Solution Brief

PROACTIVE CYBER SECURITY FOR THE RETAIL INDUSTRY

Empowering retailers to simplify their digital transformation, security and compliance journey

Overview

Retailers deal with thousands of transactions and an equally enormous amount of consumer data that help them tweak their customer's buying experience and improve profitability. Retailers adopt modern approaches to achieve their goals, and the core component that helps them keep up to the competition is their IT infrastructure. It's a costly oversight to become a victim of a cyber-attack, eventually hurting the business and brand reputation.

According to a recent PwC annual Global State of Information Security Survey (2017), there was an average of 4,000 security incidents that affected enterprises in the retail and consumer sector in the preceding year.

ColorTokens Unified Security Platform is a software-defined security solution. ColorTokens enables retailers to take a proactive approach towards security and meet compliance and audit requirements, easing their digital transformation journey. ColorTokens technology secures workloads, application environments, endpoints and users in traditional and hybrid infrastructures against internal and external threats. ColorTokens zero-trust architecture and intent-based security enables proactive security and compliance and reduces CAPEX/OPEX by consolidating point security and siloed networking products.

ColorTokens Retail Solution

ColorTokens Unified Security Platform enables retailers to take a proactive approach towards security and meet compliance and audit requirements, easing their digital transformation journey.

Benefits:

- Secure and centralized platform-independent solution with no vendor lock-in headache
- Zero-trust network for proactive protection against data breaches, APT and other unknown threats to comply with PCI DSS requirements
- User and application endpoint security without additional hardware investment
- Security posture and compliance visualization across application environments, workloads, users and endpoints
- Signature-less endpoint security, to protect even unsupported/unpatched legacy systems
- Fast deployment

Security and Compliance Challenges in Retail

- ***Reactive Security:*** The emergence of digital channels, modern payment technologies and the fierce competition has made many retailers adopt new technologies at a rapid pace. The retail sector is a honeypot for hackers, owing to the availability cardholder and other consumer data from compromised POS terminals and database servers. Unfortunately, most of the retail security systems and strategy in place is reactive – it took almost a good three weeks to detect the credit card data breach in Target. This reactive firefighting will only fix the holes in the system, momentarily, while the hackers may be discovering newer ways to breach the systems and fixes in place, like firewalls, software patches, antivirus, IDS and IPS systems.
- ***Threats from Within:*** The practice of assigning privilege accounts to employees to access POS systems and card data environment resources (CDE) is still ad hoc – some are automated, but most follow the manual assignment process, which is difficult to keep

track of when employees move across departments or exit the company. In retail, the employee turnover rate is quite high, considering both the full-time and part-time workforce. There's a possibility of a data breach when one of these employees/former (disgruntled) employees turn malicious. Having said that, not all insider attacks are malicious. It could be from a regular employee unwittingly clicking an email attachment containing malware, ransomware, or a configuration error on an internal firewall leaving the CDE exposed and vulnerable.

- *Increasing Attack Surface:* Geographically distributed retail stores and the race for digital transformation to create an omni-channel experience has led to an exponential increase in endpoint devices, POS terminals, and retail application and database servers. This in turn, has eventually increased the attack surface of the retail IT infrastructure. Retailers invest in several point security products to minimize the security gaps. However, considering the employee turnover, insufficient security training/hygiene, lack of skilled security personnel and involvement of third-party contractors only seem to increase the security gaps. Also, with the migration of old applications and the creation of newer ones, there is a potential risk of the production data being accessed from the development and staging environments, deliberately or inadvertently, if these environments are not isolated and monitored properly.

> According to the Verizon Data Breach Investigations report (2018), 68% of the breaches took several months to discover.

- *Audits and Compliance:* Retailers deal with enormous amount of card holder data, and it's imperative they comply with Payment Card Industry Data Security Standard (PCI DSS) compliance regulations. With reactive security strategies, employee turnover and the increasing attack surface, retailers are challenged to continuously audit their systems and IT environment to ensure compliance and avoid regulatory fines, which in turn directly impacts their brand reputation and revenue. It's not just the audit failure that the retailers must be worried about. Periodic PCI audits across local and distributed IT infrastructure are alone very expensive, if the scope is not limited by auditable sections using proper network segmentation.

ColorTokens Solution

ColorTokens Unified Security Platform simplifies the retail IT challenges by taking a unified and proactive approach towards security and compliance. Retailers that have their IT spread across geographical locations, and on on-premise and multiple clouds, need not fight with disparate IT management tools to ensure the stores' security posture and the PCI DSS compliance requirements are met. ColorTokens offers retail IT enterprises the simplicity, flexibility and reliability required to achieve their business goals, eliminate data breach and protect the brand reputation.

ColorTokens Unified Visibility and Threat Analytics – Granular Visibility, Everywhere

ColorTokens provides granular visibility of cross-segment traffic in your on-premise or hybrid data centers, without the need for separate visualization tools that add to the operational overhead. ColorTokens goes beyond visualization by providing residual risk metrics and contextual analytics that help retail IT teams to continuously assess and improve the security posture of the infrastructure.

This centralized in-depth visibility across the multi-vendor IT environment helps retailers visualize the communications happening among the CDE, POS and other incoming/outgoing external connections. Retailers can visually validate PCI DSS compliance requirements, know how the security posture is changing, and be audit-ready.

ColorTokens Intent-Based Micro-Segmentation - Secure Micro-Segments to Limit Audit Scope and Attack Surface

ColorTokens helps retailers with multiple business, POS, CDE, transactional and application development segments implement secure micro-segmentation in their multi-cloud, multi-vendor data center, without requiring additional investment on high-capacity internal firewalls. IT admins in retail chains need not deal with thousands of firewall rules and time-consuming, error-prone VLAN/ACL configurations.

ColorTokens secure micro-segmentation helps retailers reduce the attack surface and limit the propagation of APT lateral threats, and other unauthorized resource accesses, from within or from outside the infrastructure. ColorTokens enables end-to-end encryption of POS terminals, making the data communication tamper-proof. ColorTokens automates security across every segment of your data center and ensures uniform security posture even when resources move across clouds or on-premise data centers. ColorTokens micro-segmentation also helps retailers limit and define the scope of the network segments to be audited efficiently.

ColorTokens RADAR360 – Two-Fisted Process-Level Lockdown of POS Terminals and Endpoints

ColorTokens protects POS systems, endpoints, and other critical assets from malware, ransomware, RAM scrapers, and other unknown threats. ColorTokens takes a straightforward yet robust signature-less approach helping retailers worry less about legacy, unpatched and unsupported endpoints as well. ColorTokens provides exceptional security to retail workstations, kiosks, POS terminals, without the need for multiple anti-virus tools, signature updates and patch management headache – protects even if the POS systems/retail workstations are offline. ColorTokens can help extend the life of POS, and provide a greater ROI.

Conclusion

Information security has become a boardroom discussion, owing to the frequency and the sophistication of the attacks and the brand and revenue damage that it can create. Retailers, in their quest for digital transformation, should take a proactive approach in securing sensitive customer and card holder data, no matter the type of data centers they have or where they're located. While retailers may be short-staffed in IT, or don't have the necessary skilled personnel to protect the assets, they must embrace a unified and platform agnostic security solution that will scale and grow along with their business, while keeping the operational complexity to a minimum. ColorTokens empowers retailers in simplifying their digital transformation and security journey.

About ColorTokens

ColorTokens is a Silicon Valley company, backed by legendary investors and advisors who have helped structure the IT industry over last 30+ years. ColorTokens' core team brings deep and innovative industry experience from brands such as Cisco, Juniper, VMware, Microsoft, and Zscaler in domain areas including cybersecurity, networking, and infrastructure. With customers and partners worldwide, ColorTokens is headquartered in Santa Clara (Silicon Valley), CA, USA with a major center of development and sales in Bengaluru, India.

COLORTOKENS

Email: sales@colortokens.com | Call +1 (408) 341-6030 | www.colortokens.com