jamf

ZTNA and Trusted Access:

Best practices for identity access and security compliance

Zero Trust has taken the cybersecurity world by storm. According to **Okta's The State of Zero Trust Security 2022** report, the percentage of companies developing or implementing Zero Trust in the next 12-18 months rose from 16% in 2019 to 97% in 2022. The elimination of the network perimeter that resulted from the pandemic's rise in remote work made Zero Trust architecture a need, not just a nice-to-have.

Zero Trust Network Access, or ZTNA, is a pillar of a Zero Trust implementation. Think of Zero Trust architecture as your multi-chambered, locked-down castle hosting your network — ZTNA is the garrison verifying the identity of any guest, opening the gate and escorting them to the chambers they're permitted to access. If the guest's intentions become suspicious at any point, they're immediately removed from the premises and their permission is revoked.

Medieval analogies aside, understanding ZTNA is critical to advancing cybersecurity.

In this paper, we address:

- Granting least-privilege access
- Verifying identity with multifactor authentication (MFA) and cloud identity providers (IdP)
- Compliance and security
- Supporting the end user

Least-privilege access

The principle of least privilege is simple: users and their devices only have access to what is necessary for their job function and nothing more. On one hand, this adds to some bookkeeping since you have to keep track of who needs access to what and who currently has that access. On the other hand, you won't be spending money on an excess number of licenses. But the real power comes in reducing your attack surface — if you limit the number of users with permissions, you limit the number of accounts that can compromise your network via a given resource. This also reduces the risk of lateral movement if a bad actor does get into your network since users don't have access to your network as a whole.

ZTNA applies the principle of least privilege by creating a software-defined perimeter (SDP). An SDP doesn't separate network connections through VLAN or network address; through split-tunneling, it grants access to only the subset of resources the user has permission to access regardless of where they live on the company network. Resources the user does not have permission to access are kept invisible and inaccessible to the user.

Identity: authentication and authorization

The foundation of ZTNA is identity. "Never trust, always verify," the mantra of Zero Trust, means always forcing users and devices to prove their identity when logging into resources, regardless of the frequency or recency of a successful login.

Establishing identity in a remote environment has its challenges. Organizations can't rely on on-premises Active Directory (AD) or LDAP configurations — especially on Apple devices that AD wasn't made for. That's where cloud identity providers (IdPs) come in, like Okta, G Suite and Microsoft Entra ID.

Cloud IdPs provide the directory service wherever your users are located. Your IdP keeps track of a user's information: who they are, what their role is and what applications they have permission to access. In other words, it authenticates the user and determines their authorization to company resources.

Application-based microtunneling

When we talk about ZTNA, we often mention user identity, but another relevant aspect is application identity. Application-based microtunneling policies work behind the scenes to make ZTNA a reality. By assigning applications an identity that's network-agnostic, you achieve finer network segmentation while allowing any policies to remain valid regardless of the location of the application on an on-premises server or cloud. This makes enforcing north-south and east-west security policies easier by giving you clear visibility into the application's traffic.

Using cloud IdPs with this type of microtunneling lets you take advantage of a cloud-based implementation. You don't have to manage identity or host applications solely on your servers — your ZTNA provider can redirect the traffic as needed. This way, you don't have to maintain or supervise servers or hardware you don't want to while giving users the secure and convenient access they need.

Unified access policy

This all culminates in a unified access policy. This policy should cover all hosts relevant to your organization, whether on-premises, in a private or public cloud, within an SaaS application, on a modern OS or other management paradigm. An effective policy includes:

- Directory services and single sign-on capabilities through a cloud IdP
- Multifactor authentication
- Role-based access control following least-privilege principles
- SSO-enabled repository of allowed applications
- A control system to direct traffic to the appropriate network locations (including on-premises, cloud, SaaS and non-business web traffic)

Compliance and security

Identity is half the battle in ZTNA — the other half is compliance. You don't want to let compromised or at-risk devices have access to your company resources, even with your other safeguards in place.

So how do you ensure the devices connecting to your resources are compliant? As "zero trust" implies, you can't trust that any devices, servers or applications are free from compromise. Your access policies should include methods for identifying vulnerable and/or compromised devices.

Your compliance software can check for:

- Unpatched/vulnerable operating system or application versions
- Active endpoint protection software
- Suspicious activity uncharacteristic for the user
- Threats on the device or malicious sites accessed by the user

If a device's compliance comes into question, you can cut off their access to company resources. Implementing these compliance checks looks different depending on the device type and whether the device is company-owned or personal. Either way, the device should have some type of management software when connecting to corporate applications — though user privacy should still be respected. Bring your own (BYO) devices should route personal traffic directly, not through company monitoring software, and personal and business data should be kept totally separate for security and privacy.

Continuous verification

Verifying a device's compliance doesn't just happen at login. It's part of the "never trust, always verify" paradigm — the device could become compromised at any time. Continuous verification of a device's status is paramount; even the best-intentioned user can fall victim to a phishing attempt or malware infiltration.

The end-user experience

A ZTNA service that's clunky, hard to use and unreliable doesn't bode well for its success. If the service hinders users, it's more likely they'll try to bypass the measures you put into place to secure your resources.

However you implement ZTNA, it should be hardly noticeable to users while providing seamless and always available access to business apps. The local application on the device that manages the connection shouldn't affect battery life and should automatically establish tunnels to business applications when requested, reconnecting if there's a disruption. Not only does this make your users' lives easier (and probably happier), it prevents shadow IT from introducing hidden vulnerabilities in your infrastructure.

Using Single Sign-on (SSO) with your cloud IdP can further streamline the process by managing a user's password to any available application and simplifying the authentication process. After all, it's much simpler to remember one password and verify with biometrics or other MFA than to remember passwords to all your business apps.

ZTNA software that:

- Uses the power of SSO and cloud IdPs for simple authentication
- Works wherever resources are located on internal or external networks
- Creates secure microtunnels to an application without providing holistic access to corporate networks
- Makes apps easily and readily available when a user and device health is verified
- Protects user privacy while keeping company data secure
- Acts unnoticed by the end user is a recipe for a successful implementation that keeps users, IT and security teams happy and productive

Enter Trusted Access

While you can't blindly trust the devices on your network, you can trust that your access controls keep your users and company safe. Jamf's ZTNA solution is what your organization needs to achieve Trusted Access. Learn more about how trusted access unites device management, identity and access, and endpoint security. And see why Jamf's secure ZTNA solution is loved by admins and users alike with a free trial.

Request Trial

Or reach out to your favorite reseller to get started.

jamf

www.jamf.com