

Seguridad para terminales

AMP para terminales + Umbrella

AMP y Umbrella funcionan de forma coordinada para proporcionar visibilidad, contexto y control con el fin de prevenir, detectar y responder a los ataques dirigidos a los terminales antes de que se produzcan daños.

“Gracias al uso combinado de Protección frente a malware avanzado (AMP) de Cisco y Cisco Umbrella, hemos reducido a cero el número de infecciones de ransomware durante los últimos 8 meses.”

Freek Bosscha, arquitecto, NHL

“Tenemos mucha mayor confianza en la seguridad de nuestros terminales gracias al uso de Cisco Umbrella junto con AMP de Cisco. No hemos sufrido ni una sola infección de malware desde que implementamos estas soluciones hace 3 años.”


Ingeniero de servicios financieros


El 70% de las brechas seguridad empiezan en los dispositivos de los terminales de

¿Por qué?

- 1) Deficiencias de protección
- 2) Errores de usuarios
- 3) Deficiencias de visibilidad

¿Qué solución?

 **AMP para terminales** es una solución de siguiente generación de seguridad para terminales que se gestiona en la nube. Detecta rápidamente, frena y pone solución a los archivos malintencionados en caso de que estos eludan las defensas de primera línea y se infiltren en los terminales. Para tal fin, emplea motores de inspección antivirus tradicionales, aprendizaje automático, funciones de aislamiento (sandboxing), supervisión de vulnerabilidades, análisis continuo del comportamiento de archivos y detección retrospectiva.

 **Umbrella** es una plataforma de seguridad en la nube que proporciona la primera línea de defensa frente a las amenazas alojadas en Internet, ya estén los usuarios en la red corporativa o fuera de ella. Umbrella proporciona una visibilidad completa de la actividad en Internet de todas las ubicaciones y terminales, y permite, a través del uso de modelos, bloquear las solicitudes malintencionadas de forma proactiva antes incluso de establecerse una conexión.

Prevenir

Umbrella bloquea las solicitudes web malintencionadas.

AMP para terminales bloquea los archivos malintencionados y envía los elementos desconocidos a un espacio aislado (sandbox) para un control en profundidad.

Detectar

Umbrella ve y detiene las devoluciones de llamada de C&C a los servidores de los atacantes.

AMP para terminales archiva de forma continua y retrospectiva las actividades para identificar comportamientos inusuales.

Poner solución

Umbrella Investigate proporciona datos reales e históricos sobre los dominios, direcciones IP y hashes comprometidos.

AMP para terminales ofrece un historial de los ataques pasados al tiempo que permite un control y puesta en cuarentena inmediatos.

Para más información visita www.cisco.com/es/go/breach