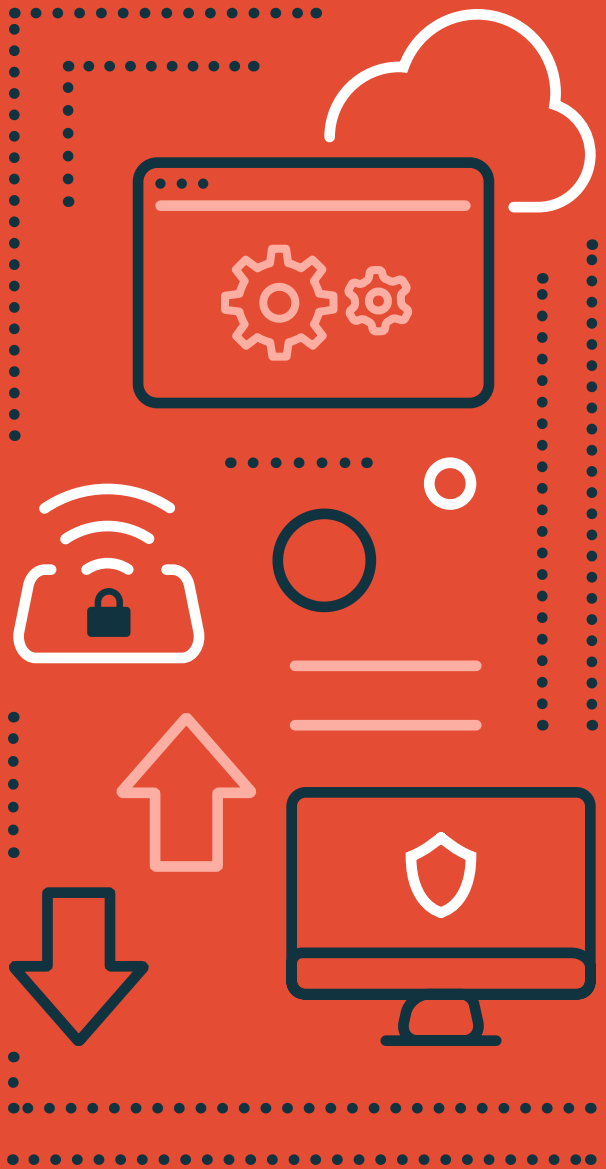


Acceso a la red de confianza cero

para principiantes

jamf

¿CONOCIMIENTO CERO DEL ACCESO A LA RED DE CONFIANZA CERO? NO HAY PROBLEMA.

De acuerdo con **Gartner**, el acceso a la red de confianza cero (ZTNA) es un **producto o servicio que crea un límite de acceso lógico basado en la identidad y el contexto en torno a una aplicación o conjunto de aplicaciones**.

En términos sencillos, la ZTNA es la sucesora de la Red Privada Virtual (VPN). Sin embargo, a diferencia de las VPN, que se remontan a 1996 y se basan en el Protocolo de Túnel de Usuario a Usuario (PPTP), **Jamf Connect se diseñó pensando en la informática moderna** al incorporar un modelo de seguridad centrado en la identidad, con administración de políticas conscientes del riesgo y microtúneles específicos para las aplicaciones. Éstos limitan el acceso a los recursos que los usuarios están autorizados a utilizar, todo ello integrado en una infraestructura basada en la nube que simplifica la administración, se amplía con un clic del ratón y no requiere mantenimiento de hardware.

SUMÉRJASE EN ESTE E-BOOK PARA CONOCER LOS FUNDAMENTOS:

- Cómo funciona Jamf
- Qué características de seguridad están incorporadas
- Por qué necesita reconsiderar su enfoque de autenticación y seguridad de la red

Y, por dónde empezar.

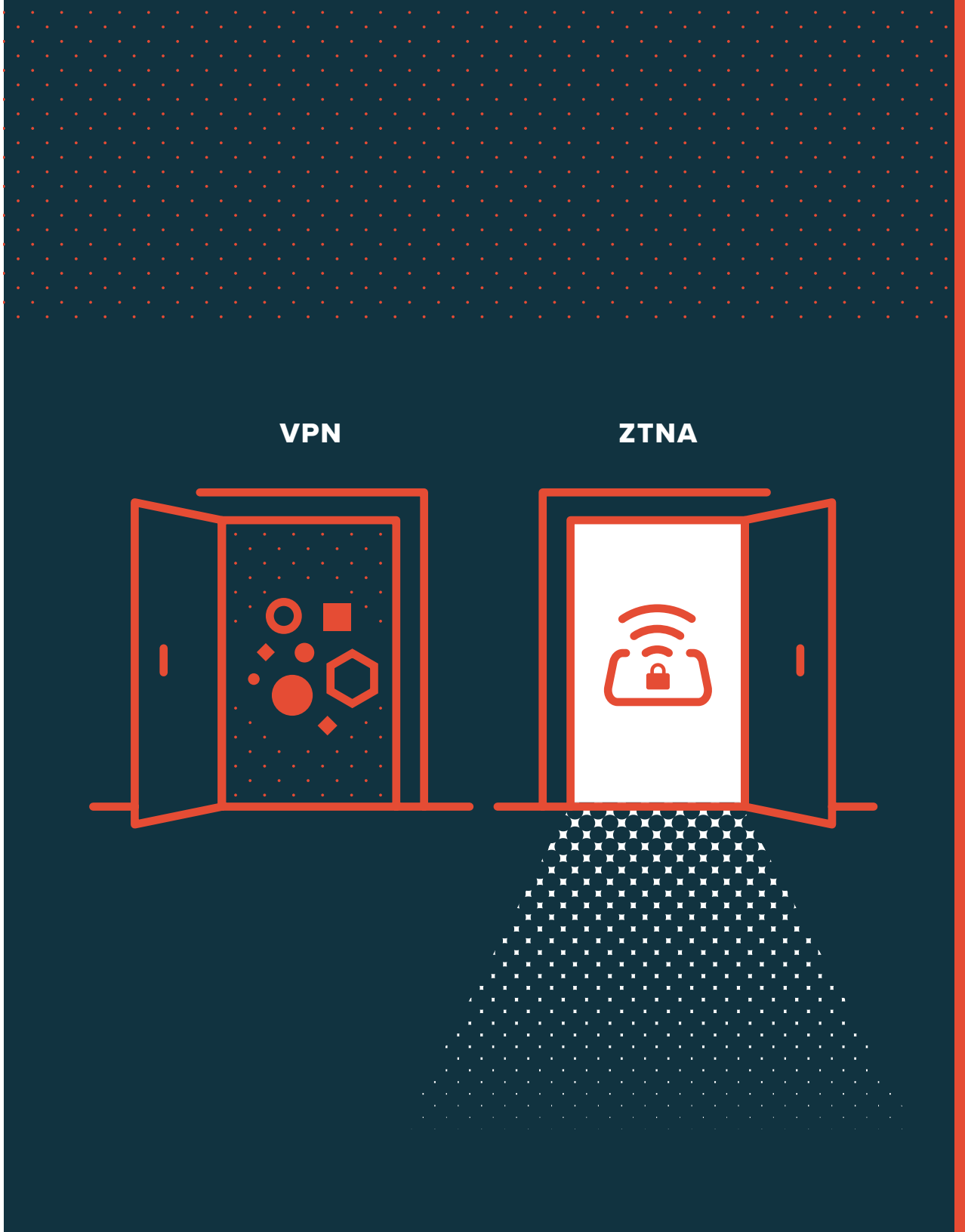
"NADIE CONFÍA EN NADIE AHORA".

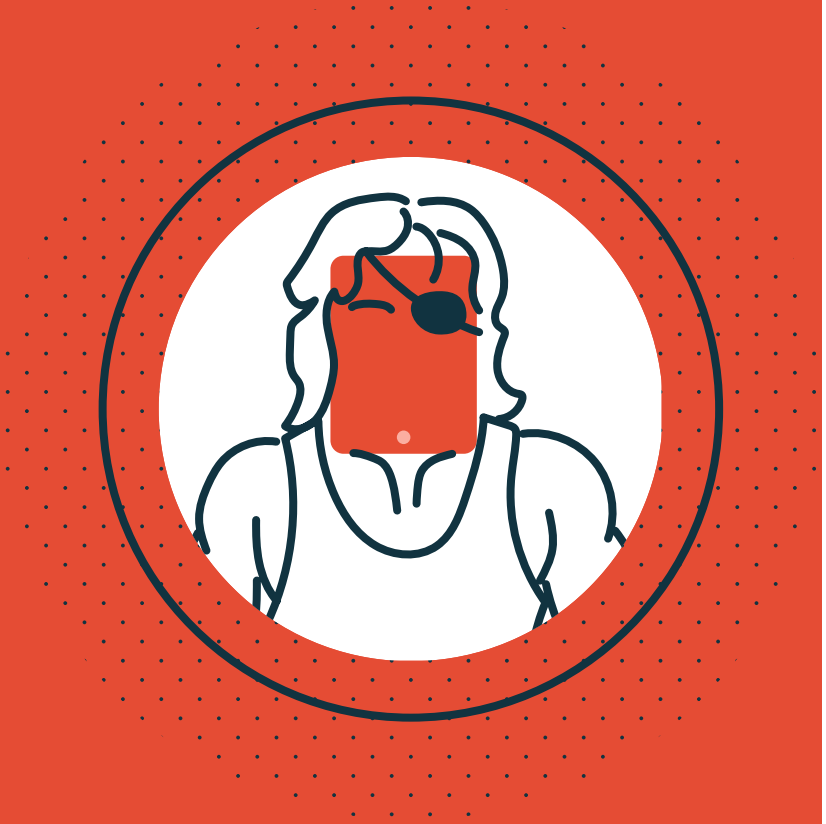
El personaje de Kurt Russell interpretado por R.J. MacReady en The Thing (La cosa) empieza a desconfiar de sus compañeros a medida que avanza la película y se acumulan los problemas. MacReady comparte este espíritu con ZTNA en el sentido de que la tecnología emplea configuraciones de seguridad basadas en el principio del mínimo privilegio y centradas en el tema común de "nunca confíes, siempre verifica".

Esencialmente, a través de la aplicación del mínimo privilegio junto con las comprobaciones de la postura del dispositivo en tiempo real, **el acceso basado en la nube se concede a cada aplicación sólo para el usuario específico y autorizado que solicita el acceso a través de sus credenciales únicas**.

Esto significa garantizar que, después de que un usuario se autentique en su dispositivo utilizando sus credenciales de identidad en la nube, las conexiones empresariales estén aseguradas, al tiempo que se permite que las aplicaciones no empresariales se dirijan directamente a Internet en un proceso denominado túnel dividido, conservando la privacidad del usuario final y optimizando la infraestructura de la red. Esto optimiza aún más la red subyacente al añadir eficiencia a la forma en que se establece la conexión o el microtúnel. Al potenciar los microtúneles, los usuarios, los dispositivos y las apps permitidos pueden estar asegurados de extremo a extremo. Si alguno de los criterios, por ejemplo, un dispositivo personal, no está configurado para el acceso —independientemente de que se introduzcan las credenciales adecuadas—, se negará el acceso a los recursos de la empresa.

A diferencia de las VPN, en las que el acceso se concede de forma global y proporciona a los usuarios acceso a toda la red de recursos, el enfoque particular de ZTNA refuerza la seguridad al conceder a los usuarios acceso sólo a lo que necesitan y cuando lo necesitan. Como resultado de la mejora de la seguridad de su organización a través de políticas personalizadas para cumplir con los requisitos de observancia, esto proporciona un apoyo mayor y más completo para salvaguardar a los usuarios finales, los dispositivos de la empresa y los datos.





"SUS REGLAS ESTÁN EMPEZANDO A MOLESTARME DE VERDAD"

Al igual que la dicotomía presentada en Escape from New York (Escape de Nueva York), donde el infame Snake Plissken pronunciaba la frase del título al verse atrapado entre las libertades concedidas a los ciudadanos y las restricciones de la ley —en vigor para mantener la paz y el orden—, los administradores de IT pueden enfrentarse a un dilema similar:

¿Cómo equilibran las organizaciones las protecciones de seguridad a la vez que proporcionan al usuario final el acceso a los recursos y datos necesarios?

Jamf hace exactamente eso.

Con políticas centradas en la identidad y la app que permiten la productividad al tiempo que eliminan la amplia capacidad para descubrir y hacer uso de datos y apps a los que los usuarios no deberían poder acceder, Jamf garantiza que la aplicación de la política de acceso unificada siga siendo coherente en los centros de datos, en las múltiples infraestructuras en la nube y en las aplicaciones SaaS, así como en todos los sistemas operativos (OS) y paradigmas de administración modernos.

Al reforzar la seguridad a través de una serie de políticas, las políticas de acceso atentas a los riesgos mejoran la seguridad al impedir el acceso a los recursos, al realizar comprobaciones recurrentes en los dispositivos para evaluar los datos de salud y al trabajar de forma proactiva para identificar los dispositivos que puedan estar comprometidos o que supongan un alto riesgo para el acceso a los recursos de forma segura, por no hablar de la postura de seguridad general de la red.

"QUE TODO EL MUNDO SE RELAJE, QUE YO ESTOY AQUÍ"

Comenzando con una base sólida, basada en la nube, la infraestructura empleada por Jamf no requiere ningún hardware que administrar, ningún contrato de soporte para navegar y no depende de la instalación y/o configuración de software complejo.

No olvidemos que la naturaleza centralizada, altamente escalable e instantánea de la nube significa que los datos están siendo protegidos desde el segundo en que sus dispositivos se inscriben en el servicio, sin importar cuántos dispositivos formen parte de su flota o en qué lugar del mundo se encuentren físicamente. Todo lo que se necesita es una conexión de red.

Al igual que el adorable, aunque algo distante, Jack Burton de Big Trouble in Little China (Rescate en el barrio chino), la naturaleza basada en la nube y las integraciones para expandir capacidades que potencian Jamf garantizan que siempre esté trabajando duro, al frente y en el centro, para proteger sus terminales al mantener las conexiones cifradas, supervisar el estado de los dispositivos e implementar flujos de trabajo automatizados para resolver los problemas detectados, manteniendo el rendimiento óptimo de los dispositivos y la seguridad de los usuarios y los datos.

CÓMO FUNCIONA JAMF

Alerta de spoiler: trabaja de forma más inteligente, no más ardua.

Un ejemplo de integración que es fundamental para la arquitectura de ZTNA es la posibilidad de habilitar la autenticación de usuarios mediante el inicio de sesión único (SSO) a través de **su proveedor de identidad (IdP) preferido en la nube.** Esto elimina la molestia de administrar los certificados para los usuarios y/o dispositivos, eliminando a su vez el requisito de mantener una Autoridad Certificadora (CA) propia, además de todos los trucos de red que se requieren cuando se configura la seguridad para este tipo de infraestructura en entornos de trabajo mayormente remotos o híbridos.

Esto permite a los administradores aprovechar eficazmente la conexión de red de cada dispositivo con la conectividad a la nube para "trabajar de forma más inteligente, no más ardua". Después de todo, menos gastos generales significa una mayor eficiencia, lo que nunca es malo. Y hablando de menos gastos generales, el propio agenteJamf no sólo se ha creado pensando en la protección del más alto nivel para sus dispositivos, usuarios y datos, sino que también se ha diseñado para utilizar el menor número de recursos posible mientras lo hace.

Jamf admite de forma nativa Okta y Azure, pero admite todos los demás IdP importantes como Google, Ping, etc., a través de la federación de Azure.

CARACTERÍSTICAS DE SEGURIDAD

Modelo de seguridad centrado en la identidad

Sólo los usuarios autorizados pueden conectarse a las aplicaciones empresariales y garantizar que la aplicación de las políticas sea coherente en los centros de datos, las nubes y las aplicaciones Saas.

Microtúneles basados en aplicaciones

Conecte a los usuarios únicamente a las apps a las que están autorizados a acceder. Los microtúneles proporcionan acceso mínimo y evitan movimientos de red lateral (un vector común en las brechas de seguridad).

Infraestructura de nube moderna

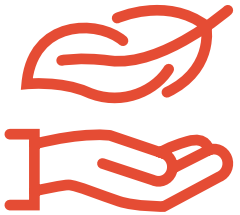
Sin hardware que administrar, contratos de soporte que renovar o software complejo que configurar. Incluso elimina la necesidad de tener el control administrativo de un dispositivo para permitir el acceso seguro.

Integración con sus servicios de identidad

Habilitar la autenticación del usuario a través de el inicio de sesión único (SSO) y eliminar la necesidad de administrar los certificados.

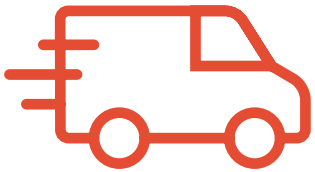
Políticas de acceso conscientes del riesgo

Mejorar la seguridad evitando acceso de usuarios y dispositivos que puedan estar comprometidos.



Aplicación de peso ligero

Establezca túneles automáticamente cuando las aplicaciones necesiten conectarse y vuelva a conectarse con fluidez si hay una interrupción.



Conectividad rápida y eficaz

Acceso a las apps empresariales — sin verse afectado por la duración de la batería— que funciona silenciosamente en segundo plano sin interferir en la experiencia del usuario.

Túnel dividido inteligente

Garantice la seguridad de las conexiones empresariales y permita que las aplicaciones no empresariales se enruten directamente a Internet. Así, conservando la privacidad del usuario final y optimizando la infraestructura de red.

Política de acceso unificado

Abarca todas las ubicaciones de alojamiento (in situ, nubes privadas y públicas, y aplicaciones SaaS), todos los sistemas operativos modernos y todos los paradigmas de administración.

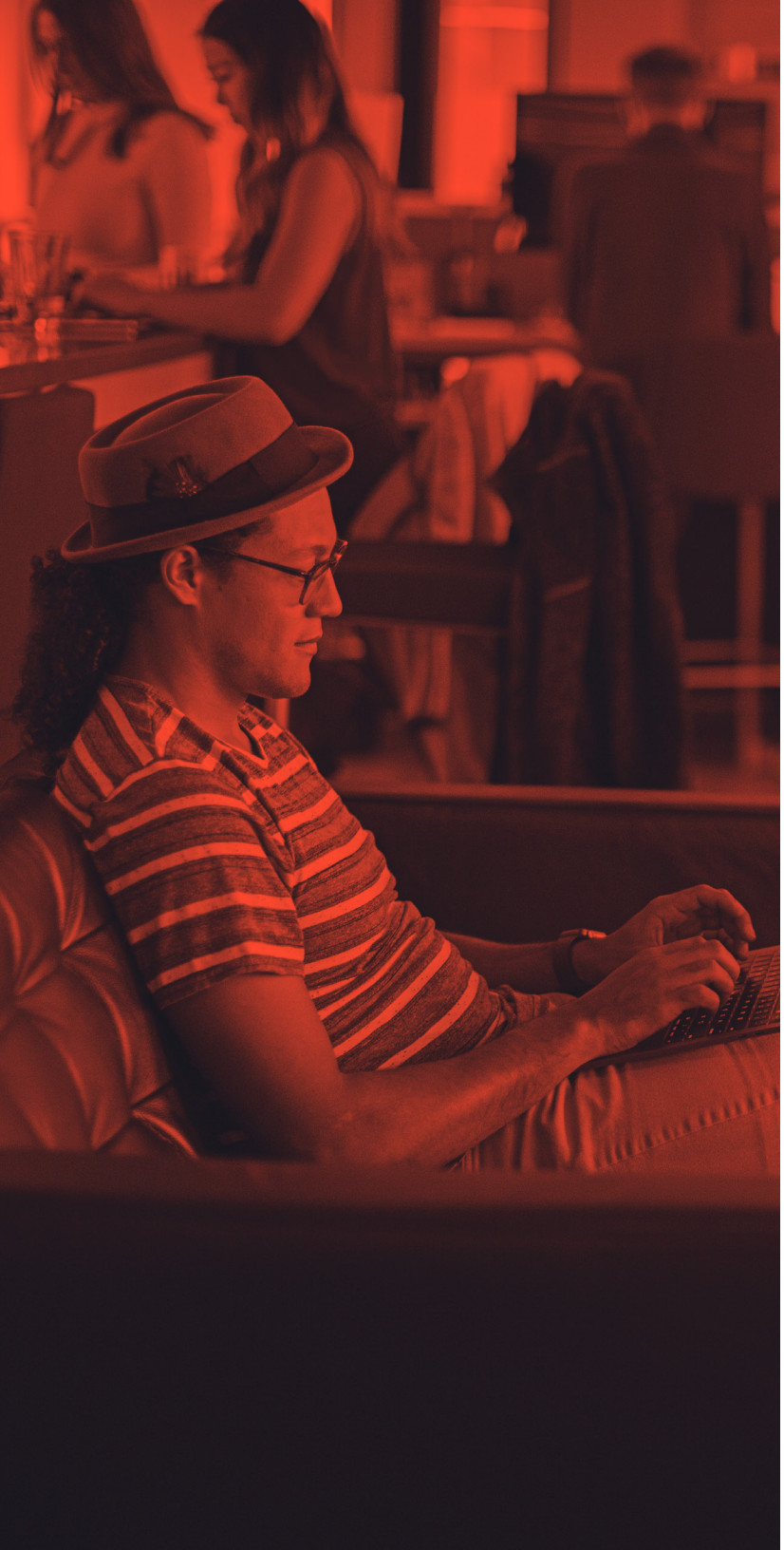
POR QUÉ RECONSIDERAR LAS VPN Y ADHERIRSE A ZTNA

Incluso cuando una VPN aborda todos sus riesgos de seguridad, queda uno: el usuario tiene que conectarse realmente a una VPN. A menudo, la resistencia o simplemente la falta de conocimiento sobre cómo conectarse a una VPN lleva a las organizaciones a poner en riesgo sus datos al no colocarlos dentro de los límites seguros de la red para garantizar que los usuarios puedan acceder a la información.

Con ZTNA, los usuarios nunca tienen que pensar cuándo o cómo acceder a los sitios seguros. Se conectan a su dispositivo y, llegado el momento, pueden acceder a los datos protegidos. Entre bastidores, la ZTNA se asegura de que el usuario esté autentificado, autorizado y que el dispositivo sea de confianza para acceder a los datos directamente. Efectivamente, ZTNA obliga a las organizaciones a asegurar sus datos correctamente al tiempo que facilita el acceso a los usuarios finales.

Se acabaron los días en los que se arriesgaban los datos para acomodar a los usuarios que habían olvidado de nuevo las instrucciones de la VPN.

Sin importar el tipo de dispositivo o el sistema operativo en el que trabajen los usuarios, el acceso a ZTNA establece automáticamente microtúneles cuando las aplicaciones necesitan conectarse y reconectarse con la misma facilidad en caso de que la sesión finalice o se interrumpa el servicio. Jamf no se apropia de los valiosos recursos de hardware ni agota la batería cuando no se utiliza.



No, en su lugar, se mantiene como un centinela preparado, a la espera de una aplicación, una solicitud de usuario o un servicio que requiera acceso a los datos protegidos para que entre en acción, tanto para preservar los recursos como para mantener una experiencia de usuario fluida, al tiempo que elimina la posibilidad de descubrir y alcanzar datos y apps a los que los usuarios no deberían poder acceder; y proporciona un perímetro definido por software (SDP) basado en la nube para asegurar los datos mientras viajan a través de conexiones aisladas para cada aplicación.

Y cuando Jamf se utiliza con Private Relay de Apple —un nuevo servicio de iCloud que protege la privacidad de una persona al ocultar su dirección IP y su ubicación de los sitios web que visita— se posibilita el acceso seguro a las aplicaciones empresariales sin los problemas de desempeño, privacidad y seguridad de las conexiones VPN empresariales heredadas.

Con este acoplamiento, los usuarios están protegidos en su navegación privada y empresarial. Los dispositivos de propiedad personal pueden ser implementados con Jamf para proteger y enrutar el tráfico de la empresa; la navegación personal seguirá siendo privada al ser enrutada a través de iCloud Private Relay. Ejecutar conjuntamente Jamf y iCloud+ Private Relay es el enfoque más acertado para la privacidad y la seguridad sin comprometer el rendimiento o la experiencia del usuario final.

¿Y AHORA QUÉ?

Hoy mismo comience a asegurar los dispositivos, los usuarios y los datos en su entorno de trabajo remoto o híbrido utilizando un enfoque de seguridad moderno: Jamf, basado en el marco Acceso a la Red de Confianza Cero para imponer el acceso con privilegios mínimos basado en un modelo de seguridad centrado en la identidad.

Realice comprobaciones del estado de los dispositivos y automatice los flujos de trabajo de corrección basados en políticas sensibles a los riesgos para elevar la postura de seguridad de su flota de redes, todo ello desde una consola centralizada basada en la nube sin interrumpir la experiencia intuitiva del usuario.

Vea lo que es posible con una prueba gratuita, o póngase en contacto con su distribuidor de Apple preferido para empezar.

Solicitar prueba