

Ciberseguridad



Usted enfrenta desafíos sin precedentes para proteger su empresa mediana contra amenazas de ciberseguridad. Las nuevas tendencias como la movilidad y la nube cambian la forma en que debe proteger los dispositivos, los datos y su red.

Para afrontar estos desafíos, necesita un modelo de seguridad basado en amenazas escalable e inteligente. Este modelo debe proporcionar políticas y controles de seguridad estándar rentables de corrección de amenazas y soporte.

Cisco puede ayudarlo. Ofrecemos ciberseguridad inteligente para el mundo real. Nuestro enfoque centrado en amenazas reduce la complejidad mientras brinda visibilidad y control superiores, lo cual le ahorra tiempo y reduce costos.

Con Cisco, obtiene protección avanzada contra amenazas en todo el continuum de ataque: antes, durante y después de este.

ANTES DE UN ATAQUE



DETECTAR • APLICAR • REFORZAR

Debe saber qué hay en su red para defenderla. Hacer un inventario de sus dispositivos, aplicaciones, usuarios y otras posibles vulnerabilidades debe ser sencillo. Necesita herramientas fáciles de usar que puedan implementar controles de acceso, apliquen políticas y bloqueen aplicaciones para ayudar a minimizar su superficie de ataque.

Prepárese:



Los firewalls Cisco® ASA de próxima generación (NGFW) de la serie 5500-X con servicios FirePOWER™ proporcionan:

- Defensa integrada contra amenazas
- Controles de acceso y políticas granulares
- Protección avanzada contra malware (AMP) de primera clase y capacidad del sistema de prevención de intrusiones (IPS) de última generación



Cisco Identity Services Engine (ISE) automatiza y simplifica:

- Control de acceso seguro para acceso cableado, inalámbrico o conectividad VPN
- Ejecución del cumplimiento y seguridad de la infraestructura mejorada

Las políticas y los controles por sí solos ya no son suficientes. Los atacantes más avanzados aún pueden encontrar y explotar las vulnerabilidades.

DURANTE UN ATAQUE

Con el panorama de amenazas actual colmado de malware y ataques de día cero, las tecnologías instantáneas por sí solas no funcionan. Necesita la mejor detección de amenazas posible para identificar continuamente la actividad maliciosa en su red.



DETECTAR • BLOQUEAR • DEFENDER



CISCO INTRUSION PREVENTION SYSTEM (IPS)



SEGURIDAD WEB Y DE CORREO ELECTRÓNICO



SEGURIDAD WEB DE NUBE



CISCO TRUSTSEC



Disminuya el impacto:

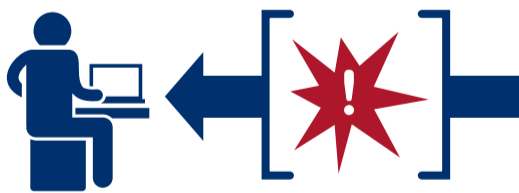
El **sistema de prevención de intrusiones (NGIPS) FirePOWER de última generación** de Cisco y los productos de seguridad de contenido pueden ayudar a brindar protección contra ataques dirigidos a los gateways:

- Cisco **FirePOWER NGIPS** ofrece una completa y avanzada protección contra amenazas altamente eficaz
- Los dispositivos de seguridad **Web y correo electrónico** de Cisco detectan y bloquean las amenazas cambiantes de correo electrónico y Web
- Cisco **Cloud Web Security** ofrece seguridad líder del sector y control de las organizaciones distribuidas
- Cisco **ASA con los servicios FirePOWER** ofrece defensa contra amenazas adaptable e integrada con el comprobado cortafuegos ASA, IPS, Protección avanzada contra malware (AMP) y el control y la visibilidad de la aplicación (AVC)

La tecnología **Cisco TrustSec®**, integrada en los switches, routers y dispositivos de seguridad, puede evitar el tráfico malicioso de cuarentena en toda la red.

Dada la naturaleza del malware actual, la mejor detección de amenazas por sí sola no es suficiente para proteger su entorno.

DESPUÉS DE UN ATAQUE



EXAMINAR • CONTENER • REMEDIAR

Bloquee y defienda:

Cisco Advanced Malware Protection (AMP) le ayuda a

- Descubrir, investigar, analizar, bloquear y remediar ataques y amenazas avanzadas persistentes (APT) contra malware
- Agilizar los tiempos de respuesta y automatizar la corrección para prevenir futuros ataques, minimizar daños y eliminar el riesgo de reinfección
- Visualizar y determinar los efectos del malware y los señadores de riesgo en la red y los niveles del sistema, mientras que proporciona análisis detallado del comportamiento del malware

Invariablemente, algunos ataques serán exitosos. Usted debe ser capaz de determinar el alcance del daño, contener el evento, remediarlo y lograr que las operaciones se desempeñen con normalidad. También debe considerar los vectores de ataque, con soluciones que funcionan en todos los sitios en que las amenazas pueden manifestarse.

El enfoque de seguridad centrado en **amenazas de Cisco** puede ayudar a reducir la complejidad de la red, las brechas de seguridad de puente y a escalar su empresa de acuerdo con sus nuevos y cambiantes modelos comerciales.



Encuentre soluciones de seguridad correctas para su empresa mediana visitando **las soluciones de Cisco para empresas medianas.** ▶

Síguenos en Twitter en **#ciscomidsize.**

Su solución de seguridad más simple, su empresa más competitiva.