CISCO
SECURE

Guía del comprador de XDR

Navegue por el mercado de detección y respuesta extendidas como un profesional

Introducción a la detección y respuesta extendidas (XDR)

¿Por qué el mundo necesita otro enfoque de seguridad?

En el panorama híbrido, de varios proveedores y de varios vectores que se presenta hoy en día, la complejidad es el mayor desafío. Los equipos de seguridad deben proteger un ecosistema en constante expansión mientras ejecutan operaciones en docenas de herramientas con una integración inconsistente. Internet de las cosas y el trabajo híbrido han dado lugar a una superficie de ataque extendida. La suplantación de identidad (phishing), el malware y el ransomware se duplican e incluso triplican año tras año. Al mismo tiempo, las empresas están más hiperconectadas que nunca. La violación a la seguridad de una empresa puede afectar a los proveedores, los partners, los clientes e incluso sectores completos de la economía.

Esta nueva normalidad precisa de ciberresiliencia, que es la capacidad de proteger la integridad de todos los aspectos de la empresa para que pueda resistir a amenazas o cambios impredecibles y resurgir con más fuerza. Y la ciberresiliencia exige más de lo que ha ofrecido el pasado.

Ventajas de XDR:

- Detección de varios proveedores
- Menor fatiga de alertas
- Mayor productividad
- Ciberresiliencia

¿Cuál es la solución?

A medida que las amenazas se vuelven cada vez más sofisticadas, el antiguo modelo de detección y respuesta basado en soluciones de seguridad puntuales y autónomas se queda corto. Aquí es donde entra en juego la XDR. La detección y respuesta extendidas (XDR) es una herramienta unificada de detección y respuesta de incidentes de seguridad. Las soluciones de XDR recopilan y correlacionan automáticamente la telemetría de varias herramientas de seguridad, aplican análisis para detectar actividad maliciosa, y luego responden y corrigen las amenazas. Las soluciones de XDR eficaces son integrales y correlacionan datos en todos los vectores (correo electrónico, terminales, servidores, cargas de trabajo en la nube y redes), lo que permite obtener la visibilidad y el contexto en todo el entorno, incluso para las amenazas más avanzadas.

¿Por qué XDR?

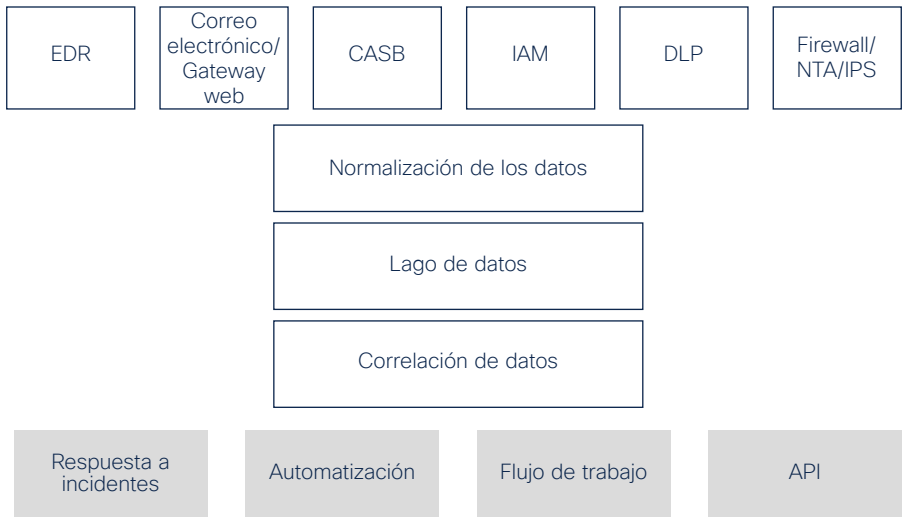
En primer lugar, permite que los equipos detecten las amenazas más sofisticadas con correlación de eventos y detecciones de varios proveedores en la red, la nube, los terminales, el correo electrónico, entre otros.

En segundo lugar, reduce la fatiga de alertas al permitir que los equipos prioricen las amenazas en función del impacto.

En tercer lugar, eleva la productividad con la automatización de tareas para que los equipos puedan hacer un uso más eficiente de los recursos del SOC.

En cuarto lugar, permite a las organizaciones crear ciberresiliencia al cerrar las brechas de seguridad y anticiparse a lo que vendrá a través de inteligencia procesable.

Arquitectura conceptual de XDR



Cinco elementos clave del funcionamiento correcto de XDR

1 Ofrece telemetría priorizada y procesable, donde sea que la necesite

¿Puede analizar de manera eficaz el mar de alertas para evaluar las amenazas?

La amplitud de la visibilidad y la profundidad de la información son fundamentales para XDR. Muchas amenazas sofisticadas no solo atacan el terminal o la red, sino que lo hacen a través de una variedad de vectores, incluidos el correo electrónico, el terminal, la red, la administración de identidades, el sandboxing y el firewall. Es por eso que necesita una solución de XDR con una amplia gama de telemetría y calidad de datos que pueda informar sus resultados de XDR y ofrecer una vista holística y completa de lo que sucede en su entorno. Pero no se debe solo recopilar información: la administración de incidentes es igualmente importante. Para que XDR tenga el efecto que promete, esta información se debe priorizar. Las soluciones de XDR que ofrecen prioridad a los incidentes basada en los riesgos (que priorizan los incidentes según mayor riesgo material) le permitirán actuar sobre lo que realmente importa, de forma más rápida. También deben ofrecer recomendaciones para los próximos pasos, para que pueda tomar decisiones informadas sobre el mejor curso de acción.

Funciones y capacidades clave	Áreas de productos relacionados
• Eficacia y precisión para minimizar el ruido de los falsos positivos. • Agrega y correlaciona alertas en todo el entorno.	Detección y respuesta de terminales (EDR)
• Monitoreo continuo de la red en tiempo real.	Detección y respuesta de red (NDR)
• Análisis avanzados que generan alertas priorizadas con contexto cuando se detectan programas maliciosos desconocidos y otros ataques sofisticados a la red.	Detección y respuesta extendidas (XDR)
• Monitoreo continuo de amenazas de correo electrónico en tiempo real y priorización de corrección automática.	Seguridad del correo electrónico

Preguntas para hacer a los proveedores

- ¿Cómo me brinda su solución visibilidad en todos mis entornos (terminales, dispositivos, redes)?
- ¿Cómo aporta información su solución? ¿Su solución proporciona telemetría priorizada?
- ¿Cómo prioriza su solución las amenazas en función del impacto y el riesgo empresarial?
- ¿Qué tipo de inteligencia de amenazas alimenta su detección? ¿De dónde proviene esa inteligencia?
- ¿Cómo valida las fuentes de datos que usa en su solución?
- ¿Cómo maneja este producto las amenazas sofisticadas como Wannacry, NotPetya y Turla?

2 Permite la detección unificada, con independencia del vector o el proveedor

¿Su solución de XDR permite que sus inversiones en seguridad funcionen en conjunto como una unidad coordinada?

Mientras las amenazas se vuelven más sofisticadas y abarcan una mayor variedad de vectores de ataque, garantizar la detección uniforme en todo el entorno nunca ha sido más importante. Hoy en día, los equipos de seguridad se enfrentan a un nivel extraordinario de complejidad, tanto en su entorno de seguridad como en un ecosistema de cadenas de suministro globales, atacantes y defensores. Las soluciones de XDR le permitirán lograrlo al agregar, correlacionar y priorizar las detecciones en función de la gravedad y el impacto. Pero para ello, su pila de seguridad debe funcionar al unísono. Al seleccionar una solución de XDR que sea abierta, extensible y esté orientada a la nube, se beneficiará con una detección y correlación de eventos unificada en todo el entorno, en lugar de agregar capas adicionales de complejidad. Cada componente de su pila de seguridad tiene elementos de detección únicos (redes, correo electrónico, firewall, etc.) que se tornan más potentes cuando se combinan. Es importante tener en cuenta que, para ofrecer una vista completa de las posibles amenazas, XDR debe abarcar las seis fuentes de telemetría, incluidos los terminales, la red, el firewall, el correo electrónico, la identidad y el DNS. Su solución de XDR debe integrarse fácilmente con toda su pila de seguridad con integración nativa de backend a frontend, de modo que la cobertura se mantenga constante incluso cuando los proveedores hagan cambios en el portafolio o si usted cambia de proveedor. Por último, para optimizar las capacidades de detección de amenazas de su pila de seguridad, vale la pena explorar las soluciones de XDR que pueden brindar un contexto local valioso y ofrecer veredictos de inteligencia de amenazas precisos en los que puede confiar.

Funciones y capacidades clave	Áreas de productos relacionados
• Detecta y bloquea el comportamiento anormal del programa en ejecución de terminales, incluidos los ataques de inyección de memoria basados en vulnerabilidades. • Determina los indicadores de compromiso (IoC) con la asignación de MITRE ATT y CK. • Monitorea la puntuación de archivos para detectar y aislar las amenazas en el punto de entrada. • Identifica las vulnerabilidades del sistema operativo en su entorno, lo que permite a los administradores priorizar la corrección en función del riesgo y reducir la superficie de ataque.	Detección y respuesta de terminales (EDR), administración de vulnerabilidades
• Usa análisis avanzados para detectar con rapidez malware desconocido, amenazas internas como exfiltración de datos, infracciones a las políticas y otros ataques sofisticados. • Detecta ataques de red en tiempo real con alertas de alta fidelidad.	Detección y respuesta extendidas (XDR), Detección y respuesta de red (NDR)
• Detecta y bloquea correo electrónico no deseado con el filtrado de reputación. • Identifica y protege contra los ataques por correo electrónico basados en el engaño, como la ingeniería social y los impostores.	Seguridad del correo electrónico

Preguntas para hacer a los proveedores

- ¿Cuántas de mis inversiones existentes puede aprovechar su plataforma de XDR?
- ¿Su plataforma de XDR es compatible con mis soluciones, independientemente del proveedor?
- ¿Sus soluciones inmediatas que se integran entre sí?
- ¿En qué son mejores sus tecnologías de detección comparadas con otras que están en el mercado?
- ¿Qué tipo de amenazas ayuda a detectar su solución? ¿Asigna alertas al marco de MITRE ATT & CK?

3 Permite responder a las amenazas con rapidez y precisión

Una vez identificado ¿con qué rapidez puede responder con confianza a las amenazas?

La unificación de la información de la red, el terminal y el correo electrónico (por mencionar algunos) proporciona una comprensión más precisa de lo que ha sucedido, cómo progresó y qué pasos deben tomarse para corregir la amenaza. Lo ideal sería poder ver el impacto y el alcance de las amenazas desde una sola ubicación y tomar medidas con solo uno o dos clics. Para que XDR sea eficaz se requieren capacidades de respuesta y corrección nativas, como aislar un host o eliminar un correo electrónico malicioso de todas las bandejas de entrada. XDR también debe facilitar la creación de acciones de respuesta personalizadas con oportunidades de automatización, de modo que los equipos puedan desarrollar su seguridad a medida que pasa el tiempo.

Funciones y capacidades clave	Áreas de productos relacionados
• Responde rápidamente a las amenazas de los terminales cuando están en riesgo.	Detección y respuesta de terminales (EDR)
• Identifica y aísla la causa raíz de un problema o incidente de red en segundos.	Detección y respuesta extendidas (XDR), Detección y respuesta de red (NDR)
• Bloquea con rapidez los sitios web maliciosos con un análisis en tiempo real de los clics.	Seguridad del correo electrónico

Preguntas para hacer a los proveedores

- ¿Qué acciones de respuesta ofrece el producto?
- ¿Se puede realizar la corrección en el terminal mediante una solución de XDR en una ubicación y escalar a otras?
- ¿Cómo se integra el producto con las herramientas de seguridad existentes que permiten responder?
- ¿Cómo acelera la corrección su solución?
- Desde la alerta de amenazas hasta la corrección, ¿cuál es el tiempo de respuesta (por ejemplo, para un ataque de suplantación de identidad [phishing])?

4 Ofrece un único punto de vista de investigación para optimizar la experiencia del usuario

¿La detección, la respuesta y la corrección de amenazas se administran desde una sola interfaz?

Al evaluar las soluciones de XDR, es importante tener en cuenta la experiencia de los analistas de seguridad. Los equipos de SecOps tienen suficiente para administrar; no es necesario ralentizarlos con docenas de herramientas y una gran cantidad de consolas. Por eso que recomendamos las soluciones de XDR diseñadas para ayudar a los analistas a detectar y responder a las amenazas de manera más rápida y eficaz dado que ofrecen una visión unificada de los datos de seguridad a través de varias herramientas de seguridad y fuentes de datos. Esto puede ayudar a optimizar los flujos de trabajo y reducir el tiempo y el esfuerzo necesarios para investigar y corregir los incidentes de seguridad. Las soluciones de XDR deben ofrecer un tablero de ciclo de vida completo que cubra cada vector de amenaza y punto de acceso. Debe facilitar la búsqueda de amenazas a través de modelos tales como MITRE ATT&CK, que harán que la búsqueda de amenazas basada en hipótesis sea accesible para quienes son nuevos en el proceso y facilitará la anticipación de lo que vendrá a continuación. Otro factor a considerar es el impacto del diseño en la experiencia del analista. Debe elevar la productividad, mejorar los tiempos de toma de decisiones asociados a las funciones clave de detección, investigación y respuesta y capacitar a un analista principiante-intermedio para realizar tareas avanzadas dentro de las operaciones de seguridad al proporcionar un mejor contexto para las alertas con revelación progresiva para determinar rápidamente el alcance y la gravedad de una amenaza potencial.

Funciones y capacidades clave	Áreas de productos relacionados
• Ofrece un tablero de ciclo de vida completo que abarca todos los vectores de amenazas y puntos de acceso. • Ofrece un conjunto de herramientas unificado que se extiende a través de sus ITOps, SecOps y NetOps. • Tiene acceso y administra datos, análisis y automatización desde una ubicación unificada única.	Detección y respuesta extendidas (XDR)

Preguntas para hacer a los proveedores

- ¿Cómo ayuda su solución a mi equipo en sus esfuerzos de búsqueda de amenazas?
- ¿Cómo se integra la solución con las tecnologías de seguridad existentes, como las soluciones SOAR y SIEM?
- ¿Puedo usar su XDR para comprender el impacto de una amenaza, descubrir el alcance de la intrusión y tomar medidas con un solo clic desde una interfaz?
- ¿Su solución ofrece soporte para la seguridad basada en roles al restringir todo o parte del acceso al sistema/subsistema a grupos autorizados y usuarios individuales?
- ¿Puede centralizar y analizar la telemetría desde toda mi tecnología de seguridad existente?
- ¿Su solución optimiza los flujos de trabajo de respuesta a incidentes para reducir la línea de tiempo general de la investigación?

5 Brinda oportunidades para elevar la productividad y reforzar la postura de seguridad

¿Sus soluciones de XDR aumentan la eficiencia de respuesta y detección de amenazas con menos gastos generales?

Un elemento importante para desarrollar la ciberresiliencia de su empresa es la automatización y la orquestación. Su personal de seguridad tiene tareas importantes que realizar. Cuando se enfrentan a una amenaza de seguridad, no hay necesidad de desperdiciar el tiempo siguiendo flujos de trabajo complicados, manuales y repetitivos. Las soluciones de XDR que aumentan la productividad mediante la automatización de los flujos de trabajo críticos (como la detección de una alerta, la correlación, la priorización y la adopción de una acción de respuesta rápidamente) liberarán a sus equipos durante todo el ciclo de vida. Una solución de XDR eficaz debe reducir el tiempo promedio de respuesta al permitir que se lleve a cabo una investigación que presente decisiones y acciones claras para permitir que los analistas respondan de manera automatizada y uniforme de acuerdo con sus políticas y procedimientos. Esto significa que sus equipos de SecOps pueden invertir su tiempo y energía en tareas de seguridad más estratégicas y proactivas, lo que fortalece aún más la postura de seguridad de su empresa.

Funciones y capacidades clave	Áreas de productos relacionados
• Detección automática de amenazas en los terminales, incluidas las de baja prevalencia. • Permite que los administradores escriban y busquen indicadores de compromiso personalizados (IoC).	Detección y respuesta de terminales (EDR)
• Corrección predictiva de amenazas de red habilitada por información impulsada por análisis de comportamiento.	Detección y respuesta extendidas (XDR), Detección y respuesta de red (NDR)
• Prioriza de forma automática la corrección de amenazas de correo electrónico.	Seguridad del correo electrónico

Preguntas para hacer a los proveedores

- Para sus integraciones de terceros, ¿los cambios de API de los proveedores violan sus scripts de automatización?
- ¿Cómo admite su solución el monitoreo desde y hacia las cargas de trabajo basadas en la nube?
- ¿Necesitaré cambiar el entorno o implementar nueva tecnología con la solución de XDR?
- ¿Su solución XDR ofrece integraciones prediseñadas y listas para usar con tecnología de seguridad de terceros?
- ¿La solución de XDR reduce el tiempo que los analistas necesitan para investigar y resolver un incidente?
- ¿Su solución de XDR informa a la administración de políticas para desarrollar la resiliencia?

Cisco XDR

XDR es un componente crítico de la ciberresiliencia

Hoy, la incertidumbre es una garantía. En respuesta, las empresas están invirtiendo en la resiliencia en todos los aspectos de su empresa, desde las finanzas hasta las cadenas de suministro. Pero esto no será suficiente si no se invierte en ciberresiliencia, es decir, la capacidad de proteger su empresa contra las amenazas y las interrupciones, y de responder a los cambios con confianza para que pueda emerger aún más fuerte.

XDR es un componente crítico para adoptar la ciberresiliencia para su empresa. Si usa XDR correctamente, aumentará su postura de seguridad al permitir que los equipos de seguridad prioricen las amenazas en función de su impacto, las detecten antes y aceleren la respuesta. Las capacidades de automatización y orquestación facilitan este proceso, lo que libera a los equipos de seguridad para que puedan centrarse en lo que más importa.

El valor de un enfoque integrado

50 %
Menos costo y riesgo de vulneración de datos

90 %
De reducción de los esfuerzos de analistas por incidente

90 %
De aumento de la eficiencia de SecOps

85 %
De reducción de los tiempos de permanencia del ataque

Fuente: The Total Economic Impact (TEI) Of Cisco SecureX, julio de 2021

Operaciones de seguridad simplificadas con Cisco XDR

Cisco está liderando el camino hacia XDR con el portafolio de seguridad más completo del mercado. En Cisco, hemos invertido de manera proactiva en la creación del portafolio de seguridad más completo del mercado, anticipándonos a las necesidades de seguridad del futuro e integrando los componentes para que la seguridad eficaz sea simple y accesible para todos los equipos, independientemente del proveedor o el vector. Entendemos que desarrollar un enfoque XDR es un proceso y queremos que sus equipos salgan del círculo vicioso de la cobertura de parches de un sector sobresaturado con soluciones puntuales. Con Cisco XDR, nuestro objetivo es descubrir la ruta más corta desde la detección hasta la respuesta con la menor fricción.

Diseñado por expertos en SOC para expertos en SOC, Cisco XDR simplifica las operaciones de seguridad para ayudar a los analistas de seguridad a mantenerse proactivos y resistentes contra las amenazas más sofisticadas. Nuestra solución es abierta, extensible y orientada a la nube, lo que le permite aprovechar las inversiones en seguridad existentes y obtener una detección de seguridad unificada en todo su entorno.

En Cisco, nos tomamos en serio la responsabilidad de proteger los recursos de los clientes, ya que también somos clientes de nuestros clientes. Queremos asociarnos con usted en su proceso de ciberresiliencia a través de Cisco Security Cloud, una plataforma de seguridad abierta que lo ayuda a proteger todo su ecosistema, sin importar lo que venga después. Únase a nosotros y experimente el poder de la seguridad integral.

¿Está listo para desarrollar las operaciones de seguridad del mañana, hoy mismo?

Explore Cisco XDR

Elementos y funcionalidades clave de XDR

Use esta tabla (páginas 9 a 10) como referencia rápida durante las conversaciones con los proveedores de XDR.

Elemento clave	Funcionalidades clave	Productos Cisco alineados
Ofrece telemetría priorizada y procesable, donde sea que la necesite	• Detección y respuesta de terminal (EDR) integrada que puede ser totalmente administrada, búsqueda proactiva de amenazas. • Administración de vulnerabilidades basada en riesgos integrada que permite una rápida identificación de vulnerabilidades, puntuación de riesgos, priorización y corrección.	Secure Endpoint
	• Análisis continuo de la actividad de la nube. • Análisis avanzado que incluye modelado de comportamiento y algoritmos de aprendizaje automático. • Una visión de toda su infraestructura de seguridad para una visibilidad unificada e inteligencia agregada y procesable.	Cisco XDR
	• Filtros de ataques masivos avanzados con análisis en tiempo real de los clics.	Secure Email
Permite la detección unificada, con independencia del vector o el proveedor	• Detección y bloqueo en tiempo de ejecución de comportamientos anormales del programa en ejecución. • Capacidad para realizar consultas avanzadas sobre el sistema operativo en el terminal en tiempo real. • Búsqueda de amenazas integrada que se asigna al marco ATT&CK de MITRE.	Secure Endpoint
	• Detecta los ataques en tiempo real en la nube con alertas de alta fidelidad enriquecidas con el contexto, como los usuarios, los dispositivos, la ubicación, la marca de hora y las aplicaciones. • Detecta y aísla amenazas con detecciones confirmadas. • Detecta entidades dudosas con NDR y automatiza la cuarentena con terminales. • Detecta hosts internos que se comunican con un host externo. • Ofrece un histórico de operaciones completo de todas las transacciones en la nube para realizar investigaciones forenses más eficaces. • Integraciones incorporadas a otras soluciones de XDR en el portafolio. • Se incorpora con soluciones de terceros a través de integraciones incorporadas, preempaquetadas o personalizadas para obtener una arquitectura de backend conectada y una experiencia de frontend uniforme. • Integraciones incorporadas con otras tecnologías en la nube, terminales, redes y aplicaciones (incluidas tecnologías de terceros).	Secure Network Analytics y Cisco XDR
	• Antispam, protección y control relacionados con URL, análisis de virus de alto rendimiento, filtros de ataque masivo y análisis de reputación para la funcionalidad de dominio. • Detección correos electrónicos falsificados para proteger contra los ataques BEC dirigidos a ejecutivos. • Análisis de malware automatizado y sandboxing.	Secure Email
Permite responder a las amenazas con rapidez y precisión	• Accede a la protección siempre activa con inteligencia de amenazas e información combinada procedentes de centros de operaciones de seguridad (SOC) globales especializados para una amplia base de clientes.	Todos los productos de Cisco Secure

Elementos y funcionalidades clave de XDR

Elemento clave	Funcionalidades clave	Productos Cisco alineados
Permite responder a las amenazas con rapidez y precisión (cont.)	· Accede a la protección siempre activa con inteligencia de amenazas e información combinada procedentes de centros de operaciones de seguridad (SOC) globales especializados para una amplia base de clientes.	Todos los productos de Cisco Secure
	· Monitoreo continuo de toda la actividad del terminal que proporciona detección en tiempo de ejecución y bloqueo de comportamientos anormales.	Secure Endpoint
	· Identifica y aísla amenazas en el tráfico cifrado sin comprometer la privacidad ni la integridad de los datos. · Activa flujos de trabajo de "respuesta" desde una ubicación. · Respuesta a amenazas que agrega reconocimiento contextual de fuentes de datos de productos de seguridad junto con inteligencia de amenazas global de Talos® y fuentes de terceros a través de las API. · Crea registros de casos de investigación de incidentes forenses.	Cisco XDR
	· Protección persistente contra amenazas basadas en URL mediante el análisis en tiempo real de enlaces potencialmente maliciosos. · Aprovechamiento continuo del monitoreo, el análisis y la inteligencia de amenazas de Talos® en tiempo real para identificar amenazas previamente desconocidas o cambios repentinos.	Secure Email
Ofrece un único punto de vista de investigación para optimizar la experiencia del usuario	· Recopila y correlaciona inteligencia global en una sola vista, lo que permite una investigación de amenazas acelerada. · Crea acciones de respuesta personalizadas para reducir el tiempo de respuesta. · Automatiza el enriquecimiento desde varias fuentes de datos, superpuesto con inteligencia de amenazas.	Cisco XDR
Brinda oportunidades para elevar la productividad y reforzar la postura de seguridad	· Identificación automática y análisis de amenazas de ejecutables de baja prevalencia. · Capacidad de escribir IoC personalizados para buscar indicadores posteriores al compromiso en toda la implementación de terminales.	Secure Endpoint
	· Modelización del comportamiento, aprendizaje automático multicapa e inteligencia de amenazas global. · Clasifica automáticamente los nuevos roles de dispositivos mientras se agregan a la red. · Integración con una solución XDR para permitir la automatización en todos los vectores de amenazas y puntos de acceso.	Secure Network Analytics y Cisco XDR
	· Activa automáticamente análisis dinámicos de la reputación y brinda visibilidad sobre dónde se originó el malware de correo electrónico, qué sistemas se vieron afectados y qué está haciendo el malware. · Toma medidas sobre el correo electrónico entrante y saliente según la información de corrección.	Secure Email
	· Automatiza las tareas de rutina mediante flujos de trabajo creados previamente que se alinean con los casos de uso comunes. · Comparte cuadernos de estrategias entre equipos de SecOps. · Evaluación y priorización automatizadas de las alertas de otras soluciones de portafolio de seguridad.	Cisco XDR

Sede central en América
Cisco Systems, Inc.
San José, CA

Sede central en Asia Pacífico
Cisco Systems (EE. UU.) Pte. Ltd.
Singapur

Sede en Europa
Cisco Systems International BV Amsterdam,
Países Bajos