ENTERPRISE THREAT PROTECTOR

Protección avanzada ante amenazas en la nube

A medida que las empresas adoptan el acceso directo a Internet (DIA), las aplicaciones 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. La dificultad para proteger a las organizaciones y a los usuarios contra amenazas específicas avanzadas, como el malware, el phishing y las exfiltraciones de datos, ha aumentado de manera exponencial. Las soluciones tradicionales requieren una gestión de las complicaciones y las dificultades relativas al punto de control de seguridad, así como de las brechas de seguridad. Enterprise Threat Protector de Akamai (ETP) es una puerta de enlace de Internet segura (SIG) que permite a los equipos de seguridad garantizar que los usuarios y los dispositivos puedan conectarse a Internet de forma segura, estén donde estén, sin las complejidades asociadas a otras soluciones de seguridad heredadas. Enterprise Threat Protector se basa en la inteligencia de amenazas en tiempo real, apoyada en la información sin precedentes y a escala global que obtiene Akamai sobre el tráfico de Internet y el sistema de nombres de dominio (DNS).

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 SIG rápida de configurar y fácil de implementar que no requiere la instalación ni el mantenimiento de ningún hardware o software adicionales.

Enterprise Threat Protector aprovecha, en tiempo real, la información recopilada por Akamai Cloud Security Intelligence y la plataforma distribuida por todo el mundo y probada de Akamai 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.

CÓMO FUNCIONA

Enterprise Threat Protector emplea varias capas de protección (DNS, URL y análisis de carga en línea), lo que le permite proporcionar una seguridad óptima y reducir la complejidad, todo ello sin perjudicar el rendimiento.

Inspección de DNS: gracias al simple hecho de dirigir el tráfico de DNS recursivo externo a Enterprise Threat Protector, todos los dominios solicitados se cotejan con la información en tiempo real de Akamai relativa al riesgo de los dominios. Los usuarios quedan bloqueados de forma proactiva para que no accedan a dominios y servicios maliciosos, y las solicitudes se redirigen a servicios y dominios seguros. Dado que esta validación tiene lugar antes de que se establezca la conexión IP, las amenazas se detienen en las primeras fases de la intrusión. Además, el DNS es 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: los dominios que se consideran peligrosos, según la inteligencia ante amenazas de Akamai, se reenvían automáticamente a un proxy en la nube de Akamai Intelligent Edge Platform. La URL solicitada se coteja con la inteligencia ante amenazas de URL de Akamai, y las URL maliciosas se bloquean automáticamente. El proxy inspecciona URL tanto HTTP como HTTPS.

Análisis de carga en línea: las cargas HTTP y HTTPS de los dominios peligrosos se analizan, en tiempo real, con varios motores de detección de malware avanzado. Estos motores utilizan una gran variedad de técnicas (como la detección de malware con y sin firma y el aprendizaje automático), que ofrecen una protección completa de día cero frente a archivos potencialmente maliciosos, como archivos ejecutables y documentos, además de otros tipos de malware que se incrustan directamente en la página web solicitada, como un JavaScript malicioso que esté oculto.

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.

BENEFICIOS PARA EL NEGOCIO

- **Mejora de las defensas de seguridad** mediante el bloqueo proactivo de las solicitudes a los sitios que difunden malware o ransomware, a los servidores de mando y control (CnC) de malware y a los dominios y URL de exfiltración de datos de DNS y de phishing, gracias a una inteligencia ante amenazas única y actualizada.
- **Bloqueo de cargas maliciosas para una mejor protección de día cero,** mediante el análisis, en tiempo real, 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.
- **Mejora del rendimiento de DIA,** filtrándose únicamente el tráfico sospechoso para la inspección de URL y el análisis de carga.
- **Incorporación instantánea de protección, sin complicaciones ni hardware,** con una solución basada al 100 % en la nube que se puede configurar e implementar globalmente en cuestión de minutos (sin ninguna interrupción para los usuarios) y escalar rápidamente.
- **Reducción de los riesgos y mejora de la seguridad en los portátiles utilizados fuera de la red, sin necesidad de una VPN,** con el conector ligero Enterprise Client Connector, que refuerza las políticas de seguridad y las PUA.
- **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.
- **Garantía de conformidad y aplicación de la 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 del DNS** con Akamai Intelligent Edge Platform.

ENTERPRISE THREAT PROTECTOR

AKAMAI CLOUD SECURITY INTELLIGENCE (CSI)

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

La inteligencia contra amenazas de Akamai está diseñada para proporcionar protección contra las amenazas actuales y pertinentes que podrían afectar a su empresa y para minimizar el número de alertas de falsos positivos que sus equipos de seguridad tienen que 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 un gran número de datos externos 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, plataforma segura, fiable y rápida. La plataforma, distribuida de forma global, ofrece un acuerdo de nivel de servicio del 100 % de disponibilidad y garantiza una fiabilidad óptima para un servicio DNS recursivo de una empresa.

PORTAL DE GESTIÓN BASADO EN LA NUBE

Todas las tareas de configuración, y la gestión continua, de Enterprise Threat Protector se llevan a cabo a través del portal Luna en la nube de Akamai, posibilitando 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.

FUNCIONES CLAVE

- **Amenazas clasificadas por Akamai:** la información sobre amenazas, actualizada minuto a minuto gracias a una visibilidad del 15-30 % del tráfico web diario en la red de Akamai, 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.
- **Análisis en tiempo real de la carga en línea:** tres motores de detección de malware avanzado identifican y bloquean las amenazas avanzadas y complejas, y mejoran la protección de día cero.
- **Políticas de uso aceptable:** aplique las políticas de uso aceptable 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.
- **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 SIEM para un ulterior análisis.
- **DNSSEC:** todas las solicitudes de DNS que se envían a Enterprise Threat Protector tienen habilitado DNSSEC.

EL ECOSISTEMA DE AKAMAI

Akamai Intelligent Edge Platform llega a todas partes, desde la empresa a la nube, lo que permite a nuestros clientes y a sus negocios ser rápidos, inteligentes y seguros. Nuestras completas soluciones se gestionan a través de la herramienta unificada y personalizable Luna 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 saber más sobre Enterprise Threat Protector y obtener una prueba gratuita, visite akamai.com/etp.

Akamai

ENTERPRISE THREAT PROTECTOR

SEGURIDAD	Guest Wi-Fi	Intelligence	Advanced Threat
Bloqueo de los dominios de distribución de malware, ransomware y phishing		X	X
Bloqueo de solicitudes de malware de mando y control (CnC)		X	X
Identificación de la exfiltración de datos basada en DNS		X	X
Inspección de dominios proxy peligrosos en las solicitudes de URL HTTP y HTTPS		X	X
Análisis en línea y en tiempo real de cargas HTTP y HTTPS peligrosas mediante varios motores de análisis y detección de malware en línea			X
Análisis en línea y en tiempo real de archivos descargados desde sitios de intercambio de archivos			X
Creación de una lista personalizada de dominios para la inspección de direcciones URL HTTP y HTTPS		X	X
Creación de una lista personalizada de dominios para el análisis de carga en línea			X
Análisis retrospectivo de los registros de tráfico del cliente para identificar y alertar sobre amenazas recién descubiertas		X	X
Creación de listas personalizadas de autorización/exclusión		X	X
Incorporación de nuevos datos de inteligencia de amenazas		X	X
Páginas de error personalizables	X	X	X
Consulta de la base de datos sobre amenazas de Akamai para lograr información sobre las URL y los dominios maliciosos		X	X
Seguridad reforzada para portátiles fuera de la red (Windows y macOS)		X	X
POLÍTICA DE USO ACEPTABLE (PUA)	**Guest Wi-Fi**	**Intelligence**	**Advanced Threat**
Supervisión o bloqueo de infracciones de la PUA para usuarios dentro y fuera de la red	X[1]	X	X
Ejecución de SafeSearch en Google, Bing y YouTube	X	X	X
ELABORACIÓN DE INFORMES, SUPERVISIÓN Y ADMINISTRACIÓN	**Guest Wi-Fi**	**Intelligence**	**Advanced Threat**
Visibilidad de toda la actividad de la empresa con paneles personalizables	X[2]	X	X
Análisis detallado de todos los eventos asociados a amenazas y a la PUA	X[2]	X	X
Visibilidad y registro completos de las solicitudes de tráfico recibidas y los eventos relacionados con las amenazas y la PUA	X[2]	X	X
Entrega de todos los registros, que se conservan durante 30 días y se pueden exportar a través de una API	X[2]	X	X
Configuración, listas de seguridad personalizadas y eventos disponibles a través de una API abierta	X[2]	X	X
Integración con otros sistemas de seguridad, como SIEM, a través de una API abierta	X	X	X
Alertas de seguridad y PUA en tiempo real por correo electrónico	X[2]	X	X
Programación de informes de correo electrónico diarios o semanales	X	X	X
Administración delegada	X	X	X
AKAMAI INTELLIGENT EDGE PLATFORM™	**Guest Wi-Fi**	**Intelligence**	**Advanced Threat**
Direcciones VIP IPv4 e IPv6 exclusivas de cada cliente para DNS recursivo	X	X	X
Acuerdo de nivel de servicio (SLA) que garantiza una disponibilidad del 100 %	X	X	X
Enrutamiento de solicitudes de DNS con Anycast para un rendimiento óptimo	X	X	X
Aplicación de DNSSEC para mayor seguridad	X	X	X
CONECTORES DE ENTERPRISE	**Guest Wi-Fi**	**Intelligence**	**Advanced Threat**
Enterprise Client Connector para proteger los portátiles fuera de la red (Windows y OSX) e informar del nombre de la máquina para eventos fuera y dentro de la red		X	X
Actualización automática de Enterprise Client Connector		X	X
Enterprise Security Connector para identificar las direcciones IP y los nombres de máquina de los dispositivos de punto final		X	X

1. La red Wi-Fi de invitados de ETP no incluye la aplicación de la PUA fuera de la red.
2. La red Wi-Fi de invitados de ETP 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.