CASE STUDY

Managed Security Services for Critical Retail Assets

Zero Trust Segmentation, Connectivity, and Security

Cyber criminals keep a watchful eye on the retail industry, continuing to capitalize on opportunities to breach and hijack systems and endpoints. Customers' credit card data is the main draw, combined with personal trend information, such as spending patterns and loyalty behaviors, which can further efforts to hijack credentials.

These criminals have many techniques at their fingertips, from exploiting retailers' busy seasons, such as Black Friday, to launching stealth techniques that go largely undetected.

Top Retail Security Requirements

Retailers want to be able to connect and protect what matters most, preventing all known and unknown threats, while enabling trusted communications and connectivity to maintain critical operations.

This end goal creates a number of security requirements, including:

- **Protecting endpoints,** such as PoS devices, from network-based attacks
- **Ensuring privacy** of cardholder information
- **Establishing trusted connectivity** for enterprise data-in-transit across retail locations
- **Reducing the scope** of risk and compliance assessments

The Security Misconception: Zero Trust Protection Comes at a Cost

A breach to critical assets hits hard at a retailer's purse strings, in terms of reputation damages, lost customers, halted operations and potential regulatory fines. However, there's a misconception that deploying network segmentation, endpoint and remote access cybersecurity solutions to prevent such breaches is a complex and costly process.

A large clothing retailer turned to Blue Ridge Networks to securely segment their networks to protect PoS devices and cardholder information while enabling rapid and highly available connectivity, with cost as the number one priority.

Clothing Retailer Trusts Blue Ridge Networks' Security Model

In an ultra-competitive market, with brand loyalty in flux, the clothing retailer recognized that eliminating the risk of breaches was a must. The CIO of the company, leading the search for a new solution, placed a premium on security and was looking for a vendor that could meet key business, networking, and security requirements to connect and protect the company's stores within a set budget.

The retailer required a solution that:

- **Was affordable**, providing a fixed cost per store
- **Secured cardholder data** in accordance with PCI Data Security Standard
- **Offered ISP redundancy** at both the store and the transaction processing site to maintain uptime of PoS devices
- **Enabled secure remote access** to each retail location
- **Was easy to implement**, limiting involvement from in-house IT staff
- **Could be centrally managed by the vendor,** reducing the need for internal firewalls and configuration for each site

Benefits At A Glance

50% Reduced CapEx and OpEx through PCI Network Simplification

Complete PCI Audits 60% Faster Without Additional IT Staff

Reduced Attack Surface by 90% through cloaking, network isolation, and encryption

Connect Remote Store Networks 70% Faster

The Solution: Zero Trust Segmentation for PCI-Compliant Networks

Blue Ridge Networks' LinkGuard platform enabled the retail organization to isolate and segment hundreds of PoS systems in order to comply with PCI DSS . The organization benefited by reducing the amount of time, costs, and effort for audits and reduced their attack surface through network segmentation, encryption, and cloaking.

Automatic and Verifiable Failover

Whether it's a service interruption, lack of broadband in rural areas, inclement weather, or any other type of disruption, retail organizations are highly susceptible to outages and downtime. To maintain IT agility, this retailer needed to ensure they had a rapid failover strategy to maintain operations without disruption or financial loss. Yet, traditional failover architectures typically consist of slow routing convergence, complex DNS configuration, link failures across wired or cellular, and often don't revert to their primary state when it is made available again.

LinkGuard allows the organization to securely connect any device, over any network, to any location, with little to no changes to the underlying network infrastructure. LinkGuard upholds a resilient, fault tolerant architecture by using a layer 2 over layer 3 approach so that regardless of the network media through which the connections are established, all the interconnected systems appear to be on a common ethernet network. Failover is now automatic and verifiable because LinkGuard's encryption and forwarding logic doesn't depend on IP addresses and protocol types. Instead, the failover information is preconfigured and contained within the policy token. Retail organizations can reap the benefits of real-time traffic routing without IP addressing issues or complex configuration changes. In addition, the LinkGuard system verifies path viability, ensuring that if Broadband fails at each remote store then it will automatically failover to wireless. All wireless connections used pooled minutes to keep operational costs to a minimum.

Seamless PCI Compliance Through Network Cloaking

According to the 2018 Thales Data Threat Report, 50 percent of U.S. retail survey respondents reported a breach in 2017. As payment security breaches have increased throughout the years, retailers are faced with an increased number of controls required by the PCI DSS and an increased fine for noncompliance. Yet, even PCI compliant organizations are still experiencing breaches. With the cost and complexity of deploying traditional IT solutions across disparate remote stores, it becomes extremely challenging to ensure all controls are in effect.

With LinkGuard, the retail organization was able to create secure and segmented networks within hours rather than days or weeks compared to traditional IT solutions. PoS devices and other critical PCI assets were segmented in their own encrypted overlay network and isolated from non-PCI networks. LinkGuard also encrypted all data in transit from PoS systems to payment processors. Additionally, LinkGuard appliances use an identity centric approach, where network access control is based on a cryptographic identity. Data is only transported after a cryptographic tunnel is created between two peer LinkGuard appliances.

This allows the overlay segments to become immune from man-in-the-middle attacks, IP spoofing, credential theft, and other network-based attacks. Any other request to communicate with the segmented devices is denied, resulting in a secure and segmented network that is cloaked from outside view and bad actors.

Managed Network Security Services Delivers Unrivalled Support

By using Blue Ridge Networks' managed services, the retailer gains continuous support for its deployment and offers security and architectural enhancments. Blue Ridge Networks' secure operations team manages firewalls to enforce strict egress and ingress security policies, including white-listed sites.

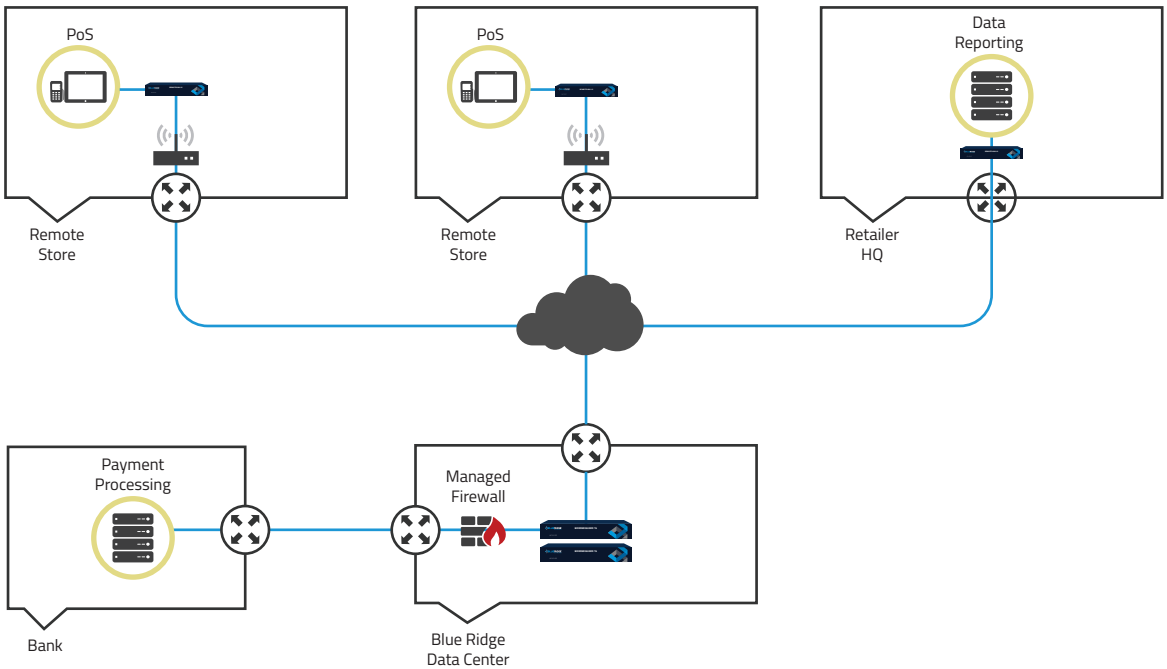
Blue Ridge Networks also provides secure access to third-party vendors to manage their equipment. A report is generated for the IT staff of the retailer which includes the health of each store, and alarms are sent if any devices are offline.

"While undergoing a PCI compliance audit, our QSA contacted us worried that there was a problem because they couldn't find any of the IP addresses of the devices and servers within our network. We assured them that all systems were up and running and that they were just undiscoverable from any outside scan because of Blue Ridge's security products."

- CIO, Large Clothing Retailer

Deployment Architecture

Redundant BorderGuards are hosted in the Blue Ridge Networks Tier 1 secure data center, pooled in an auto-failover configuration, and serve as the aggregator for encrypted traffic from each store to payment processing servers. Each of the 220 stores has a pre-configured RemoteLink, plus and internet connection, and a cellular modem for automatic failover for store communications. This sends encrypted traffic from PoS devices to the BorderGuard pool for processing. By providing secure segmentation of the PCI traffic from non-PCI data, Blue Ridge Networks ensures that the retailer's PCI standards are met. A RemoteLink is also deployed in the retailer's headquarters for reporting.



mhoffmann@blueridgenetworks.com
7044092411
BlueRidgeNetworks.com

©2019 Blue Ridge Networks, Inc.. Blue Ridge®, BorderGuard® and EdgeGuard® and all associated logos and designs are trademarks or registered trademarks of Blue Ridge Networks, Inc. All other reigstered trademarks or trademarks are property of their respective owners.