Zero Trust + IA

Proteja y optimice
su organización

DOCUMENTO TÉCNICO

¿Por qué se necesitan Zero Trust y la IA?

La manera en que se trabaja hoy en día es muy diferente a la de hace varios años. Antes los empleados iban a la oficina todos los días a trabajar. Al hacerlo, accedían a aplicaciones y recursos de TI alojados en los centros de datos locales de sus organizaciones. En pocas palabras, con los usuarios, las aplicaciones y los datos en la oficina, las organizaciones operaban esencialmente de manera local. Sin embargo, dos fenómenos que se reforzaron mutuamente cambiaron para siempre este status quo.

En primer lugar, el auge de la nube y las aplicaciones de software como servicio (SaaS) como Salesforce y Microsoft 365 significó que las organizaciones ya no tenían que crear o administrar sus recursos de TI en las instalaciones. En vez de ello, podían utilizar aplicaciones y herramientas creadas específicamente y suministradas como servicios desde las nubes de los proveedores. Esta flexibilidad mejoró significativamente el dinamismo y redujo los costos de las organizaciones.

En segundo lugar, y en gran parte debido a la adopción de aplicaciones en la nube, los usuarios comenzaron a trabajar de manera remota. Después de todo, los recursos de TI estaban fuera de las instalaciones y los usuarios ya no tenían que ir a la oficina para acceder a ellos. Lógicamente, la pandemia mundial de 2020 aceleró la adopción del trabajo remoto (y de las aplicaciones en la nube), ya que las organizaciones trataban de seguir siendo productivas a la vez que cumplían con los mandatos de refugio designado. Una vez más, el aumento de la flexibilidad sirvió tanto para el dinamismo como para el ahorro de costos.

Estas transformaciones, si bien fueron increíblemente útiles, dieron lugar a importantes desafíos en torno al ciberriesgo y la presión competitiva:

- El ciberriesgo aumentó porque los modelos de seguridad tradicionales no estaban diseñados para la nube o el trabajo remoto, y no podían seguir el ritmo de la creciente sofisticación de las amenazas modernas.
- Las presiones competitivas aumentaron porque una mayor productividad y dinamismo se convirtieron en la norma, desafiando a las organizaciones a operar lo más eficientemente posible y al mismo tiempo satisfacer las crecientes expectativas de los clientes lo más rápido posible.

Para que las organizaciones tengan éxito en la actualidad, deben abordar estos dos desafíos. Por ello, otro fenómeno increíblemente importante en este tema es la aparición de la inteligencia artificial y el aprendizaje automático (IA/ML). En muy poco tiempo, la IA se ha extendido ampliamente por todo el lugar de trabajo moderno, tanto en las empresas como en las soluciones de ciberseguridad. Aunque pueda parecer fácil desestimar la IA por ser la última palabra de moda en marketing, lo cierto es que la IA tiene la clave para abordar el doble desafío anterior; al menos cuando la IA se combina con Zero Trust. Por eso, múltiples organizaciones de todo el mundo están recurriendo a Zscaler.

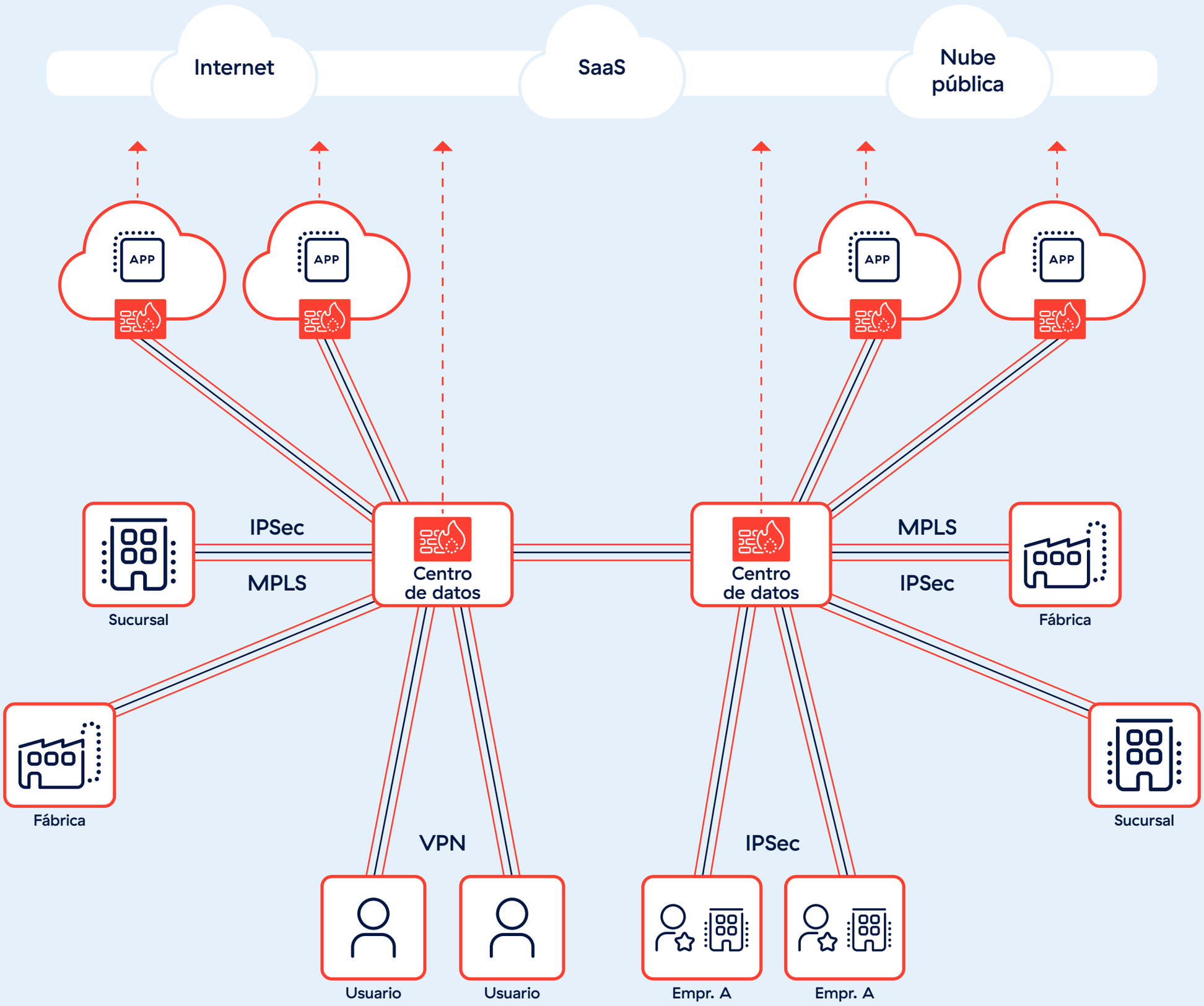
Zero Trust + IA con Zscaler

La plataforma nativa de la nube Zscaler Zero Trust Exchange ofrece una arquitectura Zero Trust dotada de IA/ML para aumentar sus capacidades. Esta potente combinación de arquitectura Zero Trust e IA resuelve los dos problemas antes mencionados en torno al aumento del riesgo y la creciente presión para hacer más con menos. Para entender por qué, analicemos cada uno de estos elementos.

ARQUITECTURA ZERO TRUST

Zero Trust no es simplemente otra palanca para mantener el status quo y no es simplemente otro producto de seguridad. Más bien, es una manera fundamentalmente diferente de hacer las cosas, distinta de las arquitecturas de seguridad estándar basadas en perímetros, libre de las deficiencias de las metodologías de ayer. Por eso es de vital importancia utilizar Zero Trust como base para implementar la IA en la seguridad. De lo contrario, intentar mejorar una arquitectura de seguridad basada en el perímetro con IA es como pulir un espejo roto: puede que brille más, pero sigue siendo defectuoso.

Arquitectura centrada en firewalls y VPN



Una red confiable conecta usuarios, sitios y aplicaciones.
Las amenazas y la protección de datos se centran en asegurar la red.

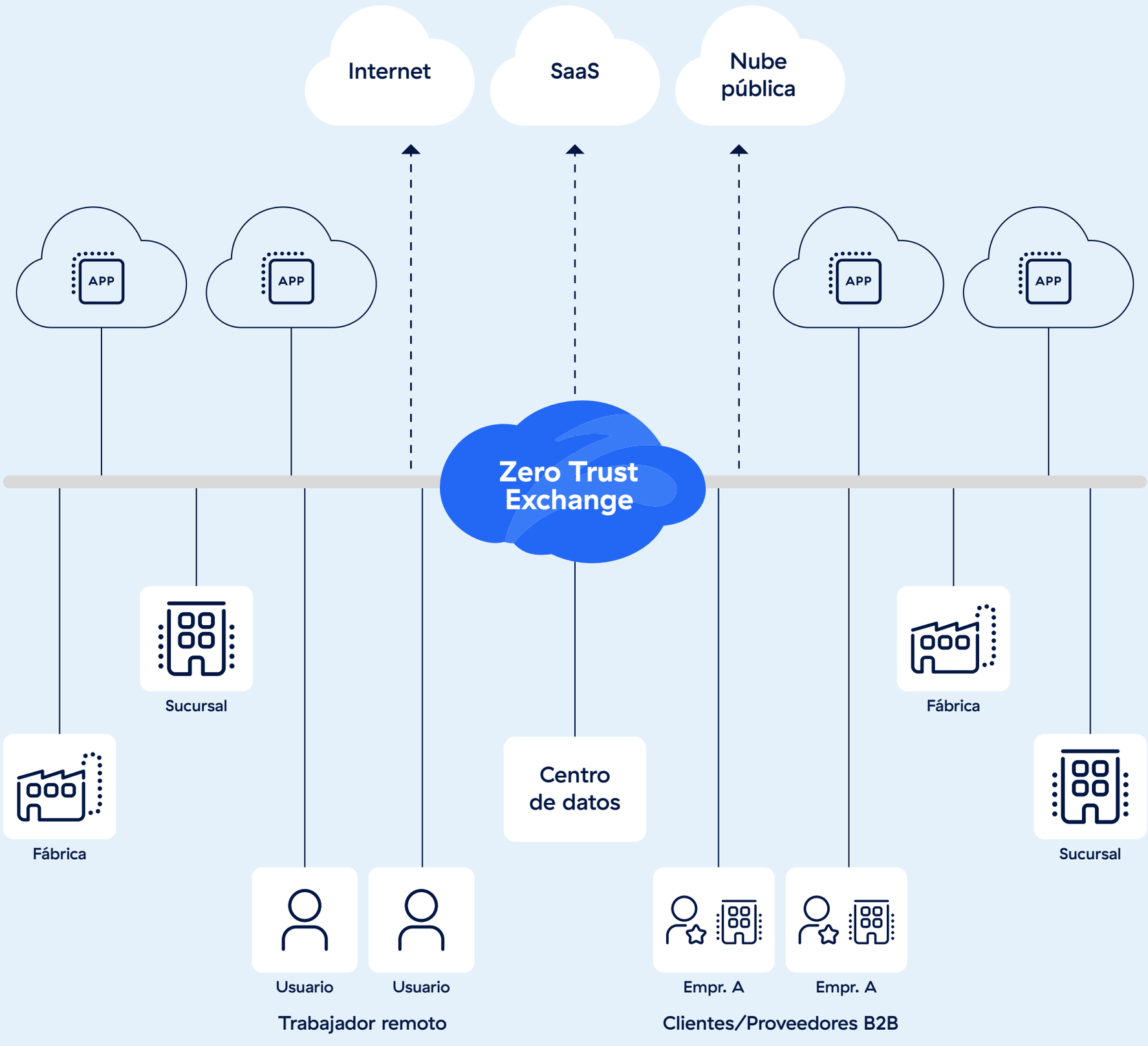
Es rígido, complejo, un riesgo para la seguridad y un obstáculo para la transformación.

Figura 1: Arquitectura basada en el perímetro

Las arquitecturas perimetrales basadas en herramientas como firewalls y VPN se centran en establecer un perímetro seguro alrededor de la red central de una organización. Por eso a menudo se les llama modelos de seguridad “castle-and-moat”. Las arquitecturas basadas en el perímetro se diseñaron para el mundo exclusivamente local, antes del auge de las aplicaciones en la nube y el trabajo remoto. Cuando las organizaciones intentan utilizarlas hoy en día, estas arquitecturas crean una serie de desafíos:

- Amplían la superficie de ataque extendiendo la red a más usuarios, dispositivos, nubes y ubicaciones, y utilizando firewalls y VPN, que tienen direcciones IP públicas.
- Permiten el compromiso porque sus dispositivos subyacentes (hardware y virtuales) carecen de la escalabilidad para inspeccionar el tráfico cifrado a escala, **donde se esconde el 86 % de las amenazas**.
- No logran detener el movimiento lateral de amenazas porque colocan a los usuarios y entidades en la red, donde pueden acceder a los diversos recursos conectados en ella.
- No pueden eliminar la pérdida de datos debido a la incapacidad de escalar e inspeccionar el tráfico cifrado y de proteger las rutas de fuga modernas, como el uso compartido en aplicaciones SaaS.
- Aumentan la complejidad y los costos a través de una cantidad de productos puntuales de seguridad y redes extensas, que son costosos de comprar, configurar y mantener.
- Perjudican la productividad del usuario porque requieren retransmitir el tráfico a un centro de datos centralizado, lo que agrega latencia que interrumpe las experiencias digitales.

En 2024 se produjeron una serie de vulnerabilidades de firewall y VPN de **Ivanti**, **Cisco** y **Palo Alto Networks**, lo que destacó la necesidad de retirar estas herramientas y adoptar una arquitectura Zero Trust.



Las políticas empresariales determinan quién puede acceder a qué a través de cualquier red; la red es solo el transporte.

Es ágil, sencillo, seguro y permite la transformación.

Figura 2: Arquitectura Zero Trust con Zscaler

Como se mencionó anteriormente, Zero Trust es fundamentalmente diferente de las arquitecturas basadas en el perímetro. En lugar de ser como un foso que protege un castillo (el perímetro de la red), Zero Trust es como una centralita inteligente que proporciona una conectividad segura individualizada: los usuarios se conectan directamente a las aplicaciones en lugar de a la red en su conjunto.

El contexto se utiliza para determinar quién debería poder acceder a qué. En otras palabras, Zscaler desvincula la seguridad y la conectividad del acceso a la red y aplica el principio de acceso con privilegios mínimos. Esta conectividad Zero Trust (y una gran cantidad de otras funcionalidades) se suministra como un servicio, en el perímetro, desde el Zero Trust Exchange, la nube de seguridad global

de alto rendimiento de Zscaler. El tráfico de retorno se convierte en cosa del pasado.

Con Zscaler, la arquitectura Zero Trust:

- Minimiza la superficie de ataque al detener la expansión infinita de la red, eliminando la necesidad de firewalls, VPN y sus direcciones IP públicas, y ocultando aplicaciones detrás de Zscaler.
- Detiene los riesgos a través de una nube de seguridad de alto rendimiento que se escala según sea necesario para inspeccionar cualquier volumen de tráfico cifrado y aplicar políticas en tiempo real.
- Previene el movimiento lateral de amenazas al conectar a los usuarios directamente a las aplicaciones a las que están autorizados a acceder en lugar de a la red con sus numerosos recursos conectados.
- Bloquea la pérdida de datos, ya sea maliciosa o accidental, en todas las rutas de fuga de datos, incluido el tráfico cifrado, las aplicaciones en la nube y los puntos finales.
- Reduce costos y complejidad al simplificar la red con conectividad directa a la aplicación y al eliminar productos puntuales de seguridad con una plataforma integral
- Mejora la productividad al mejorar las experiencias de los usuarios mediante la conectividad directa a la aplicación y el enrutamiento del tráfico por la ruta más corta hasta su destino.

Por todas estas razones, Zero Trust es la base arquitectónica ideal para implementar la IA/ML.

LIDERAZGO EN IA

Zscaler tiene claras ventajas en el área de IA/ML. Esto se debe en gran medida a que la IA solo es tan eficaz como los datos de los que es capaz de aprender; en términos simples: sale lo viejo y entra lo nuevo.

Como la mayor plataforma de seguridad del mundo, Zscaler Zero Trust Exchange ofrece conectividad segura como servicio a miles de organizaciones que comprenden más de 40 millones de usuarios en todo el mundo, por no hablar de innumerables cargas de trabajo, dispositivos IoT/OT, trabajadores externos y mucho más. Como resultado de esta escala, Zscaler procesa más de 500,000 millones de transacciones cada día (más de 45 veces el número de búsquedas diarias en Google), así como 500 billones de señales telemétricas diarias. Dado que Zscaler examina el contexto con el fin de gobernar de manera segura el acceso a los recursos de TI, hay datos ricos en torno a la identidad, el dispositivo, el contenido, el destino y la red, para cada intento de acceso. Además, Zscaler cuenta con una gran cantidad de datos de ThreatLabz, nuestro equipo interno líder en investigación de amenazas, que estudia constantemente las últimas tácticas, técnicas y tecnologías de los ciberdelincuentes. Esto dota a Zscaler de años de investigación sobre las ciberamenazas, cómo funcionan y su creciente sofisticación.

Zscaler Data Fabric for Security se ve reforzado por más de 150 integraciones prediseñadas con una variedad de soluciones comerciales y de seguridad. Las fuentes de datos de seguridad incluyen escáneres de vulnerabilidades como Tenable, Qualys y Wiz, soluciones de detección y respuesta de puntos finales (EDR) como CrowdStrike, herramientas de gestión de identidades como las de Okta, Ping Identity y Microsoft, y más de 60 fuentes de información sobre amenazas. Las fuentes de datos empresariales incluyen SAP para los datos de costos y licencias, Workday para la información sobre la estructura organizativa, ServiceNow para la base de datos de gestión de la configuración, etc. Zscaler ingiere datos de todas estas fuentes, los combina con sus conjuntos de datos propios, los deduplica y los enriquece. No es necesario agregar manualmente datos de múltiples fuentes en una sola ubicación, ya que Zscaler maneja el proceso automáticamente.

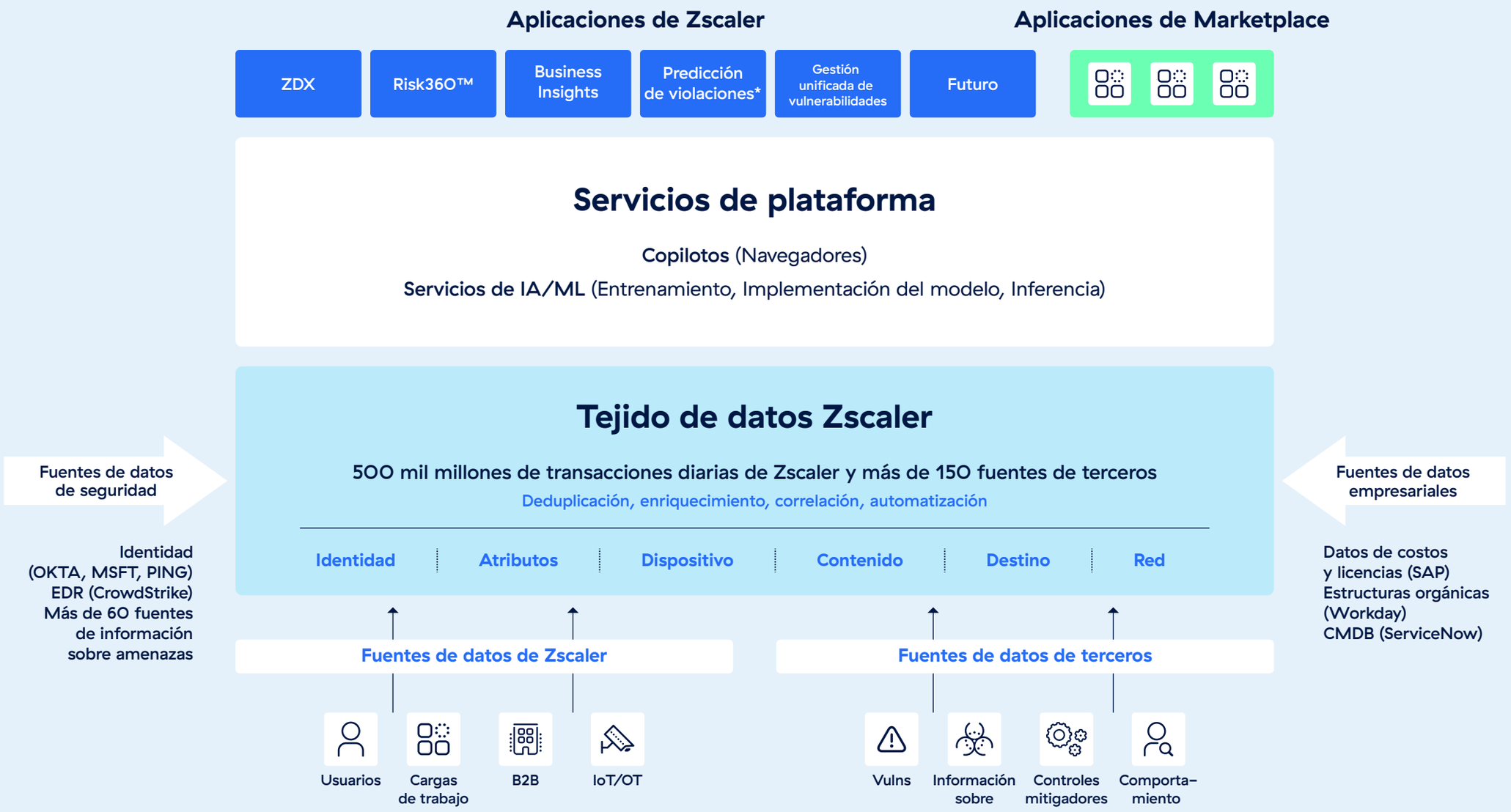


Figura 3: Liderazgo y ventaja de Zscaler en IA

Con este conjunto de datos masivo y altamente relevante que entrena modelos de lenguaje grandes (LLM) especialmente diseñados, Zscaler puede acelerar la aplicación de datos a la toma de decisiones. Las soluciones impulsadas por la IA en todo el Zero Trust Exchange cuentan con análisis, automatización y eficacia mejorados. En el resto de este documento técnico, detallaremos las diversas maneras en que la plataforma Zscaler aprovecha la IA/ML para resolver los desafíos modernos, ayudándole a asegurar y optimizar su organización.

Proteger su organización con Zscaler

La arquitectura Zero Trust, en sí misma, mejora significativamente la seguridad y disminuye el ciberriesgo al superar las debilidades de las arquitecturas basadas en perímetros. Sin embargo, combinar la solidez de la arquitectura Zero Trust con una funcionalidad de seguridad líder basada en IA fortalece aún más las defensas de las organizaciones contra los ciberdelincuentes y las amenazas avanzadas. Zscaler ofrece arquitectura Zero Trust y capacidades impulsadas por la IA para reducir el riesgo y, como beneficio adicional, mejorar la productividad tanto para los usuarios como para los administradores.

Veredicto instantáneo de IA de Cloud Sandbox

Con la creciente sofisticación de las ciberamenazas, las organizaciones necesitan capacidades de detección y mitigación en tiempo real. De lo contrario, pueden verse fácilmente comprometidos por ciberdelincuentes astutos con técnicas elusivas y en constante evolución.

La tecnología Sandbox está diseñada para detonar archivos potencialmente maliciosos en un entorno seguro, lejos del usuario, para determinar si es seguro acceder a dichos archivos.

Lamentablemente, los métodos tradicionales de análisis de espacio aislado implican inherentemente un equilibrio entre seguridad y productividad. Si los criterios de la zona de pruebas son demasiado laxos, los archivos maliciosos pueden llegar a los dispositivos de los usuarios y comprometer la organización. Si los criterios de la zona de pruebas son demasiado estrictos, es más probable que los archivos benignos queden en la zona de pruebas, que se impida innecesariamente el acceso de los usuarios durante varios minutos y que se interrumpa la productividad.

Zero Trust Exchange rompe el statu quo del sandboxing y sus innatas compensaciones entre seguridad y productividad aprovechando el poder de la IA. La integración de ML en Zscaler Sandbox, nativo de la nube, garantiza una mayor fidelidad de detección para los clientes, ya que el modelo ML ha sido entrenado y optimizado basándose en años de análisis e interacciones con más de 550 millones de muestras de archivos.

Cuando los administradores activan el ajuste "AI Instant Verdict" con solo pulsar un botón, los archivos maliciosos de alta confianza con una puntuación de amenaza IA/ML de 91 a 100 se bloquean automáticamente, sin necesidad de que el usuario espere mientras el archivo se detona en otro lugar. Esto proporciona protección inmediata contra amenazas basadas en archivos de día cero y, al mismo tiempo, garantiza que los usuarios puedan seguir siendo productivos. Además, el bloqueo instantáneo de archivos maliciosos de alta confianza minimiza la cantidad de posibles incidentes de pacientes cero que deben investigarse, lo que reduce la carga de trabajo de los equipos SOC y les permite concentrar su tiempo en otras tareas críticas de seguridad. En otras palabras, las organizaciones pueden mantenerse a salvo de las amenazas en evolución al tiempo que se aseguran de que los equipos SOC y los usuarios finales optimicen su tiempo.

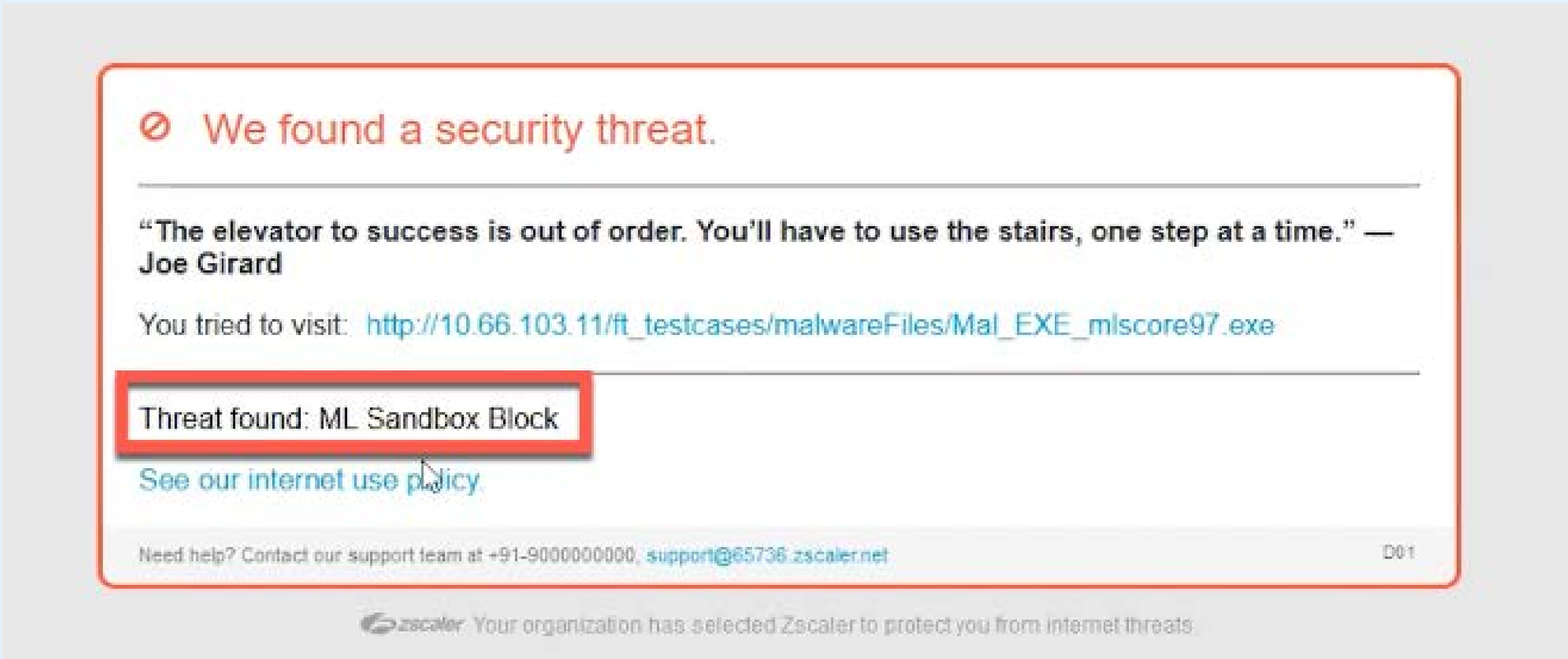


Figura 4: Notificación al usuario de AI Instant Verdict

Smart Browser Isolation

Los ciberdelincuentes utilizan sitios web maliciosos para cargar contenido peligroso en los navegadores y dispositivos de los usuarios, creando puntos de apoyo para organizar sus ataques contra las organizaciones de los usuarios. Las herramientas de filtrado de URL que pueden bloquear el acceso a varios sitios web son la solución ideal para abordar este problema. Normalmente, esto se hace filtrando sitios web maliciosos conocidos, así como dominios recién registrados que aún no han demostrado ser confiables. Lamentablemente, este enfoque tiene debilidades cruciales. En primer lugar, los sitios web confiables y probados en el tiempo aún pueden publicar contenido malicioso sin saberlo; por ejemplo, a través de anuncios o iframes de cero píxeles instalados por ciberdelincuentes. Además, bloquear todos los dominios recién registrados altera la productividad del usuario al impedir el acceso a herramientas web nuevas, pero legítimas, así como a sitios web existentes y confiables que simplemente presentan dominios actualizados; en ambos casos, la afluencia resultante de tickets del servicio de asistencia también afecta la productividad de TI.

Zscaler Smart Browser Isolation supera estos desafíos de seguridad y productividad. La solución se denomina “inteligente” porque incorpora modelos de inteligencia artificial y aprendizaje automático que le permiten reconocer automáticamente contenido web potencialmente malicioso. Como resultado, las organizaciones pueden anticiparse a las amenazas emergentes con dominios recién registrados, así como a las amenazas ocultas dentro de dominios confiables.

Con Smart Browser Isolation, cuando un usuario visita un destino web que la IA determina que tiene una alta probabilidad de ser malicioso, la sesión del usuario se “aísla”. Esto significa que la sesión web se activa en Zero Trust Exchange y solo se envían píxeles de la sesión desde la nube de Zscaler al dispositivo del usuario final. Las secuencias de imágenes de la sesión aislada siguen ofreciendo lo que parece ser la experiencia habitual del usuario, pero éste no interactúa directamente con el sitio web, por lo que el contenido activo no llega a su punto final. Esto significa que los intentos de descarga de amenazas no pueden llegar al dispositivo y la posible fuga de datos se puede controlar evitando la carga de archivos y el pegado de texto. Esto reduce enormemente el riesgo, sin el bloqueo excesivo que impide el acceso a las herramientas web legítimas que los usuarios necesitan. Eso se traduce en menos tickets de asistencia técnica y mejor productividad tanto para los usuarios finales como para TI.

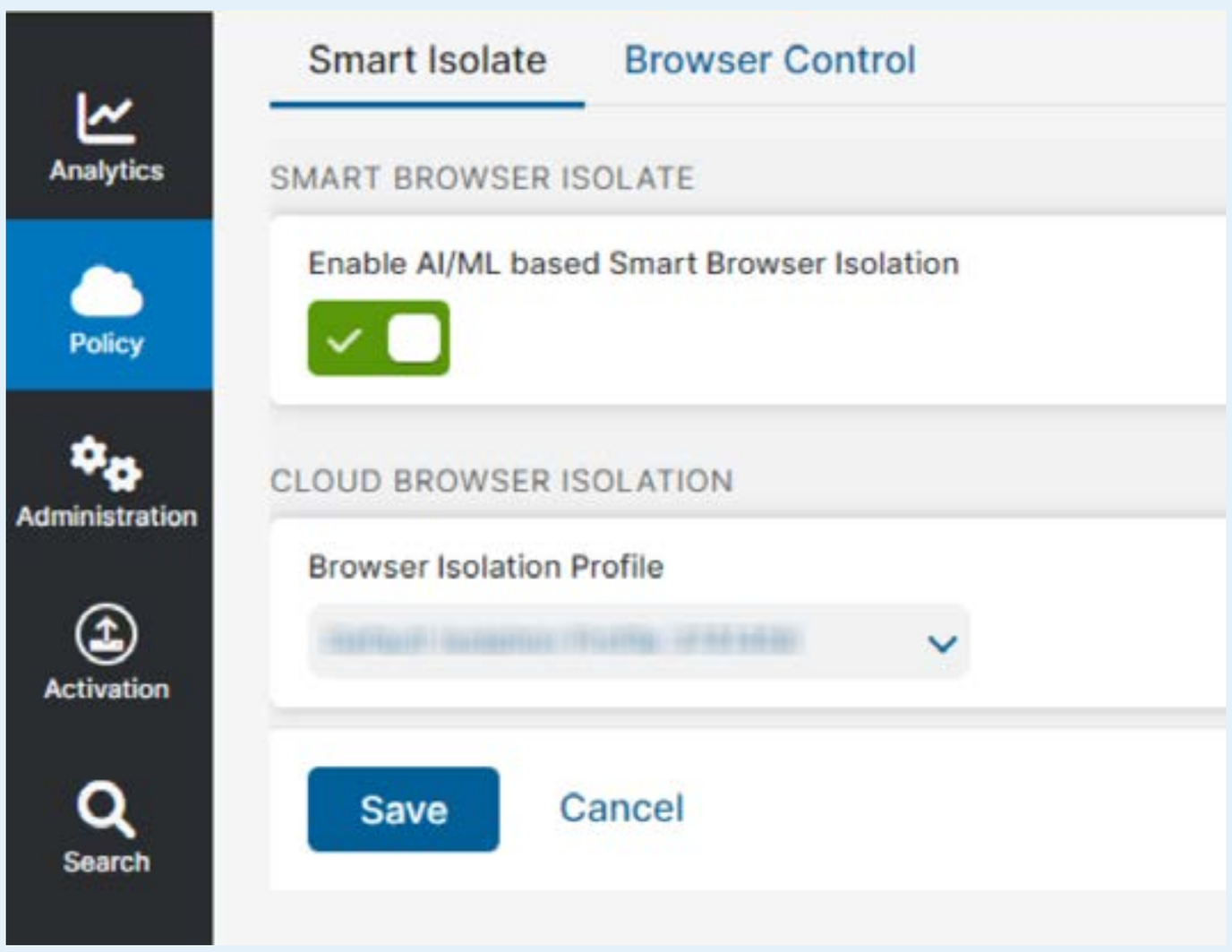


Figura 5: Activación con un solo clic de Smart Browser Isolation

Segmentación de aplicaciones con IA

Las organizaciones que dependen de arquitecturas de seguridad centradas en la red construidas con herramientas tradicionales como firewalls enfrentan un desafío importante para detener el movimiento lateral de amenazas. Como se mencionó anteriormente, el movimiento lateral se refiere a la manera en que los atacantes en la red pueden desplazarse a través de los recursos conectados y acceder a los datos confidenciales que contienen. Sin una segmentación efectiva para evitar esto, el radio de explosión de un ataque puede ser extenso, lo que permite violaciones de datos a gran escala, así como daños significativos a la reputación y a las finanzas.

Lamentablemente, las organizaciones suelen tener dificultades para implementar y mantener prácticas sólidas de segmentación de redes. Los métodos tradicionales se basan en la configuración manual, que es propensa a errores humanos y puede dar lugar a configuraciones erróneas que dejan expuestos a los activos críticos. Además, la naturaleza dinámica de las redes modernas, con la creciente adopción de servicios en la nube y el trabajo a distancia, hace que sea un desafío mantenerse al día de los constantes cambios en la topología de la red y los requisitos de acceso de los usuarios. Esta complejidad aumenta los gastos generales de gestión y obstaculiza aún más la capacidad de implementar estrategias de segmentación efectivas.

Como se explicó anteriormente, la arquitectura Zero Trust de Zscaler se basa en brindar acceso directamente a las aplicaciones en lugar de a la red. Esta segmentación Zero Trust ayuda a evitar el movimiento lateral de usuarios, cargas de trabajo, sucursales y dispositivos. Para reducir aún más el radio potencial de alcance de cualquier violación, Zscaler ofrece segmentación de aplicaciones impulsada por la IA. AI aprovechar la inteligencia artificial, Zscaler crea automáticamente segmentos de aplicaciones ideales para los clientes.

La segmentación de aplicaciones impulsada por la IA funciona mediante la supervisión y el análisis continuos del comportamiento de los usuarios y del uso de las aplicaciones. Aprovecha los algoritmos de ML para identificar patrones y anomalías de modo que pueda determinar qué empleados requieren acceso a qué aplicaciones. Por ejemplo, si solo un pequeño subconjunto de empleados accede a una aplicación financiera, Zscaler creará automáticamente un segmento que restringe el acceso a ese grupo de usuarios. Este enfoque específico reduce en gran medida la oportunidad de movimiento lateral entre aplicaciones.

La segmentación de aplicaciones impulsada por la IA representa un enfoque de segmentación fundamentalmente diferente. Identifica y limita con precisión el acceso a aplicaciones confidenciales de manera proactiva y automática. Al simplificar el proceso de segmentación, se eliminan las complejidades, los errores y los riesgos asociados con los métodos tradicionales. Esto, a su vez, reduce la carga de gestión de la configuración manual, lo que ahorra tiempo y recursos a los equipos de TI, permitiéndoles centrar sus esfuerzos en otras tareas de seguridad críticas.

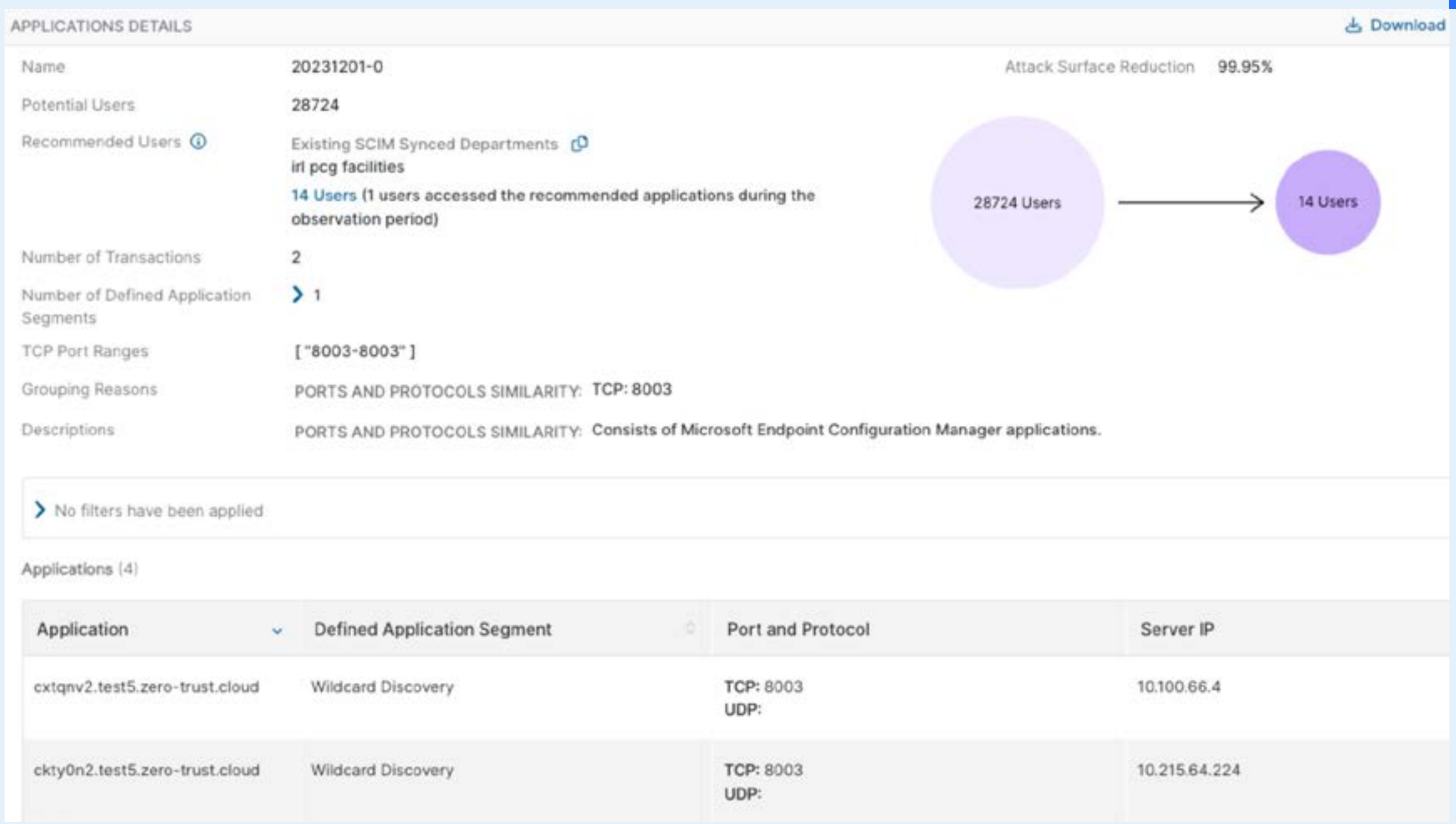


Figura 6: Recomendación de segmentación de aplicaciones basada en IA

Descubrimiento automático de datos con IA

El panorama digital actual representa un desafío importante para la seguridad de los datos. Los datos se distribuyen ampliamente fuera del centro de datos tradicional, se almacenan y se accede a ellos continuamente a través de la web, aplicaciones en la nube y dispositivos de usuarios remotos. Como resultado, las organizaciones se enfrentan a una nueva realidad que hace difícil identificar a dónde va la información confidencial. Esto hace que sea cada vez más difícil para los CISO y los equipos de protección de datos garantizar su protección.

Confiar en productos puntuales como soluciones separadas de prevención de pérdida de datos (DLP) en la red, la nube, la web y los puntos finales para proteger los datos distribuidos ha demostrado ser ineficaz. Estas herramientas suelen funcionar en silos, lo que genera brechas de visibilidad y tiempos de respuesta lentos. Además, requieren la duplicación manual de las políticas en soluciones desarticuladas, lo que constituye un proceso propenso a errores y que requiere mucho tiempo. En última instancia, este enfoque gradual aumenta el riesgo de pérdida de datos, así como el costo y la complejidad.

Con Zscaler AI Auto Data Discovery, las organizaciones pueden acelerar su capacidad para buscar, clasificar y controlar automáticamente los datos a medida que se crean y dondequiera que vayan. Zscaler AI ha sido entrenado a fondo para identificar archivos y datos confidenciales en cualquier contexto, ya sea en reposo dentro de SaaS, IaaS, o PaaS, en uso en el punto final de un usuario, o en movimiento a la web a través de tráfico cifrado. Los administradores no necesitan duplicar reglas a través de herramientas inconexas, o incluso configurar diccionarios o políticas de clasificación de datos en Zscaler, para encontrar datos confidenciales. La solución es exhaustiva en su alcance y automatizada en su ejecución, lo que minimiza las brechas de visibilidad que dejan otras herramientas

y reduce los errores derivados de la creación manual de reglas. Como resultado, las organizaciones pueden lograr una detección y una protección de datos más rápidas y precisas, garantizando que la información confidencial esté asegurada en todos los canales de fuga de datos.

Además de proporcionar una mayor protección, la detección automática de datos mediante IA también reduce la complejidad de la supervisión de la seguridad de los datos. Como ya se ha señalado, se minimiza el número de paneles de control de productos puntuales, se elimina la necesidad de duplicar manualmente las políticas y ni siquiera es necesario configurar los diccionarios de DLP. La automatización impulsada por la IA reduce la necesidad de conocimientos especializados y, al mismo tiempo, ayuda a las organizaciones a implementar y administrar programas de protección de datos más rápidamente. El resultado final es una seguridad mejorada y una mayor productividad para los administradores.

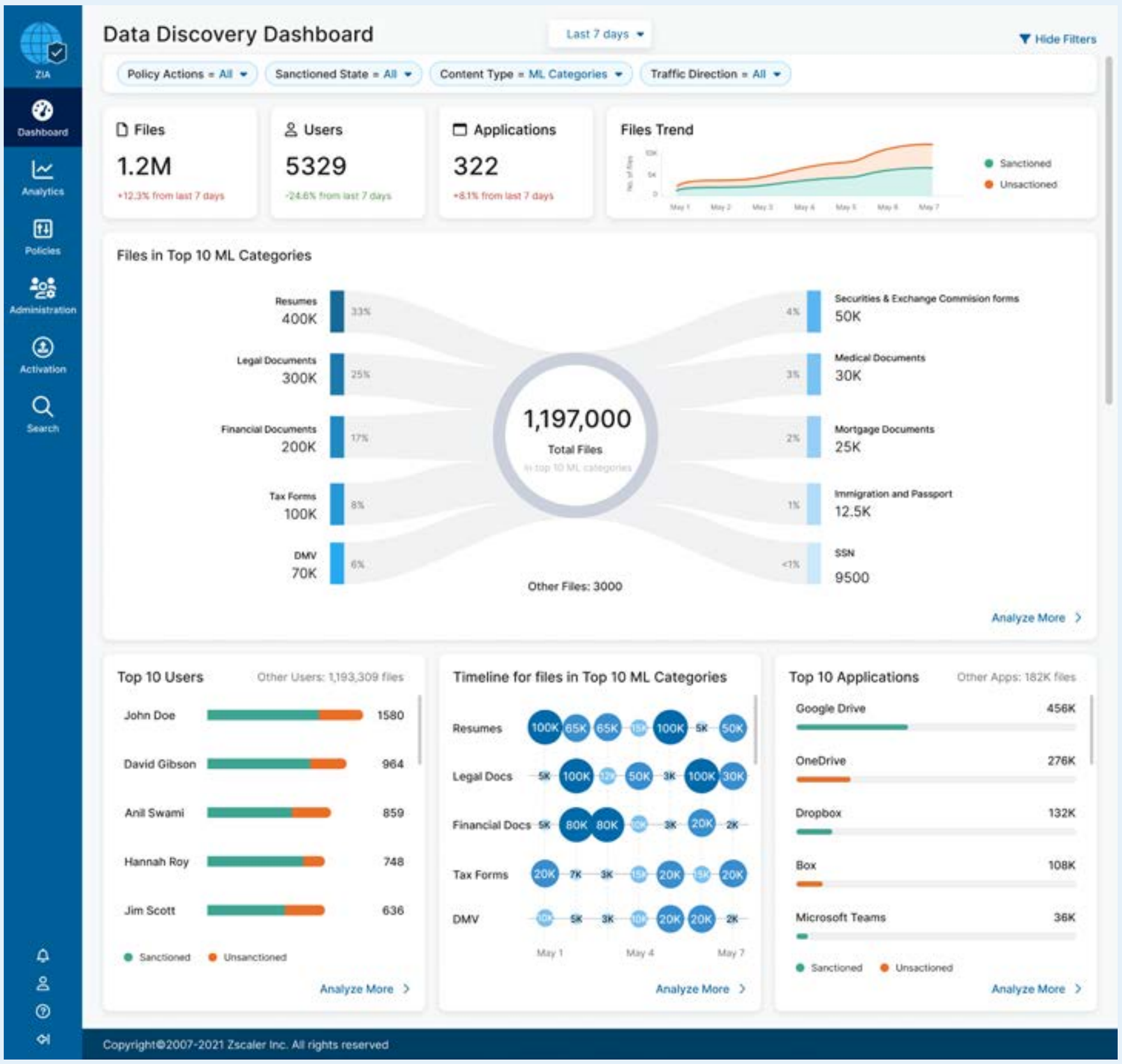


Figura 7: Panel de control de AI Auto Data Discovery

Optimización de su organización con Zscaler

La plataforma Zscaler en la nube ofrece seguridad y conectividad como servicio, lo que significa que todo el tráfico de los clientes fluye a través de Zero Trust Exchange. Gracias a su exclusiva perspectiva en línea y a las integraciones preconfiguradas con más de 150 soluciones empresariales y de seguridad, Zscaler puede generar perspectivas de gran alcance y ofrecer análisis y toma de decisiones totalmente automatizados, en tiempo real y basados en IA, sin la complejidad de la agregación y recopilación de datos. En otras palabras, al aprovechar tanto Zero Trust como la IA con Zscaler se consigue algo más que mejorar la seguridad: también se optimizan las organizaciones de las siguientes maneras.

Experiencia digital de Zscaler (ZDX)

Los usuarios de todo el mundo se apresuran a adoptar las aplicaciones en la nube y el trabajo híbrido porque proporcionan una flexibilidad superior en comparación con los entornos tradicionales exclusivamente locales. Sin embargo, la transformación digital también crea toda una amalgama de enlaces de red y enrutamiento que abarcan todo el mundo, ISP, redes Wi-Fi domésticas, dispositivos propiedad de los empleados, aplicaciones SaaS y más, muchos de los cuales se encuentran fuera del perímetro de la red corporativa. Como resultado, esta evolución crea dos problemas importantes para la productividad de cualquier organización.

En primer lugar, cada nueva nube, red, dispositivo o ubicación aumenta la complejidad y añade un punto potencial de falla más. Como resultado, es más probable que las experiencias digitales (y la productividad de los usuarios) se vean interrumpidas. En segundo lugar, los entornos multifacéticos implican una visibilidad desarticulada de las experiencias digitales. Las herramientas de supervisión de dispositivos, redes y aplicaciones utilizadas por diferentes equipos solo ven fragmentos de la cadena de distribución de aplicaciones. Esto deja puntos ciegos entre el dispositivo del usuario y la aplicación, y requiere equipos separados para exportar y correlacionar manualmente los datos de cada herramienta. En consecuencia, los equipos del servicio de asistencia tienen que esforzarse desmesuradamente para resolver los problemas, lo que supone una pérdida de tiempo muy valiosa para ellos y para el usuario final.

Zscaler Digital Experience (ZDX), parte de Zero Trust Exchange, fue diseñado para abordar los problemas anteriores. Al aprovechar la arquitectura de proxy en línea de Zscaler, ZDX tiene la base necesaria para romper los silos de supervisión de dispositivos, redes y aplicaciones, y proporcionar una visibilidad completa de extremo a extremo de las experiencias de los usuarios.

La solución utiliza la visibilidad anterior para alimentar el análisis de causas raíz impulsado por la IA, que soluciona automáticamente los problemas de la experiencia del usuario, descubre sus orígenes subyacentes y acelera la resolución, con solo pulsar un botón. Esta misma IA es aprovechada por un panel de incidencias que ofrece correlación automatizada para detectar problemas ocultos que afectan a múltiples usuarios, tanto si los problemas provienen de aplicaciones, Wi-Fi, ISP, puntos finales o cualquier otra fuente. Más recientemente, ZDX ha agregado el autoservicio para los usuarios. Un motor de IA que se ejecuta en el agente **Zscaler Client Connector** notifica a los usuarios acerca de problemas como una Wi-Fi deficiente o una elevada utilización de la CPU y les sugiere maneras de resolverlos por sí mismos, sin necesidad de abrir tickets. Por último, toda esta funcionalidad se ha ampliado al procesamiento del lenguaje natural a través de ZDX Copilot, de modo que los administradores pueden formular preguntas a un asistente de IA generativa que les ayuda a automatizar tareas, obtener información sobre la experiencia digital y realizar análisis en profundidad.

Esta potente combinación de capacidades agiliza la resolución de problemas para los equipos de TI y garantiza que los usuarios disfruten de las experiencias digitales más productivas posibles.

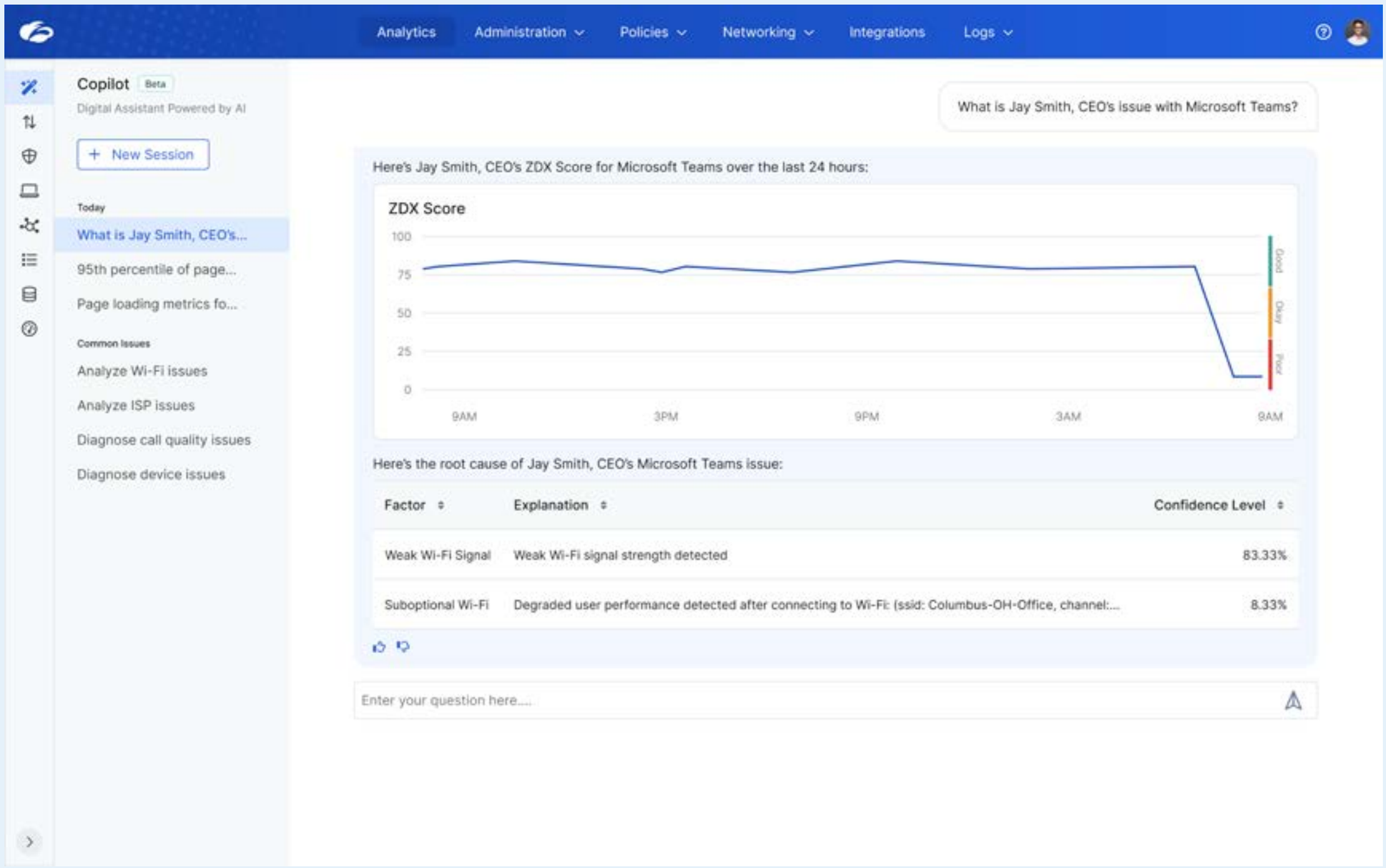


Figura 8: ZDX Copilot respondiendo a una indicación

Business Insights

Las aplicaciones SaaS mejoran la productividad y la flexibilidad de las organizaciones. Pero la facilidad con la que se pueden implementar también crea desafíos en torno a la gestión y optimización del uso de SaaS. Tener licencias independientes para aplicaciones SaaS redundantes como Box, Dropbox y Google Drive aumenta el gasto en SaaS y los gastos operativos. Las licencias y asignaciones SaaS no utilizadas también malgastan recursos.

El trabajo remoto e híbrido también favorece la flexibilidad y la productividad de los empleados. Sin embargo, alterar el lugar donde se realiza el trabajo significa intrínsecamente que las pautas tradicionales de utilización de las oficinas cambian considerablemente. Como resultado, las organizaciones tienen dificultades para determinar cómo pueden gestionar mejor su uso del espacio de oficinas, y tanto los recursos como las finanzas se malgastan inevitablemente.

Las organizaciones deben obtener visibilidad de su SaaS y del uso de la oficina si quieren optimizar sus operaciones y eliminar costos innecesarios. Pero las maneras habituales de obtener esta visibilidad suelen ser manuales, requieren mucho tiempo y son propensas a inexactitudes. Los datos aislados y las herramientas fragmentadas dificultan que los equipos de TI, adquisiciones e instalaciones tomen decisiones informadas que fomenten el ahorro.

Zscaler Business Insights proporciona a las organizaciones una visibilidad completa y precisa de sus aplicaciones y lugares de trabajo SaaS. Esto se consigue gracias a la potencia de Zero Trust Exchange, la nube de seguridad en línea de Zscaler, que procesa todo el tráfico de los clientes y puede ver quién está trabajando, dónde y cuándo, y qué recursos están utilizando. Las integraciones preconstruidas con soluciones empresariales como SAP y Workday enriquecen los datos de Zscaler con información sobre costos, licencias y estructura organizativa. La IA aprovecha el conjunto de datos combinados y permite a los líderes funcionales tomar decisiones basadas en datos que conducen a una asignación de recursos y un gasto más eficientes.

Para optimizar el SaaS, Business Insights ofrece una visibilidad completa del uso de las aplicaciones. Identifica las aplicaciones redundantes y proporciona información sobre la participación de las aplicaciones SaaS, los planes y las licencias adquiridas y los usuarios activos. Cuando se trata de planificar el espacio de trabajo y optimizar el uso de la oficina, Business Insights ofrece información útil sobre las tendencias del espacio de oficina, como los días y las horas en que los trabajadores están en el lugar, así como los departamentos que asisten a la oficina.

Business Insights permite a las organizaciones tomar decisiones informadas para poder adoptar SaaS y el trabajo híbrido de manera más eficiente.

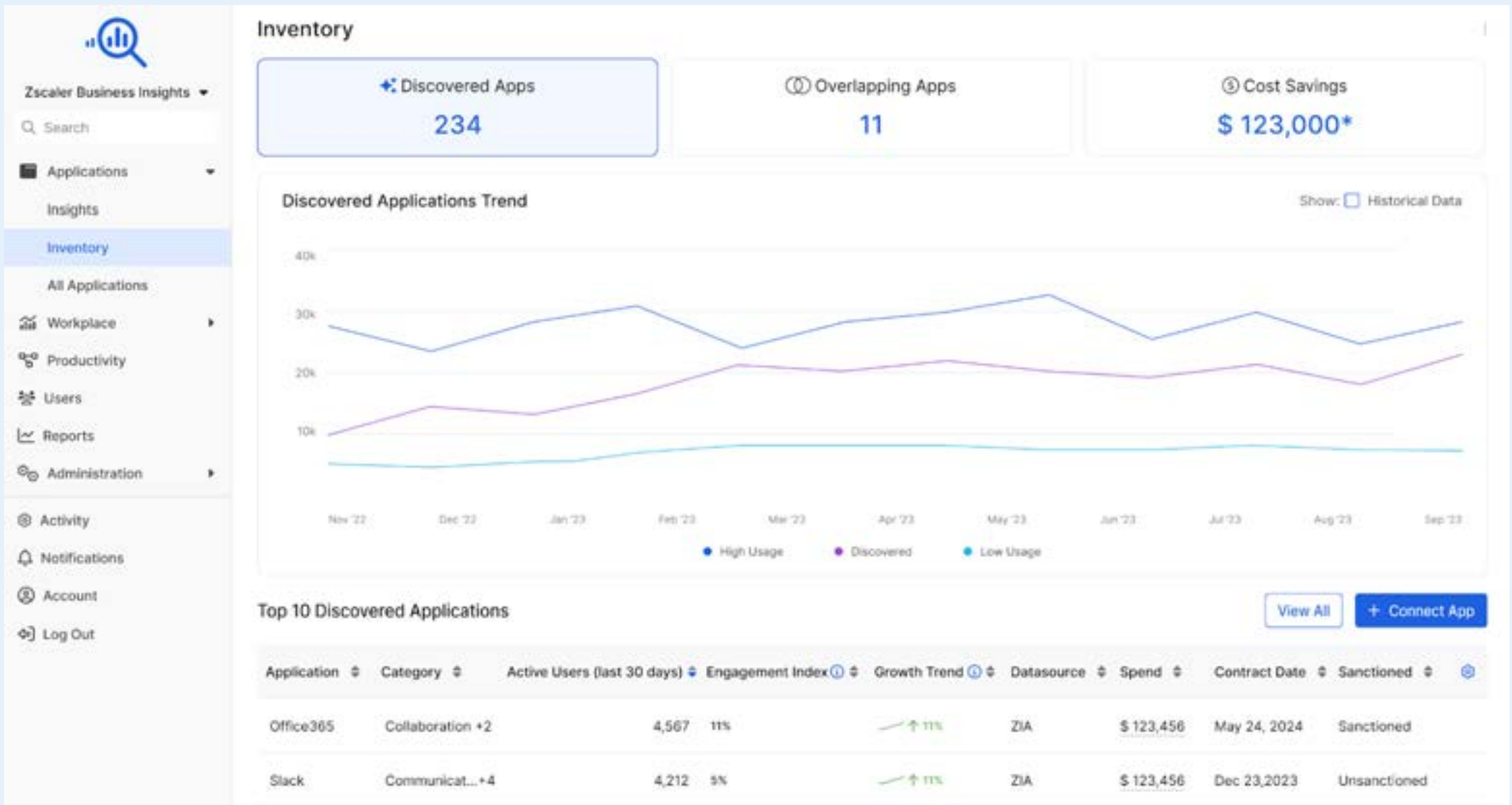


Figura 9: Panel de control de Business Insights

Risk360

En el panorama digital actual, en rápida evolución, las organizaciones se enfrentan a una complejidad cada vez mayor y a un número creciente de vulnerabilidades. Para empeorar las cosas, los ciberdelincuentes perfeccionan constantemente sus métodos, adoptan las últimas técnicas maliciosas y aumentan la sofisticación de sus ataques. Las herramientas de seguridad tradicionales y los procesos manuales se quedan cortos a la hora de proporcionar una visión completa de estos riesgos. Esto se debe a que los paneles de seguridad aislados y los datos fragmentados dificultan a los responsables de seguridad la evaluación integral y la reparación eficaz de los riesgos.

El cumplimiento de las normas de seguridad suma otra capa de dificultad. Las organizaciones deben proporcionar pruebas de prácticas de gestión de riesgos suficientes como parte de la demostración del cumplimiento de las normativas del sector. Sin embargo, sin un marco de gestión de riesgos unificado e integrado, las organizaciones tienen dificultades para asignar sus controles de seguridad a los requisitos normativos, lo que dificulta la elaboración de informes sobre la postura de riesgo y el cumplimiento de las normas.

Para comprender el riesgo y demostrar el cumplimiento, los administradores de seguridad tienen la tarea de agregar información de varias fuentes inconexas y crear informes. Pero este proceso minucioso y manual hace perder tiempo y aumenta los gastos generales de gestión.

Para hacer frente a estos desafíos, Zscaler ofrece Risk360, un marco completo y procesable que ofrece una potente cuantificación del ciberriesgo. Risk360 aprovecha automáticamente los datos en tiempo real del entorno Zscaler de una organización, fuentes externas y años de investigación de seguridad del equipo de investigación de amenazas de clase mundial Zscaler ThreatLabz. No es necesario agregar datos manualmente ni juntar informes.

Risk360 ofrece una visión integral de la postura de seguridad de una organización y cuantifica el riesgo asociado a la exposición de la superficie de ataque, el potencial de compromiso, la posibilidad de movimiento lateral y la probabilidad de pérdida de datos. Ofrece evaluaciones de la madurez de la ciberseguridad impulsadas por la IA que sustituyen a las costosas iniciativas de consultoría y dan a las empresas una mejor idea de en qué punto se encuentran en su camino hacia Zero Trust. La solución proporciona visualizaciones intuitivas de los riesgos, información granular sobre los factores de riesgo, detalles de la exposición financiera, informes listos para la junta directiva y perspectivas procesables que las organizaciones pueden poner en práctica inmediatamente para mitigar los riesgos. También ayuda con el cumplimiento de la seguridad a través de mapeos prediseñados para marcos como MITRE ATT&CK y NIST CSF, así como soporte de informes para **el artículo 106 del Reglamento S-K de la SEC**.

Con Risk360, las organizaciones pueden evaluar y minimizar sistemáticamente el riesgo, garantizar el cumplimiento normativo, reducir la carga administrativa y aliviar los gastos generales de gestión. En otras palabras, esta solución es otro ejemplo más de la capacidad de Zscaler para proteger y optimizar organizaciones con la potencia de Zero Trust y la IA.

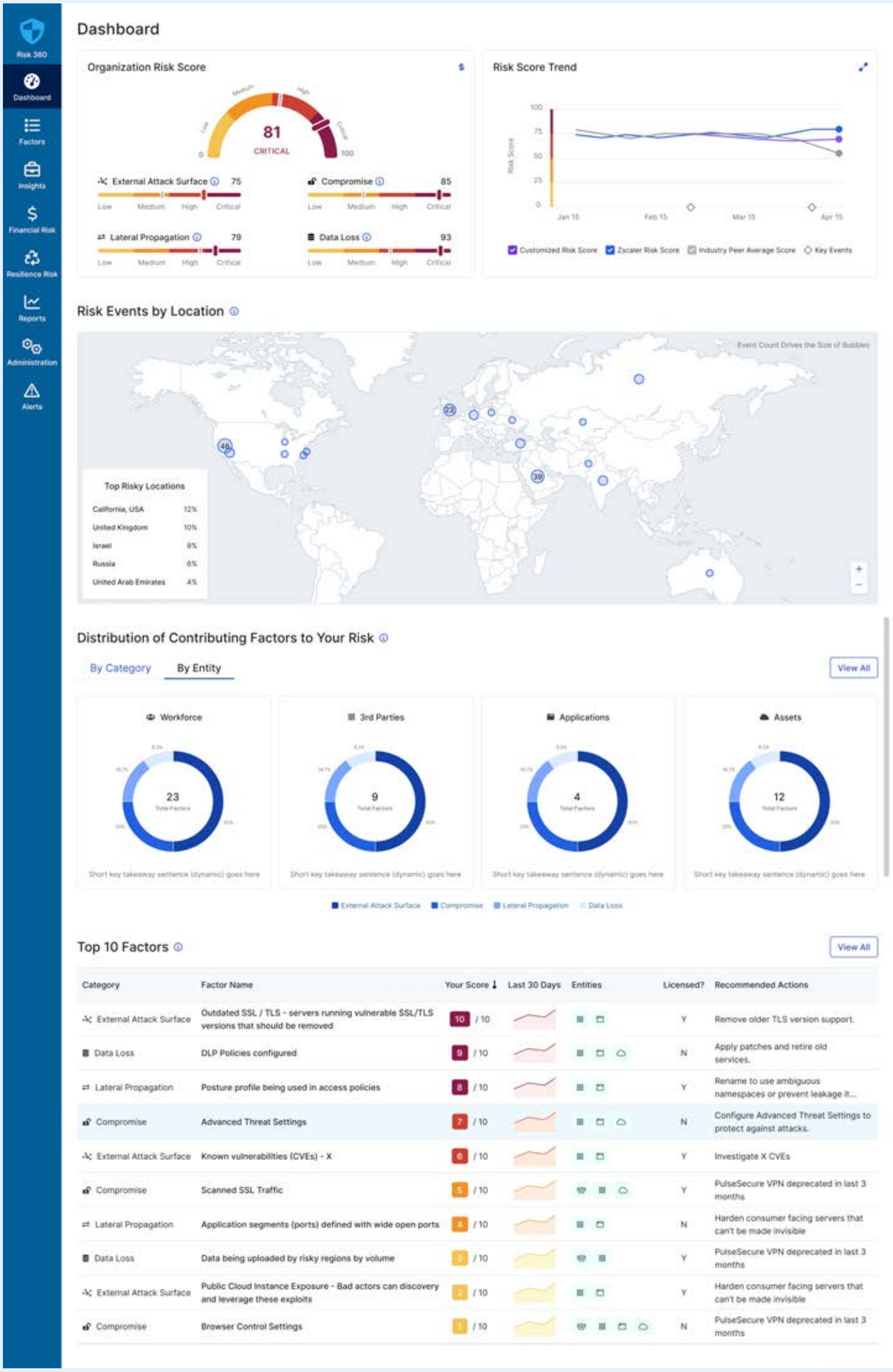


Figura 10: Panel de control de Risk360

Resumen

El doble desafío del ciberriesgo y la presión competitiva es más intenso que nunca. Para sobrevivir, las organizaciones deben detener las ciberamenazas y la pérdida de datos, así como asegurarse de operar de la manera más eficiente posible. Afortunadamente, la combinación de Zero Trust e IA es un dúo potente que se adapta perfectamente a ambos desafíos.

Como pionero original e innovador constante en materia de arquitectura Zero Trust, Zscaler reduce sistemáticamente el riesgo para un sinfín de clientes en todo el mundo. Su plataforma Zero Trust Exchange presume de una escala sin precedentes y de múltiples integraciones que potencian las ventajas estratégicas en datos e IA/ML. En otras palabras, con Zscaler, podrá proteger y optimizar su organización como nunca antes.

Si desea obtener más información sobre Zero Trust y por qué Zscaler se encuentra en una posición única para cumplir las promesas de esta arquitectura moderna, inscríbase en una de las próximas entregas de nuestro seminario web mensual, **“Zero Trust 101: comience su recorrido aquí”.** Es la primera de una serie de tres partes diseñada para guiarle durante todo su proceso de adopción de Zero Trust.

O, si desea ver las capacidades de IA analizadas en este documento técnico (y más), puede **solicitar una demostración personalizada.**

Acerca de Zscaler
Zscaler (NASDAQ: ZS) acelera la transformación digital para que los clientes puedan ser más ágiles, eficientes, resistentes y seguros. Zscaler Zero Trust Exchange protege a miles de clientes de ciberataques y pérdida de datos al conectar de manera segura usuarios, dispositivos y aplicaciones en cualquier ubicación. Distribuido en más de 150 centros de datos en todo el mundo, Zero Trust Exchange basado en SSE es la plataforma de seguridad en la nube en línea más grande del mundo. Obtenga más información en **zscaler.com/mx** o síganos en Twitter **@zscaler.**

+1 408.533.0288 **Zscaler, Inc. (Oficinas centrales) • 120 Holger Way • San José, CA 95134** **zscaler.com/mx**

zscaler™

Zero Trust Everywhere