Akamai

WHITE PAPER

Plan para una estrategia de seguridad de primera clase

Plan de acción personalizado y basado en los principios de Zero Trust

En Akamai, queremos asegurarnos de estar siempre protegidos en un panorama de constante cambio. Por eso, y para evitar bajar la guardia, recientemente evaluamos nuestro nivel de seguridad basándonos en el modelo de madurez Zero Trust (ZTMM). En este documento explicamos cómo este proceso ofrece una visión clara de las áreas de mejora y allana el camino hacia una estrategia de seguridad de primera clase.

Simplifique el camino hacia Zero Trust

En un mundo donde el acceso y la seguridad empresariales son cada vez más complejos y están en constante evolución, no es fácil saber qué áreas requieren más esfuerzos cuando se busca adoptar una estrategia de seguridad Zero Trust.

Aquí es donde entra el ZTMM, una herramienta para evaluar y visualizar su estrategia de seguridad actual y que hemos utilizado en Akamai para evaluar nuestra propia estrategia, así como la de muchos de nuestros clientes. Al final del proceso, dispondrá de una guía con medidas concretas para avanzar hacia una arquitectura Zero Trust. (Consulte el Apéndice A para más información sobre el concepto Zero Trust).

Por qué funciona el modelo de madurez Zero Trust

El primer paso para lograr una estrategia de seguridad Zero Trust es el más importante: empezar. Sin embargo, en el mundo de la ciberseguridad, tan complejo y cambiante, dar ese primer paso puede resultar abrumador. Hemos visto que muchas organizaciones tienen dificultades al tratar de decidir qué cambios implementar, cuántos y en qué orden.

Aquí es donde entra en juego el ZTMM. Este modelo crea un marco uniforme para que resulte más fácil implantar Zero Trust. No solo ayuda a las organizaciones a planificar los cambios necesarios y presupuestar actualizaciones, sino que también explica los principios de Zero Trust a los responsables de la toma de decisiones que no son expertos en TI, lo que brinda a los equipos el apoyo que necesitan.

El ZTMM es una herramienta probada y validada. La Agencia de Seguridad Cibernética y de la Infraestructura (CISA) de EE. UU. se encargó de desarrollarla y ya la han adoptado varias agencias federales estadounidenses.

Los cinco pilares y las tres capacidades del ZTMM

El ZTMM se estructura en torno a cinco pilares progresivos para ir avanzando paso a paso. Cada uno de estos pilares aborda una dimensión específica: Identidad, Dispositivos, Redes, Aplicaciones y cargas de trabajo y Datos (Figura 1). Además, incluye tres capacidades clave que están presentes de manera transversal en los cinco pilares:

- Visibilidad y análisis
- Automatización y orquestación
- Gobernanza

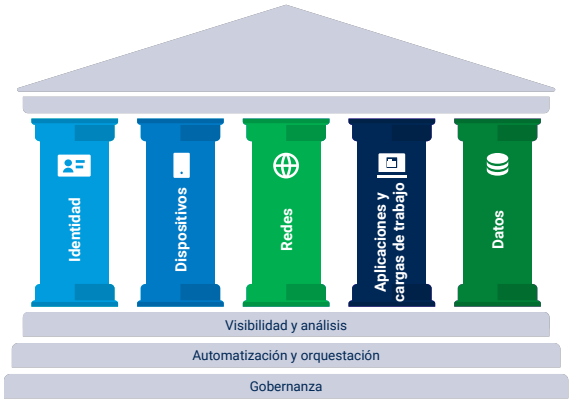


Fig. 1: El ZTMM de la CISA es uno de los muchos caminos hacia Zero Trust (Fuente: CISA)

A cada una de estas áreas se le asigna un grado de madurez que describe lo cerca que está una organización de consolidar un enfoque Zero Trust. Existen cuatro grados de madurez: Tradicional, Inicial, Avanzado y Óptimo. Representan las etapas del proceso de transición, desde el uso de configuraciones manuales y VPN hasta llegar a un modelo de "seguridad sin perímetro" ideal (Figura 2). Las organizaciones que han alcanzado el último grado otorgan a las aplicaciones únicamente los permisos mínimos necesarios, deniegan la autenticación y el acceso a dispositivos vulnerables, evitan que las amenazas internas se propaguen y detectan y responden de inmediato a los incidentes de seguridad. Consulte el Apéndice B para ver una descripción más detallada del marco ZTMM.

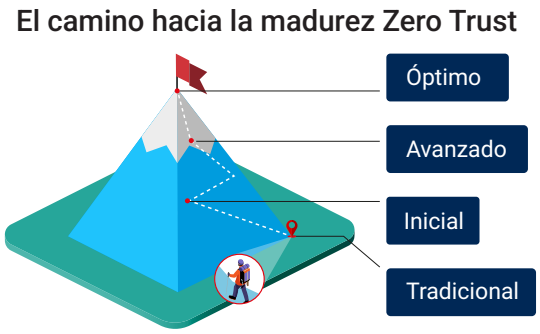


Fig. 2: El camino hacia la madurez Zero Trust (Fuente: CISA)

Al destacar las áreas con menor grado de madurez, el ZTMM ayuda a las organizaciones a crear un entorno de seguridad más equilibrado. Akamai ofrece un conjunto de soluciones de seguridad que están entre las mejores del sector. Estas, combinadas con nuestra experiencia, facilitan una transición fluida hacia una estrategia de seguridad más sólida.

¿Sus equipos tienen dificultades para implementar Zero Trust? Estamos aquí para ayudarle.

La responsabilidad de crear una arquitectura Zero Trust no recae en un solo departamento. Es un esfuerzo común que requiere el compromiso, la flexibilidad y la aprobación de varias partes interesadas dentro de la organización.

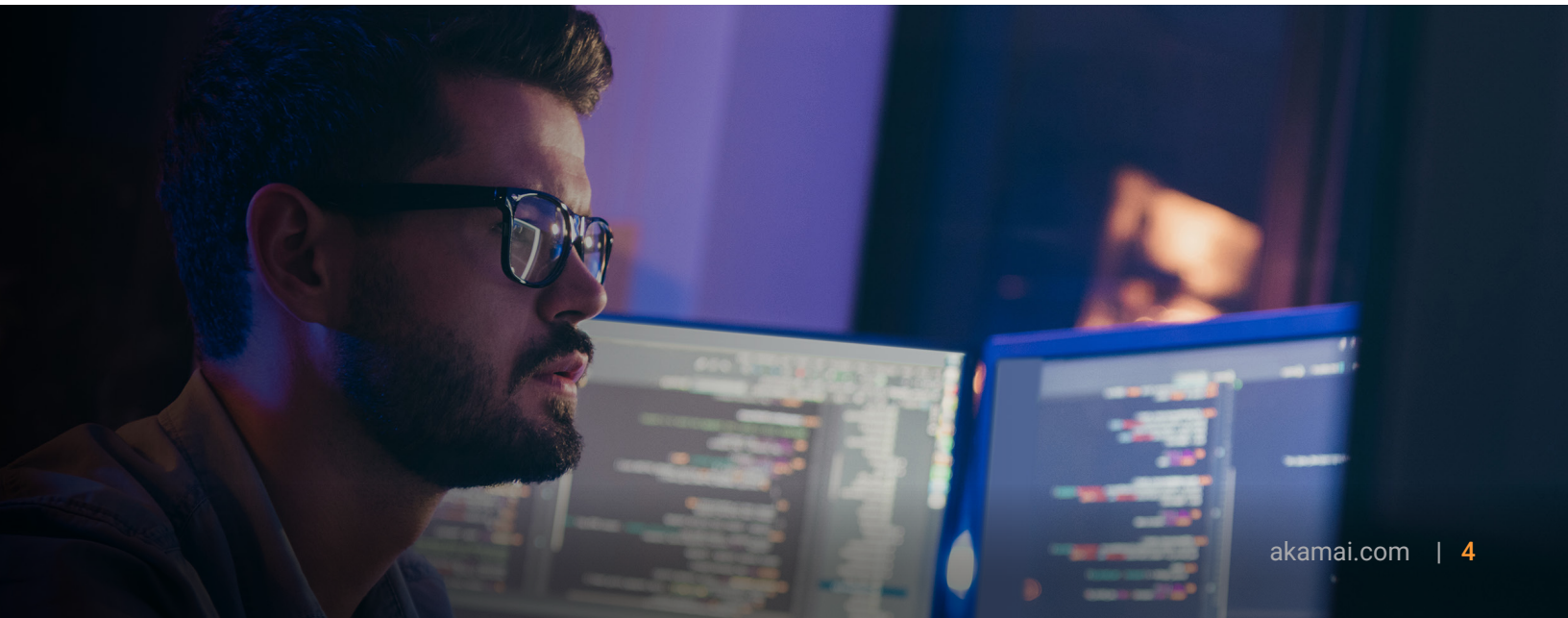
Akamai es la empresa de ciberseguridad y cloud computing que potencia y protege los negocios online. Nuestras soluciones de seguridad líderes en el mercado, nuestra inteligencia ante amenazas consolidada y nuestro equipo de operaciones globales proporcionan una defensa para proteger los datos y aplicaciones esenciales en cada punto de contacto, dondequiera que estén. Por todo esto, comprendemos los desafíos más comunes que afrontan las organizaciones al intentar adoptar una estrategia de seguridad Zero Trust y ofrecemos soluciones para superarlos.

Tres desafíos habituales de Zero Trust

1. **Saber por dónde empezar.** Normalmente recomendamos empezar por aumentar la visibilidad de las cargas de trabajo y reducir la superficie de ataque para reforzar la ciberresiliencia, pero eso depende, por supuesto, de la situación de seguridad actual de la organización.

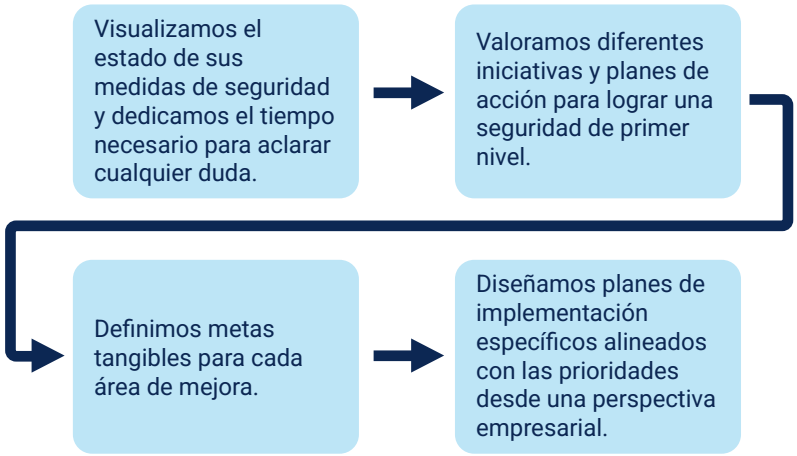
2. **Lograr el éxito rápidamente.** Adoptar un enfoque Zero Trust puede parecer tan difícil que a los equipos les cuesta centrarse en una acción concreta o alegrarse por los pequeños avances.

3. **Lograr el retorno de la inversión.** La transición no suele ser barata y, por lo general, implica una transformación tanto cultural como tecnológica dentro de la organización. Para los responsables de la seguridad y de la toma de decisiones, lo más importante es poder lograr el retorno de la inversión, ya sea mediante la reducción de la superficie de ataque, la mitigación de una brecha, la protección de vulnerabilidades o un beneficio económico.



¿Todo listo para iniciar su transición hacia Zero Trust y evaluar su estrategia de seguridad?

Tal y como hicimos en Akamai, puede utilizar el ZTMM para visualizar el grado de madurez de las medidas de seguridad actuales de su organización. Así identificará áreas donde armonizar más sus procesos y descubrirá qué cambios son necesarios para lograr una arquitectura Zero Trust.



Cómo Akamai puede guiarle hacia una estrategia de seguridad Zero Trust

Una arquitectura Zero Trust eficiente aborda los retos de seguridad con una combinación de controles y principios.

Consideraremos iniciativas y hojas de ruta para ayudarle a diseñar un plan de implementación que se alinee con su organización y sus objetivos empresariales, permitiéndole llevar su seguridad al más alto nivel. Este enfoque nos permite trabajar juntos para crear sistemas y procesos de seguridad que sean eficaces y sostenibles a largo plazo.

Utilizaremos Akamai Cloud, nuestro conjunto de productos de seguridad, que incluye una avanzada herramienta de ZTNA distribuida, microsegmentación líder en el sector, autenticación multifactorial (MFA) a prueba de phishing y un firewall de DNS proactivo, para llevar su estrategia de seguridad al grado de madurez Óptimo, todo ello con un solo agente que utiliza una única consola (Figura 3).

Fig. 3: El conjunto de productos de seguridad de Akamai puede ejecutarse con un solo agente que utiliza una única consola

Caso real

Evaluación de la estrategia de seguridad de un retailer multinacional en materia de e-commerce mediante el ZTMM

Recientemente analizamos la estrategia de seguridad de un retailer multinacional en materia de e-commerce. Durante el proceso, analizamos su seguridad actual y le facilitamos una hoja de ruta para ayudarle a perfeccionarla. Nuestro equipo de expertos identificó áreas de mejora que clasificamos de mayor a menor importancia. Estos fueron los resultados:

Un sistema desequilibrado con diferentes grados de implementación

En todos los pilares, observamos que algunas funciones se habían implementado con el grado de madurez más alto (Óptimo), como la gestión de dispositivos móviles y la automatización de la implementación de aplicaciones, mientras que otras seguían teniendo el grado Tradicional, lo que suponía graves riesgos.

Concretamente, no se habían reforzado funciones clave de los pilares Identidad y Red; siendo estos imprescindibles para una arquitectura Zero Trust. Entre estas funciones se incluían la autenticación multifactorial (MFA), la gestión integrada de la infraestructura de identidad, el control de acceso basado en el contexto y la microsegmentación.

Riesgos en la infraestructura de identidad

Nuestro equipo de análisis descubrió que el retailer confiaba principalmente en la autenticación de ID y contraseña, con la MFA limitada a unos pocos sistemas, lo que abría la puerta a abusos de credenciales de autenticación. Además, se encontraron múltiples infraestructuras de identidad inconexas, como Microsoft Entra ID, Active Directory (AD) local y el protocolo ligero de acceso a directorios (LDAP). La falta de integración entre estos sistemas representaba un peligro considerable, ya que una infraestructura con medidas de seguridad débiles, como LDAP, puede convertirse en el origen de una brecha.

Controles de autorización no integrados

Los controles de autorización tampoco estaban integrados, por lo que había que gestionar cada aplicación individualmente. De esta manera, no se podía denegar el acceso a dispositivos vulnerables ni bloquear otros accesos sospechosos, por ejemplo, si el ordenador de un empleado o partner con acceso a la red de la organización se infectaba con malware, existía un alto riesgo de que un usuario no autorizado utilizase técnicas de movimiento lateral para acceder a los sistemas y recursos de la empresa.

Segmentación inadecuada

Descubrimos que las medidas de seguridad se centraban mayormente en amenazas externas, ignorando los riesgos que suponían los atacantes que ya habían irrumpido en la red. Solo una sólida segmentación interna puede impedir que una intrusión en un almacén a través de la red Wi-Fi o de vulnerabilidades en la VPN abra la puerta al uso de técnicas de movimiento lateral, que es imposible de controlar. Esta falta de barreras internas aumentó significativamente el riesgo de que se filtrasen datos, de que un atacante pudiera moverse libremente por la red sin medidas para pararlo, de que las operaciones se vieran interrumpidas y de que el sistema se viera comprometido de forma generalizada.

Gestión y resolución insuficientes de vulnerabilidades

El retailer carecía de un sistema de gestión que vinculara una lista de materiales de software (SBOM) con los datos existentes sobre vulnerabilidades, lo que le impedía identificar y corregir rápidamente las vulnerabilidades de las aplicaciones, y suponía un peligro para la organización.

Nuestras recomendaciones

Recomendamos al retailer que siguiese estos cinco pasos para reforzar su estrategia de seguridad:

1. Incorporar medidas proactivas para reducir el riesgo de intrusiones no autorizadas y el uso de técnicas de movimiento lateral que se observan en la configuración actual.
2. Seguir integrando la infraestructura de identidad con la pila tecnológica existente.
3. Diseñar un plan para ampliar las capacidades de autenticación y autorización, e implementar el acceso de red Zero Trust.
4. Encontrar la manera más eficaz de adoptar una protección granular para las aplicaciones y cargas de trabajo.
5. Desarrollar un sistema y un protocolo de respuesta ante futuras amenazas desconocidas, así como un sistema y un proceso para fortalecer la gestión de vulnerabilidades, y formular un plan de acción.

Si tiene interés en iniciar su transición a Zero Trust, póngase en contacto con nosotros para una evaluación de seguridad gratuita.

Apéndice A: Descripción general del concepto Zero Trust

Zero Trust es una filosofía de seguridad con la idea de que ningún usuario, dispositivo o sistema dentro o fuera de la red de una organización es de fiar hasta que se demuestre lo contrario.

Así, se implementan métodos de verificación y supervisión que minimizan el riesgo, lo que incluye políticas estrictas de gestión de acceso e identidades (IAM), autenticación multifactorial (MFA) y control de acceso por roles (RBAC).

Aunque el concepto de Zero Trust tiene ya 15 años, cobró importancia durante la pandemia de COVID-19, cuando las organizaciones experimentaron un aumento del trabajo remoto y se dieron cuenta de que las medidas de seguridad que tenían dejaban de ser eficaces cuando los usuarios y los dispositivos ya no compartían la misma ubicación.

En la actualidad, sus principios se han implementado de muchas maneras, incluida la arquitectura Zero Trust, el acceso de red Zero Trust (ZTNA), la puerta de enlace web segura Zero Trust (SWG) y la microsegmentación.

Más información sobre Zero Trust

Apéndice B: El marco ZTMM 2.0

Los cinco pilares

Cada pilar puede avanzar a su propio ritmo e incluso ir por delante del resto, hasta que sea necesario que progresen al unísono.

Pilar	Descripción
Identidad	Atributo o conjunto de atributos que describen de forma específica a un usuario o entidad, incluidas las entidades no humanas.
Dispositivos	Cualquier activo que se pueda conectar a una red, como servidores, equipos de escritorio y portátiles, impresoras, teléfonos móviles, dispositivos del Internet de las cosas (IoT), equipos de red, etc.
Redes	Medio de comunicación abierto, que incluye canales comunes, como redes internas de agencias, redes inalámbricas e Internet, así como otros posibles canales utilizados para transferir mensajes.
Aplicaciones y cargas de trabajo	Sistemas de agencias, programas informáticos y servicios que se ejecutan en dispositivos móviles, entornos locales y la nube.
Datos	Archivos y fragmentos estructurados y no estructurados que residen o han residido en sistemas, dispositivos, redes, aplicaciones, bases de datos, infraestructuras y copias de seguridad, así como los metadatos asociados.

Capacidades transversales

Estas tres capacidades sostienen todo el marco Zero Trust, lo que garantiza la integración, capacidad de respuesta y coherencia de las medidas de seguridad.

Capacidad	Descripción
Visibilidad y análisis	Las organizaciones deben tener una visión clara y en tiempo real de todas las actividades de los usuarios, los estados de los dispositivos y las interacciones de red. Las amenazas se detectan y corrigen rápidamente, lo que reduce el riesgo. Las organizaciones adoptan medidas de seguridad fundamentadas y proactivas.
Automatización y orquestación	Los errores humanos están detrás de muchos problemas de seguridad, pero se pueden minimizar optimizando la automatización y la orquestación. La automatización simplifica las tareas rutinarias y la orquestación planifica las tareas de seguridad en diferentes sistemas. De este modo, se crean las condiciones adecuadas para responder de manera más rápida y coordinada a las amenazas.
Gobernanza	Una buena gobernanza fomenta la responsabilidad y garantiza que todos sigan las mismas prácticas y normativas de seguridad, al tiempo que sienta las bases de la seguridad de las operaciones. También establece directrices claras de Zero Trust y ayuda a las organizaciones a cumplir los requisitos normativos.

El concepto de madurez en el ZTMM

El ZTMM 2.0 define cuatro niveles de madurez para cada capacidad. El objetivo es determinar el grado de madurez actual de los cinco pilares y las tres capacidades y, a continuación, diseñar un plan para llevar cada una al grado máximo.

Grado de madurez	Descripción
Tradicional	Configuración, respuesta y mitigación manuales; políticas y soluciones inamovibles e inconexas
Inicial	Automatización básica, soluciones iniciales que se aplican a todos los pilares, implementación elemental del principio de privilegio mínimo y mayor visibilidad de los sistemas internos
Avanzado	Controles automatizados cuando corresponda, adopción de políticas que se aplican a todos los pilares, principio de privilegio mínimo según el nivel de riesgo y la estrategia de seguridad y adopción de medidas de mitigación predefinidas
Óptimo	Controles automatizados cuando corresponda, adopción de políticas que se aplican a todos los pilares, principio de privilegio mínimo según el nivel de riesgo y la estrategia de seguridad y adopción de medidas de mitigación predefinidas