

INFORMACIÓN SOBRE EL PRODUCTO DE AKAMAI

Secure Internet Access Enterprise, un firewall de DNS basado en la nube

A medida que las organizaciones adoptan el acceso directo a Internet, las aplicaciones de software como servicio (SaaS), los servicios en la nube, las políticas de teletrabajo y el Internet de las cosas (IoT), su superficie de ataque aumenta considerablemente y se enfrentan a multitud de nuevos desafíos de seguridad. La dificultad para proteger a los distintos departamentos y usuarios contra amenazas específicas avanzadas, como el malware, el ransomware, el phishing y las exfiltraciones de datos, ha aumentado de manera exponencial. Las complicaciones y complejidades que presentan los puntos de control de la seguridad, así como las lagunas en términos de protección que presentan las soluciones locales tradicionales, deben gestionarse con recursos limitados.

Akamai Secure Internet Access Enterprise es un firewall de sistema de nombres de dominio (DNS) basado en la nube que se ha diseñado para que los equipos de seguridad puedan garantizar a usuarios y dispositivos la posibilidad de conectarse a Internet de forma segura, estén donde estén, sin las complejidades y la sobrecarga de gestión asociadas a otras soluciones de seguridad heredadas. Secure Internet Access Enterprise utiliza una inteligencia ante amenazas en tiempo real basada en la información inigualable y a escala global que obtiene Akamai sobre el tráfico de Internet y de DNS.

Secure Internet Access Enterprise

Basado en la plataforma global Akamai Connected Cloud y en el servicio de DNS recursivo para operadores de Akamai, Secure Internet Access Enterprise es un firewall de DNS en la nube, rápido de configurar y fácil de implementar, que no requiere instalar ni mantener ningún hardware o software adicionales.

Secure Internet Access Enterprise aprovecha la inteligencia de seguridad en la nube de Akamai en tiempo real para identificar y bloquear de forma proactiva amenazas específicas, como el malware, el ransomware, el phishing y la exfiltración de datos basada en DNS de bajo rendimiento.

El portal de Akamai permite a los equipos de seguridad crear, implementar y aplicar de forma centralizada tanto políticas de seguridad unificadas como políticas de uso aceptable (PUA) en tan solo unos minutos para todos los usuarios, dondequiera que estén conectados a Internet.

VENTAJAS PARA SU EMPRESA



Traslado de la seguridad web a la nube con un firewall de DNS basado en la nube que se puede configurar y desplegar globalmente en cuestión de minutos (sin interrupciones para los usuarios) y escalar rápido.



Mejora de las defensas de seguridad mediante el bloqueo proactivo de las solicitudes a los sitios que difunden malware o ransomware, a los sitios de phishing, y a los servidores de mando y control (C2) de malware, e identificación de la exfiltración de datos vía DNS de bajo rendimiento gracias a una inteligencia ante amenazas única y actualizada.



Control del uso de TI en la sombra y aplicaciones no autorizadas mediante la identificación y el bloqueo de aplicaciones en función de su categoría o de una puntuación de riesgo.



Optimización del tiempo y la complejidad que implica la gestión de la seguridad, al reducir el número de alertas por falsos positivos, así como alertas de otras soluciones de protección, y administrando políticas de seguridad y actualizaciones desde cualquier lugar, en tan solo unos segundos, para proteger todas las sucursales.



Cómo funciona

Secure Internet Access Enterprise es un servicio de seguridad basado en la nube que se puede activar en cuestión de minutos para ofrecer seguridad y reducir la complejidad sin que el rendimiento se vea afectado. Esta protección puede ponerse en marcha sencillamente dirigiendo el tráfico de DNS recursivo a Secure Internet Access Enterprise mediante distintos métodos, como los túneles IPsec, un cliente ligero, el reenviador de DNS gestionado por Akamai o una modificación del agente de resolución de DNS existente.

Todos los dominios solicitados se cotejan con la información sobre amenazas en tiempo real de Akamai, y las solicitudes de dominios maliciosos identificados se bloquean automáticamente. El uso de DNS como capa de seguridad inicial bloquea de forma proactiva las amenazas en las primeras fases de intrusión y antes de establecer cualquier conexión web. Además, el DNS está diseñado para ser eficaz en todos los puertos y protocolos, con el fin de proteger frente al malware que no utilice puertos y protocolos web estándar. Los dominios también se pueden verificar para determinar el tipo de contenido al que un usuario está intentando acceder, y bloquearlo si ese contenido incumple la política de uso aceptable (PUA) de la organización.

Para reforzar la protección, los dominios de riesgo se pueden reenviar a un proxy en la nube para inspeccionar las URL. Esas URL HTTP y HTTPS solicitadas se comprueban con la inteligencia ante amenazas en tiempo real de Akamai, y las que resulten maliciosas se bloquean automáticamente.

Secure Internet Access Enterprise se integra fácilmente con otros productos de seguridad y herramientas de generación de informes, incluidos firewalls y soluciones de seguridad de la información y de gestión de eventos (SIEM), así como con fuentes de información sobre amenazas externas, lo que le permite optimizar la inversión en todas las capas de la pila de seguridad.

Además, la implantación del cliente ligero Secure Internet Access Enterprise en los dispositivos permite a las organizaciones proteger rápida y fácilmente los portátiles o los dispositivos móviles que se utilizan fuera de la red.

Akamai Cloud Security Intelligence

Secure Internet Access Enterprise, avalado por Cloud Security Intelligence de Akamai, proporciona información en tiempo real sobre las amenazas y los riesgos que estas pueden suponer para las empresas.

La inteligencia ante amenazas de Akamai está diseñada para proteger contra los riesgos actuales o relevantes que puedan afectar a su empresa y para minimizar el número de alertas por falsos positivos que deben investigar los equipos de seguridad.

Esta inteligencia se basa en los datos recopilados ininterrumpidamente por Akamai Connected Cloud, que puede llegar a gestionar hasta un 30 % del tráfico web mundial y distribuye hasta 11 billones de consultas de DNS diarias. La inteligencia de Akamai se complementa con cientos de fuentes de información externas sobre amenazas, y el resultado de dicha combinación se analiza y se mantiene continuamente utilizando técnicas de análisis de comportamiento avanzadas, aprendizaje automático y algoritmos propios. Conforme se van identificando nuevas amenazas, se van agregando a los servicios de Secure Internet Access Enterprise, con el fin de ofrecer protección en tiempo real.

Akamai Connected Cloud

El servicio Secure Internet Access Enterprise se basa en Akamai Connected Cloud, la plataforma más distribuida del mundo para cloud computing, seguridad y entrega de contenido. Akamai Connected Cloud ofrece un acuerdo de nivel de servicio (SLA) del 100 % de disponibilidad y garantiza una fiabilidad óptima para la seguridad web de una empresa.

VENTAJAS PARA SU EMPRESA



Reducción de los riesgos y mejora de la seguridad en los dispositivos utilizados fuera de la red, sin necesidad de una VPN, gracias al cliente ligero Secure Internet Access Enterprise, que refuerza las políticas de seguridad y las PUA.



Garantía de conformidad y aplicación de las PUA de forma rápida y uniforme al bloquear el acceso a dominios cuestionables o inapropiados y a categorías de contenido.



Aumento de la resiliencia y la fiabilidad con Akamai Connected Cloud y la plataforma de DNS para operadores de Akamai.

Portal de gestión basado en la nube

Las tareas de configuración y la gestión continua de Secure Internet Access Enterprise se llevan a cabo a través del portal en la nube de Akamai Control Center, lo que posibilita la gestión en todo momento y desde cualquier lugar.

La gestión de políticas es fácil y rápida, y los cambios se pueden enviar de manera global en solo unos minutos para garantizar la protección de sus usuarios y sucursales. Se pueden configurar notificaciones por correo electrónico en tiempo real, así como informes programados, para notificar a los equipos de seguridad los eventos críticos relativos a las políticas, lo que permite una intervención inmediata a fin de identificar y abortar las amenazas potenciales. Un panel en tiempo real proporciona una descripción general del tráfico, las amenazas y los eventos en torno a la política de uso aceptable. Se puede ver información detallada de cualquier actividad a través de un desglose de los elementos en un panel individual. Esta información detallada proporciona un valioso recurso para el análisis y la corrección de los incidentes de seguridad.

A todas las funciones del portal, se puede acceder a través de las API, y los registros de datos se pueden exportar a SIEM, lo que permite que Secure Internet Access Enterprise se integre de manera sencilla y eficaz con sus otras soluciones de seguridad y generación de informes.

Características

Seguridad
Bloqueo de los dominios y URL de distribución de malware, ransomware y phishing
Bloqueo de solicitudes de malware C2
Identificación de la exfiltración de datos basada en DNS
Inspección de dominios proxy peligrosos en las solicitudes de URL HTTP y HTTPS
Creación de una lista personalizada de dominios para la inspección de direcciones URL HTTP y HTTPS
Análisis retrospectivo de los registros de tráfico del cliente para identificar y alertar sobre amenazas recién descubiertas
Creación de listas personalizadas de autorización/exclusión
Incorporación de nuevos datos de inteligencia de amenazas
Personalización de páginas de error
Consulta de la base de datos sobre amenazas de Akamai para lograr información sobre las URL y los dominios maliciosos
Refuerzo de la seguridad para dispositivos fuera de la red (Windows, macOS, iOS, Android, Chrome)
Política de uso aceptable (PUA)
Creación de políticas PUA basadas en grupos
Supervisión o bloqueo de infracciones de la PUA para usuarios dentro y fuera de la red
Ejecución de SafeSearch en Google, Bing y YouTube

Agente seguro de acceso a la nube (en línea)
Identificación y bloqueo de las aplicaciones de TI en la sombra
Bloqueo de aplicaciones en función de la puntuación de riesgo o el grupo de las aplicaciones
Aplicación de inquilinos SaaS
Informes, supervisión y administración
Integración de IDP y Active Directory
Visibilidad de toda la actividad de la empresa con paneles personalizables
Análisis detallado de todos los eventos asociados a amenazas y a la PUA
Visibilidad y registro completos de las solicitudes de tráfico recibidas y los eventos relacionados con las amenazas y la PUA
Entrega de todos los registros, que se conservan durante 30 días y se pueden exportar a través de una API
Configuración, listas de seguridad personalizadas y eventos disponibles a través de una API
Integración con otros sistemas de seguridad, como SIEM, a través de una API
Alertas de seguridad en tiempo real por correo electrónico
Informes por correo electrónico diarios o semanales programados
Administración delegada
Plataforma Akamai Connected Cloud
Direcciones VIP IPv4 e IPv6 exclusivas de cada cliente para DNS recursivo
Acuerdo de nivel de servicio (SLA) que garantiza una disponibilidad del 100 %
Enrutamiento de solicitudes de DNS con Anycast para un rendimiento óptimo
DNSSEC, DoH y DoT para mayor seguridad
Atribución de dispositivos empresariales
Atribución en línea mediante un agente de transporte de DNS
Atribución offline mediante Security Connector
Atribución basada en cliente para portátiles y dispositivos móviles (Windows, macOS, iOS, Android, Chrome)

Para obtener más información sobre Secure Internet Access Enterprise y solicitar una prueba gratuita, visite akamai.com.