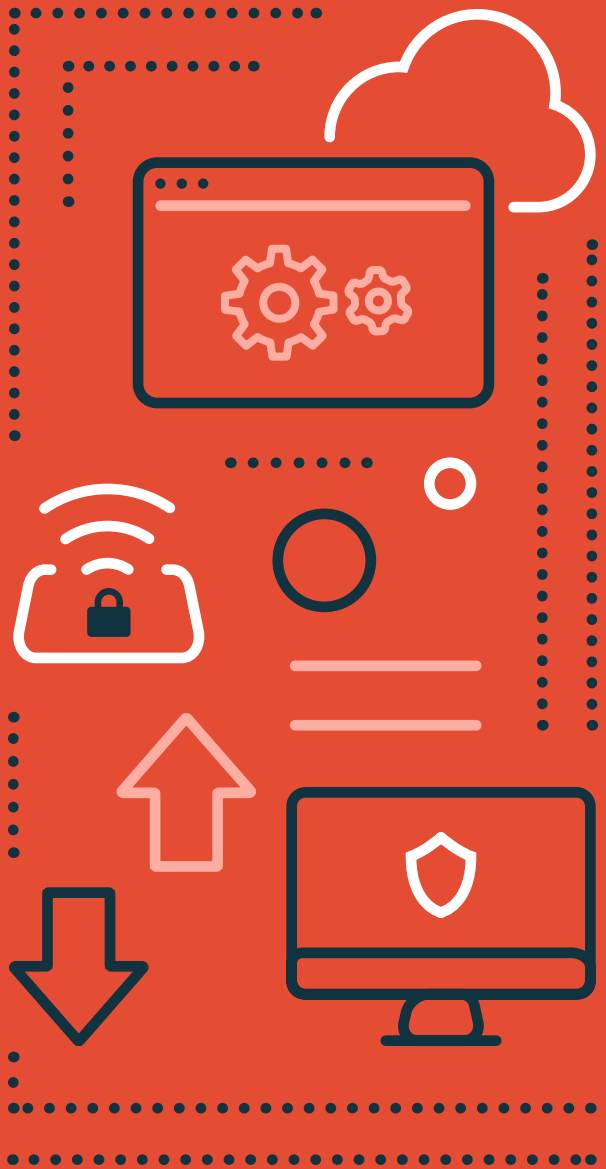


Zero Trust Network Access

for Beginners

jamf

ZERO AWARENESS OF ZERO TRUST NETWORK ACCESS? NO PROBLEM.

According to **Gartner**, Zero Trust Network Access (ZTNA) is a **product or service that creates an identity- and context-based, logical access boundary around an application or set of applications**.

In lay terms, ZTNA is the successor to Virtual Private Networking (VPN). However unlike VPN, which dates back to 1996 and based on the Peer-to-Peer Tunneling Protocol (PPTP), **Jamf Private Access was designed with modern computing in mind** by incorporating an identity-centric security model with risk-aware policy management and application-specific microtunnels. These limit access to resources users are authorized to use — all baked into a cloud-based infrastructure that both simplifies management, scales at the click of a mouse and requires no hardware to maintain.

DIVE INTO THIS E-BOOK FOR THE BASICS:

- How Jamf Private Access works
- What security features are built-in
- Why you need to reconsider your network authentication and security approach

And, where to start.

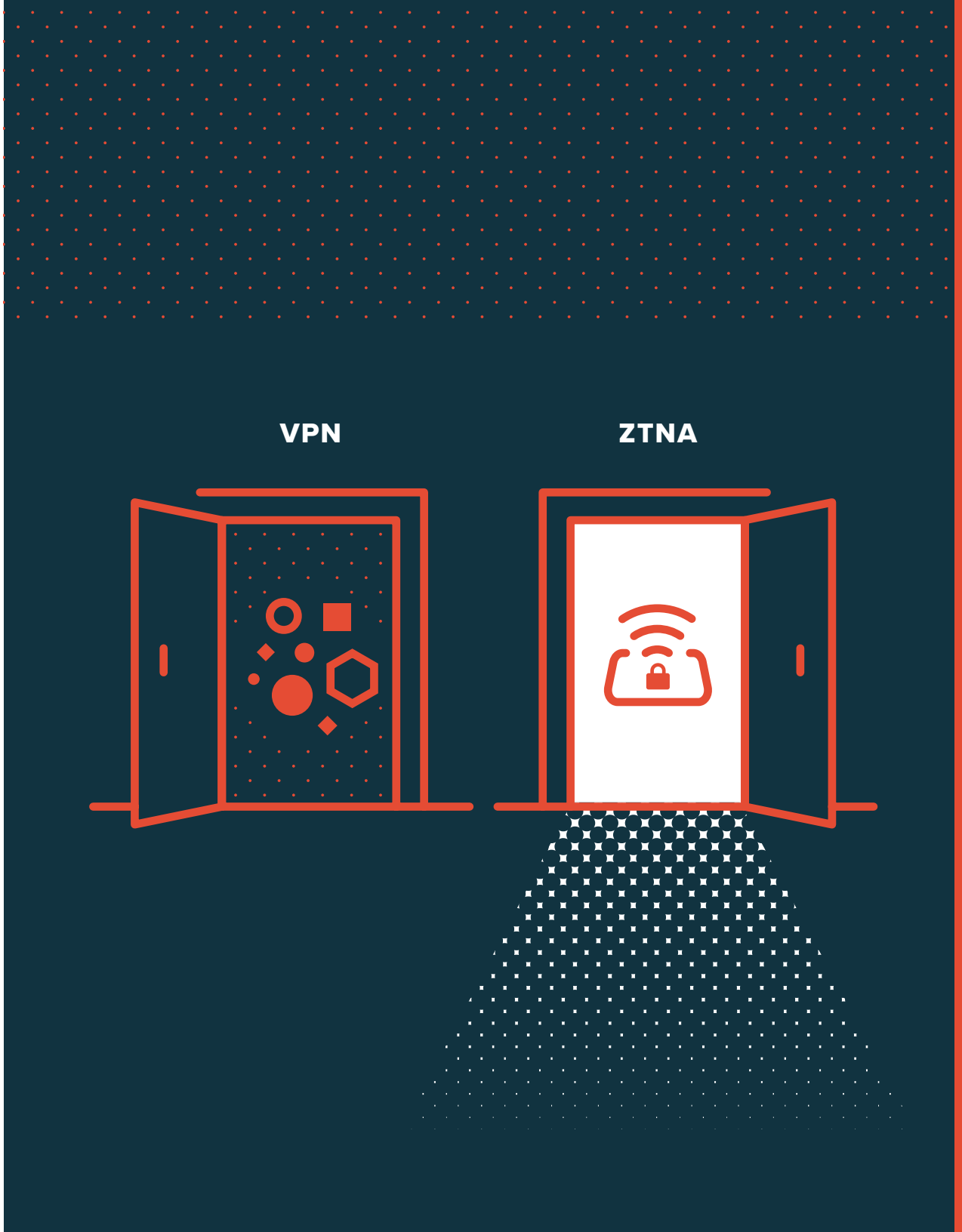
“NOBODY TRUSTS ANYBODY NOW.”

Kurt Russell’s character of R.J. MacReady in The Thing grows to distrust his fellow companions as the film goes on and the problems pile up. MacReady shares this spiritually with ZTNA in that the technology employs security configurations based on the principle of least privilege and centering around a common theme of “never trust, always verify”.

Essentially, through the enforcement of least-privilege coupled with real-time device posture checks, **cloud-based access is granted to each application only for the specific, authorized user requesting access through their unique credentials**.

This means ensuring that after a user authenticates into their device using their cloud identity credentials, business connections are secured while enabling non-business applications to route directly to the internet in a process called split tunneling, preserving end-user privacy and optimizing network infrastructure. This further optimizes the underlying network by adding efficiency to how the connection or microtunnel is established. By leveraging microtunnels, permitted users, devices and apps can be secured end-to-end. If any of the criteria, say a personal device, is not configured for access — regardless of entering the proper credentials — access to company resources will be disallowed.

Unlike VPN where access is granted holistically and provides users access to the entire network of resources, ZTNA's granular approach strengthens security by granting users access only to what they need when they need it. As a result of enhancing your organization's security through policies customized to meet compliance requirements, this provides greater, more comprehensive support to safeguarding end users, company devices and data.



“YOUR RULES ARE REALLY BEGINNING TO ANNOY ME”

Like the dichotomy presented in Escape from New York, where the infamous Snake Plissken uttered the title phrase as he is caught between the freedoms afforded to citizens and the restrictions of the law — in place to sustain peace & order — IT admins may find themselves facing a similar quandary:

How do organizations balance security protections while providing end-user access to necessary resources and data?

Jamf Private Access does exactly this.

With identity and app-centric policies that enable productivity while eliminating the broad discoverability and reachability of data and apps that users should not be able to access, Jamf Private Access ensures that unified access policy enforcement remains consistent across data centers, multiple cloud infrastructures and SaaS applications as well as to all modern operating systems (OS’s) and management paradigms.

Doubling down on hardening security through a variety of policies, risk-aware access policies enhances security by preventing access to resources, by performing recurring checks on devices to assess health data and working proactively to identify devices that may be compromised or otherwise pose a high-risk to the accessing resources securely — not to mention the overall security posture of the network.

“EVERYBODY RELAX, I’M HERE.”

Beginning with a solid, cloud-based foundation, the infrastructure employed by Jamf Private Access requires zero hardware to manage, no support contracts to navigate and doesn’t rely on installing and/or configuring complex software.

Let’s not forget that the centralized, highly scalable and instant-on nature of the cloud means that data is being protected from the second your devices are enrolled in the service — regardless of how many devices are part of your fleet or where across the globe they’re physically located. All that’s needed is a network connection.

Much like the lovable, yet somewhat aloof Jack Burton from Big Trouble in Little China, the cloud-based nature and capability-expanding integrations that power Jamf Private Access ensure that it is always hard at work, front and center, to protect your endpoints by keeping connections encrypted, monitoring device health and deploying automated workflows to remediate detected issues, keeping devices performing optimally, users and data safe.

HOW JAMF PRIVATE ACCESS WORKS

Spoiler alert: It works smarter, not harder.

One example of an integration that is critical to the ZTNA architecture is the ability to enable user authentication by way of Single Sign-On (SSO) through your preferred **cloud-based Identity Provider (IdP).** This eliminates the hassle of managing certificates for users and/or devices, in turn removing the requirement of maintaining a dedicated Certificate Authority (CA) of your own, plus all the networking hoops that are required when configuring security for this type of infrastructure in largely remote or hybrid work environments.

This allows admins to effectively leverage each device's network connection with connectivity to the cloud to "work smarter, not harder". After all, less overhead means greater efficiency, which is never a bad thing. And speaking of less overhead, the Jamf Private Access agent itself is not only built with the highest-level protection for your devices, users and data in mind, but also designed to utilize the fewest number of resources possible while doing so.

Jamf natively supports Okta and Azure natively but support all other major IdP's like Google, Ping etc via Azure federation.

PRIVATE ACCESS SECURITY FEATURES:

Identity-centric security model

Only authorized users can connect to business applications and ensure policy enforcement is consistent across data centers, clouds and Saas applications.

Application-based microtunnels

Only connect users to apps they are authorized to access. Microtunnels enforce least privilege access and prevent lateral network movement (a common vector for security breaches).

Modern cloud infrastructure

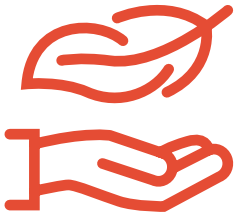
Zero hardware to manage, support contracts to renew or complex software to configure. Even eliminate the need to have administrative control of a device to enable secure access.

Integration with your identity services

Enable user authentication through single sign-on (SSO) and eliminate the need to manage certificates.

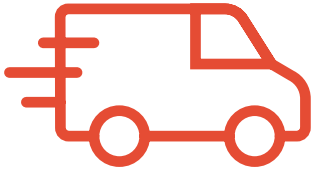
Risk-aware access policies

Enhance security by preventing access from users and devices that may be compromised.



Lightweight application

Automatically establish tunnels when applications need to connect and seamlessly reconnect if there is disruption.



Fast and efficient connectivity

Uncompromised access to business apps – without impacting battery life – and operates silently in the background without interfering with the user experience.

Intelligent split tunneling

Ensure business connections are secured while enabling nonbusiness applications to route directly to the internet, preserving end-user privacy and optimizing network infrastructure.

Unified access policy

Spans all hosting locations (onpremises, private and public clouds, and Saas applications), all modern operating systems, and all management paradigms.

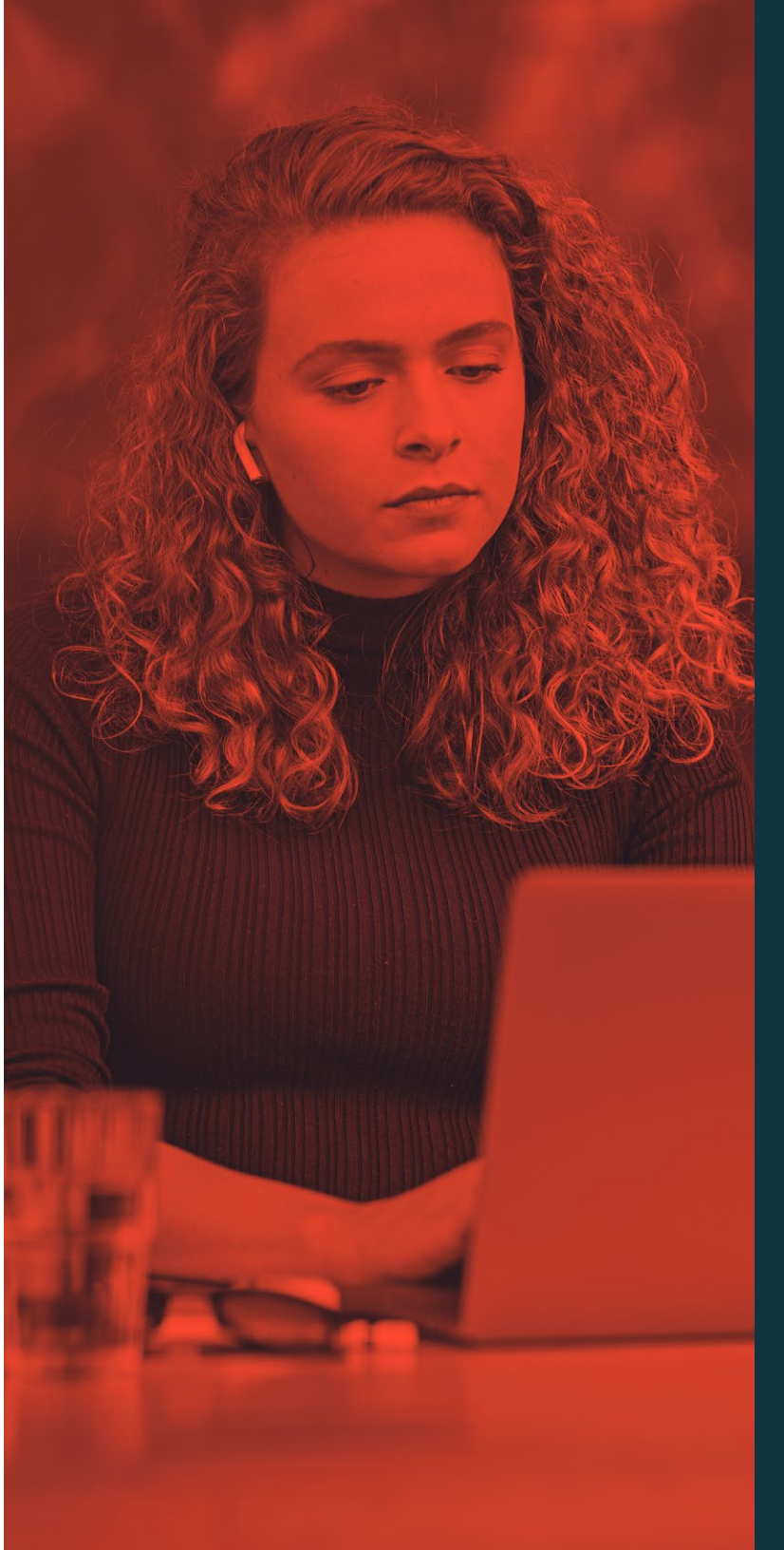
WHY RECONSIDER VPN AND EMBRACE ZTNA

Even when a VPN addresses all your security risks, one remains: the user has to actually connect to a VPN. Often, reluctance or simply a lack of knowledge on how to connect to VPN leads organizations to put their data at risk by not placing it within secured boundaries of the network to ensure that users can access the information.

With ZTNA, users never have to think about when or how to access secured sites. They log into their device and, when the time comes, can access the secured data. Behind the scenes, ZTNA ensures that the user is authenticated, authorized and that the device can be trusted to access the data directly. Effectively, ZTNA pushes organizations to secure their data correctly while making it easy for end users to access.

Gone are the days of taking risks with data to accommodate users that had again forgotten their VPN instructions!

Regardless of which device type or OS users are working on, ZTNA access automatically establishes microtunnels when applications need to connect and reconnect just as easily in the event of the session's end or service disruption. Jamf Private Access doesn't commandeer precious hardware resources or drain your battery when not in use.



No, instead it stands like a sentry at the ready, waiting for an application, user request or service that requires access to protected data for it to spring into action, both preserving resources and maintaining a seamless user experience while eliminating the discoverability and reachability of data and apps that users should not be able to access; and providing a cloud-based, software-defined perimeter (SDP) to secure data as it travels across isolated connections for each application.

And when Jamf Private Access is used with Apple's Private Relay — a new iCloud service that protects an individual's privacy by hiding their IP address and location from the websites they visit – secure access to business applications without the performance, privacy and security challenges of legacy enterprise VPN connections is made possible.

With this pairing, users are protected in their private and enterprise browsing. Personally-owned devices can be deployed with Jamf to protect and route enterprise traffic; personal browsing will remain private by being routed via iCloud Private Relay. Running both Jamf Private Access and iCloud+ Private Relay together is the most optimal approach to privacy and security without compromising performance or the end-user experience.

SO WHAT NOW?

Begin by securing devices, users and data in your remote or hybrid work environment today using modern security approach: Jamf Private Access, based on the Zero Trust Network Access framework to enforce least privilege access based on an identity-centric security model.

Conduct device health checks and automate remediation workflows based on risk-aware policies to elevate the security posture of your network fleet, all from one centralized, cloud-based console without disrupting the intuitive user experience.

See what's possible with a free trial, or contact your preferred Apple reseller to get started.

Request Trial