AT&T Business

Simplifying SASE, SSE, SD-WAN, and ZTNA

How to choose the framework that best fits your business

Table of contents

Introduction

We get it. Your network is more complex than ever, leaving you juggling tools that barely speak to each other. SASE, SSE, ZTNA, and SD-WAN are supposed to solve your problems—but they are often discussed so interchangeably, it's hard to know where to start. Our guide is here to simplify things.

We created it for teams like yours to help you learn:

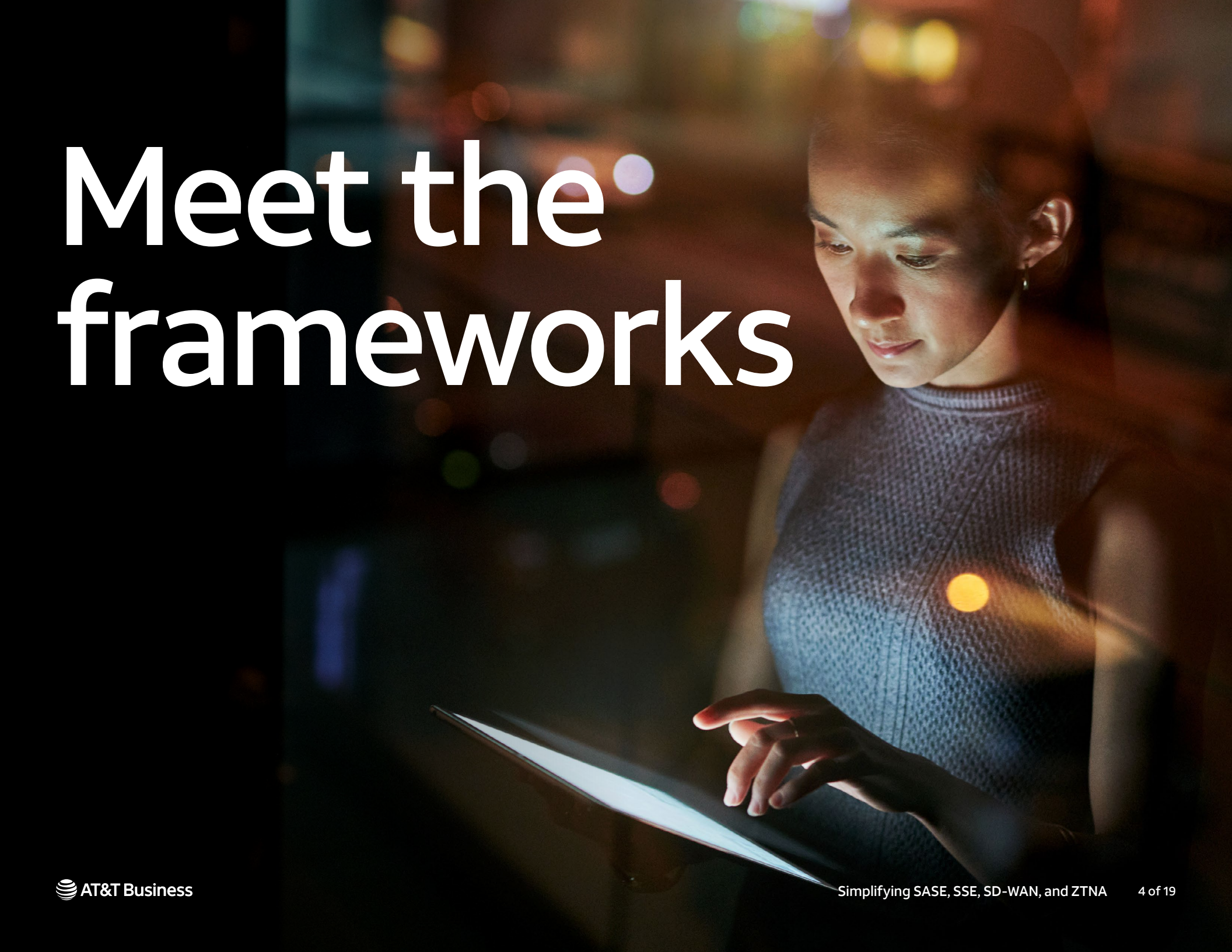
What roles SASE, SSE, ZTNA, and SD-WAN serve in modern secured connectivity

How they work together to secure and optimize your connectivity

Where to start, based on your needs and goals

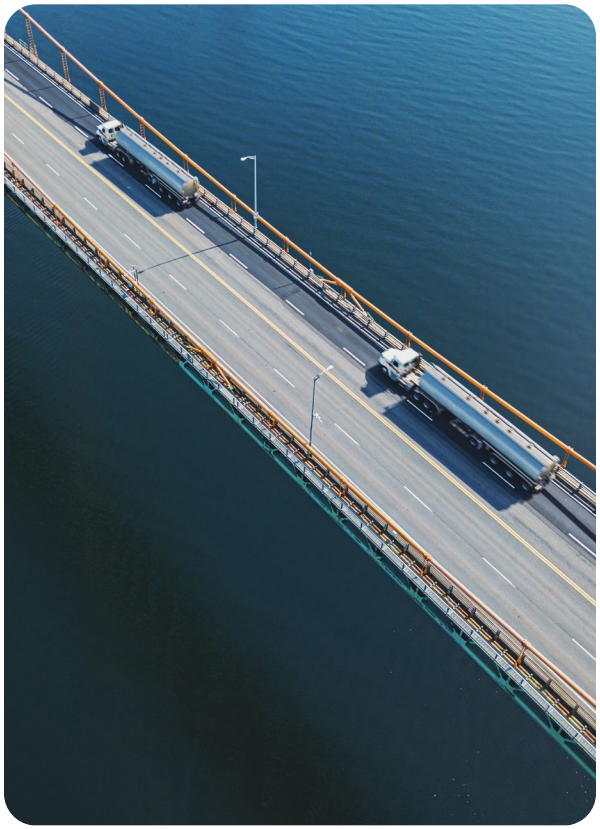
How organizations like yours evolve in security and connectivity from point solutions to more unified efficient models

Meet the frameworks



For a moment, imagine that your business is a city...

Let's call it Businessville. Twenty-four hours a day and 7 days a week, people (employees), vehicles (devices), and goods (data) are in constant motion in Businessville. Everything and everyone travels between offices (apps), warehouses (cloud storage), and homes (endpoints). As the city grows traffic patterns change, old roads get congested and the departments managing the city get larger and more complex but with little coordination between them.



This is exactly what happens to businesses in the real world. As they expand, adding security tools, supporting remote work, and adopting cloud apps, the city becomes harder to manage. Latency and congestion plague your people. Blind spots and silos hurt detection and issue resolution. Overall, maintaining performance while ensuring security becomes a much more difficult task.

In the pages ahead - we will return to Businessville to help you understand how SASE, SSE, ZTNA, and SD-WAN solve different parts of that challenge.

ZTNA: the modern VPN alternative

Zero Trust Network Access (ZTNA) replaces the legacy VPN with a cloud-delivered access control model based on identity. Instead of granting broad network access when a user logs in, ZTNA enforces the principle of "never trust, always verify." It removes implicit trust and replaces it with identity and context-based access controls.

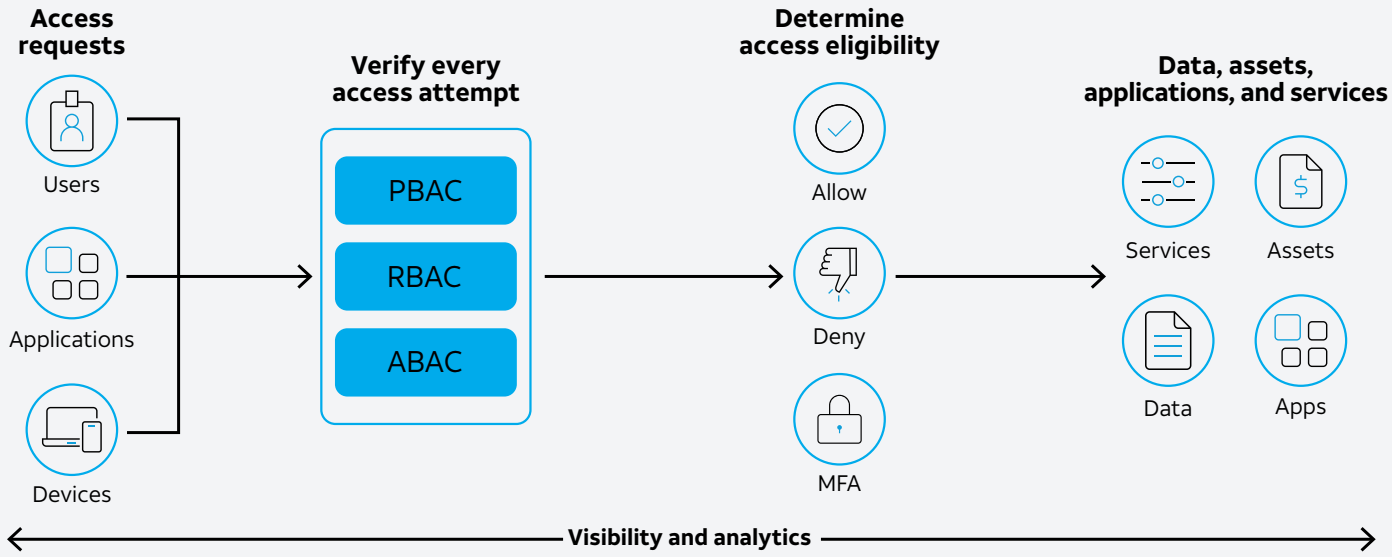
How does ZTNA work?

In Businessville, ZTNA acts like the citywide digital ID system. ZTNA verifies who and what should enter before granting access. Unlike VPN, ZTNA only unlocks the specific building or buildings in the city (apps or services) that a user is authorized to enter instead of giving them access to everything beyond the city gates. It checks their identity, device, and context every single time.

A typical ZTNA solution:

- **Employs dynamic access based on context.** ZTNA verifies every user and device every time they connect, and restricts access based on identity, device state, and what needs to be accessed. This reduces the risk of unauthorized access and lateral movement.
- **Ends latency experienced with VPN tunnels.** ZTNA connects users to the applications they are allowed to use directly instead of forcing traffic through a central VPN gateway, improving performance for remote and hybrid workers.
- **Delivers uniform identity and access controls everywhere your business operates.** This ensures consistent protection for every user, device, and application—whether on-premises, with multiple providers, or in the cloud.

Zero Trust Network Access



Why organizations are moving to ZTNA

Many organizations focused on growth often begin with employing ZTNA to replace VPNs because they were not created for a cloud-first or hybrid world. Though every organization has unique needs when it comes to identity, access, and the securing of data overall, there are some general drivers behind implementing ZTNA.

People work from everywhere. Backhauling traffic through a VPN hub causes unnecessary friction and reduces productivity. But ZTNA allows users to connect from anywhere securely and quickly, removing the friction and supporting productivity from anywhere.

VPNs aren't smart enough to stop unauthorized access. They grant broad network access after login. ZTNA removes implicit trust, shrinking the attack surface, blocking lateral movement, and containing the impacts of unauthorized access.

Cloud apps smashed the perimeter. They left the data center for Software as a Service (SaaS), Infrastructure as a Service (IaaS), and private clouds and took your data with them. VPNs add complexity and risk, but ZTNA applies consistent identity and context-based access to every app.

Compliance requires you to prove control of access to sensitive systems and data. It also requires you to show how access is governed, enforced, and audited. VPNs can't provide the level of accountability that ZTNA can because it continuously authenticates and logs every connection by every user, device, and application.

ZTNA lays the groundwork for SASE and SSE, which rely on ZTNA to function effectively.

How it's delivered

ZTNA is typically deployed as a cloud-delivered service and does not require a full network overhaul as it should integrate with your existing identity provider. Many organizations choose to roll it out in phases, replacing the VPN with ZTNA for one business unit at a time.

However, standalone ZTNA lacks the added web security, cloud visibility, and network optimization of a broader framework like SSE or SASE.

You probably need ZTNA if:

- Your employees still rely on traditional VPNs for remote access
- Your business is the steward of sensitive information and data like personally identifiable information (PII) or intellectual property (IP)
- You need to enforce granular access policies for contractors or third parties
- You want to reduce the risk of credential theft leading to broad network compromise

SSE: the security consolidator

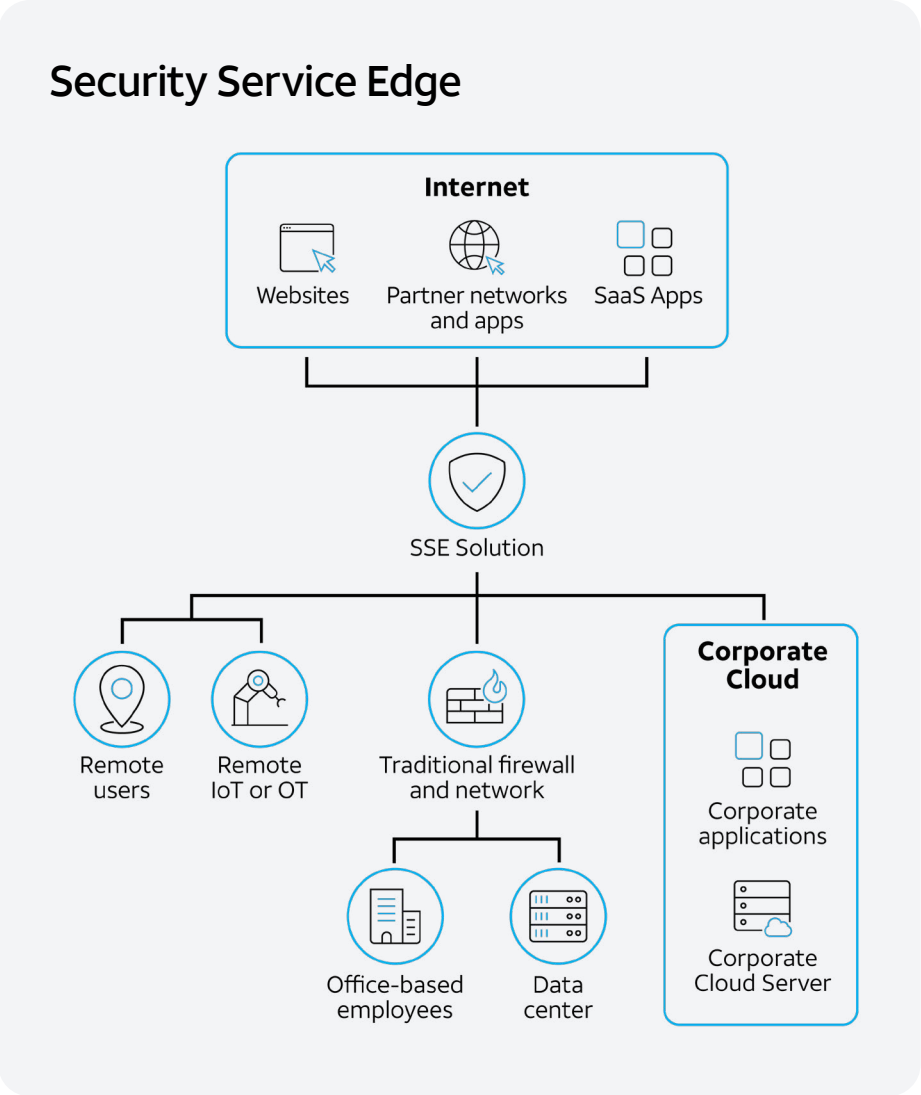
Security Service Edge (SSE) moves key protections from hardware appliances into the cloud, allowing organizations to apply consistent policies across users, devices, and locations.

How does SSE work?

In Businessville, if ZTNA acts like the citywide digital ID system, then SSE is the city's safety system, running traffic lights, security cameras, and patrols that enforce the rules.

A typical SSE framework includes:

- **ZTNA**
  Delivers identity and context-based access as a replacement for VPN
- **Secure Web Gateway (SWG)**
  Protects your internal network by enforcing security policies and providing visibility into network traffic
- **Cloud Access Security Broker (CASB)**
  Sits between users and apps to protect data by enforcing security policies
- **Firewall-as-a-Service (FWaaS)**
  Provides scalable, cloud-based firewall protection



Why organizations are moving to SSE

Organizations adopt SSE to simplify security delivery, provide visibility, and enforce security policies everywhere uniformly, without relying on outdated network perimeters or hardware. For many, when managing disconnected tools becomes too heavy a lift, they choose SSE to get unified control.

In general, organizations run into a few common roadblocks that guide them toward SSE:

You cannot secure what you cannot see. The reality is your organization's data is spread across multiple services because of shadow IT, multi-cloud environments, and remote work. SSE gives security teams the ability to identify risks, enforce policies, and protect data by centralizing visibility and control.

Protecting your data is harder than ever. Your data is constantly moving between apps, clouds, and devices. SSE applies the same security policies to your data everywhere it goes.

Detection should be closer to your users to reduce the time attackers have to act. SSE brings detection to where users connect, the cloud edge, which improves time to response.

Consolidation closes the coverage gaps and keeps enforcement consistent. SSE takes core protections, SWG, CASB, FWaaS, and ZTNA and joins them into one platform.

SSE alone, however, cannot address latency, blind spots, or bottlenecks. Without SD-WAN, the other half of the SASE equation, network performance is left unaddressed.

How it's delivered

SSE can be adopted directly from vendors or delivered as part of a managed SASE solution. For many organizations, it's a first step toward simplification, but one that eventually benefits from being paired with networking under a full SASE model.

You probably need SSE if:

- You already have a modern SD-WAN in place but lack consistent security.
- Your VPNs are straining under the weight of remote and hybrid access.
- You need to protect SaaS applications but don't want more hardware.
- You want to start consolidating point solutions now but aren't ready to modernize networking.

SD-WAN: the intelligent networking foundation

A Software Defined Wide Area Network (SD-WAN) intelligently routes traffic to prioritize critical applications, improve performance, and improve reliability across a business. Where traditional networks are hardware based, SD-WAN uses software-defined controls that adapt to network conditions in real time and provide better visibility.

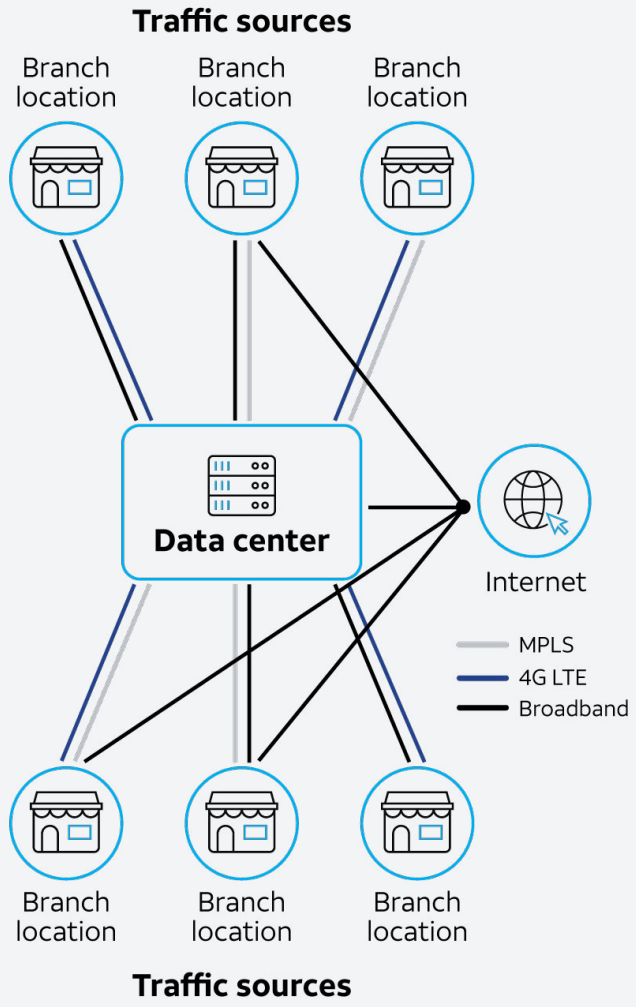
How does it work?

In Businessville, SD-WAN acts as the city's traffic management center. It monitors every route, and detects accidents and traffic jams so that it can funnel motorists to faster routes and clearer streets to keep essential services in operation.

A strong SD-WAN solution:

- **Has real-time monitoring and selects the best path for traffic.** SD-WAN measures the health of every connection, monitoring things like latency and automatically prioritizing and redirecting traffic when necessary.
- **Leverages multiple connections for resilience.** SD-WAN protects operations by combining multiple WAN links and determines in real time whether traffic should use fiber, broadband, or 5G without requiring manual intervention.
- **Puts business-critical applications first.** SD-WAN gives priority "lanes" to the things connected to a network that are critical for operations like point-of-sale (POS) terminals and payment or voice applications. In the event of a disruption, sessions stay active and businesses keep running.
- **Simplifies control and visibility.** SD-WAN centralizes monitoring and analytics across all connection paths.

SD-WAN



Why organizations are moving to SD-WAN

SD-WAN helps organizations that want to evolve past the traditional network model. Many organizations using cloud applications or distributed workforces choose SD-WAN because it gives them more flexibility, performance, and resilience.

There's a need for speed. SD-WAN is faster than traditional networks because it does not backhaul traffic through a centralized data center and finds the optimal route for all traffic, so organizations get fast, reliable connectivity.

Downtime means death. SD-WAN gives businesses an active, multi-path defense against network disruptions or link outages that would otherwise halt operations.

All roads lead to SASE. SD-WAN unlocks edge inspection and consistent access control, which prepares organizations for a full SASE deployment.

How it's delivered

SD-WAN can be deployed in two models, DIY or a managed solution. Both models use the same technology and the difference is really in who manages it day to day.

In a DIY or self-managed deployment, your IT team would have to configure everything and would be responsible for monitoring. This typically involves a vendor portal or dashboard that allows you to connect circuits and manage policies.

This option is best for organizations with strong internal networking expertise and confidence in their ability to monitor performance and troubleshoot outages.

In a managed solution deployment, your IT team would retain full visibility and the ability to customize policy, but a trusted provider would design, deploy, monitor, and maintain your SD-WAN.

This option is best for teams that need to reduce operational strain or that prefer expert configuration and support.

You probably need SD-WAN if:

- You want stronger resilience and performance
- You manage or are about to expand into multiple locations
- Your users complain of latency issues like poor video quality and lag
- Connectivity outages would be a death knell to your business

SASE: the unified choice for security and the network

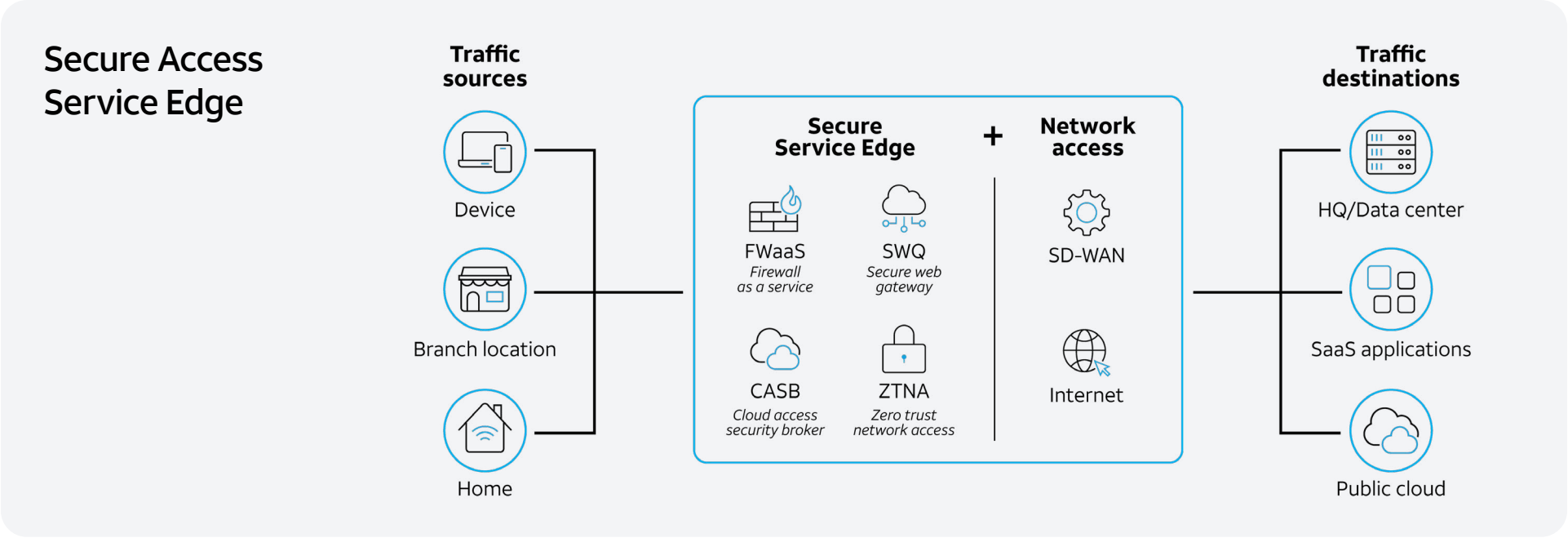
Secure Access Service Edge (SASE) combines Software-Defined Wide Area Network (SD-WAN) and Secure Service Edge (SSE) to combine networking and security and deliver them through a single cloud-based service. SASE provides organizations with a single management console to handle data protection, location connectivity, and performance management, which minimizes the need for multiple point solutions.

How does SASE work?

To recap, in our Businessville example, ZTNA is the citywide digital ID system, SD-WAN acts as the city's traffic management center, and SSE is the city's safety system. SASE functions as the intelligent grid that powers Businessville. It connects roads, lights, and safety systems in the city into one unified system to keep Businessville running safely and optimally.

A complete SASE framework consists of two main components:

- **Software-Defined Wide Area Network (SD-WAN)** operates as the networking component of SASE. The system uses SD-WAN to direct network traffic through intelligent optimization between locations and applications.
- **Secure Service Edge (SSE) works as the security part of SASE.** SSE consists of ZTNA and FWaaS alongside a core security framework that makes up its security functionality.



Why organizations are moving to SASE

Organizations are choosing SASE because tool sprawl, cloud-first architectures, and hybrid work have made it so that separate networking and security stacks have become too complex, slow, and expensive to manage. The old ways businesses have used to secure their networks just cannot keep up with the new ways we work. As a result, most organizations have similar motivations to adopt SASE.

Security and networking can't be separate anymore. Silos slow performance, add complexity, and create blind spots. SASE unifies security and networking into one framework that improves visibility, enforces consistent security policies across your organization, and improves network performance.

Added complexity means added risk. Disconnected tools increase the chance of errors and create gaps that attackers can exploit. SASE strengthens your overall security posture by simplifying your stack, converging security and networking.

Visibility and control are always going to be important. Users, devices, and policies become harder to monitor, enforce, and audit in distributed environments. SASE gives teams one pane of glass of unified insights by centralizing monitoring and enforcement.

Traditional defenses can't keep up with fast-moving threats. Modern attacks exploit speed, automation, and lateral movement to outmaneuver static defenses. SASE detects and blocks threats at the edge, bringing inspection and enforcement closer to users and data.

SASE unifies networking and security to simplify operations, strengthen security, and improve network, application, and security performance.

How it's delivered

SASE can be deployed in two ways:

DIY SASE: Organizations piece together SD-WAN + SSE from different vendors and manage integration themselves.

Managed SASE: Organizations choose a networking provider (like AT&T Business) that partners with a chosen SSE solution provider and manages the whole solution end-to-end.

If you have in-house expertise, a DIY SASE solution is feasible, but for many, managed SASE is the practical path to simplification. An experienced SASE solution provider will deliver the benefits of SASE without the operational burden.

You probably need SASE if:

- You manage separate networking and security stacks that rarely align
- Your cloud performance issues are as big a problem as your security gaps
- You're spending more time integrating tools than defending the business
- Your current VPN model is slowing users down and failing to enforce consistent policies everywhere

So, which path is right for you?

Understanding the differences is one thing. Deciding where to start is another.

Framework	What is it?	Best for	Limitations
ZTNA *Zero Trust Network Access*	Modern alternative to VPNs	Organizations that need secure access to applications for remote/hybrid users	Alone, doesn't cover other critical security needs and lacks networking optimization
SSE *Security Service Edge*	The security half of SASE, delivered via the cloud	Organizations that need stronger security controls	Lacks networking optimization
SASE *Secure Access Service Edge*	A unified architecture that combines networking and security into a single, cloud-delivered service	Organizations that want simplification and unification	Can feel like a big lift if done DIY; often best as managed SASE
SD-WAN *Software Defined Wide Area Network*	The access half of SASE. Intelligently routes and prioritizes traffic for faster, stronger connectivity	Organizations needing more resilient, intelligent connectivity	Lacks strong security controls

Here's how to think about your options based on the challenges you're feeling today.

If VPN pain is your biggest headache:

Start with ZTNA
It's the fastest way to modernize remote access and cut the risk of stolen credentials or over-privileged access.

If networking is strong but security feels scattered:

Add SSE
It brings your security stack together in the cloud, protects SaaS apps, and applies consistent policies across hybrid teams.

If you're tired of juggling vendors and integrations:

Move to SASE
It's the end state that unifies networking and security into one model, reducing sprawl and making performance and protection easier to manage.

If reliability and performance is your focus:

Adopt SD-WAN
It adds resilience with multiple active connections and optimizes cloud and SaaS performance with intelligent traffic routing.

Most organizations start where the pain is sharpest, tackling VPNs, SaaS security, or tool sprawl, and build from there.

The cost of doing nothing

For you, standing still means introducing risk, reducing productivity, increasing monetary costs, and risking the ability of the business to operate. Let's explore the cost of doing nothing while attacks increase and the nature of work evolves.

Complexity creates risk

IT teams juggle tools, vendors, and dashboards when networking and security are managed separately. In this patchwork environment you will find yourself juggling:

Policy gaps where attackers can slip through

Misconfigurations that open the door to breaches

More dashboards than people to watch them

Performance suffers

When traffic backhauls through your data center for inspection, everyone feels it.

Latency adds friction to operations, causing demos to lag, meetings to stall, and business to be interrupted.

Inspection points and VPN tunnels slow down business, which causes employees to find less secure workarounds.

Your team's innovation suffers as hours are spent troubleshooting misconfigurations or tool conflicts instead of work that can improve security posture or network performance.

The cost of doing nothing

Costs keep rising

A sprawling security stack is inefficient but also costly. You're paying for:

- Overlapping tools doing the same job
- Licenses gathering dust
- Consultants forcing systems to talk
- Emergency support when integration breaks
- Specialized expertise to manage each system

Each new solution you add will increase the total cost of ownership but will not give you a unified solution and instead will require greater investment in resources to maintain.

Threats won't wait

Attackers exploit gaps in policy enforcement, weak points between tools, and inconsistent patching cycles. While you plan next quarter's integration, attackers exploit today's cracks.

- Most breaches (86%) happen nights and weekends, when IT coverage is thin[1]
- VPNs carry 22+ known exploited vulnerabilities (CISA, 2024)[2]
- 82% of ransomware attacks target companies with fewer than 1,000 employees[3]
- The seams between tools are the weakest points

One misconfigured setting can expose customer data, while one ransomware attack can halt operations. Worse, one outage during peak sales can damage your reputation for months.

Remember, **61% of breaches start with simple misconfigurations**, gaps that often appear right here, between systems that should work together, but don't.

1 Semperis Ransomware Holiday Risk Report 2024, semperis.com/ransomware-holiday-risk-report
2 CISA; Federal Bureau of Investigation; New Zealand's Government Communications Security Bureau; New Zealand's Computer Emergency Response Team; Canadian Centre for Cyber Security. Modern Approaches to Network Access Security. Cybersecurity and Infrastructure Security Agency, June 18, 2024. Retrieved from cisa.gov/sites/default/files/2024-06/joint-guide-modern-approaches-to-secure-network-access-security-508c.pdf
3 The Ransomware Epidemic: Why SMEs Are The New Primary Target forbes.com/councils/forbestechcouncil/2025/02/27/the-ransomware-epidemic-why-smes-are-the-new-primary-target/

Now what? Your path forward

You've learned what each framework can do and how it solves modern challenges in cybersecurity. It should be clear that standalone ZTNA or SSE are great, but they cannot offer the convergence of network and security capability and visibility allotted by SASE.

But building SASE alone means taking on numerous vendors, updates, and support models, which creates delays, risk, and hidden costs. Managed SASE, however, does the heavy lifting for you by offering you visibility and control without the complexity of management and maintenance.

Here are a few things to consider when searching for a managed SASE option:

True integration > service chaining

Look for a provider that delivers genuine convergence between networking and security under one architecture instead of cobbling solutions together. Service-chained solutions create latency, policy gaps, and complicated maintenance.

Deep expertise and support

Remember, SASE unifies networking and security, so you should find a partner that has a proven record managing both. Expertise in both areas impacts your resilience. The right provider will offer 24/7 monitoring, rapid response, and anticipation of issues.

Global reach and reliability

SASE improves the security and performance of the network. Choosing a provider that relies on third-party networking infrastructure will cause performance and coverage variations for your users—the exact opposite of what SASE should be doing for your business. Look for a provider with a global network backbone so you can ensure the same experience for every user.

Your security journey does not have to be complicated. With AT&T Managed SASE, you can cut through the noise, simplify operations, and give your teams the confidence to move faster with backing from one of the most trusted networks.

AT&T Managed SASE is backed by global reach, reliability, and proven expertise. We have been connecting and growing businesses for nearly 150 years. We serve nearly 2.5 million of the largest global companies, government agencies, and small businesses.

Start your SASE journey with the provider built to deliver it.

Learn more about AT&T Managed SASE solutions, or talk to an AT&T Business sales expert.

Learn more

Please fill out this form, and we'll contact you directly.

Fill out form

Why AT&T Business

See how ultra-fast, reliable fiber, protected by built-in security, and 5G connectivity give you a new level of confidence in the possibilities of your network. Let our experts work with you to solve your challenges and accelerate outcomes. Your business deserves the AT&T Business difference—a new standard for networking.