INFORME SOBRE LA SOLUCIÓN DE AKAMAI

Simplifique y proteja con un modelo Zero Trust integral

Zero Trust es un enfoque estratégico de la ciberseguridad que protege a una organización al eliminar la confianza implícita en los usuarios, los dispositivos, las redes, los datos y las aplicaciones. En lugar de suponer que todo lo que hay detrás del firewall de la empresa está a salvo, el enfoque Zero Trust asume que pueden producirse filtraciones en cualquier momento y aplica un acceso basado en el mínimo privilegio a cada solicitud, independientemente de su origen.

Por qué es tan importante ahora una estrategia Zero Trust

Los enfoques Zero Trust se han convertido en una prioridad para las organizaciones que necesitan adaptarse de forma más eficaz a un entorno moderno en constante cambio. Estas organizaciones buscan un nuevo modelo de seguridad capaz de ajustarse a entornos de trabajo híbridos y de proteger a los usuarios, los dispositivos y las aplicaciones, independientemente de su ubicación.

Principios de la arquitectura Zero Trust moderna

- Verificación explícita y siempre en contexto
- Aplicación explícita del privilegio mínimo
- Supervisión continua

La consolidación es esencial:

un enfoque integrado de principio a fin

Un enfoque integral Zero Trust debe extenderse a todas las entidades de la organización, incluidas las identidades, la red y las aplicaciones. Zero Trust sirve como estrategia de principio a fin, por lo que requiere la integración en todos los elementos. El uso de varias soluciones puntuales poco integradas no se ajusta a este enfoque estratégico.

Akamai ha reunido una sólida cartera integral para ofrecer todas las soluciones Zero Trust esenciales para la organización moderna. En lugar de instalar, ejecutar y mantener diferentes productos de seguridad, las organizaciones pueden confiar en un único proveedor que les ofrece todas las tecnologías necesarias y disfrutar de costes reducidos y una mayor eficiencia operativa.

Intercambio de datos entre soluciones

Akamai ha integrado la automatización en toda su cartera Zero Trust, lo que reduce en gran medida la complejidad y las personalizaciones necesarias. De esta forma, los distintos productos de la cartera pueden compartir conocimientos sobre amenazas entre sí para mejorar la seguridad en cada uno de ellos. Si un producto identifica una amenaza, puede alertar a otro para que la mitigue.

Ventajas

- **Equipos de trabajo dispersos**
  Permita a los usuarios trabajar de forma más segura desde cualquier lugar, en cualquier momento y en cualquier dispositivo.
- **Migración a la nube**
  Proporcione un control de acceso seguro en entornos de nube e híbridos.
- **Mitigación de riesgos**
  Detenga las amenazas y minimice el movimiento lateral del ransomware y otros tipos de malware.
- **Conformidad**
  Garantice la conformidad con los microperímetros en torno a los datos confidenciales.

Akamai

Una cartera integral de principio a fin: usuarios, aplicaciones y red

Protección de la carga de trabajo

Akamai Guardicore Segmentation: Zero Trust para aplicaciones

Akamai Segmentation proporciona la solución de microsegmentación líder del sector, diseñada para limitar la propagación del ransomware y otros tipos de malware. El producto proporciona visibilidad y comprensión de las cargas de trabajo, los procesos y las aplicaciones. Además, permite aplicar políticas de acceso.

Protección de la red

Enterprise Application Access: acceso de red Zero Trust

La tecnología de acceso de red Zero Trust de Akamai se ha diseñado para sustituir a la tecnología VPN tradicional y para gestionar las identidades de usuario de una manera sólida. En lugar de poner en riesgo toda la red, Enterprise Application Access solo permite el acceso de los usuarios a las aplicaciones que necesitan para realizar su trabajo. Enterprise Application Access proporciona visibilidad de la identidad de los usuarios y una aplicación sólida de los parámetros de identificación y autenticación.

Protección del usuario

Secure Internet Access: acceso a Internet Zero Trust

Secure Internet Access es una puerta de enlace web segura basada en la nube. Esta solución se encarga de inspeccionar todas las solicitudes web que realizan los usuarios y aplica inteligencia contra amenazas en tiempo real y técnicas avanzadas de análisis de malware para garantizar la entrega única y exclusivamente de contenido seguro. Las solicitudes y el contenido maliciosos se bloquean de forma proactiva.

Autenticación multifactorial: identidad sólida con Zero Trust

Akamai MFA protege las cuentas de los empleados del phishing y otros ataques de máquina intermediaria. De este modo, se garantiza que solo los empleados autenticados pueden acceder a las cuentas que poseen, se deniega el acceso a otros y se evita el robo de cuentas de empleados.

Control y supervisión

Akamai Hunt: servicios de seguridad

Al adoptar un enfoque basado en "asumir siempre que se ha producido una filtración", el equipo de expertos en investigación de amenazas está constantemente a la caza de comportamientos de ataque anómalos y amenazas avanzadas, capaces de eludir a menudo las soluciones de seguridad estándar. Nuestros expertos en amenazas le notificarán inmediatamente de cualquier incidente crítico detectado en su red y, a continuación, trabajarán en estrecha colaboración con su equipo para poner en orden la situación.

La ventaja de Akamai

Akamai ofrece algunas ventajas que lo diferencian de otros proveedores Zero Trust. Ofrecemos la cobertura más amplia: sistemas heredados y modernos; Windows y Linux, entornos locales y virtualizados, contenedores y mucho más. Gracias a nuestra visibilidad sin igual, los usuarios pueden saber en cada momento qué está haciendo cada carga de trabajo y tener el contexto completo. Y nuestros excelentes servicios internos de búsqueda de amenazas amplían las capacidades de cualquier equipo de seguridad y permiten a su organización mantenerse siempre un paso por delante.

Para obtener más información sobre Zero Trust y cómo empezar, visite akamai.com.