# The Complete Guide to SASE

# Introduction/Executive Summary

## Enterprise IT no longer has the control over large portions of infrastructure that it once did.

As businesses, employees, and services continue to move away from centralized and/or physical locations and into the cloud, networks are becoming increasingly decentralized – and it's creating unprecedented security challenges.

Today's hybrid workforce is complicating things further by accessing on-site business networks and cloud applications from personal devices, using unapproved apps, and, ultimately, compromising data security.

Some solutions – Cloud Access Security Brokers (CASB), Secure Web Gateways (SWG), Firewall as a Service (FWaaS), etc. – may solve part of the problem, but not all.

The siloed and scattered nature of these piecemeal services impedes monitoring, threat reaction, reporting, and maintenance of the security infrastructure. In steps Secure Access Server Edge (or SASE).

SASE is the uncompromising combination of application experience, network automation, and zero-trust security.

SASE (pronounced "sassy") converges existing security services and deploys them as an XaaS. It brings all aspects of enterprise data security/cybersecurity under a single purview.

Taking this more holistic approach to the network's security policy and compliance enables enterprises to respond to threats faster, arrive at solutions quicker, leverage more robust reporting, and create better experiences for the end user.

A SASE architecture is particularly powerful when delivered as a managed service. As unified, centrally managed, expertly maintained, cloud-based security solutions, SASE is tough to beat. It's the answer to maintaining visibility and control when users, devices, and data are living, quite literally, everywhere.

**In this all-encompassing guide, we will explore...**

» What SASE is, in detail

» Top security pillars of SASE

» The benefits of SASE for business

» Critical features of an ideal SASE architecture

» Key criteria to look for when evaluating a SASE partner

**Ready for a deep dive into SASE? Let's begin.**

To talk with an expert about how you can better integrate networking and security functions in the cloud through SASE architecture, connect with us today or visit **FirstLight.net/sase**

# SASE FOR BEGINNERS

SASE is the evolution of network security in the face of a shifting, decentralized workforce that is (thanks to the weakened reach of traditional IT) vulnerable to ever-increasing cybersecurity threats.

First described – and the term coined – by Gartner in 2019, SASE is an integrated, cloud-delivered security model that consolidates relevant security network solutions into a single, vendor-delivered service, and it encompasses five key network security services.

## The 5 Security Pillars of SASE

SASE is a converged cybersecurity approach that combines wide area networking (WAN) and software-defined WAN (SD-WAN) with five network security services:

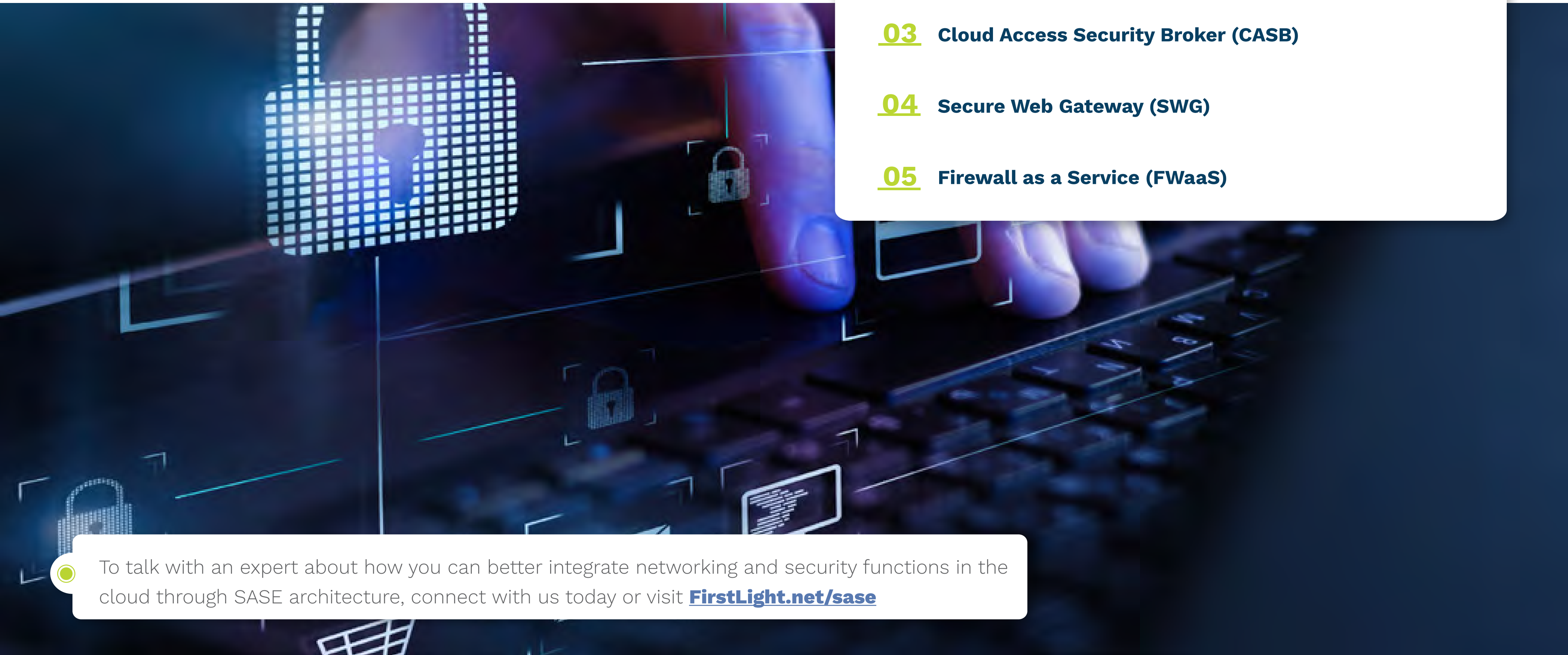
01 **Zero Trust Network Access (ZTNA)**

02 **DNS Layer Security**

03 **Cloud Access Security Broker (CASB)**

04 **Secure Web Gateway (SWG)**

05 **Firewall as a Service (FWaaS)**



To talk with an expert about how you can better integrate networking and security functions in the cloud through SASE architecture, connect with us today or visit **FirstLight.net/sase**

| | |
|---|---|
| **Zero Trust Network Access (ZTNA)** | In a ZTNA model, all access to the network – both internal and external – is presumed to be a potential threat. ZTNA is a shift in attention not presumption.<br>It's made up of security strategies, methodologies, and monitoring to verify a user's identity on a constant basis. |
| **DNS Layer Security** | DNS layer security is a VPN-less security solution that protects users on and off the network by preventing them from connecting to malicious domains.<br>DNS layer security provides visibility into all internet traffic across all users and devices, helping gain context for faster investigation. It also blocks attacks earlier, contains malware if already inside, and helps to easily enforce business and compliance policies. |
| **Cloud Access Security Broker (CASB)** | Sitting between users and cloud services, a CASB deploys enterprise security policies to cloud-based user activity.<br>While the draw of the CASB is its ability to reassert control over end users that leverage applications in the cloud, its success is the ability to assert that control on a granular level and in an unobtrusive way. |
| **Secure Web Gateway (SWG)** | SWG is akin to a CASB, but for traditional web-based activities (visiting pages, downloading files, etc.).<br>It's deployed as a physical or cloud-based solution and enforces company web policy at the user level. It's equipped with URL filtering, application control, data loss prevention, antivirus protection, and https inspection. |
| **Firewall as a Service (FWaaS)** | With FWaaS, the capabilities and security of the firewall are replicated, virtualized, and deployed to the cloud.<br>This decentralized, virtual, cloud-based firewall solution has familiar control over – and familiar insight into – network configurations that are increasingly disbursed. |

While each of these applications/ appliances, individually, serve an integral security function, it is their convergence in conjunction with their delivery as an XaaS that provides greater benefit.

However, partnering with a trusted provider that can manage a SASE solution for you is best. Doing so puts your security in the hands of dedicated experts who can monitor and maintain your network's integrity.

To talk with an expert about how you can better integrate networking and security functions in the cloud through SASE architecture, connect with us today or visit **FirstLight.net/sase**

# THE 4 PRIMARY BENEFITS OF SASE FOR BUSINESS

A SASE security model supports the overall goals of every business enterprise – ultimate security, reduced costs, absolute flexibility, and superior performance.

## Ultimate Security

SASE employs the Principle of Least Privilege (PoLP), which is the idea that end users should only be given the level of access rights to complete the task(s) they are assigned.

PoLP also assigns access rights through role not identity – this ensures that only those who need access get access.

Because it's a unified solution with multiple redundancies, SASE maintains consistent policies across the organization and all deployed systems and workstations.

A SASE approach presupposes a highly mobile/remote workforce and therefore ensures secure connections between client and cloud without a cumbersome end user experience.

Thanks to SASE deployment of IPS, advanced threat intelligence, DLP, SWG, FWaaS, and ZTNA principles, there are multiple layers of centrally managed and centrally monitored protection.

To talk with an expert about how you can better integrate networking and security functions in the cloud through SASE architecture, connect with us today or visit **FirstLight.net/sase**

## Reduced Costs

SASE reduces CapEx by eliminating upfront investment in equipment, installation, and training.

Because SASE is deployed as an XaaS, enterprises can scale up or down with ease – only paying for the size of the workforce they have at any given moment. They aren't stuck with CapEx equipment for a workforce larger than they have.

SASE drastically reduces IT staff workloads because most cybersecurity functions can be outsourced. It also unifies several products and solutions in legacy environments under a single umbrella. Doing these two things in tandem reduces IT staff sizes and salaries, and overall IT expenditure.

## Absolute Flexibility

Because it's cloud-based, SASE provides companies the ability to configure their workforce however they need to – WFH, hybrid, or in-office.

When a SASE approach is offered as an XaaS, IT leaders can scale staff and features up (or down) seamlessly.

And because managed providers assume the responsibility of keeping software/hardware up to date, internal teams are free to focus on more pressing enterprise needs.

To talk with an expert about how you can better integrate networking and security functions in the cloud through SASE architecture, connect with us today or visit **FirstLight.net/sase**

## Superior Performance

As a converged solution, SASE streamlines the security process and makes client-to-network connections faster, more intuitive, and less onerous.

By operating as a whole, the system is more secure, and the process of accessing the network for the end user (despite policies in place) is unintrusive.

It's easy to see how SASE, especially as a managed service, facilitates improvements across the entire enterprise. From cybersecurity to personnel, SASE delivers secondary and even tertiary benefits beyond network protection.

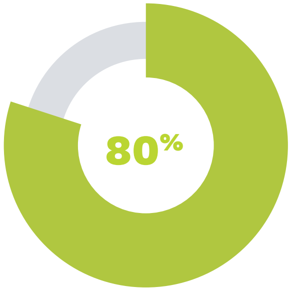
To talk with an expert about how you can better integrate networking and security functions in the cloud through SASE architecture, connect with us today or visit **FirstLight.net/sase**

# 7 NON-NEGOTIABLE FEATURES EVERY

When it comes to SASE architecture, not all deployments are created equal. To keep your enterprise (and your workforce) secure and flexible in a cloud environment, these seven features are crucial for top performance.

## 01 Application Discovery

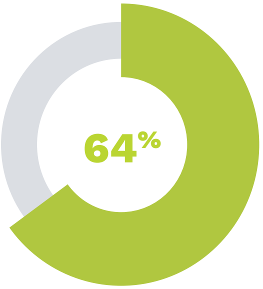
Performing application discovery to gather detailed information about the apps installed and used across the enterprise is table stakes. At the conclusion of the process, the IT department should have access to macro-level reporting to gain a thorough understanding of the risks each application poses and maintain the ability to block unapproved applications.



**of employees are using applications that aren't sanctioned by IT**

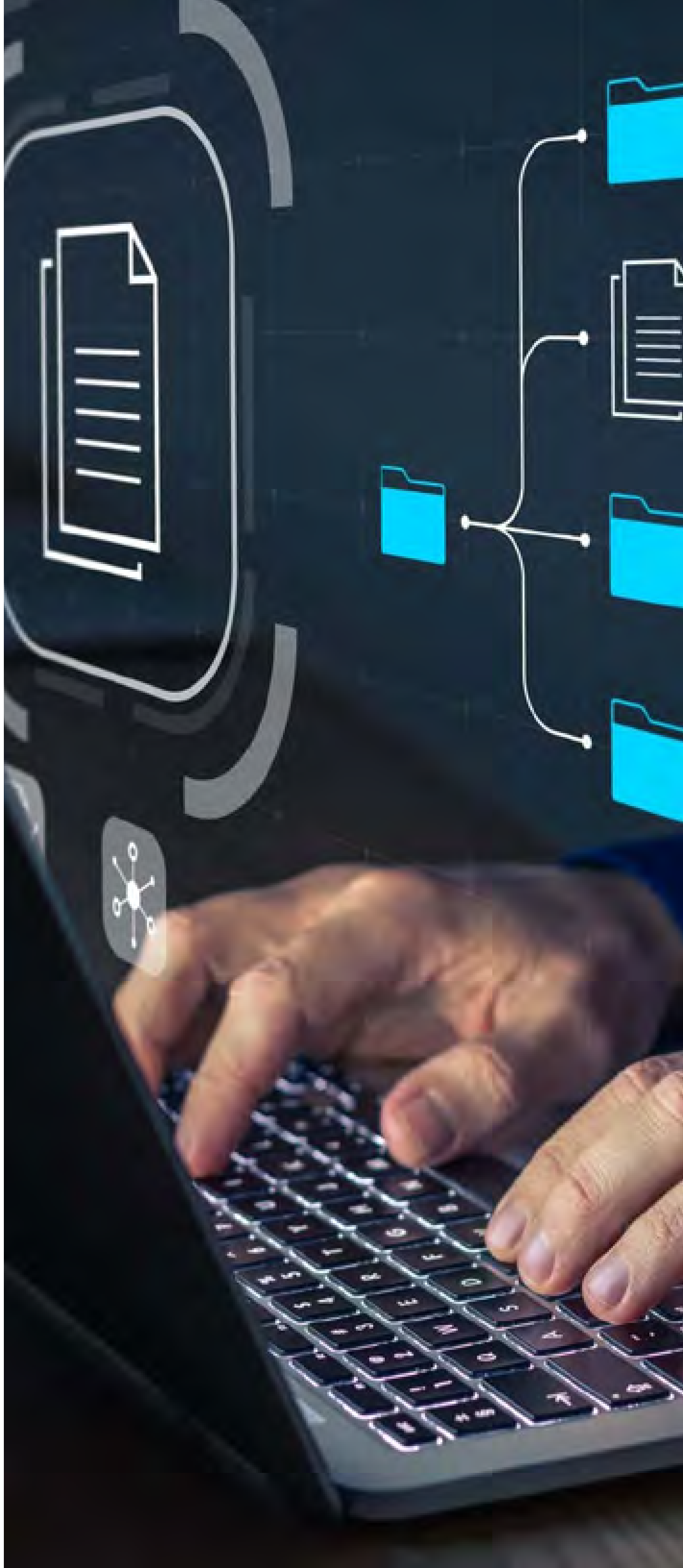
## 02 Data Loss Prevention (DLP)

It's necessary to monitor data sent over the network in real time combined with an automated mechanism to minimize the risk of accidental data leaks, prevent unauthorized access, and eliminate incidental/accidental data handling violations.



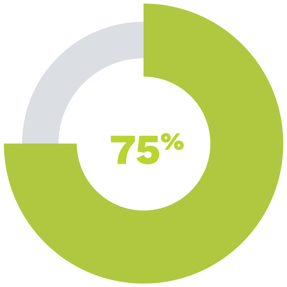
**of employees have access to 1,000 or more sensitive files**

To talk with an expert about how you can better integrate networking and security functions in the cloud through SASE architecture, connect with us today or visit **FirstLight.net/sase**



## 03 Remote Browser Isolation (RBI)

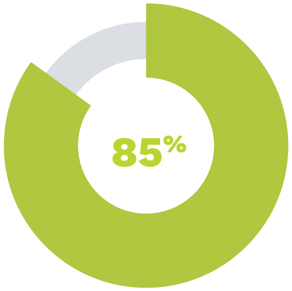
Because browsers are such popular breach points, an RBI is essential. An RBI is a cloud-based tool that seamlessly clones the end user's web session and moves it to an isolated container on the cloud to cut off potential threats from the physical hardware without impacting the user.



**of an employee's average day is spent in a**

## 04 Advanced Threat Intelligence

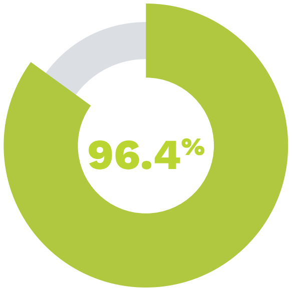
Breaches are becoming more sophisticated and more frequent with each passing year. As a result, threat detection needs to be that much smarter. Enterprise networks need an advanced threat intelligence solution like FirstLight Cloud Security, powered by Cisco Umbrella, that can perform real-time analysis accurately, effectively, and intelligently.



**of organizations reported a successful phishing attack in 2021**[ii]

## 05 Global Cloud Architecture

When almost everyone and everything operates in the cloud, the quality of that cloud – and who manages it – is everything. An architecture that can deliver fast, resilient, secure, and reliable performance is essential for SASE. With speed, reliability (uptime), and security being the most important factors, it is imperative that companies have the right cloud service.

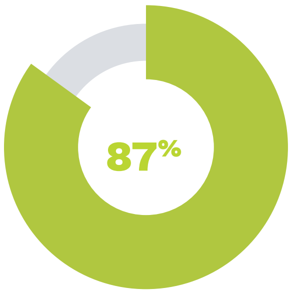


**Cisco Umbrella's industry-leading detection rate**[iii]

To talk with an expert about how you can better integrate networking and security functions in the cloud through SASE architecture, connect with us today or visit **FirstLight.net/sase**

## 06 Intrusion Prevention System (IPS)[iv]

Another real-time monitoring system, an IPS continuously scans the network for malicious activity and reports potential threats while taking preventative measures. Placed within the flow of network traffic, an IPS can identify threats and then report, block, and/or drop them via well-known threat signatures, anomalous behavior, or through defined policies.

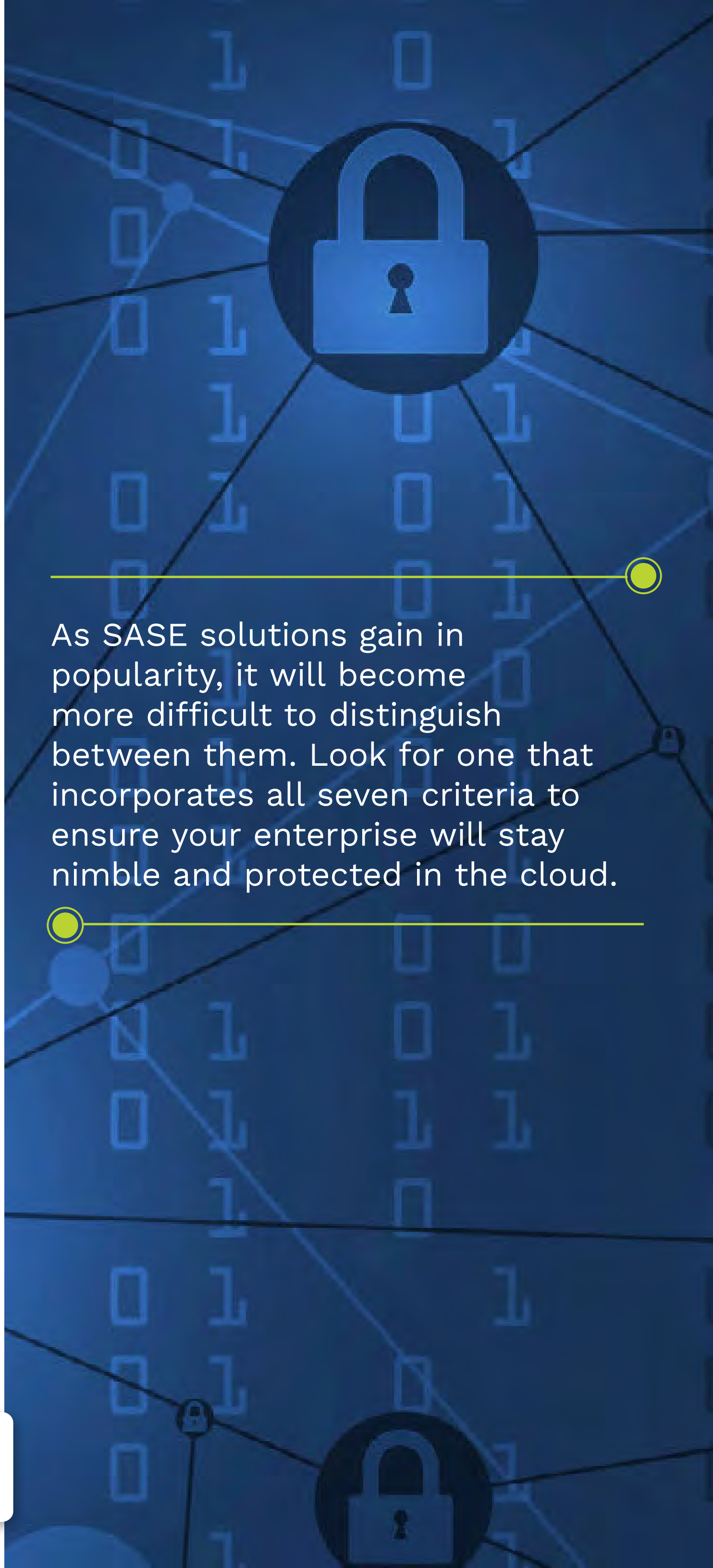


**of DDoS victims are attacked repeatedly**

## 07 A Unified Solution[v]

Converging and then managing all services under a single umbrella breaks down siloes across the system, making it that much easier to efficiently prevent, detect, and thwart threats. According to a report by the Enterprise Strategy Group, organizations that adopt a SASE architecture, specifically, are...

- 4.2 times more likely to be very confident in their ability to secure employees working from home
- 3.9 times more likely to be very confident in their visibility across their distributed cloud environments



As SASE solutions gain in popularity, it will become more difficult to distinguish between them. Look for one that incorporates all seven criteria to ensure your enterprise will stay nimble and protected in the cloud.

To talk with an expert about how you can better integrate networking and security functions in the cloud through SASE architecture, connect with us today or visit **FirstLight.net/sase**

# WHAT TO LOOK FOR IN A SASE PARTNER

If you're going to put one provider in charge of uniting all your security systems into a single, centralized deliverable, finding the best fit is crucial.

**When comparing your options, look for a SASE partner that will...**

| | |
|---|---|
| **Deliver a Complete SASE Solution** | It's not a complete SASE solution unless it combines WAN/SD-WAN with – at least – Zero Trust Network Access (ZTNA), DNS Layer Security, Cloud Access Security Broker (CASB), Secure Web Gateway (SWG), Firewall as a Service (FWaaS). Go with a partner that can deliver everything that makes SASE, SASE. |
| **Offer Flexibility** | Part of the appeal of SASE is the ability to scale quickly and easily with the size of your enterprise. Seek out a SASE provider that offers networking and security solutions in the same license. This way, you can right size seamlessly as you continue to grow. |
| **Provide a Global Cloud Architecture** | The quality of your provider's global cloud architecture will determine the efficacy of the SASE solution in place. Make sure that traffic is getting routed with high-bandwidth backbones and that their network has a large geographical footprint. |
| **Come With a Proven Track Record** | Talk is cheap in the security space. The right partner should be able to demonstrate a track record of success with the data/analytics to back the claims. |

To talk with an expert about how you can better integrate networking and security functions in the cloud through SASE architecture, connect with us today or visit **FirstLight.net/sase**

| | |
|---|---|
| **Support a Hybrid Approach** | If your organization has existing OpEx or CapEx investments that need to run their course, look for a provider that can hybridize its SASE solution and integrate existing systems as you transition. |
| **Provide Robust Threat Intelligence** | The best SASE providers bring the most robust threat intelligence to the table to identify attacks before they cause harm. Consider partners that use a smart combination of real-time analysis, human intelligence, and machine-learning models. |
| **Provide Unified Management** | Centralized operations make it easier to manage all the elements of a SASE model. Look for a provider with a unified console to help you control, customize, and monitor all aspects of your security from a single dashboard. |
| **Offer Flexible Integration With SD-WAN** | SD-WAN and network security go hand in hand. It's important to partner with a provider that can fully integrate with SD-WAN to secure cloud access and protect users, connected devices, and app usage from direct internet access breakouts. |

To talk with an expert about how you can better integrate networking and security functions in the cloud through SASE architecture, connect with us today or visit **FirstLight.net/sase**

The benefits of a SASE model are unlocked by working with one partner who can bring together best-in-class networking, security, and observability – while offering the flexibility and investment protection to transition to the cloud at your pace.

FirstLight provides all the building blocks of a SASE architecture today, brought together in a single offer.

From internet access to cutting-edge SASE security, FirstLight can manage your entire enterprise network. Where other SASE solutions offer a unified security solution, FirstLight offers a unified everything solution along with a consultative approach and custom configurations created by a team of experts – that's the FirstLight difference.

## Locally Based Service and Support

FirstLight offers locally based support teams in all the markets we serve.

Our Headquarters is located in Albany, NY and we operate Network Operations Centers (NOC) in Albany and Victor, NY, Brunswick, ME and Portsmouth, NH. In addition, we have offices in Buffalo, Binghamton, and Romulus, NY, Portsmouth and Manchester, NH, Lewiston, ME Williston, VT, and Harrisburg, PA.

The FirstLight team provides superior services, backed with the understanding that our clients' mission-critical needs demand comprehensive, proactive support.

To talk with an expert about how you can better integrate networking and security functions in the cloud through SASE architecture, connect with us today or visit **FirstLight.net/sase**

# Beyond SASE

SASE is even better when combined with other cybersecurity and network solutions – that's where FirstLight has a unique advantage. Since we own the fiber network and control its performance, we can guarantee the end-to-end experience that enterprises require. We aim to protect our customers in the industries that we serve, and we serve a lot of industries – carriers, wireless providers, banking and finance, education, state and local government, utilities, and healthcare, to name a few.

For example, FirstLight's cloud sites are part of an overall strategy to win the fight against ransomware – they offer a backup and disaster recovery solution that helps get organizations back on their feet quickly. Additionally, FirstLight offers protection from other threats like DDoS attacks with a holistic approach.

We also provide several managed services that include security, network solutions, monitoring, cloud management, ESAs, server monitoring and management, application hosting and management, and desktop as a service.

Your enterprise can rest easy knowing that all aspects of a complete SASE solution (and beyond) are covered by FirstLight.

[i] 7 must-have features for SASE infographic (cisco.com)
[ii] Dark web threat intelligence firm Cybersixgill lands $35M | VentureBeat
[iii] Cloud Architecture that cuts latency by 73% - Cisco Umbrella
[iv] What is DDoS Attack? - Check Point Software
[v] Quantifying-the-Benefits-of-SASE-WP.pdf (intelligentcio.com)

To talk with an expert about how you can better integrate networking and security functions in the cloud through SASE architecture, connect with us today or visit **FirstLight.net/sase.**

To talk with an expert about how you can better integrate networking and security functions in the cloud through SASE architecture, connect with us today or visit **FirstLight.net/sase**