lightstream

SASE

SECURE ACCESS SERVICE EDGE

The Answer to Security In An Increasingly Digital World

LIGHTSTREAM
208 N 2100 West, Suite 200
Salt Lake City, UT 84116
Phone: 877-95-LIGHT

Follow us on

Let us tell you more about the amazing things we do.

SASE
SECURE ACCESS SERVICE EDGE

Over the past few decades, organizations have slowly shifted to the cloud and started embracing digital transformation. But when the 2020 pandemic hit, those who were slow to welcome digitalization had no choice but to adapt, as nearly every workforce had to go remote to stay afloat. While virtual private networks (VPNs) were the standard before, they no longer provide the security and access control required for distributed teams.

Secure Access Service Edge (SASE) is the solution for digital enabled organizations prioritizing security. Existing technologies can't keep up with the increased security demands of distributed teams—to ensure security at every level, more and more organizations have implemented SASE solutions. Have you?

1

2 What is SASE?

In its 2019 report on network security in the cloud, Gartner first coined the term SASE to explain this emerging cybersecurity concept, which integrates security into the network architecture to deliver consistent and secure access. It consolidates wide area networking (WAN) and network security services, including cloud access security broker (CASB), zero trust, secure web gateway (SWG), and firewall as a service (FWaaS) into a single, cloud-delivered service model.

SASE is a new framework for network architecture that securely connects users and their devices to applications and data anywhere. It then applies policy-based security to deliver secure access—no matter the location of employees (users) or devices. Instead of siloed point solutions, the SASE model operates as a single cloud service.

> "SASE capabilities are delivered as a service based upon the identity of the entity, real-time context, enterprise security/compliance policies and continuous assessment of risk/trust throughout the sessions. Identities of entities can be associated with people, groups of people (branch offices), devices, applications, services, IoT systems or edge computing locations."
> — Gartner

SASE and Remote Work

As remote and hybrid work models become the norm, fewer employees work on the corporate network. Existing security solutions assume employees and applications are inside the network perimeter and can no longer protect your data or organization.

With employees working from their home offices, coffee shops, and on the go, the old approach of forwarding traffic to your data center, inspecting it, and then allowing access is no longer viable. It decreases productivity and ruins the user experience. Instead of focusing on data centers, SASE focuses on the user and device identities to provide secure, efficient access to the applications and data they need to do their jobs.

4 Benefits of SASE

Delaying digital transformation is no longer an option. Organizations that want to innovate and grow must adopt digitalization and the frameworks and technologies that ensure their security in the cloud. SASE solves for digitalization and security, but there are many other benefits to implementing a SASE solution. Let's explore a few.

Flexibility

SASE has a cloud-based infrastructure, making it easier to deliver various security services—like DNS, data loss prevention, and more—to any edge device. SASE allows access to the network from anywhere, helping propel your organization into a digital—and secure—future. And because SASE is a cloud-based service, you have more flexibility in managing changes, adapting to evolving needs, and ensuring security no matter where your employees work.

Zero Trust Network Access

"Never trust, always verify" is a core principle of zero-trust, making it one of the most secure frameworks. And it's the one SASE relies on. Using zero trust as a foundation, SASE eliminates trust by granting users access to applications and data only after a user (identity) has been verified.

SASE not only considers identity, but also takes things like location, compliance policies, and a continual evaluation of risk into account. This ensures secure access in cloud environments, on or off the corporate network.

Reduced complexity

Using multiple security products requires constant updates, management, and maintenance. By consolidating your security services into a cloud-delivered service like SASE, you can simplify your technology stack and minimize your IT staff's workload. With SASE, you can easily manage your security from a single pane of glass management system from a cloud services provider like Lightstream.

Cost savings

Organizations have added even more security solutions to their tech stack to ensure a fully secure network and cloud environment for remote workers. But with more products and services comes increased costs and the need for even more management.

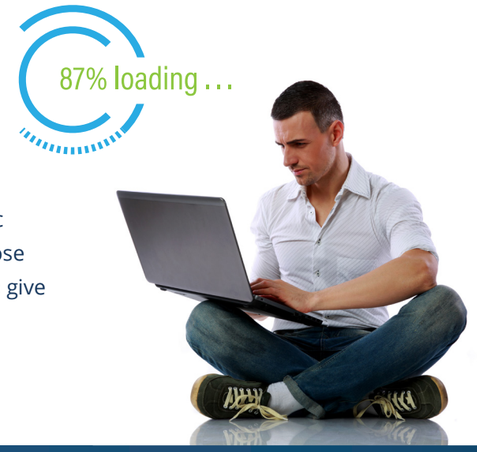
Instead of purchasing more solutions, you can implement a SASE model that uses a single platform to lessen management needs and CapEx and OpEx costs.

Threat prevention and data protection

Security is built into SASE frameworks, with components like firewall, CASB, and full content inspection that help prevent threats. It filters network traffic to stop everything from malware attacks and ransomware to phishing. All of this also ensures your data is secure.

As a solution to a remote or hybrid workforce, SASE protects data on and off the network—wherever it may go. And with a focus on identity, SASE helps prevent unauthorized access that could threaten your data and your organization.

Better performance and user experience



Cloud infrastructure allows users to connect to the resources, applications, and data they need to do their jobs—whether they're at corporate headquarters or in their home offices, creating a much better user experience.

Instead of sending traffic to a data center first, SASE routes traffic across an edge network where that traffic is processed as close as possible to the user. SASE finds the fastest possible route to give users a great experience and increase performance.

lightstream
208 N 2100 West, Suite 200
Salt Lake City, UT 84116
Phone: 877-95-LIGHT

5

SASE Components

Software-Defined Wide Area Network (SD-WAN)

Known to reduce complexity and cost as well as optimize the user experience, SD-WAN is an overlay architecture that chooses the best route for traffic to cloud applications, the internet, and data centers, reducing latency and improving user experience. It helps organizations manage policies across locations, making it ideal for hybrid and remote workforces.

Zero-Trust Network Access (ZTNA)

In a zero-trust framework, trust has to be continually verified in real-time. ZTNA verifies user identities, establishing trust before granting access to data and applications. It prevents unauthorized access and protects internal resources from data breaches.

Firewall as a Service (FWaaS)

FWaaS replaces physical systems with cloud-based firewalls that protect applications and platforms in the cloud from cyberattacks by delivering advanced Layer 7 capabilities. This includes access controls, domain name system (DNS) security, and threat prevention.

Cloud Access Security Broker (CASB)

A CASB ensures the safe (and secure) use of cloud applications and services by securing cloud apps. It offers a few security measures for cloud-based services, including:

- Preventing data leaks by securing sensitive data with access controls and data loss prevention (DLP)
- Providing visibility into unauthorized corporate systems
- Preventing malware attacks
- Ensuring compliance with security and data privacy regulations

Secure Web Gateways (SWG)

Secure web gateways prevent cyberattacks and data breaches by blocking unsecured internet traffic from entering your network. An SWG enforces security policies and protects users from malware, viruses, and malicious traffic.

You can deploy secure web gateways anywhere, which is why they're ideal for digital organizations and remote workforces.

6 How SASE Works

SASE brings together SD-WAN edge capabilities and cloud security functions (FWaaS, ZTNA, CASB, SWG), integrating security into your network architecture to provide secure access to users and their devices, no matter the location. While legacy solutions send traffic through multiprotocol label switching (MPSL) services for verification at the data center, SASE enforces security where the traffic is—often outside the corporate network at user and application endpoints.

SASE is a single, cloud-based service that manages both traffic and security. It focuses on securing the edge and expanding the network perimeter to include remote users, applications, and devices. To maintain security on the edge, SASE uses identity-based access and predetermined compliance before granting access to applications or data. It constantly monitors risk to ensure security.

7 Why You Need a SASE Infrastructure

As more organizations fall prey to malicious attackers and data breaches, security has never been more crucial. Years ago, legacy solutions would have worked well to protect your organization's data, but as you migrate to the cloud and grow your remote workforce, you need a better way to protect your most important assets.

SASE provides the security and access control your organization needs to allow users to access the applications and data they need while working from anywhere and on any device. Combining powerful security capabilities like zero trust within your network infrastructure, SASE is the best option for maintaining a secure cloud environment and network throughout your organization.

> "By 2024, at least 40% of enterprises will have explicit strategies to adopt SASE, up from less than 1% at year-end 2018."
> — Gartner

8 How Lightstream Can Help

Lightstream has built its reputation as a cloud, network, and security expert by providing exceptional cloud and security managed services, acting as a partner for its clients' security needs. We're serious about security and creating network and cloud environments that protect your data and applications by continually monitoring for threats, recommending solutions, and tailoring our approach to your specific security needs. So, if you're ready to move to a more secure environment, contact us to learn how we can help.

lightstream
208 N 2100 West, Suite 200
Salt Lake City, UT 84116
Phone: 877-95-LIGHT

Curiosity to solve the complex drives us

We live in the age of constant business transformation.

The Cloud, Big Data, AI and the Internet-of-Things open limitless possibilities—and even more expectations.

And with those expectations comes unfathomable complexity. Addressing them requires amazing strategy and execution of integrated technologies—all networked to provide greater visibility, predictability and cognition.

Fortunately, we've envisioned this day coming for a while.

We've addressed enterprise complexities of on-premise, in-the-cloud, and all the networks in between. We've offered solutions that drive business transformation. And we've worked to find more ways to help you meet higher expectations.

We are Lightstream.

Our passion to serve customers and our curiosity to solve the complex drives us.

We listen to and work with you to carve a path where vision and execution intersect—enabling new capabilities, driving efficiency, and spurring innovation and growth.

Because when you work with a partner who helps you understand where you can go and how to get there, complexity can be averted and every possibility can be realized.

That's where we live—and that's where we're ready to take you.

Complexity Averted. Possibilities Realized.

We've helped many public and private organizations to establish and implement a Zero Trust approach, both before and after the adoption of remote and hybrid work schedules. For a one-on-one consultation to discuss how to ensure your cloud is secure, contact us now.