LIBRO ELECTRÓNICO

Ciberseguridad para trabajadores remotos

Cómo proteger todos los dispositivos, en todas partes.

Cisco Umbrella

Contenido

En este libro

Cómo liberar el estrés de la seguridad

La seguridad no es para los débiles de corazón. El volumen y la sofisticación de los ataques se intensifican implacablemente; está claro que las defensas convencionales no se crearon para los trabajadores móviles, las oficinas de las sucursales y el perímetro en constante expansión en la actualidad. Depender de productos antivirus, firewalls y sistemas cerrados que no comparten datos o inteligencia es una estrategia sin salida. Con menos presupuestos, menos recursos y más empleados que trabajan desde su casa como nunca antes, es hora de buscar nuevas maneras de mejorar la seguridad digital sin gastar excesivamente ni sobrecargar al personal.

En este libro electrónico, analizaremos los desafíos que enfrentan los profesionales de seguridad actuales y exploraremos algunas medidas sencillas que puede adoptar para reducir el malware, simplificar la seguridad y proteger la creciente población de trabajadores remotos e itinerantes.

La seguridad de capa de DNS es la decisión más simple que puede tomar para proteger a los empleados y estudiantes que trabajan desde el hogar.

Nuevas defensas para nuevas amenazas

A medida que la red cambia, también lo hace la metodología de ataque. La velocidad y la adaptabilidad con las que los atacantes hacen girar la infraestructura de ataque crean nuevos desafíos en el momento de identificar y bloquear el tráfico malicioso en todas las empresas de todos los sectores, lo que incluye:

- Técnicas engañosas de spearphishing por correo electrónico que permiten a los atacantes eludir las defensas convencionales e instalar ransomware y códigos maliciosos.
- Paquetes de malware puntuales que no se pueden detectar fácilmente mediante las soluciones basadas en firmas, independientemente de la rapidez con la que se actualicen los perfiles y las firmas.
- Ataques bajos y lentos que evaden las defensas basadas en la red y permiten que los atacantes infiltren la infraestructura y tomen los datos sin ser detectados durante largos períodos de tiempo.
- Kits de malware y recursos de malware como servicio que aumentan el volumen de amenazas mediante la habilitación de la participación de perpetradores y organizaciones criminales en ciberataques, como la criptominería maliciosa, a pesar de su falta de habilidades técnicas.

Incorporación de personal

3,5 millones de puestos de ciberseguridad estarán vacantes para 2021[1]

Alertas

El 44 % ve más de 10 000 alertas diarias[2]

Coordinación

El 79 % lucha por organizar las alertas entre los proveedores[2]

1. Informe sobre puestos de trabajo en ciberseguridad de Cybersecurity Ventures | https://cybersecurityventures.com/cybersecurity-almanac-2019/
2. Encuesta de parámetros a CISO de Cisco de 2019 | https://www.cisco.com/c/dam/m/digital/elq-cmcglobal/witb/1963786/2019CISOBenchmarkReportCiscoCybersecuritySeries.pdf

Seguridad de capa de DNS: empleados seguros que trabajan desde su casa con facilidad

Es hora de usar Internet como ventaja para la seguridad. El 91 % del malware usa el DNS para tener el comando y control, exfiltrar datos o redirigir el tráfico web. Pero cuando las solicitudes de Internet se resuelven mediante un servicio de DNS recursivo, se convierten en el lugar perfecto para verificar y bloquear IP y dominios maliciosos o inapropiados. Los equipos de seguridad que no monitorean el DNS para obtener indicios de riesgo se pierden una oportunidad importante.

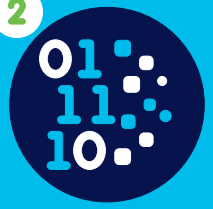
El DNS es una de las fuentes de datos más valiosas dentro de una organización. Se debe hacer una recopilación periódica y una referencia cruzada con la inteligencia de amenazas a fin de ayudar a los equipos de seguridad a obtener una mayor precisión y detección de los sistemas comprometidos y mejorar la visibilidad y la protección de la red. Los líderes de seguridad de TI deben hacer de la seguridad de capa de DNS proactiva un componente principal de sus estrategias de seguridad. Es la gran primera línea de defensa contra las amenazas para los empleados que trabajan desde el hogar.

Seguridad de capa de DNS proactiva en tres simples pasos

1

Bloquee las conexiones peligrosas entre los usuarios y los dominios maliciosos.

2



Detenga las exfiltraciones de datos y retrollamadas de comando y control (C2) de manera sencilla.

3

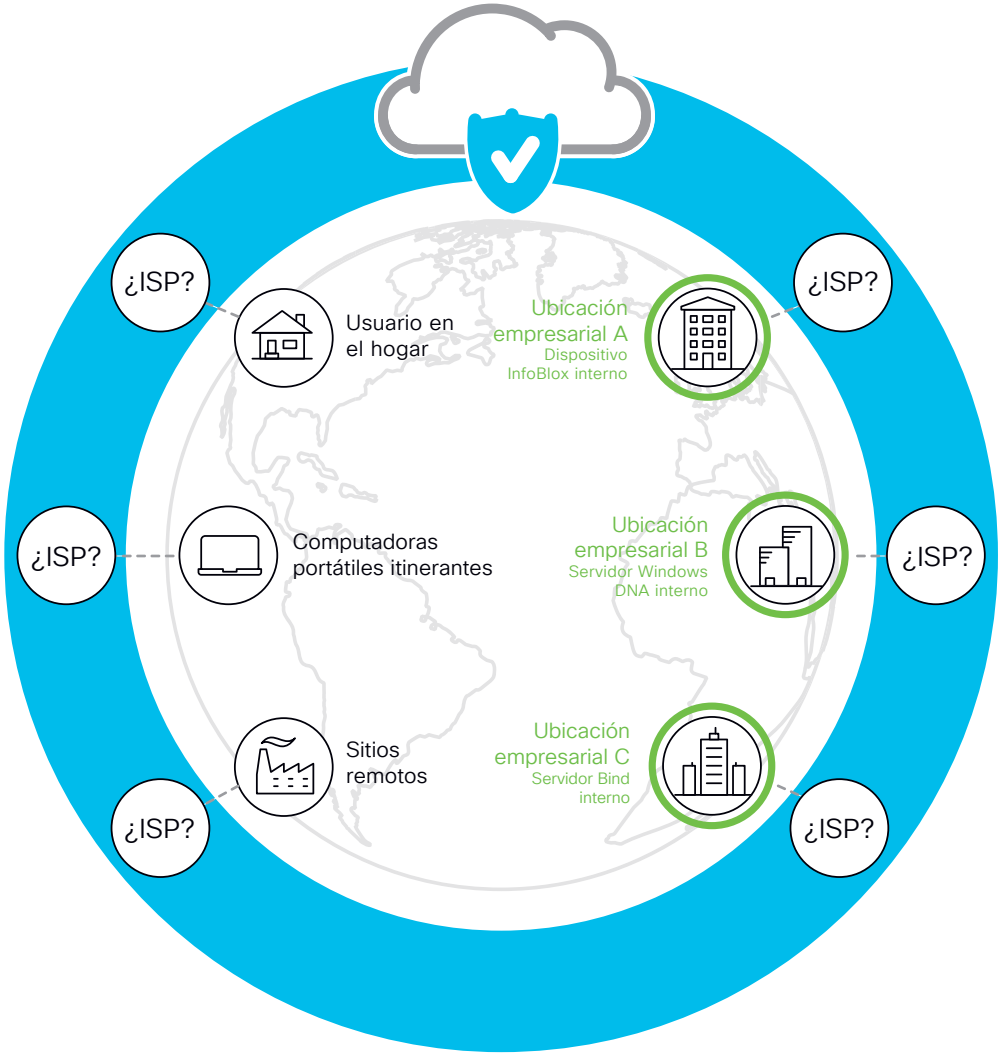
Reduzca las alertas y los incidentes de seguridad neutralizándolos antes de que ocurran.

Una mejor manera de detener las amenazas más rápidamente

Aumente la visibilidad, disminuya el riesgo y trabaje.

La mayoría de las empresas deja la resolución del DNS a su ISP. Pero, a medida que más organizaciones adoptan conexiones directas a Internet y los usuarios omiten la VPN, esto genera un punto ciego para el DNS. Las solicitudes de DNS preceden la conexión IP, lo que permite que los solventadores del DNS registren los dominios solicitados, independientemente del protocolo o el puerto de conexión. La supervisión de las solicitudes de DNS (así como de las conexiones IP posteriores) es una forma sencilla de brindar una mejor precisión y detección de sistemas en riesgo, lo que mejora la visibilidad de la seguridad y la protección de la red.

En resumen, los líderes de seguridad de TI buscan estrategias de seguridad más eficaces que no agreguen complejidad a las operaciones de seguridad.



La indispensabilidad de la seguridad de capa de DNS

La seguridad de capa de DNS funciona con el principio simple de que los ataques, independientemente de cuán sofisticados o exclusivos sean, deben originarse en algún lugar. Al bloquear de forma preventiva todas las solicitudes en cualquier puerto o protocolo a cualquier " lugar" sospechoso, la seguridad de capa de DNS puede detener la exfiltración del comando y control, la criptominería maliciosa, el ransomware y otros ataques sin la carga de identificar la naturaleza específica de esos ataques. Los dominios erróneos se bloquean porque se identifican de manera rápida y precisa como dominios defectuosos.

La seguridad de capa de DNS ofrece:

- **Identificación predictiva de hosts maliciosos**. Al agregar y analizar datos relacionados con el DNS, entre ellos, decenas de miles de millones de solicitudes de DNS diarias, registros de WHOIS e información de routing del protocolo de gateway fronterizo, es posible identificar dominios sospechosos con un alto grado de precisión.
- **Bloqueo de solicitudes de DNS como servicio en la nube**. Con una lista constantemente actualizada de dominios sospechosos, un proveedor de servicios en la nube puede bloquear de manera preventiva las solicitudes de cualquier dominio o IP que puedan representar una amenaza para el negocio.

1 de 3

empresas informó que las intrusiones podrían haber sido controladas por el DNS[3]

USD 100/200 mil millones

de pérdidas globales podrían haberse prevenido con el DNS[3]

3. " El valor económico de la seguridad del DNS" , un nuevo informe publicado por Global Cyber Alliance (GCA) | https://www.darkreading.com/network-and-perimeter-security/dns-firewalls-could-save-companies-billions/d/d-id/1334965

La seguridad de capa de DNS bloquea las amenazas que otros pasan por alto

Al aplicar la seguridad en las capas de DNS e IP, Umbrella bloquea las solicitudes de malware, ransomware, suplantación de identidad (phishing) y botnets incluso antes de establecer una conexión, deteniendo las amenazas en cualquier puerto o protocolo antes de que lleguen a los terminales sin latencia agregada. Umbrella bloquea las conexiones IP directas de las retrollamadas de comando y control para los usuarios itinerantes.

Umbrella categoriza y retiene toda la actividad de Internet para simplificar el proceso de investigación. Mediante la consola de Umbrella Investigate y la API de enriquecimiento a petición, proporciona contexto para priorizar incidentes y acelerar la respuesta ante los incidentes a fin de que pueda detectar y corregir las amenazas más rápidamente con Cisco Threat Response.

AV-TEST realizó una prueba de eficacia de las amenazas y Cisco Umbrella fue significativamente mejor que otros proveedores, con una tasa de detección del 51 % para la protección de capa de DNS. El proxy selectivo de Cisco Umbrella marca una gran diferencia en la detección eficaz de amenazas y aumentó la tasa de bloqueo al 72 %.

AV-TEST: resultados de la prueba de eficacia de la protección de capa de DNS[4]

Proveedor	Tasa de detección | Número de casos probados: 3668
Cisco Umbrella (capa de DNS con proxy selectivo)	72,6 %
Cisco Umbrella (capa de DNS)	51,8 %
Infoblox BloxOne	35,3 %
Akamai Enterprise Threat Protector	26,5 %
Firewall de próxima generación de Palo Alto Networks	13,7 %

4. https://learn-umbrella.cisco.com/analyst-reports/av-test-dns-layer-protection-and-secure-web-gateway-security-efficacy-test-results

¿Por qué Cisco Umbrella?

Umbrella se compromete a ofrecer la mejor, más confiable y más rápida experiencia de Internet a cada uno de nuestros usuarios. Somos el proveedor líder de servicios de seguridad de red y DNS, lo que permite que el mundo se conecte a Internet con confianza en cualquier dispositivo.

- **Más de una década de liderazgo en DNS**. Trece años de experiencia práctica con la tecnología y los datos del DNS brindan ventajas significativas a Cisco Umbrella a la hora de comprender y bloquear la infraestructura de los atacantes.
- **Volumen y variedad de datos del DNS incomparables**. Cisco Umbrella posee una visibilidad inigualable de la actividad del DNS en todo el mundo. La red global de Umbrella procesa 200 mil millones de solicitudes de Internet de más de 100 millones de usuarios en 190 países en todo el mundo.
- **Inteligencia predictiva y modelos estadísticos**. Cisco Umbrella ha desarrollado modelos altamente especializados que bloquean 7 millones de destinos maliciosos en un momento dado y los detecta antes que cualquier otro proveedor de seguridad del planeta.
- **Infraestructura de nube altamente resistente**. Umbrella hace alarde de un 100 % de tiempo de actividad desde 2006. Con el routing de Anycast, cualquiera de nuestros 30 centros de datos en todo el mundo están disponibles con la misma dirección IP única. Las solicitudes se envían de manera transparente al centro de datos más rápido y cercano; la conmutación por error es automática.
- **Integraciones que amplifican las inversiones**. Umbrella unifica varios servicios de seguridad en una sola plataforma de nube para garantizar el acceso a Internet y controlar los usos de las aplicaciones en la nube en cualquier lugar al que vayan los usuarios. Los usuarios pueden administrar políticas de seguridad y aplicación en toda la infraestructura desde un único panel, a través de integraciones con la arquitectura Cisco SD-WAN, los routers Cisco Meraki MR y Cisco ISR, Cisco Stealthwatch y Cisco Advanced Malware Protection.

Ventaja global de la red Umbrella:

+200 mil millones

de solicitudes de DNS diarias

100 millones

de usuarios activos globales diarios

+900

asociaciones con los principales ISP y CDN

+20 000

clientes

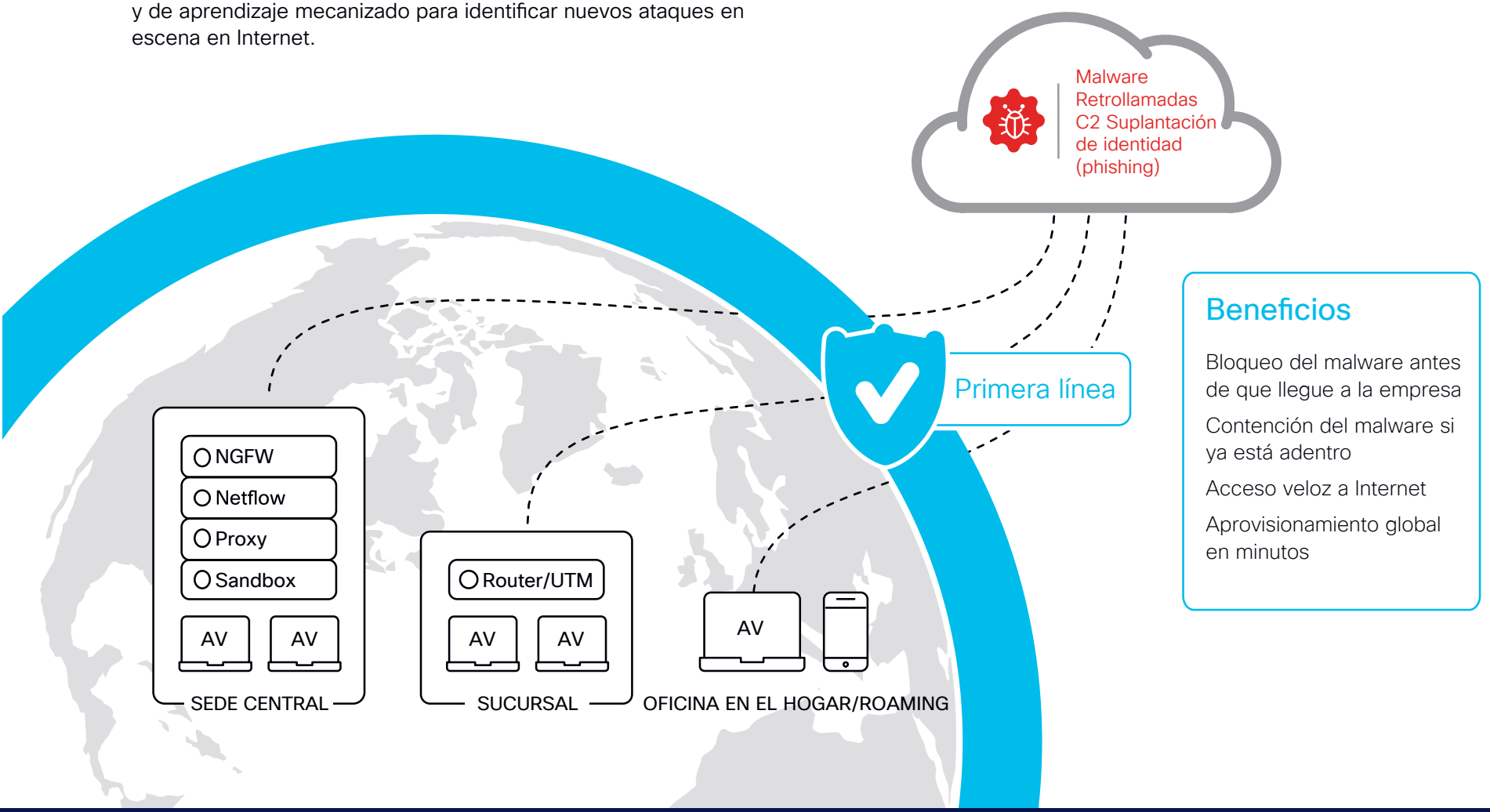
+30

centros de datos en cinco continentes

Aplicación de la seguridad para sedes centrales, sucursales y oficinas en el hogar

Aprovechando la incomparable información sobre amenazas de Cisco Talos, uno de los equipos de inteligencia de amenazas comerciales más grande del mundo, Umbrella detecta y bloquea un amplio espectro de dominios, IP, URL y archivos maliciosos que se usan en los ataques. Además, proporcionamos enormes volúmenes de actividad de Internet global combinados en modelos estadísticos y de aprendizaje mecanizado para identificar nuevos ataques en escena en Internet.

Estos atributos distintivos hacen que Umbrella sea, indiscutiblemente, la mejor opción para las empresas de todos los tamaños, desde las pequeñas empresas sin profesionales de seguridad dedicados hasta las empresas multinacionales con entornos complejos. Umbrella brinda una protección más eficaz de la seguridad y la visibilidad de toda la red, tanto dentro como fuera.



Beneficios

- Bloqueo del malware antes de que llegue a la empresa
- Contención del malware si ya está adentro
- Acceso veloz a Internet
- Aprovisionamiento global en minutos

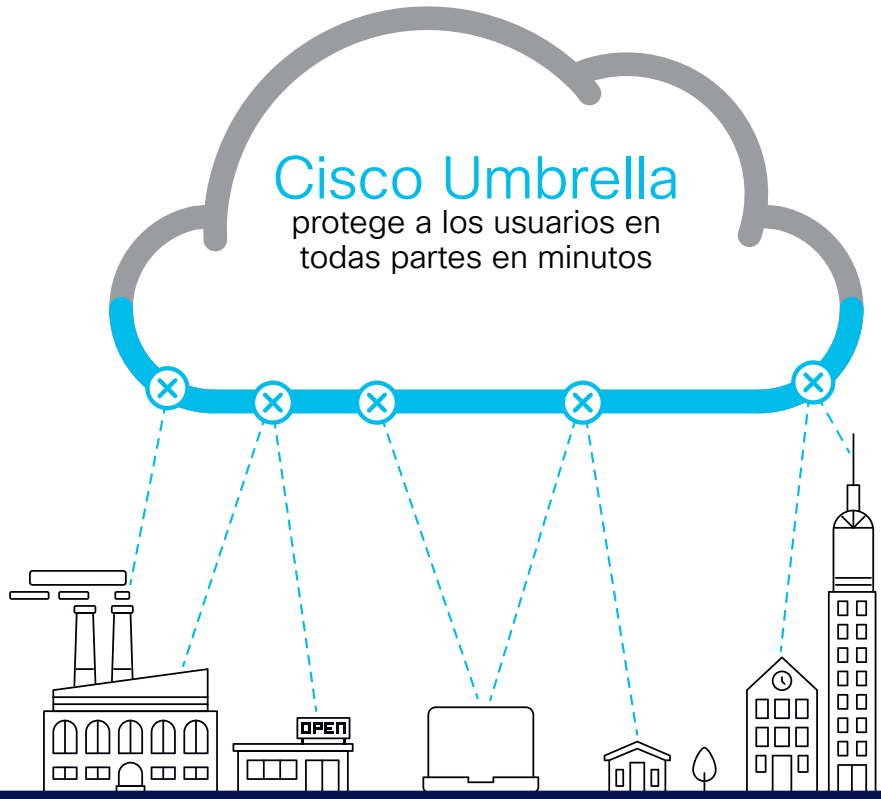
30 minutos para proteger a los trabajadores en cualquier lugar

Los clientes de Umbrella reducen el malware en un 75 %[5] y los tiempos de corrección en un 50 % o más[6].

Simplifique la seguridad para los empleados que trabajan desde el hogar

Umbrella es la manera más rápida y fácil de proteger a todos los empleados, ya sea que trabajen desde su casa, la oficina o sobre la marcha. Sin hardware que instalar ni software que actualizar manualmente, la administración continua es sencilla.

Simplemente, redirija su DNS a Cisco Umbrella. Eso es todo. Luego, puede aprovechar la huella existente de Cisco, como Cisco AnyConnect, los routers de Cisco (de la serie ISR y 4K), los controladores LAN inalámbricos de Cisco y Meraki MR/MX, para aprovisionar miles de dispositivos de red y computadoras portátiles en cuestión de minutos.



¿Le interesa probar Umbrella?

Obtenga la protección contra amenazas global en cuestión de minutos. Pruébela durante 14 días.

Inicie una prueba gratuita

5. https://www.techvalidate.com/product-research/cisco-umbrella/facts/AF2-8E2-79D
6. https://www.techvalidate.com/product-research/cisco-umbrella/charts/F83-DB9-434