SASE:
BUYER'S GUIDE

JUNIPER NETWORKS | Engineering Simplicity

CONTENTS

JUNIPER NETWORKS | Engineering Simplicity

The Buyer's Guide to SASE

Canalys estimates cloud infrastructure services grew 33% in 2020 to $142 billion, representing an increase of $45 billion in annual spend in 2019[1].

The cloud is part of our everyday lives; from sharing pictures with family and friends, streaming music, tv, and movies to remote work, it is inescapable. This increase has meant that many organizations have accelerated their move to the cloud, since adoption provides growth and competitive advantages.

These trends provide indisputable evidence that the number of organizations deploying a cloud strategy continues to accelerate. The cloud has been a healthy segment for a while and shows no signs of slowing down

We hear similar sentiments in conversations with our customers.

Jason Philp, Director of Infrastructure at Beeline, attributes this uptick to needing to support a more distributed workforce.

"For us, not only did we have to adjust to a distributed workforce, but we were also growing internationally. We needed the ability to give very end-user exactly what they need to do their job effectively. It is essential that our remote employees have the same experience as our employees that are coming into the office every day."

Over the last five years, we've changed the way we work. With such a large proportion of workforces going remote, the advantages of the cloud and cloud architecture are hard to ignore. A cloud architecture simply makes sense. Its operational simplicity, compelling economics, improved service experience, increased agility, and scale provide the flexibility required to meet business needs. It helps maintain business continuity and access to services, no matter where an organization's workforce or customers are located.

Organizations require predictable and reliable connectivity combined with intuitive management and robust information security to protect users, devices, and data. These requirements empower organizations to effectively leverage the power of the cloud for centralized and distributed workforces ensuring a consistent user experience for their end-users, wherever they are in the world.

[1] Canalys (2021). *Now and Next for the Cybersecurity Industry – Part 1.* https://www.candefero.com/content/preview.php?id=17382

The SASE Destination

A SASE architecture brings together the best of both worlds: networking converged with security that centers around granting secure access to users based on the risk they introduce at that moment in time.

It provides protection from attacks, regardless of where users are located, ensuring consistent security enforcement without having to backhaul traffic to a corporate location, reducing latency, and providing a better end-user experience.

As security and the network continue to converge, it has become even more critical for IT teams to use all connection points to provide visibility, intelligence, and enforcement against malicious activity.

Organizations have data and devices spread globally, being accessed from endpoints in multiple locations, from offices and conference centers, to homes and local coffee shops. With a SASE architecture, it's easier to secure data access with very low latency because security inspection and the application itself are geographically closer to the user.

A well-built SASE architecture delivers a threat-aware network for the cloud era and ultimately improves security while reducing complexity and streamlining management. When organizations empower the network to be threat-aware, security incidents are detected sooner and attackers are less likely to gain a foothold in the network, which safeguards users, applications, and infrastructure.

The flexibility of a SASE architecture is a game-changer because it delivers on the value of what a cloud-driven network can do and frees organizations from the limitations inherent in a static environment. With a SASE architecture, connectivity is highly performant and reliable, and security is seamless and invisible to end-users, providing an optimized and secure user experience.

How Threats Work

Security must be about what you see, what you know, and what you do.

To understand what you are seeing on the network as an attack, you must know how a threat operates. The chain of events outlined below is commonly referred to as the Cyber Security Kill Chain™. Let's take a quick look to understand how threats work and the steps they take to infiltrate a network.

RECONNAISSANCE

As we have seen in countless Hollywood blockbusters, every good heist requires research. The same is true for cybercriminals. An attacker might look to see where your vulnerabilities are. For example, let's say you are posting a job for a new IT position. That job post might list the technologies your organization uses, and they can research vulnerabilities to find out the easiest way to attack the network.

WEAPONIZATION

After all of that careful planning, the attacker is now ready to package the exploit to target the identified vulnerability, leveraging the research conducted during the reconnaissance stage.

DELIVERY

Now the plan needs to be put into action. The attacker needs to deliver the exploit (or malware in some cases). The action plan can take many forms, but a common delivery method is phishing. All that is needed is to trick an unsuspecting person into downloading a malicious file or click on a questionable link.

EXPLOITATION AND INSTALLATION

Now that the attacker has gained access, they can enable the attack code and install themselves on a victim's host machine and take control.

COMMAND + CONTROL

Threats need instructions; for the malware to work, it needs to communicate with the attacker. This communication channel is called Command and Control (C2). Like the ringleader in the heist van parked down the street radios into his associates inside, if Command and Control channel is shut down, it stops the threat in its tracks.

LATERAL MOVEMENT

Once the attacker has installed malware on the initial machine, they will most likely want to target additional devices on the network that have access to what they're after. They will try to make lateral hops to the desired victim endpoint. This process could take days, weeks, months, or sometimes years.

ACT ON THE OBJECTIVE

Attackers aren't always stealing credit card data or intellectual property. Sometimes they want to deface a website or take down a network. Like in heist movies, sometimes the attack might have been carried out for direct monetary gain, as is the case with ransomware.

SASE Made Real: A Retail Example

There is an expectation that network traffic will increase both in-store and online during certain times of the year. The demands on the network require additional resources to accommodate spikes in secure connectivity and to support secure access for point-of-sale devices, shopping websites, and payment gateways with minimal latency.

Traditionally, IT teams invest a lot of time and money in preparing for the increase in traffic and an expected barrage of cyber-attacks. This barrage forces IT teams to make tough decisions between accessibility (because additional load time for employees and shoppers means lost revenue) and security (because spikes in expected network traffic and online activity directly correlate to spikes in cyber-attacks, which also means lost revenue).

In such a traditional architecture, traffic needs to be backhauled to a centralized network hub for security inspection and then routed to the desired application or service.

A SASE architecture provides traffic inspection and makes services accessible to and from points of presence near the geo-location of each physical store and online shopper.

Extra capacity and capabilities can be added automatically to accommodate peak demand and scaled-down when demand decreases. Businesses no longer need to choose between security and performance due to the elimination of backhauling the traffic, making the end-user experience seamless, and reducing risk simultaneously.

Finding the Right Path to SASE

No two cloud journeys are the same.

No two cloud journeys are the same. Each organization has different regulatory requirements, risk tolerance, security needs, and business demands. There is no single security product that can solve all of the risk management challenges an organization faces. SASE is an architecture, and the transition will not happen overnight. Moving to a SASE architecture is a journey and requires every organization to take a thoughtful approach to this network transformation to remain secure.

SASE is a network transformation and will take place over time, and an organization needs to determine the migration path. That path is about how the organization chooses to design, build, and maintain the network architecture to optimize the user experience and secure services and data.

Threats can be introduced into the network from many different vectors. A SASE architecture can be used to protect against attacks across each step in the kill chain, regardless of where the user or service is located, by employing Zero Trust principles and ensuring consistent security enforcement. Each SASE element is essential in stopping threats in their tracks before gaining a foothold in the network. However, no single part of SASE can solely protect the network from harm. SASE is an architecture that needs every component to work in harmony to keep the network truly secure.

It is essential to understand which elements of a SASE architecture exist on the network already and which gaps need to be addressed first. Consider what dedicated resources are required to make this transformation possible. The best network can accommodate both cloud and on-premises deployments while supporting the transition to the cloud and the ongoing needs of the business. Every organization needs a diverse and adaptable architecture to support the business now and into the future.

So, what makes up a SASE architecture?

Let’s Get SASE – Building the Architecture

As with any new architecture, start with putting the right building blocks in place that will work with your current investments.

You do not have to throw out what is currently working in order to move to a SASE architecture.

Before you start taking inventory of your existing investments, let’s consider the components of a SASE architecture:

Unified Security Management

- Zero-Trust Network Access (ZTNA)
- Firewall-as-a-Service (FWaaS)
- Cloud Access Security Broker (CASB)
- Software-Defined Wide Area Networking (SD-WAN)
- Secure Web Gateway (SWG)

Unified Security Management

The journey to SASE starts with a great user experience. Unified security management must be your first step towards SASE to ensure a seamless migration of services that doesn't create a heavy operational burden for your team. Consistent security policy and visibility is essential for safeguarding users, applications, and infrastructure across every point of connection on the network.

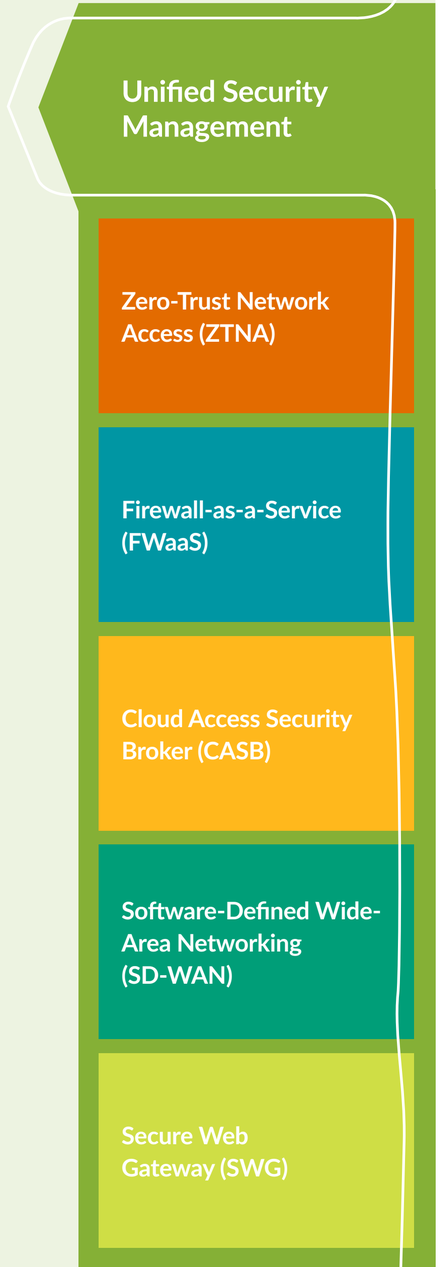
Security tools typically come equipped with their own individual management system, each of which has its configuration and interoperability challenges with other tools. These challenges produce visibility gaps, especially when an integration is suboptimal or stops working altogether, increasing risk and keeping administration and operations teams busy with lengthy fixes and workarounds.

Unified Security Management addresses these challenges and enables a seamless and secure transition to a SASE architecture by providing an easy-to-use UI, consistent security policy constructs that follow the user, device, or application without manual, time-consuming processes, such as copying over or recreating rule sets. Management should help organizations bridge current security deployments with their future SASE rollouts seamlessly and securely, and deliver orchestration and monitoring to deployments anywhere and everywhere, on-premises and in the cloud.

Unified security management should include centralized orchestration, administration, zero-touch provisioning, site and policy monitoring, and analytics to provide a unified view of the entire network, including enhanced session statistics, which are essential in both centralized and distributed environments. Administrators need complete network visibility to do their jobs effectively and require detailed reports on users, traffic events, and both network and security incidents. These reports and dashboards help to better detect and prevent network attacks while satisfying compliance requirements and maintaining network uptime.

REQUIREMENTS
For a successful SASE architecture, Unified Security Management must have:

- **Complete Security Visibility.** Pervasive visibility to all components of the network – users, applications, devices, and traffic — with customizable reporting and dashboards.
- **Scalability.** Effectively scale management for physical, virtual, and cloud-based security environments.
- **Bi-Directional Sync.** Synchronize changes between on-premises and cloud-based deployments to provide a cohesive experience as services migrate to the cloud.
- **Consistent Security Policy.** Easily manage and enforce consistent security policy across on-premises and cloud environments simultaneously, with policy constructs that follow the user, device, and application without having to copy or recreate rule sets.
- **Integrations.** Unified Security Management must easily integrate with existing security management systems to provide seamless visibility, control, and secure data sharing.



Zero-Trust Network Access (ZTNA)

Assessing risk is complicated because it is dynamic and unique to each organization. An organization's overall risk posture constantly changes as users, devices, and applications connect and disconnect. Previously, it was difficult for security teams to see how data was protected. As bring-your-own-device (BYOD) has become more widespread in offices and across distributed workforces, many organizations are assuming additional risk that they did not previously have to worry about.

Authentication and risk mitigation measures must stretch across the entire network from client to cloud, application, and workflow. Within a SASE architecture, your users can connect to your network directly using your nearest cloud point of presence (PoP) without having to reroute traffic to a corporate office, campus, or branch location. Zero-Trust Network Access (ZTNA) makes secure access possible in a SASE architecture. It provides users with secure remote access and authentication to applications and services based on defined access control.

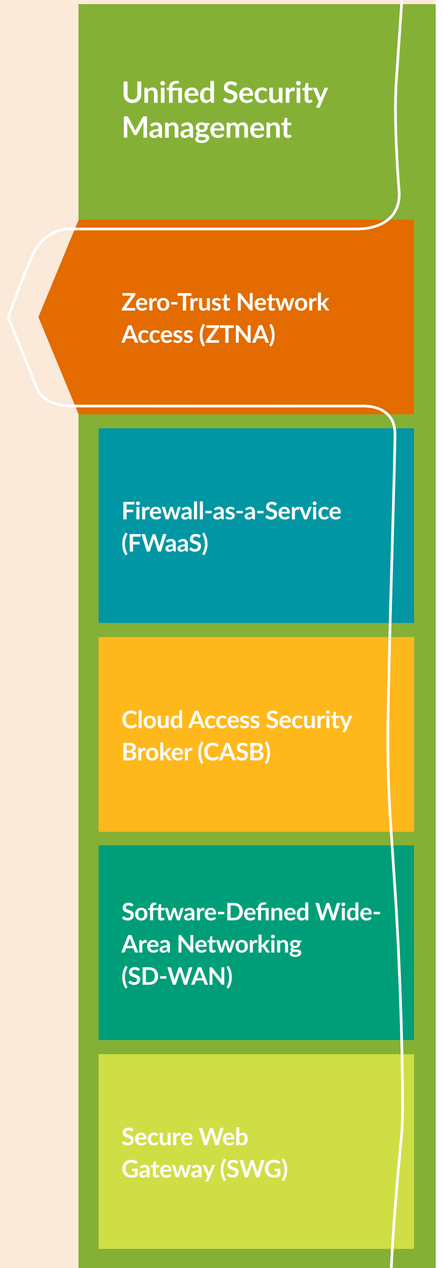
ZTNA verifies the identity and risk posture all in one process, routing the user to the nearest cloud point of presence where the security policies are monitored and enforced. ZTNA provides an optimized network experience, giving administrative teams the ability to prioritize and deprioritize traffic based on specific network needs and manage the experience for all users on the network.

Effective ZTNA cannot happen without a Zero Trust Fabric. Prescriptive control over who accesses what and how is fundamental to ZTNA, and simplifies operations for administrators, and improves overall user experience.

Every organization has different regulatory requirements for how their remote users connect to the corporate network; some support VPN, ZTNA, and more than likely, they support both.

REQUIREMENTS
For a successful SASE architecture, ZTNA must have:

- **Access Controls and Microsegmentation.** Use the network to authenticate and authorize users and devices, and control who can access specific resources at a granular level wherever they are. This includes authenticating sessions at each point of connection to ensure session integrity.
- **Monitor User Behavior.** Visibility into user and device activity on the network. Use granular controls and monitor user risk profiles in real-time.
- **User and Entity Behavior Analytics.** Bring contextual awareness to the network by associating transient sessions with the applications and services they enable. Gain visibility and establish profiling criteria based on suspicious user and device activity across applications and SaaS services.
- **Risk Management.** Verify the user's identity and risk posture all in one process, routing the user to the nearest point of presence where the security policies are monitored and enforced. Additionally, monitor devices and users accessing the network and ensure compliance. This visibility gives administrators the information they need to make critical decisions, such as granting users access to certain individuals for specific applications and data as required. Empower administrators to set policy and block suspicious websites and behaviors on the network before they cause a problem for the organization.



Zero-Trust Network Access (ZTNA)

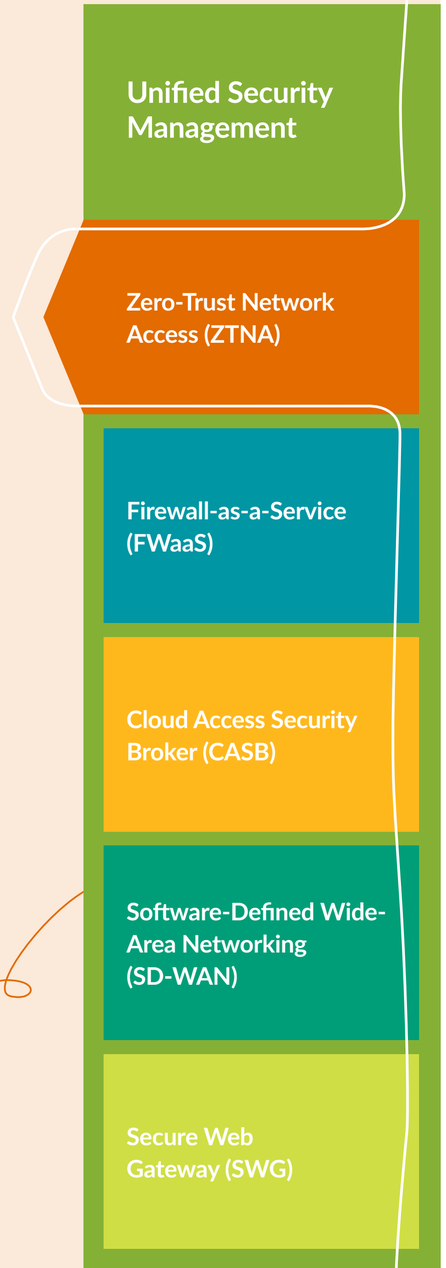
Some organizations may require the ability to monitor and report who is accessing the network and when as part of their regulatory requirements.. It is critical to address these capabilities when looking at VPN and ZTNA solutions.

While both support consistent security policies that extend anywhere users are, it is vital to understand their differences. VPNs typically route all traffic through a tunnel to the company network, including secure public Software-as-a-Service (SaaS) applications, standard Internet access, and services hosted on customer premises.

A ZTNA solution brings contextual awareness to the network by associating transient sessions with the applications and services they enable, and tying those sessions to verified user identity and authorization. ZTNA must simplify how enterprises support the needs of both an centralized and distributed workforce by providing consolidated management, hypersegmentation, individualized flows, and integrated functions—all with infused security and dynamic traffic control.

ZTNA enables organizations to simplify control of services, tenancy, and policy information, which minimizes complexity, improves visibility and lowers costs. This context-aware approach must support the needs of every organization and help fuel success, especially as unexpected challenges arise and the ability to support remote workers becomes critical. With ZTNA, the operational experience is simplified dramatically. No matter where security functions exist, they should be configurable through a single management console, improving IT and security teams and end-users' overall experience.

Through ZTNA, organizations can extend secure access anywhere and everywhere that users are and use the network infrastructure to authenticate users and devices, maintain session integrity, assess risk, and deny attack traffic. By building a threat-aware network for the cloud era, organizations can benefit from operational simplicity and security at scale that is invisible to the end-user.



Firewall-as-a-Service (FWaaS)

Constant shifts in application use, user behavior, and network infrastructure have created a threat landscape that continues to expose organizations to an increasing attack surface. Users need access to a growing number of applications hosted in the cloud and operate across different devices. While seamless access to these applications is critical for the end-user, security must also be considered. Application traffic should not increase the organization's risk.

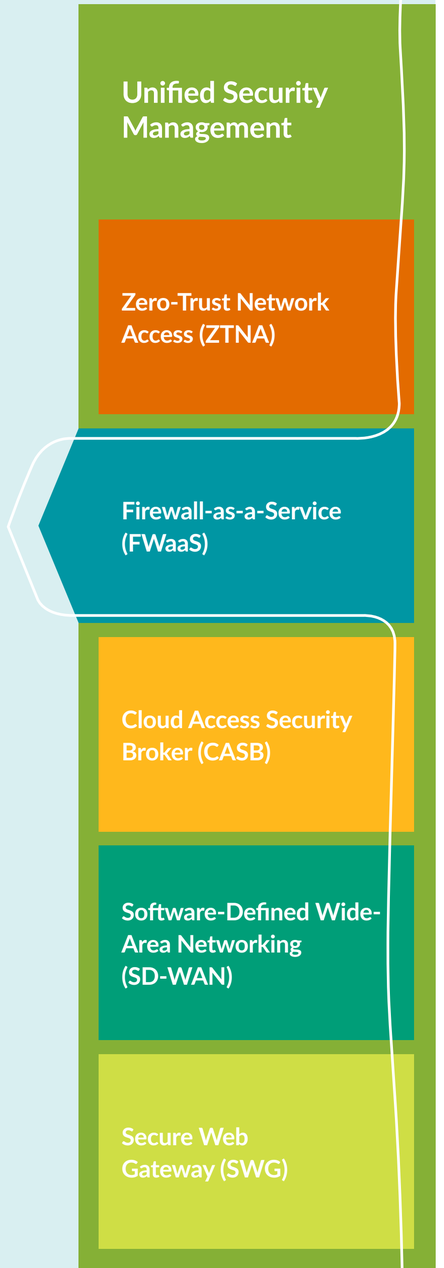
Security policies must identify and stop threats at every point in the Cyber Security Kill Chain, reducing overall risk and improving security posture. Contextual security is needed to combat these threats on-premises and in the cloud while maintaining authorized user access to new applications on different devices. FWaaS must reduce the risk of attack and provide granular control of applications, users, and devices through identity-based policies, microsegmentation, VPN connectivity, and validated threat prevention.

FWaaS must deliver integrated protection services with application awareness, user identity, and content inspection. These services must offer wide range of security mechanisms that address multiple stages within the Kill Chain™.

It is essential for FWaaS to recognize applications and their underlying services, and surface the application name, description of the service, and inherent risk level.

REQUIREMENTS
For a successful SASE architecture, FWaaS must have:

- **Application Visibility and Control.** Identify network traffic by application and underlying service, and provide granular controls around usage, risk allowance, and inspection policy.
- **User Identification and Access Control.** Integrate with directory services to create security policies associated with specific users or groups to enforce security protection.
- **Exploit Protection.** Constantly monitor for network and application exploits, including against recently discovered vulnerabilities. Provide comprehensive protection against a broad range of known security exploits in applications, databases, and operating systems with minimal latency.
- **Network Anti-Malware.** Protect against malware, grayware, viruses, phishing attacks, spam, botnets, and other threats through antivirus, antispam, and content filtering. Implement real-time security defense that ensures businesses have up-to-date signatures that provide visibility into new and commodity threats.
- **Microsegmentation.** Secure applications and defend against lateral threat propagation by defining which users and device types may access which applications and services at the session level. This includes segmenting based on the risk level or compromise status of the user, device, and/or application to protect against lateral threat movement.
- **Global & Local Threat Intelligence.** Leveraging a global IoC database to deliver validated threat intelligence, along with dynamic malware analysis, encrypted traffic inference, and share local threat intelligence from different parts of the network to ensure a fully informed and cohesive network defense. FWaaS should protect against trojans, worms, ransomware, C2 traffic, botnets, mobile malware, and IoT threats.



Firewall-as-a-Service (FWaaS)

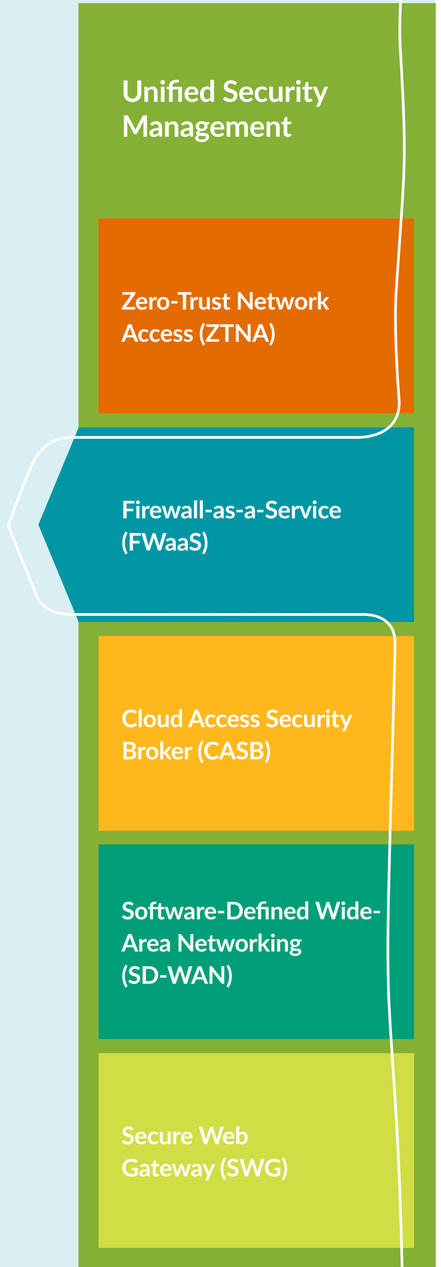
FWaaS must provide the context that links application use to individual users, regardless of location and device. Additionally, it must enable administrators to granularly control or outright block risky applications before they can do any damage. FWaaS must reduce an application's threat footprint by allowing the definition of granular security policies, such as the level of deep packet inspection and which users or groups are allowed access.

FWaaS must be able to inspect traffic for threats, including decrypting encrypted connections. For client-to-server communications an application-level Secure Sockets Layer (SSL) proxy must sit between client and server, intercepting encrypted traffic, terminating the session, and re-initiating the connection towards the end destination. It can be used as an SSL "forward" proxy that sits between users on the corporate LAN and their access to the Internet, protecting the end client. It must intercept HTTPS traffic by acting as a gateway at the organization's perimeter, terminating encrypted traffic before it enters the organization. At that point, unencrypted traffic is immediately inspected to determine compliance with security policy, as set by the security team. Traffic is then handled by proactive malware engines that will instantly block malware, thwarting potential security breaches.

Malicious files, including ransomware and adware, continue to increase from multiple attack vectors. These threats compromise network endpoints and facilitate data theft, including credentials and personally identifiable information (PII). Detecting and blocking malware and unwanted files at the network level before making it onto an endpoint is critical to safeguarding users, applications, and infrastructure against attacks. Anti-malware protection must combine cloud-based file reputation, threat intelligence comprising different indicators of compromise, and malware signatures. The result is a highly effective perimeter defense against many known threats, which doesn't slow down users or the business.

Advanced malware detection and prevention leveraged by FWaaS should be able to discover zero-day malware and malicious connections, which typically means leveraging machine learning algorithms and applying them in different ways, including detecting threats without breaking decryption and surfacing compromised devices. By leveraging a global threat database to deliver threat intelligence, along with dynamic malware analysis, encrypted traffic inference, and global and local intelligence sharing to ensure a secure network experience. FWaaS should protect against trojans, worms, ransomware, botnets, and IoT threats.

FWaaS should include several key components that provide a powerful platform to protect against constant cyber-attacks.



Cloud Access Security Broker (CASB)

As we have seen over the past few years, the use of software-as-a-service (SaaS) applications has been steadily increasing with no signs of slowing down.

In fact, according to Technavio, the projected size of the global SaaS market will grow to $60.36B by 2023.[2]

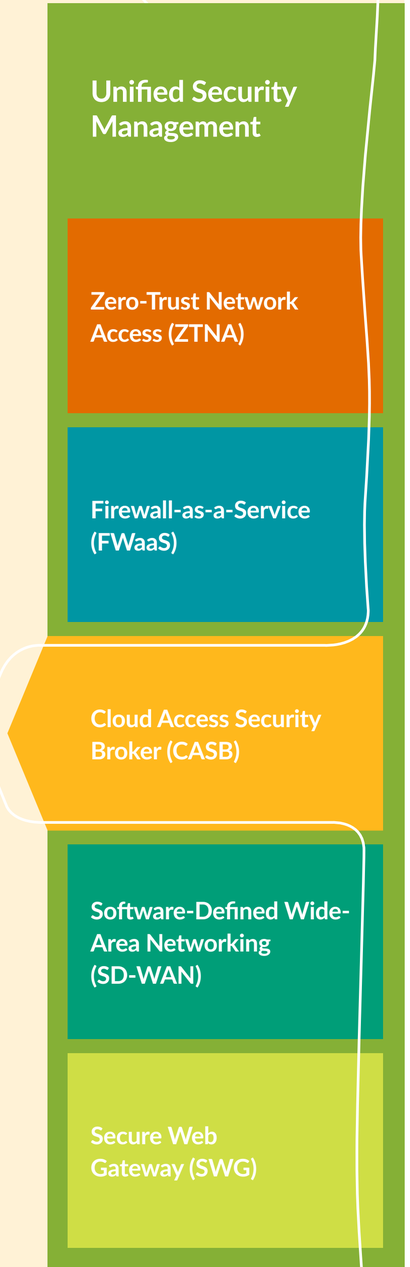
In fact, according to Technavio, the projected size of the global SaaS market will grow to $60.36B by 2023. For every SaaS application available on the Internet today, one thing is true: applications reside outside the jurisdiction of an organization's IT and Security team and inhibit their ability to manage them.

Organizations can't simply hand their security over to the likes of Salesforce, Atlassian, and Box, without having security measures in place to address the data being hosted. Even though SaaS companies do their utmost to protect their customers, an organization's individual security requirements are unique to them and must be addressed accordingly. A complete and exhaustive set of security tools should be applied when sending web traffic to the Internet or receiving traffic from the Internet. Over the past ten years, the percentage of traffic to the Internet from a branch versus the corporate data center has increased from 20% to 80%. This increase is likely due to corporations implementing SaaS services for accounting, CRM, Office 365, and many others.

Over the past ten years, the percentage of traffic to the Internet from a branch versus the corporate data center has increased from 20% to 80%. This increase is likely due to corporations implementing SaaS services for accounting, CRM, Office 365, and many others.

Security for cloud-based application access is essential for enforcing an organization's security measures because SaaS applications run on networks that are not controlled by the organization, and because they are built to be easily accessed, which may introduce risk from unsanctioned applications. CASB allows organizations to control security policies of their SaaS instances, and eliminates shadow IT. CASB helps organizations with granular application and access controls, and a way to segment users, their roles, and what actions they're allowed to take given the risk. For example, an organization may only want users with a specific domain to have access with edit and download privileges to a particular file-hosting application, while all others are limited to read-only or no access at all.

As important as its access controls, CASB scans SaaS instances for malware. Every file that gets uploaded goes through a reputation check or sandboxing process to identify whether malware is present. If malware is present, the upload will not be allowed to continue, or the file will be uploaded, but not accessible.



[2] https://www.businesswire.com/news/home/20190626005438/en/Software-as-a-Service-SaaS-Market-Worth-USD-60.36-Billion-at-9-CAGR-During-2019-2023-Technavio

Cloud Access Security Broker (CASB)

Data authentication and encryption are centralized in hubs across the network and can be accessed by all endpoints on the network, including personal devices. CASB gives security teams visibility into how data is accessed and protected, which they previously couldn't see, increasing their security risk. With CASB, organizations can see where their cloud data is and help keep it protected.

As more organizations move to the cloud every day, the importance of CASB becomes more and more relevant. While the cloud offers fantastic benefits, organizations must provide consistent security across both on-premises and multiple cloud environments and applications, protecting the data being used by employees and customers.

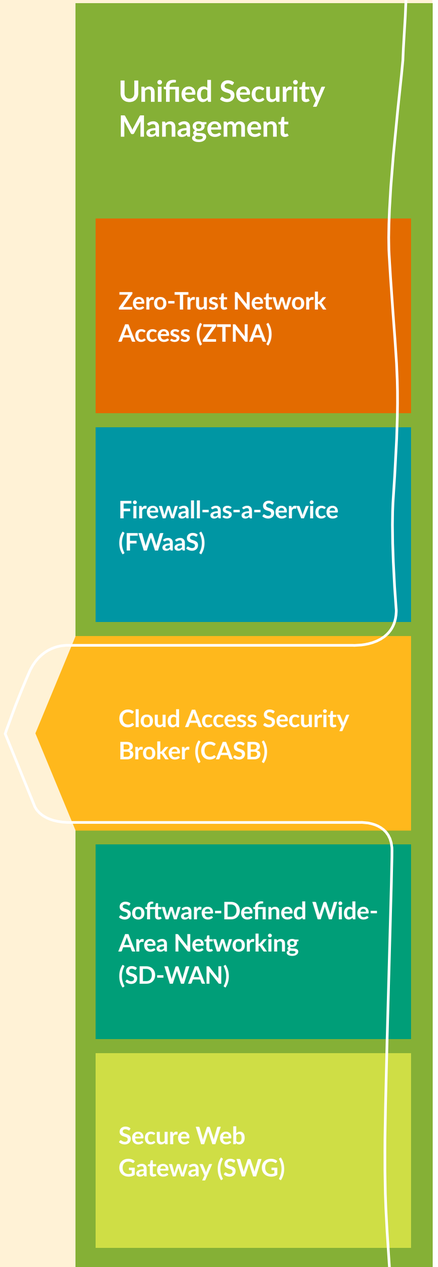
CASB provides deeper visibility and granular controls into what is being accessed within SaaS applications and by whom — not just the file being accessed, but the name of the file and the type of data being used. Data classification and loss prevention (DLP) reads files, and classifies content, such as credit card numbers, social security numbers, and addresses, and tags the file as containing a specific type of data. That data gets consumed by the organization's DLP policy. This policy is essential, as you can add in granular controls for documents with specific tags, such as HIPAA and PII. The policy allows an organization to limit who has access to a file based on the type of data it contains, to keep the data safe and the company secure.

Visibility into SaaS applications is critical to quickly assess application and network health, compliance, and identify potentially malicious activity. CASB gives administrators visibility into what is happening on the network and into SaaS applications that an organization uses as an extension of their network.

CASB delivers vastly improved security that leverages connection points to apply security policy and enforce threat prevention. CASB helps enable a threat-aware network by extending visibility, intelligence, and enforcement to every point of connection on the network.

REQUIREMENTS
For a successful SASE architecture, CASB must deliver on:

- **Management.** A clear line of sight is necessary to see what is happening within SaaS applications, including clear and concise reporting, and the ability to remediate an attack.
- **App Discovery and Usage Visibility.** Deep visibility into usage of cloud applications with key user, device, and location information. Discover SaaS applications being used and support custom applications on demand.
- **Service Access Control.** Determine and regulate when and how applications and data are accessed and by whom both across all SaaS applications.
- **Data and User Security.** Monitor and manage access controls and enforce security policy for SaaS applications, including data encryption and application actions.
- **Advanced Threat Protection.** Detect malware and malicious connections, including botnets and C2 hiding in encrypted traffic. Enforcing granular protection mechanisms, such as file quarantine and reduced access rights.
- **DLP.** Classify and monitor data transactions and enable enforcement with a strict set of customizable controls for security policy, ensuring business compliance requirements and data protection rules are followed.
- **Compliance.** Monitor, report on and identify service usage and behaviors to govern compliance issues for security teams to address, helping the organization remain compliant with regulatory and administrative requirements.



Software-Defined Wide-Area Networking (SD-WAN)

Gartner defines SASE as a transformational technology that combines elements of SD-WAN and network security into a single cloud-managed package.

For SASE to be truly successful, the network must dynamically detect where services, such as SaaS applications or applications hosted in public or private clouds, are located to deliver valid sessions to those services, and this is where the evolution of SD-WAN plays an important role.

An organization's SASE architecture has SD-WAN built in to deliver network connectivity as efficiently as possible without adversely impacting risk posture or service experience. Since sessions make up the active connections to a given service (for example, a Zoom video call), SD-WAN routing should recognize and route based on sessions, and ensure that sessions are delivered based on user and device identity and context following real-time policies for performance requirements. SD-WAN must provide efficient networking and secure access for users and devices distributed in multiple locations around the world — this is a key requirement for a implementing a SASE architecture.

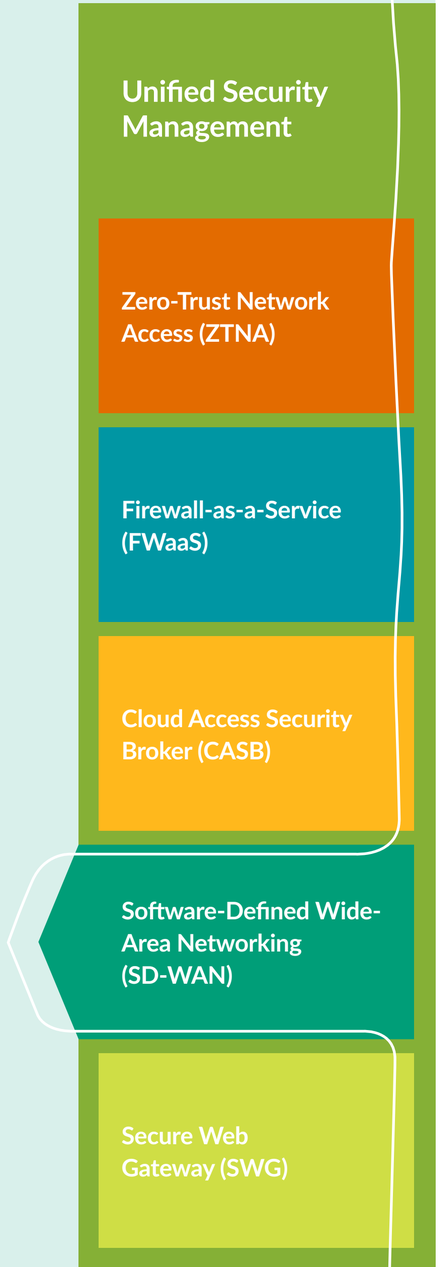
SD-WAN edge devices within a SASE architecture dynamically provide secure access to services by discovering connecting user and network devices and their privileges, and then securing the traffic as it moves between connection points. SD-WAN delivered within a SASE architecture has built-in capabilities to provide these security services across the entire network.

SD-WAN is designed around the applications that users consume. Service-centric networking is a top-down approach for configuring the dynamic routes. Administrators need to be able too describe the services within the network, as well as the group(s) within the network allowed to access each one. This process enables the network to route sessions towards services rather than towards IP addresses. Once the SD-WAN edge devices know that the sessions are valid, they can direct them towards the services with which they are meant to connect. This step ensures that only valid sessions are sent towards services authorized to consume them, and is a key part of ensuring a Zero Trust network.

Session intelligence within SD-WAN plays an important role in securing connectivity. Without knowledge of services, an SD-WAN edge device would simply forward packets without verifying a user's identity and blindly connecting them to a destination IP address. This lack of intelligence leaves the network vulnerable to attack.

The SD-WAN edge device should allow network administrators to deliver a user-centric, intent-based networking solution that follows business logic to securely connect users to services and applications.

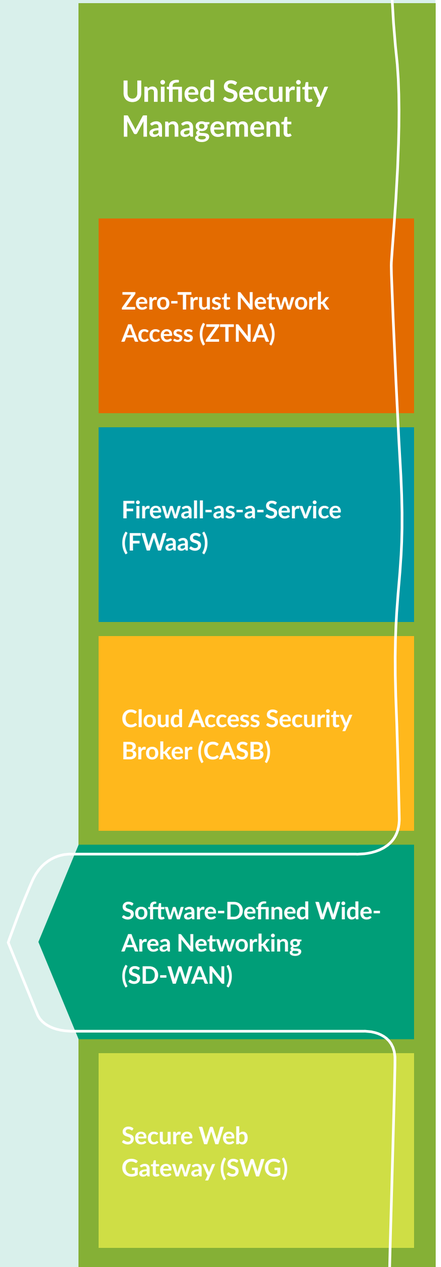
The networking side of a SASE architecture provided by SD-WAN must provide additional security mechanisms, such as deny-by-default routing, policy-based forwarding, enforcement, and built-in corporate network firewall functions. SD-WAN should enable end-to-end segmentation and Zero Trust security at the network layer, allowing enterprises to ensure a secure user experience at any site.



Software-Defined Wide-Area Networking (SD-WAN)

REQUIREMENTS
For a successful SASE architecture, SD-WAN must have:

- **Application Quality of Service.** Prioritize applications based on an organization's business and bandwidth needs. An organization can allow users to prioritize traffic and limit and shape bandwidth based on application information and context for improved application and network performance.
- **Advanced Policy-Based Routing.** Classify sessions based on applications and apply the configured rules to route the traffic. An organization can route traffic over different WAN links and assign higher priority to business-critical applications.
- **Application-Oriented SD-WAN.** Application-oriented, intent-based routing that follows business logic and uses real-time information to intelligently decide how to connect applications. Dynamic service discovery should allow enterprises to scale new sessions for existing services based on load, add new services, and remove or modify existing services.
- **Define Service Capability.** Network administrators can define services to represent capabilities that the network is designed to deliver to consumers. It should enable the exchange of this service capability to all SD-WAN edge devices along with reachability and other parameters to connect to these services.
- **Detect Service Location.** Dynamically detect where services are located to deliver valid sessions to those services. The router should exchange service and connection information to those users using a service-oriented paradigm.
- **Policy Awareness.** Every device on the network must be aware of access policies and discover changes in identities, encrypt and authenticate sessions, resist attacks, and enable threat inspection.
- **Secure Session Integrity.** SD-WAN should facilitate a SASE architecture built on Zero Trust principles with deny-by-default routing, policy-based forwarding, enforcement, and session authentication as they are routed. SD-WAN should enable end-to-end segmentation down to the directionality, allowing enterprises to provide secure connectivity to services.



Secure Web Gateway (SWG)

Users spend more than half of their time browsing the Internet and using web-based tools. However, Web sites have created an attack surface that threat actors love to take advantage of.

According to Canalys, in 2020, more records were compromised in those 12 months than the previous 15 years combined.[3]

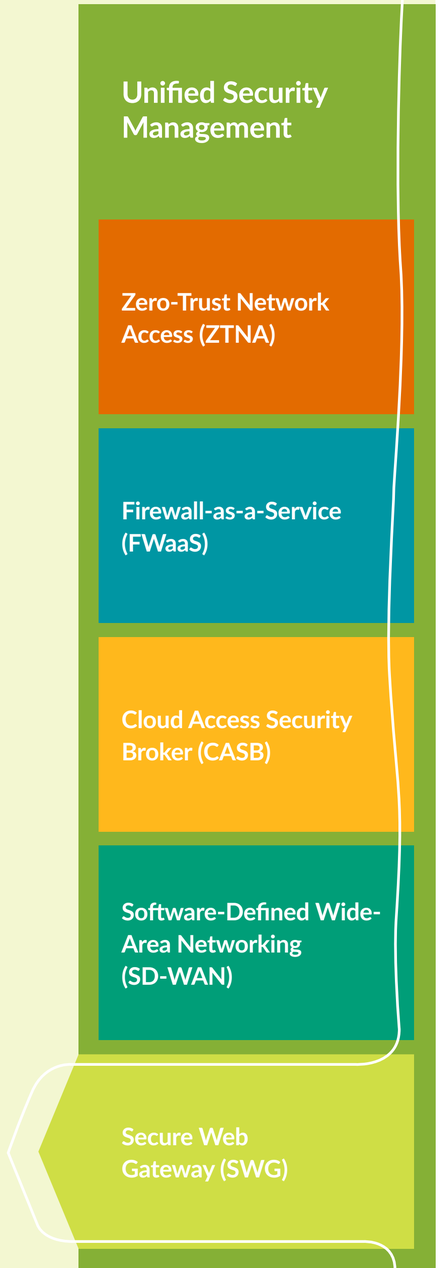
According to Google, more than 95% of traffic across Google is encrypted. Since so many attacks use encryption to evade detection, regulatory requirements for not decrypting certain types of web traffic shouldn't mean that an organization must accept that business risk.[4]

To address this, organizations must protect against web-borne threats, including within encrypted HTTP traffic where the session cannot be decrypted by the organization's security tools due to regulatory compliance, such as employees' banking and healthcare sites.

Still, users need access to a growing number of web applications that operate across different devices. While seamless access to these applications is critical for the end-user, effectively securing Web traffic must also be considered. Access to the Web should not unnecessarily increase the organization's risk. Additional security to protect against web-borne threats, such as malicious links, web application exploits, and drive-by downloads, is needed to combat these threats while maintaining user access to new Web applications on different devices with application awareness, user identity, and content inspection.

A Secure Web Gateway (SWG) provides Web traffic control through granular URL-based policies, content inspection, selective SSL decryption, and encrypted traffic insights to protect against Web-based attacks. A SWG filters out non-compliant Web sites, removes malware from allowed Web traffic. To accomplish this, SWGs include features such as URL filtering, intrusion prevention, selective SSL inspection, and machine-learning-based malware detection that also profiles HTTPS connections for malicious traffic. However, a SWG can't defend the network by itself; it requires additional security elements to combat threats while maintaining user access to new web applications on different devices.

Cloud-based anti-malware protection brings together file reputation, threat intelligence, and malware signatures. The result is a highly efficacious dynamic defense against many threats, which keeps users safe as they access web services and applications.



[3] Canalys (2021). Now and Next for the Cybersecurity Industry – Part 1. https://www.candefero.com/content/preview.php?id=17382

[4] Google Transparency Report. https://transparencyreport.google.com/https/overview?hl=en

Secure Web Gateway (SWG)

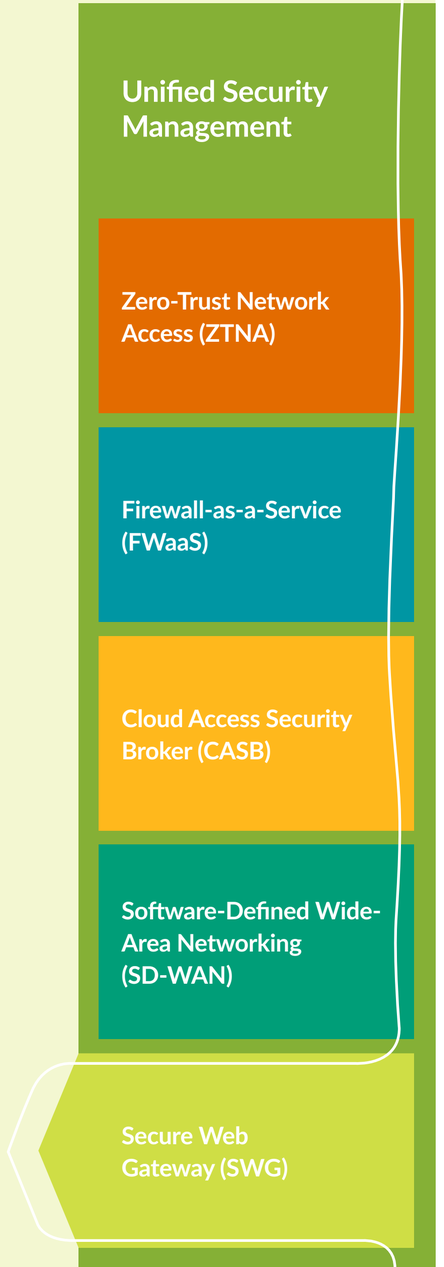
Simultaneously, certain data within web applications, such as online banking or healthcare, must remain private as required by regulations in certain countries, so decryption and inspection is not always possible. URL filtering allows administrators to block unwanted URL categories, such as gambling and malware sites, and enables selective decryption within URL policy to keep business traffic safe from threats while users' personal traffic remains private. To reduce attacks and provide granular Web control, URL filtering features should contain many URL categories that can be used within your network security policies and SWG policies based on a multitude of parameters (for example, by geo-location, user group, device status, etc.). It's also very important for network security and SWG rule constructs be similar and managed through unified policies, to reduce operational overhead and the likelihood for human error to create gaps in Web security policy.

Web-borne malware, including ransomware and adware, continue to compromise endpoints and make them facilitate extortion and data theft, including credentials and PII. Detecting and blocking compromised Web sites, malware, and unwanted files before they install themselves on endpoints is critical to safeguarding users, applications, and infrastructure against attacks. In addition, SWGs must natively integrate with network connection points to block or quarantine endpoints that do become compromised, even when those endpoints are not equipped with agents.

SWGs use machine learning to find and block known and unknown malware, C2 connections, and Web sites rife with unpatched CVEs.

User identity is a core requirement to enable administrators to create security policies that reflect business needs rather than network requirements. This flexibility makes for a powerful mechanism in defining, managing, and refining security policies based on user identity rather than IP address. A SWG associates Web traffic to a specific user through integration with directory services and ZTNA. Policies can be defined to allow Web application use based on individual users, user groups, and inherent risk, enabling more powerful but much simpler security controls. These granular rulesets should be expressed in terms of groups, allowing security policies to continue functioning as users are added or deleted.

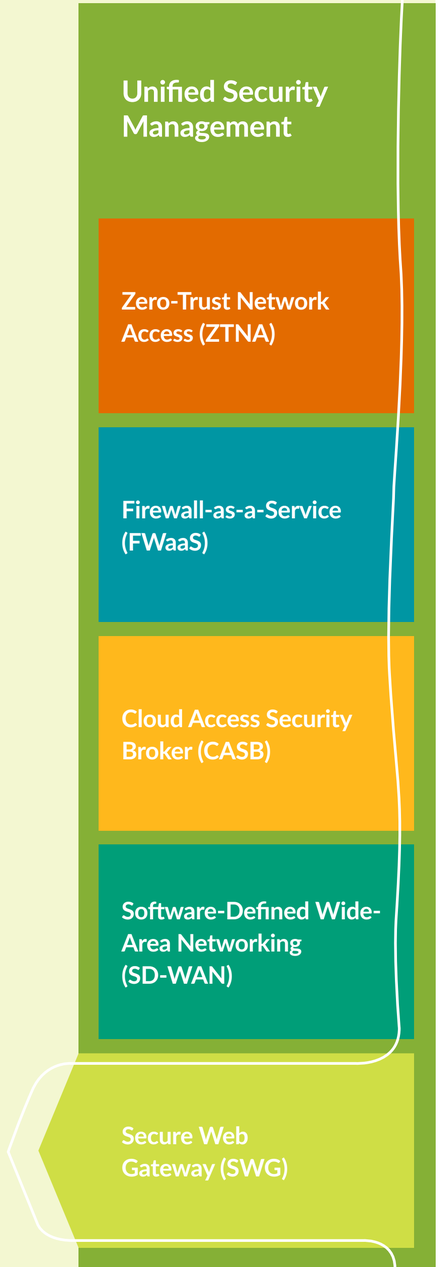
A SWG should support encrypted traffic inference and collect relevant SSL/TLS connection data, including certificates used, cipher suites negotiated, and connection behavior to detect malicious Web connections for traffic that cannot be decrypted and inspected. Organizations can restore visibility lost due to encryption without the heavy burden of full TLS/SSL decryption.



Secure Web Gateway (SWG)

REQUIREMENTS
For a true SASE architecture, SWG must have:

- **URL Filtering.** Provides Web traffic categorizations that can be incorporated into application and security policy, including one or multiple “malicious” categories to prevent Web-borne threats and unwanted browsing activity.
- **Unknown Threats.** Provide cloud-based service that performs sophisticated advanced malware detection through machine learning algorithms to identify previously unseen threats. Organizations can accurately identify unknown and never-before-seen malware that eludes conventional methods, ensuring complete protection.
- **Known Threats.** Protect against known malware, viruses, phishing attacks, intrusions, spam, and other threats through antivirus, and Web and content filtering. Organizations should have up-to-date signatures that provide visibility into threats and effective protection.
- **Encrypted Traffic Defense.** Selectively intercept encrypted traffic, terminating the session and inspecting for threats, re-initiating the connection towards the end destination. For traffic that cannot be decrypted, analyze connection telemetry to identify and block malicious connections, ensuring that privacy and security are no longer at odds. Organizations can prevent users from directly downloading malware hidden within encrypted traffic onto their end clients.
- **Global and Local Intelligence Sharing.** Leverage IoCs sourced globally and locally and use them to increase threat detection within Web traffic. Improve threat response times by taking real-time threat information and pushing it out to all points across the network.
- **Application Identification.** Provide a traffic classification engine that accurately identifies Web applications, including applications known for using evasive techniques to avoid identification. Organizations can gain more granular control by identifying unique applications rather than IP addresses to enforce corporate security policies to match their specific business requirements.



Let's Think About RFP

In the previous section, we established the critical use cases your organization's SASE architecture must provide.

This section will translate those requirements into tools you can use to identify and select a SASE provider. There are many elements to consider when evaluating how effectively a provider can deliver a SASE architecture that gives security and control with less complexity for security professionals.

It is equally as important to find a SASE provider who can meet an you where you are on your SASE journey by managing physical, virtual and cloud-based network security requirements without imposing the limitations of their approach on your organization and shifting operational overhead to your teams. Identify a SASE provider who can enable a seamless and secure transition to a SASE architecture by accommodating both traditional network security architecture and a SASE architecture simultaneously.

Unified Security Management
Every excellent user experience starts with management. The security industry has spent decades bringing technologies together under one management experience, only to break it now during this architectural shift when organizations need it most. For most providers, on-premises security policies are managed separately from cloud-based security policies and structured differently. When applications move, security teams must recreate and reapply policies, which takes time and introduces the likelihood that human error will create security gaps.
To ensure your RFP covers Unified Security Management, consider the following:

- How does the solution provide complete security visibility with customizable reports and dashboards?
- Is the solution scalable? How easily does it scale? How does it provide management capabilities for physical, virtual, and cloud-based security deployments?
- How does the solution sync between on-premises management, cloud-based management, and individual firewalls and sites?
- How does the solution manage and enforce consistent security policy across on-premises and cloud environments? How similar are the policy constructs? Describe how policies follow the user, device, and application without copying over or recreating rule sets?
- How does the solution integrate with existing security management systems? Does it provide seamless visibility?
- How does the solution convert on-premises security policies to cloud-based security policies?

Zero-Trust Network Access (ZTNA)
Zero-Trust Network Access (ZTNA) must empower organizations to build service-centric fabrics that deliver breakthroughs in simplicity, security, performance, and savings, and dynamically assess access levels based on risk..

To ensure your RFP covers Zero-Trust Network Access, consider the following:

- How does the solution authenticate and authorize users and devices? How is resource access controlled?
- How does the solution provide visibility into user and device activity on the network? How are user risk profiles monitored and controlled?
- How does the solution accommodate for both VPN and ZTNA deployment?
- How does the solution establish profiling criteria?
- How is secure access extended to users?
- How does the solution verify a user's identity and risk posture? Is it in all one process?
- Describe how the solution ensures session authentication between the client and destination
- How does the solution provide the data that administrators need to make critical decisions to grant access?
- Describe how the solution helps administrators set policies and block suspicious behaviors on the endpoint?

Firewall-as-a-Service (FWaaS)
FWaaS must identify and stop threats at multiple points in the Cyber Security Kill Chain™, reducing risk and ensuring

Let's Think About RFP

improved overall risk posture. FWaaS must reduce the risk of attack and provide granular control of applications, users, devices, and traffic content through identity-based policies, segmentation, and validated threat prevention.

To ensure your RFP covers FWaaS, consider the following:

- How does the solution provide insight into the context that links application use to a user, regardless of location and device?
- How does the solution surface application behaviors and identify risk? How does the solution block risky applications before they can do any damage?
- How does the solution integrate with directory services to create security policies? Are the security policies associated with specific users or groups to enforce security protection?
- How frequently are new threat signatures added?
- Has the solution's security efficacy been validated by a reputable third-party within the past year, and what was its efficacy score?
- Does the solution provide 100% resistance to different types of network evasions?
- Does the solution provide comprehensive protection against a broad range of known security exploits in applications, databases, and operating systems? Does it provide validated protection from malware?
- How does the solution protect against malware, viruses, phishing attacks, intrusions, spam, and other threats? How does it identify zero-day malware, IoT botnets, and mobile malware?
- How does the solution defend against lateral threat propagation? Does this require a separate endpoint agent?
- How are policies migrated from a traditional firewall construct to a SaaS-based firewall construct?

Cloud Access Security Broker (CASB)

CASB provides deeper visibility and granular controls into SaaS applications, including identifying shadow IT, scanning for and isolating malware, and protecting against data loss. CASB policies allow an organization to keep the data with SaaS applications secure.

To ensure your RFP covers CASB, consider the following:

- How does the solution surface insight into what is happening within SaaS applications? Is this integrated into a common UI and reporting structure?
- Does it provide key user, device, and location information?
- How are CASB policies integrated into a unified policy construct that is shared with other SASE architecture components, such as SWG and FWaaS?
- How does the solution uncover zero-day threats and malicious connections, including botnets and C2 servers hiding in encrypted traffic? How is this threat intelligence shared to other parts of the network?
- How does the solution address DLP and ensure controls for security policy? How do they ensure business requirements and data protections are followed?
- How does the solution monitor, report on and identify service usage and behaviors to govern compliance issues?
- How does it help organizations remain compliant with regulatory and administrative requirements?

SD-WAN

An organization's SASE architecture includes built-in SD-WAN to provide secure connectivity and must route based on the session. The routing should ensure that sessions are delivered based on identity and context to users and devices following real-time policies for performance requirements. SD-WAN must provide efficient networking and secure access to users and devices anywhere.

To ensure your RFP covers SD-WAN, consider the following:

- How does the solution prioritize applications based on an organization's business and bandwidth needs? Can administrators prioritize traffic and limit and shape bandwidth based on application information and contexts to improve application and network performance?
- How does the solution classify sessions based on applications? How are configured rules applied to successfully route the traffic? Can administrators route

Let's Think About RFP

traffic over different WAN links and assign higher priority to business-critical applications?

- Does the solution deliver an application-oriented, intent-based SD-WAN? How do routers autonomously decide how to connect applications?
- Does the solution enable enterprises to scale new routes for existing services based on loads, add new services, and remove or modify existing services?
- How does the solution define services to represent capabilities that the network is designed to deliver to consumers? Can it enable the exchange of this service capability to all SD-WAN edge devices along with reachability and other parameters to connect to these services?
- How does this solution detect where services are located to deliver valid sessions to those services?
- Is every device on the network aware of access policies? Can these devices discover changes in identities, encrypt and authenticate sessions, and segment based on connection directionality?
- How does this solution accommodate both VPN and ZTNA?
- How is encrypted traffic handled?

Secure Web Gateway (SWG)

SWG sits between the network and Internet, and should protect endpoints and the network from Web-borne threats and non-compliance. A SWG should filter malware from web traffic and enforce policy compliance. These gateways must include URL filtering, intrusion prevention, SSL inspection, and known and unknown threat detection for Web-based applications.

To ensure your RFP covers SWG, consider the following:

- How does the solution provide Web traffic categorizations that can be incorporated into application and security policy? How often are these categories updated?
- How does it prevent web-borne threats and unwanted browser activity?
- How does the solution protect against malware, viruses, phishing attacks, intrusions, spam, and other threats? Does it have up-to-date signatures that provide visibility into threats from all over the world?
- How does the solution intercept encrypted traffic, terminate the session, and re-initiate the end destination's connection? Can it prevent users from directly downloading malware hidden within encrypted traffic onto their end clients?
- Where does decryption and inspection happen? Is an endpoint agent required?
- How does the solution provide security for traffic that cannot be decrypted?
- If TLS 1.3 is used, how are policies applied and how is session privacy respected? Does the solution downgrade to TLS 1.2?
- Can the solution generate threat feeds including attacker IPs, C&C, GeoIP, and infected hosts?
- How does the solution provide web traffic categorizations? Does it prevent web-borne threats and unwanted browsing activity?
- Does the solution provide a detailed analysis of application volume and usage throughout the network based on bytes, packets, and sessions? How are these details reported?
- Does the solution integrate reporting and dashboards with other SASE components, such as FWaaS and CASB?
- Does the solution track usage and risk metrics and analyze traffic patterns? How does the solution improve overall network management and visibility?

Conclusion

When you commit to SASE, you're committing to a secure future.

The promise of a SASE architecture is incredible, but every organization must transition at its own pace. For some organizations, that means rapid adoption, and for others, a more methodical and steady transformation.

Whichever path an organization chooses, it is crucial to have a partner in clearing the way for you to implement a SASE architecture by meeting you where you are in your architectural shift, and that supports both networking and security technology. Finding a partner who can help you with both elements of a SASE architecture is essential for success.

SASE is about how the organization chooses to design, build, and maintain the network architecture to optimize the user experience and secure services and data. Understanding where you are today and where you need to go is the first step to a secure future for your organization.