

Cisco Secure Firewall para manufactura



Convierta toda su red en una extensión de su arquitectura de seguridad

Con las aplicaciones críticas para el negocio que cada vez usan más una combinación de implementaciones en la nube y en las instalaciones y los usuarios que ahora necesitan acceso seguro a los recursos desde cualquier lugar, el enfoque de firewall tradicional ya no funciona. Nuestro perímetro de la red único ha evolucionado a múltiples microperímetros. Para muchas organizaciones, la aplicación es el nuevo perímetro y las implementaciones de firewall tradicional han evolucionado hacia una combinación de dispositivos físicos, virtuales y nativos de la nube. Como resultado, las organizaciones luchan por poner en funcionamiento el soporte para entornos de aplicaciones modernos. El desafío es mantener la aplicación de políticas y una visibilidad uniforme de las amenazas sin abrir vulnerabilidades que expongan a las organizaciones al riesgo.

En Cisco estamos creando una visión de seguridad de red, NetWORK, que permite un enfoque más ágil, automatizado e integrado para unificar las políticas y su cumplimiento en aplicaciones dinámicas modernas y redes cada vez más heterogéneas. Cisco Secure Firewall le ofrece el conjunto más completo de integraciones entre las funciones principales de la red y la seguridad de la red, lo que brinda la arquitectura más segura que haya existido. El resultado es un portafolio completo de seguridad que protege sus aplicaciones y sus usuarios en todas partes.

Beneficios

- Seguridad unificada en tiempo real de la red y las cargas de trabajo para un control integrado en entornos dinámicos de manufactura.
- Enfoque de plataforma para la seguridad de la red que aprovecha y comparte la inteligencia de fuentes clave para una detección, respuesta y corrección más rápidas.
- Protección de los trabajadores remotos con acceso empresarial sumamente seguro en cualquier momento y en cualquier lugar, desde cualquier dispositivo, y potentes funcionalidades de prevención de amenazas que protegen la organización, los usuarios y las aplicaciones críticas.
- Acceso incluido a SecureX™ con cada Cisco® Secure Firewall para un enfoque estrechamente integrado a la seguridad que permite la correlación de amenazas a través del portafolio de Cisco Secure y acelera la respuesta a incidentes.

Visibilidad y control superior

Las amenazas se han vuelto más sofisticadas y las redes, más complejas. Muy pocas organizaciones, de existir, tienen los recursos para dedicarse a mantenerse actualizadas y defenderse con éxito de las amenazas en constante evolución.

A medida que las amenazas y las redes se vuelven más complejas, es imprescindible contar con las herramientas adecuadas para proteger sus datos, sus aplicaciones y sus redes. Cisco Secure Firewall tiene la potencia y la flexibilidad que necesita para estar un paso adelante de las amenazas. Ofrece un aumento notorio del rendimiento 3 veces superior a la generación anterior de dispositivos, además de capacidades exclusivas basadas en hardware para inspeccionar el tráfico cifrado a escala. Las reglas legibles para los humanos de Snort 3 IPS también ayudan a simplificar la seguridad. La visibilidad y el control dinámicos de las aplicaciones están disponibles a través de la integración de Cisco Secure Workload para brindar una protección uniforme para las aplicaciones modernas actuales en toda la red y la carga de trabajo.

[Encuentre el firewall ideal para su empresa](#)

Administración de políticas simplificada y uniforme

Con el portafolio de Secure Firewall, obtiene una postura de seguridad más sólida, equipada con una administración flexible y preparada para el futuro. Cisco ofrece una variedad de opciones de administración personalizadas para satisfacer sus necesidades empresariales:

- **Administrador de dispositivos Cisco Secure Firewall:** administra un único firewall de manera local; es una solución de administración en el dispositivo para Firewall Threat Defense.
- **Cisco Secure Firewall Management Center:** administra la implementación del firewall a gran escala. Está disponible en todos los factores de forma, por ejemplo, en las instalaciones, la nube privada, la nube pública y el software como servicio (SaaS).
- **Cisco Defense Orchestrator:** un administrador basado en la nube que optimiza las políticas de seguridad y la administración de dispositivos en varios productos de Cisco, como Cisco Secure Firewall, Meraki® MX y dispositivos Cisco IOS®.

Cisco también ofrece Cisco Security Analytics and Logging para una administración de registros escalable. Mejora la detección de amenazas y satisface los mandatos de cumplimiento en toda la organización con capacidades de análisis de comportamiento y retención más prolongadas.

[Historia del cliente](#)

¿Por qué Cisco?

El portafolio de Cisco Secure Firewall ofrece mayores protecciones para su red contra un conjunto de amenazas cada vez más complejo y en constante evolución para los fabricantes. Con Cisco, usted invierte en una base para la seguridad que es ágil y está integrada, lo que lleva a la postura de seguridad más sólida disponible en la actualidad y en el futuro.

Desde su centro de datos, la planta de la fábrica, entornos de nube y cualquier otro espacio intermedio, puede aprovechar el poder de Cisco para convertir su infraestructura de red existente en una extensión de su solución de firewall, lo que crea controles de seguridad de primera clase dondequiera que los necesite.

La actual inversión en dispositivos Secure Firewall brinda protecciones sólidas contra las amenazas más sofisticadas sin comprometer el rendimiento al inspeccionar el tráfico cifrado. Además, las integraciones con otras soluciones de Cisco y de terceros le brindan un portafolio amplio y completo de productos de seguridad que funcionan en conjunto para correlacionar eventos previamente desconectados, eliminar el ruido y detener las amenazas más rápidamente.

Funcionalidades avanzadas de Cisco Secure Firewall

Funcionalidad avanzada	Detalles
Integración de Cisco Secure Workload	<ul style="list-style-type: none"> La integración de Cisco Secure Workload (antes Tetration®) permite una visibilidad completa y la ejecución de políticas para aplicaciones modernas distribuidas y dinámicas en toda la red y la carga de trabajo para un cumplimiento uniforme y escalable.
Cisco Secure Firewall Cloud Native	<ul style="list-style-type: none"> Creada con Kubernetes y disponible por primera vez en AWS, Secure Firewall Cloud Native es una solución de acceso a aplicaciones fácil de usar para desarrolladores con el fin de crear una infraestructura nativa de la nube sumamente elástica.
Soporte de políticas dinámicas	<ul style="list-style-type: none"> Los atributos dinámicos admiten etiquetas de VMware, AWS y Azure para situaciones en las que las direcciones IP estáticas no están disponibles. Cisco ha sido pionero en políticas basadas en etiquetas con etiquetas de grupo de seguridad (SGT) y soporte de atributos de Cisco Identity Services Engine (ISE).
Sistema de prevención de intrusiones Snort 3	<ul style="list-style-type: none"> El siguiente paso en la protección contra amenazas con Snort 3 de código abierto, líder en el sector, ayuda a mejorar la detección, simplificar la personalización y optimizar el rendimiento.
Detección e identidad del servidor de seguridad de la capa de transporte (TLS)	<ul style="list-style-type: none"> Le permite mantener políticas de capa 7 en tráfico TLS 1.3 cifrado. Mantenga la visibilidad y el control en un mundo cifrado donde no es factible descifrar e inspeccionar cada flujo de tráfico. Los firewalls de la competencia rompen las políticas de capa 7 con tráfico TLS 1.3 cifrado.
Cisco Secure Firewall Management Center	<ul style="list-style-type: none"> Ofrece una administración unificada de firewalls, control de aplicaciones, prevención de intrusiones, filtrado de URL y políticas de defensa contra malware. La integración con Cisco Secure Workload (antes Tetration) permite una visibilidad completa y la ejecución de políticas para aplicaciones dinámicas en toda la red y la carga de trabajo.
Cisco Defense Orchestrator	<ul style="list-style-type: none"> Administración de firewall basada en la nube que permite administrar las políticas de manera uniforme y sencilla en Cisco Secure Firewalls.
Cisco Security Analytics and Logging	<ul style="list-style-type: none"> Administración de registros de firewalls de gran escalabilidad en las instalaciones y basada en la nube con análisis del comportamiento para la detección de amenazas en tiempo real y tiempos de respuesta más rápidos. Además ofrece análisis continuo para refinar aún más su postura de seguridad para defenderse mejor de futuros intentos. Satisfaga sus necesidades de cumplimiento con la agregación de registros en Cisco Secure Firewalls. Integración estrecha con los administradores de firewalls para un registro y análisis extendidos, así como para agregar datos de registro de firewalls en una única vista intuitiva.
Cisco SecureX	<ul style="list-style-type: none"> Aproveche la plataforma SecureX para acelerar la detección y detección de amenazas. Cada Secure Firewall incluye acceso a Cisco SecureX. La nueva cinta de SecureX en Firewall Management Center permite que SecOps gire al instante a la plataforma abierta de SecureX, lo que acelera la respuesta a incidentes.
Inteligencia de amenazas de Cisco Talos®	<ul style="list-style-type: none"> Cisco Talos Intelligence Group es uno de los equipos de inteligencia de amenazas comerciales más grandes del mundo. Crea inteligencia de amenazas precisa, rápida y procesable para los clientes, los productos y los servicios de Cisco. Talos mantiene los conjuntos de reglas oficiales de Snort.org, ClamAV y SpamCop.

Próximos pasos

Para obtener más información sobre Cisco Secure Firewall, visite cisco.com/site/mx/es/products/security/firewalls/index. Para conocer las opciones de compra y comunicarse con un representante de ventas de Cisco, visite cisco.com/c/es_mx/buy. Para obtener más información sobre las soluciones de manufactura de Cisco, visite cs.co/manufacturingportfolio.

Sede central en América

Cisco Systems, Inc.
San José. CA

Sede Central en Asia Pacífico

Cisco Systems (EE. UU.) Pte. Ltd.
Singapur

Sede Central en Europa

Cisco Systems International BV Amsterdam.
Países Bajos

Cisco cuenta con más de 200 oficinas en todo el mundo. Las direcciones, los números de teléfono y de fax están disponibles en el sitio web de Cisco: www.cisco.com/go/offices.

Cisco y el logotipo de Cisco son marcas registradas o marcas comerciales de Cisco y/o de sus filiales en los Estados Unidos y en otros países. Para ver una lista de las marcas registradas de Cisco, visite la siguiente URL: www.cisco.com/go/trademarks. Las marcas registradas de terceros que se mencionan aquí son de propiedad exclusiva de sus respectivos titulares. El uso de la palabra “partner” no implica que exista una relación de asociación entre Cisco y otra empresa. (1110R)