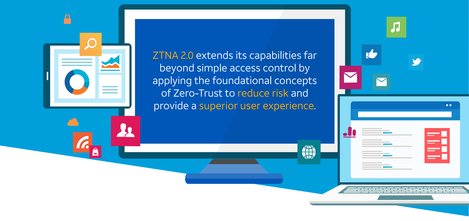
AT&T Business | paloalto NETWORKS

The next evolution of Zero Trust

Work is an activity, not a place.

Traditional Zero Trust network access (ZTNA) enables organizations to provide consistent, high-performance access to applications wherever users choose to connect, **but that's where it leaves off—still giving too much access while providing too little, inconsistent security.**



ZTNA is built around 5 key principles.

1 Least privilege access

Applications are identified based on app-IDs at layer seven, which enables the ability to grant access at a sub-application level.

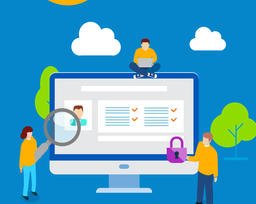
2 Continuous trust verification

Once access is granted, trust is continuously assessed based on changes in device posture, user behavior, and application behavior.

3 Continuous security inspection

Provides deep and ongoing inspection for all traffic, including allowed connections, to protect against threats and threat vectors.

4 Comprehensive data protection



Consistent data protection across applications, whether hosted in the data center or the cloud with a single data loss prevention (DLP) policy.

5 Complete application security

Protection and security for applications across the organization, including private, cloud, and SaaS.

Introducing the next evolution in managed security

AT&T Secure Remote Access and AT&T Secure Web Gateway—both powered by Palo Alto Networks—come together to bring you ZTNA 2.0.

- Enhanced user experience
- Limit access to only required applications and data
- Inspect traffic for indicators of compromise
- Identify suspicious behavior to revoke access in real time
- Protect sensitive data against loss or unauthorized sharing
- Reduce the burden on lean technology teams with AT&T managed services

Find out how ZTNA 2.0 can help secure your hybrid workforce.