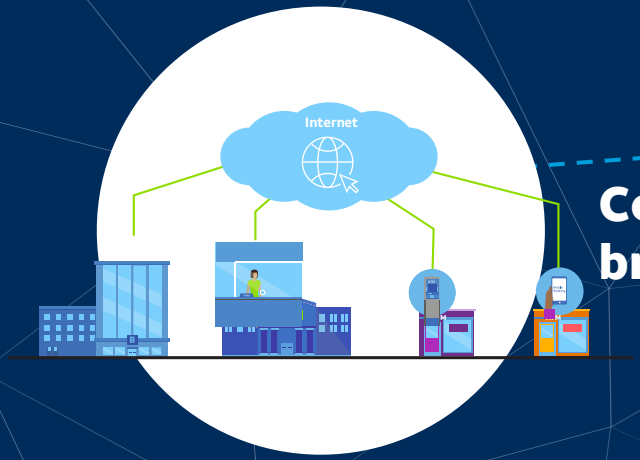
AT&T Business SASE

Click an image to learn more

Migration to cloud

Identity-based application access

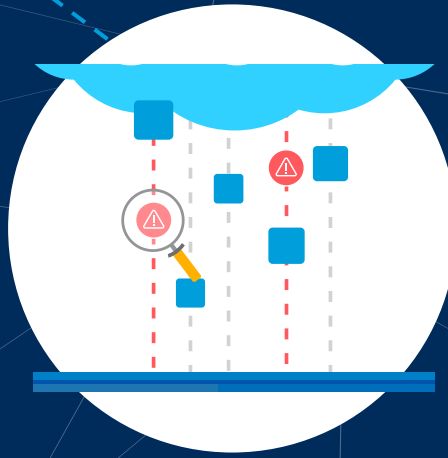
Connected branch



Safer internet browsing

Remote workforce

Inspection of web traffic



2021 AT&T Intellectual Property. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property. All other marks are the property of their respective owners. The information contained herein is not an offer, commitment, representation, or warranty by AT&T and is subject to change.

AT&T Proprietary - Not for use or disclosure outside the AT&T companies except under written agreement

Use case 1

Migration to cloud

How it works

Overview

Moving applications out of the data center and into the cloud offers many benefits. This includes access to the most up-to-date versions, lower capital expenses, and reduced overhead.

Business challenge

- Each time a user interacts with a cloud application, communications are required between their device and the resource, which is causing a massive increase in network traffic. This uptick in activity is overloading transport circuits, contributing to latency and a poor user experience.
- Technology teams often don't know which cloud applications are in use, which makes it impossible to control access or protect sensitive data.

How AT&T SASE can help

- Accelerate application performance by connecting users directly to cloud applications without backhauling traffic to the data center
- Prioritize bandwidth to business-critical applications such as voice over Internet Protocol (VoIP) and video conferencing with intelligent path routing
- Gain visibility into all applications being utilized, including unsanctioned programs, then apply policies that specify what may be accessed and how data may be shared

AT&T Business

Use case 1 Migration to cloud - How does it work?

Accelerate application performance

Branch and remote users connect directly to cloud applications over the internet. Secure Access Service Edge (SASE) provides cloud-based security services including firewall-as-a-service (FWaaS) and secure web gateway (SWG).

Recommended solution: AT&T SASE with AT&T Secure Web Gateway

Prioritize business critical applications

Edge appliances at the branch provide intelligent path routing, using software defined wide-area network (SD-WAN), to the application.

Recommended solution: AT&T SASE with AT&T SD-WAN

Eliminate shadow IT

Identify web-based applications being utilized, including unsanctioned and tolerated applications. Cloud access security broker (CASB) provides centralized visibility and reporting, both in-line and using application programming interface (API) integrations with cloud providers.

Recommended solution: AT&T SASE with AT&T Secure Web Gateway, and CASB

Enforce Policy

Apply policies, based on zero trust network access (ZTNA) principles that specify what may be accessed, by who, when, and how.

Recommended solution: AT&T SASE with AT&T Secure Web Gateway

Use case 2

Connected branch

How it works

Overview

Many organizations are modernizing their network by connecting branch locations directly to the internet, using multiple widely available transport circuits, then deploying software defined wide-area network (SD-WAN) to manage the data flows.

Business challenge

- Each connected branch creates a new gateway into the network that can be exploited.
- Traffic that does not flow through the data center bypasses any security controls hosted there.
- The security features native to stand-alone SD-WAN solutions may be insufficient to protect branch offices against all modern attacks.

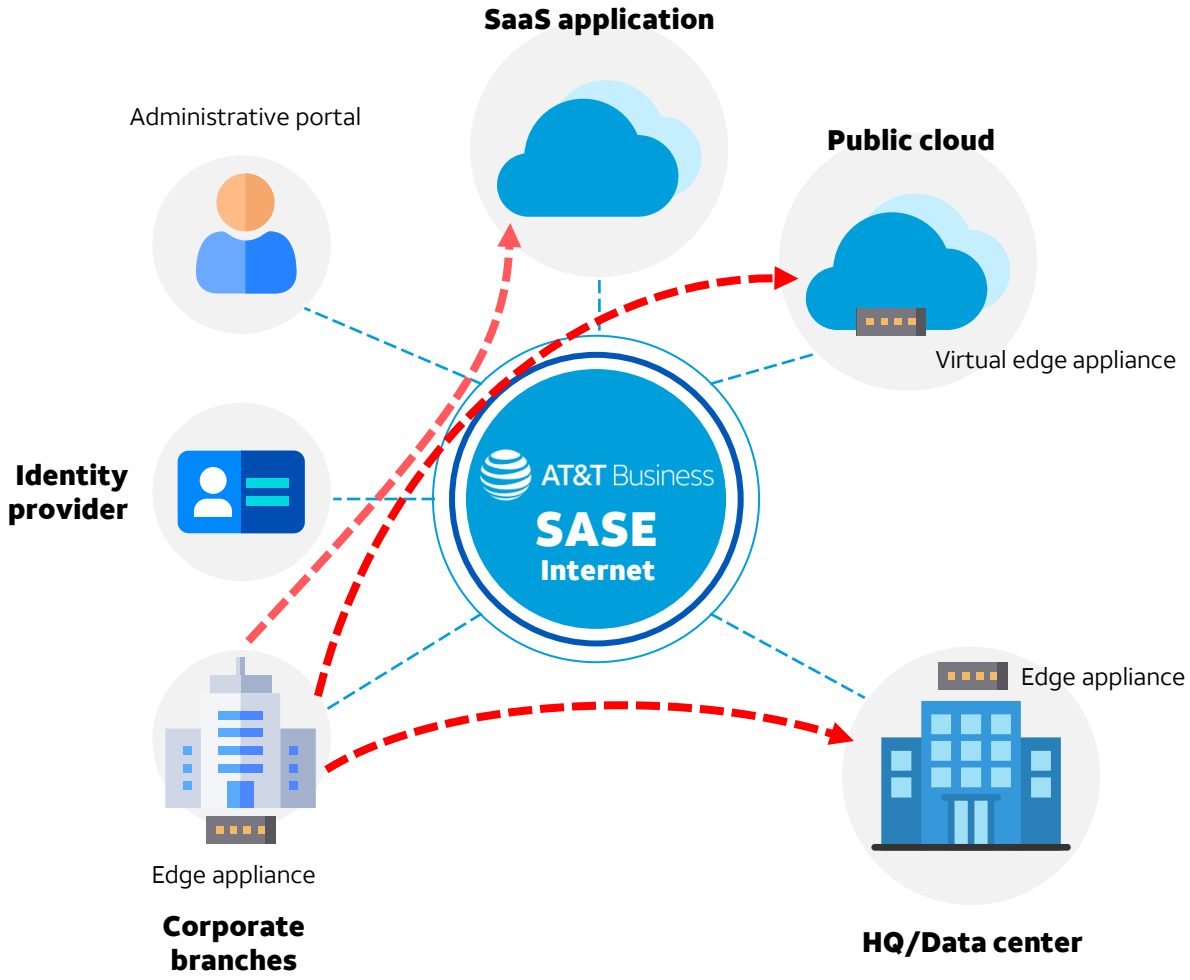
How AT&T SASE can help

- Prioritize bandwidth to business-critical applications such as voice over Internet Protocol (VoIP) and video conferencing with intelligent path routing
- Gain visibility into the health of the network circuits and security policies across locations and users
- Reduce risk with integrated and unified security that protects every device and user from a wide range of modern threats

SASE use cases / October 2021 / © 2021 AT&T Intellectual Property - AT&T Proprietary

Use case 2

Connected branch – How does it work?



Prioritize bandwidth to business-critical applications

Edge appliances provide intelligent path routing and bandwidth prioritization, using software defined wide-area network (SD-WAN), to ensure continued and optimal connectivity to the application across available circuits. The application could be cloud-based or hosted in the corporate data center.

Recommended solution: AT&T SASE with AT&T SD-WAN and AT&T Secure Web Gateway

Visibility into network health and security policies

Edge appliances provide detailed visibility and reporting of the health of network circuits and end-to-end connectivity to business-critical applications.

The Secure Access Service Edge (SASE) architecture applies global security policies to ensure a consistent security policy based on zero trust network access (ZTNA) principles.

Recommended solution: AT&T SASE with AT&T SD-WAN and AT&T Secure Web Gateway

Reduce risk with integrated and unified security

SASE provides global, cloud-based security including firewall-as-a-service (FWaaS), secure web gateway (SWG), ZTNA, cloud access security broker (CASB) and other optional services.

Recommended solution: AT&T SASE with AT&T Secure Web Gateway, CASB and data loss prevention (DLP)

SASE use cases / October 2021 / © 2021 AT&T Intellectual Property - AT&T Proprietary

Use case 3

Remote workforce

How it works

Overview

With the rise in cloud-based applications and mobility, many workers have been trading their cubicles for home offices, airports, or even coffee shops. The global health events of 2020 accelerated this trend, with many businesses finding themselves in the position of suddenly having to support an entirely remote workforce.

Business challenge

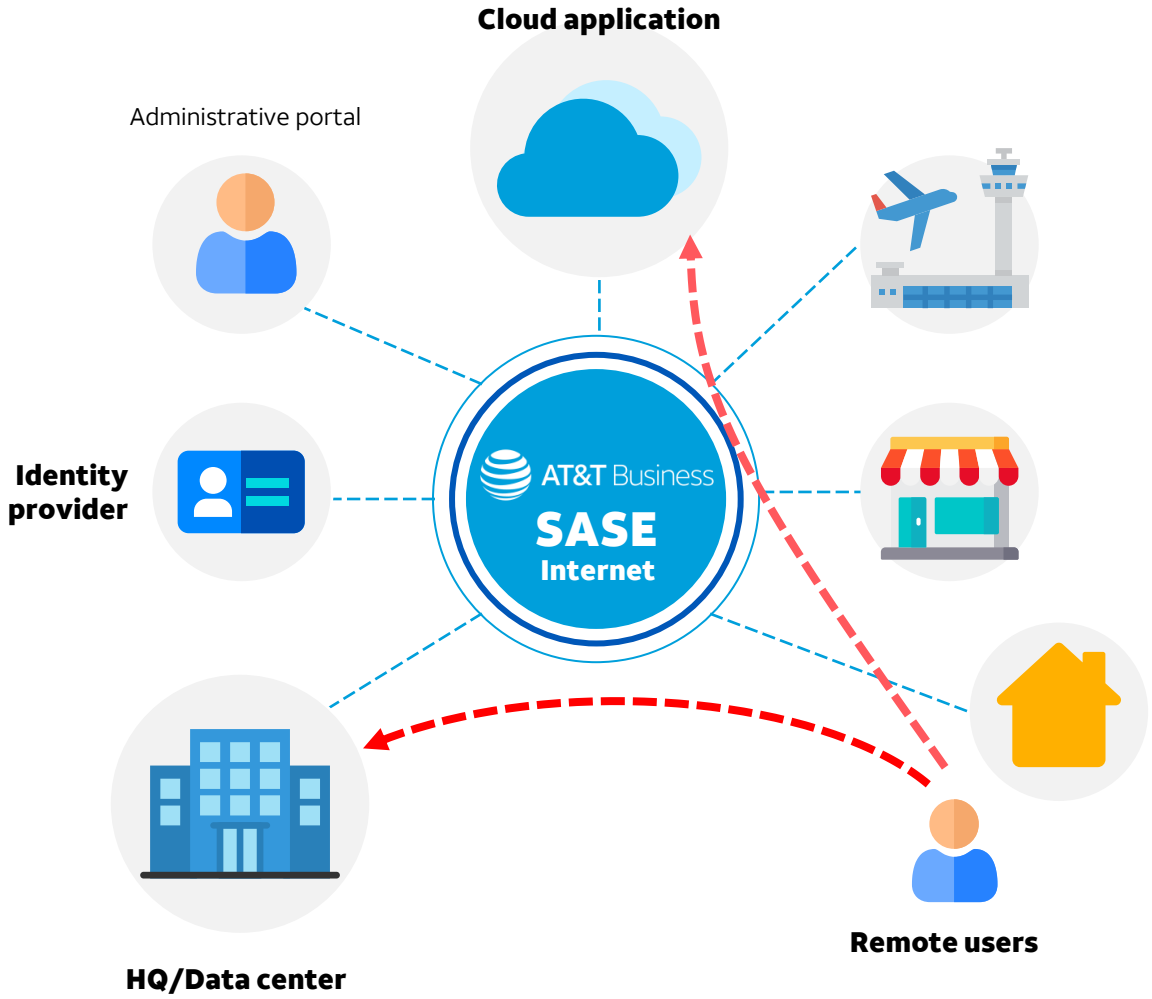
- Legacy virtual private networks (VPNs) were never designed to support a large percentage of the work force connecting simultaneously. As a result, users may find it difficult to connect to VPN at all, or experience sluggish connections.
- Users work from many locations, using company-issued and personal devices. They may work off-network or use company devices for purposes completely unrelated to work.

How AT&T SASE can help

- Reduce unauthorized access by providing identity-based access to precise applications and data users require to do their job
- Enhance user experience by connecting users directly to cloud applications without hairpinning traffic to the data center
- Enable safer internet browsing with cloud-based security that protects users from web-based threats, including zero-day attacks, regardless of how or where they connect

SASE use cases / October 2021 / © 2021 AT&T Intellectual Property - AT&T Proprietary

Use case 3 Remote workforce - How does it work?



Reduce unauthorized access

By integrating with the corporate identity provider, Secure Access Service Edge (SASE) applies zero trust network access (ZTNA) principles that specify what may be accessed, by who, when, and how.

Users connect to global SASE points of presence (PoPs) using an endpoint client or clientless virtual private network (VPN) access.

Recommended solution: AT&T SASE with AT&T Secure Remote Access, identity provider

Enhance user experience

Remote users connect directly to cloud applications over the internet, minimizing latency and removing other bottlenecks.

Recommended solution: AT&T SASE with AT&T Secure Remote Access

Safer Internet browsing

Users are protected from malicious websites and other web-based threats, including zero-day attacks with sandboxing and remote browser isolation technologies.

Recommended solution: AT&T SASE with AT&T Secure Remote Access, endpoint and mobile security

Use case 4

Identity-based application access

How it works

Overview

Employees and third-parties need access to applications and data in order to perform their job duties and serve customers. These applications may be hosted in the data center, hosted in public or private clouds, or delivered via software-as-a-service (SaaS).

Business challenge

- Legacy virtual private networks (VPNs) were never designed to support a large percentage of the work force connecting simultaneously. As a result, users may find it difficult to connect to VPN at all, or experience sluggish connections.
- Users often gain access to an entire network segment, which is more than required and may needlessly expose sensitive information.

How AT&T SASE can help

- Enhance user experience by connecting users directly to cloud applications without hairpinning traffic to the data center
- Reduce unauthorized access by providing identity-based access to precise applications and data users require to do their job
- Inhibit the effects of malware by minimizing access to the network

AT&T Business

Use case 4 Identity-based application access - How does it work?

Enhance user experience

Branch and remote users connect directly to cloud applications over the internet, minimizing latency and removing other bottlenecks.

Recommended solution: AT&T SASE with AT&T Secure Web Gateway and AT&T Secure Remote Access

Reduce unauthorized access

By integrating with the corporate identity provider, Secure Access Service Edge (SASE) applies zero trust network access (ZTNA) principles that specify what may be accessed, by who, when, and how.

Users connect to global SASE points of presence (PoPs) using an endpoint client or clientless virtual private network (VPN) access.

The identity provider provides authentication and authorization, as well as conditional access.

Recommended solution: AT&T SASE with AT&T Secure Web Gateway and AT&T Secure Remote Access, identity provider

Inhibit the effects of malware

Users are protected from malicious websites and other web-based threats using content scanning and an intrusion prevention system (IPS). Protection from zero-day attacks with sandboxing and remote browser isolation technologies. Protection of endpoints using with advanced endpoint detection and response.

Recommended solution: AT&T SASE with AT&T Secure Web Gateway and AT&T Secure Remote Access, endpoint and mobile security

Use case 5

Safer internet browsing

How it works

Overview

Many organizations are modernizing their network by connecting branch locations directly to the internet, using multiple widely available transport circuits, then deploying software defined wide-area network (SD-WAN) to manage the data flows.

Business challenge

- Users are highly distributed, conducting business from many locations using company issued and personal devices
- Employees often work off-network, connecting to the internet directly to accomplish whatever work is possible without connecting to virtual private network (VPN), which bypasses premises-based security controls

How AT&T SASE can help

- Enable safer internet browsing with cloud-based security that protects users from web-based threats, including zero-day attacks, regardless of how or where they connect
- Enforce acceptable use policies to reduce productivity loss from time-wasting websites and block those that are inappropriate for the workplace
- Reduce risk by decrypting Secure Socket Layer (SSL) packets to validate that they are free of malware before allowing them onto your network

Use case 5 Safer internet browsing - How does it work?

Enable safer Internet browsing

Users are protected from malicious websites and other web-based threats using content scanning and an intrusion prevention system (IPS). Protection from zero-day attacks with sandboxing and remote browser isolation technologies. Protection of endpoints using with advanced endpoint detection and response.

Recommended solution: AT&T SASE with AT&T Secure Web Gateway and AT&T Secure Remote Access, endpoint and mobile security

Enforce acceptable use policies

Block or restrict access to time-wasting websites that reduce productivity, as well as those inappropriate to the business.

Prioritize bandwidth for business-critical applications.

Recommended solution: AT&T SASE with AT&T Secure Web Gateway

Reduce risk by decrypting SSL packets

Malware is often hidden inside encrypted sessions and legacy decryption methods using on-prem appliances had serious throughput limitations. Decrypt sessions using cloud-based capabilities with the required scale.

Recommended solution: AT&T SASE with AT&T Secure Web Gateway

Use case 6

Inspection of web traffic

How it works

Overview

The vast majority of today's web traffic is encrypted. Encryption technology has been an asset in the protection of privacy for individuals and businesses alike and helps to ensure that any sensitive information captured in a man-in-the-middle attack cannot be disseminated.

Business challenge

- Bad actors are take advantage of the cloak this service provides by hiding various malware in encrypted files in order to bypass network perimeter security.
- Many businesses aren't performing deep packet inspection on Secure Socket Layer/Transport Layer Security (SSL/TLS) traffic originating from the web because of the impact to performance this function has on the firewalls.

How AT&T SASE can help

- Offload SSL decryption to the cloud, removing the burden of inspection from firewalls, with minimal impact to network performance
- Reduce the number of products to purchase and maintain by eliminating the need for dedicated SSL/TLS decryption appliances

SASE use cases / October 2021 / © 2021 AT&T Intellectual Property - AT&T Proprietary

Use case 6 Inspection of web traffic - How does it work?

Offload SSL decryption to the cloud

Secure Socket Layer (SSL) inspection is very processor intensive and performing it at multiple locations is extremely expensive and creates throughput bottlenecks.

Secure Access Service Edge (SASE) performs SSL inspection in the cloud at 'cloud scale,' providing visibility without the performance impairment.

Recommended solution: AT&T SASE with AT&T Secure Web Gateway and AT&T Secure Remote Access

Reduce the number of SSL inspection engines

Performing SSL inspection on multiple appliances is expensive, difficult to upgrade, complex to manage, and often introduces performance bottlenecks.

Providing cloud-based SSL inspection ensures that resources are available, packets are decrypted just once, as well as centralized management and visibility.

Recommended solution: AT&T SASE with AT&T Secure Web Gateway and AT&T Secure Remote Access

AT&T Business