Protecting Retail Customers by Simplifying Security Operations and Reducing Network Complexities

A Next Generation Security Fabric Mitigates Advanced Threats While Improving Customer Satisfaction

Many cyber criminals view retailers as highly attractive "low hanging fruit." Sophisticated hackers can gain access to sensitive information when data is transmitted across a wide area network (WAN) and to and from public and private clouds. The advent of omnichannel retailing has created new challenges in branch locations where customer experience (CX) can decline due to low performance and security friction. Retail digital transformation (DX) initiatives seek insights on customer behaviors to help improve CX and lower cart abandonment, but cybersecurity requirements often cause roadblocks or DX failures. Nearly all retailers are in a battle with other firms to recruit and retain security professionals, and they can no longer afford to purchase and manage a garage full of security point solutions.

Almost 95 percent of retailers are expanding the use of cloud, big data, mobile phones, and Internet of Things (IoT), which increases security risks and network complexities[1]. While retailers top the list of most targeted firms by cyber criminals, the industry in general ranks at the bottom in terms of social engineering security[2]. As such, retailers are at high risk for exposing personally identifiable information (PII), which could violate the Payment Card Industry Data Security Standard (PCI-DSS) and trigger fines, lawsuits, and negative publicity by failing to meet Civil Codes in 48 of 50 U.S. States. Many retailers believe their networks and domains are secure, but a SecurityScorecard report found that almost 98 percent had at least one potential compliance issue that ran contrary to PCI-DSS Requirements 6 and 11, which focus on continuous visibility to maintain secure networks and infrastructures[2].

WWT's Retail Security Best Practice Recommendations

Implementing an end-to-end Security Fabric can offer you the benefits of seamless integration across your entire security stack while facilitating workflow automation, threat visibility, and compliance. Prebuilt fabric connectors with a robust application programming interface (API) give you the ability to integrate third-party solutions. An optimal Security Fabric should also offer:

High Visibility

WWT recommends the Fortinet Security Fabric to help you achieve centralized visibility and control of all your security solutions deployed across the entire network. Built-in connectors and an open API framework ensure integration and simplified management of all security solutions.

WWT at a Glance

Founded in 1990

6000+ Employees

Nearly $12 billion in Annual Revenue

Efficient Automation

WWT has found that Fortinet solutions can ensure automated threat detection and response, policy enforcement, and compliance report generation, which can reduce your security team's workload while improving efficiency. Automation includes prebuilt workflows for effective event management and reporting for industry standards such as PCI DSS, the National Institute of Standards and Technology (NIST) Cybersecurity Framework, and many others.

Proactive Threat Intelligence

WWT experts see global threat intelligence powered by AI and machine learning (ML) as a critical component to allow fast communication across the Security Fabric in real time. This will also allow you to detect and eliminate evolving threats that target point-of-sale (POS) systems, cloud deployments, and other retail network infrastructure.

High Performance

To maintain excellent CX and prevent customer friction, WWT recommends FortiGate next-generation firewalls (NGFWs). They offer the industry's lowest latency and allow deep inspection of secure sockets layer (SSL)/transport layer security (TLS) encrypted traffic with minimal impact on network performance.

Customer Insights and Engagement

Many solutions compromise security for CX and revenue, but Fortinet's FortiAP enables a WiFi experience that keeps customers engaged while FortiPresence analyzes customer WiFi smartphone signals to uncover valuable behavioral insights to boost traffic and sales.

WWT at a Glance (cont.)

Privately Held

Work with 70% of Fortune 100 Companies

Great Places to Work 8 Years in a Row

Conclusion

WWT's security experts have found that avoiding the serious consequences of a security breach or compliance failure now requires more advanced and effective network and security technologies. These solutions need to exist in a single security fabric that seamlessly integrates into a retailer's network. They must also share information in real-time and automate security tasks to protect retailers and customers while creating omnichannel shopping experiences to improve rather than hinder sales. Retailers need transparent visibility and real-time security workflows underscored by global threat intelligence, along with efficient automation to reduce workloads and security team demands to lower total cost of ownership (TCO).

WWT is a Fortinet Authorized Platinum Partner that uses a proven and innovative approach to help our customers discover, evaluate, architect, and implement advanced technology. We take an integrated approach to security rather than focusing on point solutions. This helps us align business goals and objectives to technical solutions, providing more effective outcomes and solutions that further the development of an enterprise architecture. Learn more about how we can integrate and deploy Fortinet solutions to help you reduce vulnerabilities, which can set the stage for future innovation.

Contact Information

References

1. https://www.govtech.com/blogs/lohrmann-on-cybersecurity/2019-the-year-ransomware-targeted-state--local-governments.html

2. https://www.zdnet.com/article/over-500-us-schools-were-hit-by-ransomware-in-2019/

3. https://www.idc.com/getdoc.jsp?containerId=prUS45612419

4. "The CIS Critical Security Controls for Effective Cyber Defense," SANS Institute, accessed May 8, 2018.

5. CoSN Cybersecurity Leadership Initiative, CoSN, accessed May 8, 2018.

FORTINET.

www.fortinet.com

April 28, 2020 11:44 PM

D:\Fortinet\Image Graphics\Pam Seeds\645657 - 2020 Q2 WWT Retail\sb-2020-q2-wwt-retail-4282020-1144PM

645657-0-0-EN