# 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 2.0 extends its capabilities far beyond simple access control by applying the foundational concepts of Zero-Trust to reduce risk and provide a superior user experience.

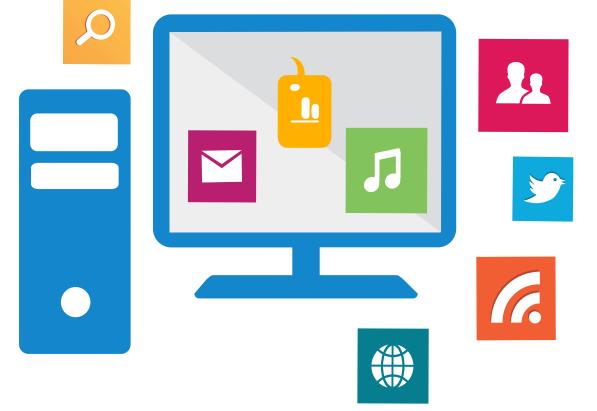
#### ZTNA 2.0 is built around 5 key principles.



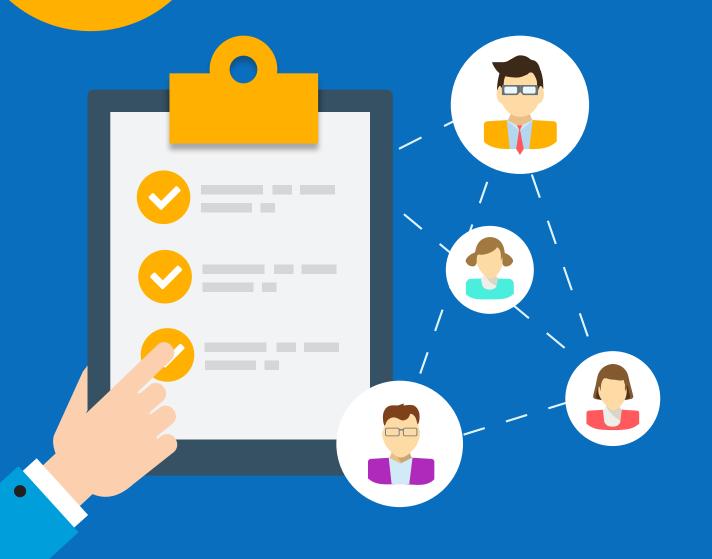


Applications are identified based on app-IDs at layer seven, which enables the ability to grant access at a sub-application level.

2



#### Continuous trust verification



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

3

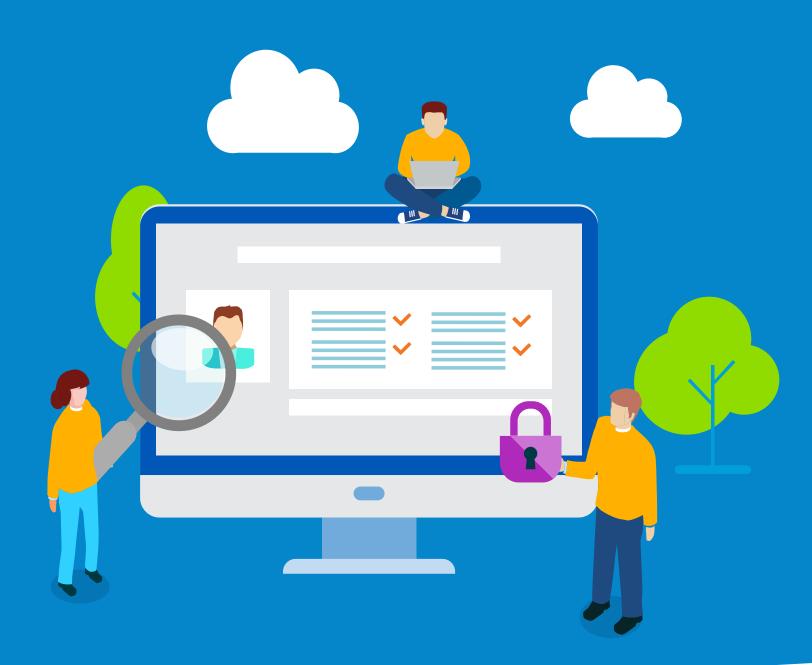
2

#### Continuous security inspection

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



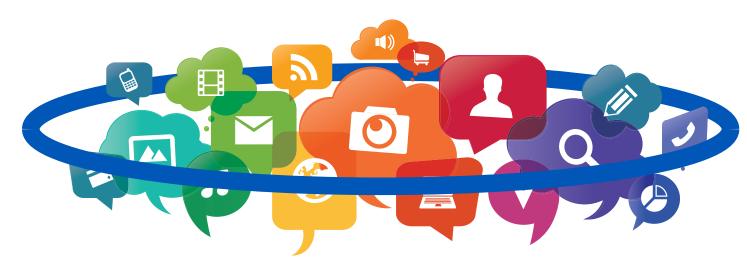
### Comprehensive data protection



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

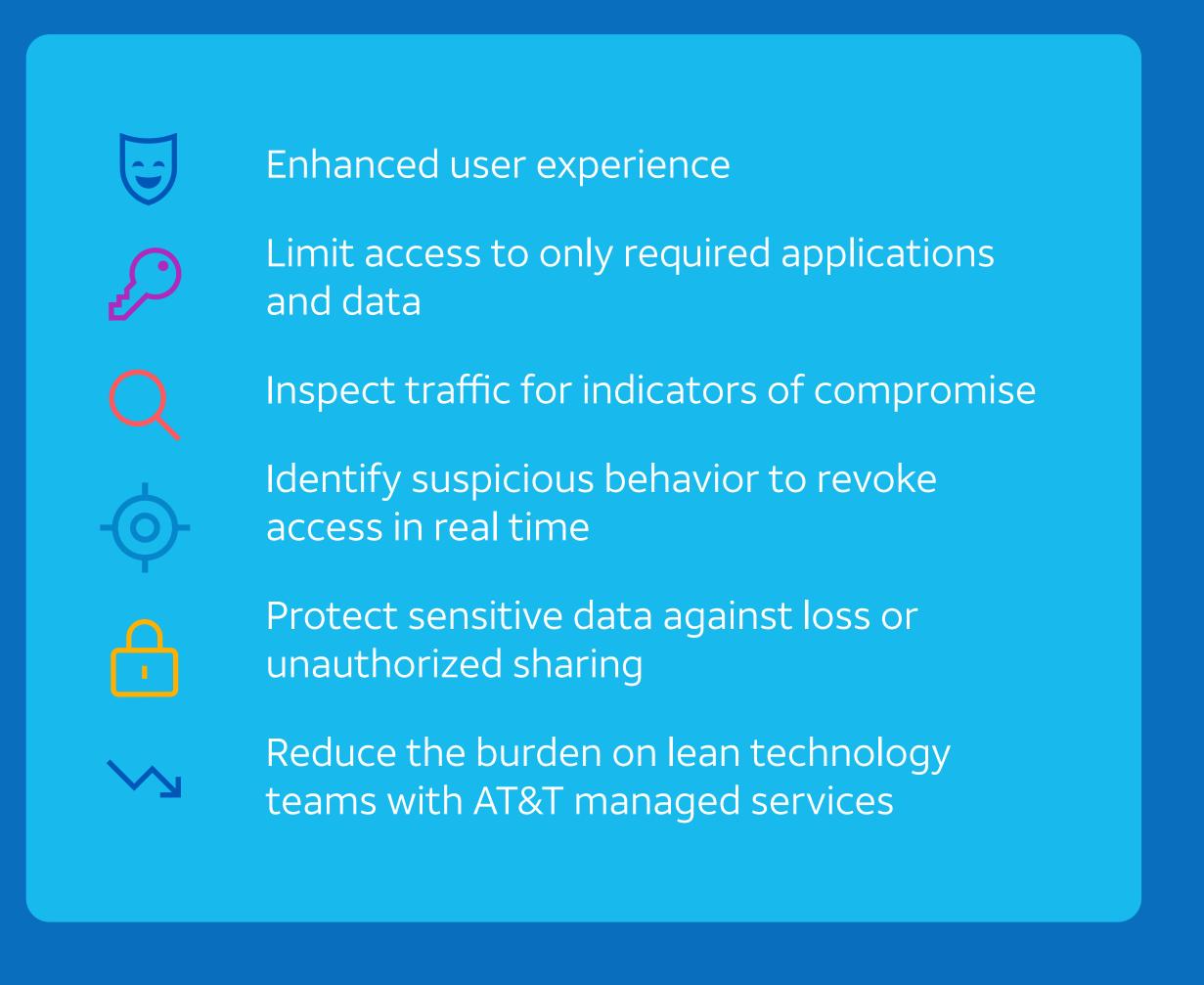
## Complete application security

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.



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



© 2022 AT&T Intellectual Property. All rights reserved. AT&T, Globe logo and other marks are trademarks and service marks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein 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.

© 2022 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at https://www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.