Market trends driving the shift to software-centric cloud networking and security

AT&T Secure Access Services Edge (SASE)

Corporate Data Centers

Many businesses now have more users and applications located outside of the data center than within Networks and security need to be transformed to offer low-latency access and unified security

Remote/Mobile Workers

Users, sensitive data, and network access will be highly distributed across company owned and personal devices The future of work will be "mobile first" and from anywhere

Zero Trust Network Architecture

Organizations can no longer operate under the old model of everyone within the network being trusted and simply guarding the perimeter against external threats Security controls are moving closer to the data with the assumption that traffic is untrusted unless explicitly defined

Corporate Data Centers

Many businesses now have more users and applications located outside of the data center than within Networks and security need to be transformed to offer low-latency access and unified security

What is driving the trends?

New Data Center Markets Emerge	A more mobile and remote workforce	Focus on security first approach to architecture	Adoption of SaaS and cloud-based applications
Hyperscale cloud platforms expand their physical infrastructure to metros	**62%** of employed Americans are working from home	**95%** of enterprises are in various stages of a Zero Trust initiative in their network	**94%** of companies use more than one cloud platform
-Data Center Knowledge	*-Gallup*	*-AT&T Cybersecurity Insights Report*	*- Palo Alto Networks*

AT&T Cybersecurity

Legacy Static Network VS Modern Enterprise Network

The past was a Static Network

Legacy network architecture is generally charaterized as a well-defined, static, wired, finite network perimeter. The firewall is the gateway to the perimeter. Accessing cloud served applications and services require a hair-pin turn at the datacenter gateway firewall. Remote users utilize legacy VPN tunnels to access the network. Security is considered inherent once a user authenticates with the firewall via Active Directory authentication. Cloud Access Security Brokers are a thing of the future and thus not used or poorly integrated with the legacy network. Therefore, making accessing and properly securing cloud and SaaS workloads nearly impossible. This network architecture only truly protects data that resides inside the perimeter of the environment.

Intelligent secure connected network for the **HYPER-DISTRIBUTED** *enterprise.*

Network of The Modern Enterprise

The network of the modern enterprise is also a well-defined network architecture that deploys software-defined resources to ensure "on the fly" flexibility, CASB integrated cloud, and SaaS workloads, Software-defined Wide Area Networking (SDWAN) that monitors latency, jitter, line condition and identifies applications at the layer-7 to ensure that the proper class of service is assigned. Doing so dynamically ensuring that the end-user gets the best possible user-experience from the network. Authentication is performed at the cloud level security stack so that users can have a secure experience in the network, while ensuring that data throughout the network is properly protected.

User centric, dynamic, elastic, multi access, **SOFTWARE-DEFINED PERIMETER**

Legacy Static Network hexagons

Increasing complexity — Additional features mean more hardware and software. Equating to more complexity integrating disparate systems together.

Higher latency — No peering agreements at the carrier level. Only Best available internet speeds and feeds.

Higher opex costs — More infrastructure means more operational costs for things like power, shelter and man-power.

Lack of flexibility — Static on premise boxes that are inflexible. No on the fly upgrades.

No Application Layer Security — Lack of security at the application layer and failure to address user experience

Lack of Advanced Networking — Lack of advanced software-defined networking to connect on-demand, with the appropriate level of security continuously protecting proprietary data.

Modern Enterprise Network hexagons

Increased Performance — Through latency-optimized routing, reduces number of hops and singular insertion of policies on the wire

Ease Of Use — Consistent access experience regardless of user location and types of apps accessed

Reduce Complexity & Costs — Consolidate highly secure network access services from single provider. Reduce number of appliances in the branch

Reduce Customer OPEX — Customers without large IT staffs and expertise, SASE does all the work for them. SASE cloud is providing instant connections

Enable Zero Trust Network Access — Evaluates trust every time a device or user requests access to a resource through multi-factor authentication

Improve Security — Apply content inspection such as scanning for sensitive data using consistent policy regardless of where the user/device is located

---

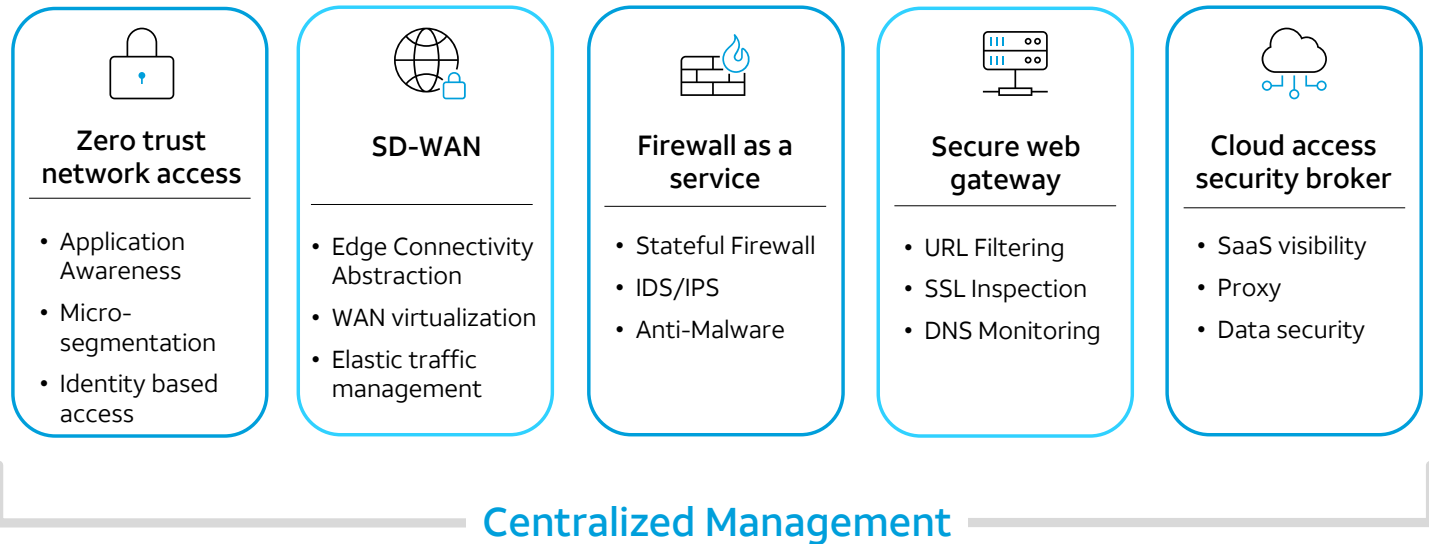**85%** Organizations operating in a multi-cloud environment today.

40% By 2024, at least 40% of enterprises will have explicit strategies to adopt SASE.
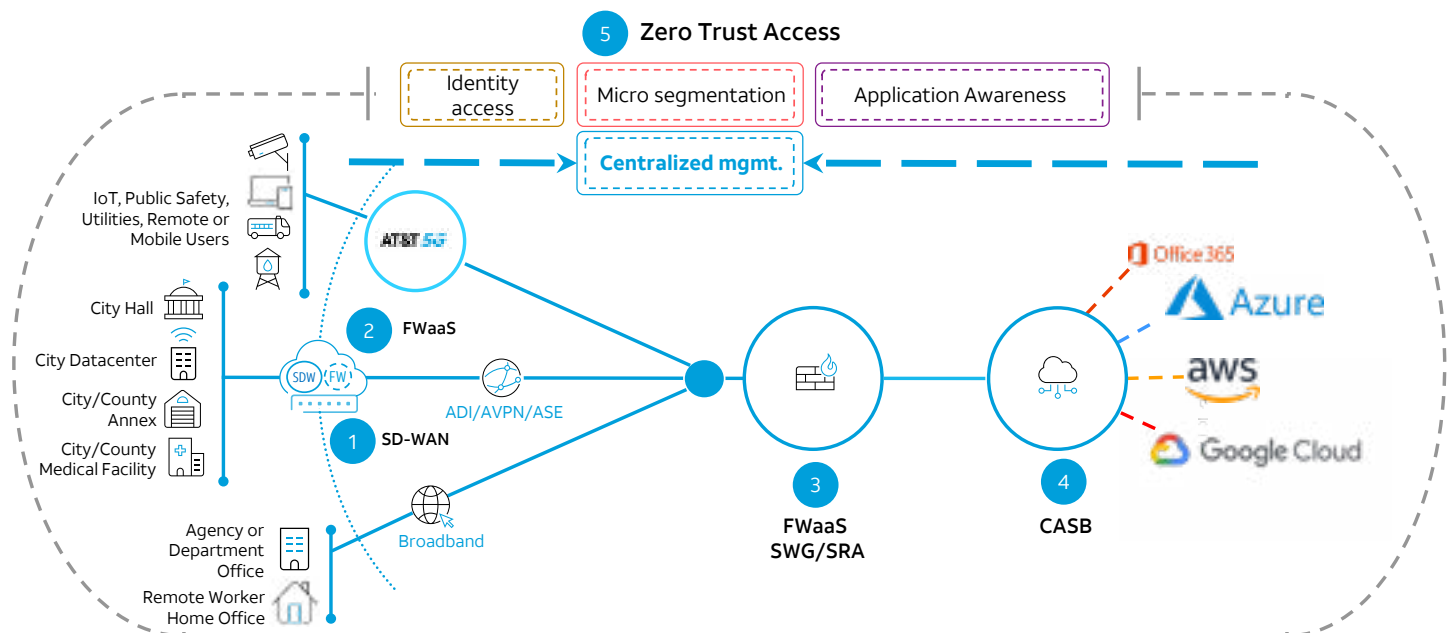
82% Post COVID, 82% of companies plan to allow employees to work remotely - some of the time.

Core technologies in a Secure Access Service Edge (SASE) framework

Zero trust network access
- Application Awareness
- Micro-segmentation
- Identity based access

SD-WAN
- Edge Connectivity Abstraction
- WAN virtualization
- Elastic traffic management

Firewall as a service
- Stateful Firewall
- IDS/IPS
- Anti-Malware

Secure web gateway
- URL Filtering
- SSL Inspection
- DNS Monitoring

Cloud access security broker
- SaaS visibility
- Proxy
- Data security

Centralized Management

The Roadmap to Secure Access Service Edge (SASE) with AT&T

5 Zero Trust Access

Identity access | Micro segmentation | Application Awareness

Centralized mgmt.

AT&T 5G

IoT, Public Safety, Utilities, Remote or Mobile Users

City Hall

City Datacenter

City/County Annex

City/County Medical Facility

Agency or Department Office

Remote Worker Home Office

SDW FW

2 FWaaS

ADI/AVPN/ASE

1 SD-WAN

Broadband

3 FWaaS SWG/SRA

4 CASB

Office 365

Azure

aws

Google Cloud

AT&T named Global Leader among MSSPs 2021
IDC

Ranked #1 MSSP among top 250 MSSPs in 2020
MSSP*Alert*

J.D. Power Recognizes AT&T in Customer Satisfaction Rankings 2020

AT&T named #1 Managed SD-WAN provider in North America 2020
Frost and Sullivan

AT&T Cybersecurity