. Knowing what is on the network is the first step in protecting it.
- **"Zero Trust" Access to the Network**
  Aruba ClearPass NAC (Network Access Control) delivers discovery, profiling, authentication and authorization of users, their devices and IoT devices before letting them on the network or giving them access to IT resources. These pre-admission controls are critical because cybercriminals are adept at quickly advancing and moving laterally within seconds after gaining access to a network.
- **Precise Control of Access to IT Resources and Assets**
  ClearPass provides adaptive, granular policy-based access controls by user, device, role and location, including for applications. These controls ensure that each user, device or IoT only has access to the network and IT resources and assets they are approved for, especially important when trying to ensure PCI compliance.
- **Intelligent Segmentation**
  Aruba Dynamic Segmentation leverages the Aruba secure infrastructure, PEF and ClearPass to deliver a network edge that securely connects and automatically partitions user and device traffic across wired and wireless networks based upon policies.

NEXT STEPS FOR A HEALTHIER SECURITY POSTURE

With advanced access controls and interoperability with over 140 multi-vendor network and security solutions, you can rest assured with the visibility and confidence that your security posture is in a much healthier state.

LEARN MORE

- https://www.arubanetworks.com/assets/wp/WP_PCIDSS.pdf
- https://www.arubanetworks.com/solutions/retail/
- https://www.arubanetworks.com/solutions/security/

aruba
a Hewlett Packard Enterprise company

AAG_SecurityInRetail_SK_012920 a00091534enw