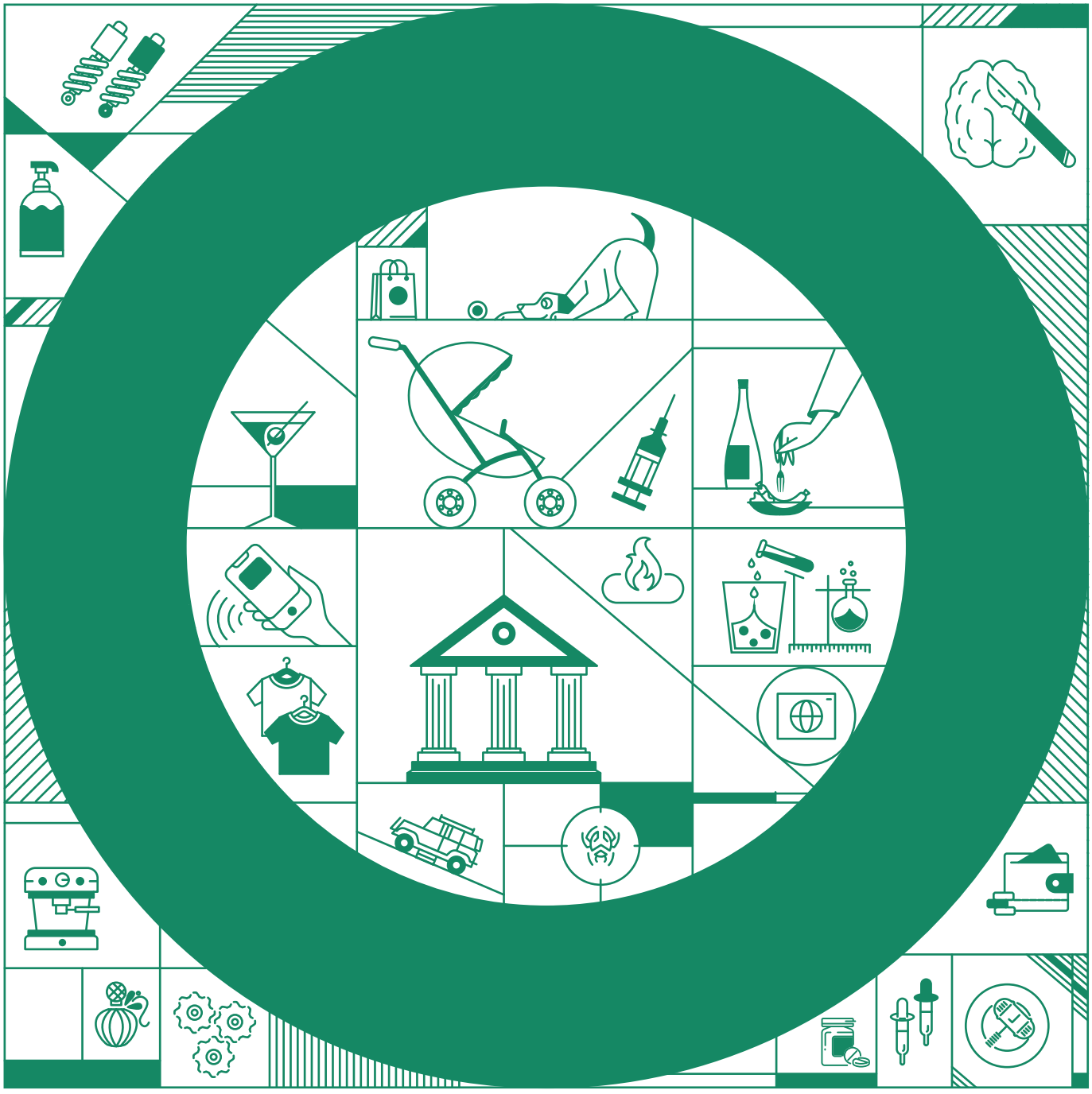
CATO NETWORKS

ENTELEGENT SOLUTIONS

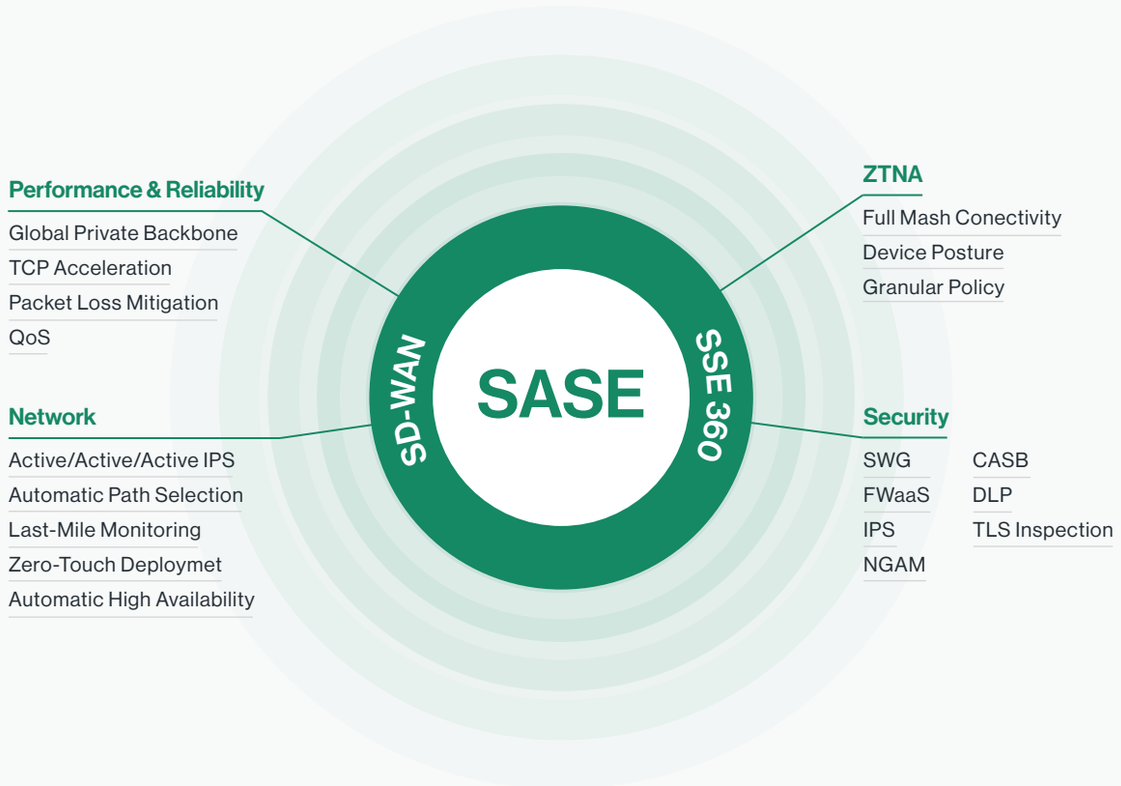
SASE for Different Verticals



Overview

Gartner defined the Secure Access Service Edge or SASE in 2019. SASE represents the convergence of networking and security capabilities delivered as a cloud-native service. SASE allows organizations of all sizes and verticals to deliver comprehensive networking and security capabilities to all users and locations without compromising performance.

> **The adoption of cloud and edge computing and work-from-anywhere initiatives has radically shifted access requirements. For most organizations, there are now more users, devices, applications, services and data located outside of an enterprise than inside.**
>
> **Gartner**
>
> Market Guide for Single-Vendor SASE ›



This eBook looks at how SASE aligns with the security and connectivity needs of Retail & Hospitality, Manufacturing, Credit Unions, Pharmaceutical & Health, and Technology organizations. Since SASE enables cloud adoption, work from anywhere, and digital transformation at scale, there will be some commonalities across these verticals, but the primary focus will be on how SASE addresses the concerns and needs of each.

Retail & Hospitality

Retail & Hospitality is a unique vertical; these organizations are striving to increase efficiency and reduce costs while ensuring an excellent experience for their customers, in-store and online. Traditionally, delivering performance and user experience came at the cost of security, as deploying a comprehensive, high-performance security stack to every location would create extreme complexity and be cost-prohibitive.

This has become more challenging over time as many resources that were once centralized in the data center, such as VOIP and POS and are now delivered as cloud services. Adding to the challenge is the critical nature of connectivity for retail locations. Without the ability to communicate, check inventory status, and process credit card transactions, business comes to a standstill resulting in lost revenue.

Most retailers are managing connectivity and security for multiple geo-diverse locations, sometimes globally, with a need to prioritize critical systems, deliver guest wi-fi and protect against insider threats and targeting by organized threat actors. In the legacy model, this was often accomplished by utilizing costly MPLS links or complex VPN tunnel connectivity between retail locations and a centralized data center where security was applied, and the business resources were hosted. However, MPLS is not always available, and the public Internet is better suited for cloud access and the flexibility required to handle the turbulent retail market.

The public Internet also creates concerns as ISPs prefer cost-savings over performance, introducing an unpredictable transport that suffers from packet loss, jitter, and latency issues, not to mention a complete lack of security. In 2021, the average cost of a retail data breach was $3.27 million (IBM Cost of a Data Breach Report 2021), with many incidents occurring at well-known retailers: Guess, Hobby Lobby, and Carters among others.

SASE addresses these issues, starting with branch connectivity. Native SD-WAN as part of a SASE solution, reduces cost and complexity while allowing organizations to deliver reliable connectivity using commodity broadband links and 4G/5G wireless connectivity. This hardware is often readily available and easy to deploy and procured as a low-cost OPEX subscription, making it possible to deploy high-availability pairs at every location.

From here, traffic is sent to the closest SASE point of presence (PoP), where security and zero-trust access policies are applied. Guest wi-fi can be filtered using SWG, while IPS & NGAM protect the location from threats, and DLP & CASB help to maintain data sovereignty and PCI compliance. Next, traffic is sent over a global private backbone while applying QoS bandwidth prioritization policies, TCP acceleration, and packet-loss mitigation, egressing at another PoP close to the destination, whether it's a private data center, public cloud, or SaaS application. This improves performance and reliability while ensuring that all data in transit is secured.

Overall, SASE enables consistent, comprehensive security for retailers of all sizes without creating complexity or adding to administrative overhead and costs. Organizations can minimize business interruptions and deliver exceptional user experience without compromises, enabling transformation and cloud adoption. All of this with the agility and flexibility of the cloud, futureproofing the deployment for whatever is next.

Manufacturing

Digital transformation, cloud adoption, and IoT are driving what is commonly referred to as Industry 4.0. This allows manufacturing organizations to rapidly collect and analyze data for greater efficiency and better decision-making but also makes security and network connectivity a critical factor in success. Like the retail use case we discussed previously, manufacturing is also seeing cloud migration as manufacturing execution systems (MES) and other critical resources are moving into cloud-delivered services.

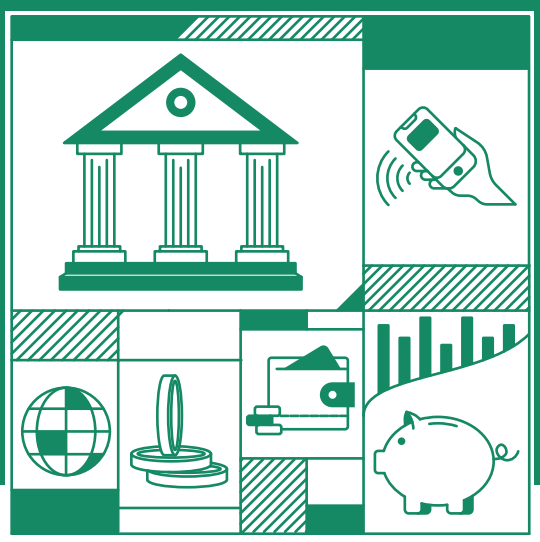
Industry 4.0 has led to significant increases in the utilization of data and automation in the manufacturing process. Smart factories are emerging, utilizing connected devices to streamline manufacturing and collect data that is used to anticipate needs. Materials are ordered automatically for just-in-time (JIT) management, and equipment service needs are predicted, reducing downtime, and improving LEAN manufacturing processes. Beyond smart factories, lights-off or dark factories are also becoming more common. These factories are fully automated and can operate literally with the lights off, with systems and processes monitored by personnel remotely.

Adding to the challenge is the fact that the sensors, robots, and other connected devices used by manufacturers are not often designed with security in mind, making them vulnerable to compromise and creating opportunities for bad actors. In addition to the security challenges, many manufacturers have a broad global presence, including facilities in China, Vietnam and Latin America, making connectivity a challenge. Manufacturing organizations need to secure their systems (HMI, SCADA, OT, IIoT) and data (CAD files, etc.) while ensuring consistent network performance and highspeed data transfer. Secure remote access is also becoming a priority with its own connectivity and security requirements.

SASE enables Industry 4.0 and manufacturing organizations to reduce complexity and accelerate digital transformation. All locations are connected securely via encrypted tunnels, instantly granting full visibility and control with the performance of network optimization and a global private backbone. SASE can even help remote or rural locations, providing reliable middle-mile connectivity. If you have or are planning to open remote facilities at connectivity-challenging locations like China, Vietnam, and Latin America – make sure your SASE vendor of choice has full-featured PoPs available in those locations with connectivity to their private backbone.

On top of the seamless, simplified connectivity between locations, user access is enabled for employees and third parties to monitor, configure, and operate the equipment. Remote users connect based on zero-trust policies and enjoy the same benefits as locations regarding network performance and reliability. Regardless of how the connection into the SASE cloud is established, SD-WAN device, IPSEC tunnel, User Client, or Clientless Web Access, all traffic is inspected and secured by multiple engines (SWG, FWaaS, IPS, NGAM, DLP, etc), ensuring nothing harmful comes in, and nothing sensitive gets out.

Credit Unions



Like the retail case presented above, or maybe even more so, Credit Unions and financial services, in general, have seen a significant shift in business operations over the past 20 years. You may recall that most banking operations were done in person at a branch location, but now employees and customers alike are using laptops and mobile phones rather than at brick & mortar locations. In addition, what was once a paper-based process is now managed digitally, elevating the need for comprehensive cyber security controls.

While physical locations are still an essential component of the credit union business, the 2022 Digital Banking Survey by Forbes indicates that 78% of Americans prefer to bank via mobile app or website, further illustrating the digital transformation in progress. 41% of banks (including credit unions) have already adopted a cloud presence (Cornerstone Advisors). This migration to the cloud and demand for a digital user experience put additional focus on connectivity and security.

As with all financial institutions, credit unions have strict regulatory compliance measures that they must adhere to, including PCI-DSS and policies from the National Credit Union Administration (NCUA). The NCUA approved a proposed rule on July 21st, 2022, that requires federally insured credit unions to report cyber security incidents no later than 72 hours after there is a reasonable belief that an incident has occurred. Additionally, the NCUA does not discourage cloud adoption but cautions that “management should not assume that effective security and resilience controls exist simply because the technology systems are operating in a cloud computing environment”.

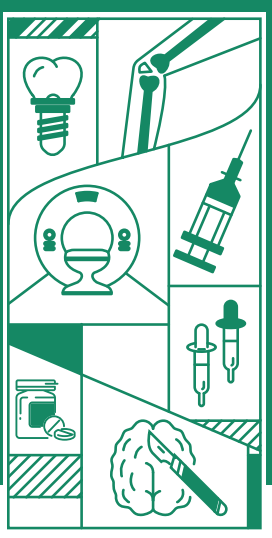
The primary challenge for credit unions is balancing security and performance with cost and complexity. Credit unions are non-profit organizations that exist to serve their members while beholden to comparable regulatory requirements like the large banks that are worth billions or trillions of dollars. This means that there is a greater focus on efficiency and lean operations. Credit unions typically have smaller IT and security teams, and it can be challenging or impossible to manage complex networks and security point products.

SASE simplifies the architecting, deployment, and operation of network and security controls allowing teams of any size to manage the solution with limited product-specific knowledge. Administrators onboard locations with zero-touch SD-WAN devices or IPSEC tunnels and mobile users with a self-service client portal and process. From there, every user and location has optimized, reliable zero-trust access to the resources they need with inspection by a complete security stack. Comprehensive visibility into link performance, application usage, and threat activity are gained instantly.

IT and security teams can focus their time and attention on projects related to their core business of servicing members’ financial needs rather than the chores of managing and updating networking and security products. SASE provides consistent policies configured centrally with all traffic inspected unless explicitly bypassed. New locations and users can be quickly onboarded to gain access to required resources while maintaining compliance with organizational security standards.

Adding to the ease of use is the scale at which SASE is delivered. Organizations no longer must worry about refreshing their hardware every few years or when new functionality is desired. Instead, new functionality can be added without the deployment of hardware and software. For example, DLP appliances were traditionally challenging to manage. Organizations had to define and send only appropriate traffic through the device for policy enforcement. With SASE, any credit union can quickly adopt DLP policies to ensure compliance with PCI-DSS and other regulatory standards. Just upgrade your subscription, turn the feature on and configure appropriate policies. What used to take months can now be accomplished in just days due to complexity elimination and is just one example of how SASE enables the adoption of robust security capabilities.

Pharmaceuticals & Health



Pharmaceutical companies have a culmination of multiple drivers that make SASE an appropriate and effective fit. Multiple factors create complexity for these organizations including global presence, acquisitions, OT, IoT, compliance requirements and safeguarding of intellectual property. While pharmaceuticals may not run as lean as Credit Unions discussed above, they are still businesses that are looking to balance effectiveness with cost. Additionally, they still face the skill gaps and talent shortages that are prevalent in cyber security.

Like manufacturing organizations, pharmaceutical and other health companies make appealing targets to threat actors due to their broad attack surface and reliance on intellectual property. However, these organizations have the additional risk of security incidents impacting human lives. For example, in 2019, for the first time, a ransomware attack may have contributed to the death of a newborn in an Alabama hospital. Beyond this, attackers may be able to gain access to medical equipment and devices or leak proprietary information leading to the creation of counterfeit drugs. Both scenarios are a matter of life and death and could have broad impacts on innocent individuals in addition to the breached company.

User experience is a key factor in delivering effective security, and the security engines should be transparent to the user. This prevents users from looking for ways to bypass security to maintain the desired level of productivity. Medical and Pharmaceutical companies are prime examples, doctors are important employees or leaders in these organizations, and anything that slows them down will be a problem. SASE helps to deliver an exceptional user experience with SD-WAN, a global private backbone, and networking optimization capabilities – all without compromising security. Traffic typically doesn't have to be split-tunneled or bypassed and users enjoy fast download times and reliable connectivity to their applications.

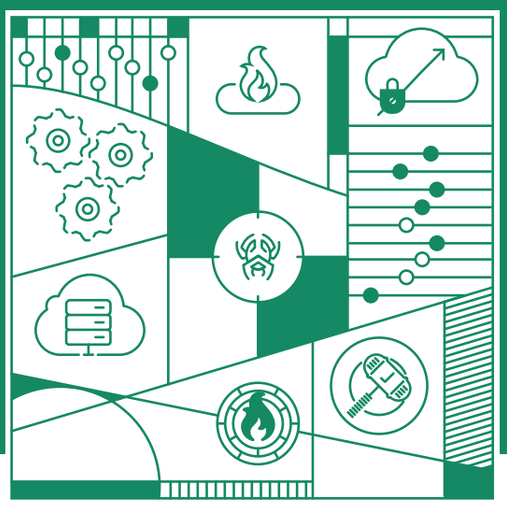
You may have read our eBook on ransomware, where we detail the four ransomware costs: loss of productivity, the primary ransom, the secondary ransom, and reputation damage. Ransomware is a great example for pharmaceutical and health companies because they will feel significant impacts in all these areas. With human lives hanging in the balance, the loss of productivity can be deadly, while fines, litigation, and loss of investor confidence could lead to the company's end.

We mentioned how important data sovereignty is to pharmaceutical and health organizations, due to both HIPPA and other compliance requirements as well as the sensitivity of intellectual property. DLP, as detailed in the previous section, is an effective tool that SASE enables organizations to adopt easily, and Cloud Access Security Broker (CASB) is also something that shouldn't be overlooked.

CASB enables organizations to identify all cloud applications in use and allows administrators to tag them as sanctioned or unsanctioned. Beyond this, CASB provides granular controls for user actions in SaaS applications and broad controls regarding the security and compliance capabilities of the applications themselves. For example, while an organization may standardize a specific cloud file sharing application, they may be unable to block others due to interaction with customers and vendors who have their own standard.

With CASB, organizations can restrict specific actions, allowing download from Dropbox and blocking upload, allowing reading of webmail but blocking downloads and sending attachments, or even allowing Facebook but preventing posting. For the broader policies, organizations can restrict entire categories of applications based on factors such as HIPAA, ISO 27001 or SOC2 compliance and security capabilities such as multi-factor authentication (MFA), encryption of data at rest, and role-based access control (RBAC) to name a few.

Technology



Companies that provide SaaS and other technology products can also benefit from SASE in a variety of ways. Like manufacturing organizations, these companies often have a global presence but with a greater volume of remote workers. Like pharmaceutical and health companies, protecting intellectual property such as source code is also a key focus. But technology companies also have some unique factors that make SASE an ideal solution.

Technology companies are typically more cloud-based, utilizing public cloud infrastructure in multiple cloud services as well as a variety of SaaS applications in everyday business. Employees across the globe depend on these applications for real-time collaboration and have high expectations for the user experience. Many of these employees are in high demand and may consider pursuing new employment opportunities if their productivity suffers due to intrusive security tools or poor connectivity.

Managing security and access for SaaS and multi-cloud deployments can be a challenge for even the most technical of IT teams. Especially when you add the unpredictability of user location and local internet quality. Configuring secure access to cloud infrastructure can be plagued with misconfigurations that leave data and systems exposed to threat actors. For example, Pegasus Airlines had 3TB of data compromised due to an improperly secured AWS S3 bucket. This type of risk has led to a multitude of point products and even the deployment of virtual firewalls into cloud infrastructure to help facilitate security connectivity, only increasing cost and complexity.

SASE simplifies the approach by providing a global private network to organizations, seamlessly connecting their users, locations, data centers, and cloud resources with full encryption and granular zero-trust policies. Cloud data centers can be connected using IPsec tunnels or lightweight virtual appliances, with policies centrally managed from the SASE management application. Additionally, traffic to critical resources is optimized and prioritized while benefitting from the predictability of a global private backbone. Traffic can even be egressed from a dedicated private IP address, allowing configuration of source IP anchoring and adaptive MFA policies for SaaS applications.

Mobile users also benefit from these networking capabilities, making it possible to deliver reliable VOIP and collaboration tools to remote users, delivering the user experience high-tech employees expect. Users are automatically connected to the closest SASE PoP to their current location, ensuring this experience stays consistent, even with travel. All traffic is encrypted and secured using the security engines described throughout this eBook without being backhauled to just one or two data centers or split tunneled due to performance concerns. SASE truly delivers the experience, simplified connectivity, ease of management, and robust security capabilities that technology companies require.

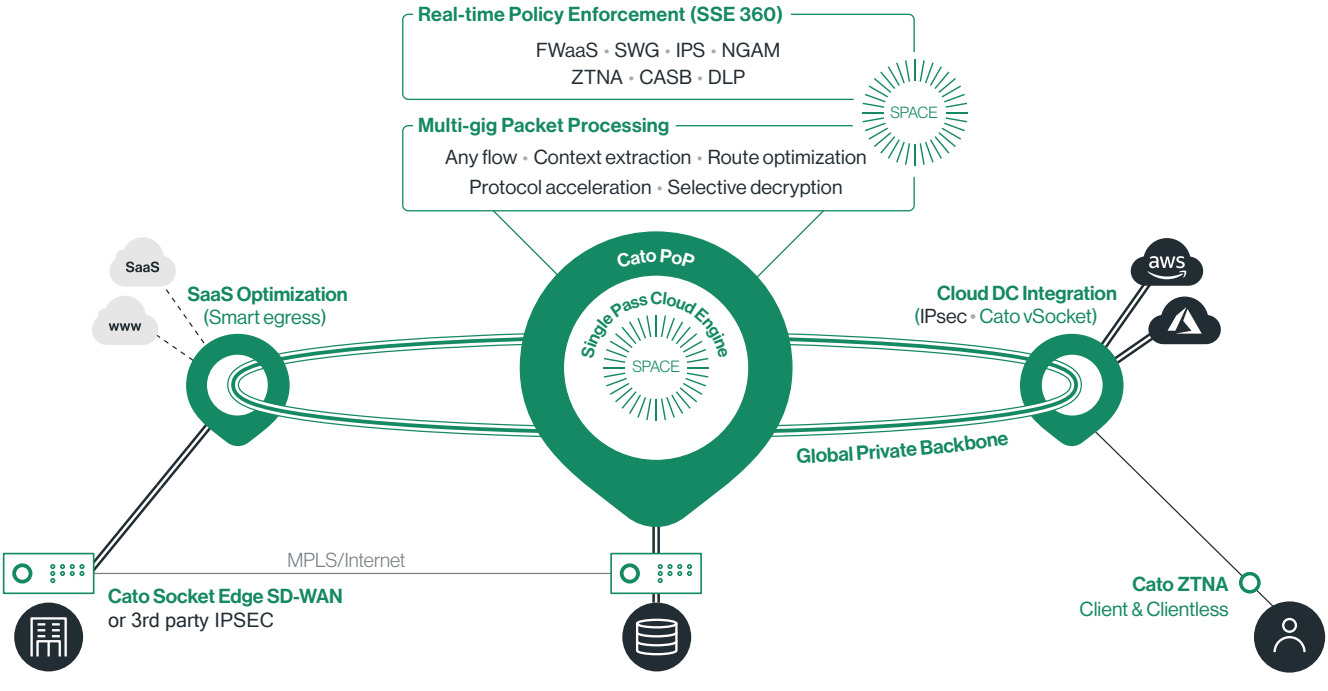
SASE for ALL Verticals

While we focused on specific capabilities for specific industries and verticals in this eBook, you should consider that SASE has broad appeal, and all the capabilities can be valuable for any organization of almost any size. Delivering reliable, performance connectivity to SaaS apps and private resources for locations and users on the go, with comprehensive security capabilities at a global scale, would be a challenge for most companies. SASE makes it possible for your organization to deliver all of this as a simple-to-deploy and manage cloud-native service, much in the same way that Azure and AWS simplify provisioning infrastructure and resources.

If you skipped and only read the section on your company's vertical, we strongly encourage you to read the rest of this eBook. Most of the information can help provide you with context on how SASE can enable organizations in general. If your vertical was not covered in this eBook, hopefully, you still found the information valuable

About Cato Networks

Cato provides the world's leading single-vendor SASE platform, converging Cato SD-WAN and a cloud-native security service edge, Cato SSE 360, into a global cloud service. Cato SASE Cloud optimizes and secures application access for all users and locations everywhere. Using Cato, customers easily replace costly and rigid legacy MPLS with modern network architecture based on SD-WAN, secure and optimize a hybrid workforce working from anywhere, and enable seamless cloud migration. Cato enforces granular access policies, protects users against threats, and prevents sensitive data loss, all easily managed from a single pane of glass. With Cato your business is ready for whatever's next.



For more details, please contact us

Sales
EnTelegent Solutions, Inc.
2520 Whitehall Park Dr.
Ste 200
Charlotte, NC 28273
800-975-7192
sales@entelegent.com
entelegent.com

Cato. Ready for Whatever's Next.

SASE, SSE, ZTNA, SD-WAN:
Your Journey, Your Way.

Cato SASE Cloud

SSE 360

Secure Remote Access

Edge SD-WAN

Global Private Backbone

Multi-cloud / Hybrid-cloud

SaaS Optimization

Cato Management Application

Use Cases

MPLS Migration to SD-WAN

Secure Remote Access

Secure Branch Internet Access

Optimized Global Connectivity

Secure Hybrid-cloud and Multi-cloud

Work From Home