Enterprise Threat Protector

Protección avanzada ante amenazas en la nube

A medida que las empresas adoptan el acceso directo a Internet (DIA), las aplicaciones de software como servicio (SaaS), los servicios en la nube, la movilidad y el Internet de las cosas (IoT), su superficie de ataque aumenta drásticamente y se enfrentan a multitud de nuevos desafíos en materia 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 soluciones locales tradicionales requieren una gestión de las complicaciones y las dificultades relativas al punto de control de seguridad, así como de las brechas de seguridad, con recursos limitados.

Enterprise Threat Protector es una puerta de enlace web segura (SWG) basada en la nube que se ha diseñado para que los equipos de seguridad puedan garantizar que los usuarios y los dispositivos pueden conectarse a Internet de forma segura, estén donde estén, sin las complejidades y la sobrecarga de gestión asociadas a otras soluciones de seguridad heredadas. Enterprise Threat Protector se basa en la inteligencia de amenazas en tiempo real, apoyada en la información inigualable y a escala global que obtiene Akamai sobre el tráfico de Internet y el sistema de nombres de dominio (DNS), y en varios motores de detección de malware.

Enterprise Threat Protector

Integrada en Akamai Intelligent Edge Platform y en el servicio DNS recursivo para operadores de Akamai, Enterprise Threat Protector es una plataforma SWG rápida de configurar y fácil de implementar que no requiere la instalación ni el mantenimiento de ningún hardware o software adicionales.

Enterprise Threat Protector cuenta con una serie de capas de protección que utilizan, en tiempo real, la información recopilada por Akamai Cloud Security Intelligence, así como varios motores estáticos y dinámicos de detección de malware, para identificar y bloquear proactivamente amenazas específicas, como el malware, el ransomware, el phishing y las exfiltraciones de datos de DNS. El portal de Akamai permite a los equipos de seguridad crear, implementar y aplicar de forma centralizada tanto políticas de seguridad unificadas como las políticas de uso aceptable (PUA) en tan solo unos minutos para todos los empleados, dondequiera que estén conectados a Internet.

Funcionamiento

Enterprise Threat Protector cuenta con varias capas de protección (DNS, URL y análisis de carga), lo que le permite garantizar la seguridad y reducir la complejidad, todo ello sin perjudicar el rendimiento. Para poder ofrecer esta protección solo hay que dirigir el tráfico web a Enterprise Threat Protector mediante un cliente ligero, o bien reenviar el tráfico web desde otro proxy web a través de cadenas de proxies.

Enterprise Threat Protector

Protección avanzada ante amenazas en la nube

Inspección de DNS: 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 comprobar para determinar el tipo de contenido al que un usuario está intentando acceder, y bloquearlo si dicho contenido incumple la política de uso aceptable (PUA) de la empresa.

Inspección de URL: las URL HTTP y HTTPS solicitadas se cotejan con la información sobre amenazas en tiempo real de Akamai, y las URL maliciosas se bloquean automáticamente.

Análisis de carga: las cargas HTTP/S se analizan en línea u offline mediante varios motores de detección de malware avanzado. Estos motores utilizan una gran variedad de técnicas (como la detección de malware con y sin firma, el aprendizaje automático y los entornos de pruebas), que ofrecen una protección completa de día cero frente a archivos potencialmente maliciosos, como archivos ejecutables y documentos. Este análisis también protege contra el malware que se incrusta directamente en la página web solicitada, como un JavaScript malicioso que esté oculto o las páginas de phishing de día cero.

Ventajas para la empresa

- **Traslado de la seguridad web a la nube** con una puerta de enlace web segura basada 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 la exfiltración de datos de DNS y las solicitudes a los sitios que difunden malware o ransomware, a los sitios de phishing, a los servidores de mando y control (C2) de malware, gracias a una inteligencia ante amenazas única y actualizada.
- **Bloqueo de cargas maliciosas para una mejor protección de día cero,** mediante el análisis de los archivos y contenido web solicitados, con el fin de detener la amenaza antes de que alcance a los dispositivos de punto final y comprometa su seguridad.
- **Optimización del tiempo y la complejidad que implica la gestión de la seguridad,** reduciendo el número de alertas de seguridad de falsos positivos, así como alertas de otros productos de seguridad, y administrando políticas de seguridad y actualizaciones desde cualquier lugar en tan solo unos segundos para proteger todas las sucursales.
- **Simplificación de la seguridad del acceso directo a Internet (DIA),** al eliminar la necesidad de dispositivos de seguridad para sucursales.
- **Reducción de los riesgos y mejora de la seguridad en los portátiles utilizados fuera de la red, sin necesidad de una VPN,** gracias al conector ligero Enterprise Client Connector, 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 Intelligent Edge Platform.

Enterprise Threat Protector se integra fácilmente con otros productos de seguridad y herramientas de generación de informes, incluidos firewall y 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 de su empresa.

Además, con la implementación del conector de seguridad ligero Enterprise Client Connector en los portátiles gestionados, las empresas pueden añadir rápidamente una capa adicional de seguridad proactiva cuando los utilizan fuera de la red.

Enterprise Threat Protector
Protección avanzada ante amenazas en la nube

Akamai Cloud Security Intelligence

Enterprise Threat Protector, 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 contra 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 los equipos de seguridad deben investigar.

Esta inteligencia se basa en los datos recopilados ininterrumpidamente por Akamai Intelligent Edge Platform, que puede llegar a gestionar hasta un 30 % del tráfico web mundial y distribuye hasta 2,2 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 Enterprise Threat Protector, lo que supone protección en tiempo real.

Akamai Intelligent Edge Platform

El servicio Enterprise Threat Protector se incluye en Akamai Intelligent Edge Platform, una plataforma rápida, inteligente y segura. La plataforma, distribuida de forma global, ofrece un acuerdo de nivel de servicio (SLA) del 100 % de disponibilidad y garantiza una fiabilidad óptima para la seguridad web de una empresa.

Portal de gestión basado en la nube

Las tareas de configuración y la gestión continua de Enterprise Threat Protector 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 de los eventos críticos relativos a las políticas, lo que permite una intervención inmediata a fin de identificar y abortar rápidamente 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 Enterprise Threat Protector se integre de manera sencilla y eficaz con sus otras soluciones de seguridad y generación de informes.

Enterprise Threat Protector

Protección avanzada ante amenazas en la nube

Funciones clave

- **Amenazas clasificadas por Akamai:** la información sobre amenazas, actualizada minuto a minuto gracias a una visibilidad en la red de Akamai de entre el 15 % y el 30 % de todo el tráfico web diario, se combina con 2,2 billones de solicitudes de DNS diarias a su nube de DNS recursivo.
- **Amenazas clasificadas por el cliente:** los equipos de seguridad pueden integrar rápidamente sus fuentes de información sobre amenazas existentes, aumentando el valor de sus inversiones en seguridad actuales.
- **Políticas de uso aceptable:** aplique las PUA de la empresa y garantice el cumplimiento mediante la limitación de las categorías de contenido a las que se puede o no se puede acceder.
- **DNSSEC:** todas las solicitudes de DNS que se envían a Enterprise Threat Protector tienen habilitado DNSSEC.
- **Análisis de carga en línea y offline:** cuatro motores de detección de malware avanzado identifican y bloquean las amenazas avanzadas y complejas, y mejoran la protección de día cero.
- **Análisis e informes:** los paneles proporcionan información en tiempo real sobre todo el tráfico web de salida de la empresa, así como de los eventos asociados a las amenazas y a las políticas de uso aceptable.
- **Información sobre seguridad:** entienda rápidamente por qué Akamai ha añadido un dominio o una URL a sus listas de inteligencia ante amenazas.
- **Registro:** los registros de tráfico se conservan durante 30 días y se pueden exportar fácilmente en formato de archivo .CSV o integrarse en un sistema SIEM para un ulterior análisis.

El ecosistema de Akamai

Akamai Intelligent Edge Platform llega a todas partes, desde la empresa a la nube, para garantizar a nuestros clientes y a sus negocios la máxima eficacia, rapidez y seguridad. Nuestras completas soluciones se gestionan a través de la herramienta unificada y personalizable Akamai Control Center para ofrecerle una mejor visibilidad y un mayor control. Además, cuenta con el soporte de los expertos de servicios profesionales de Akamai, que le ayudarán a ponerse en marcha con facilidad y a impulsar la innovación a medida que sus estrategias evolucionen.

Para obtener más información sobre Enterprise Threat Protector y obtener una prueba GRATUITA, visite akamai.com/etp.

Enterprise Threat Protector

Protección avanzada ante amenazas en la nube

Security	Guest Wi-Fi	Intelligence	Advanced Threat
Bloqueo de los dominios de distribución y URL de malware, ransomware y phishing		✓	✓
Bloqueo de solicitudes de mando y control (C2) de malware		✓	✓
Identificación de la exfiltración de datos basada en DNS		✓	✓
Inspección de dominios proxy peligrosos en las solicitudes de URL HTTP y HTTPS		✓	✓
Filtrado mediante proxy de todo el tráfico web para DNS, URL y análisis de carga			✓
Análisis en línea y offline de cargas HTTP y HTTPS mediante varios motores de análisis y detección de malware*			✓
Entorno de pruebas en la nube para el análisis dinámico de cargas offline			✓
Análisis en línea y en tiempo real de páginas web para la detección de páginas de phishing de día cero*			✓
Análisis en línea u offline, en tiempo real, de archivos descargados desde sitios de intercambio de archivos			✓
Creación de una lista personalizada de dominios para la inspección de direcciones URL HTTP y HTTPS		✓	✓
Creación de una lista personalizada de dominios para el análisis de carga en línea u offline			✓
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		✓	✓
Páginas de error personalizables	✓	✓	✓
Consulta de la base de datos sobre amenazas de Akamai para lograr información sobre las URL y los dominios maliciosos		✓	✓
Seguridad reforzada para portátiles fuera de la red (Windows y macOS)		✓	✓
Acceptable Use Policy (AUP)	**Guest Wi-Fi**	**Intelligence**	**Advanced Threat**
Creación de políticas PUA basadas en grupos			✓
Supervisión o bloqueo de infracciones de la PUA para usuarios dentro y fuera de la red	✓[1]	✓	✓
Ejecución de SafeSearch en Google, Bing y YouTube	✓	✓	✓

Enterprise Threat Protector

Protección avanzada ante amenazas en la nube

Reporting, Monitoring and Administration	Guest Wi-Fi	Intelligence	Advanced Threat
Integración de IDP y Active Directory			✓
Visibilidad de toda la actividad de la empresa con paneles personalizables	✓ [2]	✓	✓
Análisis detallado de todos los eventos asociados a amenazas y a la PUA	✓ [2]	✓	✓
Visibilidad y registro completos de las solicitudes de tráfico recibidas y los eventos relacionados con las amenazas y la PUA	✓ [2]	✓	✓
Entrega de todos los registros, que se conservan durante 30 días y se pueden exportar a través de una API	✓ [2]	✓	✓
Configuración, listas de seguridad personalizadas y eventos disponibles a través de una API abierta	✓ [2]	✓	✓
Integración con otros sistemas de seguridad, como SIEM, a través de una API abierta	✓	✓	✓
Alertas de seguridad y PUA en tiempo real por correo electrónico	✓ [2]	✓	✓
Programación de informes de correo electrónico diarios o semanales	✓	✓	✓
Administración delegada	✓	✓	✓
Akamai Intelligent Edge Platform	**Guest Wi-Fi**	**Intelligence**	**Advanced Threat**
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	✓	✓	✓
Aplicación de DNSSEC para mayor seguridad	✓	✓	✓
Enterprise Connectors	**Guest Wi-Fi**	**Intelligence**	**Advanced Threat**
Enterprise Client Connector para proteger los portátiles fuera de la red (Windows y OS X) e informar del nombre de la máquina para eventos fuera y dentro de la red		✓	✓
Actualización automática de Enterprise Client Connector		✓	✓
Enterprise Security Connector para identificar las direcciones IP y los nombres de máquina de los dispositivos de punto final		✓	✓

* El entorno de pruebas en la nube es un complemento opcional y es necesario para el análisis offline de archivos grandes.

1) ETP Guest Wi-Fi no incluye la aplicación de la PUA fuera de la red.

2) ETP Guest Wi-Fi no incluye ningún tipo de control de seguridad, por lo que las alertas, los análisis, los paneles y los registros solo incluyen las actividades y eventos de la PUA.

Akamai garantiza experiencias digitales seguras a las empresas más importantes del mundo. La plataforma inteligente de Akamai en el Edge llega a todas partes, desde la empresa a la nube, para garantizar a nuestros clientes y a sus negocios la máxima eficacia, rapidez y seguridad. Las mejores marcas del mundo confían en Akamai para lograr su ventaja competitiva gracias a soluciones ágiles que permiten destapar todo el potencial de sus arquitecturas multinube. En Akamai mantenemos las decisiones, las aplicaciones y las experiencias más cerca de los usuarios que nadie; y los ataques y las amenazas, a raya. La cartera de soluciones de seguridad en el Edge, rendimiento web y móvil, acceso empresarial y distribución de vídeo de Akamai está respaldada por un servicio de atención al cliente y análisis excepcional, y por una supervisión ininterrumpida, durante todo el año. Para descubrir por qué las marcas más importantes del mundo confían en Akamai, visite www.akamai.com y blogs.akamai.com, o siga a @Akamai en Twitter. Puede encontrar los datos de contacto de todas nuestras oficinas en www.akamai.com/locations. Publicado en marzo de 2020.