BEST PRACTICES:

ZTNA

Zero Trust Network Access

These best practice principles of ZTNA should always be top-of-mind:

- → Grant access using the principle of least privilege.
- → Verify identity with MFA and cloud IdPs.
- → Set compliance requirements to manage and secure users, devices and more.
- → Never trust, always verify for continuous verification even following initial access.

If you’re just getting started with modern identity and access, read on to learn how to set the course for your modern identity and access strategy.

You walk into your bank to make a withdrawal. Your identity is verified with your account number and your ID; if your name is on the account, you're given access to that account, and that account only. Now imagine: you hand over your ID and the teller leads you directly to their vault with all the contents for your taking. Sounds crazy, right? So why would you do that with your network access?

A VPN (virtual private network) gives users access to your entire network, regardless if they need holistic access or not; this puts your data at risk. **Zero Trust Network Access (ZTNA) locks down the vault of your company information by providing least-privilege access to only the resources employees need while strictly verifying user and device identity for each application.** It also reduces bandwidth demands to your network and preserves user privacy by split tunneling. In other words, VPN has got to go.

So how does ZTNA work? At its most basic, it demands to know:

1. **Identity:** Who are you, are you who you claim to be and do you have authorization?
2. **Security:** Is your device secure?
3. **Context:** Are you requesting access to only the resources you need?

Implementing successful ZTNA technology needs to address these questions. ZTNA requires both the user and their device to prove their identity. The device must be a known and authorized device. This can be accomplished by enrolling the device tied to a specific user into your device management solution. The user must also provide correct credentials and responses to their cloud identity provider's multi-factor authentication.

Despite identity verification, it's important to ensure devices are secure to mitigate further risks when attempting to access company resources. This means that devices should be in compliance with your security policies and should have the latest operating systems and vulnerabilities patched.

Once identity and security have been verified, users are granted access to the applications they need. In ZTNA architecture, users can only see what they have permission to access. To achieve this, only pre-approved apps are provisioned to each user. This way, you know that when users try to access these apps, they already should have permission.

Jamf does all of this for you: device management, app provisioning, integrations with cloud identity providers, software updates, endpoint protection and more. Learn more about how we seamlessly deliver ZTNA in our Zero Trust Network Access for Beginners e-book.

Want to lock down your data with ZTNA? Learn about how to accomplish this, and more, with Jamf's Trusted Access.

jamf

www.jamf.com