RFCODE
CRITICAL ASSET TRACKING & PROTECTION

WHITE PAPER

# Retailers On The Edge

## Managing Edge Deployments to Drive Customer Engagement

## Introduction

While e-commerce is a growing segment in retail, 90% of retail purchases[1] are still made in a physical store. This means the in-store customer experience can play a crucial role in making the sale. Today's consumers have grown accustomed to seamless interactions online and are increasingly comfortable with omnichannel shopping. And they look to bricks and mortar retailers for the same service – addressing their questions and needs in real time. These expectations make it mission critical for retailers to have the IT infrastructure in place to keep their customers satisfied.

The in-store retail experience is important for building customer engagement and driving revenue as quickly as possible. Consumers want what they want, when they want it – 85% expect[2] in-store retail associates to be able to check inventory and pricing in real time with handheld or fixed devices. And customers are willing to walk way when a retailer can't give it to them – 69% of consumers[3] are more likely to shop with a competitor after just one bad experience in a retail store. Ignoring this is not an option: Digital interactions, either in-store or online, influence 56 cents of every dollar spent[4] in a physical store.

> *"Digital sales continue to grow, but it's no longer a competition between online and offline. Today, many retailers find that half of their online sales are supported by their stores."*
>
> *- Robert Hetu, Gartner*

How do retailers support the IT infrastructure required to provide real-time, location specific digital service to enable these experiences for customers? By employing

1 US E-Commerce Sales as Percent of Retail Sales , https://ycharts.com/indicators/us_ecommerce_sales_as_percent_retail_sales
2 Annual Connected Retailer Survey: New SOTI Survey Reveals U.S. Consumers Prefer Speed and Convenience When Shopping with Limited Human Interaction , https://www.soti.net/resources/newsroom/2019/annual-connected-retailer-survey-new-soti-survey-reveals-us-consumers-prefer-speed-and-convenience-when-shopping-with-limited-human-interaction/
3 The 4 Reasons Shoppers Don't Come Back to Stores , https://www.mytotalretail.com/article/the-4-reasons-shoppers-dont-come-back-to-stores/
4 Deloitte Studie: Global Powers of Retailing 2018 , https://www2.deloitte.com/content/dam/Deloitte/at/Documents/about-deloitte/global-powers-of-retailing-2018.pdf

edge computing as a tether between in-store interactions and the enterprise network. This is the only way to successfully support the technologies that modern consumers expect like point of sale devices, real-time inventory updates, and analytics that offer up personalized service. If you wonder how important the edge is for retailers, just ask Target[5] what happened when their systems went down for two hours one Saturday in June.

## How Retailers Are Using The Edge

Edge computing requires IT equipment close to the point of sale – servers, routers, gateways, and switches in closets or micro data centers. Retailers use the real-time capabilities of edge computing for these mission critical services

1. Point of sale devices: Cashless checkout stations, self-checkout kiosks, handheld devices

2. Report real-time inventory: For customer service, improved inventory tracking (including tracking temperature to avoid spoilage of food products), demand forecasting, and dynamic pricing

3. Geolocation: Using beacons and GPS to drive advertising and apps and make localized offers

4. Smart technologies: Robots that can scan and restock shelves, greet customers, and answer customers' questions; digital signs, video displays, virtual reality, fitting rooms with augmented reality mirrors (consumers can see how they look in clothes without physically trying them on)

5. Video: Security, managing lines at the checkout, and video analytics (including analyzing facial expressions for customer satisfaction and demographics)

6. Big data analytics: Capturing customer information while in the store, from bar codes and checkout scanners

7. In-store ATMs

5 Target says cash registers back online and customers can make purchases again after systems outage , https://www.cnbc.com/2019/06/15/targets-in-store-payment-is-system-down-impacting-stores-nationwide.html

These services require continuous, reliable, low latency service. And that requires equipment like servers and routers in each store that offers these capabilities – connected to the enterprise network and also able to operate independently from it. No matter how far this equipment is from the core data center, it has the same demands and accountability requirements as the rest of the enterprise IT infrastructure. Yet unlike a data center that is staffed and monitored 24/7, edge computing equipment is usually left on its own, without IT staff on-site or even physically close to the store. Meaning it can take critical minutes or hours to service the equipment and meet computing demands if something goes wrong.

Retailers don't always view edge computers and servers with the same filter as they do the IT equipment in the core data center. While they discuss the technical side of the equation – like latency and storage requirements – some still consider edge computing equipment a nice to have feature. Yet with the edge enabling increasingly mission critical services like those above, edge IT infrastructure and network operations need to be secure and to perform seamlessly, just like the core data center, to meet customer expectations and drive company revenue.

### Benefits of the Edge

Edge computing is all about increasing bandwidth and IT availability to handle local transactions and stream massive amounts of data without interruption. And to do this without relying on central or regional data centers and the time it would take to send data there and back.

Distributed computing like this also gives retailers a level of resiliency for business continuity. By using computing equipment close to the end-user location, rather than the enterprise data center, a retailer can continue to operate when a centralized function fails. By capturing data and storing it locally, edge facilities protect customer experience, and safeguard a retailer's reputation and revenue.

Had Target been using edge data centers in all of its locations, the story of a two-hour outage in June 2019 would be quite different. The outage affected all Target stores on the eve of Father's Day in the U.S., and cost the retailer an estimated $50 million in sales[6]. The non-security related internal technology issue disabled registers in all Target stores because they relied on the central data center.

## Challenges of The Edge for Retailers

There are two major challenges for retailers dealing with edge deployments in their store locations: managing the edge equipment and services, and security.

Managing edge deployments requires planning beyond that for a traditional, on-premise data center. Given the number of outlets many retailers have, this makes the enterprise IT network exponentially more complicated to operate and monitor. To be an effective strategy, the edge equipment has to manage itself and work independently of the network topology, as well as be reliable, with 100% uptime.

Security is always a particular concern for retailers. Among their own proprietary software and sales and analytics data, edge equipment handles customers' credit card data and personally identifiable information. Threats to the safety of that information come from both the environmental conditions of the location housing the edge equipment and a physical breach of doors and safety measures protecting the assets.

6 A $50 Million Glitch? Target Takes a Hit From Register Outage , https://www.datacenterknowledge.com/uptime/50-million-glitch-target-takes-hit-register-outage


Environmental conditions can threaten equipment on the edge, such as damage from storms, fires, or a leaking pipe that impacts a retail location or the area where the equipment is housed. This can be disastrous when data is lost before being backed up.

Physical protection from hackers is an issue, too. With server and routers and other equipment dispersed in locations without on-site IT staff, retailers rarely know who accesses equipment and when or if those individuals are authorized. Roughly 30% of breaches[7] are attributed to a hacker having direct, physical access to IT infrastructure, making physical protection critical for securing the equipment and the data it houses.

There are several regulations that require businesses to both physically and logically protect customers' financial data and personally identifiable information (PII).

## PCI DSS

The Payment Card Industry Data Security Standard (PCI DSS[8]) is a global security standard that applies to any businesses that handle credit cards. The purpose is to ensure that retailers and other businesses who deal with PII and credit card information take steps to prevent fraud or data theft. It requires the physical security of IT equipment housing this type of information, including access control and video monitoring.

This level of protection is a must given that this information is a treasure trove for hackers. Retailers are a particularly appealing target as credit and debit cards account for two-thirds of purchases[9] in the U.S. Retailers handling credit cards that don't comply with this standard can be fined up to $100,000 a month or $500,000 per security incident.

## Sarbanes-Oxley Act SOX

The Sarbanes-Oxley Act (SOX) applies to public companies in the U.S., and is designed to protect shareholders and the public from fraud and accounting errors. The act addresses how companies report on and control their financial information. This requires that companies secure their IT infrastructure that deals with financial data, as well as securing the data itself.

## HIPAA

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a U.S. federal law that applies to retail pharmacies, which have access to protected health information (PHI), both in physical and electronic form. HIPAA dictates how pharmacies can use and disclose the information and requires that information is safeguarded at all times to "ensure the confidentiality, integrity, and availability[10] of physical and electronic PHI."

Health information is particularly sensitive and there are significant fines for violating HIPAA protections. In 2009, CVS settled a case for $2.25 million after discovering that PHI on prescription bottles and receipts had been improperly disposed. In 2010, Rite Aid settled for $1 million for a similar violation.

7 Revolutionizing the consumer experience at the edge , https://www.datacenterdynamics.com/analysis/revolutionizing-consumer-experience-edge/
8 PCI Securtity, https://www.pcisecuritystandards.org/pci_security/
9 Verizon 2015 PCI Compliance Report Executive Summary , https://enterprise.verizon.com/resources/reports/2015/pci-report-2015-executive-summary.pdf
10 HIPAA Compliance for Pharmacies , https://www.hipaajournal.com/hipaa-compliance-for-pharmacies/

## The Problematic Edge

In today's in-store retail environment, the edge can complicate matters for retailers even as it allows them new opportunities to compete for consumers' attention and drive real-time and omnichannel experiences. A true edge deployment requires a server closet or small data center in each physical location. This means that in addition to the enterprise data center a retailer's IT team can be responsible for hundreds of geographically dispersed locations, each with several pieces of equipment. This enlarges the network's footprint significantly.

Because retailers usually lease store locations, IT teams have little ability to customize the spaces to create an environment similar (or closer to) their traditional data center. There is little consistency – each space, in each retail location, presents its own issues in terms of managing IT equipment like power supply, air circulation, cooling, internet access, and bandwidth. Some locations may have dedicated space for servers and routers and other equipment, while others may have to use a broom closet or corner of their stock room to set up the equipment. The IT team has to choose the equipment, deploy it and connect it to the network, and then secure it, no matter what the physical locations look like.

In most cases, it's simply not possible to physically secure these non-traditional physical locations to the same level as the core enterprise data center. In addition to the physical limitations of the various environments, store personnel are not equivalent to trained IT staff. These individuals likely don't have awareness or training to secure and protect the IT equipment. Without on-site IT, the enterprise loses critical visibility to ensure physical security and optimal operating conditions. This makes it difficult to identify, diagnose, and fix problems in edge deployments quickly.

Managing the retail edge is only feasible at scale with hands-off operations and management. As these servers and micro data centers become more distributed and interconnected, it's more critical to be able to monitor and manage the equipment from a centralized location to enable real-time solutions in each retail outlet.

## The Solution

This distributed retail environment requires a secure, manageable edge, that can be deployed in remote locations without any on-site IT support. The only way to do that effectively is to have the ability to monitor each edge deployment from afar, back in the enterprise data center or headquarters facility. Visibility into these highly distributed spaces is required for IT to diagnose and fix problems quickly and enable uninterrupted operation.

Real-time monitoring with sensors and video, and alerts when they are exceptions to normal conditions (such as water on the equipment or an unlocked or open door), enables immediate response to issues to avoid or minimize downtime.

## Asset Management

Monitoring critical assets means using sensors to understand their state of being – on or off, provisioned or idle, etc., and their physical location – such as in storage or on the loading dock or in a rack or closet at the retail store. This becomes more difficult and complex as assets are deployed across potentially hundreds or thousands of edge locations.

For example, if you need to take a specific number of servers out of service because they're at the end of their lifecycle, it makes the job simpler and cost effective when you know where they're located. It also makes the job easier when you know what servers you have in inventory to deploy as replacements, to prevent overprovisioning and ensure you're effectively using your capital assets.

## Physical Security

Sensors alert you to unauthorized access to remote facilities to access the data or remove the equipment, which can result in theft of equipment or sensitive data and even regulatory violations because of inadequate privacy policies. Proper monitoring with sensors and video protects companies from additional regulatory fines or reputational risk after theft or a security breach by proving that equipment was protected at an acceptable level.

## Environmental Conditions

Monitoring environmental conditions means sensors that track the atmosphere in the physical space – including temperature, humidity, airflow, air pressure, water, vibration, etc. Monitoring the environmental conditions across what can be thousands of edge facilities is equally as complicated as tracking physical location. For example, different weather conditions in disparate geographical locations require unique understanding of climate, seasonal fluctuations, and local weather and how that impacts sensitive IT equipment.

Keeping track of locations and conditions of IT assets is only the half the reason monitoring matters. The other half is using the information to make informed decisions and then take action. Monitoring and exception alerting can reduce the time to resolution for servicing equipment or environmental hazards – giving your IT team time to respond to a location or send local resources to server or repair; or to take the proper security steps when it has been ; determined that unauthorized personnel have accessed equipment.

# CenterScape Edge Manager

RF Code's CenterScape Edge Manager addresses retailers' edge deployment needs. This solution monitors the edge environment (power and cooling, access and activity) and the assets (servers, networks, storage, racks and mobile devices) holistically and at scale. This hardware and software solution provides value beyond core enterprise data centers and into retail store locations. With real-time visibility and monitoring, exception alerting, and advanced reporting, this complete solution presents your IT team with actionable data to ensure safe, secure, and uninterrupted operations.

Combining easy-to-deploy wire-free sensors, a dedicated and secure infrastructure, and powerful data management software, CenterScape provides the continuous monitoring and the instant alerting necessary for retailers' IT staff to safely and securely deploy edge locations, anywhere, worldwide. It is designed to address the unique challenges and complexity of edge computing environments, increase operational efficiencies, improve security posture, reduce costs of managing equipment and deliver the simplicity, savings, and visibility needed to effectively operate on the edge.

If you're a retailer with data on the edge, which is likely given that retail is the fastest growing segment of the $6 billion edge computing market[11], you need a comprehensive edge management strategy for these highly distributed and difficult to monitor facilities. CenterScape Edge Manager is a key element of that strategy, tracking all your assets and their current location, down to the rack level, and monitoring environmental conditions and facility access.

Specifically designed with the unique monitoring and notification requirements of edge deployments, CenterScape provides real-time insight, and control over operational risks, costs, and compliance. This easy to use solution, accurate to the rack level and operating 24/7, provides reporting and accountability for compliance with regulations and service level agreements (SLA). As an open platform, this solution is designed to easily integrate with other data center management solutions like building management (BMS), data center infrastructure (DCIM), and integrated systems management (ITSM).

Edge facilities only bring that value when they're working efficiently, effectively, and at capacity. That requires granular, real-time intelligence and alerts for each of your retail locations. As edge computing is becoming more mainstream, RF Code's CenterScape Edge Manager empowers enterprises to leverage the edge effectively, make more informed decisions and make them faster, and optimize their performance and support business growth. To learn more about how monitoring your edge facilities can transform your company, contact RF Code today.

11 The edge takes shape: The 5G telco cloud that would compete with Amazon , https://www.zdnet.com/article/the-edge-takes-shape-the-5g-telco-cloud-that-would-compete-with-amazon/