

SASE: A stronger, more secure network, no matter your size

Robust connectivity and security that easily scales to meet the needs of your growing business



Potential benefits

- Improved user experience and productivity
- Increased network performance and resiliency
- Reduced risk of unauthorized access, malware, and data loss
- Centralized visibility into what is occurring on-site and within the network
- Highly scalable to flex as business needs change
- Decreased burden on lean in-house technology teams

A shift in the IT landscape

In this new and modern world we live in, the need for consistent, high-performance connectivity has never been greater. Employees and contractors conduct business from multiple locations and devices, while customers interact with kiosks and connect to Wi-Fi to shop or browse the internet. Further complicating things, we now rely on a wide range of Internet of Things (IoT) devices to drive efficiencies, including everything from security cameras to medical devices and manufacturing equipment. While this agility drives improved productivity and user experiences, it also makes security complex, particularly for resource-constrained small- and mid-sized businesses. Threats, including ransomware and phishing attacks, are increasing in sophistication and frequently target smaller businesses that don't have the same level of protection as their larger counterparts.

A new approach to creating an exceptional user experiences

In this new working environment, businesses—no matter their size—need flexible, scalable, and consolidated solutions that enable secure work from anywhere. Small and mid-size businesses, in particular, require a network that can expand as they designate new workplaces, grow in size, or experience other changes. They also need high-performing, resilient, and secure networks that protect against cybersecurity threats and continue supporting many concurrent users and devices, even in an outage.

Network solutions must provide visibility into which applications are being accessed and where sensitive data is being stored. They must also control access, so companies can be confident that their sensitive data and communications are secure—or react quickly if they're not. Network solutions must be agile, cloud-based technologies that don't compromise security or compliance while providing actionable customer insights that can be used to grow the business.

Connecting and protecting every user, device, and network edge

AT&T SASE with Cisco Meraki can provide simple and powerful networking and security for companies of any size. This solution enables unified, secure, and consistent access to every user, wherever they're located. As a holistic approach to networking and security service delivery, AT&T SASE with Cisco Meraki connects and protects every edge of the network—data centers, branch locations, IoT devices, public and private cloud—with one cloud-delivered platform.

<h3>AT&T Business Wi-Fi with Cisco Meraki</h3>	<h3>AT&T Secure Remote Access with Cisco</h3>	<h3>AT&T Secure Web Gateway with Cisco</h3>
<ul style="list-style-type: none"> Optimized wired and wireless connectivity Site-to-site virtual private network (VPN) in just 3 clicks that secures users in any location Support for multiple network circuits with the ability to prioritize bandwidth to business-critical applications 	<ul style="list-style-type: none"> Verifies user identity and device health before allowing connection to company resources and sensitive information Provides secure access to specific applications users need to complete job duties 	<ul style="list-style-type: none"> Cloud-delivered security that protects users from web-based threats, wherever they are located Blocks access to malicious, inappropriate, or time-wasting websites
<h3>AT&T Managed Services</h3>		<ul style="list-style-type: none"> AT&T Business network and security experts provide deployment, policy design and configuration, maintenance, 24x7 monitoring and help desk support to reduce the burden on lean in-house technology teams.

Challenges

The adoption of cloud applications and the number of connected devices are causing latency and an inconsistent user experience

Benefits

High-performing, resilient, and secure networks that accommodate wired or wireless connectivity, actionable customer insights, and IT agility

Use case: Secure edge

The diagram illustrates the 'Secure edge' use case. A central box labeled 'AT&T SASE WITH CISCO' contains three components: 'AT&T Secure Web Gateway with Cisco', 'AT&T Secure Remote Access with Cisco', and 'AT&T Business Wi-Fi with Cisco Meraki'. Arrows from this central box point to three cloud icons representing 'Internet', 'SaaS', and 'Private/Public cloud'.

Challenges

Legacy remote access technology is straining under increased demand, and users may be working off-network, accessing malicious websites and opening the door for hackers and malware

Benefits

High-performance access to applications hosted at the data center or in the cloud and security that follows users wherever they work, on network or off

Use case: Secure remote workforce

The diagram illustrates the 'Secure remote workforce' use case. A central box labeled 'AT&T SASE WITH CISCO' contains two components: 'AT&T Secure Web Gateway with Cisco' and 'AT&T Secure Remote Access with Cisco'. An icon of a house with a Wi-Fi signal is connected to the box. Arrows from the box point to three cloud icons representing 'Internet', 'Public cloud/SaaS', and 'Private apps/nets Co-location nets'.

Network and security expertise at scale: Managed Services from AT&T

When it comes to complex security challenges, it can be difficult to know what to do next. AT&T Managed Services takes the guesswork out of combating cyberthreats while strengthening your response to attack. With configuration, monitoring, maintenance and help desk support in the hands of AT&T cybersecurity experts, you can stay focused on delivering value to your business' bottom line.