Akamai

WHITE PAPER

Una base para crear una arquitectura Zero Trust

Tabla de contenido

Introducción

El concepto Zero Trust apareció en 2009, cuando Forrester Research hizo referencia a él por primera vez y advirtió a las organizaciones de que era necesario revisar el método tradicional mediante el cual se concedía acceso sin restricciones a cualquier usuario o aplicación que traspasara el perímetro de la red. En su lugar, se debía verificar cada dispositivo, usuario y flujo de red antes de conceder pleno acceso. Desde entonces, la necesidad de adoptar el concepto Zero Trust no ha hecho más que crecer debido a diferentes factores. La pandemia de COVID-19 provocó un aumento del número de empleados que trabajan a distancia, fuera del perímetro de la red. La frecuencia y el grado de sofisticación de los ataques de ransomware son cada vez mayores, lo que incrementa las posibilidades de que un atacante burle sus defensas y de que el coste de ese ciberataque sea mayor. El coste medio de una filtración de datos alcanzó la cifra récord de 9,44 millones de dólares en Estados Unidos, según el informe IBM Cost of a Data Breach 2022 (Coste de la vulneración de datos 2022). Además, el aumento de los dispositivos conectados a la red, como los dispositivos del Internet de las cosas (IoT), y los requisitos adicionales de acceso de red que exigen los partners y clientes amplían la superficie de ataque de las empresas de manera significativa. En este panorama de ciberseguridad en constante evolución, los proveedores de software de red y seguridad no han tardado en introducir nuevos productos o etiquetar los que ya ofrecían como Zero Trust. Por su parte, los consultores y analistas han acuñado nuevos acrónimos y definiciones de mercado. Esto ha hecho que los equipos de seguridad tengan dificultades para explicar conceptos que pueden ser complejos, así como para tomar decisiones de compra que sienten las bases para iniciar una transición hacia una estrategia Zero Trust.

Hemos diseñado este white paper con el objetivo de proporcionar a los equipos de seguridad una guía para invertir en tecnología Zero Trust. Para ello, identificamos el punto de partida y resumimos los factores diferenciadores clave.

El teletrabajo y las aplicaciones en la nube rompen el paradigma de la seguridad de la red

Las personas han dejado atrás las cuatro paredes de su oficina y ahora trabajan en cualquier momento y de forma distinta.

Como resultado, el perímetro de la red ya no existe, al menos no de la forma a la que estábamos acostumbrados. Ahora, es posible encontrar a los usuarios tanto a un lado como al otro del foso tradicional. Proliferan, asimismo, las aplicaciones de tipo software como servicio (SaaS) y las implementaciones multinube. Además, con el surgimiento de las amenazas persistentes y avanzadas, es muy probable que esté dejando entrar a agentes maliciosos en la red de forma involuntaria y ofreciéndoles acceso completo a sus activos más valiosos. Una vez que están dentro, si no cuenta con un programa integral de seguridad Zero Trust, los agentes maliciosos tienen la vía libre.

Esto no es solo una teoría, sino una realidad que se desprende claramente de la propagación y el coste de las filtraciones observadas durante los últimos años, la gran mayoría de ellas derivadas del exceso de confianza dentro del perímetro de la red.

Al mismo tiempo, las aplicaciones que fueron diseñadas para actuar dentro de un perímetro de red suelen ser las que tienen los peores perfiles de seguridad. Después de todo, si usted hubiera sido un programador que suponía que solo los empleados autorizados con buenas intenciones podían acceder a su sistema, ¿se habría andado con tanto cuidado como el programador de hoy en día, que sabe que un enorme ejército de hackers intentará explotar su aplicación basada en Internet?

La solución a estos desafíos del mercado es Zero Trust.

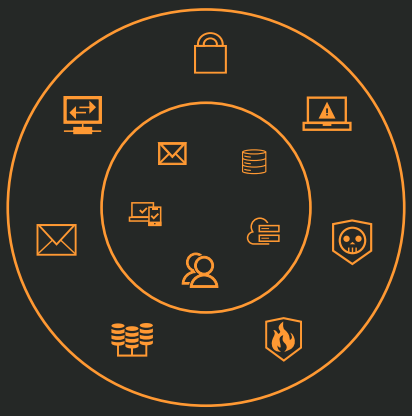
Arquitectura de seguridad Zero Trust

El principio detrás del concepto Zero Trust es bastante sencillo, pero muy efectivo: la confianza no es una cualidad de la ubicación. No se debe confiar en algo simplemente porque está detrás del firewall. En su lugar, solo se debe confiar en una acción, independientemente de dónde ocurra, si se ha permitido de manera explícita. En definitiva, solo *puede* suceder aquello que está *previsto* que suceda. Las organizaciones deben retirar toda la confianza implícita en acciones que no sean necesarias. Por ejemplo, otorgar acceso al sistema financiero a todos los usuarios del equipo de contabilidad cuando solo unos pocos lo necesitan genera riesgos y no aporta ningún valor.

Lo que se debe hacer es realizar un control estricto de autenticación y autorización, y los sistemas no deben transferir ningún dato hasta que se sepa bien que no existe ningún peligro. Además, se deben emplear métodos de análisis y registro para comprobar el comportamiento, y prestar siempre atención a las posibles señales de riesgo.

Este cambio radical podría evitar muchos de los riesgos que hemos observado en la última década. Los atacantes ya no podrían superar el foso para explotar las debilidades de su perímetro y, posteriormente, sus datos y aplicaciones confidenciales. Ya no hay foso que cruzar. Solo hay aplicaciones y usuarios, cada uno de los cuales debe autenticarse mutuamente y cuya autorización debe verificarse antes de conceder cualquier acceso.

Arquitectura de seguridad tradicional



Realidad moderna

¿Cómo crea una organización una arquitectura Zero Trust?

En primer lugar, todas las empresas deben diseñar una estrategia para su entorno actual y determinar si necesitarán incorporar nuevos empleados a la plantilla y cuándo deberán hacerlo. Podríamos dedicar un documento entero a este paso clave del proceso, pero los productos que realmente pueden ayudar en la adopción de una estrategia Zero Trust deben basarse en tres objetivos.

1. **No confíe en ninguna entidad, verifique constantemente.** La máxima "no confíe y verifique constantemente" parece más sencilla de lo que es en realidad. No puede limitarse a retirar el acceso a todos los sistemas y los datos, ya que terminará por bloquear su red. El verdadero desafío consiste en llevar a cabo verificaciones constantes sin que esto cree grandes interrupciones en el negocio, especialmente cuando la mayoría de los sistemas se diseñaron con la confianza implícita en mente. Necesita una visibilidad y un control amplios para todos los tipos de acceso y métodos sencillos y prácticos para aplicar y mantener las políticas.
2. **Tras la verificación, asegúrese de proporcionar el mínimo acceso.** En un entorno Zero Trust, una vez que se ha verificado a un usuario, solo se le debe conceder acceso a las funciones que requiera su puesto.
3. **Supervise las amenazas continuamente.** La mayoría de los expertos del sector le dirán que el modelo Zero Trust es un ejercicio continuo. Los atacantes emplean técnicas cada vez más sofisticadas para tratar de vulnerar las defensas de una empresa, y la organización debe supervisar, verificar y limitar el acceso de forma continua. Una de las ventajas del modelo Zero Trust es que no se centra en lo que hacen los agentes maliciosos, sino en lo que hace la propia empresa. Si cuenta con una verdadera política Zero Trust, las cadenas de ataque tendrán dificultades para trastocar los activos que su empresa necesita para funcionar. Podrá detener cualquier ataque en algún punto de la cadena. Esto incluye la capacidad de detener ataques que todavía no se han concebido. No importa si se trata de un ataque de día cero o no, la seguridad Zero Trust puede ayudarle a mitigarlo.

El lado oscuro de la Zero Trust

Sin embargo, a medida que una organización se embarca en la implementación del modelo Zero Trust, también debe tener en cuenta la otra cara de la moneda de la desconfianza y las restricciones de acceso. Un aspecto fundamental de la Zero Trust es restringir el acceso, principalmente a través de la creación de listas de autorización. Esta es la práctica de dictar lo que puede suceder; todo lo demás se rechaza por defecto. No obstante, al disminuir la capacidad de un atacante de llevar a cabo su acción maliciosa, las organizaciones aumentan la probabilidad de impedir accidentalmente que los usuarios legítimos hagan su trabajo. Además, la constante comprobación de las cargas de trabajo y los dispositivos pueden sumar retrasos y aumentar la frustración. Una estrategia Zero Trust que impida a las personas hacer su trabajo de forma eficaz ni siquiera puede llamarse estrategia.

Por lo tanto, una buena estrategia Zero Trust será aquella que consiga mantener el equilibrio entre seguridad y acceso. También deberá encontrar un equilibrio entre lo que se puede lograr eficazmente y los recursos, tanto presupuestarios como de personal, de los que dispone su equipo de seguridad.

Elementos de la Zero Trust

Han pasado más de 10 años desde que Forrester describió por primera vez el concepto Zero Trust. Muchas organizaciones acaban de comenzar su transición hacia un modelo Zero Trust y se enfrentan a un complicado mercado de productos de software. Algunos productos llevan años en el mercado y se ocupan de partes específicas de la arquitectura Zero Trust. También han surgido nuevos productos, y muchos proveedores de software no han tardado en rebautizar sus ofertas con el apelativo Zero Trust. Además, como manifiestan muchos analistas y expertos del sector, "el modelo Zero Trust debe concebirse como una estrategia integral, no como un producto; no se trata de una meta, sino de un camino". Sin embargo, aunque esta idea se repite una y otra vez, no sirve de gran ayuda para quienes deben tomar decisiones de compra de soluciones tecnológicas Zero Trust e incluso puede crear más confusión.

No existe un único producto que permita a las empresas adoptar directamente un enfoque Zero Trust. Además, cada organización tendrá diferentes prioridades y vulnerabilidades, por lo que el punto de partida será diferente en cada caso. Sin embargo, gracias a los avances tecnológicos y a la consolidación del sector, las empresas ahora pueden obtener las herramientas necesarias para implementar una política Zero Trust utilizando un único proveedor. Las empresas de analistas también están empezando a darse cuenta de esta circunstancia. Gartner hace un seguimiento de lo que denomina el perímetro de servicios de seguridad o SSE, una combinación de puertas de enlace web seguras, agentes seguros de acceso a la nube y acceso de red Zero Trust (ZTNA). En su informe What Are Practical Projects for Implementing Zero Trust? (¿Qué proyectos son prácticos para implementar la Zero Trust?), Gartner también incluye la microsegmentación (que denomina segmentación entre cargas de trabajo) y recomienda que "las organizaciones que deseen pasar a una implementación práctica deben centrarse en dos proyectos clave: la segmentación entre usuarios y aplicaciones (ZTNA) y la segmentación entre cargas de trabajo (segmentación basada en identidades)".

Del mismo modo, IDC divide el modelo Zero Trust en acceso seguro y segmentación, y lo concibe como una visión integral de las tecnologías emergentes y heredadas que se utilizan para proteger los sistemas informáticos, los recursos y los datos mediante la segmentación lógica, el control de acceso y la detección de amenazas.

La mayoría de los expertos espera que el mercado se una a esta tendencia y adopte varias aplicaciones de un único proveedor. En su informe Predicts 2022: Consolidated Security Platforms Are the Future (Previsiones de 2022: las plataformas de seguridad consolidadas son el futuro), Gartner prevé que "para 2025, el 80 % de las empresas habrá adoptado una estrategia para unificar el acceso a la web, los servicios en la nube y las aplicaciones privadas mediante una plataforma SSE de un único proveedor".

Sin embargo, agrupar los diferentes sistemas en una estrategia cohesionada se convierte en un reto fundamental. ¿Cuáles son los elementos clave? ¿Qué deberían buscar los directores de tecnología (CIO), los directores de seguridad de la información (CISO) y el resto de profesionales de la seguridad a la hora de crear una arquitectura Zero Trust adecuada para su organización?

Los principios de la arquitectura Zero Trust

Acceso de red Zero Trust

Aunque en ocasiones se confunde con el enfoque general de Zero Trust, el acceso de red Zero Trust (ZTNA) es una parte fundamental de la pila tecnológica. El acceso seguro es un paso inicial clave en cualquier marco Zero Trust. Lamentablemente, como ocurre con muchos elementos del proceso, suele tornarse más complejo de lo que parece con rapidez. El acceso seguro no es una decisión binaria. Proporcionar a los usuarios apropiados el nivel de acceso adecuado a las aplicaciones que necesitan en todo momento se ha vuelto una tarea mucho más compleja, ya que tanto los unos como las otras están ampliamente distribuidos. De hecho, el concepto de usuario ahora abarca mucho más que el empleado y puede incluir a clientes, proveedores y partners. Al mismo tiempo, las aplicaciones pueden incluir aplicaciones heredadas, SaaS o aplicaciones móviles que requieren acceso bidireccional al centro de datos, Internet o entornos en la nube.

Una solución ZTNA eficaz verificará la identidad del usuario y su dispositivo, así como que tiene acceso a las aplicaciones que necesita, independientemente de dónde se encuentre. De esta forma, se reduce la superficie de ataque posible y se mejora la flexibilidad y la supervisión. Durante décadas, las organizaciones han confiado en redes privadas virtuales (VPN) de proveedores de identidad para proporcionar acceso. Esas VPN, cuyo diseño pertenece a otra época, ya no son suficiente para suplir los requisitos de tamaño y alcance que presentan los equipos de trabajo dispersos a nivel geográfico de hoy en día. El modelo ZTNA ha evolucionado para convertirse en algo más que una simple solución para sustituir las VPN. Ahora, además de otorgar acceso mediante la verificación de la identidad del usuario y su dispositivo, lo hace mediante atributos como la fecha y la hora, la geolocalización y el perfil del dispositivo, a fin de garantizar el nivel de confianza adecuado.

Consideraciones clave para adquirir soluciones de acceso de red Zero Trust

A medida que las empresas empiezan a sustituir sus antiguas VPN por soluciones de gestión de identidades más sofisticadas, deben tener en cuenta diferentes aspectos. Las soluciones más avanzadas de hoy en día deben combinar la gestión de acceso e identidades, la seguridad de las aplicaciones, la autenticación multifactorial (MFA) y el inicio de sesión único, todo ello con visibilidad y control de la gestión, en una única interfaz. Las organizaciones que desean desarrollar iniciativas Zero Trust tienen que buscar soluciones que puedan satisfacer sus necesidades actuales, pero que también se adapten al crecimiento del negocio y les permitan incorporar rápidamente nuevos empleados tras una fusión o adquisición empresarial, instalar la fabricación o la producción en diferentes mercados o zonas geográficas, agregar y quitar contratistas fácilmente para adaptarse a las cambiantes necesidades empresariales y migrar las aplicaciones a la nube de forma rentable sin sacrificar la seguridad.

Las organizaciones deben asegurarse de que las soluciones se puedan integrar directamente con las infraestructuras de identidad actuales, incluso si estas incluyen varios directorios y proveedores de servicios de identidad. Esto permite implementar el servicio ZTNA rápidamente sin necesidad de cambiar la infraestructura o la arquitectura de identidad existente.

El enfoque de Edge

Existe un importante factor diferenciador entre los productos del mercado que es posible que los equipos encargados de la toma de decisiones de compra de soluciones Zero Trust no tengan en cuenta, pero al que deberían prestar atención. Las soluciones que se combinan con las plataformas de Edge en la nube pueden ofrecer ventajas adicionales, ya que actúan como un proxy con reconocimiento de identidades que abstrae la conectividad a la plataforma de Edge. Esto garantiza que toda la autenticación se lleve a cabo en el Edge y fuera del centro de datos. Aunque algunas empresas recurren a arquitecturas de proxy de acceso que se ejecutan dentro de la zona desmilitarizada (DMZ), esta solución no aprovecha la capacidad de la nube para absorber mejor los ataques, proporcionar ancho de banda para el almacenamiento en caché y ofrecer escalabilidad automática según sea necesario. Un proxy con reconocimiento de identidades integrado en la nube puede aumentar sus recursos para responder a la demanda, ejecutar recursos que tienen un alto consumo de CPU y absorber los ataques. Además, se ubica en una dirección IP privada a la que no se puede acceder directamente desde Internet. Las actividades que requieren un mayor nivel de rendimiento y seguridad se llevan a cabo en el Edge, más cerca del usuario final. Además, la entrada vulnerable a la aplicación se realiza a través de un túnel de aplicaciones invertido, lo que elimina de forma eficaz la visibilidad de la IP del perímetro y reduce el riesgo de sufrir ataques volumétricos.

> **Las soluciones que se combinan con las plataformas de Edge en la nube pueden ofrecer ventajas adicionales, ya que actúan como un proxy con reconocimiento de identidades.**

Consideraciones sobre la autenticación multifactorial al crear un modelo Zero Trust

El aumento del teletrabajo y la necesidad de un mayor acceso han hecho que la mayoría de las organizaciones ya hayan adoptado la MFA y cuenten con algún tipo de solución para abordarla. Sin embargo, no hay que perder de vista que la combinación del acceso para toda la empresa y la MFA supera la suma de ambas partes. La MFA es fundamental para el concepto de la confianza, ya que requiere algo más que una simple contraseña. Necesita una segunda verificación para asegurarse de que no cae en la trampa de una de las áreas en las que más se abusa de la confianza. Cabe recordar también que no todas las soluciones de MFA se crean de la misma manera.

Al evaluar las soluciones de MFA como parte de una estrategia Zero Trust, las organizaciones deben buscar soluciones que ofrezcan:

- Integración con la gestión de identidades y el acceso empresarial.
- Cumplimiento del estándar FIDO2 para garantizar que las credenciales de usuario estén descentralizadas, aisladas y cifradas en los dispositivos personales de los usuarios, lo que es especialmente importante para defenderse de los ataques de phishing.
- Capacidad para verificar a los usuarios a través de su smartphone sin depender de una llave física.

Microsegmentación

No existe un estado de Zero Trust perfecto. Inevitablemente, habrá lagunas en la protección que los atacantes más persistentes sean capaces de encontrar y aprovechar. Por lo tanto, cualquier enfoque completo de Zero Trust requerirá microsegmentación. En la actualidad, la mayoría de las redes no están segmentadas y, si lo están, no cuentan con muchos segmentos. De hecho, las organizaciones tradicionalmente han protegido sus aplicaciones esenciales mediante firewalls, una solución que es poco eficaz por varios motivos. Básicamente, los firewalls exigen que se aplique una política de red, lo que genera un punto de estrangulamiento. Esto hace que las conexiones de red deban pasar por un firewall que se encarece rápidamente, no detecta muchos de los riesgos del tráfico de red moderno y es extremadamente difícil de cambiar. Como alternativa, las organizaciones están recurriendo a la microsegmentación basada en software, ya que simplifica muchos de estos laboriosos procesos.

Diferenciadores en la microsegmentación

A pesar de ser un requisito fundamental de cualquier iniciativa Zero Trust, la microsegmentación a menudo se ha considerado un elemento independiente de las soluciones básicas de ZTNA. Los compradores pueden adquirirla como una solución independiente y como parte de las plataformas de seguridad de diferentes proveedores, pero existen algunas diferencias fundamentales que deben conocer.

¿Dónde se puede implementar? Las soluciones de microsegmentación que se crearon como herramientas de red, en lugar de con un enfoque centrado en la seguridad, o las que se crearon para sistemas locales deberían activar las señales de alarma de los posibles compradores. Las herramientas actuales deberían poder implementarse en la nube, en entornos locales, en dispositivos (incluidos aquellos en los que no se pueden instalar agentes) y en los contenedores de entornos híbridos. Esta capacidad suele requerir un software basado en la nube. Si una solución de microsegmentación solo sirve para el 80 % de su entorno, no será suficiente.

¿Qué nivel de visibilidad proporciona? Aunque las soluciones de microsegmentación restringen el acceso, una restricción excesiva puede interrumpir los procesos empresariales y provocar una llamada de atención del director de operaciones (COO). La microsegmentación requiere un conocimiento exhaustivo del entorno. ¿A qué servidores puede acceder cada servidor? ¿Se pueden definir políticas entre un clúster de Kubernetes y un servidor Windows Server 2008? Muchas herramientas no cuentan con agentes que sean compatibles con versiones tan antiguas como las de 2008 ni tienen unas capacidades tan avanzadas como la aplicación de políticas en Kubernetes. Si desea implementar el modelo Zero Trust de forma eficaz, su software de microsegmentación debe ser capaz de abordar este tipo de dificultades. Además, los compradores de software de microsegmentación deben tener en cuenta el nivel de detalle de las políticas que ofrecerá el producto. La mayoría de los sistemas podrán aplicar políticas en la capa de aplicación en todos los puertos y procesos, pero los productos más sofisticados también podrán hacerlo en la capa de microservicios. Por ejemplo, los atacantes pueden utilizar algunos de los servicios de svchost, como el programador de tareas, para moverse lateralmente por la red. Sin embargo, las empresas no pueden bloquear directamente el proceso svchost, ya que se encarga de muchas tareas importantes. Ahí es donde una solución de microsegmentación que aplica políticas en la capa de microservicios puede marcar la diferencia.

¿Es difícil implementarla? La facilidad con la que expresa su política actual, así como las capacidades que necesitará en el futuro son importantes factores clave que debe tener en cuenta al elegir una solución de microsegmentación. Ya se trate de una política preventiva para cuando se encuentre en una fase de planificación, o una política proactiva para cuando su entorno se vea amenazado y necesite bloquearlo, debe asegurarse de que el motor en el que invierte sea compatible con ambos casos. Por ejemplo, empezar a crear listas de autorización en un proyecto de microsegmentación puede resultar una tarea intimidante para los equipos de seguridad, ya que corren el riesgo de denegar por error una aplicación o un servicio necesario. Una solución de microsegmentación sofisticada debe incluir plantillas de listas de denegación que los equipos puedan implementar de forma rápida y sencilla para lograr algunos avances rápidos en el proyecto. Una vez conseguido esto, las organizaciones pueden proseguir su camino hacia una protección completa basada en listas de autorización que incluya funciones precisas de asignación de dependencias e inventario contextual.

> **Las soluciones de microsegmentación que se crearon como herramientas de red, en lugar de con un enfoque centrado en la seguridad, o las que se crearon para sistemas locales deberían activar las señales de alarma de los posibles compradores.**

Puerta de enlace web segura

En un entorno Zero Trust, no solo se debe desconfiar de las personas, sino del propio Internet. Los empleados necesitan acceso a Internet y, conforme aumentan las aplicaciones móviles y SaaS, los servicios en la nube, el teletrabajo y los dispositivos de IoT, también lo hace la superficie de ataque de una organización. La dificultad para proteger a los distintos departamentos y usuarios contra amenazas, como el malware, el ransomware, el phishing y las exfiltraciones de datos, ha aumentado de manera exponencial. Las organizaciones disponen de recursos limitados para gestionar las complicaciones y complejidades que presentan los puntos de control de la seguridad, así como las lagunas en términos de protección que tienen las soluciones locales tradicionales.

La aplicación de un modelo Zero Trust entre una persona e Internet requiere una puerta de enlace web segura (SWG), lo que la convierte en un elemento central de cualquier iniciativa Zero Trust.

Requisitos básicos de Zero Trust para cualquier inversión de puerta de enlace web segura

Aunque parezca sencillo, hay una serie de requisitos que los compradores de tecnología deben tener en cuenta al invertir en una SWG. Muchas organizaciones ya cuentan con SWG locales desplegadas, pero necesitan ampliar esa protección a los usuarios, independientemente de cuál sea su ubicación. Como ocurre con la gestión de identidades, los proveedores que tienen plataformas de Edge sólidas suelen contar con una mayor seguridad de SWG gracias a la inteligencia de la plataforma ampliada. Los responsables de la toma de decisiones deben examinar detenidamente los requisitos básicos que se enumeran a continuación.

Inspección de DNS: los proveedores deben ser capaces de proporcionar inspecciones en tiempo real de todos los dominios con inteligencia ante amenazas sofisticada y bloqueo automático de dominios maliciosos. Las soluciones también deben ser eficaces en todos los puertos y protocolos, con el fin de proteger frente al malware que no utilice puertos y protocolos web estándar. La calidad de la inspección de DNS puede variar mucho entre los diferentes proveedores, y los compradores deben decantarse por aquellos con experiencia en el mercado y buenos resultados con sus clientes.

Inspección de URL: del mismo modo, se deben comprobar todas las solicitudes de HTTP y HTTPS en tiempo real y bloquear las URL maliciosas automáticamente.

Análisis de carga: se deben analizar todas las cargas en busca de malware mediante varias técnicas para proporcionar una protección integral de día cero contra archivos maliciosos. Lo ideal es que la información proporcionada por sus productos de SWG se comparta con otros productos de seguridad para garantizar el aislamiento o la restricción de acceso a los activos comprometidos.

Supervisión de amenazas

El último elemento de la tecnología Zero Trust es la supervisión de amenazas. Aunque la máxima del modelo Zero Trust es no confiar en nada de manera implícita, y la SWG ayuda a bloquear el ransomware y el malware, las organizaciones deben permanecer alerta para detectar ataques emergentes y en curso, así como posibles riesgos (por ejemplo, configuraciones incorrectas o derechos de acceso demasiado permisivos). Cuando los equipos de seguridad evalúen el software disponible en el mercado, deben revisar los tres aspectos que se muestran a continuación para garantizar una supervisión de amenazas eficaz.

Consideraciones clave

- **Algoritmos eficaces**
  Cualquier servicio de supervisión de amenazas debe tener algoritmos sofisticados con un historial de éxito que se basen en anomalías en la actividad de usuarios y redes, análisis ejecutables, análisis de registros y mucho más.

- **Detección potente de señales**
  Aunque el software y la inteligencia artificial son herramientas fundamentales en la supervisión de amenazas, los responsables de la toma de decisiones en torno a Zero Trust deben evaluar la experiencia interna de los proveedores con los que están colaborando. Los servicios de supervisión de amenazas deben ser capaces de distinguir las señales buenas de las malas, a fin de evitar la fatiga de la exposición a alertas, así como proporcionar notificaciones inmediatas sobre cualquier incidente. Las organizaciones también deberían recibir informes periódicos que incluyan el análisis de cualquier campaña con un perfil de alto riesgo.

- **Personal cualificado**
  Además de estar disponibles de manera ininterrumpida, los equipos deben estar formados por personas procedentes de diferentes ámbitos laborales, incluidas la inteligencia militar, la seguridad ofensiva, la respuesta a incidentes o la ciencia de datos. Este es un ámbito en el que los proveedores de distribución de contenido pueden ofrecer ventajas considerables. La información que se obtiene a partir de la supervisión de cientos de terabytes por segundo aporta una perspectiva única de cualquier detección de señales.

Primeros pasos

Las iniciativas Zero Trust pueden ser infinitas. Normalmente, lo primero que se preguntan las personas que están valorando los requisitos de software, hardware y contratación es por qué tecnología deben empezar.

Como suele ocurrir, la respuesta dependerá de los puntos fuertes y débiles, las evaluaciones de riesgos y las necesidades específicas de cada empresa. Para muchos expertos del sector, el punto de partida debe ser la implementación de ZTNA. Es cierto que proteger a la organización del tráfico norte-sur malicioso puede ser un primer paso prudente. Sin embargo, también existe la creencia de que un enfoque este-oeste con microsegmentación, en especial la microsegmentación definida por software, es la mejor opción.

Motivos para poner en marcha la microsegmentación

Si, al igual que la mayoría de los expertos, considera que la defensa perfecta no existe y que los ataques maliciosos terminarán por abrirse camino, seguro que estará interesado en proteger sus activos más valiosos. Esto es precisamente lo que ofrece la microsegmentación.

Uno de los motivos por los que las organizaciones pueden ser reacias a empezar con la microsegmentación es porque creen que se trata de algo complejo. En primer lugar, la microsegmentación no es un enfoque de "todo o nada". Al igual que el modelo Zero Trust, se puede llevar a cabo por etapas. Las organizaciones pueden empezar identificando los activos más valiosos. Para ello, debe centrarse en aquello que sea crítico. Asegúrese de que, si alguien entra en su sistema, no hunda su negocio. La importancia de un activo puede depender de los datos que contiene o del nivel de protección con el

que cuenta. En muchos casos, estos activos serán sus sistemas heredados, ya que los proveedores de seguridad no son compatibles con ellos.

En segundo lugar, la microsegmentación definida por software elimina gran parte de esa percepción de complejidad. Olvídese de tener que lidiar con el hardware y llamar a sus arquitectos de red y seguridad cada dos por tres. Basta con implementar el software para reducir en gran medida las barreras de entrada.

Una vez que ponga en marcha la iniciativa de microsegmentación, las primeras ventajas serán más que evidentes y servirán de impulso para el resto del proyecto. Por ejemplo, tendrá a su disposición una fuente de información fiable sobre lo que está sucediendo en su entorno. Puede acceder a ella de inmediato sin necesidad de aplicar políticas y, una vez que lo haga, conocerá el funcionamiento de los flujos en profundidad.

Además, cuando una organización comienza a aplicar el acordonamiento de aplicaciones, puede bloquear de forma rápida y sencilla las aplicaciones críticas para que solo se comuniquen a través de puertos y procesos específicos. Otro avance rápido podría ser centrarse en las políticas específicas para amenazas. Las plataformas de microsegmentación más sofisticadas tendrán listas de denegación integradas. Esto le permitirá crear rápidamente una política para detener conexiones innecesarias entre los servicios de escritorio remoto e Internet. Por ejemplo, las organizaciones pueden cerrar rápidamente el tipo de vulnerabilidad que desencadenó el ciberataque a Colonial Pipeline.

Sea cual sea el punto de partida, la clave de cualquier camino hacia la Zero Trust es el equilibrio. Por ejemplo, una gestión de identidades perfecta combinada con una segmentación deficiente o una protección débil del acceso web no ofrecerán una buena seguridad.

Plataforma frente a herramientas especializadas

Al igual que ocurre con muchas decisiones tecnológicas, la compra de software Zero Trust suele reducirse a la elección entre especialistas independientes y una plataforma que combina varios componentes. El impacto de Zero Trust en los equipos de seguridad, los encargados de las integraciones, los arquitectos y los analistas, así como su necesidad de mantener políticas en varias consolas y diferentes agentes e integraciones ofrecen argumentos convincentes para optar por una plataforma. Esto es especialmente relevante en un mercado laboral restringido que sufre una escasez de profesionales cualificados en ciberseguridad. La gestión de soluciones de varios proveedores puede aumentar los costes de personal significativamente, ya que las soluciones que no se comunican de forma eficaz generan falsos positivos que suponen una carga para los usuarios finales y pueden requerir asistencia y formación adicionales.

Además, en lo que respecta a las negociaciones de contratos y soporte, la idea de contar con un único proveedor al que acudir suele ser un argumento convincente para implementar el modelo Zero Trust con un proveedor de plataforma.

> **Uno de los motivos por los que las organizaciones pueden ser reacias a empezar con la microsegmentación es porque creen que se trata de algo complejo.**

Revisión de los elementos de la Zero Trust

Sepa quiénes son sus usuarios.
Asegúrese de que están verificados.

Proteja sus activos.
Autentique/autorice todas las transacciones.

Proteja a sus usuarios.
Evite que el malware infecte a los usuarios.

Conclusión

En definitiva, la mayoría de las organizaciones interesadas en protegerse frente a los ciberataques reconocen la necesidad de empezar a adoptar cuanto antes una arquitectura Zero Trust. El aumento del teletrabajo ha hecho que muchas empresas ya hayan iniciado esta transición de manera gradual o más repentina. Sin embargo, a medida que los atacantes se vuelven más sofisticados, las superficies de amenaza se multiplican y el número de participantes que requieren acceso remoto aumenta, la necesidad de contar con una cartera completa de aplicaciones integradas se vuelve cada vez más apremiante.

Si desea obtener más información sobre aspectos específicos del enfoque de Akamai en torno a la seguridad Zero Trust, póngase en contacto con uno de nuestros expertos.

Akamai

Akamai potencia y protege la vida online. Las empresas líderes de todo el mundo eligen Akamai para crear, proteger y ofrecer sus experiencias digitales, ayudando así a millones de personas a vivir, trabajar y jugar cada día. Gracias a la plataforma informática más distribuida del mundo, de la nube al Edge, nuestros clientes pueden desarrollar y ejecutar las aplicaciones con facilidad, mientras acercamos las experiencias a los usuarios y mantenemos las amenazas a raya. Para obtener más información acerca de las soluciones de seguridad, informática y distribución de Akamai, visite akamai.com y akamai.com/blog, o siga a Akamai Technologies en Twitter y LinkedIn. Publicado en enero de 2023.