



4 razones por las que su empresa necesita implementar una arquitectura Zero Trust

Tabla de contenido

Introducción	3 - 4
01. Aumento de los ataques de ransomware	5 - 7
02. Entorno de trabajo híbrido	8 - 10
03. Adopción de recursos de cloud computing	11 - 13
04. Requisitos de cumplimiento normativo rigurosos	14 - 16
Un banco internacional logra el cumplimiento de SWIFT en dos semanas	17 - 18

Introducción

A medida que los atacantes aumentan su nivel de sofisticación, los grupos de ransomware proliferan y los avances tecnológicos introducen nuevas vulnerabilidades, las organizaciones recurren cada vez más a un modelo de seguridad Zero Trust. En esencia, este enfoque elimina la confianza implícita en razón de los usuarios, las aplicaciones y los dispositivos, algo que era un principio central de los enfoques de seguridad anteriores. En términos prácticos, existen cuatro situaciones clave en las que una organización se beneficiará de un modelo de seguridad Zero Trust: un ataque de ransomware contra la empresa, un cambio al teletrabajo, la necesidad de proteger su entorno de nube o una próxima auditoría.

Estas situaciones son el resultado de tendencias recientes, como el aumento de los ataques de ransomware, el cambio a un entorno de trabajo híbrido, la migración

al cloud computing y unas mayores exigencias en las auditorías de seguridad. Todo esto requiere un enfoque de seguridad basado en la verificación de identidades, independientemente de la ubicación, y en medidas proactivas en caso de infiltraciones. Zero Trust es el único enfoque que requiere un control eficaz de las identidades de usuario para acceder a los datos y proporciona mecanismos de mitigación proactivos una vez que se ha producido un ataque.

La implementación de una estrategia Zero Trust puede parecer abrumadora para los equipos de seguridad, ya de por sí sobrecargados, pero no tiene por qué serlo. Si adopta un enfoque por fases y se centra en obtener beneficios rápidos, puede reducir parte de la complejidad y el riesgo asociados a las soluciones de seguridad tradicionales, así como mejorar su estrategia de seguridad.

Para empezar, no tiene que deshacerse de su tecnología actual ni sustituirla. Comience por adaptar sus inversiones de Zero Trust a sus necesidades empresariales más urgentes. Opte por un proveedor de soluciones Zero Trust de confianza, en lugar de los que han evolucionado de la noche a la mañana y han reconvertido sus antiguas soluciones en modelos Zero Trust. Plántese seriamente el uso de un proveedor que pueda combinar varios elementos de seguridad Zero Trust (acceso de red Zero Trust, firewall de DNS, microsegmentación, etc.) en una sola plataforma. Sea cual sea el motivo de la adopción, con un enfoque Zero Trust logrará agilidad empresarial, optimizará costes, consolidará herramientas y mejorará sus operaciones en general.

Las 4 principales razones por las que las organizaciones recurren a Zero Trust



Aumento de los ataques de ransomware



Entorno de trabajo híbrido



Adopción de recursos de cloud computing



Requisitos de cumplimiento normativo rigurosos

01

Aumento de los ataques de ransomware

Aumento de la protección contra el ransomware

En los últimos años, organizaciones de todo el mundo han sufrido interrupciones por ataques de ransomware, desde hospitales y bancos hasta oleoductos y otras infraestructuras esenciales. De hecho, **Cybersecurity Ventures** prevé que el coste del ransomware podría ascender hasta alcanzar aproximadamente los 265 000 millones de dólares al año en 2031. Predice que los autores de ataques de ransomware lanzarán un nuevo ataque (contra un consumidor o una empresa) cada dos segundos a medida que perfeccionen progresivamente sus cargas de malware y las actividades de extorsión relacionadas.

Sin una estrategia Zero Trust, los grupos de ataque mediante ransomware pueden aprovechar las siguientes debilidades:



Confianza implícita en los usuarios, las aplicaciones y las redes, lo que permite a los atacantes que han logrado vulnerar la red moverse lateralmente y propagar malware



Políticas de acceso demasiado permisivas que posibilitan que las infecciones se usen para inyectar programas de ransomware



Sistemas que confían únicamente en una contraseña, lo que ofrece una oportunidad para el robo de credenciales

Cómo ayuda Zero Trust

Las empresas que implantan una arquitectura Zero Trust tienen políticas de control de acceso y utilizan servicios de microsegmentación que minimizan el daño que puede causar un ataque. Para los atacantes no solo resulta más difícil infiltrarse en el sistema, también tienen limitada la capacidad de expandirse por él.

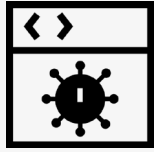
Cómo neutraliza Akamai la cadena de exterminio del ransomware

Un ataque de ransomware suele implicar una infección inicial, un movimiento lateral y la exfiltración y el cifrado de datos. Con los enfoques Zero Trust, las organizaciones pueden abordar cada paso a medida que ocurre, o incluso antes.



“El ransomware
atacará a una
empresa, un
consumidor o un
dispositivo cada
dos segundos”

En 2031, según el informe Who's Who in Ransomware Report 2023 de Cybersecurity Ventures.



Infección inicial

La plataforma Akamai Guardicore ayuda a evitar que un ataque se extienda más allá del punto de entrada inicial, mientras que Akamai MFA protege a los usuarios frente al robo y el abuso de sus credenciales.



Movimiento lateral

La plataforma Akamai Guardicore reduce las rutas de propagación y ayuda a evitar el movimiento lateral. Akamai Guardicore Access limita la capacidad del atacante de moverse para infectar la aplicación que buscaba explotar. Akamai Hunt detecta y mitiga las amenazas avanzadas más evasivas de su red.



Exfiltración y cifrado de datos

La plataforma Akamai Guardicore limita el acceso a las aplicaciones esenciales, lo que impide que los atacantes accedan a datos confidenciales dentro de una red comprometida. Akamai Secure Internet Access Enterprise bloquea las solicitudes a sitios de phishing y a sitios de mando y control. Por último, Akamai Hunt detecta el comportamiento anómalo y evita que los atacantes cifren datos valiosos que pueden ser objeto de rescate.

02

Entorno de trabajo híbrido

Protección del nuevo entorno híbrido

Proteger un entorno híbrido nuevo que ha crecido y se ha expandido debido a la pandemia de COVID-19 es más difícil si las organizaciones confían en herramientas de seguridad obsoletas, como los firewalls y las VPN. Cuando se introdujeron por primera vez las VPN de acceso remoto hace unos 30 años, todo era diferente: Internet estaba en sus inicios, las aplicaciones se ejecutaban en el centro de datos y había muchos menos usuarios conectados desde

ubicaciones remotas. Seguir autenticando a los usuarios con una VPN y darles acceso luego a toda la red aumenta la superficie de ataque y abre la puerta a muchas de las vulnerabilidades de día cero asociadas a las VPN heredadas. Cualquier usuario con las credenciales necesarias puede iniciar sesión en una VPN corporativa y, una vez dentro, moverse lateralmente por la red y acceder a los recursos que la VPN debía proteger.

Cómo ayuda Zero Trust

Basado en el principio de acceso con los privilegios mínimos, Zero Trust asume que ningún usuario o aplicación es, inherentemente, de confianza. El acceso de red Zero Trust (ZTNA) adopta un enfoque completamente diferente al de las VPN para proteger el acceso de los trabajadores remotos. En lugar de poner en riesgo toda la red, los usuarios se conectan directa y exclusivamente a las aplicaciones y los datos que necesitan, lo que impide el movimiento lateral de usuarios malintencionados con un acceso demasiado permisivo a datos y recursos confidenciales. En caso de que se produzca una filtración, una solución de microsegmentación Zero Trust eficaz puede segmentar la red interna para que dicha filtración no se propague a otras partes de la red ni las dañe. Según **Gartner**, al menos el 70 % de las nuevas implementaciones de acceso remoto serán atendidas principalmente por sistemas ZTNA en lugar de por servicios de VPN en 2025, en comparación con menos del 10 % a finales de 2021.

“Según Gartner, al menos el 70 % de las nuevas implementaciones de acceso remoto serán atendidas principalmente por sistemas ZTNA en lugar de por servicios de VPN en 2025, en comparación con menos del 10 % a finales de 2021.”

Cómo facilita Akamai el trabajo híbrido y el teletrabajo

La completa plataforma Zero Trust de Akamai responde a las necesidades de su entorno de trabajo híbrido. Entre las ventajas se incluyen las siguientes:



Menores riesgos

Akamai conecta directamente al usuario correcto con la aplicación correcta, lo que reduce la superficie de ataque y limita el movimiento lateral.



Experiencia de usuario mejorada

Los usuarios remotos disfrutan de acceso a los recursos independientemente de la aplicación, el dispositivo o su ubicación, lo que elimina la necesidad de conectarse y desconectarse de la VPN.



Más agilidad

Dado que la solución de Akamai se utiliza como servicio, las organizaciones no tienen que implementar ningún hardware ni preocuparse por la escalabilidad a medida que aumenta la demanda, lo que reduce los costes y la complejidad.

03

Adopción de recursos de cloud computing

Migración sencilla a la nube

Las organizaciones están migrando sus aplicaciones a la nube para lograr flexibilidad y agilidad, así como para modernizar su infraestructura. Sin embargo, estos entornos de nube están ampliando la superficie de ataque e introduciendo nuevos requisitos de seguridad. Las integraciones entre diferentes nubes y entornos locales pueden generar fisuras en las aplicaciones y poner en riesgo la seguridad. Cuando las organizaciones intentan migrar sus aplicaciones a la nube mediante estructuras de red tradicionales (VPN y firewalls), suelen enfrentarse

a un mayor riesgo de amenazas laterales, una escalabilidad deficiente y costes elevados. Incluso después de completar la migración, los recursos deben protegerse, y los usuarios deben autenticarse según los permisos asociados a su rol. Los usuarios de la infraestructura de nube normalmente tienen un acceso más amplio a los recursos, los servicios y los derechos de gestión del que podrían tener en los entornos locales, lo que supone un riesgo adicional y la posibilidad de que se generen interrupciones.

Cómo ayuda Zero Trust

Las estrategias Zero Trust facilitan la migración a la nube. Zero Trust elimina la confianza implícita inherente a muchas aplicaciones basadas en la nube, especialmente las aplicaciones de terceros, que pueden introducir vulnerabilidades. Las soluciones Zero Trust garantizan que las organizaciones puedan implementar sus aplicaciones basadas en la nube con mayor facilidad con una protección más sólida. Algunas de las ventajas de implementar Zero Trust en la nube incluyen los siguientes aspectos:

- ✓ Mejor visibilidad de los activos y los riesgos
- ✓ Reducción de la superficie de ataque gracias a la segmentación Zero Trust y al acceso con los privilegios mínimos a los recursos de nube
- ✓ Infraestructura de red modernizada que ofrece velocidad y agilidad
- ✓ Reducción de los costes operativos y de la complejidad



Cómo mejora Akamai la migración a la nube

Las soluciones Zero Trust de Akamai pueden ayudarle a migrar automáticamente sus recursos y sus respectivas políticas. Todo ello sin tiempos de inactividad y sin interrupciones en sus operaciones. Akamai ofrece:



Mayor visibilidad

Gracias a la mejor comprensión de las dependencias de las aplicaciones, puede crear políticas eficaces de segmentación de la nube para reducir la superficie de ataque y minimizar el riesgo.



Acceso de red Zero Trust

Los usuarios solo pueden conectarse a las aplicaciones para las que tienen autorizado el acceso, mediante una autenticación estricta.



Búsqueda de amenazas

El equipo de expertos de Akamai, dedicados a cazar amenazas, investiga continuamente comportamientos de ataque anómalos en entornos de nube y notifica a los clientes de cualquier riesgo para su red.

04

Requisitos de cumplimiento normativo rigurosos

Simplificación del cumplimiento normativo y reducción del riesgo

Si bien los responsables de seguridad saben que cumplir los requisitos de conformidad no equivale a una organización realmente segura, las auditorías de seguridad siguen siendo una prioridad para los equipos ejecutivos. Saben que las auditorías no superadas pueden provocar importantes interrupciones en el negocio y afectar a los resultados. Una evaluación de cumplimiento es una de las actividades que más tiempo lleva y que consume más recursos de los equipos de seguridad. Además, el paso a entornos digitales sin perímetro y la prevalencia del teletrabajo han dificultado el cumplimiento aún más. Por lo general, las organizaciones necesitan aislar sus entornos y acordonar sus activos regulados para satisfacer los estándares de cumplimiento, como el estándar de seguridad de datos del sector de las tarjetas de pago (PCI-DSS), la ley de transferibilidad y responsabilidad de seguros médicos (HIPAA) y el sistema SWIFT (sociedad para las telecomunicaciones financieras interbancarias internacionales).

Las organizaciones también tienen que atender a usuarios remotos, usuarios corporativos presenciales, partners, proveedores y mucho más, con lo que el perímetro del entorno de una organización es casi imposible de delimitar. A medida que los equipos de seguridad se preparan para auditorías en las que el control del acceso es un determinante fundamental del éxito, deben abordar las siguientes preguntas:

- ¿Cómo podemos restringir el acceso a la información confidencial únicamente a los usuarios autorizados?
- ¿Cómo podemos delimitar el entorno de auditoría?
- ¿Cómo podemos hacer que el proceso de auditoría sea más sencillo y menos caótico?

Cómo ayuda Zero Trust

Afortunadamente, un enfoque Zero Trust puede ayudar a abordar todas estas cuestiones y mucho más. Los dos pilares clave de Zero Trust, la capacidad de realizar comprobaciones explícitas y dar acceso con los privilegios mínimos, simplifican enormemente el proceso de cumplimiento. Las organizaciones pueden aislar sus activos regulados de otro tráfico en su centro de datos o nube, y permitir el acceso en función de identidades, independientemente de la ubicación. La visibilidad mejorada muestra lo que entra y sale de su entorno regulado, y ayuda a identificar lo que es relevante. Todo esto reduce en gran medida la complejidad y el coste de la auditoría, y facilita la tarea del auditor.

Cómo facilita Akamai el cumplimiento

La completa cartera de soluciones Zero Trust de Akamai le ayuda en la preparación para cada auditoría, ya sea de PCI-DSS, HIPAA, ISO, Sarbanes-Oxley (SOX) o cualquier otro marco. Akamai Enterprise Application Access controla el acceso de terceros a la información personal confidencial, cumpliendo así los requisitos del Reglamento General de Protección de Datos (RGPD). Akamai Guardicore Segmentation mejora la comprensión de los activos regulados según la norma PCI-DSS, aísla las funciones del centro de compensación para cumplir con los estándares HIPAA, y restringe el acceso a Internet y aísla los sistemas críticos para cumplir con las normativas de SWIFT. Akamai MFA protege la información de los pacientes conforme a HIPAA de los atacantes que han obtenido contraseñas para los sistemas sanitarios, y refuerza el cumplimiento de SWIFT al evitar la usurpación de las credenciales.



Un banco internacional logra el cumplimiento de SWIFT en dos semanas

Entidades reguladoras externas requerían que uno de los clientes de Akamai, un banco global, acordonara todas sus aplicaciones críticas para cumplir los requisitos de SWIFT con el fin de garantizar una transferencia segura de dinero entre instituciones financieras. Normalmente, una aplicación como esta requiere más de 100 servidores implementados en ubicaciones diferentes, incluidos servidores bare metal y virtuales. De media, este proceso tardaría entre 8 y 12 meses en planificarse y ejecutarse para un banco de este tamaño, ya que tendría que crearse una red de área local virtual (VLAN) para su segmento en distintas ubicaciones. Identificar las dependencias de la aplicación SWIFT y asegurarse de que el conjunto de reglas

fuera correcto y no afectara negativamente a nada habría implicado aún más tiempo. Mientras tanto, el proyecto también suponía la compra de nuevos equipos de firewalls. Y, dado que la aplicación SWIFT es fundamental para las actividades bancarias, la entidad no podía permitirse ningún tiempo de inactividad. En general, la expectativa era que el proyecto de segmentación conllevara un esfuerzo masivo por parte de muchas personas. Sin embargo, con Akamai, para el proceso completo solo se necesitó que un ingeniero dedicara unas dos semanas. No fue necesario aplicar ningún cambio en la red y el banco no tuvo que hacer cambios en sus aplicaciones ni interrumpir sus servicios.

Simplificación y aceleración del cumplimiento



Banco global

- Necesidad de acordonar la aplicación SWIFT
- Entorno complejo con servidores bare metal, VMware y OpenStack



Segmentación tradicional

- Dificultad de definir segmentos en infraestructuras complejas
- Sin visibilidad de las aplicaciones y dependencias
- Requiere tiempo de inactividad
Tiempo: de 8 a 12 meses
Personas: al menos 5



Akamai Guardicore Segmentation

- Asignación de la aplicación SWIFT completada en horas
- Políticas de segmentación sugeridas y ajustadas automáticamente
- No es necesario adquirir ni implementar hardware ni firewalls nuevos
- Sin tiempo de inactividad
Tiempo: 2 semanas
Personas: 1 arquitecto de TI

Descubra cómo puede satisfacer sus necesidades empresariales con la cartera de soluciones Zero Trust de Akamai

Más información

La seguridad de Akamai protege las aplicaciones que impulsan su negocio en cada punto de interacción sin comprometer el rendimiento ni la experiencia del cliente. Gracias a la escala de nuestra plataforma global y su visibilidad de las amenazas, colaboramos con usted para prevenirlas, detectarlas y mitigarlas, de forma que pueda generar confianza en la marca y cumplir su visión. Para obtener más información acerca de las soluciones de cloud computing, seguridad y distribución de contenido de Akamai, visite **akamai.com** y **akamai.com/blog**, o siga a Akamai Technologies en **X**, antes conocido como Twitter, y **LinkedIn**. Publicado en septiembre de 2024.