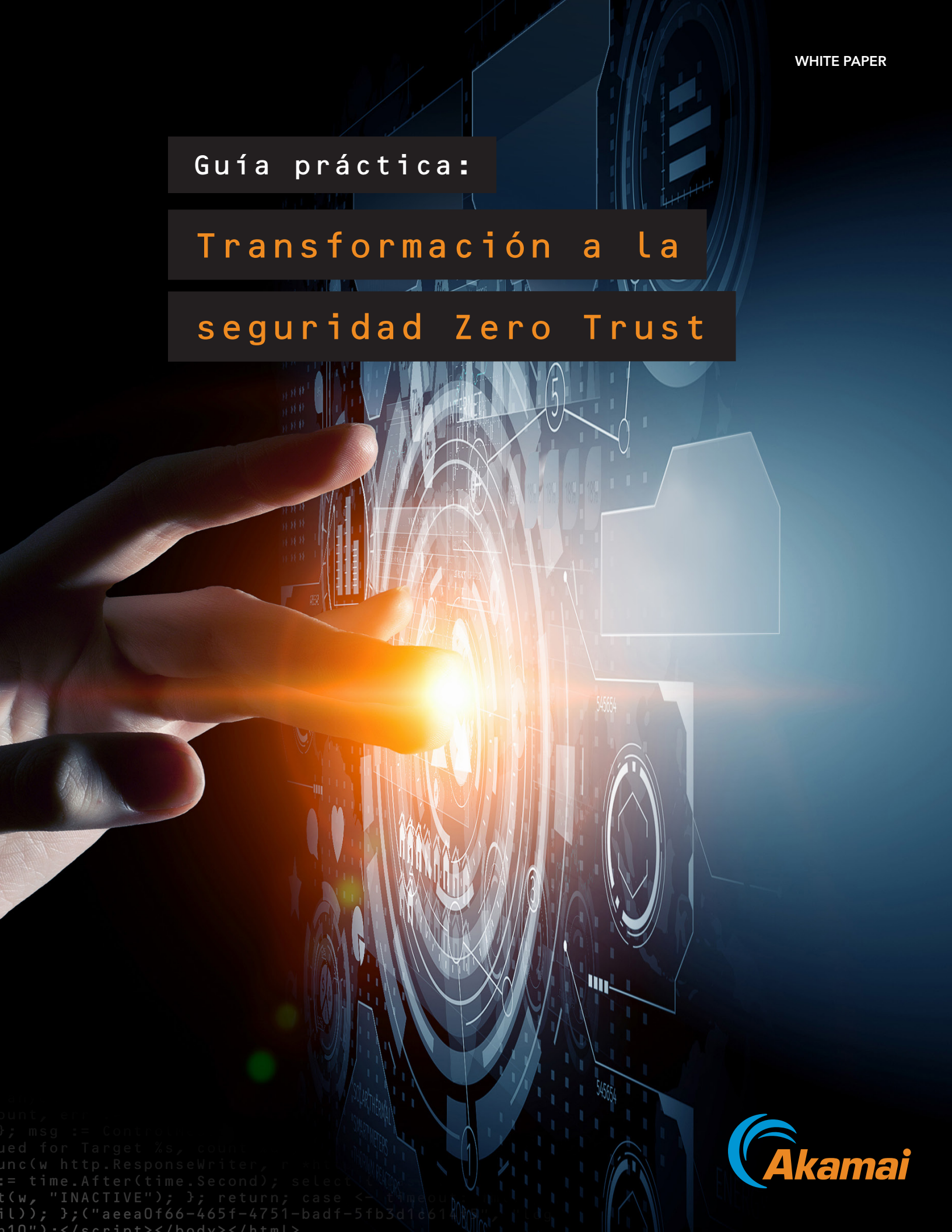
WHITE PAPER

Guía práctica:

Transformación a la seguridad Zero Trust



Akamai

Resumen ejecutivo

La noción de un perímetro de red, en el que todo el que está fuera de la zona de control de la empresa es malicioso y todo el que se encuentra dentro es honesto y bienintencionado, no es algo en lo que se pueda confiar en el panorama empresarial actual. La amplia adopción de aplicaciones SaaS, la migración a arquitecturas basadas en la nube, un número creciente de usuarios remotos y un flujo cada vez mayor de dispositivos BYOD han convertido la seguridad perimetral en irrelevante. Además, una defensa centrada en el perímetro requiere la gestión de políticas de seguridad y de dispositivos, así como frecuentes actualizaciones de software, lo que eleva la complejidad operativa e impone una carga adicional a los ya desbordados equipos de TI. A medida que crece la superficie de ataque y los limitados recursos de TI se esfuerzan por controlar una arquitectura de red cada vez más enrevesada, los ciberdelincuentes se hacen cada vez más competentes y sofisticados, y están más incentivados para evadir las medidas de seguridad. Se necesita un marco de seguridad estratégico que haga frente a estos retos.

¿Qué es la seguridad Zero Trust y por qué es importante?

El modelo Zero Trust sustituye a la arquitectura de seguridad centrada en el perímetro. Garantiza que las decisiones de seguridad y acceso se apliquen de forma dinámica en función de la identidad, el dispositivo y el contexto del usuario. El marco de seguridad Zero Trust también impone que solo los usuarios y dispositivos autenticados y autorizados puedan acceder a las aplicaciones y a los datos. Al mismo tiempo, protege esas aplicaciones y usuarios frente a amenazas avanzadas de Internet.

Para avanzar con la adopción de Zero Trust y proteger a los usuarios y aplicaciones (y el futuro de la empresa), le sugerimos que:

Proporcione a los usuarios acceso solo a las aplicaciones, no a toda la red

Las tecnologías de acceso remoto heredadas, como las redes privadas virtuales (VPN), no son capaces de satisfacer las crecientes exigencias de las empresas digitales, sin perímetro, de hoy. La VPN tradicional supone una amenaza para la seguridad de la empresa porque, de forma inherente, crea un agujero en el firewall, lo que proporciona un acceso a la red sin restricciones. Una vez dentro, el atacante puede moverse lateralmente para acceder y aprovechar cualquier sistema o aplicación de la red. Las redes VPN tradicionales no solo exponen a la empresa a riesgos de seguridad, sino que son soluciones complejas que requieren importantes recursos de TI para la gestión del hardware y el software, y son costosas de mantener y de ampliar.

La segmentación de red, que a veces se considera una contramedida frente al acceso por barrido, ha demostrado ser cara, difícil de llevar a la práctica y compleja en su gestión. Y, en última instancia, ni siquiera reduce el riesgo; con el acceso "ilimitado", sigue siendo posible el movimiento lateral dentro de la red. Aunque compartimenta el tráfico de este a oeste dentro de una subred, no puede detener la propagación horizontal dentro de la misma.

Para proteger su empresa e implantar el modelo Zero Trust, conceda acceso a los usuarios únicamente a las aplicaciones que necesitan para su función. Base este acceso en derechos, en la identidad del usuario, el perfil del dispositivo, la autenticación y la autorización. Siguiendo estas prácticas recomendadas se reducirán los ataques laterales y se limitará la exposición de la red. La eliminación de las VPN tradicionales mejora la experiencia del usuario, aumenta la productividad de la plantilla y reduce las solicitudes de asistencia técnica. Y alejarse de la dependencia de firewalls, hardware y software supone una reducción de los costes de mantenimiento de TI. Además, los permisos de solo aplicación mejoran el control, al proporcionar visibilidad e información sobre quién accede a las aplicaciones, a dónde van los datos y cómo se accede a ellos.

Conceda a los usuarios acceso únicamente a las aplicaciones que necesiten y base este acceso en derechos, en la identidad del usuario, el perfil del dispositivo, la autenticación y la autorización.

Aísle su infraestructura de red de la red pública de Internet

La exposición de las aplicaciones internas y la infraestructura de acceso a Internet las hace vulnerables a los ataques DDoS, la inyección SQL y otros ataques dirigidos a la capa de aplicación. Los ciberdelincuentes son cada vez más sagaces. Utilizan técnicas en constante evolución para analizar la configuración de la red empresarial y descubrir aplicaciones vulnerables y datos valiosos. Por lo tanto, las empresas deben aislar la arquitectura de acceso y las aplicaciones de la red pública de Internet para evitar ataques por parte de agentes malintencionados que utilizan puertos de escucha abiertos. Si los ciberdelincuentes no pueden encontrar la red ni determinar qué aplicaciones y servicios está ejecutando el dispositivo de destino, entonces no pueden atacar.

Implante un WAF para proteger las aplicaciones corporativas

Los ciberataques modernos llegan a un nivel de personalización altísimo. Los agentes maliciosos se valen de la ingeniería social —correo electrónico, redes sociales, mensajería instantánea, SMS, etc.— para atacar individualmente a los usuarios usando cebos muy relevantes y personalizados. Los ciberdelincuentes buscan usuarios específicos con el grado, las competencias y los niveles de acceso deseados y, a continuación, lanzan ataques contra las aplicaciones para conseguir los permisos de esos usuarios.

Si la máquina de un usuario se ve afectada, a menudo se utiliza como dispositivo zombi y, sin que su propietario lo sepa, ejecuta ataques contra aplicaciones corporativas que teóricamente están seguras detrás del firewall. Aunque la mayoría de las organizaciones utilizan un firewall de aplicaciones web (WAF) para proteger sus aplicaciones con exposición externa frente a esos ataques, muchas no han ampliado esta protección a las aplicaciones corporativas dentro de la red. El WAF puede proteger las aplicaciones internas y los datos que se encuentran detrás de ellas frente a ataques de inyección y de capa de aplicación, como la inyección SQL, la ejecución de archivos maliciosos, la falsificación de solicitudes entre sitios (CSRF) y las secuencias de comandos en sitios cruzados.

Los ciberdelincuentes fijarán un dispositivo como objetivo, lo convertirán en una máquina zombi y lo utilizarán para atacar aplicaciones teóricamente seguras detrás de un firewall.

Establezca las identidades, la autenticación y la autorización antes de dar acceso

Los sistemas digitales dan acceso a cualquier persona que introduzca la contraseña correcta, sin verificar la identidad de esa persona. Unas credenciales débiles y la reutilización de contraseñas aumentan de forma significativa la superficie de ataque y el riesgo para una empresa. Con todas las amenazas que existen en la actualidad, ya no basta con una autenticación de factor único, como el nombre de usuario y la contraseña. La autenticación multifactorial (MFA) proporciona un nivel adicional de verificación y seguridad; garantiza que solo los usuarios validados obtengan acceso a las aplicaciones esenciales para el negocio.

La autenticación multifactorial es imprescindible. Unas credenciales débiles, junto con la reutilización de nombres de usuario y contraseñas en las aplicaciones, aumentan significativamente la superficie de ataque de una empresa.

Una vez que el usuario se autentica y autoriza a través de la MFA, el inicio de sesión único (SSO) le permite iniciar sesión en todas las aplicaciones con un único conjunto de credenciales. De esta manera, se mejora la productividad, ya que no es necesario volver a confirmar la identidad en cada aplicación ni se producen problemas de sincronización entre aplicaciones. La continua toma de decisiones de acceso basada en multitud de señales, lo que incluye la MFA y el SSO en aplicaciones IaaS, in situ y SaaS, proporciona mayor protección a la empresa y comodidad a los usuarios finales.

Use la protección avanzada frente a amenazas para combatir el phishing, el malware de día cero y la exfiltración de datos basada en DNS

A pesar de la adopción generalizada de una seguridad por capas por parte de las empresas, los agentes maliciosos siguen introduciéndose en los sistemas de estas aprovechando las debilidades de seguridad. Incluso con firewalls, puertas de enlace web seguras, entornos de pruebas, sistemas de prevención de intrusiones y antivirus de punto final desplegados, las empresas están expuestas al phishing, el malware de día cero y la exfiltración de datos basada en DNS. Entonces, ¿qué falta en las empresas?

El DNS es un vector que a menudo se pasa por alto. Además, los ciberdelincuentes han desarrollado malware específicamente diseñado para aprovechar esta brecha de seguridad, con el que evitan las capas de seguridad existentes para infiltrarse en la red y exfiltrar los datos. Es fundamental añadir una capa de seguridad que utilice el protocolo DNS; usando esta fase de consulta inicial como punto de control de seguridad, la solución de seguridad DNS puede detectar y detener los ciberataques en las primeras fases de la cadena de destrucción y, así, proteger la empresa de forma proactiva.

Las empresas deben utilizar el protocolo DNS como un punto de control de seguridad para detectar y detener los ciberataques en las primeras fases de la cadena de destrucción.

Supervise el tráfico y la actividad vinculados a Internet

Las empresas deben asumir que el entorno es hostil. Este es el principio básico de Zero Trust. Así, las organizaciones deben comprometerse a auditar y confirmar todas las actividades, sin permitirlas a ciegas. Para ello, las empresas necesitan visibilidad de lo que ocurre en sus redes, con un amplio tráfico e inteligencia para realizar las comparaciones relevantes.

Las empresas deben supervisar y verificar todas las solicitudes de DNS de los dispositivos, tanto de dentro como de fuera de la red corporativa –ya sean procedentes de portátiles, teléfonos móviles, equipos de escritorio, tablets, Wi-Fi de invitado o dispositivos IoT–, para garantizar que las consultas no se dirigen a sitios maliciosos o inaceptables. Las organizaciones también requieren la capacidad de examinar el comportamiento del tráfico en busca de signos de actividad sospechosa, como la comunicación con un servidor de mando y control o la exfiltración de datos, y alertar inmediatamente al personal de TI de cualquier problema. Una visión del volumen de tráfico global y de las tendencias de las amenazas facilita a los departamentos de TI la identificación de patrones irregulares o peligrosos.

Favorezca la integración con sistemas de gestión de eventos e información de seguridad (SIEM) y la orquestación a través de las API RESTful

Las empresas pueden tener cientos, o incluso miles, de aplicaciones. Estas deben configurarse a través de una API para desplegar rápidamente aplicaciones en bloque y también para definir controles de políticas de acceso. Se trata de una función esencial para cualquier entorno de aplicaciones a gran escala que desee migrar rápidamente del acceso VPN tradicional al acceso específico de aplicación. La adopción de API sigue aumentando a medida que las empresas integran la metodología DevSecOps y buscan tareas de supervisión y configuración disponibles a través de la API RESTful. También necesitan complementos para incorporar datos de amenazas y eventos en SIEM con el fin de llevar a cabo investigaciones y correlaciones adicionales. Un sistema ampliable debe integrarse, además, con plataformas de automatización de flujos de trabajo y con la intervención frente a amenazas mediante la señalización en soluciones de respuesta y detección de puntos finales de terceros.

Conclusión

La transformación digital es una realidad, y las empresas deben adoptar un modelo de seguridad Zero Trust para desarrollar con éxito el negocio, permitiendo la innovación y la agilidad, pero sin poner en peligro la seguridad. La protección avanzada frente a amenazas, la aceleración de aplicaciones y el uso de la MFA y el SSO en todas las aplicaciones (SaaS, in situ e IaaS) son algunas de las ventajas clave de trabajar en un entorno Zero Trust. Además, el modelo de seguridad Zero Trust permite la orquestación a través de API, así como la integración con SIEM y plataformas de automatización de flujos de trabajo, lo que ofrece visibilidad de usuarios y aplicaciones y facilita despliegues a gran escala en una fracción del tiempo habitualmente necesario.

Akamai puede ayudarle a dirigir la evolución de su red y su seguridad. Realice la evaluación Zero Trust de siete preguntas para saber en qué grado está preparado su negocio para un marco de seguridad Zero Trust. Recibirá un conjunto de próximos pasos personalizados para transformar la red. O bien, si desea obtener recursos para iniciar rápidamente la transición, visite akamai.com/3waystozerotrust.

Akamai