INFORMACIÓN SOBRE EL PRODUCTO DE AKAMAI

Akamai Guardicore Access

ZTNA y microsegmentación unificados

Una única consola que ofrece visibilidad y control, capaz de simplificar y acelerar los modelos Zero Trust

Las organizaciones están adoptando rápidamente la seguridad Zero Trust para detener el ransomware, cumplir las normativas y proteger su entorno de trabajo híbrido y su infraestructura en la nube. El acceso de red Zero Trust (ZTNA) y la microsegmentación son las dos soluciones más importantes para aquellas empresas que se están pasando a una arquitectura Zero Trust. Con estos modelos, se reduce la superficie de ataque, se contienen las filtraciones, se controla más estrechamente el acceso y se mejora la experiencia del usuario.

El poder de la unificación

Akamai Guardicore Access combina la segmentación y el ZTNA, que se implementan con un único agente y se gestionan con una única consola. Este enfoque innovador garantiza una visibilidad completa desde el usuario hasta la carga de trabajo (norte-sur) y de terminal a terminal o carga de trabajo (este-oeste), lo que permite controlar el acceso a las aplicaciones en función de la identidad y segmentar los terminales a la vez. Al combinar estas tecnologías, las empresas se benefician de un marco de seguridad sólido que refuerza las defensas de la red, mitiga los riesgos y fomenta un entorno seguro y conforme a las normas.

Akamai Guardicore es la primera plataforma de seguridad que combina una microsegmentación líder en el sector y el ZTNA para ayudar a los equipos de seguridad a prevenir el ransomware, garantizar el cumplimiento de las normativas y proteger tanto al entorno de trabajo híbrido como a la infraestructura en la nube.

Por primera vez, las organizaciones pueden implementar la segmentación para minimizar su superficie de ataque y, al mismo tiempo, gestionar fácilmente el acceso a su entorno de trabajo híbrido desde cualquier lugar; y todo ello con un único agente que utiliza una misma consola en todo tipo de recursos e infraestructuras.

Funciones clave

Visibilidad integral
Comprenda a fondo su red gracias a la visibilidad integral, que se muestra tanto en el mapa como en los registros y que proporciona información sobre los patrones de acceso de los usuarios finales. Esto solo es posible gracias a la combinación de segmentación y ZTNA en un único producto. Conozca las vías de conexión, desde los terminales hasta las cargas de trabajo, incluido el nivel de proceso. Visibilidad histórica y casi en tiempo real para facilitar la realización de análisis forenses y acelerar la mitigación.

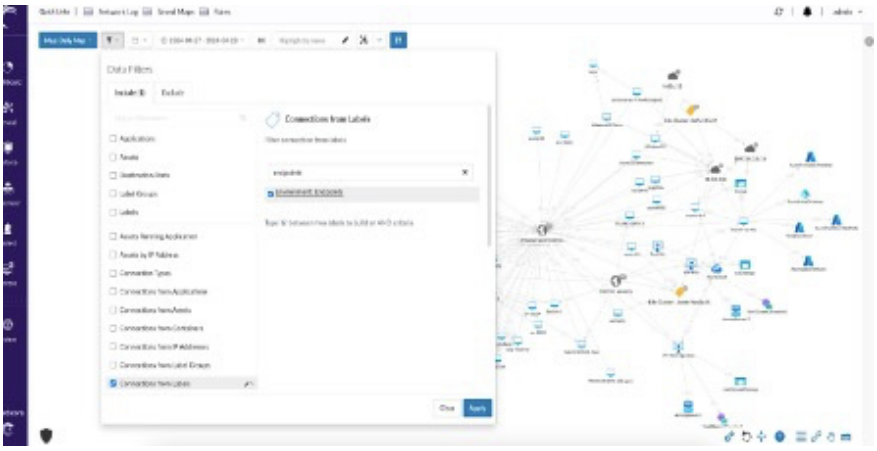
Ventajas para su empresa

Consola y agente únicos
Implemente la segmentación para minimizar la superficie de ataque al tiempo que gestiona fácilmente el acceso a un entorno de trabajo híbrido desde cualquier lugar, y todo ello con un solo agente que usa una única consola.

Amplia cobertura
Aplique controles de acceso en cualquier lugar y proteja al personal que trabaja a distancia y en la oficina.

Política unificada
Aplique las políticas para el tráfico este-oeste y el acceso norte-sur sin cambiar la sintaxis o las consolas. De este modo, dispondrá de la plataforma Zero Trust más sencilla y eficaz.

Detección de aplicaciones
Reduzca el tiempo de implementación de las políticas al identificar rápidamente las aplicaciones que necesitan permisos de acceso. Descubra sin esfuerzo sus aplicaciones privadas y obtenga información valiosa sobre sus patrones de uso, incluidos el acceso y la frecuencia de los usuarios.



Descubra fácilmente las aplicaciones para las que se requiere acceso

Sincronización de políticas de acceso y segmentación
Sincronice automáticamente los controles de acceso y las reglas de segmentación para reducir las dependencias entre equipos y eliminar el margen de error humano.

Casos de uso principales

Protección integral contra el ransomware: reduzca la probabilidad y el impacto del ransomware y otros ataques de malware con políticas basadas en identidades y de máquina a máquina. Asegúrese de que los terminales acceden a los recursos con el menor número de privilegios posible, al tiempo que se aplican controles de acceso granulares.

- Proteja los activos de alto valor: permita que los usuarios accedan a los activos esenciales con controles de acceso seguros y bloquee el tráfico VPN directo.
- Restrinja usuarios con privilegios: bloquee el tráfico VPN a los puertos de administración explotables para proporcionar un acceso seguro a los administradores.

Distribución del personal: permita que se trabaje desde cualquier lugar gracias a controles de acceso estrictos, que garantizan que cada dispositivo solo se conecte a los recursos que necesita. Esto minimiza la superficie de ataque y reduce el movimiento lateral dentro de la red.

Cumplimiento normativo: implemente políticas de segmentación de terminales para que las empresas puedan asegurarse de que sus terminales cumplen las normas y reglamentos pertinentes del sector, lo que reduce el riesgo de sanciones por incumplimiento y refuerza su estrategia general de seguridad.

Acceso de terceros: enrute y autentique el acceso de los contratistas y partners a través de un portal dedicado de Akamai para que puedan conectarse a aplicaciones específicas sin necesidad de instalar un agente.

Visite Seguridad Zero Trust de Akamai para obtener más información

| Publicado en octubre de 2024