FORTINET

What Today's Retailers Need in a Security Architecture

Essential Solution Selection Criteria

Table of Contents

FORTINET

Executive Overview

Retail cybersecurity in the age of the omnichannel customer experience requires CIOs and vice presidents of IT to take a 30,000-foot view. Supporting multiple point-of-sale (POS) solutions, an assortment of cloud-based applications, distributed networking software, customer mobile devices, and other emerging technologies requires an assortment of specialized security solutions. But IT decision-makers can't select these security products in a vacuum; to be effective, they need to integrate tightly. They need to provide a consolidated, single-pane-of-glass view of threats, while managing security skills shortages and the impact of security on network performance.

01 Security for an Industry in Transition

Corporate executives rely on their IT teams to drive innovations that support business growth. This is true across a wide swath of industries, but it's especially pertinent to retail. Specifically, the "omnichannel" shopping experience is a must-have for retailers. Explains one analyst: "Shoppers check prices, compare products, research reviews, and consult social media before buying. If you're not available everywhere, your limited presence will derail both the user experience and your bottom line."[1]

However, as retailers introduce omnichannel shopping experiences to streamline sales and service for consumers—as well as gain an advantage over their competitors—they simultaneously introduce new facets to their organization's attack surface. The corporate security architecture must transform to keep up with emerging threats designed to take advantage of network complexity and a lack of transparency in security activities. Retail CIOs and their security teams need to keep their company's myriad new vulnerabilities top of mind as they plan the roadmap for the near future of their network. The following are some of the core security requirements for retailers:

Protecting a Complex Retail Solution Environment

The primary challenge in designing an effective security architecture for a modern retailer is to address all the complexities of the corporate network. Reliable connectivity is mandatory for a retailer's POS software, as well as for email and web-facing applications. But IT decision-makers also can't lose sight of security as they focus on providing fast and easy access to the functionality the organization needs.

Many retail businesses are running multiple POS applications. The solutions serve geographically dispersed branches, and because they contain sensitive customer financial data, they are highly attractive targets for those looking to compromise. It's crucial to protect these systems using an endpoint security solution that enables IT staff to discover, monitor, and assess endpoint risks in real time. Many retailers confront the risks by segmenting endpoints across the network so that compromised systems can be quarantined, minimizing the impact of a breach.

Incorporation of SD-WAN

Another consideration is that some retailers rely on software-defined wide-area network (SD-WAN) technology to provide high-speed connectivity to their diverse POS systems and other applications. Many organizations have adopted SD-WAN solutions to prevent network bottlenecks through application prioritization and to accelerate performance between branches in distant geographies. One benefit of SD-WAN technologies is that because traffic no longer needs to be routed through the corporate data center, branches receive faster internet connections. However, this also means new vulnerabilities are exposed because data-center security controls are not applied. Further, most SD-WAN solutions do not include effective security.

Properly securing an infrastructure that incorporates SD-WAN requires a solution that addresses network performance while delivering robust security. Retail CIOs who need to secure an SD-WAN environment should look for a next-generation firewall (NGFW) that protects the distributed network against malware, while minimizing total cost of ownership (TCO) by containing upfront acquisition costs, ongoing fees, and labor for installation, maintenance, and upkeep.

Multi-cloud Security

At the same time, retailers are rethinking their on-premises technology infrastructure. Additionally, most also operate in a multi-cloud environment, utilizing applications and storing important data in a public, private, hybrid, and/or Software-as-a-Service (SaaS) cloud. These cloud-based applications are an excellent answer for providing certain types of functionality to a distributed retail organization, but they also amplify the complexity of the corporate IT structure and open another set of windows to potential cyberattacks.

Cloud-based applications are, by their nature, challenging to secure. Because they run on hardware located outside the corporate data center, and its traditional security measures, cloud-based applications require a new approach to security. Security solutions need to be able to break down silos between the different clouds a company relies on, so that IT staff gain clear and consolidated visibility into and incident analysis of threats and mitigation efforts across all the company's applications, regardless of where they're housed.

63%

of retail data breaches result from the hacking of a web-based application.[2]

Email and Web Applications

Like every business, retailers must give employees access to email and web applications so that they can get their jobs done. Email remains a favorite target for cyberattackers, and it requires a sophisticated and targeted security solution. Research shows that 94% of companies experienced a phishing attack in the past year.[3]

Traditional email security is often disconnected from broader network security. But when the email security system fails to share information about attacks (whether successful or not) with the rest of the organization's security infrastructure, it creates an opportunity for a successful intrusion elsewhere. At the same time, attacks may fail elsewhere but then succeed at the email vector.

A recent survey found that 84% of all endpoint breaches included more than one endpoint—they involved a combination of desktops, laptops, servers, Internet-of-Things (IoT) devices, and/or endpoints in the cloud.[4] In fact, 20% of breaches involved 100 or more endpoints. When an attack targets email on many different endpoints, effective response requires coordination among the company's different security solutions.

Web applications also open the door to web-based threats. 63% of retail data breaches result from the hacking of a web-based application.[5] A cyberattack is concerning to any CIO, but in an omnichannel retail organization that generates a significant proportion of its income through an online store, ensuring that the website is secure and provides uninterrupted uptime is mission critical. In many cases, securing the website is more important to retailers than securing POS systems.

The result is that retail IT leaders need a sophisticated, multilayered approach to web application security that is proven to protect against the Open Web Application Security Project (OWASP) Top 10 threats, distributed denial-of-service (DDoS) attacks, and other known attack modes. At the same time, retailers need a web application firewall with artificial intelligence (AI) capabilities that can detect advanced threats the security architecture was previously unaware of. Specifically, tools that reduce the frequency of false positives in the web application firewall improve its efficiency, increasing its likelihood of detecting attacks in real time.

Like other security technologies, a retailer's email and web application security solutions need to integrate into a larger security architecture in which they share information with the corporate firewalls, networking security, cloud protection solutions, and other security elements.

Wireless Access Points

Retailers embracing the omnichannel customer experience also need to consider the vulnerabilities they're introducing by giving customers wireless internet access within stores. Standard switching technologies do not properly address the vulnerabilities created by opening in-store networks to third-party devices. And this is a problem, as security of wireless access points is business critical for retailers, requiring both secure wireless access points and specialized switching security solutions.

02 Complexity of Security Architecture

As retail IT teams design a security architecture that extends well beyond perimeter protection, they often are tempted to select independent solutions that seem like the best-of-breed fit for each specific need—from endpoint protection to cloud security, and from email to the firewall or even wireless access control solution. However, this results in piecemeal security policies and practices that ultimately undermine network security. Security solutions that don't integrate tightly may fail to share crucial information about threats, and thus will be unable to mount a coordinated response in the face of a cyberattack.

What retailers need is a set of security solutions that integrate tightly while individually protecting all of the network's points of vulnerability—endpoints, email, web applications, SD-WAN connectivity, wireless access points, as well as the firewalls at the network edges.

When one security element detects a threat, it needs to immediately alert the rest of the security fabric about the threat. This enables each solution to respond to the threat automatically. Specifically, an integrated security architecture designed to provide coordinated threat response, in a timely manner across the organization's entire attack surface, is crucial for organizations seeking to keep pace with the advanced threat landscape and to manage security staff in the face of an acute security skills shortage.[6] Any delay in response to an attack creates more opportunity for the attacker to wreak havoc.

Visibility Issues Complicate Compliance

Amid all these new security concerns, retail businesses must also consider regulatory compliance needs. From the EU's General Data Protection Regulation (GDPR), to industry regulations such as the Payment Card Industry Data Security Standard (PCI DSS), to security standards such as the National Institute of Standards and Technology (NIST), compliance requires the corporate IT team to harness security data, both to generate reports for targeted audiences and to respond quickly in the event of a data breach. Meeting these demands requires not only centralized and consistent policy controls but also immediate transparency across the corporate attack surface.

Only 12% of respondents in a recent survey said their NOC and SOC teams have strong technical integration.[7]

Reduced Barriers Between NOC and SOC

Another area in which retail IT teams should focus their attention when designing their security architectures is the relationship between their security operations center (SOC) and their network operations center (NOC). For many, the SOC and NOC are completely separate, with independent processes and different teams, an approach that undermines a retailer's security posture.[8]

A company's NOC stores information about where applications are running and whether security patches are up to date. In the event of an attack, the NOC can provide insight into which endpoints are vulnerable and how concerned the company should be—vital information in effective threat response. However, identifying those attacks depends on information about emerging threats, which is collected and maintained within the SOC.

When NOCs and SOCs fail to share important threat information, IT staff do not have the real-time threat intelligence they need. Unfortunately, many businesses still run these functions in silos: Only 12% of respondents in a recent survey said their NOC and SOC teams have strong technical integration.[9]

NOC-SOC integration is crucial. Reaching that point requires purpose-built security management and analytics tools that provide transparent visibility through coordinated and streamlined dashboards and workflows.

03 Additional Considerations

In addition to ensuring that each of their security elements communicates with one another, retail security teams also need to make sure that they provide for segmentation or microsegmentation of the network. For example, the ability to segment the network on the fly can trap potential threats in small spaces. This limits their access to data and applications, which minimizes the damage they can cause.

Network Access Control

A security architecture that includes microsegmentation of network endpoints should also include network policies and access controls that use analytical technologies to profile the network's various endpoints and then assign appropriate levels of access and segmentation for each. This approach, combined with continuous monitoring of endpoint risks, significantly reduces the company's vulnerability to both known and unknown threats.

Retailers often operate with razor-thin margins, so efficiency in network security—as in every area of the business—is key to success, or even survival.

TCO in Security Management

Retailers often operate with razor-thin margins, so efficiency in network security—as in every area of the business—is key to success, or even survival. Security solutions with automated threat response and automated information sharing between the SOC and the NOC eliminate many hours of manual monitoring, event logging, ticket submission, and other tasks. Plug-and-play capabilities for zero-touch deployment are also significant timesavers. Such features reduce errors and make it easier to enforce network policies. The cumulative effect of all these capabilities is easier security management and a low TCO.

No Reduction in Network Performance

All the technologies that make an omnichannel customer experience possible can also drag down broadband bandwidth across a retailer's different locations. Adding to performance challenges, retailers are increasingly adopting presence analytics technologies, which track customers' physical movements via their mobile devices, then determine how much time they spend in a store, what types of products they look at, and the like. The insights provided by these "presence analytics" systems can lead to improved decisions around when and how to make specific offers to individual customers, but they also require extensive resources, which can slow down everything else that happens on the network.

In this environment, retailers designing a security architecture must be especially careful to make sure that their security solutions do not place a drag on network performance. As CIOs shop for solutions that will integrate tightly, they also need to consider the means of communication among devices. The ideal solution architecture weaves all the company's security products into an integrated fabric, connecting devices via a high-performance virtual private network (VPN) to keep communications secure without affecting network performance for the organization's other applications.

04 Conclusion

Modern retailers need a network infrastructure in which security is integrated across all the diverse facets of the attack surface. This has always been true, but as the typical retail network evolves to incorporate new, more varied devices, to support mobile, IoT, and other aspects of digital transformation, achieving integrated security has become more important—and more challenging—than ever before.

The solutions securing all of a retailer's network devices, from edge to endpoint to the cloud, need to share threat intelligence. They also need to provide visibility into security, in one place and with continuous risk assessment and built-in analytics, to accelerate threat response. Securing a modern retail business is challenging. But smart solution selection decisions can make the security infrastructure more effective and better able to meet the organization's needs.

[1] "Omni-Channel Retail Strategy: The What, Why, and How of 'In-Store' Shopping," Shopify Plus, January 9, 2018.

[2] "2019 Data Breach Investigations Report," Verizon, March 2019.

[3] "The State of Email Security: 2019 Report," Mimecast, accessed May 28, 2019.

[4] Lee Neely, "Endpoint Protection and Response: A SANS Survey," SANS Institute, June 12, 2018.

[5] "2019 Data Breach Investigations Report," Verizon, March 2019.

[6] "The CISO Ascends from Technologist to Strategic Business Enabler: Understanding the Cybersecurity Skills Shortage," Fortinet, August 15, 2018.

[7] Nelson Hernandez, "NOC/SOC Integration: Opportunities for Increased Efficiency in Incident Response within Cyber-Security," SANS Institute, January 26, 2018.

[8] "The NOC and SOC Divide Increases Risk While Breeding Inefficiencies," Fortinet, September 11, 2018.

[9] Nelson Hernandez, "NOC/SOC Integration: Opportunities for Increased Efficiency in Incident Response within Cyber-Security," SANS Institute, January 26, 2018.

www.fortinet.com

Copyright © 2019 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

414260-0-0-EN

June 14, 2019 9:59 PM

eb-retailers-security-architecture