CATO NETWORKS

vizst TECHNOLOGY

Securing Retail's Digital Edge

How SASE Protects Trust and Drives Competitive Advantage

Securing retail's digital edge:

How SASE protects trust and drives competitive advantage

The winners and losers in the retail industry are often separated by the narrowest of lines. Margins are razor-thin, competition is tough, and consumer preferences shift constantly in unpredictable ways.
In a hyper-connected world where customer expectations are high, businesses must ensure secure and reliable operations to stay ahead. A single security incident that hits a retailer can be the difference between profit and loss.

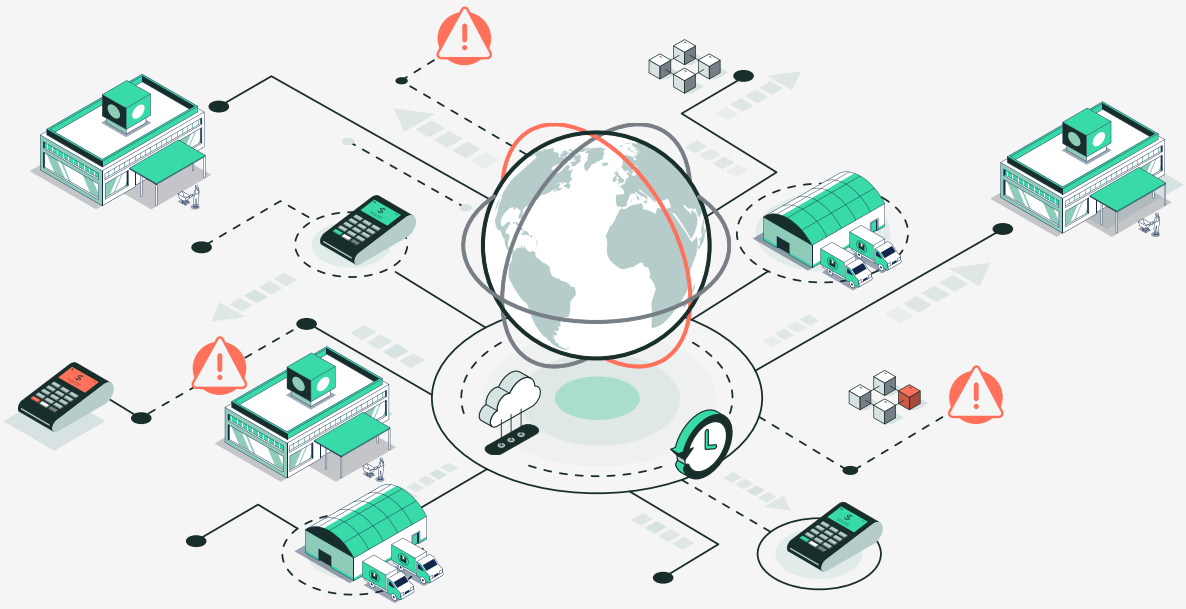
The cost of a breach: Trust at risk

According to IBM's Cost of a Data Breach Report 2023, as discussed in a recent "Cato Networks Cybersecurity Masterclass: Cost of a Data Breach — The Numbers Behind the Numbers", the global average cost of a breach rose to $4.45 million in 2023—a 15% increase over three years. That figure is almost certainly low, since certain costs are difficult to measure, such as an erosion of public trust.

Yet, when researchers attempt to measure things like trust and fear, the findings show that the impact of a breach affects many consumers' states of mind.

According to research from the Binghamton University School of Management, data breaches can trigger fear in consumers, and if the breach is large enough, fear and loss of trust tend to correspond with drops in the breached company's stock price.

Beyond security:
Retail's operational and digital risks



But it's not just security problems that can sink a retail business.

Retailers face a slew of other threats. Slow transaction times, supply chain issues, and even the failure to move quickly to capitalize on new product/service opportunities can put them at a competitive disadvantage against more nimble competition.

These challenges have triggered digital transformation initiatives across the retail sector. In this white paper, we'll investigate how to build and maintain trust with your customers, employees, partners, and investors with a security-first digital foundation.

- **Slow transaction times**
- **Supply chain issues**
- **Failure to move quickly to capitalize on new product/ service opportunities**

Why digital transformation efforts often fail to deliver on expectations

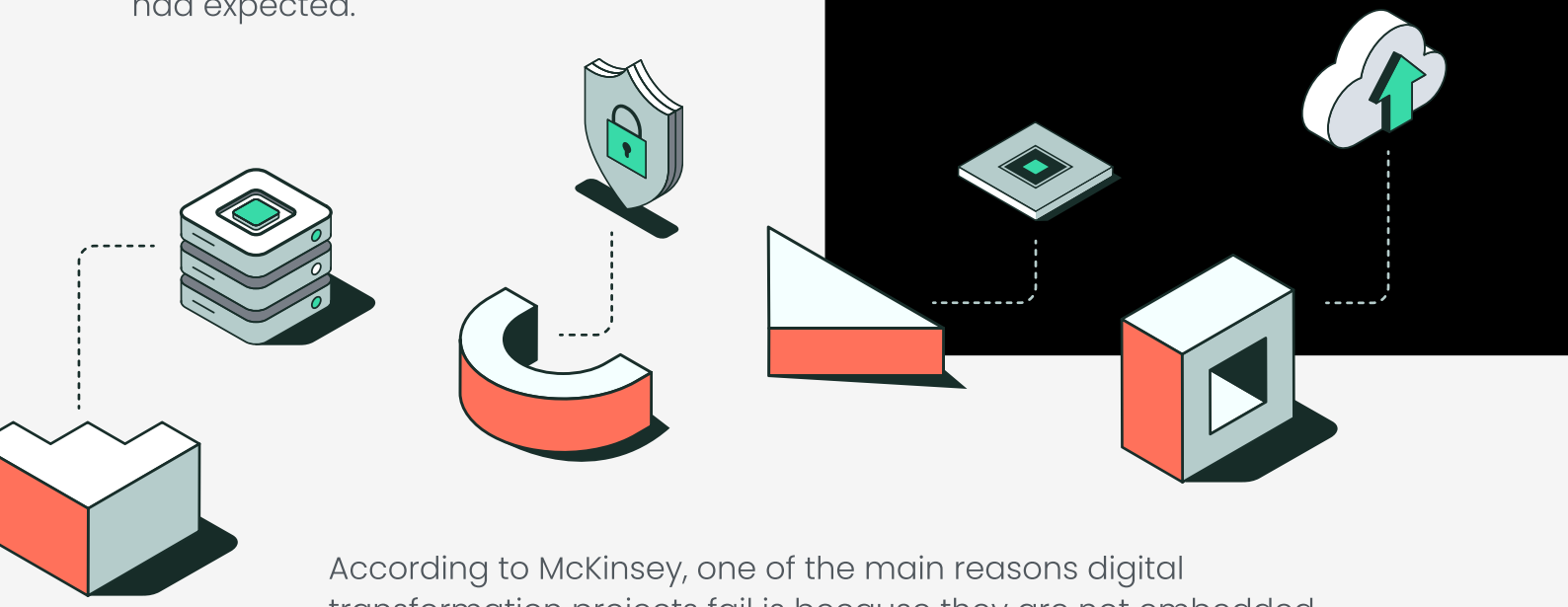
The rise of e-commerce has driven transformation across retail organizations—from warehouses to offices to storefronts—but many of these initiatives fail.

According to a 2022 study by McKinsey, which surveyed more than 600 businesses that have embarked on digital transformation journeys, only 20 percent managed to attain three-quarters or more of the revenue gains they had anticipated going into the transformation project. And only 17% managed to drive down costs by three-quarters or more of what they had expected.

only

20%

of retailers achieve at least 75% of their expected revenue gains from digital transformation.



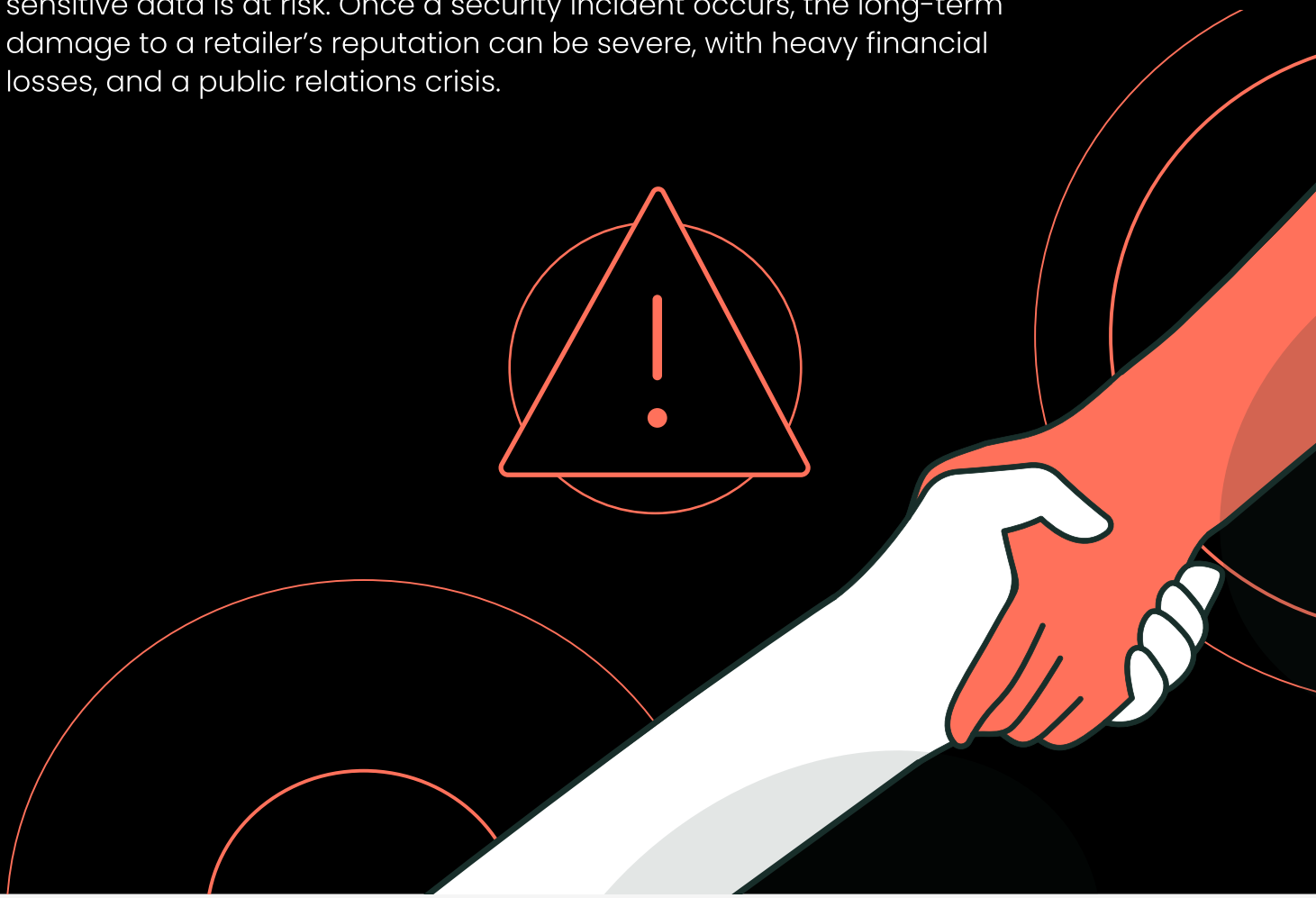
According to McKinsey, one of the main reasons digital transformation projects fail is because they are not embedded throughout the organization. Digital transformation tends to be isolated in departments, with efforts uncoordinated, often duplicated, and even worse, at cross-purposes with other projects siloed somewhere else in the organization.

To keep up with competitors digitally, retailers must synchronize their transformation efforts to deliver on and maintain three essential characteristics to succeed in a digital economy. Those characteristics are value, convenience, and trust.

How legacy solutions undermine value, convenience, and trust during digital transformation

To compete today, retailers must provide their products/services at the right price point (value), at the right time, usually "right now" (convenience), in a secure way that doesn't expose consumers' personal information to thieves, scammers, and other bad actors (trust).

Retailers face major challenges in maintaining trust, especially when their systems are outdated. Trust is the basis of consumer and customer loyalty, and when things go wrong, any issue can start trust erosion. Nothing shakes customers more than the fear that their sensitive data is at risk. Once a security incident occurs, the long-term damage to a retailer's reputation can be severe, with heavy financial losses, and a public relations crisis.

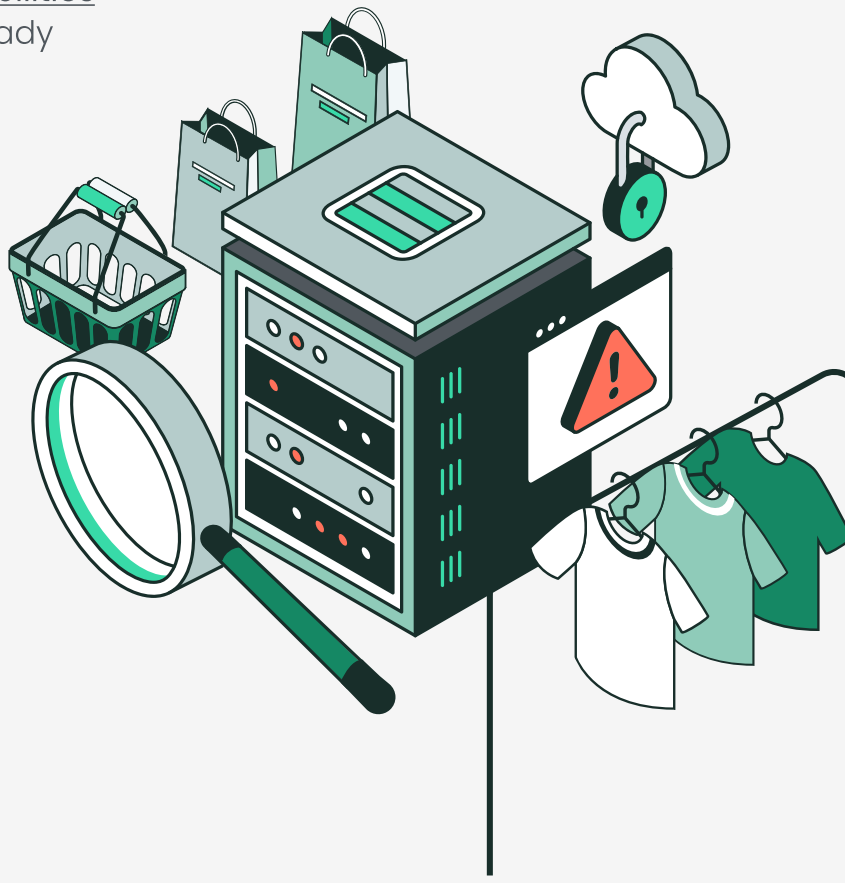


The risks of modernizing on legacy infrastructure

While retailers invest heavily in modern IT—migrating systems to the cloud, containerizing applications, and interconnecting the value chain from warehouses to websites to brick-and-mortar stores—legacy constraints threaten to undermine the benefits of transformation.

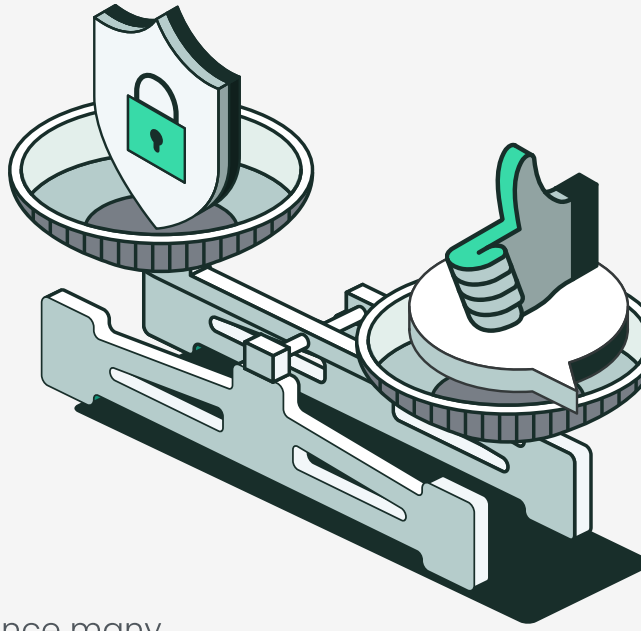
Digital transformation may provide a competitive advantage against more technophobic competitors, but only when value, convenience, and trust are maintained during the transformation process. If, on the other hand, retailers move too many sensitive assets into poorly secured systems, their attack surface expands, and a single security failure could cause significant damage.

This is why legacy technologies can be especially dangerous in retail environments. Attackers exploit known vulnerabilities, i.e., vulnerabilities that should have been patched or closed with updated tools. It happens so often that the U.S. Cybersecurity and Infrastructure Security Agency (CISA) maintains a catalog of known vulnerabilities that attackers can exploit or have already exploited. Traditional security products and solutions often leave known vulnerabilities exposed.



Security can't come at the expense of retail agility

Security vulnerabilities are just one part of the equation though, since retailers must also deliver fast transaction times and a seamless retail experience, whether in person or online. To maintain value, convenience and trust, retailers must pull off the balancing act of migrating to better services without impacting customer experiences in the process. Otherwise, the result will be a drop in traffic to online stores, abandoned shopping carts, and less foot traffic to physical stores.



Legacy services not only complicate that process since many were not designed for today's cloud-first, connectivity-everywhere world, but they also lack features that correspond with the modern retail environment. Integrated with modern cloud, app-based, software-as-a-service (SaaS)-dependent environments, legacy solutions create a brittle point of failure that is labor-intensive and expensive to maintain and manage.

To successfully transform retail organizations into digital, data-powered businesses, retailers must modernize in a way that is:

- ✓ **Secure**
- ✓ **Supports cloud adoption**
- ✓ **Improves connectivity**
- ✓ **Cuts costs**
- ✓ **Maintains top-notch retail experiences**

Retailers also face a range of **other challenges** that impact their ability to consistently deliver value, convenience, and trust to their customers.

These include:

Geographical complexity

Any business larger than a mom-and-pop store needs to deliver secure connectivity to multiple locations and multiple types of locations (i.e., HQ, branch offices, warehouses, retail sites, etc.).

Network reach

Retailers require high-performing and secure connectivity for the most diverse locations. They need to connect retail locations to each other and to a central data center. Using legacy MPLS or VPNs is expensive, complicated, unreliable, and insecure.

Escalating costs

Over time, the cost of legacy technologies climbs sharply. Newer technologies not only deliver new features that better match current business conditions, but they also tend to be cheaper to maintain and manage, while also offering a lower TCO. Retailers need to minimize their costs while increasing employee productivity. But MPLS links are costly and VPN tunneling is complex. Alternatively, relying on the public Internet is inefficient and unreliable because ISPs prefer cost-savings over performance. This often results in packet loss, jitter, or latency that can torpedo real-time, mission-critical applications. Providing secure connectivity alone can be a huge cost center.

Administrative overhead

Legacy, non-cloud-native technologies have sky-high administrative overhead. Whether delivering complimentary guest Wi-Fi or connecting to cloud-based, mission-critical business systems, retailers' IT teams need to ensure high performance and security, otherwise the business will lose revenue. Procuring, managing and updating a tech stack that answers those needs is a huge hassle. In addition, the transition of data center services, like voice-over-IP (VoIP) and point of sale (PoS), to the cloud requires IT to learn and manage a completely new set of tools.

Evolving threats

Cybersecurity is a constant arms race between legitimate businesses and online crooks. Today, the threat landscape is more dangerous and difficult to manage than ever before, with ransomware groups, state-sponsored malware, and AI-generated targeted malware representing just a few of the emerging threats that legacy tools can't counter.

Compliance requirements

Various regulations mandate that retailers protect personal and PCI DSS information related to transactions, retail memberships, and loyalty programs via a strict set of security requirements.

Why SASE is the key to secure, speedy, growth-oriented digital transformation

To be successful over the long haul, digital transformation projects should be integrated across organizations and constructed on a secure foundation that was designed to address retail challenges now, and in the future.

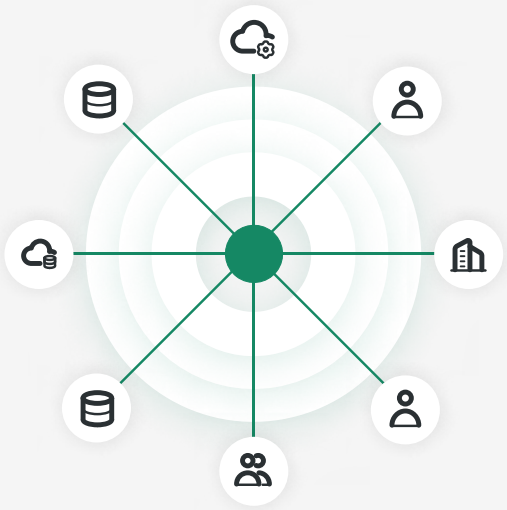
SASE (Secure Access Service Edge) converges networking and security into a single, cloud-native service. It enables retailers to consistently deliver value, convenience, and trust, while boosting digital transformation efforts.

Not all SASE is the same.

Many providers stitch together disparate networking and security solutions to fit the requirements of SASE as determined by Gartner®. Even if each solution were best-in-class, this approach would still be a management nightmare, escalating costs and complexity. You might argue it's "best of breed", but at what price? Plus, what a SASE vendor touts as the best in one area may fall short when integrated with other tools, or even when applied to different challenges.

A better approach is to seek a single-vendor SASE solution that is architected for purpose.

Single-vendor SASE:
A foundational technology upgrade



Deploying single-vendor SASE as the foundation for digital transformation allows retailers to shift their focus away from IT management back to their own core business, strengthening competitive advantage and innovating for growth.

Single-vendor SASE supports site setups in hours or days—rather than weeks or months for competing technologies—and helps retailers future-proof IT, serving as a holistic, scalable, and secure architecture on which to build.

What to look for in single-vendor SASE

When Gartner outlined the concept of SASE in 2019, the research firm noted that enterprises need a service that consolidates key networking and security functions into a single solution. Since that time, the market has rapidly expanded, and Gartner predicts it will expand at a 29% compound annual growth rate (CAGR) through 2026 to reach $25 billion in 2027.

When evaluating single-vendor SASE, retailers must assess how any SASE solution will help them meet the challenges of the modern retail environment.

What retailers need from networking

Retailers need to achieve several capabilities to compete in today's digital retail world:

- **They need blazing-fast transaction speeds for both in-store and online transactions.**
- **They need to blanket all of their locations around the globe with reliable bandwidth.**
- **They must accommodate remote and mobile employees, as well as partners and suppliers.**

Single-vendor SASE enables all these capabilities with cloud-native WAN connectivity, WAN optimization, SaaS acceleration, and more.

Key questions

to ask SASE providers about networking

- Does the SASE service deliver reliable, stable SD-WAN connectivity to geo-diverse store locations and facilities, while improving efficiencies and reducing costs?
- Does the SD-WAN network connect to a private backbone that will not only deliver connectivity to regions, but also connect any site to any other site, partner sites, or service-provider clouds located anywhere around the globe through a global footprint of points of presence (PoPs)?
- Does the SASE solution have the ability to route traffic based on quality-of-service (QoS) bandwidth prioritization policies that we set?
- Does the SASE solution accelerate applications such as PoS, so that they function as truly real-time apps?
- Are features such as TCP acceleration, packet-loss mitigation, and route optimization standard?

What retailers need from security

Speed cannot come at the expense of privacy and security, especially in heavily regulated sectors like retail. The following questions will help you balance your networking and security needs.

Key questions

to ask SASE providers about security

- Are connections private, encrypted, and reliable?
- Does the solution include advanced data protection to safeguard sensitive information such as PoS transactions, membership data, inventory management, guest/customer wi-fi, and compliance?
- Does the solution streamline compliance through policy enforcement and automated reporting?
- Does the solution deliver next-generation security features, such as ZTNA (zero-trust network access), SWG (secure web gateway), NGAM (next-generation anti-malware), FWaaS (firewall-as-a-service), CASB (cloud access security broker), DLP (data loss prevention), RBI (remote browser isolation), EPP (endpoint protection), and XDR (extended detection and response)?
- Do these converged security features provide a holistic approach to protecting users and data,

  ensuring compliance and detecting attacks, or are they provided by a patchwork of point solutions?

Other questions
to ask SASE providers

- Does the solution consolidate the management of diverse networking and security features? That is, can IT teams manage all network and security operations through a single pane of glass or a single management console?
- Does the solution bring runaway costs back under control?
- Is the solution cloud-native and delivered as a service? I.e., is the SASE service opex-based so we don't have to shoulder heavy upfront costs?
- Is your solution delivered as single-vendor SASE, making consolidated management, integration, and cost control easier in a retail setting?
- Going forward, can we add capacity as needed (and throttle back when desired) without having to waste money planning for peak periods and paying for excess capacity year-round?

Cato SASE Cloud platform enables retail stability, growth, and innovation

In an evolving market, retailers must continuously improve customer and user experiences to keep up with competitors.

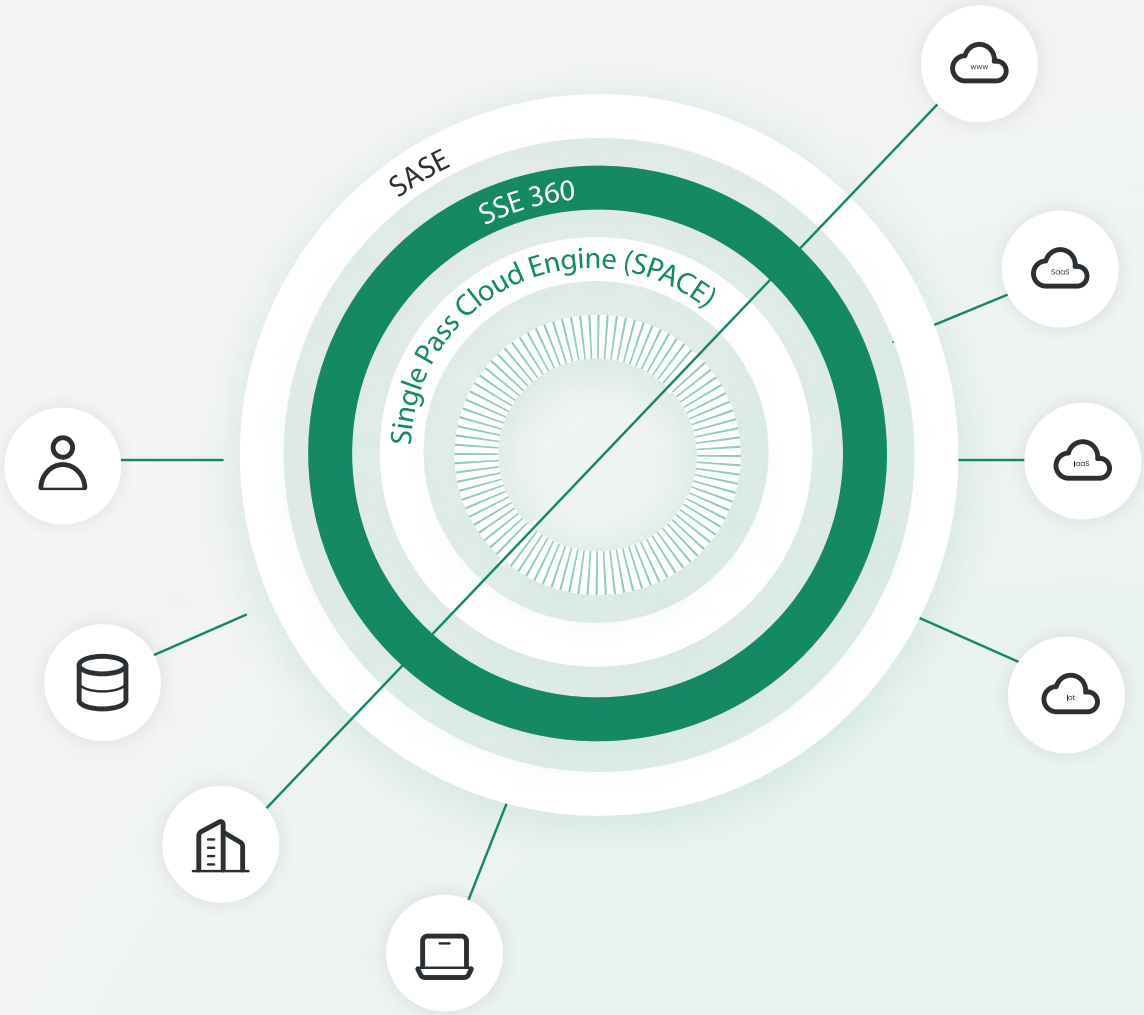
Businesses that migrate from legacy technologies — such as MPLS, IPSec VPNs, and SD-WAN overlays — to a single-vendor SASE platform will see dramatic network and security improvements that allow IT to focus on other strategic goals.

SASE not only enhances retailers' competitive edge, but also provides a secure foundation for digital transformation efforts and the adoption of other advanced technologies, so the business can continue to grow and innovate, safely and securely.

The power of a platform

The Cato SASE Cloud Platform brings powerful capabilities together in a user-friendly and cost-effective solution. Because Cato SASE Cloud is a single-vendor platform-based service, retailers can consume both traditional and next-gen networking and security features as a unified service that they can manage through a single pane of glass.

Cato SASE Cloud is built on a global private cloud network that delivers a seamless customer experience. It is designed with a future-proof, self-healing, auto-scaling, and auto-updating architecture that makes managing enterprise networks and security simple and easy. With a worldwide network of PoPs, it is the only purpose-built SASE cloud service designed from the ground up to deliver advanced networking and security services from a single architecture.



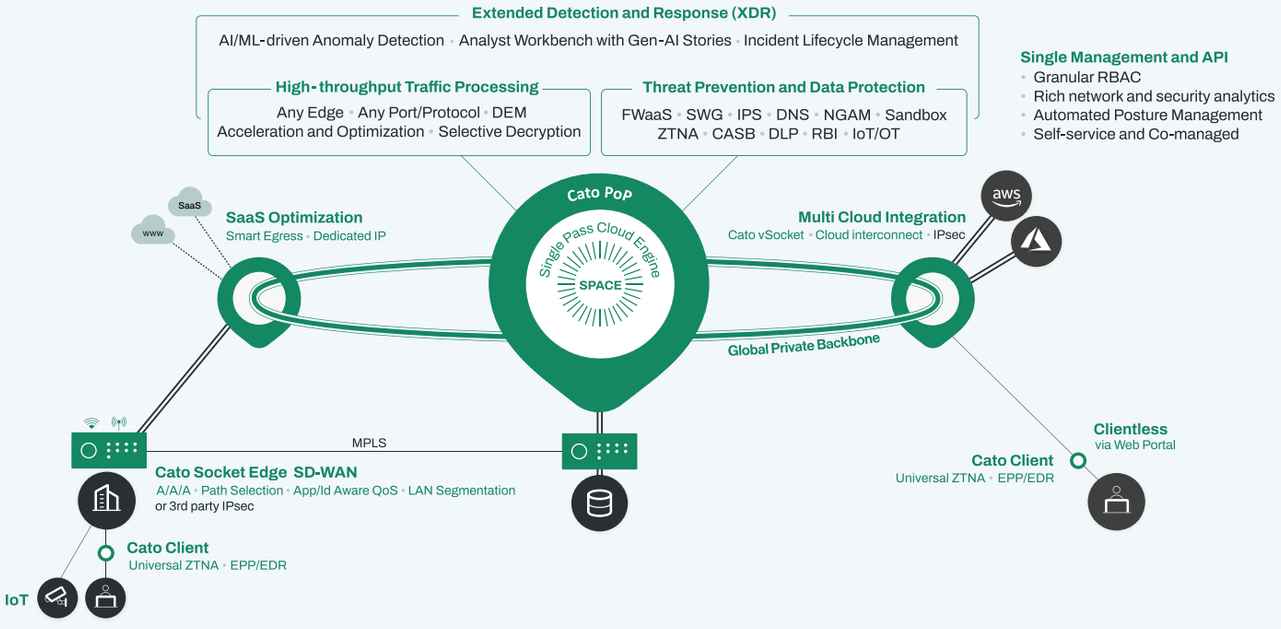
The Single Pass Cloud Engine (SPACE) is the core security engine of Cato SASE Cloud and provides 360-degree visibility and control. This is critical for delivering continuous protection for retailers and helps mitigate security risks such as data loss and malware propagation across all physical, remote, and cloud locations.

By strategically deploying single-vendor SASE, not only will your retail organization streamline connectivity and networking, but it will also enjoy greater agility, lower costs, simplified management, and the ability to scale globally in step with your expanding retail business.

About Cato Networks

Cato Networks is the leader in SASE, delivering enterprise security and network access in a single cloud platform. With Cato, organizations replace costly and rigid legacy infrastructure with an open and modular SASE architecture based on SD-WAN, a purpose-built global cloud network, and an embedded cloud-native security stack.

Cato SASE Cloud Platform



For more details, please contact us:

Gemma Roalf
Vizst Technology
Acorn Business Park, Poole, Dorset, BH12 4NZ
+44 333 344 2204
gemma.roalf@vizst.com
www.vizst.com

Cato. WE ARE SASE.

Cato SASE Cloud Platform

Connect
Cloud Network
Cloud On-Ramps

Protect
Network Security
Endpoint Security

Detect
Incident Life Cycle Management

Run
Unified Management and API

Use Cases

Network Transformation
MPLS to SD-WAN Migration
Global Access Optimization
Hybrid Cloud & Multi-Cloud

Business Transformation
Vendor Consolidation
Spend Optimization
M&A and Geo Expansion

Security Transformation
Secure Hybrid Work
Secure Direct Internet Access
Secure Application and Data Access
Incident Detection and Response

Contact Us