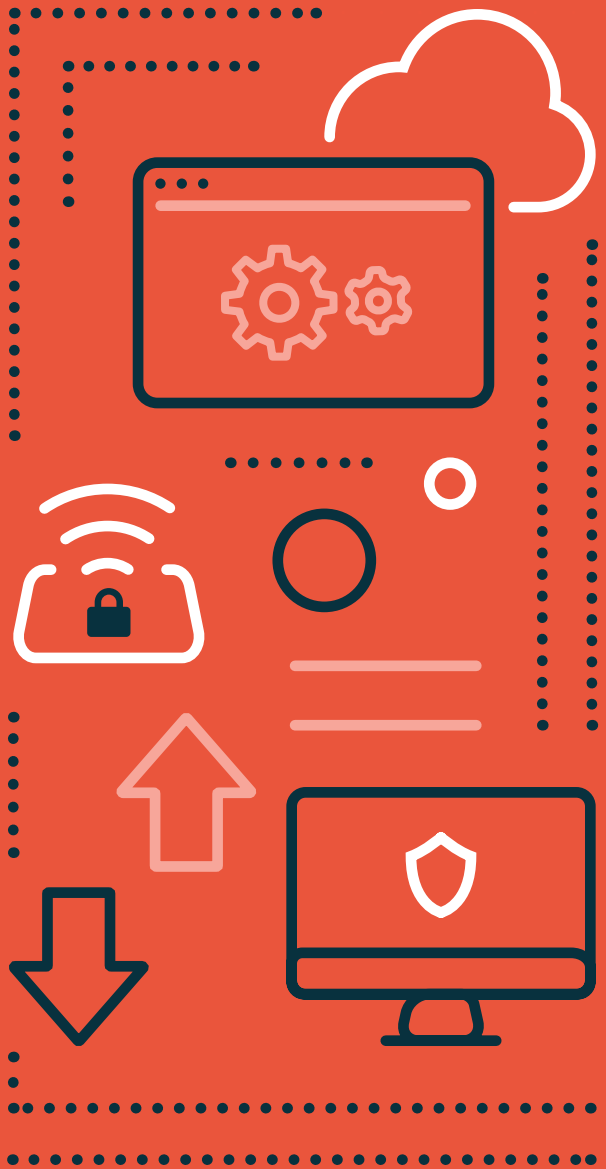


Zero Trust Netzwerk Zugriff

für Einsteiger

jamf

KEINE AHNUNG VON ZERO-TRUST-NETZWERKZUGANG? KEIN PROBLEM.

Laut **Gartner** ist Zero Trust Network Access (ZTNA) ein **Produkt oder Service, der eine identitäts- und kontextbasierte logische Zugriffsgrenze um eine App oder eine Reihe von Apps erzeugt**.

Einfach gesagt ist ZTNA der Nachfolger des Virtual Private Networking (VPN). Aber im Gegensatz zu VPN, das seit 1996 existiert und auf dem Peer-to-PeerTunneling Protocol (PPTP) basiert, **wurde eine Jamf Connect ZTNA Lösung mit modernen IT-Methoden entwickelt** und verwendet ein identitätszentriertes Sicherheitsmodell mit risikobewusster Richtlinienverwaltung und anwendungsspezifischen Microtunnels. Diese begrenzen den Ressourcenzugriff für Benutzer als Teil einer cloudbasierten Infrastruktur, die das Management vereinfacht, per Mausklick skalierbar ist und zur Pflege keine Hardware benötigt.

SEHEN SIE SICH DIESES E-BOOK AN, UM DIE GRUNDLAGEN ZU VERSTEHEN:

- So funktioniert Jamf Private Access
- Eingebaute Sicherheitsfunktionen
- Warum Sie Ihre Methode zur Netzwerkauthentifizierung und Sicherung überdenken müssen

Und wo Sie anfangen sollten.

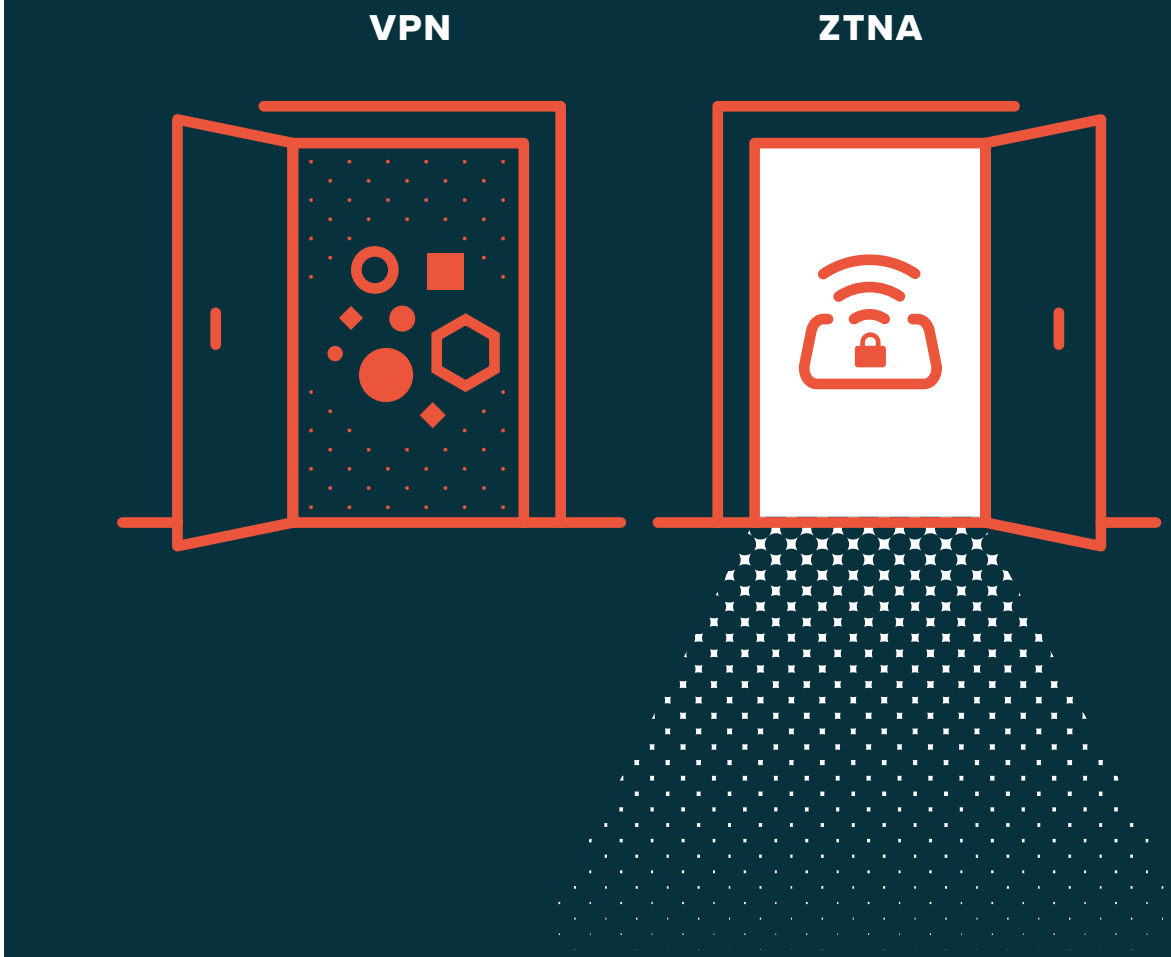
„NIEMAND VERTRAUT JETZT NOCH JEMANDEM.“

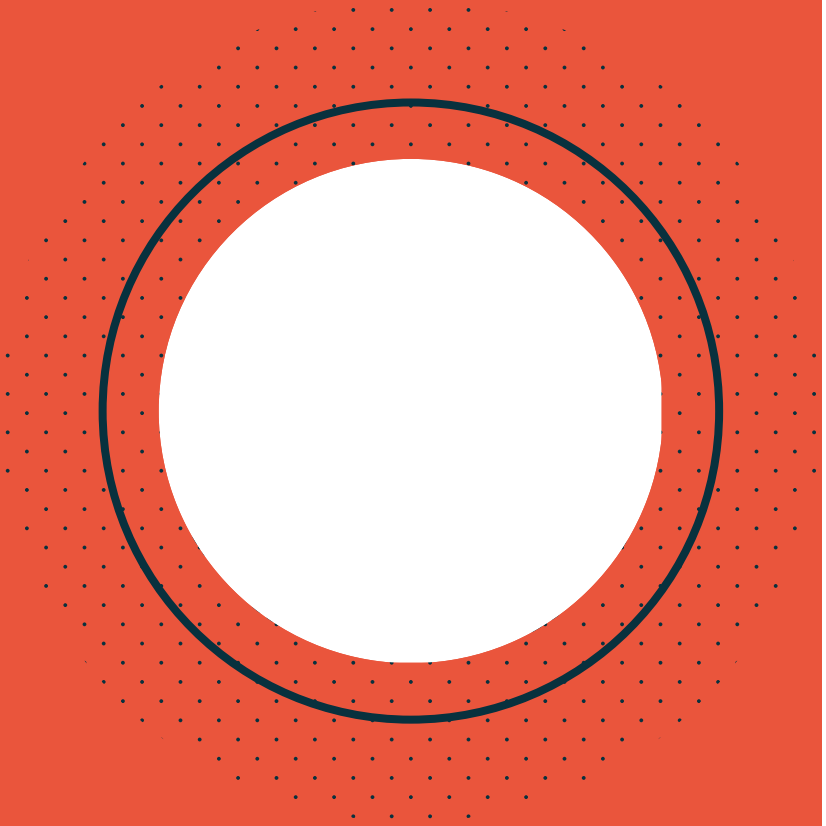
Kurt Russells Rolle als R. J. MacReady in Das Ding aus einer anderen Welt misstraut seinen Kollegen im Laufe des Films, und die Probleme nehmen zu. MacReady ähnelt damit ZTNA, da die Technologie Sicherheitskonfigurationen auf der Grundlage des Prinzips der geringsten Privilegien einsetzt und dem Thema „nie vertrauen, immer verifizieren“ folgt.

Im Grunde wird durch die Durchsetzung des Prinzips des geringsten Privilegs in Kombination mit Tests des Gerätezustands in Echtzeit **der Zugriff auf jede Anwendung nur für bestimmte autorisierte Benutzer gewährt, die dies mit ihren einzigartigen Anmeldedaten anfordern**.

Dadurch muss sichergestellt werden, dass nach der Authentifizierung eines Benutzers mit den Cloud-Identitätsdaten die geschäftlichen Verbindungen gesichert werden, während nicht zum Unternehmen gehörende Apps direkt mit dem Internet verbunden werden. Dieses Verfahren wird als Split-Tunneling bezeichnet und schützt die Privatsphäre des Endbenutzers, während die Netzwerkinfrastruktur optimiert wird. Dies verbessert das zugrundeliegende Netzwerk weiter, indem es die Erstellung der Microtunnels effizienter macht. Durch die Nutzung der Microtunnels können zugelassene Benutzer, Geräte und Apps durchgängig gesichert werden. Wenn eines der Kriterien, wie ein persönliches Gerät, nicht für den Zugriff konfiguriert ist – unabhängig davon, ob die richtigen Anmeldedaten eingegeben wurden – wird der Zugriff auf Unternehmensressourcen gesperrt.

Im Gegensatz zu VPN, wo der Zugriff holistisch gewährt wird und Benutzern Zugang zum ganzen Ressourcennetzwerk bietet, stärkt die detaillierte Methode von ZTNA die Sicherheit dadurch, dass Benutzer nur auf das zugreifen, was sie benötigen und wenn sie es benötigen. Durch die Verbesserung der Sicherheit Ihrer Organisation mit Richtlinien zur Erfüllung von Complianceanforderungen sichern Sie die Endbenutzer, Firmengeräte und Daten auf eine umfassendere Weise.





„IHRE REGELN GEHEN MIR LANGSAM AUF DIE NERVEN“

Wie die Dichotomie im Film Die Klapperschlange, wo der berüchtigte Snake Plissken das sagte, als er zwischen den Freiheiten der Bürger und den Einschränkungen des Gesetztes gefangen war – die ja für Frieden und Ordnung sorgen sollen – befinden sich IT-Administratoren in einer ähnlichen Zwangslage.

Wie können Organisationen das Gleichgewicht zwischen Sicherheit und dem Zugriff der Endbenutzer auf nötige Ressourcen und Daten finden?

Jamf Private Access erfüllt diese Aufgabe.

Mit Identitäts- und App-zentrierten Richtlinien, welche die Produktivität ermöglichen, während sie die umfassende Entdeckbarkeit und Erreichbarkeit von Daten und Apps eliminieren, die Benutzer nicht erreichen sollten, stellt Jamf Private Access sicher, dass die Durchsetzung einer gemeinsamen Zugriffsrichtlinie über alle Rechenzentren, mehrfache Cloud-Infrastrukturen und SaaS-Apps sowie alle modernen Betriebssysteme (OS) und Verwaltungsparadigmen hinweg gleich bleibt.

Die Intensivierung der Sicherheit über eine Vielzahl von risikobewussten Richtlinien verbessert die Schutzlage durch die Verhinderung des Zugriffs auf Ressourcen, durch wiederholte Tests von Geräten, um deren Status zu messen. Zudem werden proaktiv Geräte identifiziert, die kompromittiert sind oder anderweitig ein hohes Risiko für den sicheren Ressourcenzugriff darstellen – ganz abgesehen vom Sicherheitsstatus des Netzwerk insgesamt.

„ENTSPANNT EUCH ALLE, ICH BIN HIER.“

Auf der Grundlage einer soliden, cloudbasierten Infrastruktur erfordert Jamf Private Access keine zu verwaltende Hardware, keine Support-Verträge und verlässt sich nicht auf die Installation und/oder Konfiguration komplexer Software.

Vergessen wir nicht, dass die zentralisierte, hochskalierbare und sofort einsetzbare Natur der Cloud bedeutet, dass Daten von der ersten Sekunde an geschützt werden, in der Sie Ihre Geräte beim Service anmelden – ganz gleich wie viele Geräte Sie haben, oder wo sie sich geographisch befinden. Es ist lediglich eine Netzwerkverbindung erforderlich.

Ganz wie der liebenswerte aber etwas distanzierte Jack Burton aus dem Film Big Trouble in Little China stellen die cloudbasierte Natur und die Integrationen zur Erweiterungen der Fähigkeiten in Jamf Private Access sicher, dass es immer daran arbeitet, Ihre Endgeräte zu sichern. Hierzu verschlüsselt es die Verbindungen, überwacht den Gerätestatus und setzt automatisierte Workflows ein, um entdeckte Probleme zu beheben und zu gewährleisten, dass Geräte optimal funktionieren und Benutzer und Daten sicher sind.

SO FUNKTIONIERT JAMF PRIVATE ACCESS

Spoiler-Warnung: Es arbeitet intelligenter, nicht härter.

Ein Beispiel für eine Integration, die für die ZTNA-Architektur wichtig ist, wäre die Fähigkeit zur Authentifizierung der Benutzer über Single Sign-On (SSO) durch Ihren bevorzugten **cloudbasierten Identity Provider (IdP)** zu ermöglichen. Das eliminiert die Mühe, Zertifikate für Benutzer und/oder Geräte zu verwalten, was wiederum eine dedizierte Zertifizierungsstelle (CA) überflüssig macht. Zudem wird die Konfiguration der Sicherheit für diese Art der Infrastruktur in primär auf Tele- oder Hybridarbeit ausgerichteten Umgebungen deutlich erleichtert.

Dies erlaubt es Administratoren, die Netzwerkverbindung jedes Geräts mit der Konnektivität zur Cloud zu kombinieren, um „intelligenter, nicht härter“ zu arbeiten. Schließlich bedeutet weniger Aufwand eine höhere Effizienz, was nie schlecht ist. Und weil wir von weniger Aufwand sprechen, der Jamf Connect Agent ist nicht nur mit erstklassigen Schutz für Ihre Geräte, Benutzer und Daten ausgestattet, sondern verwendet dabei auch möglichst wenige Ressourcen.

Jamf unterstützt nativ Okta und Azure, sowie alle anderen wichtigen IdPs wie Google, Ping usw. über Azure-Föderation

PRIVATE ACCESS SICHERHEITSFUNKTIONEN:

Identitätszentriertes Sicherheitsmodell

Nur autorisierte Benutzer sich mit Unternehmens-Apps verbinden und sicherstellen, dass die Richtliniendurchsetzung über alle Rechenzentren, Clouds und SaaS-Anwendungen hinweg konsistent ist.

App-basierte Microtunnels

Verbinden Benutzer nur mit Apps, auf die sie zugreifen dürfen. Microtunnels setzen den Zugang nach dem Least-Privilege-Prinzip durch und verhindern laterale Netzwerkbewegung (was häufig ein Einfallstor für Sicherheitsverstöße darstellt.)

Moderne Cloud-Infrastruktur

Null Hardware zu verwalten, Support-Verträge zu verlängern oder komplexe Software zu konfigurieren. Sie können sogar die Notwendigkeit eliminieren, administrative Kontrolle über ein Gerät zu haben, um sicheren Zugriff zu ermöglichen.

Integration in Ihre Identitätsdienste

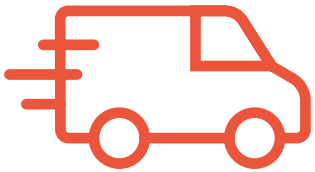
Authentifizierung der Benutzer durch Single Sign-On (SSO) ermöglichen und die Notwendigkeit zur Verwaltung von Zertifikaten eliminieren.

Risikobewusste Zugriffsrichtlinien

Verbesserte Sicherheit durch Verhinderung des Zugriffs durch Benutzer und Geräte, die vielleicht kompromittiert sind.

Leichtgewichtige App

Richten Sie Tunnels automatisch ein, wenn Apps sich verbinden und nahtlos nach einer Unterbrechung erneut verbinden müssen.



Schnelle und effektive Konnektivität

Unbehinderter Zugriff auf Unternehmens-Apps – ohne Beeinträchtigung der Akkulaufzeit – arbeitet stillschweigend im Hintergrund, ohne Benutzererfahrung zu stören.

Intelligente Split-Tunneling

Gewährleisten Sie, dass Unternehmensverbindungen gesichert sind, während Sie nicht geschäftliche Apps direkt ins Internet leiten. Das schützt die Privatsphäre des Endbenutzers, während die Netzwerkinfrastruktur optimiert wird.

Einheitliche Zugriffsrichtlinie

Unterstützt alle Hosting-Standorte (Vor Ort, Private und Public Clouds und SaaS Apps), alle modernen Betriebssysteme und alle Management-Paradigmen.

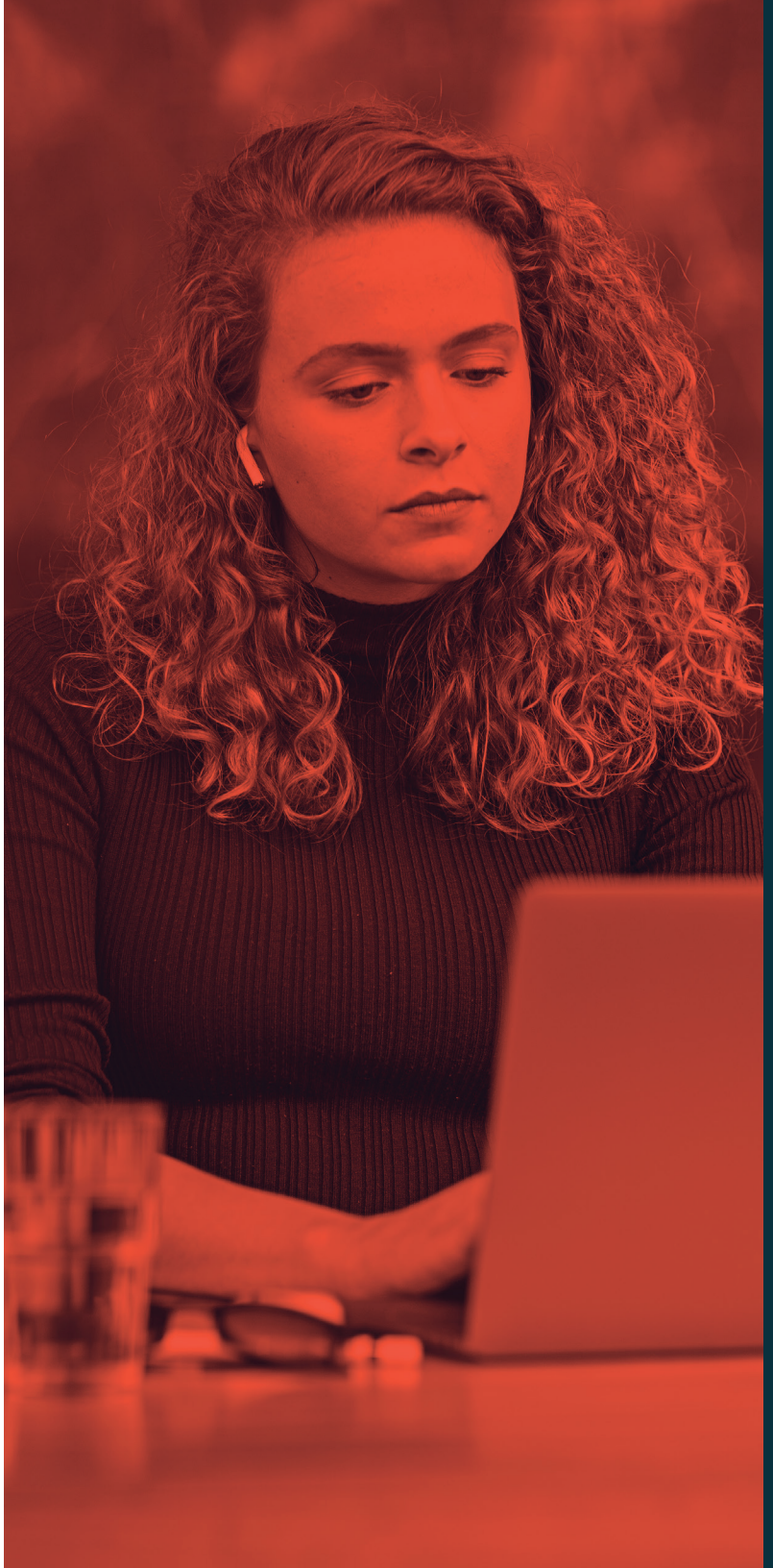
VPN ÜBERDENKEN UND ZTNA EINFÜHREN

Selbst wenn ein VPN alle Ihre Sicherheitsrisiken angeht, bleibt doch noch eines: Benutzer müssen sich tatsächlich mit einem VPN verbinden. Oft zögern Benutzer, oder wissen nicht einmal, wie man sich mit VPNs verbindet. Das führt dazu, dass Organisationen ihre Daten gefährden, indem sie diese nicht in die gesicherte Grenzen des Netzwerks platzieren, um zu gewährleisten, dass Benutzer auf die Informationen zugreifen können.

Bei ZTNA müssen Benutzer nie darüber nachdenken, wann oder wie sie auf gesicherte Websites zugreifen. Sie melden sich bei ihrem Gerät an, und wenn die Zeit kommt, können sie auf die gesicherten Daten zugreifen. Hinter den Kulissen sorgt ZTNA dafür, dass Benutzer authentifiziert und autorisiert werden, und dass das Gerät vertrauenswürdig ist und auf die Daten zugreifen kann. Im Grunde drängt ZTNA Organisationen dazu, ihre Daten korrekt zu schützen, während sie Benutzern den Zugriff erleichtert.

Vorbei sind die Tage, an denen man Daten riskierte, weil Benutzer wieder einmal vergessen hatten, wie man sich bei einem VPN anmeldet!

Unabhängig davon, auf welchem Gerätetyp oder Betriebssystem Benutzer arbeiten, stellt ZTNA automatisch Microtunnels her, wenn Apps sich verbinden und erneut verbinden müssen, falls eine Sitzung endet oder der Service unterbrochen wird. Jamf Private Access verlangt weder kostbare Hardwareressourcen, noch entleert es den Akku, wenn es nicht verwendet wird.



Stattdessen steht es wie ein Wächter bereit, und wartet, dass eine App, eine Benutzeranfrage oder ein Service Zugriff auf geschützte Daten benötigt. Dann wird es aktiv, bewahrt Ressourcen und garantiert eine nahtlose Benutzererfahrung, während es die Entdeckbarkeit und Erreichbarkeit von Daten und Apps eliminiert, auf die Benutzer nicht zugreifen sollten. Es bietet einen cloudbasierten und softwaredefinierten Perimeter, der Daten schützt, während sie sich für jede App über isolierte Verbindungen bewegen.

Und wenn Jamf Private Access mit Apple Privat-Relay verwendet wird – einem neuen iCloud-Service, der die Privatsphäre einer Person schützt, indem er ihre IP-Adresse und ihren Standort vor den Websites versteckt, die sie besucht – wird ein sicherer Zugriff auf Unternehmensapps möglich, ohne die Probleme bezüglich Leistung, Datenschutz und Sicherheit, die bei alten Unternehmens-VPN-Verbindungen auftreten.

Durch diese Kombination sind Benutzer bei ihrem Browsing geschützt, ganz gleich ob zu privaten Zwecken oder bei der Arbeit. Persönliche Geräte können mit Jamf bereitgestellt werden, um den Datenverkehr des Unternehmens zu schützen und zu leiten. Das persönliche Browsing bleibt privat, indem es über iCloud Privat-Relay geleitet wird. Die gemeinsame Verwendung von Jamf Private Access und iCloud+ Privat-Relay ist der optimale Ansatz bei Datenschutz und Sicherheit, ohne die Leistung oder das Endbenutzererlebnis zu beeinträchtigen.

WAS JETZT?

Beginnen Sie noch heute damit, Geräte, Benutzer und Daten bei Remote-Office oder bei hybriden Arbeitsmodellen zu sichern, indem Sie die moderne Methode verwenden – Jamf Private Access auf der Grundlage des Zero Network Access Framework, um den Least-Privilege-Access durchzusetzen, der auf einem identitätszentrierten Sicherheitsmodell basiert. Sie werden:

- Prüfungen des Gerätestatus durchführen.
- Behebungs-Workflows auf der Grundlage von risikobewussten Richtlinien automatisieren, um den Sicherheitsstatus Ihrer Netzwerkgeräte zu steigern.

All das machen Sie von einer zentralisierten, cloudbasierten Konsole aus, ohne dass Sie die Benutzererfahrung beeinträchtigen.

Sehen Sie, was mit einer Testversion möglich ist, oder kontaktieren Sie Ihren Apple Partner, um die ersten Schritte durchzuführen.

Testversion anfordern