Guía rápida de Cisco Umbrella.

En el pasado, los equipos de escritorio, las aplicaciones empresariales y la infraestructura crítica se encontraba detrás del firewall. En la actualidad, cada vez más cosas suceden fuera de la red. Más usuarios itinerantes. Más ordenadores portátiles corporativos que acceden a Internet desde otras redes. Más aplicaciones en la nube, lo que significa que los usuarios no tienen que estar en la red corporativa para hacer su trabajo. Y más sucursales que se conectan directamente a Internet.

Para el año 2021, Gartner predice que la empresa media tendrá un 25 % de su tráfico de datos corporativo más allá del perímetro de la red. Cuando un usuario está fuera de la red, es más vulnerable y la organización no tiene visibilidad y protección. Si solo confía en la seguridad del perímetro no está completamente protegido. Estas brechas abren la puerta para el malware, ransomware y otros ataques.

La primera línea de defensa

Como gateway de Internet seguro, Cisco Umbrella ofrece el primer nivel de defensa frente a las amenazas que llegan de Internet allá donde vayan los usuarios. Umbrella ofrece una visibilidad completa de la actividad de Internet en todas las ubicaciones, dispositivos y usuarios y bloquea las amenazas antes de que lleguen a la red o a los terminales. Como plataforma abierta a través de la nube, Umbrella se integra fácilmente con su stack de seguridad existente y ofrece inteligencia de amenazas en vivo sobre amenazas actuales y emergentes.

Mediante el análisis y el aprendizaje de los patrones de la actividad de Internet, Umbrella descubre automáticamente la infraestructura de los atacantes dispuesta para los ataques y bloquea de forma proactiva las solicitudes a destinos maliciosos antes incluso de que se establezca una conexión sin añadir latencia para los usuarios.

Con Umbrella podrá detener el phishing y las infecciones de malware mucho antes, identificar de una manera más rápida los dispositivos que ya están infectados y evitar la exfiltración de datos.

Cumplimiento integrado en la esencia de Internet

El sistema de nombres de dominio (DNS) es un componente básico de internet, la asignación de nombres de dominio a las direcciones IP. Cuando hace clic en un enlace o escribe una URL, una solicitud DNS inicia el proceso de conectar cualquier dispositivo a Internet. Umbrella utiliza DNS como uno de los mecanismos principales para dirigir el tráfico a nuestra plataforma en la nube y lo utiliza también para reforzar la seguridad.

Cuando Umbrella recibe una solicitud DNS, utiliza la inteligencia para determinar si la solicitud es segura, maliciosa o arriesgada, lo que significa que el dominio contiene contenido malicioso y legítimo. Las solicitudes seguras y maliciosas se enrutan como de costumbre o se bloquean, respectivamente. Las solicitudes arriesgadas se enrutan a nuestro proxy basado en la nube para una inspección más exhaustiva.

El proxy de Umbrella utiliza la reputación web de Cisco Talos y otras fuentes de terceros para determinar si una URL es maliciosa. Nuestro proxy también inspecciona archivos que se intentan descargar de dichos sitios arriesgados utilizando motores de antivirus (AV) y Protección frente a malware avanzado de Cisco (AMP). Y, según los resultados de esta inspección, la conexión se permite o se bloquea.

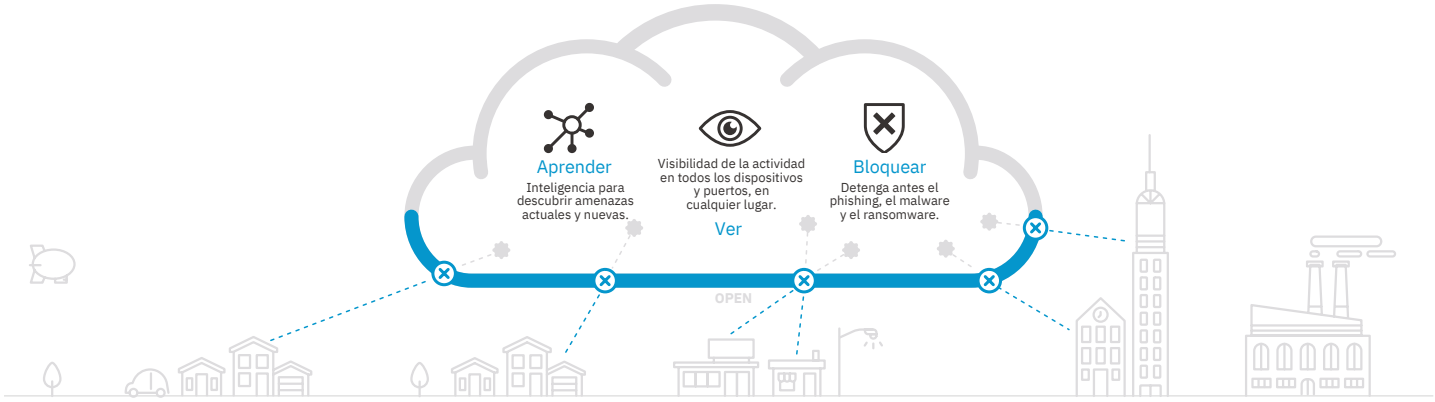
Ventajas

Mitigar los costes de remediación y daños de las brechas: como Cisco Umbrella es la primera línea de defensa, los equipos de seguridad tendrán menos infecciones de malware que remediar y se detendrán las amenazas antes de que puedan causar daños.

Reducir el tiempo necesario para detectar y contener las amenazas: Cisco Umbrella contiene las llamadas de comando y control por cualquier puerto o protocolo y proporciona informes en tiempo real de la actividad.

Aumentar la visibilidad de la actividad de Internet en todas las ubicaciones y usuarios: Cisco Umbrella proporciona una visibilidad vital para la respuesta a incidentes y también le ofrece la confianza que lo verá todo.

Identificar las aplicaciones en la nube utilizadas en toda la empresa: Cisco Umbrella proporciona visibilidad de los servicios en la nube autorizados y no autorizados en uso en toda la empresa, por lo que puede descubrir nuevos servicios que se utilizan, ver quién los está utilizando e identificar posibles riesgos.



cisco Partner

Brotek.

Inteligencia para detener los ataques antes de que se inicien

La red global de Umbrella, que es la red que en que se basa nuestro servicio de DNS recursivo, resuelve miles de millones de solicitudes de Internet de millones de usuarios de todo el mundo cada día. Analizamos esta enorme cantidad de datos para detectar patrones y descubrir la infraestructura del atacante.

Introducimos todos esos datos de la actividad en Internet de nuestra red global en tiempo real en nuestra base de datos gráfica masiva y, a continuación, ejecutamos continuamente modelos estadísticos y de machine learning en ellos.
Esta información es también constantemente analizada por los investigadores de seguridad de Umbrella y se complementa con inteligencia de Cisco Talos. Utilizando esta combinación de inteligencia humana y machine learning identificamos sitios maliciosos, ya sea dominios, direcciones IP o URL, todo ello a través de Internet.

Características clave

- Visibilidad y protección en cualquier lugar
- Inteligencia para detectar los ataques antes
- Implementación y gestión sencillas
- Plataforma abierta para la integración
- Infraestructura de nube rápida y fiable

Funciona perfectamente con otros

Umbrella se integra con su stack de seguridad existente, incluidos los dispositivos de seguridad, plataformas de inteligencia y controles de agente de seguridad de acceso a la nube (CASB). Umbrella puede transferir los datos del registro sobre la actividad en Internet a sus sistemas de gestión de logs o SIEM y, mediante nuestra API de cumplimiento, puede enviar de forma programática los dominios maliciosos a Umbrella para su bloqueo. Esto le permite aumentar las inversiones existentes y ampliar fácilmente la protección a todas partes.

Implementación en toda la empresa en minutos

Umbrella es la forma más rápida y sencilla de proteger a todos sus usuarios en cuestión de minutos. Debido a que se entrega desde la nube, no hay hardware que instalar ni software que actualizar manualmente. Se pueden aprovisionar todos los dispositivos en red, incluidos los dispositivos BYOD e IoT, en unos minutos y utilizar su presencia de Cisco existente, AnyConnect, router de servicios integrados (ISR) serie 1K y 4K, y los controladores LAN inalámbricos 5520 y 8540, para aprovisionar rápidamente miles de equipos externos a la red y portátiles en itinerancia. Además, con la aplicación Cisco Security Connector, puede utilizar la extensión de Umbrella para proteger dispositivos supervisados con iOS 11.

Números clave

- 125. 000 millones de solicitudes de Internet diarias
- 90 millones de usuarios
- 27 datacenters en todo el mundo
- Más de 7 millones de destinos maliciosos reforzados simultáneamente en la capa DNS

Siguientes pasos

Hable con un representante de ventas o partner de Cisco sobre cómo Cisco Umbrella puede ayudar a proteger su organización móvil conectada a la nube de amenazas avanzadas. Visite signup.umbrella.com para obtener una prueba gratuita durante 14 días de Umbrella. Si su organización tiene más de 1000 usuarios, es apta para Umbrella Security Report, que proporciona un análisis detallado después de la prueba.