Asegurar el mundo post-IA para los servicios financieros con Zero Trust

Un enfoque estratégico para la ciberseguridad en la era de la IA

©2024 Zscaler, Inc. Todos los derechos reservados.

Resumen de la solución

Resumen ejecutivo: Navegar por el bosque oscuro

En un mundo post–IA, los servicios financieros deben navegar por un "bosque oscuro" de amenazas e incertidumbres ocultas, donde cada interacción podría suponer un riesgo. Así como uno debe extremar las precauciones en un entorno peligroso e impredecible, los servicios financieros deben abordar la seguridad de la IA con vigilancia. Este informe describe los pasos que pueden tomar las organizaciones de servicios financieros para protegerse al ingresar a este panorama impulsado por la inteligencia artificial.

Exploraremos cómo la IA está transformando el panorama de amenazas, introduciendo nuevas vulnerabilidades como el fraude impulsado por IA y los ciberataques automatizados. Además, destacaremos tendencias y predicciones clave, ayudando a las organizaciones a anticipar el impacto de la IA y responder estratégicamente.

La mejor defensa en este entorno de alto riesgo, donde ninguna entidad, ni dentro ni fuera de la organización, es confiable, es Zero Trust. Este informe proporciona una ruta clara para que las organizaciones de servicios financieros inicien su transición hacia la confianza cero, ofreciendo pasos prácticos para garantizar un futuro de IA seguro y resiliente.

IA y el panorama de amenazas en evolución

La IA está transformando rápidamente el panorama de amenazas, introduciendo riesgos complejos que desafían los modelos de seguridad tradicionales. Los ataques han evolucionado y se han vuelto más efectivos a escala, lo que permite a las víctimas seguir operando mientras los atacantes amenazan con exponer sus datos. Si bien hay muchas megatendencias y predicciones de IA, analizaremos tres tendencias para 2024–2025 que han estado evolucionando a un ritmo más rápido.

2024 – 2025: Tres tendencias a tener en cuenta

Desarrollo de IA de secuencia principal

Los modelos de lenguaje grande (LLM) de IA han transformado la manera en que pensamos sobre la IA generativa al expandir sus capacidades más allá de resultados limitados y específicos de cada tarea hacia soluciones más dinámicas y conscientes del contexto. Pero al igual que el mundo real, todo, incluida la IA, seguirá evolucionando. Estos LLM nos atraparon una vez que cruzaron el valle inquietante.

El valle inquietante es el sentimiento inquietante que experimentan las personas cuando la IA se vuelve casi (pero no del todo) indistinguible de los humanos, lo que crea una sensación de incomodidad debido a su imitación casi perfecta.

GenAI y ChatGPT, en particular, superaron el límite inquietante al alcanzar los 100 millones de usuarios en dos meses, lo cual es notable. Ahora que lo han superado, se avecinan más avances que podrían tener un mayor impacto desde una perspectiva neurológica y en la búsqueda de la cognición, más allá de GenAI.

Ataques de ransomware sin cifrado

Anteriormente, el cifrado se utilizaba para el ransomware; su objetivo principal era robar sus datos, exigir un rescate por su operación y, si no paga, no puede dirigir su negocio.

© 2024 Zscaler, Inc. Todos los derechos reservados.

Sin embargo, con el tiempo, los atacantes de ransomware se han dado cuenta de que si reducen la cantidad de dinero que buscan y no impiden que sus víctimas realicen negocios, obtendrán un mayor rendimiento. Por ejemplo, supongamos que bajan el rescate de 10 millones de dólares a 2 millones y se pasa de un 5 % de probabilidad de pago a un 70—80 % de probabilidad de pago: se convierte en un modelo de negocio de ransomware "mejor" a gran escala. Este es un ransomware sin cifrado.

En el ransomware sin cifrado, toman los datos, lo amenazan y en muchos casos le permitirán continuar con las operaciones porque no quieren detener su negocio.

Al no interrumpir el negocio, pueden ocurrir menos daños a la reputación. Los atacantes también pueden intentar convencer a la víctima de que no informe el rescate a la SEC o al regulador porque "no es lo suficientemente relevante".

Ataques de ransomware impulsados por IA

Los ataques de ransomware impulsados por IA son más efectivos para mejorar el rendimiento, la penetración y la automatización de los ataques. En este caso, los atacantes aprovechan la IA para automatizar y mejorar la sofisticación de los ciberataques, haciéndolos más rápidos, más específicos y más difíciles de detectar.

Cuatro formas en que los servicios financieros pueden navegar el cambiante panorama de la IA

El uso de IA empresarial está en aumento, junto con los riesgos. Los cuatro niveles de consideración estratégica corporativa pueden guiar a las organizaciones de servicios financieros a la hora de navegar por las complejidades de un mundo post-IA en constante evolución.

En 2024, el uso de herramientas de IA/ML creció un 594 % y el uso de ChatGPT aumentó un 634 % (Zscaler ThreatLabz 2024 AI Security Report).

Política y ética

Los servicios financieros deben desarrollar políticas integrales que rijan el uso ético de la IA, garantizando el cumplimiento de la normativa y fomentando la confianza de los clientes. Esto implica crear un marco que aborde la privacidad de los datos, la transparencia algorítmica y la mitigación de sesgos, haciendo hincapié en prácticas responsables de IA.

Actividad principal

¿Cómo impacta la IA en el negocio principal? Harvard Business Review realizó un estudio que mostró una diferencia estadísticamente significativa en el desempeño de las empresas que usan IA contra aquellas que no lo hacen en una industria determinada, y que esa brecha continúa ampliándose.

Entonces, ¿cómo se va a incorporar la IA al negocio? ¿Va a hacer esto con un compañero o va a hacer las cosas de forma privada? ¿Va a tener sus propios modelos? ¿Va a participar en modelos más grandes? ¿Y cuál es el caso de uso implicado?

Las organizaciones deben evaluar cómo la IA puede mejorar sus operaciones comerciales principales, como mejorar los servicios al cliente, optimizar el procesamiento y permitir la toma de decisiones basada en datos.

© 2024 Zscaler, Inc. Todos los derechos reservados.

Las organizaciones deberían evaluar cómo la IA puede mejorar sus operaciones centrales, como la optimización de la atención al cliente, la eficiencia de los procesos y la toma de decisiones basada en datos. Al identificar las áreas clave en las que la IA puede aportar valor, las organizaciones de servicios financieros pueden crear ventajas competitivas e impulsar la innovación en línea con sus objetivos estratégicos.

I+D e infraestructura.

A medida que las herramientas de IA se incorporan al sector empresarial, ¿cómo gestionarlas? Invertir en una infraestructura robusta que respalde las capacidades de IA, como la computación en la nube, el análisis de big data y el aprendizaje automático, permitirá a las organizaciones aprovechar las tecnologías emergentes y desarrollar nuevas soluciones para satisfacer las cambiantes necesidades de los clientes.

Ventajas de la ciberseguridad.

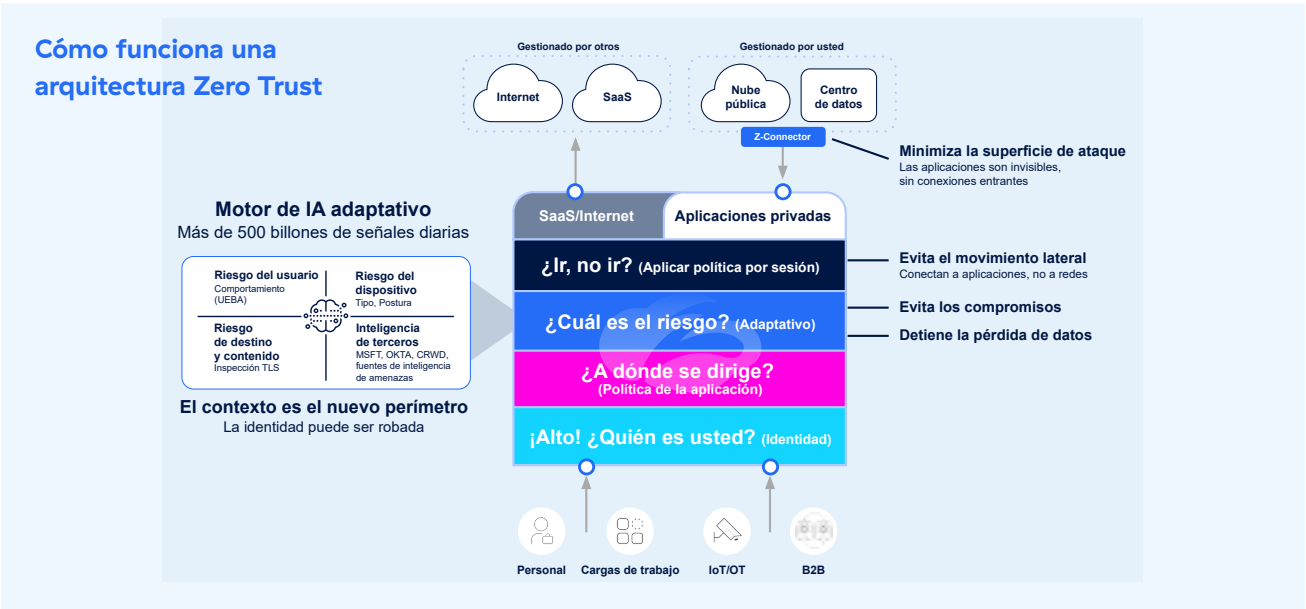
Las instituciones financieras pueden mejorar su postura de ciberseguridad utilizando soluciones de seguridad que aprovechan la IA para identificar y responder a las amenazas en tiempo real.

Debería preguntarse: ¿cuáles son las ventajas para la IA y la ciberseguridad o cuáles son las amenazas potenciales? ¿Cómo lo van a utilizar en su contra? ¿Cómo puede prepararse para eso? Al implementar medidas de seguridad impulsadas por IA, las organizaciones pueden proteger mejor los datos y activos confidenciales y garantizar la resiliencia frente a amenazas sofisticadas.

El papel de Zero Trust en la reducción del riesgo cibernético

A pesar del aumento en el uso de la IA empresarial, las empresas bloquean **el 18,5 %** de todas las transacciones de IA, un aumento**del 577 %,** lo que indica una creciente preocupación por la seguridad (Informe de Seguridad de IA de Zscaler ThreatLabz 2024). La mejor defensa en este entorno de alto riesgo, donde no se puede confiar en ninguna entidad, ni dentro ni fuera de la organización, es Zero Trust.

Zero Trust es la estrategia que nos ayuda a navegar por el bosque oscuro al permitir solo lo que la empresa necesita cuando lo necesita. La implementación de un enfoque Zero Trust que no implica confiar en nadie garantiza que, independientemente del usuario, la carga de trabajo, el dispositivo u otra empresa, pueda reducir significativamente el riesgo cibernético:



© 2024 Zscaler, Inc. Todos los derechos reservados.

1. Autenticar la identidad: ¡Alto! ¿Quién es usted?

a. ¿Quién se está conectando?

b. ¿Cuales son los atributos?

c. ¿A dónde va la conexión?

2. Política de la aplicación de control: ¿A dónde se intenta llegar?

a. ¿A dónde se está intentando ir? En este paso, Zero Trust analiza el riesgo utilizando el contexto, lo que previene el compromiso y la pérdida de datos.

3. Riesgo contextual adaptativo: ¿Cuál es el riesgo?

a. ¿Cuál es el riesgo? Evite los riesgos y detenga la pérdida de datos evaluando el riesgo del usuario, el riesgo del dispositivo, el destino, el riesgo del contenido y la información de terceros (Okta, CrowdStrike, etc.).

4. Aplicar las políticas

a. Evite el movimiento lateral para conectarse a aplicaciones, no a redes. b. Aplicar políticas tanto para SaaS como para conexiones a Internet sobre una base por sesión y por usuario c. Aplicaciones privadas: minimice la superficie de ataque para que las aplicaciones sean invisibles y no se puedan producir conexiones entrantes.

Un viaje Zero Trust

Para proteger su negocio contra la creciente cantidad de ciberamenazas impulsadas por IA, es esencial embarcarse en un viaje Zero Trust. La implementación de un proceso Zero Trust debe verse como un proceso gradual, dividido en pasos manejables que se alineen con las prioridades comerciales y los objetivos de seguridad, lo que garantiza que su seguridad evolucione de una manera que sea escalable y resiliente.

1. Proteja al personal

a. Fase 1A: sin cambios en la red

i. Ciberprotección y protección de datos, experiencia digital y cuantificación del riesgo

b. Fase 1B — simplificación de la red

i. Sucursal con modelo de confianza cero/cibercafé, estrategia avanzada de ciberprotección y protección de datos, y obtención de información empresarial

2. Cargas de trabajo seguras

a. Ciberseguridad y protección de datos para cargas de trabajo

b. Redes y segmentación de cargas de trabajo Zero Trust

3. Acceso de terceros

a. Acceso a aplicaciones de terceros Zero Trust

b. Conectividad de sitios de terceros Zero Trust

4. Dispositivos seguros (IoT/OT)

a. Ciberseguridad y protección de datos para IoT/OT

b. Conectividad Zero Trust IoT/OT

© 2024 Zscaler, Inc. Todos los derechos reservados.

Conclusión

Zero Trust ofrece la mejor defensa en este panorama de rápida evolución, donde no se puede confiar de forma inherente en ninguna entidad (dentro o fuera de la organización). A medida que la tecnología y la IA siguen evolucionando y eventualmente llegan al mismo tiempo, la adopción de una estrategia Zero Trust garantiza que solo los usuarios y procesos adecuados accedan a lo que se necesita, cuando se necesita, lo que garantiza que pueda seguir siendo resiliente y preparar su organización para el futuro.

Reduzca su riesgo cibernético, comience su viaje Zero Trust obteniendo más información en zscaler.com/es

Conozca al autor

Con más de tres décadas como emprendedor, experto en ciberseguridad y directivo en empresas como RSA, Arbor Networks, CA, McAfee, Cybereason y otras, Sam está dedicado a empoderar a los defensores en el conflicto cibernético y a cumplir la promesa de la seguridad, posibilitando un mundo seguro, fiable y conectado. Actualmente, Sam Curry es Vicepresidente Global y CISO en Zscaler y, en su tiempo libre, es conferencista, conduce un pódcast (On the Hook), participa en diversos consejos y publicaciones, y es mentor en ciberseguridad. Conéctese conmigo en LinkedIn.

zscaler™ | Experience your world, secured.™

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 los ciberataques y la pérdida de datos mediante la conexión segura de usuarios, dispositivos y aplicaciones en cualquier lugar. Distribuido en más de 150 centros de datos en todo el mundo, Zero Trust Exchange basada en SSE es la mayor plataforma de seguridad en la nube en línea del mundo. Obtenga más información en **zscaler.com/es** o síganos en Twitter **@zscaler**.

©2024 Zscaler, Inc. Todos los derechos reservados. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™ y ZPA™ y otras marcas comerciales mencionadas en **zscaler.com/es/legal/trademarks** son (i) marcas comerciales o marcas de servicio registradas o (ii) marcas comerciales o marcas de servicio de Zscaler, Inc. en los Estados Unidos y/o en otros países. Cualquier otra marca registrada es propiedad de sus respectivos dueños.