USE CASE:

Security Validation in Retail - A Vital Component in Protecting e-Commerce

Ridge Security Technology Inc. www.ridgesecurity.ai

The retail industry's digital transformation has introduced new services and conveniences, creating an urgent need to address security challenges. This urgency cannot be overlooked, making security validation crucial in protecting online retail. Consider these retail cybersecurity statistics.

24%
Of cyberattacks targeted retailers, more than any other industry.

34%
Considered cyberattacks or privacy breaches their most serious digital threat.

34%
Of retailers said cybersecurity worries were their primary hindrance in moving to e-commerce.

99%
Of retail cyberattacks were driven by financial motives.

42%
Of compromised data in an attack is payment information.

41%
Of compromised data in an attack is personally identifiable data.

Business Context

A major retailer with a robust online presence is seeking to validate the security of its e-commerce platform. This platform is the custodian of sensitive customer information, including payment details, personal data, and order history.

The company sells various products through physical stores and an e-commerce platform. With a significant headquarters, over 100 stores and showrooms nationwide, more than 1800 employees, and an extensive online presence, the retailer needs greater cyber protection to support its resource-limited security team.

Given the high volume of transactions and the data sensitivity, ensuring the platform is protected against potential cyber threats is a top priority. The company also aims to safeguard additional endpoint devices, servers, and

applications against malware, software and configuration risk exposures, social engineering, and other cyber threats. The number of IP addresses across its digital ecosystem is over 20,000.

Challenge - Ensuring Proactive Security

The company is responsible for protecting customer data, including personal information, payment details, and purchase history. They needed to ensure the confidentiality and integrity of this data. The company determined that continuous security validation testing was required to identify and mitigate vulnerabilities. This would allow them to simulate attacks, such as SQL injection and unauthorized access, and validate and proactively address security weaknesses.

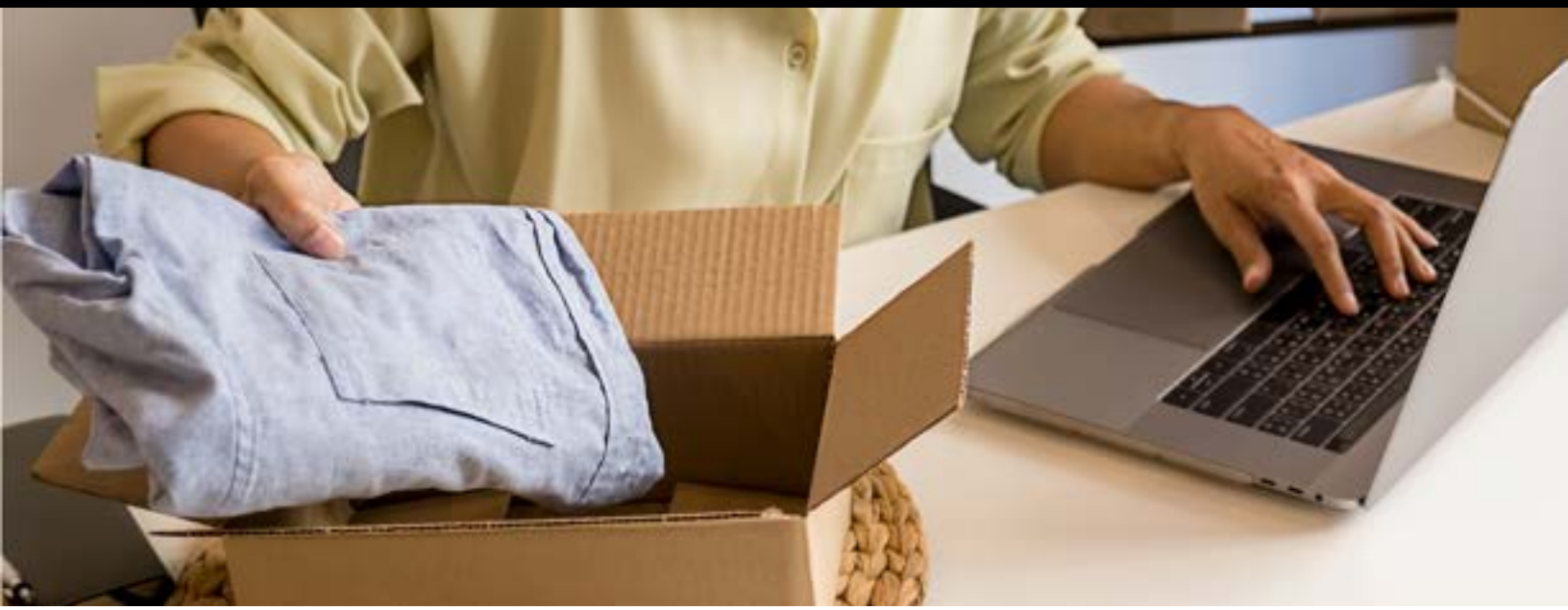
The company uses various devices, including point-of-sale (POS) terminals, inventory scanners, and employee workstations. These devices are potential targets for cyberattacks. With security validation, they can verify the security configurations of these devices and look for weak default passwords, outdated firmware, and other entry point exposures for malware.

The retailer relies on servers for their e-commerce website, inventory management, and customer support systems, where any server compromise could disrupt operations and put sensitive customer data at risk. The ability to conduct regular penetration testing, validation, and vulnerability assessments would help identify weaknesses in server configurations, software patches, and access controls.

The company must prioritize security across its operations to maintain customer trust and protect its business. Any flaws in web applications could lead to data breaches or financial losses. Security validation testing will enable them to focus on web application security. This includes testing for common vulnerabilities, such as cross-site scripting, input validation issues, and insecure APIs to prevent exploitation.

Security Objective

“Our objective is crystal clear: We are committed to ensuring the security and integrity of our online presence. This involves identifying and mitigating potential security vulnerabilities across our diverse digital ecosystem. We firmly believe that a comprehensive security approach is the key to staying ahead of the curve in the face of evolving cyber threats.” - The retailer’s Chief Security Officer



Critical Areas of Security Validation Testing Focus

- User Authentication and Authorization
- Payment Processing
- Data Storage and Encryption
- Web Application Security
- IT infrastructure

The Solution

The retailer selected RidgeBot, an advanced AI-powered security validation platform that proactively detects and removes threats through automated penetration testing and continuous security validation.

Results

Finished testing all stores in three months, much shorter than the planned year and a half.

Found many risks and vulnerabilities, including their IP printers, which were the weak points in their overall security.

Found their security posture is not strong enough and plan to enhance it by deploying multiple tools.

What the customer likes about RidgeBot

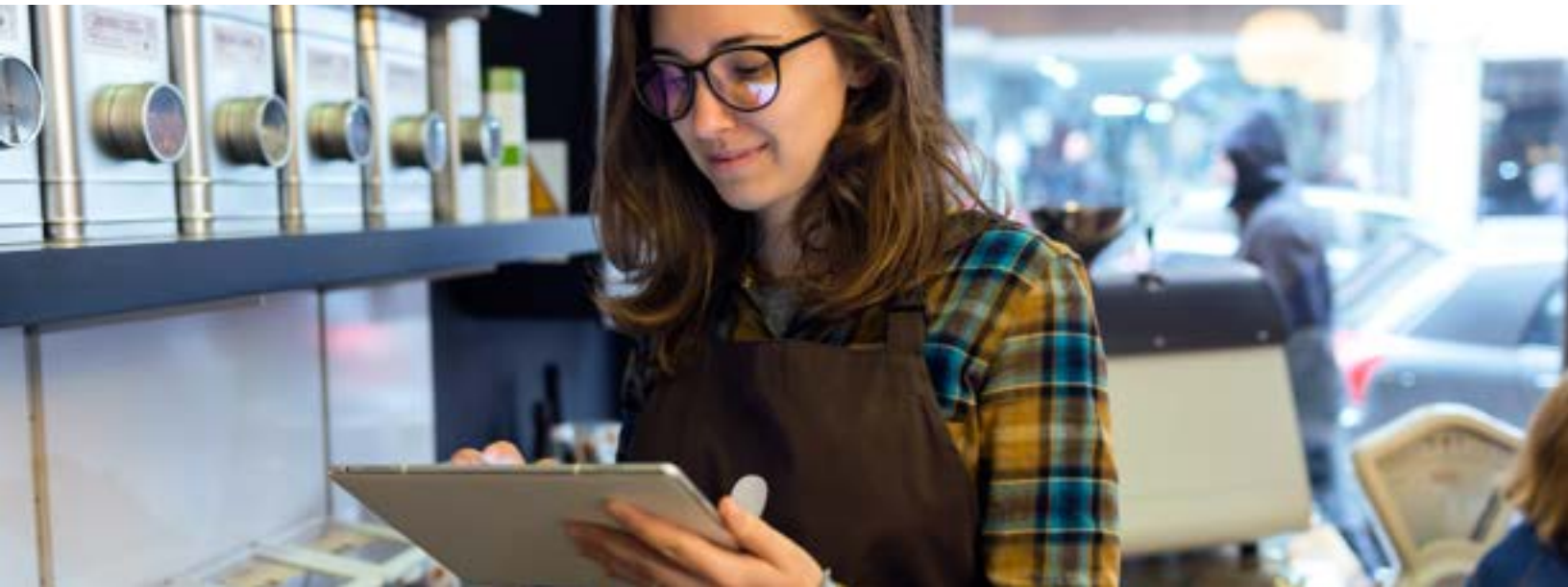
- Ease of use
- Saved a year of time
- Able to test diverse and a large amount of assets simultaneously.
- Ability to cover vulnerabilities and risk findings in a wide range of IP devices, including IP printers and cameras

RidgeBot's reporting features, including kill chain analysis for remediation, provide the security team with clear visibility and logical breakdowns of each step to exploit system vulnerabilities. RidgeBot identifies vulnerabilities in connected systems without disrupting critical operations if a server is compromised.

RidgeBot uses IP addresses to assess the retailer's CCTV cameras and system servers. During the test, RidgeBot interacts with the cameras' web interfaces, mimicking potential hacker actions to identify vulnerabilities for swift resolution by the retailer's staff.

Additionally, the retailer utilizes RidgeBot for security assessments against ransomware, information leaks, Active Directory integrity, and weak password vulnerabilities. These capabilities significantly bolster the retailer's security posture and ensure robust protection.

RidgeBot has proven invaluable in uncovering overlooked device vulnerabilities, including printers, security cameras, IoT devices, and more. Its speed and precision outperform manual testing by delivering zero false positives, accurately validating vulnerabilities, and substantiating risks through real-time reporting.



By leveraging RidgeBot, the retailer has minimized exposure to new vulnerabilities, optimized the productivity of its security team, and effectively prioritized mitigation efforts toward critical risks. RidgeBot security validation helped the company overcome its resource limitations. The three-member team needed to complete pentesting and security validation for all 100+ stores within 1.5 years. RidgeBot automation enabled them to complete all store testing in just three months.

The company needed to cover more IP-based assets beyond its core e-commerce platform. However, it could not target all its Internet-connected assets through manual testing. With RidgeBot's automated testing, it easily tests all of its network-connected devices, systems, and applications.

Benefits of RidgeBot Security Validation Deployment

- **Risk Mitigation:** By proactively identifying and addressing security gaps, the company reduced the risk of data breaches, financial losses, and reputational damage.
- **Operational Continuity**: Proactive security measures prevented disruptions to the retailer's online and in-store operations.
- **Customer Trust:** Demonstrating commitment to security built customer trust, encouraging repeat business.
- **Compliance:** Regular testing ensures compliance with industry standards, such as PCI DSS for payment card data security.

The company leveraged RidgeBot's security validation testing to protect its data, devices, servers, and applications. This has ensured robust protection of sensitive customer data and secure payment processing while maintaining customer trust and confidence.

About Ridge Security

Ridge Security is a leader in exposure management and is dedicated to developing innovative cybersecurity products that benefit CISOs and security teams by reducing risk through validation and using automation to improve efficiencies. Ridge Security's products incorporate advanced artificial intelligence to deliver comprehensive security validation, powerful workload protection and cloud security monitoring.

Request a Demo

RIDGE SECURITY