Achieve Digital Transformation Without Compromising Business Continuity and Data Security at All of Your Stores

How specialty retailers innovate while protecting the brand and profitability with a software-defined branch network (SD-Branch)
Innovating for the sake of customer experience is a must, but it comes with risks that are not easily tolerated by the tech-savvy retail business. A heavily leveraged network that is increasingly reliant on optimal performance and uptime is a disaster waiting to happen if it’s not properly secured and monitored.

You’re under increased pressure to cater to new generations of hyper-connected shoppers and optimize Point-of-Sale (POS) transactions. This means streamlining operations while improving customer experiences like self-checkout, loyalty program applications, plus cloud-connected IoT devices. But how do you address the security and business continuity challenges this creates?

**Four key challenges facing retail digital transformation**

**Security challenges**

As a retail technology professional, you are well aware of the large number of devices that connect to the network via Ethernet and Wi-Fi. IT sprawl at each store adds complexity to network visibility and security, and that complexity means increased risks of a breach. Endpoint security alone, without proper edge security, won’t be enough to reduce risks. Even a next-gen firewall service won’t always be sufficient to secure the perimeter.

It all comes down to your level of risk tolerance, but week after week organizations are breached that fail to detect the threat early, and respond rapidly and effectively. Traditional network security solutions do not provide the level of visibility and control that is required to face today’s threats, like ransomware.

*Ransomware attacks occur every 14 seconds*

Source: Cybersecurity Ventures

Business continuity challenges

Network performance and resilience also suffer from the increase of connected devices and apps, and subsequent growth of bandwidth demand that comes along with the digital transformation of the business. Quality of Service (QoS) is now a major concern, especially when migrating out of legacy Multi-protocol Label Switching (MPLS) links to reduce cost, increase bandwidth, and gain operational efficiencies.

To avoid store-and-forward of payments and prevent revenue loss, retailers find themselves with the need to preserve optimal uptime. Blackouts and brownouts not only impact short-term revenue but may also impact long-term when the customer experience is negative due to business downtime. It is paramount to be able to accept and process payments even during a blackout of the ISP broadband connection while keeping the mission-critical applications connected and be able to connect to key cloud-based apps.

Nearly 50% of customers avoid a retailer or brand in the future if they had to wait longer than five minutes in line. One out of three customers will abandon the checkout line if forced to wait that much.

– Retail Customer Experience.

Like with the security challenges mentioned earlier, it all comes down to the risk tolerance of business downtime. When security fails, a blackout may ensue. But most of the time blackouts are inevitable because they originate at the ISP. ISP reliability can become a headwind rather than a tailwind, blowing against the digital transformation of the retail business when their traditional approaches to network resilience and availability no longer suffice. An uptime of 99.9% is no longer enough.

Agility and versatility challenges

Digital transformation at brick and mortar retail business can drive an increase in IT complexity and hardware sprawl at the stores. It would not be surprising these days to find a closet full of appliances, cables, and blinking LED lights at any given point-of-sale. The reality is that most of that hardware goes under-utilized and is expensive to manage and provision. Frequent truck rolls/technician visits are the norm, and capital and operation expenses go up with each new gadget.

Furthermore, connecting and securing new locations can take weeks or even months if connecting an MPLS link to a branch location. Besides, MPLS is cost-prohibitive at many locations and has bandwidth limitations. Attempts to deliver a better on-site digital experience can backfire if the network is not properly designed to be agile and versatile in nature.

Infographic: MPLS vs SD-WAN
netsurion.com/knowledge-center/infographics/mpls-vs-sd-wan

On average, every minute of POS downtime costs the retailer $4,700 – Source: Standish Group.
On the other end of the spectrum, stores connecting via broadband using Virtual Private Network (VPN) tunnels to other stores, to headquarters, or to a colocation, face the difficulties of managing those hub-to-spoke and spoke-to-spoke WAN configurations. Hybrid networks are complex to manage and secure; the lack of enough talented cybersecurity specialists only makes it more challenging.

To reap the rewards of digital transformation in this market, retailers and the Managed Service Providers (MSPs) that serve them need to simplify network security, reduce the amount of single-purpose hardware solutions, consolidate IT bills as much as possible, and minimize the number of truck rolls to the store locations.

Compliance management challenges

Payment Card Industry Data Security Standard (PCI DSS) compliance, although a basis to start when building a sound cybersecurity strategy, gets challenged when new types of devices connect to a store’s network, such as IoT devices and innovative POS systems. PCI DSS is not a checklist; it is a minimum practice to manage. But the risk of exposure to vulnerabilities increases with every new type of device that connects from within the LAN. “Fear the hacker, not the auditor”, it’s been said.

In short, being PCI DSS compliant is not enough these days. New digital experiences for shoppers require increasing the protection of their transactions and information, while also making sure a zero-trust security policy is in place and that full visibility and control of the network is possible. It is absolutely necessary to separate mission-critical from non-critical traffic.
When Digital Transformation Equals Digital Disruption

SD-Branch helps overcome those challenges

**What is SD-Branch?**

Software-defined branch networking is the next step in the evolution of branch technology. SD-Branch can be defined as a single hardware platform that supports SD-WAN, routing, integrated security, and LAN/Wi-Fi functions that can all be configured and managed centrally via the cloud. This hardware platform is known as the “universal Customer Premise Equipment” (uCPE), which is essentially a multi-function edge appliance that delivers all-in-one connectivity, resilience and security services to a branch location. The uCPE is managed via an orchestrator, a web-based console, that runs in the cloud and enables the SD-WAN functionalities.

**SD-Branch vs security challenges**

One advantage of a robust SD-Branch solution is the capability to deliver multiple security functions using a single device, the uCPE, installed at the retail shop. By connecting the uCPE between the ISP modem and the LAN, it is possible to see and control all the traffic that comes in and out of the network (not all SD-Branch solutions can deliver this capability). Deep Packet Inspection of all encrypted data, including first packet detection at layer 7 (app level), enables threat detection and response at the edge. A robust SD-Branch can see all the applications communicating within the LAN to the internet, and who they are communicating with.

Although an SD-Branch appliance can replace an on-premise firewall or Universal Threat Management (UTM) box at the location in many use cases, it isn’t necessary to do so. An SD-Branch solution can complement a firewall and UTM, but for small-to-medium size retail shops, it often makes more sense to rip and replace in favor of a single SD-Branch device at the edge. This allows for consolidating functions into a single piece of hardware, which reduces IT sprawl at the site, and ultimately, exposure to cyber threats.

Netsurion BranchSDO (netsurion.com/solutions/sd-branch) adds additional capabilities such as cellular failover, Auto VPN site-to-site meshing, orchestrated internal vulnerability scans, cloud-delivered next-gen firewall, smart traffic steering, PCI DSS compliance tools and support, and other features.
**SD-Branch vs business continuity challenges**

The multi-carrier cellular failover capabilities of a robust SD-Branch solution delivered via integrated modem is central to delivering the network resilience necessary for a successful brick and mortar retail business. When broadband connectivity fails, it becomes imperative to stay in business, not just for the sake of avoiding revenue loss, but also to continually deliver a positive experience to the customer. Cellular failover kicks in only when needed, whether during a blackout or when overall QoS drops below a pre-established threshold. The goal is to move from a 99.9% uptime standard to the “four nines”, which is 99.99%. A positive by-product of automatic cellular failover is avoiding store-and-forward transactions and potentially losing revenue.

By building the cellular modem into the uCPE box and managing it via the cloud-based orchestrator, SD-Branch reduces hardware sprawl at the location and simplifies business continuity management. External modems are no longer needed and there is one less management console to deal with.

Resilience not only means ensuring that the stores are always connected to the internet, but it also means that they can always reach headquarters, a colocation, cloud apps, and the other branches via any of the secure VPN tunnels. VPN management can be extremely complex and work-intensive but the ideal SD-Branch solution includes Auto VPN, which delivers that network resilience and availability.

The ideal uCPE for a retail store use case includes an integrated modem and dual SIM for dual carriers. Netsurion BranchSDO has the ability to steer traffic based on pre-established policies and is able to manage various LAN segments differently during a blackout or brownout. Dual carrier capability enables the system to select the one with the strongest signal in that area at the time. With the broad deployment of 5G networks in 2020, any latency concern about connecting via cellular would disappear.

Whitepaper: Top Considerations When Choosing a Failover Solution - [netsurion.com/knowledge-center/whitepapers/4g-failover](netsurion.com/knowledge-center/whitepapers/4g-failover)
**SD-Branch vs agility and versatility challenges**

By adding managed services delivered through the appliance, SD-Branch facilitates transitioning from a CapEx model to an OpEx model in which services can be scaled up and down based on needs at the time. The total cost of ownership (TCO) is vastly reduced and franchises can focus on selling rather than troubleshooting expensive, and often under-utilized, network security appliances.

But is a uCPE a single point of failure? The reality is that the uCPE boxes come pre-configured and can be re-configured remotely very quickly, making replacing a malfunctioning device simple. Indeed, connecting a new retail store can be done by non-technical staff in a matter of minutes. The same applies for a replacement. The ease and speed of deployment are among the most valued benefits of SD-Branch by highly distributed businesses and the MSPs that serve them.

BranchSDO also facilitates the orchestration of Internal Vulnerability Scans (IVS). It is possible to schedule regular scans of different stores across the network, choosing the best times for each in order to be as non-intrusive as possible. Another example of agility is the speed and ease to create site-to-site VPN meshing. The virtualization of network functions has benefited distributed businesses and MSPs as much as it has benefited data centers. Agility is the element of SD-Branch that is most valued by MSPs serving cost-conscious clients because of the rapid service and the cost-efficiencies.

If you are curious about how easy it is to connect a uCPE, check out the following video: [youtube.com/watch?v=Q52cCcSk6C0](https://youtube.com/watch?v=Q52cCcSk6C0)

**SD-Branch vs compliance challenges**

Branch solutions check many boxes when it comes to PCI DSS compliance. The ability to segment traffic is essential to ensure that credit card transactions are protected from untrusted traffic. Going beyond PCI DSS compliance is the possibility to switch LAN ports in the uCPE to WAN and vice versa, and to close the unused ones to prevent rogue devices to be connected to the network via ethernet. BranchSDO is a comprehensive SD-Branch solution with security at its core, which offers PCI DSS tools and support. The Netsurion CXD edge appliances are purpose-built for small-to-medium size branches typical of the specialty retail industry. They also offer audit trail, log keeping, and fulfill many PCI DSS requirements. An SD-Branch solution that caters to retailers must offer the necessary add-ons to help not only demonstrate compliance but to go beyond the minimum and comprehensively protect their brands.
The future of retail networks

SD-Branch is the future of retail network management. SD-Branch delivers the scalability and versatility needed to keep innovating and transforming the business to stay competitive while addressing network security and business continuity. As hybrid networks become more complex, threat prevention, detection, response, and prediction becomes more demanding intellectually and financially. SD-Branch responds to those challenges by reducing complexity and cost and by improving security and resilience. A managed SD-Branch service is the way to go specialty retailers. Ready to see how SD-Branch can help you more cost-effectively drive innovation without risking security, resilience, or compliance? Contact Netsurion to speak a solution advisor.

Additional Resources:

Article: The Four Elements that Build a Better SD-WAN for retail
netsurion.com/knowledge-center/articles/2019/april-2019/the-four-elements-that-build-a-better-sd-wan-for-retail

Webcast: Building a Better Branch with SD-WAN
netsurion.com/knowledge-center/videos/building-a-better-retail-branch-with-sd-wan
Netsurion powers secure and agile networks for highly distributed and small-to-medium enterprises and the IT providers that serve them. In such environments, the convergence of threat protection and network management are driving the need for greater interoperability between the NOC (network operations center) and the SOC (security operations center) as well as solutions that fuse technology and service to achieve optimal results. To this end, Netsurion has converged purpose-built network hardware, innovative security software, and flexible managed services. Netsurion’s SD-Branch solution, BranchSDO, is a comprehensive network management and security solution consisting of SD-WAN, next-gen security, cellular, Wi-Fi, and PCI DSS compliance tools and support. At the heart of the solution is the CXD, Netsurion’s SD-WAN edge appliance.

Netsurion’s Security Operations solution, EventTracker, delivers advanced threat protection and compliance benefits in a variety of deployment options: a SIEM platform, a co-managed SIEM service with 24/7 SOC, and a managed SIEM for MSPs.