



EBOOK

The CISO's guide to SASE adoption

How to evaluate SASE platforms for high-priority use cases



The mission to achieve cyber resilience

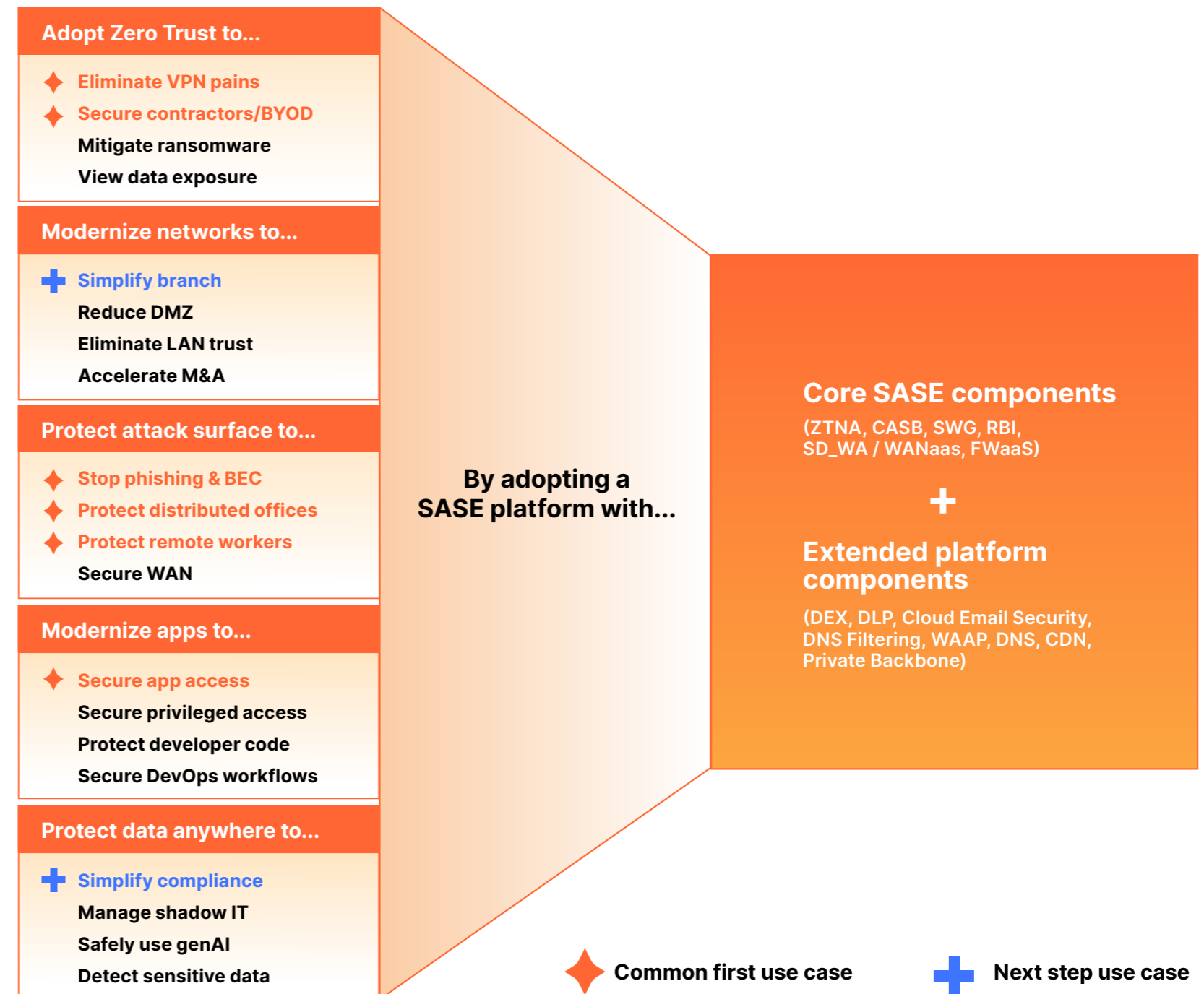
The National Institute of Standards and Technology (NIST) [defines cyber resiliency](#) as the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources.

However, strengthening cyber resilience — while reducing breach mitigation costs — also presents several challenges:

- **Cyber criminals continue to evolve their tactics:** As attackers develop more sophisticated tools, techniques, and procedures, the threat landscape becomes even harder for organizations to secure
- **IT environments are becoming more complex:** Due to the abundant number of devices and applications connected across multicloud architectures, securing these environments is a costly and complicated process
- **Internal teams are overloaded:** Organizations may run into resource constraints, as budgets get tighter and internal teams become overtaxed

To overcome these challenges, many CISOs are turning to a [secure access service edge \(SASE\)](#) framework. Unlike past networking approaches, a SASE 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 — to allow enterprises to provide simple, secure access to any user, app, device, or network, regardless of location.

This guide covers some of the most common use cases for SASE and outlines key steps to kickstarting your SASE implementation — so you can strengthen your cyber resilience and establish quick wins.



Use case #1:

Adopt Zero Trust network access (ZTNA)

Relying on traditional perimeter-based security for hybrid work arrangements, multicloud environments, and unmanaged devices leaves organizations with limited visibility, conflicting configurations, and excessive risk. A Zero Trust approach — in which granular access controls ensure that no entity is trusted by default — can help modernize your security strategy in the following ways:

Replacing traditional hardware-based security

Traditional network perimeter controls, such as virtual private networks (VPNs), can be difficult to scale, impact visibility, and make it difficult for security teams to spot and remediate attacks. A SASE model provides a secure alternative by implementing Zero Trust network access (ZTNA), while also routing and processing network traffic across a global cloud network — helping reduce both end-user friction and lateral movement.

Managing device access

Giving access to third-party users — like contractors, agencies, and suppliers — can introduce risk when organizations accidentally over-provision privileges or grant access to unmanaged devices. SASE allows organizations to set clientless Zero Trust policies, thereby ensuring that third-party users only have access to what they need.

Preventing ransomware attacks

Ransomware can quickly spread across an entire network — and in some cases, may even spread across multiple networks and organizations. SASE helps prevent the spread of ransomware attacks by revoking network and application access as soon as an infection is detected. Backed by the Zero Trust principle of 'least-privilege access control,' this approach makes it difficult for attackers to escalate privileges and move laterally within a network.

Limiting data exposure

Data exposure and exfiltration can pose a serious threat to organizations as users upload or distribute sensitive information across sanctioned and unsanctioned applications. SASE Zero Trust policies can help prevent data exposure by limiting which applications each user has access to, while also scanning popular SaaS suites for sensitive data and misconfigurations.



CASE STUDY

Adopting Zero Trust

A Fortune 500 telecommunications provider used Cloudflare's SASE platform to secure their hybrid work environment for 100,000+ employees — across hundreds of applications hosted on AWS, Azure, and other cloud environments. With an identity-based Zero Trust network architecture, secure web gateway, and unified access controls, they were able to protect users from threats without needing to juggle multiple policy-building interfaces, VPNs, and Internet filtering services.

Use case #2:

Protect attack surfaces

Digital transformation and remote work has expanded the attack surface, with more dispersed users and unmanaged devices requiring access to internal resources. But extending on-premise firewalls to the cloud and scaling networks via VPNs can increase exposure to both external and internal threats, while simultaneously reducing visibility. With a SASE architecture, organizations can extend visibility and controls to support a “perimeter-less” model and enforce consistent protection in the following ways:

Avoiding multi-channel phishing

Attackers often launch phishing attacks into channels where users tend to let their guard down about where they click — especially those tools not typically protected by email security controls. A unified SASE platform enables comprehensive protection across all of your environments to mitigate the risk of credential theft, account takeovers, and data exfiltration.

Defending remote workers

Remote work requires users to connect from multiple locations and devices, often outside the purview of the organizations that employ them. A SASE architecture allows organizations to secure employee and third-party access to critical environments and data, helping ensure a protected, productive work-from-anywhere approach.

Improving user experiences

Traditional approaches for scrubbing office traffic often require backhauling the traffic to centralized corporate data centers, which can add latency and hurt productivity. But the alternative — giving users direct access to the Internet — introduces security risks and creates inconsistent user experiences. SASE intelligently manages and optimizes direct connections to any cloud or Internet destination, and enforces policies and protections as close to end users as possible.

Securing wide area networks (WANs)

Some WANs bypass cloud security for traffic between branches, so integration claims between security services and software-defined WANs may not be what they initially seem. SASE enables organizations to simplify and secure how they connect over WANs by filtering and inspecting traffic between offices, data centers, public clouds, and other locations inside and outside of the broader Internet.



CASE STUDY

Protecting expanding attack surfaces

Werner Enterprises seamlessly deployed SASE services during their cloud migration — without any critical business or customer service interruptions. After their deployment, they reduced malicious emails by 50%+ while also minimizing manual email triage efforts by several hours per day, so their security team could focus on more strategic business goals.

Use case #3:

Protect data anywhere

As data spans more environments, organizations often find it difficult to track. Sensitive data may be exposed through the unsanctioned use of generative artificial intelligence and shadow IT, leading to compromise or breaches that may be costly to remediate. SASE converges data visibility and controls across web, SaaS, and private application environments, helping organizations accomplish the following:

Simplifying compliance with data privacy regulations

With the rise of large language models (LLMs) and other AI tools, compliance standards need to evolve to protect user data. SASE keeps data safe and private by unifying data controls, so security teams can lock down regulated data classes, reduce the risk of breaches, and ensure continued compliance with strict data requirements.

Managing shadow IT

Shadow IT — unsanctioned applications that are not managed or secured by the organizations that use them — can introduce risk as sensitive data is moved into or through them. SASE helps minimize this risk by proxying traffic through inline cloud access security brokers (CASB), which log every connection and request to reveal the presence of unsanctioned applications, then allow organizations to control how those apps are accessed and used.

Using generative AI safely

As more organizations adopt AI, the risk of exposing sensitive data also increases. With a secure web gateway and an inline cloud-access security broker, a SASE approach enables security teams to detect and approve AI application usage, scan for misconfigurations that risk data leaks, or run AI apps in isolated web browsers to restrict data inputs and output.

Protecting sensitive data

A SASE architecture allows 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 regulated personal data and intellectual property, blocking Internet threats like phishing and ransomware, and implementing additional protections against data theft and inadvertent leaks.



CASE STUDY

Protecting data anywhere

Applied Systems adopted SASE services to secure access to self-hosted applications and infrastructure for 2,500+ employees. This new approach gives their security team the flexibility to apply rigorous controls to meet different user needs while also controlling how their data is shared with AI tools.

Choosing a SASE solution:

Single-vendor consolidation vs. multiple point solutions

A single-vendor SASE provider converges network and security capabilities into a single cloud-delivered service. This allows businesses to consolidate different point products, eliminate appliances, and ensure consistent policy enforcement. While a multi-vendor SASE implementation may achieve similar results to a single-vendor approach, it often increases complexity and cost while reducing internal visibility and flexibility.

Consolidating these capabilities on a unified platform enables you to fulfill the true promise of SASE: a simplified, efficient network and security infrastructure that reduces your total cost of ownership and easily adapts to meet your evolving business needs.

As you evaluate potential SASE providers, keep the following questions in mind:

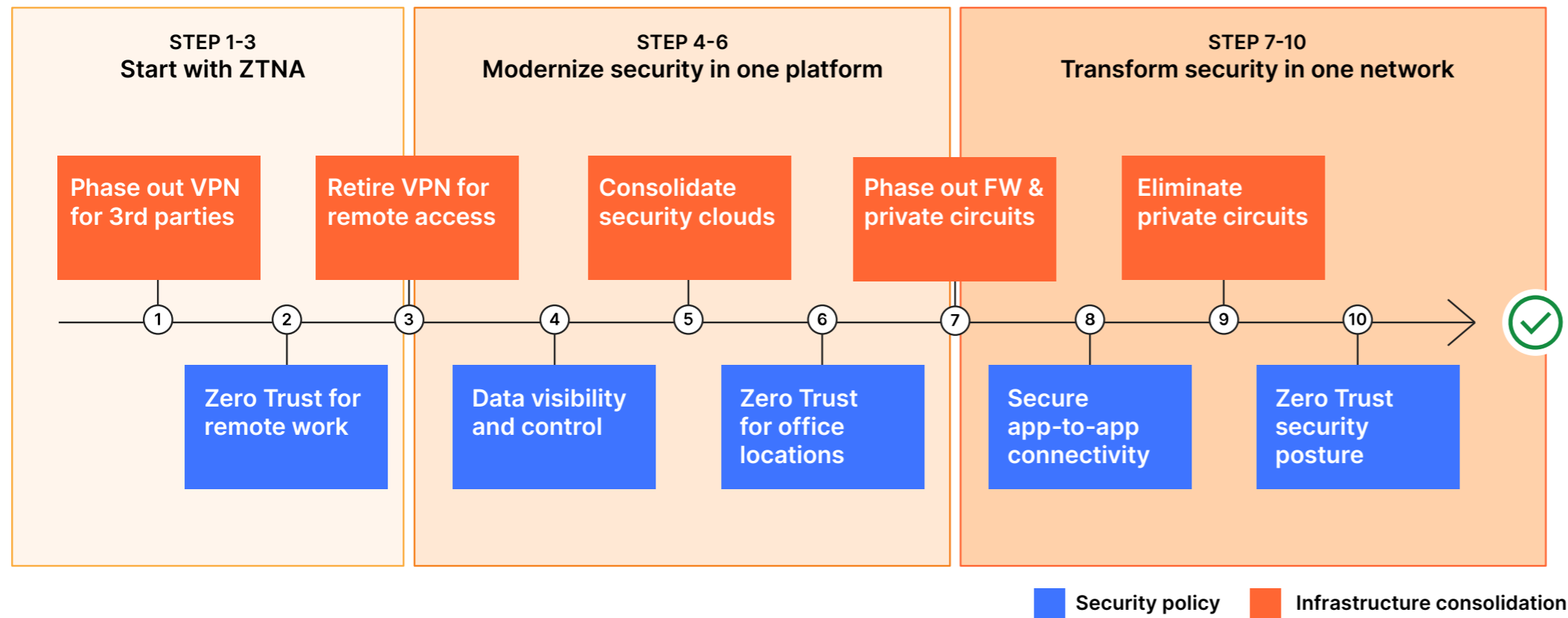
1. Is application traffic decrypted and inspected by threat and sensitive data detection engines in a single pass? Are there any deployment caveats?
2. Are all data flows and communications through SaaS suites protected across every channel (inline and out-of-band web and email activity)?
3. Is remote browser isolation enabled for every user and application? How does this impact productivity? Does it incur additional fees?
4. Are any security functions bypassed based on any network on-ramps?
5. Is it possible to ensure customer traffic is isolated and private across a multi-tenant cloud architecture?
6. What data localization capabilities are available? Does enabling data localization add latency for remote users that connect outside of your localized region?
7. Can you integrate your threat intelligence feeds into their architecture? How does the platform reduce false positives from threat intelligence feeds?
8. What kind of user/device risk scoring and analytics are available? Can risk scores be uniformly enforced across all applications?




How Cloudflare delivers SASE

To complete the journey to a unified SASE platform, many enterprises trust Cloudflare. We are the only SASE provider to start with a Zero Trust Network architecture with identity and context-based connectivity consistently built-in across our entire platform.

Your long-term roadmap for a complete SASE architecture may follow a similar flow to the example below:



Backed by a global network that spans 310+ cities worldwide, Cloudflare helps CISOs achieve enterprise-grade security, resiliency, and performance. Our single control plane converges point solutions across multiple security domains, so organizations can simplify their security operations and ensure consistent protection against evolving threats.

 Visit our website to learn more about [Cloudflare](#) and the [Cloudflare SASE platform](#).



© 2024 Cloudflare Inc. All rights reserved.
The Cloudflare logo is a trademark of Cloudflare. All other
company and product names may be trademarks of the
respective companies with which they are associated.

Call: 1 888 99 FLARE
Email: enterprise@cloudflare.com
Visit: cloudflare.com

REV:BDES-6017.2024JUNE06