SECURING ACCESS TO YOUR APPS WITH A ZERO TRUST APPROACH

DYNAMIC ACCESS TO ENTERPRISE APPS AND DATA WITH LOOKOUT ZERO TRUST NETWORK ACCESS

Remote employees expect seamless access to what they need

Cloud-based infrastructure has enabled your employees to be productive from anywhere on any device. This has driven the need for seamless access to corporate data to get their work done.

Traditional security models assume every user and device inside the network can be trusted — but that puts your infrastructure at risk. Once a user is inside your perimeter, they have nearly unrestricted access to everything. This means your data is vulnerable to anyone capable of gaining access to the involved network, system, or applications.

Secure remote access needs to be dynamic

Your workforce is no longer bound by a traditional network perimeter. With more of your data and apps now in the cloud, your employees can stay productive regardless of the network or the device they use.

Many organizations have turned to virtual private networks (VPNs) to support remote workers, but this approach falls short in a number of ways. First, VPNs give whomever is connected unrestricted access without the contextual awareness of who or what wants access.

BENEFITS

- Granular identity and context-aware access controls
- Consistent security and user experience across onpremise, IaaS and SaaS applications
- Application-centric control limits access only to those who need it
- Application cloaking prevents discovery on the public Internet
- Extends advanced security to legacy applications with identity and access management
- Agentless access from any endpoint device

Second, they don't understand whether the device connecting into the network is free of malware or if the user is who they say they are.

Third, a VPN can also give access to other devices connected to the user's network that are frequently not under your control.

Securing access with Lookout Zero Trust Network Access

Lookout Zero Trust Network Access (ZTNA) continuously monitors the identity of those requesting access to your apps and understands what they need for work. These insights enable a Zero Trust approach, providing dynamic identity and context-aware access to data depending on the risk level of the user and device.

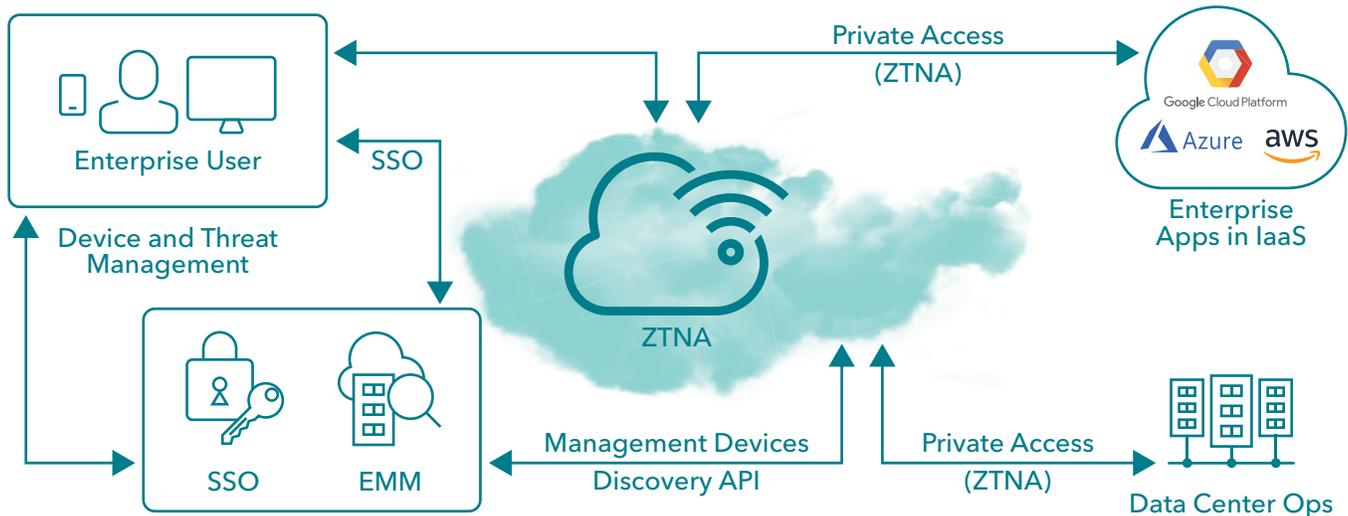### Context-aware access policies at the user and device level

We act on device and user behavior independently of each other as a way to create more granular context-aware policies. This helps admins reduce security risks associated with compromised devices and accounts.

Secure legacy applications with your cloud-based tools

We invoke the same strong authentication security benefits associated with SaaS applications and web services for legacy, IaaS and private applications. Lookout ZTNA integrates with multi-factor authentication and identity solutions to reduce user friction and improve overall access controls.

Isolate application access from network access with microsegmentation

Lookout ZTNA mitigates the risk of breaches caused by overentitlement of services. This also prevents threat actors from getting into your infrastructure, then moving laterally to steal more data.

Enterprise User

Device and Threat Management

SSO

SSO   EMM

Private Access (ZTNA)

ZTNA

Google Cloud Platform
Azure   aws

Enterprise Apps in IaaS

Management Devices Discovery API

Private Access (ZTNA)

Data Center Ops

Lookout

About Lookout

Lookout is an integrated endpoint-to-cloud security company. Our mission is to secure and empower our digital future in a privacy-focused world where mobility and cloud are essential to all we do for work and play. We enable consumers and employees to protect their data, and to securely stay connected without violating their privacy and trust. Lookout is trusted by millions of consumers, the largest enterprises and government agencies, and partners such as AT&T, Verizon, Vodafone, Microsoft, Google, and Apple. Headquartered in San Francisco, Lookout has offices in Amsterdam, Boston, London, Sydney, Tokyo, Toronto and Washington, D.C. To learn more, visit **www.lookout.com** and follow Lookout on its **blog**, **LinkedIn**, and **Twitter**.

For more information visit
lookout.com

Request a demo at
lookout.com/request-a-demo

Integrated endpoint-to-cloud security

Learn more at **lookout.com**

Lookout®