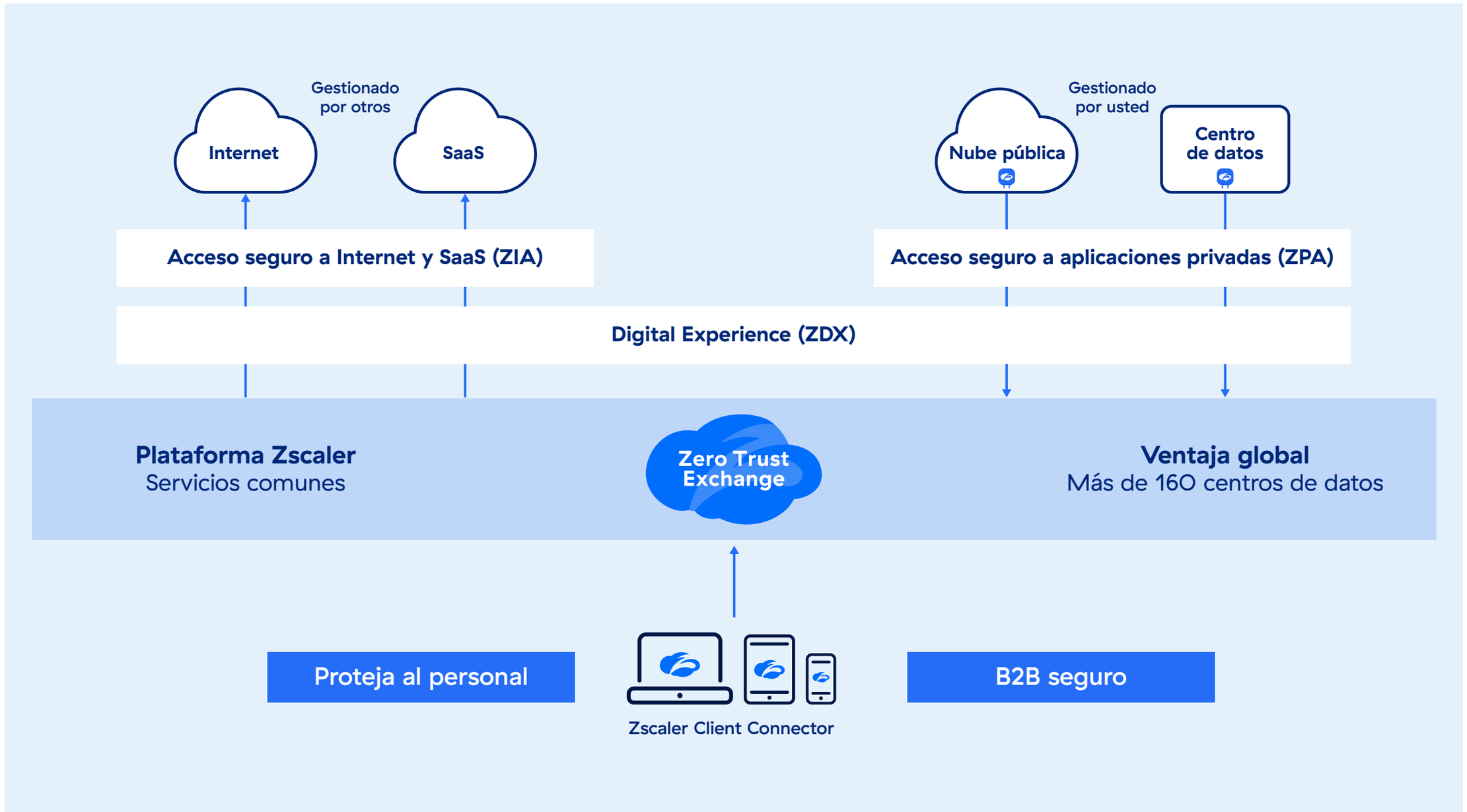
Zscaler Client Connector

Acceso rápido, seguro y confiable a cualquier destino, desde cualquier ubicación o dispositivo.

FICHA DE DATOS

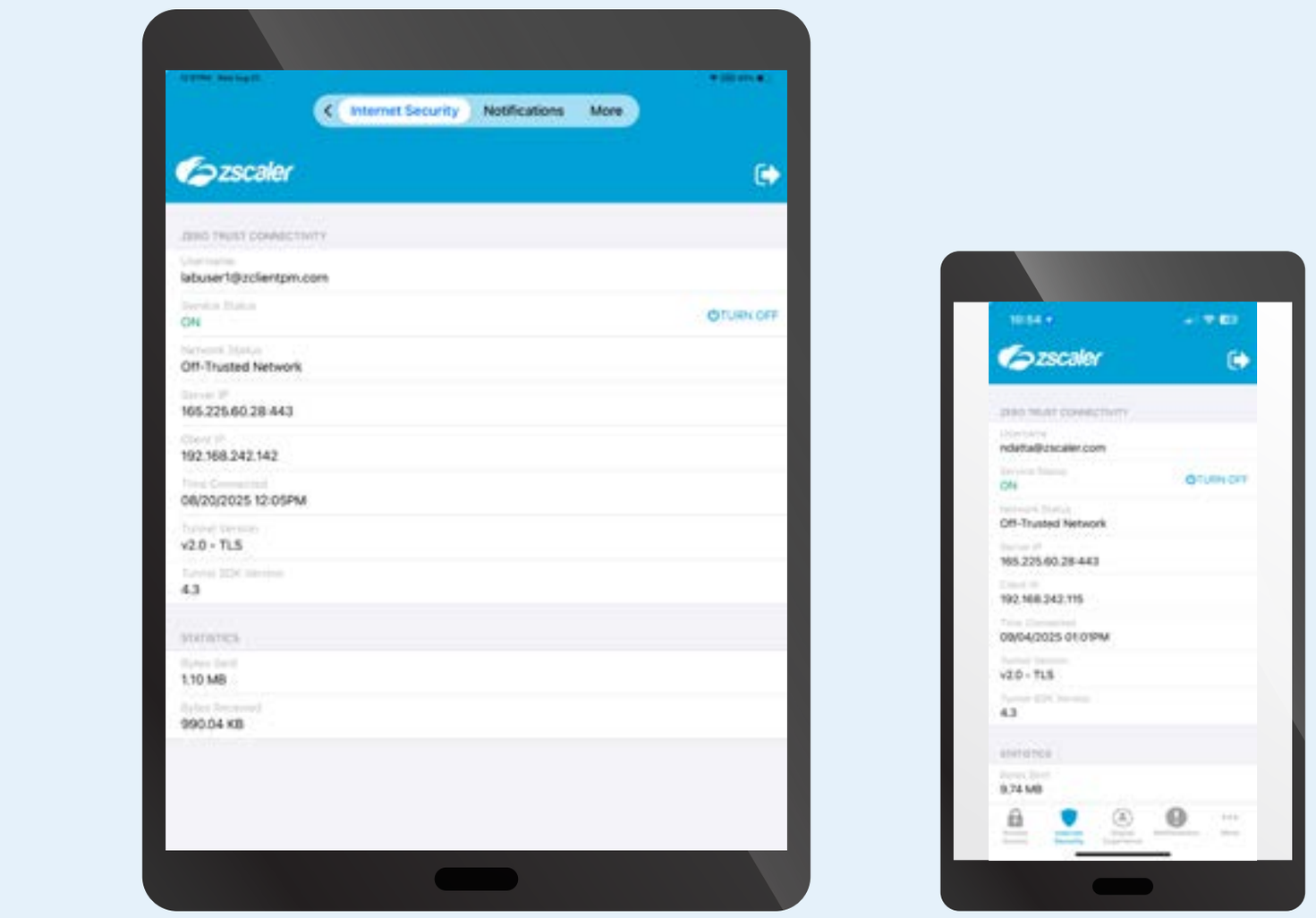


Los empleados de hoy trabajan de manera drásticamente diferente a como lo hacían antes. Ahora pueden utilizar una amplia variedad de dispositivos, mientras trabajan desde cualquier lugar, para acceder a aplicaciones en la nube y otros destinos alrededor del mundo. Este nuevo personal híbrido exige un acceso rápido y sin inconvenientes a los recursos de TI, pero eso no puede lograrse a costa de exponer los datos a riesgos. Por lo tanto, cualquier organización que quiera tener éxito hoy en día debe proteger los terminales distribuidos globalmente y, al mismo tiempo, garantizar experiencias de usuario productivas. Para lograr esto, innumerables equipos de TI recurren a Zscaler y su agente de terminal, Client Connector.

Antes, cuando los usuarios y las aplicaciones se ubicaban en la oficina, era lógico confiar en soluciones de seguridad y conectividad centradas en la red. Sin embargo, hoy en día, los empleados externos acceden a aplicaciones externas a través de redes que los equipos de TI no controlan. El retorno de este tráfico al centro de datos para protegerlo añade latencia que interrumpe la productividad. y lo que es más importante, el retorno aumenta el riesgo al conectar a los usuarios a la red corporativa, lo que les permite abusar de permisos excesivos y moverse lateralmente por los recursos conectados a la red. Además, amplía la superficie de ataque y conlleva otras vulnerabilidades de seguridad clave.

La arquitectura de zero trust es la solución a estos problemas. Zscaler lo ofrece como un servicio de Zero Trust Exchange, la mayor plataforma de seguridad en la nube del mundo, que actúa como una centralita inteligente para proporcionar comunicaciones de zero trust entre cualquier persona mediante políticas comerciales, no redes. Zero Trust Exchange brinda acceso con privilegios mínimos directamente a los recursos de TI en función del contexto en lugar de la dirección IP del usuario, y lo hace en el borde desde más de 160 puntos de presencia en todo el mundo. En otras palabras, los equipos de TI pueden detener las amenazas y la pérdida de datos y, al mismo tiempo, brindar a los usuarios experiencias digitales excepcionales en cualquier dispositivo y en cualquier lugar.

Zscaler Client Connector juega un papel central a la hora de brindar comunicaciones de zero trust entre cualquier persona. Es el agente de terminal ligero pero multifacético de Zscaler, que facilita el acceso de alto rendimiento y con mínimos privilegios directamente a Internet y a los recursos de TI para los usuarios en todas partes. Además, proporciona una gran cantidad de otras funcionalidades que mejoran aún más la seguridad y la conectividad al tiempo que eliminan los productos puntuales y sus agentes dedicados.



©2025 Zscaler, Inc. Todos los derechos reservados.

Beneficios de Client Connector de Zscaler

Los beneficios de Client Connector se pueden agrupar más o menos en las siete categorías que se muestran a continuación. Para obtener más detalles, consulte la tabla al final de esta hoja de datos.

Comunicaciones de zero trust a cualquier destino. Las organizaciones ya no necesitan soluciones independientes con agentes independientes para proteger el acceso a diferentes destinos. Client Connector proporciona acceso de zero trust con privilegios mínimos a cualquier destino, incluidas la web, SaaS y aplicaciones privadas. Esto se ajusta a la visión de Gartner sobre SSE y SASE y garantiza que los dispositivos no se ralenticen por la sobrecarga de agentes.

Comunicaciones de zero trust para cualquier dispositivo. Además de proteger el acceso a cualquier destino, las organizaciones deben proteger el acceso en cualquier dispositivo. Esto se debe a que los empleados ahora utilizan una amplia variedad de ordenadores de sobremesa, portátiles, tabletas y teléfonos inteligentes con diversos sistemas operativos. Afortunadamente, Client Connector puede proteger cualquier dispositivo, manteniendo a sus empleados seguros y productivos.

Seguridad inteligente y sensible al contexto. La identidad por sí sola no basta para controlar el acceso a los recursos de TI (las identidades pueden ser robadas e incluso usuarios legítimos pueden perjudicar a sus empleadores sin cuidado). Las organizaciones deben gestionar el acceso según el contexto y el riesgo. Client Connector lo permite al proporcionar información sobre la postura de seguridad del dispositivo que facilita un control de acceso inteligente y adaptativo.

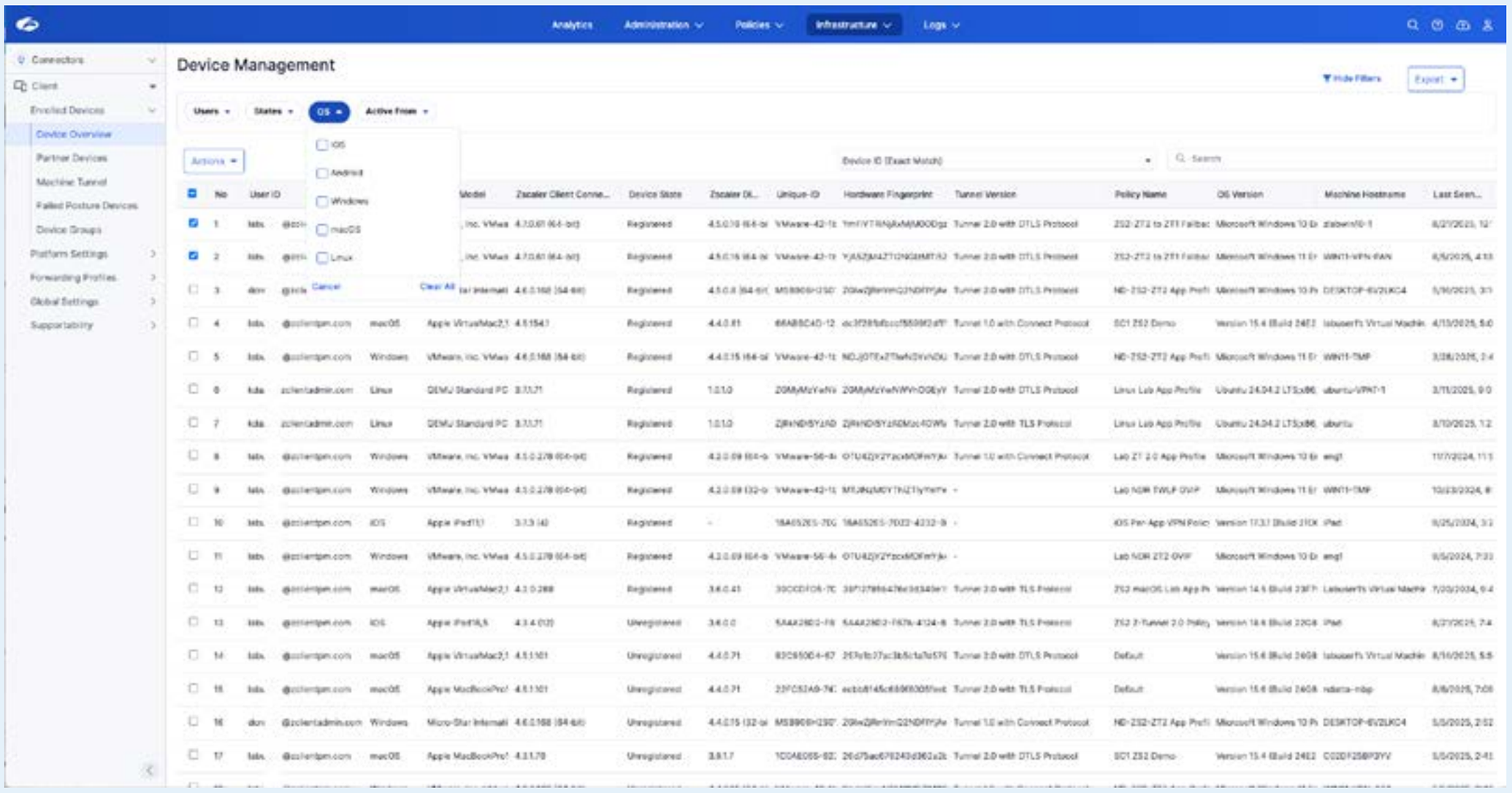
Protección de datos en dispositivos de usuario final. Como parte de la completa oferta de seguridad de datos de Zscaler, que protege cualquier canal de filtración, Client Connector ofrece DLP para terminales. Con esta solución, las organizaciones pueden proteger el almacenamiento extraíble, los recursos compartidos de red, la sincronización del almacenamiento personal en la nube y la impresión en terminales sin necesidad de otro producto específico que deba gestionarse por separado.

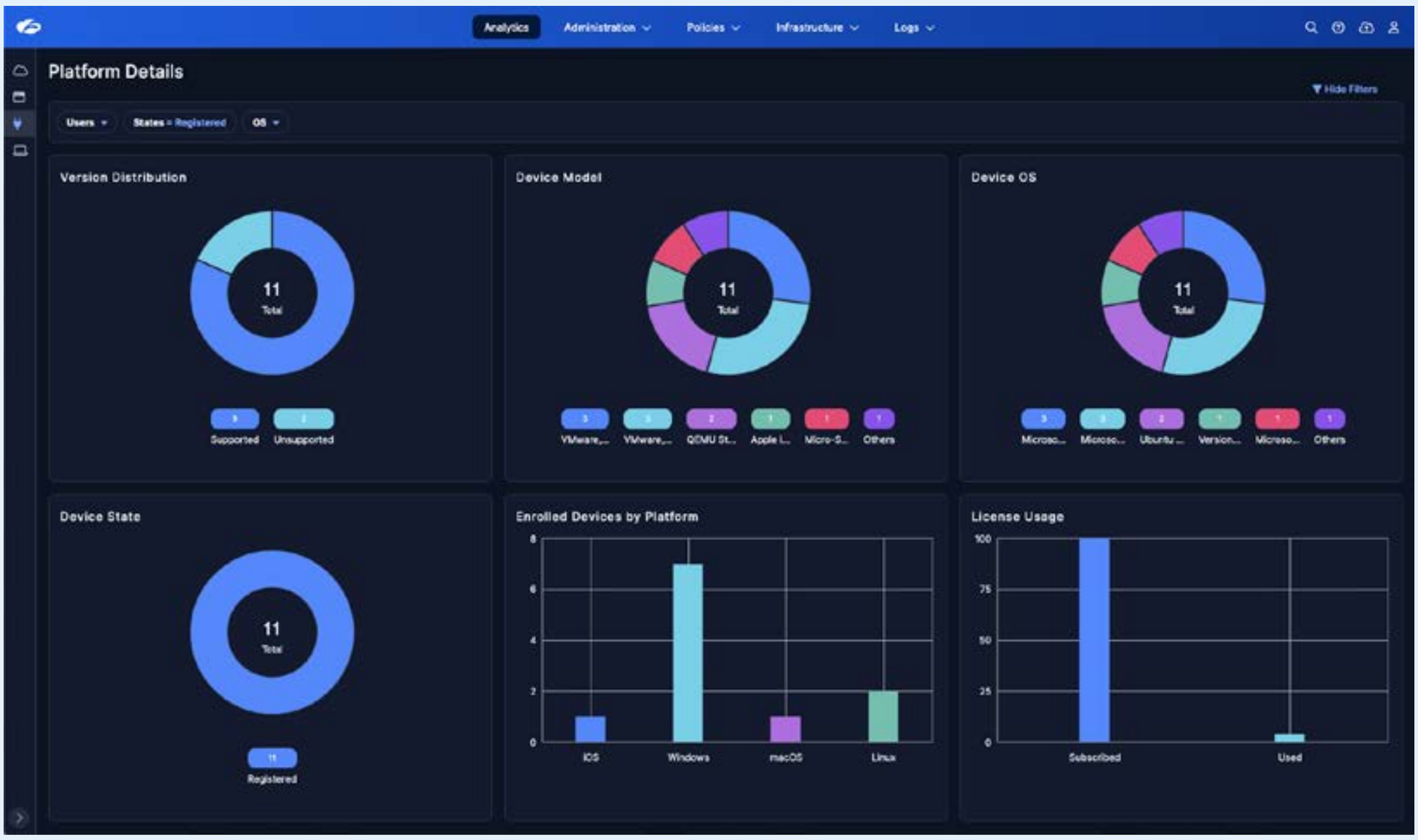
Detección de amenazas ocultas en su entorno. Los adversarios sigilosos suelen ocultarse en los entornos de las organizaciones para realizar tareas de reconocimiento en busca de esquemas maliciosos. Client Connector emplea tecnología de engaño que utiliza señuelos realistas de marcadores de aplicaciones, cookies, sesiones y contraseñas para atraer a estos atacantes. Una vez que se accede a los señuelos, genera alertas de alta fidelidad.

Experiencias de usuario y productividad superiores. a diferencia de las herramientas tradicionales que redireccionan el tráfico, Client Connector dirige el tráfico por la ruta más corta hasta su destino. Además, proporciona a Zscaler Digital Experience (ZDX) visibilidad sobre los eventos y el estado del dispositivo, lo que ofrece a los administradores una visión completa de la conexión del usuario, acelera la resolución de problemas de experiencia de usuario y mejora la productividad de usuarios y administradores.

Gestión optimizada basada en la nube. La gestión del Client Connector con la interfaz de usuario unificada de Zscaler, Experience Center, permite alcanzar la excelencia operativa. Permite la gestión continua de políticas y del ciclo de vida para administrar el reenvío y la seguridad, así como las actualizaciones y reversiones, con paneles e informes integrados. Los administradores también pueden automatizar tareas mediante OneAPI, una API única para toda la plataforma Zscaler.

©2025 Zscaler, Inc. Todos los derechos reservados.





©2025 Zscaler, Inc. Todos los derechos reservados.

MÓDULOS DE CLIENT CONNECTOR DE ZSCALER	
Zscaler Internet Access	Basada en una década de liderazgo en el Cuadrante Mágico para Secure Web Gateway (SWG), ZIA es la solución de Zscaler que protege el acceso a Internet al tiempo que aplica una variedad de funciones granulares de protección contra amenazas.
Zscaler Private Access	Zscaler Private Access ofrece comunicaciones fluidas de zero trust para todos los usuarios que acceden a cualquier aplicación privada, con segmentación de usuario a aplicación impulsada por IA y políticas conscientes del contexto que ayudan a reducir el riesgo.
Zscaler Digital Experience	Zscaler Digital Experience proporciona visibilidad de extremo a extremo de las experiencias de los usuarios y permite la detección, resolución y solución rápida de problemas de rendimiento, lo que mejora la productividad tanto de los administradores como de los usuarios finales.
Zscaler Endpoint DLP	Zscaler Endpoint Data Loss Prevention (DLP) es parte de la solución completa Zscaler Data Security. Proporciona la visibilidad y el control que necesita sobre los datos del dispositivo, al tiempo que reduce el coste y la complejidad de la seguridad de los datos.
Zscaler Deception	Zscaler Deception implementa activos señuelo realistas en todo su entorno de TI para atraer adversarios ocultos y generar alertas de alta fidelidad que permiten a las organizaciones detectar y detener amenazas más rápidamente.

CARACTERÍSTICAS Y DETALLES DE CLIENT CONNECTOR	
Soporte completo del sistema operativo	**Clientes de escritorio y ligeros:** • Microsoft Windows 11 y Windows 10 en x64 y ARM64 • Apple macOS Tahoe (26), Sequoia (15) y Sonoma (14) en Intel y Apple Silicon • Escritorios Linux (RHEL, CentOS, Fedora, Ubuntu, Debian, openSUSE, Arch Linux, Maya OS) • Google Android en ChromeOS • Sistema operativo eLux e IGEL **Móvil:** • Apple iOS 17, 18 y 26 • Google Android 10, 11, 12, 13, 14, 15 y 16
Compatibilidad con VDI para usuarios individuales y múltiples	• PC en la nube con Windows 365, escritorio virtual de Azure • Espacios de trabajo de AWS • Aplicaciones y escritorios virtuales de Citrix • Omnissa Horizon y Horizon Cloud Entornos VDI multisesión compatibles con Client Connector para VDI

©2025 Zscaler, Inc. Todos los derechos reservados.

Amplio soporte para tipos de tráfico	• Todos los puertos y protocolos (Z-Tunnel 2.0) • Solo tráfico web (Z-Tunnel 1.0) • Tráfico de cliente a cliente • Tráfico de servidor a cliente
Transporte en túneles	DTLS 1.2, TLS 1.2 y HTTP CONNECT
Cifrado	• Autenticación TLS mutua • Fijación SSL para la conectividad del canal de control • Cumplimiento de FIPS140
Selección óptima de DC	Selección automática basada en políticas: geolocalización, DC preferidos, latencia y destino del tráfico
Compatibilidad con el protocolo de capa 3	IPv4 e IPv6
Métodos de conectividad flexibles	• Iniciado por el usuario • A demanda • Soporte previo al inicio de sesión con Machine Tunnels • Siempre activo • Compatibilidad con perfiles VPN empresariales o perfiles VPN por aplicación en iOS • Compatibilidad con túnel dual (VPN empresarial y perfil VPN por aplicación) en iOS • Compatibilidad con perfiles de trabajo para Android
Opciones de implementación y ciclo de vida	• Implementar utilizando MDM y UEM como Intune, Workspace ONE, JAMF Pro, MobileIron, MaaS360, SCCM y otras soluciones • Implementar mediante Microsoft GPO en Active Directory (AD) • Implementaciones manuales mediante descargas directas desde Zscaler • Actualizaciones de versiones administradas en la nube y soporte de reversión • Distribución fluida de certificados CA raíz de confianza para la inspección SSL • Gestión de políticas y dispositivos basada en API
Aprovisionamiento de usuarios estándar del sector	• Sistema para la gestión de identidad entre dominios (SCIM) • Aprovisionamiento basado en SAML 2.0 justo a tiempo • Aprovisionamiento justo a tiempo para usuarios de emergencia • Aprovisionamiento automático de dispositivos basado en claves de máquina • Aprovisionamiento automático de usuario/dispositivo basado en token de dispositivo • Aprovisionamiento de certificados basado en SCEP* • Sincronización del servidor de directorio Microsoft AD o LDAP • Adición manual o carga masiva de usuarios a la base de datos de usuarios alojada

©2025 Zscaler, Inc. Todos los derechos reservados.

Opciones de autenticación admitidas	• SAML 2.0 • Kerberos • Certificados y tarjetas inteligentes • Autenticación multifactor (MFA) • Compatibilidad con tokens de hardware compatibles con FIDO2 • Autenticación de dispositivos basada en clave de máquina para soporte previo al inicio de sesión • Autentificación de usuario/dispositivo basado en tokens • Contraseñas • Compatible con autenticación incremental • Autenticación basada en navegador
inicio de sesión único	• Inicio de sesión único sin interrupciones para Windows • Inicio de sesión único de Kerberos • Complemento SSO de Microsoft Enterprise para macOS e iOS • Compatible con Apple Enterprise SSO Framework • Compatible con extensión SSO de OKTA
Restricciones de usuario basadas en políticas	• Soporte antimanipulación • Restricciones de OTP y contraseña para controlar el cierre de sesión del usuario, la salida del cliente y las restricciones de detención del servicio
Idiomas admitidos	Inglés, francés
Notificaciones al usuario final	**Compatibilidad con notificaciones de escritorio:** • Notificaciones de la Política de uso aceptable • Estado del servicio • Actualizaciones de software • Autenticación y reautenticaciones periódicas • Eventos de seguridad de datos en línea • Notificaciones y flujo de trabajo de DLP de terminales • Notificaciones de eventos de políticas de acceso a Internet y aplicaciones privadas • Protección contra amenazas avanzadas • Notificaciones de seguridad de DNS, IPS y cortafuegos de zero trust de Zscaler • Compatible con notificación de Co-pilot de Zscaler Digital Experience
Herramientas de resolución de problemas integradas	• Obtención automatizada de registros cifrados • Exportaciones manuales de registros • Soporte para captura de paquetes automatizada y manual • Soporte de automatización para la supervisión y gestión de servicios

©2025 Zscaler, Inc. Todos los derechos reservados.

Amplio soporte postural	• Ruta del archivo • Clave y valor del registro • Certificado de confianza • Certificado de cliente con CRL • Certificado de cliente validado por el servidor • Estado del cortafuegos • Cifrado de disco completo • Estado de unión al dominio AD • Estado de unión del dominio Entra • Comprobaciones de procesos • Detección de Carbon Black en tiempo real • IP de salida del cliente • Detección de Microsoft Defender en tiempo real	• Detección de CrowdStrike en tiempo real • Puntuación del sistema operativo del dispositivo CrowdStrike ZTA • Puntuación del sensor CrowdStrike ZTA • Detectar antivirus • Comprobaciones de la versión del sistema operativo • Detección de agentes JAMF • Nivel de riesgo de JAMF • Modificación no autorizada • Variable de propiedad • Versión de lanzamiento de Client Connector de Zscaler
Otras capacidades	• Soporte de recuperación ante desastres y continuidad del negocio • Manejo de portal cautivo integrado con bloqueo de red opcional • Administración del cortafuegos de terminal de Client Connector con bloqueo de LAN local • Compatibilidad con cuarentena de dispositivos • Detección y conmutación automatizadas de redes de confianza • Compatibilidad con entornos sin ruta predeterminada (NDR)	

Acerca de Zscaler

Zscaler (NASDAQ: ZS) acelera la transformación digital para que los clientes puedan ser más ágiles, eficientes, resilientes y seguros. Zscaler Zero Trust Exchange™ protege a miles de clientes de ciberataques y de la pérdida de datos gracias a la conexión segura de usuarios, dispositivos y aplicaciones ubicados en cualquier lugar. Distribuida en más de 150 centros de datos en todo el mundo , Zero Trust Exchange™ basada en SSE es la mayor plataforma de seguridad en línea en la nube del mundo. Para obtener más información, visite **www.zscaler.com/es** o síganos en Twitter **@zscaler**.

© 2025 Zscaler, Inc. Todos los derechos reservados. Zscaler™ y otras marcas comerciales enumeradas en **zscaler.com/legal/trademarks** son (i) marcas comerciales registradas o marcas de servicio o (ii) marcas comerciales o marcas de servicio de Zscaler, Inc. en los Estados Unidos y/u otros países. Cualquier otra marca registrada es propiedad de sus respectivos dueños.

+1 408.533.0288 **Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134** **zscaler.com/es**

zscaler™

Zero Trust Everywhere