Secure Access Service Edge (SASE) for Retailers

Recently, the retail industry has seen dramatic shifts in everything from customer transaction habits to how the workforces behind retail chains and online stores have adapted their work practices amid a global pandemic.

People shopped from home, for more goods than usual, more often, because of stay at home order restrictions and for general safety. At the onset of the pandemic, every retail company was forced to adapt to this online-first trend or else be prone to dwindling sales, closing physical locations or at worst, risk completely bankrupting their business and brand.

Savvy brands double downed on enabling better online experiences to adapt to their customers' new habits. Equipping customers with simplified checkout processes, promoting online-stores and mobile app usage, up-leveling online customer service functions and even shifting more budget toward online marketing were all things retail businesses did to capture as much revenue as possible online.

Online Shopping and Rise of Consumer Risks

In retail, a quick and seamless purchase experience is king; the faster the revenue can be captured, the better for the business. Though ironically it is this approach that often leaves companies exposed to attackers aiming to exploit their customers.

Retailers often need to manage massive databases of customer Personally Identifiable Information (PII) to offer loyalty programs which provide incentives for customers to make future purchases. Online commerce stores are also designed to authorize purchases and buys with as little friction (like security checks) to maximize sales. Companies looking to provide these customer-optimized shopping experiences store bank details, card information, physical addresses, names, phone numbers, and email addresses in their corporate databases and applications.

All this information is highly monetizable for cybercriminals, who historically follow where the money is.

The post COVID-19 circumstances meant that most retail companies saw a disproportionate amount of their revenues coming from online streams. As online sales and activity spiked, these cyber criminals were quick to evolve their tactics, taking advantage of vulnerabilities on e-commerce platforms.

The type of data compromised in the retail sector includes Payment (42%), Personal (41%), Credentials (33%), and Other breaches (16%).

- Verizon's 2021 Data Breach Investigations Report

Weak authentication controls allow attackers to access existing customer accounts, where stored payment details or customer rewards points could be stolen and abused. One time use "fake accounts" can easily be made online to be used with stolen credit cards for a very difficult to trace online theft.

With all the methodologies available to attackers looking to exploit an increasingly digital buying landscape, it has become more important than ever for retail companies to find the tools which provide the right balance between facilitating customer sales online and protecting customer data.

Securing a Distributed Retail Workforce

With back-office staff working from home and accessing sensitive customer and payment data on their personal or unmanaged devices through unregulated home networks, cybercriminals gained additional inroads into corporate networks without adequate safeguards. More retail staff became targets for social engineering attacks, whereby they were conned into giving attackers access to confidential customer information.

A distributed workforce also means a necessary adoption of cloud tools and platforms. Many of these tools store valuable digital assets, as the tools are used for internal staff collaboration, communication, and file sharing. Protecting assets stored and distributed across clouds requires an understanding of the nuances within the different environments, as well as expertise in managing multiple sets of security policies. With increased use of cloud collaboration tools, the available attack surface will continue to expand, as well as the expertise required to defend it (reflected by the proportionally increasing number of data breaches within retail in the past few years alone).

In this current era, employees accessing applications from HQ data centers and cloud apps need connections to be fast, reliable, and secure, though many of the biggest online retailers today are powered by legacy wide area network setups and perimeter-based firewalls. These companies find themselves struggling to support the security and access requirements that new work habits demand post pandemic, as their infrastructure was designed to only secure data stored within the corporate network perimeter.

This problem with distributed data access poses other problems on the customer side; e-commerce applications are typically bandwidth intensive and require constant availability, without which bring risks of losing sales to a competitor whose website is running and able to process sales when the customer demands it.

The results of these combined dynamics are worrisome for retailer brands: network disruptions, site down time, frustrated employees, and dissatisfied customers, all of which on a long enough timeline impact long term revenue and could tarnish brand loyalty and reputation.

Fragmentation in Security Lead to Critical Blindspots

For security teams, network and cloud visibility is a necessary asset, but is often yet another issue organizations face when it comes to controlling user access and enforcing consistent security.

Because their legacy wide area networks were designed to secure data within a corporate perimeter, the traditional remedy for most retail CISO and CIOs has been to install security products ad-hoc along the "riskiest" through points of their network, with the aim of securing data and devices within their perimeters.

Though with this approach, the integration and interoperability limitations of these tools make consistent enforcement across multiple platforms time-intensive, error prone, and costly, and further obscure the comprehensive view of the entire organization with product fragmentation and analytics fatigue.

Misconfigurations of access policy in the cloud result in serious consequences.

The median breach caused by cloud misconfigurations in 2020 resulted in the compromise of 10 million records, though one "mega breach" resulted in the exposure of over 20 billion records.

- Rapid7 2021 Cloud Misconfigurations Report

This fragmentation does no favors for retailers aiming to stay compliant with all industry-wide regulatory frameworks. Complying with GDPR, CPRA, and PCI-DSS requires maintaining a uniform security posture across the entire network and auditing capabilities to understand when an entity accessed or stored a particular type of data asset; two things which are incredibly difficult to achieve with a scattered collection security tools. Siloed security solutions fail to provide real-time information on changing security dynamics, user behavior, and threat vectors, and leave security teams with inadequate control over asset access.

This lack of a proactive security approach which uses real-time intelligence renders retailers ill-equipped to response in the event of a cyberattack. Retailers face network blind spots, policy misconfigurations, and ultimately data breaches if the traditional methods of protecting corporate and customer data are followed.

A Modern Solution for Modern Retailers

The modern line of thinking for retailers looking to secure their customers and data demands simplified access policies, holistic network visibility, and addresses customer data protection without sacrificing accessibility in an increasingly distributed workforce.

Secure Access Service Edge, or SASE, represents this approach, where proactive security services can enable both protection and seamless access to everything users have privileges to, anytime, and from anywhere. Versa SASE is the simplest way to secure and connect millions of access points in and out of company resources at scale.

Versa SASE includes security and networking services, though at its core entails Software-Defined Wide Area Networking (SD-WAN), Zero Trust Network Access (ZTNA), Secure Web Gateways (SWG), Cloud Access Security Broker (CASB), Firewall as a Service (FWaaS), and Remote Browser Isolation (RBI). All services are delivered through a single software stack, flexibly, through any deployment model (cloud, on-premises, or hybrid).

With Versa SASE, retailers have a single software stack delivering security and network services that address the complexities of the rapidly shifting demands of a distributed workforce and consumer data protection.

Consistent Policy Enforcement Everywhere

Access to the troves of customer PII data, such as credit card details, addresses, names, email addresses, require retailers to be vigilant about how they safeguard such critical information. Versa SASE enables simplified and comprehensive management for retailers to bring digital technologies, cloud platforms, branch offices, remote and mobile users under one single pane of glass to deliver access privileges to any user or device in the network or in the cloud.

This single-pane-of-glass interface, high-fidelity visibility into users (regardless of location), devices, applications, and security services across the entire organization becomes a tangible security asset.

Centralized control and real-time analytics help position security teams for effective capacity management, troubleshooting, threat detection, and network design validation. With this cohesive organizational view, retailer organizations can manage and update access policies of their entire workforce from a single interface, protecting all customer data at scale. Versa SASE operates from the cloud and delivers all security capabilities with a single unified framework, eliminating the need for stand-alone services.

Simplify Compliance Auditing

Adherence to GDPR, CPRA, and PCI-DSS and other regulatory codes that govern the retail service sector can seem like aiming at a shifting target. It can take hundreds of hours of employee and 3rd party effort to comply with these frameworks, and often there is little guarantee of avoiding fines or breaches. Retailers trying to abide might find themselves purchasing fragmented security products in hopes of compliance, only to learn that the rules changed.

With Versa SASE, organizations gain full picture visibility into all user and device access attempts, traffic throughput, and architecture. Security and governance teams can now gain the benefits of a single security event management console, complete with centralized reporting, logging and access controls, reducing the number of vendor audits from what could be dozens of tools down to one. In addition, change management for new compliance requirement are easy to manage through Versa SASE's single pane of glass policy configuration and reporting.

Happier Customers with High Performance Applications

Retailers are always looking for ways to make the shopping experience for the customer faster and easier. As the portion of online retail sales grows for many companies, a website optimized for the end consumer is necessary to compete for mindshare and purchases.

Secure SD-WAN, part of the Versa SASE architecture, lets retailers leverage economical transport routes such as broadband and 4G, 5G, and LTE to meet increased bandwidth demands. Traffic is automatically routed over the ideal transport route to ensure all applications run seamlessly and reliably, which means your customers can always have an excellent shopping experience and your entire workforce can focus on exceeding customer expectations.

Protecting the Future of Work

With the surge in customer purchases online, the growing trend of employees working remotely, and the evolving methodologies of attackers looking to scam businesses and consumers, the retail space is as difficult an industry to succeed in today as any other.

In a traditional perspective, corporate data access and protection is seen as a necessary practice which hampers employee productivity and prevents sales. Employees need to authenticate, authorize, and re-authenticate multiple times throughout the day just to be able to do their day to day basic duties.

Now, with VersaA SASE, access policy and security tooling can allow retailers easier corporate resource access for all employees, more website up-time instead of less, and complete visibility and policy management through a uniform, centralized console. Because Versa is able to leverage contextual information about the user and the device, authentication is only prompted based on risk rather than static policy. The dymanic model of protecting user access when risk is detected allows a distributed workforce to work both more securely and seamlessly.

In addition to protecting user access, data security is critical to the protection of PII data used in staff collaboration, communication, and file sharing tools. Versa SASE has the interoperability to work with 3rd party cloud platform to consistently enforce data policies across different environments such as Google Cloud, AWS, and Microsoft Azure. With increased use of cloud collaboration tools, the interoperability of security services everywhere is critical to protecting against breaches in the cloud and in the corporate network.

VERSA NETWORKS

Versa Networks, Inc, 6001 America Center Dr, 4th floor, Suite 400, San Jose, CA 95002 | Tel: +1 408.385.7660 | Email: info@versa-networks.com | www.versa-networks.com