SCHNEIDER DOWNS

Big Thinking. Personal Focus.

Enhancing Retail Cybersecurity

Essential Tools and Software for Strengthening Business Protection

SCHNEIDER DOWNS
Big Thinking. Personal Focus.

Enhancing Retail Cybersecurity

Essential Tools and Software for Strengthening Business Protection

The retail industry's digital transformation introduced unparalleled conveniences for both businesses and consumers. However, this digital evolution also brought about new security challenges. In this rapidly evolving retail industry landscape, one aspect remains constant: the need for robust cybersecurity tools and software.

Why is Cybersecurity Critical for the Retail Industry?

In 2020, U.S. consumers spent **$861.12 billion** on online retail transactions – 44% more than in 2019. Many retailers have launched or revamped their e-commerce stores since then, offering services such as curbside pickup, to help meet the growing demand.

While these trends create great opportunities, they also generate new attack vectors. Cybercriminals are continually developing sophisticated tactics to exploit vulnerabilities in retail networks and systems. To counter these threats, retailers must leverage cutting-edge cybersecurity tools and software.

What Tools and Software Offer the Best Protection?

Here are some of the most essential cybersecurity tools and software that are indispensable for securing the retail industry.

Access Control and Identity Management | Access control and identity management tools ensure that only authorized personnel have access to specific systems and data. This is vital in preventing insider threats and unauthorized access. Two-factor authentication (2FA) and single sign-on (SSO) solutions enhance access control.

Antivirus and Anti-Malware Solutions | Retailers need robust antivirus and anti-malware software to detect and eliminate malicious software from their systems. These solutions constantly scan for malware and suspicious files, providing real-time protection against known and emerging threats.

Encryption Tools | Data encryption is a fundamental aspect of retail security. Retailers should use encryption tools to protect sensitive data, such as customer information and payment details, both in transit and at rest. Encryption ensures that even if a breach occurs, the stolen data remains unreadable to unauthorized parties.

Endpoint Security Software | Endpoint security software secures individual devices (e.g., point-of-sale terminals, employee workstations and mobile devices) from threats. It includes features like antivirus protection, firewall capabilities and data encryption to safeguard data on endpoint devices.

Firewalls and Intrusion Detection/Prevention Systems | Firewalls and Intrusion Detection/Prevention Systems (IDS/IPS) are the front line of defense against cyber threats. Firewalls filter incoming and outgoing network traffic, allowing only authorized communication. IDS/IPS systems monitor network activity, identify suspicious patterns and take action to prevent unauthorized access or data breaches.

Incident Response and Forensic Tools | In the event of a security breach, incident response and forensic tools help retailers investigate the incident, determine its scope and take appropriate actions to mitigate the damage and prevent future attacks. In the event of a serious security breach, it is best to reach out to a security firm that works with these issues daily. It takes experts to fully remove an attacker from the network.

Mobile Device Management (MDM) Solutions | Given the prevalence of mobile devices in retail operations, MDM solutions are crucial for securing these endpoints. MDM allows retailers to enforce security policies, remotely wipe lost or stolen devices and manage app installations.

Network Segmentation Software | Network segmentation divides a network into distinct segments, each with its own security policies. This approach limits the lateral movement of attackers, containing potential breaches and safeguarding critical systems. Be sure and segment any third-party vendor's network from your own and only allow access to the resources they need.

Security Awareness Training Platforms | Human error remains a significant vulnerability in the retail industry. Security awareness training platforms provide retailers with a means to educate employees about cybersecurity best practices, phishing awareness and how to recognize and respond to security threats. Security, like a chain, is only as strong as its weakest link, and the user is the weakest link in network security.

Security Information and Event Management (SIEM) Systems | SIEM systems collect and analyze data from various sources to provide a comprehensive view of a network's security posture. These tools help retailers detect anomalies, manage security incidents and respond promptly to potential threats.

Vulnerability Scanners | Regular vulnerability assessments are essential for identifying and addressing weaknesses in the retail network. Vulnerability scanners help retailers find and fix vulnerabilities in their systems and applications before cybercriminals can exploit them. Be sure and scan any IoT devices you have on the network.

Wireless Security | Today in the retail industry, the use of wireless devices is ever more present. Wireless inventory-scanning tools are a great time-saving convenience, but wireless is using radio waves to send data, so like with any radio signal, someone in the area can pick up those signals, so use strong encryption on all connections to the access point. Also, restrict access to the access points from the known devices you have. This is accomplished by whitelisting the MAC addresses of the company devices and only allowing access to the access point from these devices.

In the evolving landscape of the retail industry, staying ahead of cyber threats is imperative. The adoption of these essential cybersecurity tools and software solutions can significantly enhance a retailer's security posture, protect sensitive customer data and safeguard the integrity of its operations. By investing in and implementing these technologies, retailers can build a robust defense against the ever-present cybersecurity challenges in the digital age.

About Schneider Downs Cybersecurity

The Schneider Downs Cybersecurity practice consists of experts offering a comprehensive set of information technology security services, including penetration testing, intrusion prevention/detection review, ransomware security, vulnerability assessments and a robust digital forensics and incident response team. In addition, our Digital Forensics and Incident Response teams are available 24x7x365 at 1-800-993-8937 if you suspect or are experiencing a network incident of any kind.

For more information, please contact our team at **contactsd@schneiderdowns.com** or visit **www.schneiderdowns.com/cybersecurity**.

Schneider Downs is a certified Qualified Security Assessor (QSA) Company, which authorizes us to provide audit services for merchants and service providers to comply with credit card security standards. More information is available at ***www.schneiderdowns.com/pcidss.***

SCHNEIDER DOWNS
Big Thinking. Personal Focus.

www.schneiderdowns.com

TAX
AUDIT AND ASSURANCE
CONSULTING
WEALTH MANAGEMENT

PITTSBURGH
One PPG Place
Suite 1700
Pittsburgh, PA 15222
P 412.261.3644

COLUMBUS
65 E. State Street
Suite 2000
Columbus, OH 43215
P 614.621.4060

METROPOLITAN WASHINGTON
1660 International Drive
Suite 600
McLean, VA 22102
P 571.380.9003