



Ensuring Brand Protection

Extreme Networks for Retail

Introduction

How a retailers' brand is perceived by consumers, and the strategic ways they establish a meaningful connection between brand and customer, is a key component of the business' success. Equally important for the retail brand in today's digital economy, are the ways they ensure the brand remains protected. What does brand protection mean?

Retail brands can build trust and demonstrate value with their customer base by understanding the digital and mobile expectations of today's shopper, and then align how they engage with their customers based off these expectations. This approach is a core tenant for retail brands today, but it also poses risks. The volume and variety of guests, devices, and applications in retail environments today has increased dramatically, leaving businesses and their customers highly susceptible to cybersecurity attacks. To avoid becoming another unfortunate headline and to keep the trust of their customers, retailers must keep their customers and their organization protected from these threats.

Retailers can achieve Brand Protection with complete, end-to-end intelligence of and security for all wired, wireless, and IoT devices across their environments. This is

accomplished with unified wired and wireless policy-based network architecture, secure and automated IoT and device onboarding, and robust threat detection and network surveillance. All with integrated network compliance checks and maintenance.

Critical Technology Challenges and Core Competencies

Meeting the Digital and Mobile Expectations of Customers

The role of brick and mortar is changing. The experience of online retail has forced the makeup of the store to change. No longer just a place to buy products, retailers are reconfiguring their stores to deliver quality digital experiences, showcase products in creative ways, and of course build more meaningful connections between the brand and its customer base - ultimately driving loyalty and profitability. The onus is on retailers to meet the heightened expectations of the connected shopper. This means offering seamless and secure Wi-Fi connectivity in-store, delivering convenience, reducing friction points, focusing on personalization, and incorporating mobile centric services as part of the in-store shopping experience.

End-to-End Intelligence of All Online Retail Business Environments

Managing, monitoring, and maintaining wired and wireless networks for all of the business' properties is a consuming task, especially for retail businesses that traditionally have smaller IT teams. Not to mention, the network edge makes up a significant percentage of retail deployments; a cornerstone of brick and mortar stores, the network edge is where guests and devices access and engage with the IT-driven services provided by an organization. It is the point where an organization and its customers meet; it is where users engage, mobile transactions occur, and IoT devices connect and are managed. Of equal importance, the network edge is also the first line of defense for cybersecurity threats and where a large majority of breaches occur.

Security, Onboarding, and Enablement of IoT Devices

While retailers can be somewhat slow to adopt innovative technologies, IoT (or the Internet of Things) is a disruptive technology that is already making an impressive impact on the industry, for both online and brick and mortar stores. This is because it poses compelling benefits for the retail shopping experience as well as the logistics arm of retail businesses. IoT solutions can enhance the visibility of the supply chain, improve the in-store experience by accessing customer analytics, more accurately track and manage inventory, as well as support automation.

Robust Threat Detection, Protection, and Network Surveillance

It's important the network also includes robust, built-in security capabilities to prevent the exposure or loss of confidential data for shoppers or the business. With an increase of mobile-based payments and transactions, connected devices and IoT things in the environment, this is critical for retailers today. The retail landscape, and the businesses that are part of it, are evolving at a rapid rate; retail brands should confidently embrace innovative projects that digitally transform the business without being fearful of the potential security risks.

Integrated Compliance Checks and Maintenance

Retail businesses face a litany of unique compliance challenges; for brick and mortar stores, managing physical

locations requires hiring remote contractors, improving existing processes, maintaining secure facilities, and protecting against insurance issues. From a digital and technological perspective, the retail industry faces several compliance challenges as well.

Retailers have a high number of employees, many of whom have personal devices, which makes it challenging to manage the compliance for these devices. Brick and mortar stores also need to efficiently and securely manage customer devices without compromising the confidential data of the user or the business, and while maintaining a consistent, quality experience. This is especially difficult with the adoption of mobile payment systems and the proliferation of IoT devices, creating network vulnerabilities and increasingly the likelihood of cybersecurity attacks. Finally, retail businesses have a diverse set of workstations, servers, in-house devices and applications that exist throughout multiple, distributed locations that come online and operate at various times, which makes it difficult to control all these assets and roll out updates in real-time.

Conclusion

Retailers can achieve Brand Protection with complete, end-to-end intelligence of and security for all wired, wireless, and IoT devices across their environments. This is accomplished with unified wired and wireless policy-based network architecture, secure and automated IoT and device onboarding, and robust threat detection and network surveillance. All with integrated network compliance checks and maintenance.

Additional Resources

To learn more please visit the [Retail Solution Center](#).

Extreme's Message to Retailers: Retailers are using digital transformation to reinvent themselves to deliver the same level of service and convenience to in-store customers as is delivered online. Extreme Networks enables retailers to create a highly-personalized, mobile-centric shopping experience, and to optimize store operations. We provide the solutions to build intelligent, adaptive, and secure autonomous networks that strategically integrate wireless and wired technologies, guest access, analytics, location-based services, and centralized network management. For these reasons and our #1 rated customer support, we count some of the world's largest retailers including Meijer, Walmart, Kohl's, Lowe's, CVS, and Macy's among our customers.



<http://www.extremenetworks.com/contact>

©2021 Extreme Networks, Inc. All rights reserved. Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries. All other names are the property of their respective owners. For additional information on Extreme Networks Trademarks please see <http://www.extremenetworks.com/company/legal/trademarks>. Specifications and product availability are subject to change without notice. 24322-0321-04