CLOUDFLARE

WHITEPAPER

The Buyer's Guide to SASE Use Cases

How to navigate priorities and select the right platform for your journey

Table of Contents

How to use this guide

Who is this for?

Although modernizing networking and security toward a Secure Access Service Edge (SASE) will ultimately benefit everyone across your organization, **The Buyer's Guide to SASE Use Cases** is primarily designed for:

CIOs

responsible for the organization's overall digital modernization strategy and optimizing IT costs

Heads of Networking

responsible for delivering highly-performant, resilient, and secure modern networks that support corporate goals

CISOs

focused on improving cyber threat resilience, strengthening the overall security posture, and reducing breach costs

Whether your organization's SASE journey starts as security-led, networking-led, or an idealistic fully collaborative and cross-functional IT effort across security, traditional networking, and modern DevOps teams, the technical platform(s) you select need to serve every team. A true SASE architecture should be flexible and composable enough to accomplish the prioritized use cases on every team's short- and long-term roadmap; this guide will help you lead those planning conversations as you determine use cases and narrow down vendors.

What can you use it for?

Many organizations today understand the promise of adopting a SASE architecture, yet there is no "one size fits all" roadmap to get there. There are a broad spectrum of security and network modernization challenges along each organization's unique SASE journey, and not every implementation of SASE will be the same.

To help you find a starting point for your unique journey to SASE, use **"The Buyer's Guide to SASE Use Cases"** to:

- **Determine starting use case(s)** and "quick wins" with SASE alongside a long-term yet agile project roadmap. Reflect on internal priorities to facilitate cross-functional discussions that may help rank them.
- **Plan conversations with vendors** with sample questions to ask that push beyond "me too" claims and commoditized features. Dig into the heart of vendors' technical architectures — both the front-end interface and the back-end network, compute, and storage — and long-term business strategies.
- **Evaluate SASE options** with sample considerations organized across core service components. Understand the unique elements of vendors' platforms to watch for that can push beyond the basic, expected components.

This guide assumes familiarity with the main principles and components of a SASE architecture, but includes an extended "SASE Primer" in the appendix for clarity.

Find your starting point: priority use cases

Gartner®, Inc. identifies three single-vendor SASE use cases[1] that can help differentiate organizations' top priorities:

1. **Basic SASE** — This use case covers an easy-to-operate offering typically involving midsize enterprises (MSEs) looking to secure users of public and private applications.
2. **Network-driven SASE** — This use case covers an enterprise looking to deploy SASE with advanced network functionalities.
3. **SASE with advanced security** — This is for an organization that requires the best security, while ease of use is lower priority.

Cloudflare has also noticed some customers mainly focused on improving end-user experience and thus simplifying infrastructure through a trend sometimes referred to as **"coffee shop networking."**

While this model is generally useful, many organizations prefer discussing narrower use cases that resemble a scoped, achievable project in an effort to simplify their journey and better clarify short- vs. long-term goals. Starting small on your journey to SASE can also help prove efficacy, gain internal momentum, and increase support from stakeholders, improving the likelihood of buy-in for larger projects in the future.

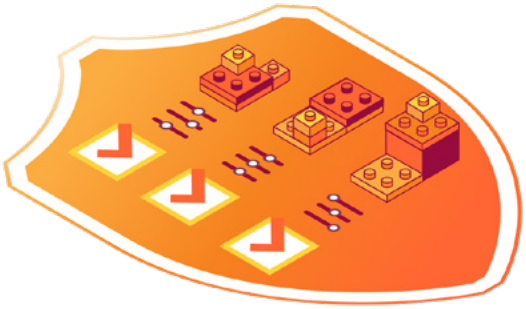
There is no perfect answer for how to choose a starting point, but frequently-cited internal decision factors include:

- **Flexibility and openness to change** — for example, the security team might be the best first customer for a starting point SASE use case if a pilot project can be more tightly scoped and done in tandem with existing infrastructure
- **Speed of implementation** — contractors, in particular, have limited remote access needs that can often be fulfilled without installing end-user software, which can simplify a project rollout and provide a "quick win" for strengthening security
- **Users/roles that are at greater risk for attacks** — developers who have access to valuable intellectual property, security/risk professionals, or executives may be prime targets
- **Apps that are at greater risk for attacks**—such as sensitive internal apps housing customer or financial data
- **Employee experience feedback** — consider end-user complaints to determine which internal workflows could benefit the most from efforts to improve business productivity
- **Existing contract timing/logistics** — upcoming contract renewals for current point solutions could steer your focus toward a relevant use case to address, and help create goal timelines for legacy solution augmentation or replacement

Take a look at the use cases below, organized into larger company initiatives, to reflect on which could have the most immediate impact on your organization's goals within the context of a longer-term project roadmap. While your internal priorities and existing IT stack ultimately will steer your best path, most organizations choose starting use cases that combine several of the above prioritization criteria like augmenting their VPN, securing contractor access, preventing multi-channel phishing, protecting remote workers and distributed offices, or simplifying branch connectivity.

That said, one of the best parts of a programmable, composable SASE architecture is that there is no perfect order of operations. Changes in business priorities and new tech integrations can all be accommodated over time. A long-term roadmap is recommended, but you should expect to stay agile.

The key is to not over-plan to the point that you delay getting started any longer than is necessary. **The dozens of use cases solved by a SASE architecture can instead be thought of as cumulative:** effort towards one or two use cases still make your organization's security posture stronger, and due to cross-service interactions across a SASE platform, implementing one use case may make another future use case easier.



Initiative: Adopt Zero Trust

Modern work (e.g. hybrid work, multi-cloud sprawl, unmanaged devices, etc.) presents new security challenges. Reliance on traditional perimeter-based security has left organizations with limited visibility, conflicting configurations, and excessive risk.

As a result, organizations are turning towards Zero Trust security best practices as a core tenet of their larger SASE journey — which are based on the principle of maintaining granular access controls for verification and not trusting anyone or anything (even those inside a network perimeter), by default.

Use case: Augment or replace risky VPNs

Network perimeter-based controls such as virtual private networks (VPNs) can increase your attack surface, limit visibility, and frustrate end users. VPNs are increasingly the target of attacks and increasingly vulnerable to breaches; they also "trombone" all traffic to and from central on-prem appliances, which can lead to latency (and impact productivity) when accessing internal tools and data.

As a result, one common driver for moving to a SASE model is to improve resource access and connectivity. Routing and processing network traffic across a global cloud network as close to the user as possible — i.e., with Zero Trust Network Access (ZTNA) instead of through VPNs — reduces end user friction, while eliminating the risk of lateral movement. Start offloading critical apps for better security and end user experience.

Use case: Secure contractor/unmanaged device access

Setting up secure access for third-party users (contractors, agencies, suppliers, partners, etc.) can introduce additional risk and administrative overhead. These collaborators frequently only need access to a limited set of resources for a limited time, yet traditional access control approaches can accidentally overprovision privileges. Issuing corporate devices to everyone is also usually not an option, and unmanaged devices lack the protections and visibility of corporate-issued devices, increasing risk. Especially given that contract and temporary work are as popular as ever due to hybrid work, many teams choose to secure contractor access early on in their SASE journey.

Setting Zero Trust policies ensures that contractors only access what they need for the time that they need it. Clientless ZTNA in particular is quick to deploy and helps contractors onboard quickly, given there is no end user software requirement. Contractors can "bring their own" identities through social login options, with ZTNA acting as an aggregation layer for all identities. Other data protection measures can also easily be added for strengthened posture.

Use case: Mitigate ransomware attacks

Because Zero Trust continuously monitors and regularly re-authenticates both users and devices, it can prevent ransomware attacks from spreading by revoking network and application access as soon as an infection is detected. Zero Trust also follows a principle of "least privilege" for access control, making it difficult for ransomware to escalate its privileges and move laterally to gain control over a network.

Use case: View and reduce data exposure

Limiting who can access which apps with Zero Trust policies can help prevent data exfiltration, but you can take further steps to mitigate the risks of data leaks with a data protection strategy that helps detect potential exposure and improve security posture. This can include scanning popular SaaS suites like Google Workspace, GitHub, or Salesforce for sensitive data and misconfigurations that risk leaks, and then acting on prescriptive guidance to remediate via blocking or other admin actions.

Case Study: Adopt Zero Trust

Fortune 500 telecommunications provider secures over 100,000 hybrid workers with Cloudflare

- Global leader in Information, Communications, and Technology (ICT) solutions
- One of the primary providers for 5G network infrastructure
- Employs over 100,000 people across Europe, India, and the United States

Challenge:

Scaling access controls across departments and regions

Following decades of technical innovation and growth, a Fortune 500 telecom provider had developed a complex IT and security architecture that spanned over several hundred legacy applications.

Maintaining on-premises infrastructure was becoming untenable. IT complexity slowed down their ability to strengthen their security and implement Zero Trust best practices. And, relying on Cisco Umbrella was burdensome — policies were difficult to tailor to specific user groups; basic network access required extensive administrative oversight; and the threat protection it offered left gaps across the company's architecture.

The company started looking for ways to move to a more agile cloud environment. This included:

- Selecting a security partner to support the migration of applications from on-premises environments to AWS, Azure, and other cloud environments
- Replacing Cisco Umbrella with simpler, more cost-efficient DNS filtering

Key results

with Cloudflare's ZTNA and SWG services:

The company recognized that supporting its hybrid workforce and digital transformation ambitions would require consolidating security onto a single cloud-based platform.

After deploying Cloudflare's ZTNA and secure web gateway (SWG) services (Cloudflare Access and Cloudflare Gateway, respectively), the company:

- **Secured hybrid work** for more than 100,000 employees with unified controls for both application and Internet access
- **Replaced Cisco Umbrella** with Cloudflare to protect from malware, phishing, and other threats
- **Implemented identity-based, Zero Trust policies** for hundreds of applications across AWS, Azure, and other cloud environments
- **No longer needs to juggle multiple policy-building interfaces** for disparate VPN and Internet filtering services
- **Centralized logging,** which simplifies SOC incident response and any compliance audits

Initiative: Modernize your network

Instead of maintaining legacy corporate networks for as long as possible in today's distributed environment, organizations can tap into distributed and dynamic cloud-native SASE services for network modernization.

Consolidating networking and security services reduces complexity and risk, which — in turn — helps businesses become more agile and competitive.

Use case: Simplify branch connectivity / transition from MPLS or traditional SD-WAN

Connecting branches efficiently is a challenge. Multiprotocol label switching (MPLS) provisioning and adjusting point solutions takes too much time; backhauling traffic through a patchwork of security appliances provides a poor, insecure experience; and there are a number of inefficiencies that multiply too quickly. Meanwhile, traditional SD-WAN implementations may increase risk if they bypass the cloud security for traffic between branches

With a SASE architecture, you can augment or replace a patchwork of MPLS circuits and traditional network appliances to more easily route traffic between branch offices, and to facilitate site-to-site connectivity across locations. Deploy the minimum required hardware within physical locations, and use low-cost Internet connectivity to reach the nearest "service edge" location.

Use case: Reduce / eliminate the DMZ

Organizations use DMZs (demilitarized zone networks) to host public or private applications in a network segment partitioned off of the enterprise firewall, designed to prevent exposure of the rest of the enterprise's network. However, the DMZ as a network construct is diminishing in importance, because there are alternative ways to build and host applications without having exposure.

In addition to taking steps with modern application and network services to shift DMZ security to the cloud, organizations can start reducing or eliminating the need for the DMZ (and VPNs) altogether. By adopting a Zero Trust approach, organizations can provide simple, secure access without allowing inbound traffic. This dramatically reduces the attack surface and improves visibility for who has access to what, without requiring auditing the firewall or network.

Use case: Eliminate elevated trust on the LAN

In the past, it used to make sense to provide users in the office with access to resources in the data center. However, elevated levels of access opens the door to lateral movement, and most organizations are now looking towards how to implement Zero Trust, especially in situations like shared workspaces.

Improve your security by making your local area network (LAN) just as untrusted as the guest network or the coffee shop Wi-Fi, and control access to applications using a granular, identity-centric approach instead.

Use case: Accelerate connectivity for M&A

Traditional IT challenges during an M&A include very manual and lengthy due diligence processes and implementation steps, incompatibility and scalability issues, and the risk of new vulnerabilities (especially if companies' security postures are not identical). ZTNA acts as an aggregation layer for secure access across both companies' existing users and applications, maintaining business continuity during M&A flux.

By enforcing Zero Trust rules on a per-app basis instead of relying on a traditional network-based access model, organizations undergoing M&A may never need to perform a network merge at all. With ZTNA delivered through a SASE platform, you can accelerate secure access for all users to authorized resources from day one.

Case Study: Modernize your network

Network-as-a-service lets shoe retailer DTLR take steps toward Zero Trust

- Founded in 1982
- U.S.-based footwear and streetwear retailer with nearly 250 locations
- Employs more than 3,000 store associates

Challenge:

Boost security at the network edge

Lifestyle retailer DTLR was pushing hard on digital transformation. Store managers sought better data analytics, and the business wanted to enable customers to pick up their online orders from a physical store within two hours.

However, their IT infrastructure struggled to keep pace. For instance, their security framework included IPSec VPNs connecting stores to a centralized location, which "was a complete lack of control from IT's point of view."

DTLR also had unique security challenges (such as safely broadcasting DTLR Radio content to all store locations).

As their director of IT, Nigel Williams-Lucas, noted to Network World, "...We need to have a single view for our team to be able to execute changes that take effect across our retail stores without having to go around to each one. We want to be able to audit things to make sure they're correct. And for cybersecurity, I need to be able to see traffic moving in and out."

DTLR®

Key results

with Cloudflare's Zero Trust and network services:

DTLR needed to move gradually and methodically toward the cloud, while maintaining predictable costs.

The company (which was already using Cloudflare's DNS service), chose Cloudflare's network-as-a-service (NaaS) to start their phased journey toward Zero Trust.

With Cloudflare, DTLR:

- **Deployed applications in a Zero Trust model** using Cloudflare Tunnel, without having to change out firewalls
- **Boosted network performance,** with each store now connecting to the closest Cloudflare point-of-presence (PoP)
- **Gained visibility** into endpoint traffic flows, and shut down legacy endpoints that were no longer in use
- **Improved their overall security posture**: "We now understand what flows through our networks, so we should be able to build out a better, stronger security posture for tomorrow."

Initiative: Protect your attack surface

As businesses innovate, scale, and diversify their digital footprints — from cloud migrations to increased API-driven functionality — they inadvertently create additional entry points and vectors for adversaries to exploit.

A SASE approach protects against the expanding attack surface as organizations embrace distributed / hybrid work, accelerate cloud migration, and invest in digital transformation.

Use case: Prevent multi-channel phishing and business email compromise

Attackers are increasingly casting phishing lures into channels where users are less cautious about where they click. In "multichannel" phishing, attacks may originate beyond email — in SMS/text messaging, IM, social media, cloud collaboration/productivity services, and other tools not typically protected by email security controls. SASE enables comprehensive protections across all these environments from a single platform — mitigating the risk of credential theft, account takeovers, or data exfiltration via advanced phishing tactics.

Use case: Protect remote workers

Remote work has expanded the attack surface, with more dispersed users and unmanaged devices all requiring access to internal resources. Adopting a SASE architecture extends visibility and controls to support the "perimeter-less" model, enabling you to enforce consistent protections against threats both on- or off-network, via one unified platform. Expanding the security perimeter to fit a 'work-from-anywhere' approach also ensures a productive user experience, and helps retain the best talent from any location.

Use case: Protect distributed offices

Traditional approaches for scrubbing office traffic involved backhauling the traffic to centralized corporate data centers, which can add latency and hurt productivity. At the same time, allowing employees direct Internet access leads to inconsistent, inefficient, and ineffective protections that vary from location to location. In contrast, a SASE approach enables consistent, performant security across offices to enable hybrid work, while reducing the overhead of managing site-specific firewalls or other on-premises appliances.

Use case: Secure the WAN

SASE enables organizations to simplify how they connect and secure their offices, data centers and clouds. This means applying filters and inspections for traffic between locations (branches, data centers, etc.) and to/from those locations in/out of the broader Internet by layering on firewall and proxy-based SWG controls to your wide area network (WAN). Some WAN solutions bypass the cloud security for traffic between branches, so integration claims between security services and SD-WAN may not be what they initially seem, depending on the vendor.

Case Study: Protect your attack surface

Werner Enterprises works with Cloudflare to consolidate email, app, and network security solutions

- Founded 1956
- One of the largest truckload carriers in North America
- Uses best-in-class technology to provide customers with optimized freight management services and resources on the road

Challenge:

Stop phishing and BEC attacks, and secure a hybrid on-prem/cloud infrastructure

Due to the size and geographical diversity of its workforce, as well as its widespread use of email for communications, Werner Enterprises had concerns about phishing and business email compromise (BEC) attacks. With increasing email-borne threats, the company's previous email security system was not keeping up.

Additionally, Werner was systematically migrating its legacy on-prem applications to the cloud so its North American resources could work free of the limitations of a traditional VPN.

Maintaining the availability of these core systems during the transition was critical, as was protecting their customers' commercial history and their employees' personally identifiable information (PII).

The company also sought to minimize tool sprawl and reduce the complexity of managing multiple vendor's security solutions.

Key results

with Cloudflare's email security and network security services:

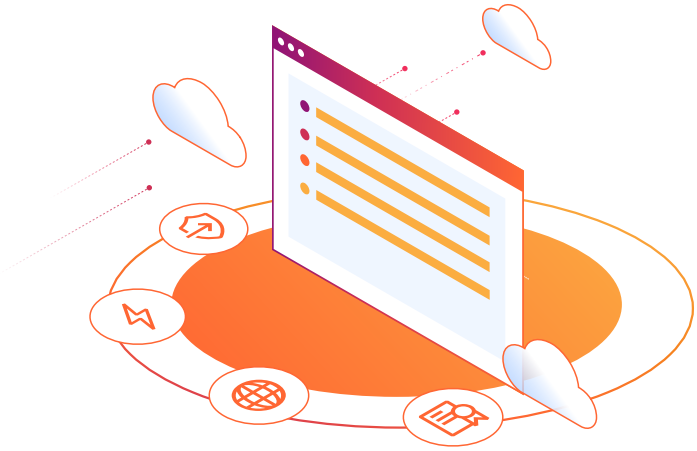
Werner wanted a unified set of tools that would take them into the cloud to mitigate threats, improve performance, and provide their clients and users with the same security they would have if they were actually in the building. With Cloudflare's email security and network security services, the company:

- **Reduced malicious emails** in user inboxes by more than 50%
- **Cut manual email triage efforts** by several hours per day, allowing teams to reinvest their efforts into strategic business goals
- **Migrated core legacy services** to the cloud without critical business or customer service interruptions

By consolidating to a single-vendor, single-interface solution, Werner has reduced its system complexity, facilitated automation, and improved data visibility.

WERNER ENTERPRISES

Initiative: Modernize your applications



Everything can now be done from an app, from ordering breakfast to processing payroll. However, legacy apps (whether consumer-facing or for back-office functions), require modernization in order to be more data-driven or AI-powered.

Apps also need to be secure, resilient, and performant for end users — with the scalability to handle growth in data while still meeting data governance requirements. A SASE architecture can help simplify several stages of the app modernization process for developers and their key collaborators, while keeping them secure.

Use case: Secure application access and cloud migrations

Developers should be able to focus on building out new apps through the lens of the business value they aim to deliver, not worrying about creating custom secure access mechanisms from scratch. ZTNA acts as an access aggregation layer for all of an organization's resources, integrating with all modern identity protocols to simplify secure access for new apps in a consistent manner across the business.

For teams modernizing legacy on-prem apps and migrating them to the cloud, a modernized access solution can also ease the transition and ensure continuity in end user access experiences throughout the cutover by connecting both the on-prem and cloud instances through the same ZTNA solution.

Use case: Protect privileged (developer/IT) access

Developers need privileged access to critical infrastructure, making them an attractive attack target. They need access to many different resource types (SaaS, self-hosted, SSH/VNC/RDP, etc.) but can't feel held back by overly rigid security. A Zero Trust approach helps privileged users stay productive with slick, low-latency user experiences, while maintaining least-privilege access. Session logging can provide further visibility into privileged user sessions, tightening visibility into higher risk workflows.

Use case: Prevent leaks and theft of developer code

Code data is growing rapidly. Developer code fuels digital business, but that same high-value source code can be exposed or targeted for theft across many developer tools. Protect code stored and shared in SaaS data repositories like GitHub or AI tools like GitHub Copilot, and — with SASE — see exposed code and control where it can go.

Use case: Secure DevOps workflows

DevOps teams need easier ways to establish secure, Zero Trust connectivity to accelerate testing. Some SASE solutions extend their reach beyond user-to-app use cases to cover mesh and peer-to-peer secure networking and support service-to-service workflows and bidirectional traffic. Modernizing toward true any-to-any connectivity can help streamline the continuous integration and continuous delivery (CI/CD) pipeline and its associated traffic flows.

Case Study: Modernize your applications

Cloudflare Zero Trust secures work-from-home access for 5,000+ Creditas employees

- Brazil's largest loan fintech platform
- $4.7 billion valuation
- Offers home equity, automobile, and secured loans, and other services across Latin America, Europe, and Mexico

Challenge:

Provide 5,000 employees secure access to internal tools and applications — overnight

When COVID-19 hit Brazil, the Brazilian government instructed Creditas to send everyone home. Creditas had 48 hours to change its entire working model to go from being 100% onsite, to almost entirely remote.

As they prepared to meet this requirement, the engineering team faced multiple challenges, including:

- Maintaining a legacy VPN that demanded complex configuration to run on different operating systems, and could only support a limited subset of employees
- Time-consuming collaborations between Creditas teams and their third-party vendors to modify new VPN tools before they were safe to use
- Upholding security and data protection standards and regulatory compliance

Key results

with Cloudflare's ZTNA services:

Creditas (which had started as a customer of Cloudflare's core application security suite) pivoted to streamline employee connectivity and securing access to internal resources to meet the high-pressure government deadline to secure remote work.

Creditas rapidly deployed Cloudflare's ZTNA service (Cloudflare Access), which enforced identity-based authentication per application across their workforce.

Key results included:

- **Increased DevOps productivity** by reducing time spent on application commissioning and implementation from 2-4 weeks, to two days
- **Streamlined employee connectivity** and secured 45 vulnerable applications and internal resources
- **100% employee growth** with less than 30% increase in engineering support staff

creditas

Initiative: Protect your data anywhere

Data spans more environments than most organizations can keep track of; for example, sensitive data can be exposed through the unsanctioned use of generative AI (GenAI) and shadow IT. These sprawling cloud and SaaS environments create more risks.

Because SASE converges data visibility and controls across web, SaaS, and private app environments into one architecture, it helps simplify the way organizations keep up with regulatory requirements and stay ahead of modern data risks.

Use case: Simplify compliance with data privacy regulations

Data privacy has never been more top of mind; for example, in 2023, legislators issued a record-breaking €1.2 billion fine for GDPR non-compliance. Businesses can continue to expect stricter requirements to protect user data, particularly with the increased use of GenAI, large language models, and other AI tools.

SASE helps organizations in their efforts to keep data safe and private: unifying controls and visibility across environments makes it easier to lock down regulated data classes, maintain detailed audit trails via logs, and improve your security posture to reduce the risk of breaches.

Use case: Manage shadow IT

SASE helps organizations regain control over and mitigate the risks posed by shadow IT. Proxying traffic through the inline cloud access security broker (CASB) logs every connection and request to reveal unsanctioned SaaS apps, and what actions users are taking within them. Administrators can then review these apps, approve / block them, and apply identity- and device-driven policies accordingly.

Use case: Safely use generative AI

SASE services help organizations use generative AI safely and efficiently, with controls and visibility applied from wherever traffic originates (whether from your workforce or automated services), to wherever it is going (e.g., public apps like ChatGPT or private AI apps).

For example, using a SASE platform's secure web gateway (SWG)/inline CASB services, security teams can detect and approve of AI app usage, scan for misconfigurations that risk data leaks via the API-driven CASB, or run AI apps in isolated web browsers to restrict data inputs and output.

Use case: Protect your sensitive data

SASE services enable organizations to detect and control how sensitive data moves into, around, and out of their IT environments. This includes scanning apps and inspecting traffic for sensitive data, which can be regulated (like PII, health, financial info) and high-value (like developer code or intellectual property). Additional SASE protections against data theft or inadvertent leaks include securing access to data with Zero Trust best practices, and blocking Internet threats like phishing and ransomware.

Case Study: Protect your data anywhere

Applied Systems consolidates security across employees, applications, and networks to accelerate digital transformation

- Established 1983
- Builds SaaS solutions for the insurance industry
- Employs more than 2,500 workers across the US, UK, Canada, Western Europe, and India

Challenge:

Accelerate digital transformation

Security is of paramount importance to Applied Systems, which must safeguard large volumes of financial data, payment records, PII, and other regulated and sensitive classes of information for its insurance customers.

With the introduction of a new executive team, Applied Systems sought opportunities to become more agile, more efficient, and more secure. They had components from different vendors, but there were complaints; for instance, their developers complained about Zscaler blocking work-critical websites and hurting productivity.

Applied Systems focused on consolidating large swaths of security and networking functionalities, including:

- Protections and performance enhancements across public-facing websites and apps
- Secure and scalable connectivity across network infrastructure
- Zero Trust security posture for employees and internal resources

Key results

with Cloudflare's application services and Zero Trust portfolio:

Applied Systems wanted a partnership with a vendor who was cloud-native, and understood what clould-native customers expected. To improve technological efficiency and support its business growth and ambitions, Applied Systems deployed a number of Cloudflare's application services, Zero Trust, and network connectivity services.

Key results have included:

- **Secure access** for 2500+ employees across self-hosted apps and infrastructure, replacing Zscaler and Cisco
- **Flexibility** to apply more rigorous or less rigorous controls to meet different user needs
- **Data protected** within emerging AI tools including ChatGPT and Bard

Applied Systems' CISO notes, "When we get asked about regulatory compliance by our customers, we can just tell the CISO on the other side that we are Cloudflare customers and explain the products we are using."

APPLIED

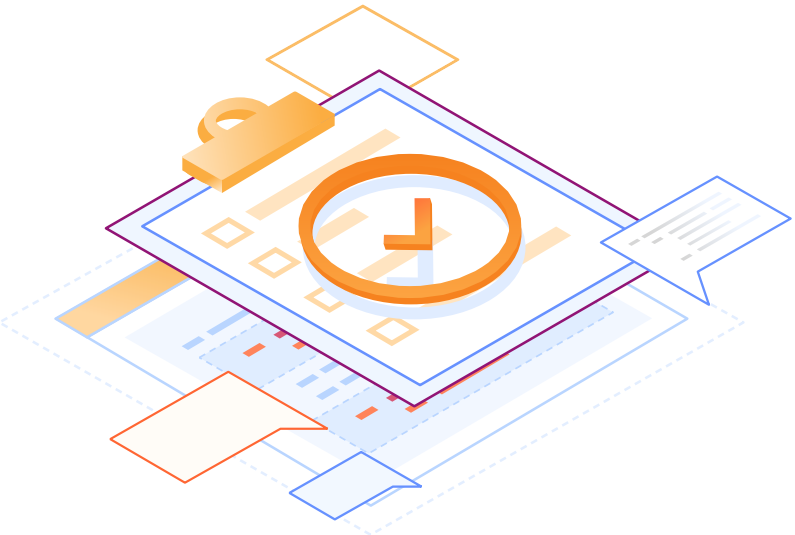
Conducting vendor assessments

After developing a thorough understanding of your organization's needs, **look for a vendor that can meet you wherever you are on the journey to SASE** — and integrate with your existing tools for network on-ramps, identity management, endpoint security, log storage, and other pieces of the network security equation.

Many vendors champion an all-in-one platform, but in actuality, require organizations to integrate several different point products.

Persona-based conversation starters

While traditional vendor "side-by-side" comparisons are still valuable, too often they steer toward feature checklists, which are tough to objectively conduct in a market that itself is moving so quickly. New widgets could appear tomorrow in any given vendor's solution, but deep underlying architectural strengths (or flaws) will stick around much longer.



Some SASE providers also started with one or two core services more than a decade ago and have since rushed to bolt on acquisitions to appear to complete their SASE portfolios. Those vendors' points of view or asserted checklists may inherently bias toward their longer standing strengths. If you first dig into internal priorities to determine what capabilities you need most for your desired SASE use cases, you will feel more prepared to navigate the vendor landscape. Write down what you will actually "do" with each vendor's top claimed differentiators; after all, the most advanced widget in the world means nothing if it ends up merely sitting on the shelf.

Consider the following comparative topics to discuss with vendors, based on your key stakeholders. SASE vendor features are rapidly iterating (and may even vary significantly month to month), so finding deeper criteria and discussion points will help you select the best long-term partner as you navigate this crowded market of similar claims.

Office of the CIO

Note that many of these questions are directly applicable to other teams as well.

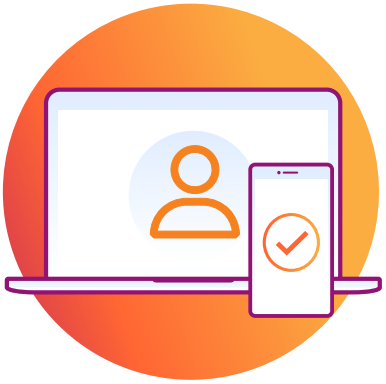
Key Priorities

- Improving team productivity
- Improving user experiences
- Accelerating digital modernization
- Reducing total cost of ownership

Questions to ask the vendor

Team Productivity

- Is there one centralized user interface across every SASE function (i.e. you log in once) or many?
- Is there one centralized API across every SASE function (i.e. one API key) or many?
- Are the security (e.g. ZTNA, SWG, CASB) and networking (e.g. WANaaS, SD-WAN, FWaaS) functions natively integrated by default or do they require manual steps by you, or by us?
- Do we integrate our identity provider (e.g. Microsoft, Okta, Ping) to the SASE platform one time or many to enable identity-based access policies to every application (web, SaaS, and private)?
- Can your user device agent connect composably to any other network on-ramp (e.g. WAN connectors, app connectors, and mesh/P2P connectivity with other device agents)?
- Can our security and DevOps teams achieve bidirectional any-to-any connectivity between users, applications, and/or service workflows without asking my networking team to deploy appliances or change network routing?
- To what extent do you offer automation (beyond having an API)? How complete is your Infrastructure as Code (e.g., Terraform) provider?
- How quickly can I start a free trial of your complete platform with all security and networking services and on-ramps available? Can I get up and running today?



User Experiences

- Is every data center location on your global network map available to every customer, or are some exclusive to your telecommunication partners' customers?
- Is every SASE function delivered from every data center location on your global network map or do some functions (e.g., RBI) only run in limited locations?
- Can every SASE network on-ramp (i.e., device agent, WAN connector, app connector) connect to every data center location on your global network map without paying extra fees or bandwidth surcharges?
- How many interconnects exist between your POPs and other networks to minimize intermediary transit provider hops and latency?

Digital Modernization

- Is each connectivity method and SASE service interoperable with each other in every location? Where can I read more about the underlying architecture?
- What certifications does your platform have? (ISO27701, SOC2, FedRAMP, etc.)
- Is it interoperable with any existing cloud or on-prem system? Is the L2-7 connectivity fully API-programmable?
- What happens to our SASE services/costs if we switch between clouds?
- How will you serve where my organization is trying to go 5, 10 years from now?
- How can your current ecosystem (including technology partners) support my existing investments?

Total Cost of Ownership

- How is your Zero Trust offering priced? Will I be charged for app connectors deployed or bandwidth used?
- Do any data center locations run from public cloud providers (Azure, AWS, GCP, Oracle)?
- Do you have any caps on usage of traffic in any tier of your offering?
- Are there any hardware or virtual appliances to activate, manage, or scale per location?
- Do any network security functions used to protect branch offices run on-prem, or are all cloud-native?
- What are your egress fees for moving my data between clouds?

Heads of Networking

Note that many of the Office of the CIO questions are directly applicable to the networking team as well.

Key Priorities

- Network modernization to meet future requirements
- Increasing business agility
- Resiliency and maintaining 100% uptime

Questions to ask the vendor

Network Modernization

- Does the SASE network cover all traffic flows (inbound, outbound, WAN, public cloud networking) or some? And is the backend architecture the same or different across traffic flows?
- Within how many distinct cities and countries do you maintain your own data center infrastructure? Are there any shown on your global network map that by default my traffic cannot be routed to?
- What are all the different options for connecting my network to yours? Is every connect option available at every data center location on your global network map without paying extra fees or bandwidth surcharges?
- Can you instantly provision every SASE service in every data center location if we need more capacity or lower latency?

Business Agility

- What advanced networking functionality do you provide (e.g., private backbone transport, caching, protocol and application optimizations, advanced routing, SaaS optimization, private backbone, application optimization/accelerations)?
- What network monitoring, visibility, and observability features do you provide?
- How do you handle traffic steering, shaping, and failover to make sure our packets always take the best available path?

Performance and Resiliency

- What is your SLA? Do you offer uptime and/or end-user latency guarantees when any SASE service (e.g. decrypted traffic inspected by all threat and data protection functions) is actively in use?
- Are latency guarantees measuring time from the traffic source to the SASE network, for traffic to pass through the SASE network, or for the full round trip (traffic source to destination)?
- Do you use Unicast or Anycast for network routing? If Anycast, do you maintain your own network hardware? How do you ensure traffic does not 'flap' between multiple locations?
- How do you ensure network resiliency if one or many entire data centers are taken offline due to either unplanned outage (e.g. power cut, DDoS attack) or planned maintenance? Are secondary/fallback traffic routes managed by you or us?
- How will you ensure business continuity if there are outages elsewhere on the public Internet between our network locations and your data center locations?

Office of the CISO

Note that many of the Office of the CIO questions are directly applicable to the security team as well.

Key Priorities

- Reducing cyber risk and attack surface
- Improving security posture
- Supporting efficiency and reducing response times

Questions to ask the vendor

Cyber Risk / Attack Surface Reduction

- Is all application (web, SaaS, private) traffic decrypted and inspected by your threat and sensitive data detection engines (e.g., AV, DLP) in a single pass without any deployment caveats?
- Are all data flows and communications through SaaS suites (e.g. Microsoft 365, Google Workspace) protected across every channel — inline web activity, inline email activity, and out-of-band web or email activity?
- Can RBI be enabled for every user and every browser-based application (web, SaaS, private) without impacting user productivity or incurring additional fees?

Consistent Security Posture

- Are any security functions bypassed based on the network on-ramp used?
- How do you ensure customer traffic is isolated and private across your multi-tenant cloud architecture?
- How do you provide data localization capabilities? Will enabling these capabilities add latency for remote users that connect outside the localized region?

Efficiency and Response Times

- Do we integrate our data lakes and analytics (i.e., SIEM, XDR, cloud storage buckets) to your SASE platform one time or many to enable access log visibility to every application (web, SaaS, and private)?
- How can we integrate our threat intelligence feeds into your SASE architecture?
- What kind of analytics into dynamic device and user risk scoring are provided by you or via technology partnership integrations?
  Can these scores be uniformly enforced when users access any application (web, SaaS, and private)?
- How do you reduce false positives from your threat intelligence feeds?

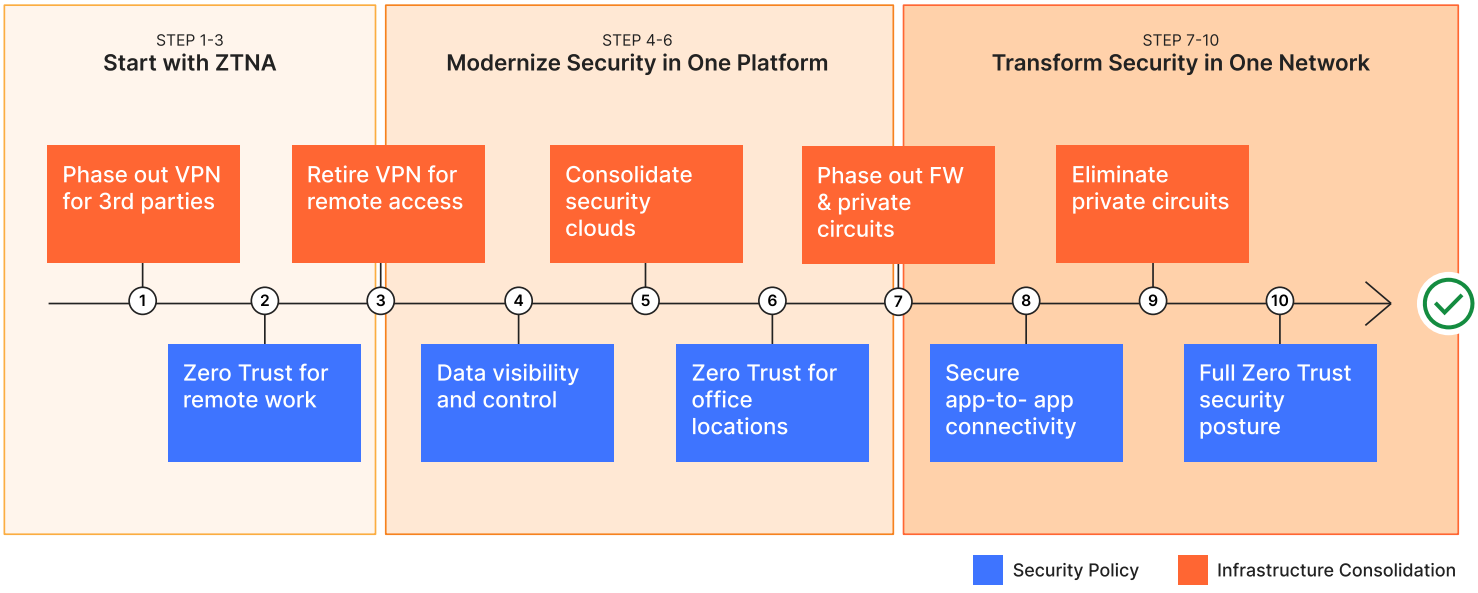
The case for single-vendor SASE consolidation

Most large enterprises can expect to move towards a SASE architecture progressively rather than all at once. In that process, they may choose to use SASE services from multiple vendors (especially since many vendors that market a full SASE solution have actually stitched together separate products, leading to a non-converged experience similar to what you would see managing multiple separate vendors anyway).

However, deploying and managing all the components of SASE with a single vendor — versus piecing together different solutions for networking and security — significantly simplifies deployment and management by reducing complexity, bypassed security, and potential integration or connectivity challenges.

Consolidating on a single-vendor SASE platform enables organizations to fulfill the true promise of SASE: **a simplified, efficient, and highly secure network and security infrastructure that reduces your total cost of ownership and adapts to the evolving demands of the modern digital landscape.**

While there is no perfect order of operations and every organization should assess their unique priorities, a long-term roadmap for a single-vendor SASE architecture may follow a similar flow to the below example

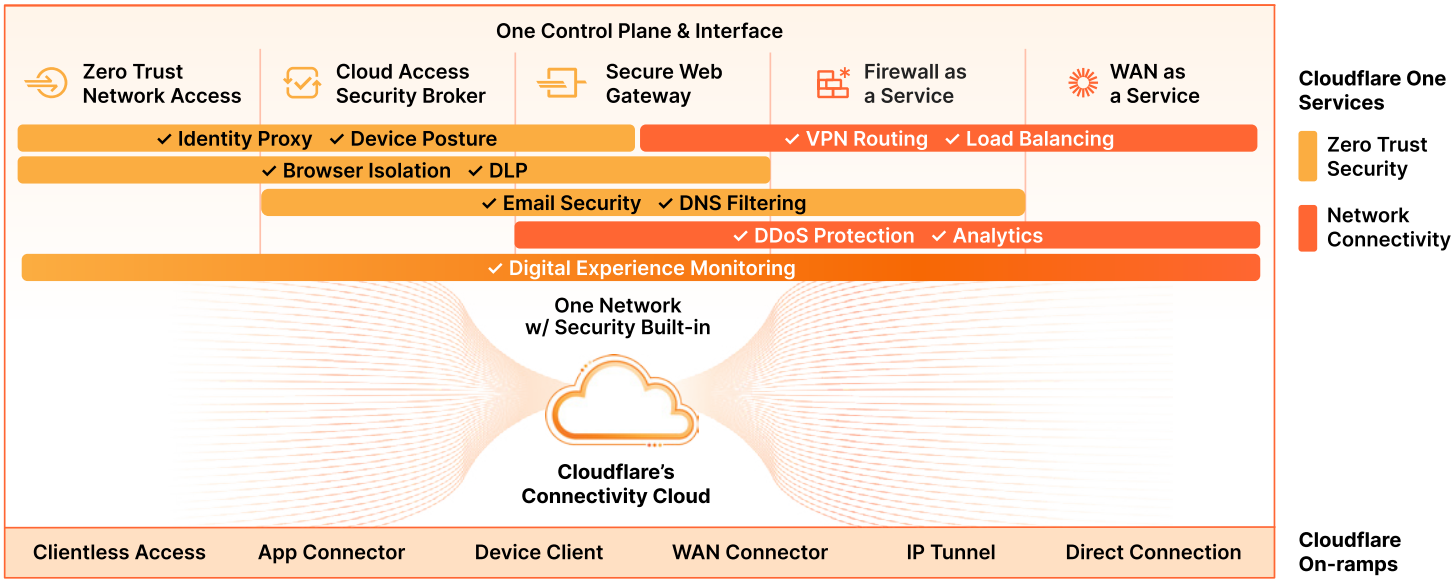


Why Cloudflare One?

Cloudflare's single-vendor SASE platform, Cloudflare One, is built in our connectivity cloud — the next evolution of the public cloud, providing a unified, intelligent platform of programmable, composable services that enable any-to-any connectivity between all networks (enterprise and Internet), clouds, apps, and users.

Other SASE vendors separately architect North-South Internet gateways in the cloud from East-West traffic overlays via on-premises devices, leaving organizations minimal control over East-West traffic paths without an MPLS circuit backup to ensure resilient performance. Cloudflare's middle mile global backbone converges both North-South Internet gateways and East-West private traffic transport natively to ensure enterprise-grade resiliency and performance-all over low-cost Internet connectivity.

Some SASE vendors also build on public (captivity) clouds and pass on a hefty toll to customers; they were designed to be a final destination of data, whereas Cloudflare is designed to transport data to any destination without sacrificing enterprise agility, resiliency, or control. We built our global network and world-class application security such that the proxy, firewall, decryption, traffic scanning, data processing, management and more were reusable for future services. **We used that foundation to become the only SASE provider to start with ZTNA such that identity and context-based connectivity was consistently built-in across our entire platform.**



Cloudflare helps organizations achieve true network modernization to simplify SASE implementation, regardless of the team leading the initiative. Our platform makes SASE networking more flexible and accessible for security teams, more efficient for traditional networking teams, and uniquely extends its reach to an underserved technical team in the larger SASE connectivity conversation: DevOps. Our connectivity cloud provides best-of-breed flexibility to make any-to-any connectivity a more approachable reality for organizations implementing a SASE architecture, accommodating deployment preferences alongside prescriptive guidance.

Today, our consolidated security platform and connective tissue positions Cloudflare alongside other hyperscalers vs. other SASE point players. For instance, Cloudflare's connectivity cloud offers other services that improve application performance and security, such as an API gateway, WAF, content delivery network (CDN), and DDoS mitigation — all of which can complement an organization's SASE architecture.

Cloudflare offers the breadth and depth needed to help organizations regain IT control through single-vendor SASE and beyond, all using the same Cloudflare proxies that route ~20% of all websites. As digital initiatives and security risks keep evolving faster, our network is the most agile to keep organizations connected and protected for the long term.

FORRESTER®

Cloudflare named a Strong Performer in "The Forrester Wave™: Zero Trust Platforms, Q3 2023

Read the report >

IDC

Cloudflare named a "Leader" in 2023 IDC MarketScape for Zero Trust Network Access (ZTNA)

Read the report >

kuppingercole ANALYSTS

Cloudflare named a "Leader" in 2023 KuppingerCole Leadership Compass for SASE

Read the report >

Learn More

Cloudflare One simplifies your journey to adopt Zero Trust, modernize networks, protect your attack surface, modernize apps, and protect data anywhere, no matter where you start.

To learn more, read our reference architecture, "Evolving to a SASE architecture with Cloudflare," or talk to a Cloudflare One expert.

Appendix A: SASE Primer

According to Gartner®, Inc., "over the next five years, the market for secure access service edge (SASE) will grow at a compound annual growth rate of 29%, reaching over $25 billion by 2027[2]." **Why the demand?**

Today's IT and security leaders are expected to help achieve rapid digital modernization priorities to fulfill the imperative to connect, protect, and build everything everywhere, with network security and infrastructure that can support:

- **Distributed, dynamic cloud services** for more protection, more compute, and more capacity
- **Secure hybrid work** and connecting users, apps, and data everywhere — in a compliant way
- **Cyber risk reduction** through Zero Trust security without compromising fast, reliable connectivity
- **Lower total cost of ownership**, with a reduction in CapEx/OpEx costs and consolidation of point solutions
- **Agility and flexibility** to swiftly adapt to new technology, functionality, and scalability requirements

However, traditional physical and virtualized networking systems — which are based on the "castle and moat" approach — are impractical for effectively addressing all of these needs. While they may have made sense in their time, today they are too costly to build, complex to maintain, and not optimized for cloud or remote work.

In other words: networks are long overdue for modernization with SASE.

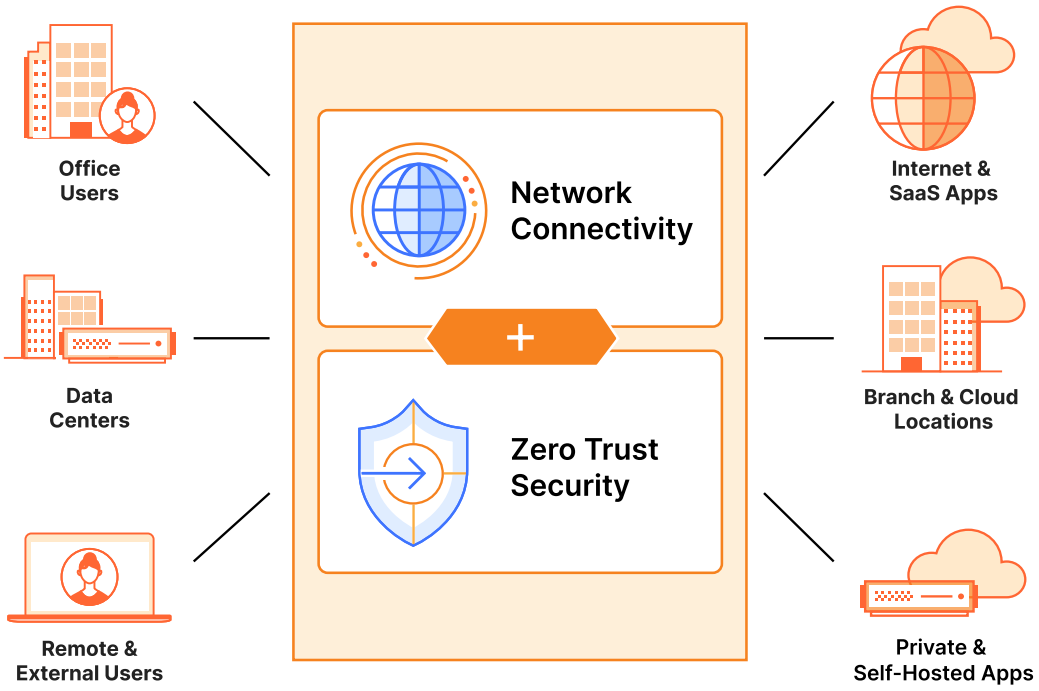
Although the full "before and after" scope of IT environment changes can feel overwhelming, most organizations are embarking on a several-year SASE roadmap to keep their implementation realistic, with incremental adoption of additional use cases over time. Legacy appliances can be fractionally augmented by a SASE platform in stages well before full replacement is achieved, bringing new value to the business along the way. IT modernization here is inevitable, as is bringing together cross-functional stakeholders to collaborate internally to achieve SASE success.

What is SASE?

In traditional enterprise networking (unlike SASE), data and applications live in a core data center. To access those resources, users, branch offices, and applications connect to the data center from within a localized private network or a secondary network (which typically connects to the primary one through a secure leased line or VPN).

However, that perimeter-based model is ill-equipped to handle the rise of remote/hybrid work, SaaS and cloud migrations, and multi-vector, multi-channel cyber threats.

Unlike past networking approaches, a SASE (pronounced "sassy") architecture unifies security and networking onto one cloud platform, for consistent visibility and control. SASE places network controls on the cloud edge — not the corporate data center. **This allows enterprises to provide simple, secure access to any user, app, device, or network, regardless of location.**



More specifically, SASE platforms converge network connectivity with a number of Zero Trust security functions managed from one interface, delivered from one control plane. By merging those services into a unified, composable architecture, SASE simplifies networking and network security infrastructure in a way that enables businesses to stay agile as their priorities shift over time.

The following explains core SASE services and components in more detail. **However, before diving deep into the individual SASE architectural components and capabilities, first clarify the most significant challenges you are looking to solve.**

Making the business case for SASE

Because SASE architecture involves converging a number of traditionally disparate services, embarking on your SASE journey can initially seem overwhelming. Before the technical aspects can even begin, you should first align business, IT, security, and networking stakeholders on all the business outcomes other organizations are achieving through SASE, while prioritizing which are most important to your specific goals.

Before kicking off the lengthy RFP process and shortlisting vendors, prepare your business and IT case for SASE transformation — and decide which changes need to be made sooner vs. later.

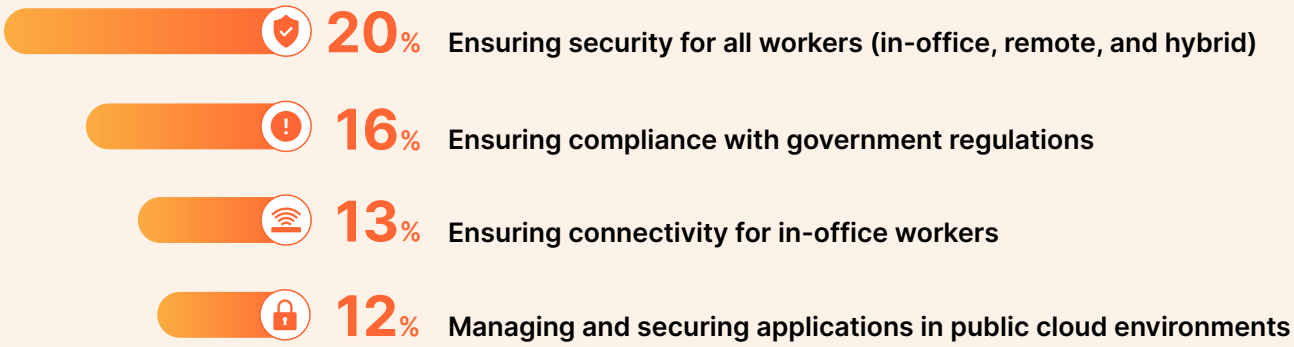
Define business and IT drivers

What would security and network modernization help your organization accomplish?

The responsibilities of global IT and security decision makers have significantly increased over the last three years, according to a global Forrester Consulting survey commissioned by Cloudflare. If you are considering SASE today, chances are your organization is facing similar challenges:

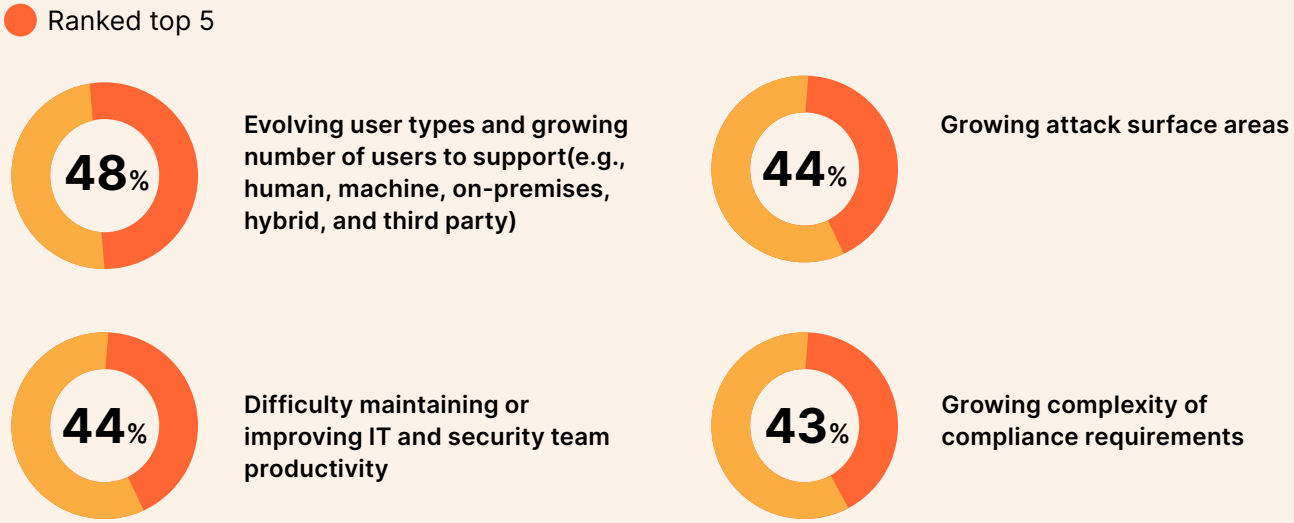
IT And Security Team Responsibilities Increases Over The Last Five Years

(Showing "We were not responsible for this five years ago")



Base: 449 global decision-makers at the director level or higher influence or direct organizations choice of enterprise solutions
Note: Showing four responses
Source: A commissioned study conducted by Forrester Consulting on behalf of Cloudflare, August 2023

"What are the top challenges your organization's IT and security teams are currently facing?"



Base: 449 global decision-makers at the director level or higher influence or direct organizations choice of enterprise solutions
Note: Showing top 4 responses
Source: A commissioned study conducted by Forrester Consulting on behalf of Cloudflare, August 2023

If you are being asked to explain the business and IT case for SASE, start by considering the answers to these questions:

- *Does your current architecture enable vs. hinder your ability to efficiently connect and protect all users, devices, applications, and data?*
- *What will it cost to maintain/upgrade your current systems (which are typically from a sprawl of disparate vendors and complex to maintain) over the next 12 months? What about the next 3-5 years? The next 10?*
- *What IT budget and resources do you need vs. have to meet the organization's expanding digital demands? Have executive expectations changed when it comes to technology investment ROI?*
- *Have there been significant impacts to the customer experience, employee productivity, or ability to innovate due to past network downtime and other network vulnerabilities?*
- *Has your organization been the recent victim of a preventable supply chain breach and/or data losses due to a security or networking vendor's vulnerability?*

Before building out a roadmap to adopt a SASE architecture, enterprises often start with their big picture needs, like improving business agility, lowering IT/security complexity, reducing cyber risks, and increasing overall tech efficiency — all of which, combined, improve total cost of ownership.

The chart below can help you assess which of your highest-priority challenges can be addressed by consolidating networking and security into a SASE architecture.

List and rank: What are your biggest challenges?	
CHALLENGE: Accelerate business agility	
This is a **core business driver** if your modernization goals are to…	→ Simplify and accelerate secure connectivity for any user, on any device, anywhere → Increase network reliability and reduce latency for users on any device, wherever they are → Reduce or eliminate downtime and service disruptions when adding network capacity/functionality → Reduce the time spent on IT administration and troubleshooting
However, you need a new solution because **your current infrastructure…**	⊘ **Does not scale with your business.** In the past, organizations only needed networking to support desk workers, but now applications touch every job function. Therefore, if your architecture is based on the "castle-and-moat" approach, more connectivity requirements mean adding more data center equipment, everywhere you operate. But, provisioning more firewalls, routers, load balancers, and other equipment as your workforce grows introduces new risks, downtime, and potential service disruptions. ⊘ **Creates poor user experiences.** Organizations historically deploy VPN appliances to connect users to the company network where the applications are hosted. However, with the need for remote access, many applications now live in cloud infrastructure-as-a-service (IaaS) platforms, where traditional VPN solutions are hard to configure. This often results in poor application and connectivity performance for end users. ⊘ **Is inefficient.** Traditional networking concentrates egress through a perimeter / data center firewall. For instance, whether branch traffic is destined to a data center or to the cloud/ Internet, it's routed through headquarters. This is especially inefficient for reaching the Internet, as it requires backhauling the traffic to reach security services for egress.

	⊘ **Is inflexible.** Managing multiple cloud providers can create dependencies on each individual provider's approach to security. Juggling configurations and requirements that are specific to each provider can become exceedingly complex and lead to security gaps.
CHALLENGE: Lower complexity	
This is a **core business driver** if your modernization goals are to…	→ Sunset legacy data platforms, consolidate vendors, and optimize cloud spending → Reduce hardware and the operational (including bandwidth) costs of maintaining network security appliances → Free up IT and security resources for more long-term strategic projects and new technologies
However, you need a new solution because **your current infrastructure…**	⊘ **Keeps driving up costs.** Enterprise networks are massive cost centers for many reasons. The network has to be overprovisioned to support projected capacity; equipment (e.g., VPNs, hardware firewalls, and MPLS connections) must be purchased in pairs for failover and also refreshed every few years; more users and devices need more connectivity; more apps means more bandwidth costs; and on, and on, and on. ⊘ **Is inherently complex.** For example, you may have network layer connectivity between two local servers (enforcing security through firewalls), a number of users that connect over NAC WiFi or VPN (each with their own access policies) and a multitude of users coming from managed devices, unmanaged devices, corporate-managed browsers, bring-your-own-device (BYOD) apps, and so forth. Complexity compounds as more technology is added — in turn, your network design is more brittle and resistant to change. ⊘ **Poses complex, reactive, non-scalable processes.** Your IT/security teams spend too much time managing siloed deployments, multiple dashboards, complex user interfaces, and redundant capabilities.

CHALLENGE: Reduce cyber risk and protect growing attack surfaces	
This is a **core business driver** if your modernization goals are to...	→ Reduce the likelihood of data breaches, multi-channel phishing, ransomware, business email compromise, API abuse, and DDoS attacks → Ensure that your organization can use generative AI safely, without putting intellectual property and customer data at risk → Monitor and protect regulated data (e.g., financial data, health data, PII, exact data matches) → Reduce the overall time spent on incident response
However, you need a new solution because **your current infrastructure...**	⊘ **Lacks a Zero Trust approach.** Perimeter-based network design principles focused on trusting internal users and applications, and blocking external threats. But it was not designed for connecting and protecting anywhere users (internal or external), anywhere applications (on-prem, data centers, or clouds), and anywhere threats. In other words: your current systems lack granular, consistent security policies to cover all users, devices, and environments. ⊘ **Lacks full visibility and enforcement.** Due to the indeterminate number of ways that users and applications are connected, there are inconsistent security and networking controls affecting your ability to understand what is at risk. ⊘ **Is increasingly vulnerable.** Legacy infrastructure (such as data centers and WANs) and legacy security point solutions (such as firewalls and VPNs) are, themselves, points of entry for lateral movement. Surging remote work is placing a strain on your VPNs — and vulnerable VPNs can let cyber attackers move virtually anywhere within your network. ⊘ **Lacks built-in privacy and data protection**. As you continue to migrate more apps and data to the cloud, some of your legacy vendors struggle to comply with constantly-changing data privacy and data protection requirements.

Appendix B: Defining SASE's scope

SASE has emerged as the aspirational architecture to address the IT and business challenges highlighted above.

In a true SASE approach, network connectivity and security services are converged on a single cloud platform and delivered from one control plane to reduce complexity.

As such, your shortlist of vendors should provide a programmable, composable network architecture that delivers all your needed services with minimal latency:

- ☑ **Network services** that forward layer 2-7 traffic from a variety of networks into a single global corporate network. These services provide capabilities like firewalling, routing, and load balancing.
- ☑ **Security services** that inspect traffic flowing over the network, allowing for firewall-proxy-based filtering of layer 3 (IP); layer 4 (TCP, UDP, ICMP); and layer 7 (DNS, HTTP, SSH) traffic with default-deny controls to segment who can access what.
- ☑ **Operational services** that provide platform-wide capabilities like logging, API access, and comprehensive Infrastructure-as-Code support through providers like Terraform.
- ☑ **Integration across all services** that allow admins to define policies once and reuse them contextually across all connected services.

Core components of a SASE architecture

Zero Trust Network Access (ZTNA)

What is it?

The Zero Trust security model assumes threats are present both inside and outside a network; therefore, strict contextual verification is required every time a person, app, or device tries to access resources on a corporate network.

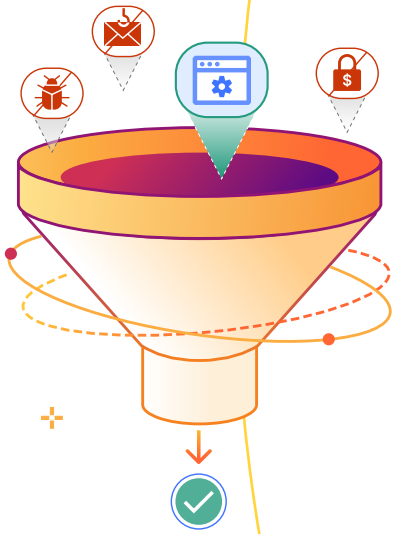
In contrast to traditional remote access tools like VPNs that overprovision network access, Zero Trust Network Access (ZTNA) — which is a primary technology that makes the Zero Trust approach possible — sets up one-to-one connections between users and the resources they need, and requires periodic re-verification and recreation of those connections.

Considerations:

- Verify that the type of ZTNA solution the SASE vendor offers can fit your short- and long-term architectural needs. For example:
- **Client-based ZTNA** requires the installation of a software application called a "client" or "agent" on all endpoint devices. If an organization is concerned about private network access, a growing mix of managed and unmanaged devices, or device posture, client-based ZTNA may be an effective option.
- **Clientless ZTNA** enforces Zero Trust access policies without the need for endpoint software. If an organization is primarily focused on locking down certain web-based apps or enforcing simple, secure access for contractors or unmanaged devices, then the clientless model can be rolled out swiftly.

Other important ZTNA considerations include:

- **Level of effort**: App connector workflows may vary widely depending on vendor architectures, e.g., virtual machines vs. lightweight daemons installed on customer infrastructure, and their associated throughput limitations, if any.
- **Support for legacy applications**: Some organizations still have on-prem legacy applications that are critical for the business. Most ZTNA solutions support cloud and web apps easily, but implementation details may vary for the long-tail of resources businesses need to support, like those within private networks or involving bidirectional traffic.
- **Identity provider (IdP) integration:** any organizations have an IdP already in place. Some ZTNA solutions are more flexible than others regarding supporting multiple IdPs simultaneously, or even multiple instances of the same IdP, which can be particularly helpful for organizations susceptible to mergers and acquisitions (M&A) or divestitures.



Secure Web Gateway (SWG)

What is it?

A secure web gateway (SWG) prevents cyber threats by filtering unwanted web traffic content and blocking risky or unauthorized user behavior online. SWGs can be deployed anywhere, making them ideal for securing hybrid work.

Like many security products, a SWG is a point product that is often managed separately from other networking and network security functions. With a SASE framework in place, however, companies can consolidate and maintain their networks and network security from a single cloud-based vendor.

Considerations:

A SWG needs to be fast because it inspects an organization's Internet-bound traffic. If a SWG is slow, then any traffic from users out to the Internet will be slow; if traffic out to the Internet is slow, users may see web pages load slowly, video calls with jitter or loss, or be generally unable to do their jobs.

In order to reduce latency and ensure a good user experience:

- **Get as close to end users as possible**: The SWG service in your selected SASE platform should shorten the time requests spend on the public Internet.
- **Network interconnect partnerships**: If your SASE provider has strong peering relationships with many ISPs or hosting providers worldwide, those providers will send traffic directly to the network, instead of a third party. This skips congested paths between transit providers, and lets users quickly get to the services they need.

Additionally, a SWG protects data by working in conjunction with inline cloud access security broker (CASB) controls — which are covered in the next section — to control the movement of data.

Cloud Access Security Broker (CASB)

What is it?

Using the cloud and SaaS apps makes it harder to ensure that data stays private and secure. Teams may be using certain SaaS apps without the IT/security teams' permission (e.g., shadow IT), which can lead to potential data loss and data leakage.

To protect data in the cloud, organizations typically use security services that are cloud-based as well. CASBs ideally intertwine with data loss prevention (DLP) capabilities to more effectively protect SaaS apps, but many organizations are holding on to legacy on-prem DLP appliances that simply weren't designed to protect the cloud. This adds to the "point solution" problem and creates challenges: several contracts have to be negotiated separately, security policies have to be configured numerous times, and implementing and managing multiple platforms increases IT complexity.

A modernized cloud access security broker (CASB), which includes SaaS security posture management (SSPM) as a native capability rather than as a bolted-on product, is one solution to these challenges: CASBs provide data security controls over (and visibility into) an organization's cloud-hosted services and applications.

Considerations:

- **Scalability**: CASBs have to manage a lot of data and multiple cloud platforms and applications. Your SASE vendor's CASB capabilities should be able to scale up as your organization grows.
- **Ease of integration**: Ensure that the CASB will integrate with your top applications (e.g., Google Workspace, Microsoft 365, Salesforce) with quick, API-driven integrations. Without robust integrations for your top priority apps, the CASB will not have enough visibility into unauthorized IT and potential security threats.
- **Data privacy**: Will the CASB service keep data private, or is it just one more external party touching sensitive data? If the CASB solution moves their customers' data to the cloud, how secure and private is it? These are especially important questions for organizations that operate under strict data privacy regulations.
- **Mitigation**: Not all CASBs offer the ability to stop security threats once they are identified. Some SASE solutions go beyond detection with "find and fix" workflows to help admins more effectively take remediation action against security findings.
- **Integrated DLP**: A CASB service that integrates with data loss prevention (DLP) more easily extends visibility and unifies data protection across all apps, users, and services.

Remote Browser Isolation (RBI)

What is it?

RBI applies the Zero Trust principle to web browsing by assuming no website code (e.g. HTML, CSS, JavaScript) should be trusted to run by default. RBI loads webpages and executes any associated code in the cloud — away from users' local devices. This separation helps prevent malware downloads, minimizes the risk of zero-day browser vulnerabilities, and defends against other browser-borne threats.

Broad data protection controls can also prevent risky user actions within the isolated browser like restricting download, upload, copy-paste, keyboard input, and printing functionalities. Some organizations use a clientless deployment of RBI to help protect data from unmanaged devices.

Considerations:

- **Compatibility**: First-generation technologies like Document Object Model (DOM) manipulation and pixel-pushing disrupted user interactivity with modern SaaS and HTML5-based apps. SKIA-based network vector rendering (NVR) pushes HTML5 draw commands instead of pixels to work seamlessly with any user interaction with any app in any browser.
- **Scalability**: NVR technology alone is not enough to be transparent for everyday browsing by all end users if the remote browser runs too far away from local devices. The RBI service must be delivered across a global network with data centers located within milliseconds of all Internet users. And every server in every data center location must be architected with significant compute resources to truly scale the RBI service everywhere.
- **Deployment**: Due to hybrid work and so much of the workforce now composed of contractors, both client-based and clientless deployment options are required to cover any user. Clientless options should support both office users already on-ramped to the SASE network (e.g. via a WAN connector) as well as remote users on unmanaged devices.
- **Composability**: All SWG, ZTNA and DLP functions should be available within the remote browser for both client-based and clientless deployments with the same policy controls and visibility. Native integration with clientless ZTNA protects data in use within SaaS apps for contractors and unmanaged devices. And native integration with cloud email security enables isolating suspicious email links for multi-channel phishing protection.

Software-defined WAN (SD-WAN) or WANaaS

What is it?

In a SASE architecture, organizations can adopt either software-defined networking (SD-WAN) or WANaaS, also sometimes referred to as network-as-a-service (NaaS), to connect and scale operations (e.g., offices, retail stores, data centers) across large distances.

- **SD-WAN**: Large organizations often use a wide area network (WAN) to connect their various branch offices and locations (local area networks, or LANs) to the central corporate network. A software-defined WAN (SD-WAN) is a more flexible WAN architecture that connects LANs using controlling software for routing, which works with a variety of networking hardware platforms and connectivity options.
- **WANaaS** is a cloud service model in which customers use networking services from cloud providers. It follows a "light branch, heavy cloud" approach to primarily run networking functions using software, essentially allowing companies to modernize their networks without large changes to their own networking infrastructure — all they need is Internet connectivity. WANaaS can replace VPNs, multiprotocol label switching (MPLS) connections, or other legacy network configurations. It can also replace legacy on-prem networking hardware such as firewall appliances and load balancers.

Considerations:

- Some SD-WAN implementations may increase risk if they bypass the cloud security for traffic between branches. Therefore, a SASE solution that offers native network connectivity and Zero Trust security is typically more desirable for organizations that want to minimize performance and security tradeoffs.
- With WANaaS, networking services are purchased from a cloud provider, as opposed to an organization solely configuring their own network. For WANaaS, your organization would only need Internet connectivity to configure and use the internal network. Depending on how the service is configured, this may offer greater flexibility and more cost savings compared to SD-WANs, just as other cloud service models like SaaS and IaaS do compared to traditional on-premises computing.

Enterprise network firewall or FWaaS

What is it?

Enterprises use firewalls to protect their network, control traffic flows, and enforce policies for interacting with the Internet. The use of the firewall and the services it provides have evolved over time, with a variety of functions and form factors.

- **Enterprise network firewalls:** Most organizations use an enterprise firewall appliance at their network edge, which is used to insulate the organization's internal network from the Internet. Organizations may also use a combination of hardware and virtualized firewalls to isolate traffic to its internal private cloud.
- **Firewall as a Service (FWaaS)**: Enterprise network firewalls are geographically constrained, because they are only located in a limited number of locations. This creates problems with supporting hybrid workforces and cloud applications. To support such use cases, a FWaaS delivers enforcement of firewall policies without having to manage and deploy an appliance. This helps organizations address scaling and architecture challenges by consuming firewall services from the cloud rather than managing firewall appliances.

Considerations:

- Instead of making a hardware firewall perform functions it was never designed to do, consider what functions are best delivered from a cloud service.
- As a baseline, organizations may use FWaaS to deliver defense in depth, thus providing upstream protection from traffic that hits the organization's network.
- FWaaS complements a secure web gateway, helping organizations improve security by funneling traffic through web & cloud inspections and blocking the use of evasion techniques.
- Consider using FWaaS when adopting a "light edge" (i.e. minimal hardware and minimal management) philosophy for connecting and securing remote sites such as stores and branch offices.

Additional components in platforms built on a connectivity cloud

SASE incorporates a user's secure access as part of the network architecture. *(It is worth noting here that industry analyst firm Forrester categorizes the SASE model as "Zero Trust Edge," or ZTE)*. However, not all organizations have a cohesive approach across IT, network security, and networking teams. Therefore, they may prioritize security service edge (SSE) — a subset of SASE functionality primarily focused on securing access to the web, cloud services, and private applications.

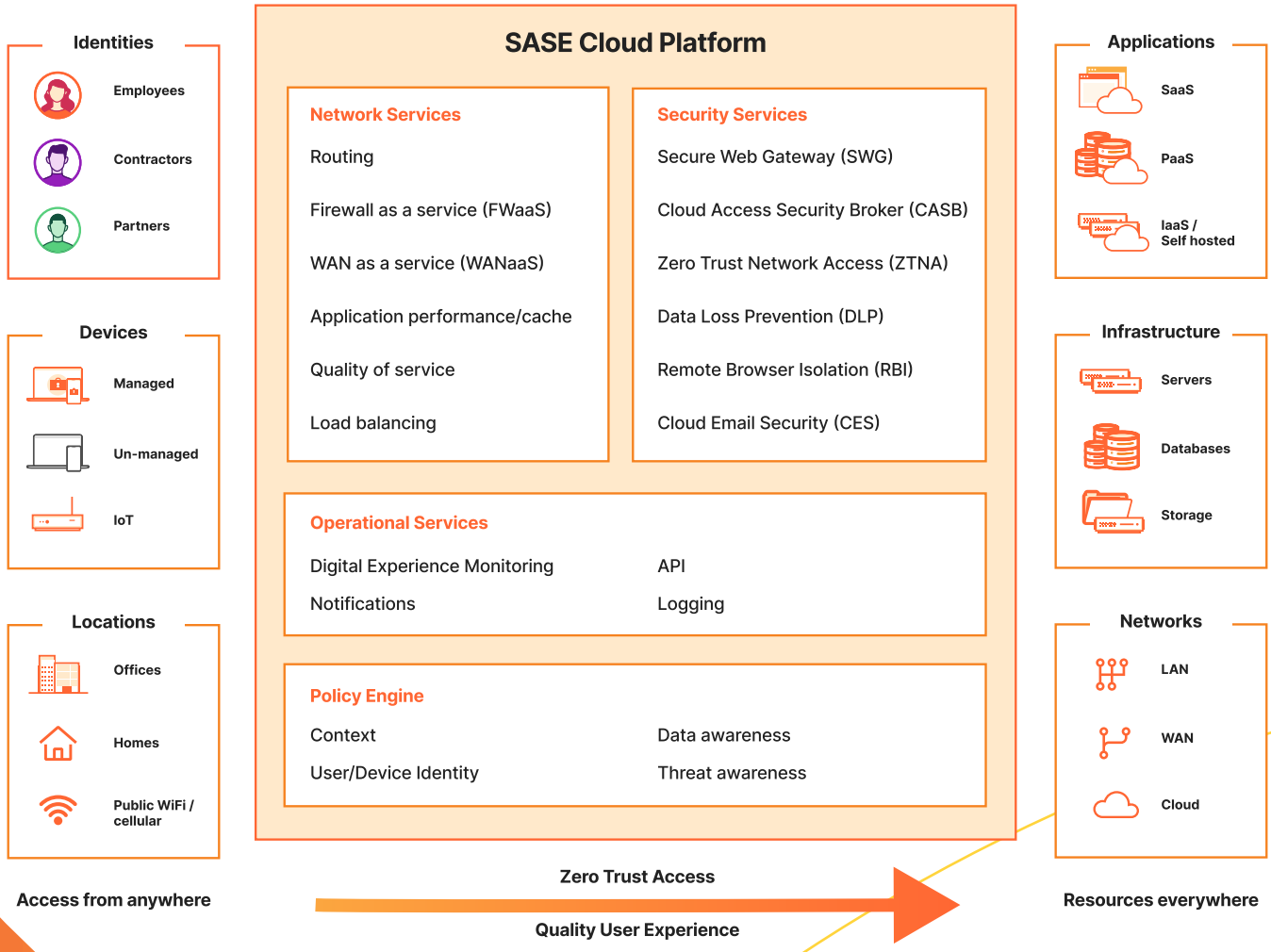
While most SASE platforms include the core capabilities noted earlier, **a single-vendor SASE platform built on a connectivity cloud will bundle additional SSE capabilities** (described further below). A connectivity cloud is a unified platform of cloud-native services that simplifies secure "any-to-any" connectivity across IT environments.

Additional capabilities in a SASE platform built on a connectivity cloud	
Cloud email security (CES)	Email is the #1 way organizations communicate, and research suggests that more than 90% of all cyber attacks begin with a phishing email. Phishing attacks prey on the trust of your users to gain entry without having to rely on network intrusion, malware drive-bys, or command and control callbacks. And, multichannel phishing campaigns (as described earlier) take the problem one step further — engaging users across a variety of applications. To face this growing risk, cloud email security that complements your cloud email provider's built-in security capabilities — and that also integrates with other SASE services — can provide comprehensive protection against multichannel threats that go beyond just email.
Data loss prevention (DLP)	To prevent data from being stolen or destroyed without permission, DLP technologies can detect the presence of sensitive data in transit, in use, and at rest and across web, SaaS, and private applications, especially as part of a broader SASE platform. For instance, In combination with a SWG, DLP solutions can control data in transit; in combination with a CASB, DLP solutions can detect data at rest.
Digital experience monitoring (DEX)	DEX is a tool for monitoring user behavior and their experiences with website traffic and app performance. It helps organizations capture real-time data around network issues, performance slow-downs, and application outages. This helps to pinpoint network issues and identify the root causes of connectivity anomalies.

Recursive DNS filtering	DNS filtering stops malicious, risky, or unacceptable websites and applications from being accessible over any port and protocol on any device by blocking or overriding the resolution of domain names into IP destinations. When it is offered as part of a recursive DNS resolution service, it enables quickly and transparently protecting anything connected to a large number of network locations, such as distributed offices, without device agents, network connectors, or routing changes. It can be included as part of a SWG, along with other technologies that keep internal users and devices secure.
Authoritative DNS security	DNS security protects DNS infrastructure from cyber attacks in order to keep it performing quickly and reliably. An effective DNS security strategy incorporates a number of overlapping defenses, including establishing redundant DNS servers, applying security protocols like DNSSEC, and requiring rigorous DNS logging. Authoritative DNS security provided through an extended single-vendor SASE platform can further bolster security for public hostnames protected through clientless ZTNA.
Content delivery network (CDN)	A CDN delivers fast, efficient, and secure delivery of content to websites and Internet services. If properly configured, a CDN can also help protect websites against threats like DDoS attacks. A CDN further improves performance for public-facing resources when provided through an extended single-vendor SASE approach, minimizing hops as traffic flows through other single-pass security steps, like CASB or SWG.
Web application and API protection (WAAP)	WAAP is an overarching category of security solutions designed to protect web applications and APIs. It includes web application firewalls (WAFs), bot management, DDoS mitigation, and API protection services (e.g., rate limiting, schema validation, API authentication). These capabilities bolster core SASE services for Layer 7 resources, such as internal ZTNA-protected apps, by strengthening protection against insider threats and lateral movement. WAAP and core SASE services can converge in a connectivity cloud to maintain strong performance even while introducing additional security services to web traffic flows.
Private backbone	While SASE providers promise cloud-delivered networking, in reality many vendors build their networks for outbound traffic to the Internet, with no interconnectivity between their data center locations. As a result, the performance of WAN network connections over long distances becomes unpredictable. To deliver an enterprise grade network experience, ensure that your SASE vendor has a proper private backbone to support your WAN traffic. A private backbone is a dedicated network that acts as a fast lane between data centers in different regions. This eliminates major sources of latency by avoiding the congestion and unpredictable performance of public networks.

Although every enterprise IT environment comprises highly specific tooling, processes, and architectural configurations, a connectivity cloud adapts to an organization's unique needs while still providing consistent user experiences. This gives technology leaders a customizable control plane for their entire SASE platform.

Learn more about evolving to a single-vendor SASE architecture built on a connectivity cloud in Cloudflare's SASE reference architecture.



Citations

[1] Gartner, Critical Capabilities for Single-Vendor SASE. Andrew Lerner, Jonathan Forest, Nat Smith, John Watts. 21 August 2023.

[2] Gartner, Forecast Analysis: Secure Access Service Edge, Worldwide. Nat Smith, Neil MacDonald, Christian Canales, Andrew Lerner, Jonathan Forest, John Watts, Shailendra Upadhyay, Charlie Winckless. 10 October 2023.

1 888 99 FLARE | enterprise@cloudflare.com | Cloudflare.com

REV:BDES-5482.2024FEB05