The next evolution in zero trust access and protection

Potential benefits

- Granular access control at the application and sub-application level helps ensure that users can only connect to what's needed to complete job duties
- Continuous trust verification can ID suspicious behavior and revokes access in real time
- Deep, ongoing security inspection monitors all traffic for indicators of compromise
- Single data loss prevention (DLP) policy protects information stored across premises-based and cloud-hosted locations
- Secures applications across the organization (private, cloud, and SaaS)
- AT&T managed services certifies features, assists with deployment, and handles day-to-day maintenance

Convenient access for employees—and threat actors

Once a luxury, it's now essential for many companies to offer employees the option to work from anywhere, on any device. This has led to the rise of the hybrid workforce—with highly distributed data and, on average, 110 SaaS applications per organization.[1]

Unfortunately, many businesses are finding that their traditional remote access solutions were not designed to support so many concurrent users and are straining under the increased workload, resulting in latency. They also commonly grant access to an entire network segment, needlessly exposing sensitive information and opening the door for the spread of malware. To bypass these rigid and slow processes, users often work off-network, which bypasses perimeter-based security. And while cloud applications may unlock new capabilities, they frequently create a blind spot for administrators charged with protecting sensitive data.

Zero trust network access is no longer enough

Zero trust network access (ZTNA) sought to address these pain points by granting consistent, high-performance access to specific applications wherever users chose to connect. But this "silver bullet" for network security is limited in what it can protect.

The first generation of ZTNA solutions identify applications based on broad constructs like port number and IP address, which can be a problem with programs for which those are dynamic. Once it verifies that a user is permitted access to an application, it simply makes the connection and stops there, which gives opportunity to insider threats. ZTNA was designed purely as an access control mechanism; therefore, it does not have the ability to detect or act against malicious traffic and—similar to its predecessor—provides no visibility or capability to protect data stored in the cloud.

Zero trust for today's highly distributed business environment

AT&T Secure Remote Access and AT&T Secure Web Gateway, both powered by Palo Alto Networks, solve these shortcomings. Together in one package, they bring you the next iteration of Zero Trust: ZTNA 2.0.

ZTNA 2.0 uses the most stringent enforcement of the principle of least privilege, allowing businesses to apply granular permissions to specific functions of an application while delivering continuous trust verification in real-time to identify suspicious behavior and revoke access. Constant security inspection monitors all traffic, including allowed connections, for indicators of compromise. A single data loss prevention (DLP) policy protects sensitive information wherever it is stored, and all applications are secured—including those with dynamic ports and server-initiated connections.

Expected outcomes

- Increased productivity and better user experience
- Reduced risk of security breach and data loss
- Decreased burden on in-house technology teams
- Improved flexibility to accommodate new users, locations, and workplace designations

ZTNA 2.0 is at the core of AT&T SASE powered by Palo Alto Networks, a modular and integrated architecture to support digital transformation with rigorous security enforcements. It provides a great user experience with a truly cloud-native architecture built to secure today's digital enterprises with a unified access and protection at cloud scale.

AT&T Managed Services

These ZTNA 2.0 solutions are offered as an AT&T managed service:

- Feature certification and interoperability testing
- Deployment services, including configuration and security policy design
- 24x7 help desk support and monitoring by our eight global security operations centers
- Ongoing maintenance, including approved updates and security patches

Why AT&T Cybersecurity?

AT&T Cybersecurity is your trusted advisor, making it safer for your business to innovate through network resiliency. We help to design, deploy, and manage the highly secure network that you aspire to, by proactively identifying areas of cyber risk and preventive measures to protect digital connections.

[1] "Average number of software as a service (SaaS) applications used by organizations worldwide from 2015 to 2021," Statista, February 16, 2022, https://www statista com/statistics/1233538/average-number-saas-apps-yearly/