Bloquee su nube:

Mejores prácticas para proteger aplicaciones críticas

DOCUMENTO TÉCNICO

Tabla de contenido

¿Qué sucede cuando las aplicaciones se trasladan a la nube pública? 4

La importancia de proteger las aplicaciones críticas en la nube 5

Desafíos en la protección de aplicaciones críticas para la misión 6

- El modelo de responsabilidad compartida y sus inconvenientes 6
- Retos de seguridad generales para proteger aplicaciones críticas para la misión 7

5 mejores prácticas para proteger aplicaciones críticas en la nube 7

Cómo Zscaler ayuda a las empresas a proteger las aplicaciones críticas para su misión 9

- Validación del impacto de Zscaler: conclusiones de la reseña del producto realizada por SANS 9

Consiga una seguridad integral en la nube 10

Para muchas organizaciones, la migración de los centros de datos locales tradicionales a plataformas de nube pública está en su recta final, y podría completarse en tan solo unos años. Para 2027, Gartner predice que el 90 % de las organizaciones mantendrán al menos algunas de sus aplicaciones en nubes públicas. El año siguiente, la computación en la nube habrá completado su transición de disruptor tecnológico a necesidad empresarial, y con razón.

Los entornos de nube permiten a las organizaciones aumentar rápidamente los recursos, implementar nuevos servicios y reducir los costos de infraestructura en comparación con las configuraciones locales tradicionales. Al priorizar la adopción de la nube para cargas de trabajo de misión crítica, las empresas pueden adaptarse, innovar y prosperar rápidamente en el panorama dinámico de la actualidad.

Pero las nuevas oportunidades conllevan un mayor riesgo.

En la carrera por migrar a la nube, algunas organizaciones han priorizado la rápida transformación digital por encima de las mejores prácticas de seguridad, lo que las ha dejado en una posición vulnerable. En consecuencia, los ciberatacantes ven los objetivos basados en la nube como caminos potencialmente fáciles para obtener ganancias sustanciales y están evolucionando sus tácticas para explotar estas vulnerabilidades.

En el mundo híbrido y multinube actual, las organizaciones tienen más libertad que nunca para construir dónde y cuándo quieran. Pero esto se contrasta con una preocupación generalizada por la seguridad de las nubes públicas, lo que indica la necesidad de adoptar mejores herramientas y prácticas de seguridad.

Para navegar por este panorama complejo, las empresas están recurriendo a la zero trust: un marco de seguridad moderno y nativo de la nube que garantiza que solo los usuarios y dispositivos autorizados obtengan acceso a recursos críticos de la nube. Con una estrategia de seguridad en la nube bien diseñada, las organizaciones pueden avanzar en gran medida en la prevención de violaciones, mejorar el cumplimiento y generar una mayor confianza de los clientes.

A medida que las organizaciones trasladan sus aplicaciones críticas a la nube, es fundamental repensar sus estrategias de seguridad, en particular con la gobernanza y el cumplimiento de los datos bajo el microscopio regulatorio.

Este documento técnico destaca los riesgos clave que enfrentan los líderes de TI y los equipos de seguridad en la nube al intentar proteger las transformaciones en la nube. También analizaremos en profundidad las estrategias probadas y las mejores prácticas que utilizan las empresas para proteger las aplicaciones de misión crítica en entornos de nube pública.

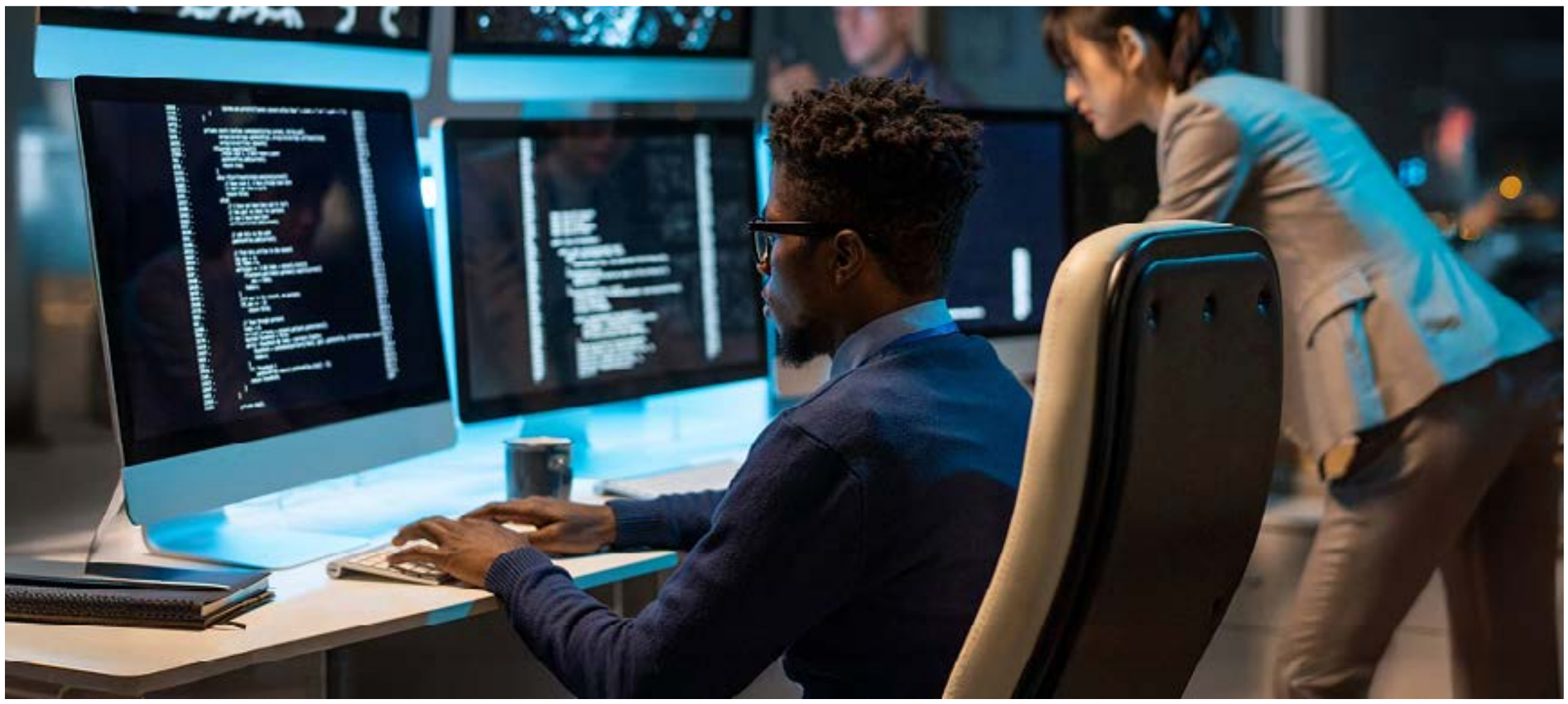
¿Qué sucede cuando las aplicaciones se trasladan a la nube pública?

Cuando las aplicaciones dan el salto a la nube pública, es como si cambiasen sus antiguas casas de ladrillo y cemento por elegantes y modernos apartamentos en una metrópolis vibrante. Esto es lo que ocurre en esta emocionante, pero compleja, transición:

- **Del monolito a los microservicios:** En lugar de una aplicación masiva, piense en una colección de servicios más pequeños e independientes, o microservicios. Cada microservicio está diseñado para realizar funciones específicas y puede desarrollarse, implementarse y escalarse de forma independiente.

- **API comunicativas:** Las aplicaciones nativas de la nube utilizan API para comunicarse entre sí, lo que crea un entorno muy "comunicativo" en el que los servicios interactúan constantemente. Aunque mejoran la flexibilidad y la escalabilidad, las API también aumentan la vulnerabilidad ante las amenazas de seguridad.

- **Cargas de trabajo en movimiento:** Las aplicaciones ya no están confinadas a una sola sala de servidores, sino que ahora están dispersas en diferentes entornos de nube en varias regiones, zonas de disponibilidad y configuraciones híbridas.



La importancia de proteger las aplicaciones críticas en la nube

Las aplicaciones de misión crítica son el elemento vital de cualquier empresa: la base que sustenta las operaciones comerciales. Estas aplicaciones vitales, que pueden incluir sistemas de transacciones financieras, plataformas de atención médica, automatización industrial y sistemas de planificación de recursos empresariales (ERP), exigen disponibilidad constante, procesamiento instantáneo en tiempo real y estricto cumplimiento normativo.

El problema es que cualquier interrupción puede provocar daños importantes a la empresa, a las finanzas y a la reputación.

Si bien trasladar aplicaciones críticas a la nube tiene sus beneficios (escalabilidad, agilidad y ahorro de costos, por nombrar algunos), también presenta una serie de posibles desventajas, como:

- **Mayor exposición a amenazas cibernéticas:** Las aplicaciones que procesan datos altamente confidenciales son los principales objetivos de los atacantes que buscan explotar vulnerabilidades.
- **Complejidad operativa:** El cambio a entornos multinube introduce arquitecturas distribuidas, comunicación impulsada por API y cargas de trabajo dinámicas, que aumentan la superficie de ataque.
- **Desafíos del cumplimiento normativo:** Las empresas que operan en sectores como la salud, las finanzas y la administración pública deben adherirse a estrictos marcos de cumplimiento como HIPAA, RGPD y PCI DSS, lo que hace que la gobernanza de la seguridad en la nube sea crucial. En lugar de una aplicación masiva, piense en un conjunto de servicios más pequeños e independientes, o microservicios. Cada microservicio está diseñado para realizar funciones específicas y puede desarrollarse, implementarse y escalarse de forma independiente.

40 %

DE LAS VIOLACIONES DE DATOS AFECTARON A DATOS ALMACENADOS EN MÚLTIPLES ENTORNOS.[3]

Probablemente no sea una sorpresa que las arquitecturas heredadas simplemente no sean capaces de proteger cargas de trabajo críticas para la misión en la nube. Esto es porque...

1. Las soluciones de seguridad heredadas, como cortafuegos, VPN y defensas basadas en perímetro, fueron diseñadas para entornos locales estáticos y carecen de la flexibilidad necesaria para proteger cargas de trabajo en la nube altamente dinámicas.
2. La seguridad tradicional basada en red no proporciona controles granulares a nivel de aplicación, lo que deja brechas en la protección de arquitecturas basadas en microservicios e impulsadas por API.
3. Los modelos de acceso heredados se basan en la confianza implícita, lo que los hace vulnerables a ataques basados en credenciales, amenazas de movimiento lateral y riesgos internos.

Y EN EL EXIGENTE MUNDO DE LAS APLICACIONES DE MISIÓN CRÍTICA, UNA SOLA FALLA DE SEGURIDAD PUEDE DESENCADENAR UNA CASCADA DEVASTADORA DE CONSECUENCIAS.

El tiempo de inactividad puede:

- Paralizar las operaciones
- Reducir los ingresos
- Erosionar la confianza del cliente

Las violaciones de datos exponen información confidencial, lo que conduce a:

- Multas regulatorias
- Batallas legales
- Daño irreparable a la reputación

5.17 MILLONES DE DÓLARES

COSTO PROMEDIO DE LOS DATOS VULNERADOS ALMACENADOS EN NUBES PÚBLICAS.[4]

Desafíos en la protección de aplicaciones críticas para la misión

El modelo de responsabilidad compartida y sus inconvenientes.

En los últimos años, la nube ha pasado de ser una tecnología emergente a un pilar indispensable para las empresas modernas. Sin embargo, es importante reconocer que la nube no es intrínsecamente segura. En cambio, la seguridad en la nube funciona como una responsabilidad compartida entre el cliente y el proveedor. Imagínese vivir en un edificio donde el propietario mantiene la estructura, pero usted es responsable de la seguridad de su apartamento y sus pertenencias.

En este modelo de responsabilidad compartida, los proveedores de nube protegen la infraestructura de nube subyacente, mientras que los clientes son responsables de proteger sus cargas de trabajo, aplicaciones y datos. Este modelo se suele malinterpretar y se asume erróneamente que los proveedores de servicios en la nube protegen completamente las cargas de trabajo de los clientes. Esto puede resultar en:

- **Buckets de almacenamiento expuestos,** almacenamiento en la nube configurado incorrectamente que permite el acceso público a datos confidenciales.
- **Controles de identidad y acceso débiles,** roles de IAM demasiado permisivos que permiten el acceso no autorizado a aplicaciones de misión crítica.
- **Fallos de cumplimiento,** falta de seguimiento y aplicación continuos, que dan lugar a sanciones regulatorias.

Desafíos de seguridad más amplios para proteger aplicaciones críticas.

Más allá de los posibles inconvenientes del modelo de responsabilidad compartida, las empresas enfrentan riesgos adicionales al proteger cargas de trabajo críticas en la nube. Estos incluyen:

- **Movimiento lateral no autorizado:** Los modelos de seguridad tradicionales, como cortafuegos, VPN y defensas basadas en perímetro, tienen dificultades para proteger entornos de nube dinámicos, lo que aumenta el riesgo de acceso no autorizado y movimiento lateral.

- **Brechas de visibilidad:** El mantenimiento de políticas de seguridad consistentes en entornos híbridos y multinube es difícil, lo que genera posturas de seguridad fragmentadas y brechas de visibilidad.

- **Escasa estandarización de políticas:** La complejidad de los entornos multinube genera riesgos adicionales, ya que los distintos proveedores de servicios en la nube tienen marcos de seguridad inconsistentes, lo que dificulta la estandarización de políticas.

- **Falta de segmentación:** La protección y segmentación integradas insuficientes de los datos permiten a los atacantes propagarse por los entornos en la nube tras un único punto de compromiso.

79 %

ORGANIZACIONES QUE CITAN LA SEGURIDAD EN LA NUBE COMO UNO DE LOS PRINCIPALES DESAFÍOS.[5]

5 mejores prácticas para proteger aplicaciones críticas en la nube

¿Qué estrategias deben incluir las empresas en su conjunto de herramientas de seguridad para proteger eficazmente las aplicaciones críticas en la nube? Dado que no es automáticamente impenetrable, requiere una planificación estratégica y defensas sólidas.

Considere estas cinco prácticas recomendadas como la piedra angular de su estrategia de seguridad en la nube, ya que cada una de ellas desempeña un papel fundamental en la protección de sus activos basados en la nube y en el mantenimiento del cumplimiento normativo.

1 Implemente acceso con privilegios mínimos basado en identidad y autenticación

- Adopte controles de acceso de zero trust para garantizar que solo los usuarios, dispositivos y cargas de trabajo autorizados puedan comunicarse con aplicaciones de misión crítica.
- Oculte sus aplicaciones al no publicar direcciones IP. Lo que está oculto no puede ser atacado por actores malintencionados.
- Monitoree y adapte continuamente las políticas de acceso en función del comportamiento del usuario y del análisis de riesgos en tiempo real.

2 Aplicaciones seguras, no redes

- Aléjese de la seguridad tradicional basada en red conectando aplicaciones en lugar de redes enteras, eliminando así la necesidad de tráfico de retorno, cortafuegos y VPN.
- Adopte soluciones de seguridad basadas en la nube que protejan las cargas de trabajo a nivel de aplicación, garantizando una conectividad directa y segura sin exponer la red en general.
- Aproveche el acceso a la red de zero trust (ZTNA) para proporcionar un acceso seguro y granular a las aplicaciones sin
- aumentar las superficies de ataque.

3 Implemente protección integrada contra amenazas e inspección de seguridad en tiempo real.

- Implemente protección avanzada contra amenazas, incluida detección de intrusiones, análisis de comportamiento y detección de anomalías impulsada por IA para identificar y mitigar las amenazas cibernéticas.
- Utilice soluciones de protección de datos que proporcionen cifrado de extremo a extremo, prevención de pérdida de datos (DLP) y
- supervisión continua.
- Utilice una plataforma de seguridad basada en la nube capaz de inspeccionar amenazas en tiempo real a gran escala para detectar actividades maliciosas antes de que afecten a las aplicaciones críticas.

4 Aplique la segmentación de las cargas de trabajo para evitar el movimiento lateral.

- Aplique la microsegmentación para aislar las cargas de trabajo, limitar el tráfico de este a oeste y evitar que los atacantes se muevan lateralmente a través de entornos de nube.
- Garantice la segmentación en múltiples capas de la nube, incluyendo:

A. **Segmentación a nivel de proceso:** Restrinja la comunicación entre cargas de trabajo dentro de un host.

B. **Segmentación de VPC y zonas de disponibilidad:** Limite el acceso entre diferentes entornos de nube para minimizar la exposición.

C. **Segmentación multinube:** Aplique políticas de seguridad uniformes en AWS, Azure, Google Cloud e infraestructuras híbridas.

5 Aproveche la aplicación automatizada para el cumplimiento normativo

- Alinee las estrategias de seguridad en la nube con las regulaciones específicas de la industria, como HIPAA, GDPR, PCI DSS y NIST.
- Utilice la aplicación automatizada de políticas y la auditoría de cumplimiento para garantizar el cumplimiento continuo de los marcos de seguridad.

Cómo Zscaler ayuda a las empresas a proteger las aplicaciones críticas para su misión

Zscaler es un poderoso aliado para las empresas que se esfuerzan por proteger sus aplicaciones críticas. Con su plataforma Zero Trust Exchange™ nativa de la nube, Zscaler ofrece una conectividad directa y segura entre cargas de trabajo, lo que elimina de forma eficaz la necesidad de VPN, cortafuegos y retornos de tráfico tradicionales, al tiempo que mantiene las aplicaciones protegidas de las amenazas de Internet. Mediante la inspección continua del tráfico, la detección de amenazas y la aplicación de políticas en entornos híbridos y multinube, Zscaler garantiza una visibilidad en tiempo real y una protección sólida para las cargas de trabajo en la nube.

- **Zero Trust Exchange™ totalmente nativa de la nube** ofrece conectividad directa y segura entre cargas de trabajo sin exponer las aplicaciones a Internet ni depender de VPN, cortafuegos o tráfico de retorno.
- **La visibilidad y protección en tiempo real para cargas de trabajo en la nube** inspecciona continuamente el tráfico, detecta amenazas y aplica políticas en entornos híbridos y multinube.
- **La aplicación automatizada de políticas para un acceso seguro y conforme a las normas** garantiza la coherencia de las políticas de seguridad de las aplicaciones, lo que reduce el riesgo de configuraciones erróneas e incumplimientos normativos.

Validación del impacto de Zscaler: conclusiones de la reseña del producto realizada por SANS.

La reseña del producto realizada por SANS ofrece una validación profesional de las capacidades de Zscaler para proteger aplicaciones críticas.[6] A continuación, se detallan las áreas clave en las que Zscaler destaca, según la reseña:

- **Modelo de zero trust:** Zscaler elimina las superficies de ataque conectando directamente las cargas de trabajo, lo que reduce la exposición y el riesgo. Este enfoque garantiza que las cargas de trabajo sean menos detectables y reduce el riesgo de explotación.
- **Prevención de movimiento lateral:** Zscaler aplica microsegmentación y políticas basadas en identidad en todas las cargas de trabajo en la nube, lo que mitiga el movimiento lateral a través de la segmentación de aplicación a aplicación.
- **Mitigación de amenazas en el mundo real:** La inspección del tráfico en tiempo real, el monitoreo continuo y el análisis de seguridad impulsado por IA mitigan eficazmente las amenazas, con protección de datos a través de DLP y SSL a escala.
- **Supervisión y control integrales:** La plataforma Cloud Connector de Zscaler supervisa y controla el acceso a las aplicaciones y los servicios en la nube, gestiona el flujo de datos y evalúa la postura de seguridad de las aplicaciones.
- **Interfaz intuitiva:** La interfaz y el motor de políticas son fáciles de usar, lo que simplifica la configuración y la gestión de las políticas de seguridad.

En resumen, la revisión de SANS confirma que el modelo de seguridad nativo en la nube de Zscaler es líder en el sector, ya que ayuda a empresas globales como Siemens, Micron y Mahindra Group a proteger sus aplicaciones más críticas, cumplir los requisitos de conformidad y simplificar la complejidad de la seguridad multinube.

Consiga una seguridad integral en la nube

A medida que las empresas trasladan aplicaciones de misión crítica a la nube, enfrentan riesgos de seguridad importantes que exigen atención inmediata. Pero las estrategias adecuadas pueden allanar el camino para operaciones seguras y eficientes.

Una arquitectura moderna de zero trust permite a las organizaciones conectar aplicaciones de forma segura en cualquier lugar para minimizar la superficie de ataque, evitar el movimiento lateral y reducir el riesgo de que los actores malintencionados obtengan acceso a sus datos. Esto permite a las empresas afrontar con confianza las complejidades de la seguridad en la nube y lograr una protección integral de sus activos más valiosos.

Dé el siguiente paso para garantizar la seguridad e integridad de sus activos basados en la nube. Solicite una demostración para ver de primera mano cómo puede simplificar radicalmente la protección de la carga de trabajo en la nube.

SOLICITE UNA DEMOSTRACIÓN

O bien, pruebe usted mismo Zero Trust Cloud en nuestro laboratorio autoguiado.

VER LA GUÍA

[1] Gartner Forecasts Worldwide Public Cloud End-User Spending to Total $723 Billion in 2025
[2] Gartner Says Cloud Will Become a Business Necessity by 2028
[3] IBM Cost of Data Breach Report, 2024
[4] IBM Cost of Data Breach Report, 2024
[5] Flexera 2023 State of the Cloud Report
[6] How to Use Zero Trust to Secure Workloads in the Public Cloud, SANS, 2023

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