## Talos
(está incluido al adquirir cualquier solución de Seguridad)

Cisco Talos es nuestro grupo de inteligencia amenazas y es fundamental para nuestra completa arquitectura de seguridad. Ya que nos va a brindar la inteligencia en nuestras soluciones. Incluye la mayor red de detecciónde amenazas del mundo.

- Talos es reconocido líder en la detección de amenazas validado por NSS Labs.
- Con más de 250 ingenieros altamente calificados, dedicados al análisis de amenazas, ingenieros de investigación de vulnerabilidad de día cero.
- Talos analiza el 35% del correo a nivel mundial.
- Identifica 50 mil intrusiones de red por día, y actualiza automáticamente con las soluciones de Cisco.

## AMP
(Advance Malware Protection)

Es nuestra solución contra amenazas avanzadas. Como sabemos, los antivirus y los firewalls hacen su tarea, pero en esta época ya no son suficientes, sabemos que hay amenazas avanzadas que un Av no va a poder bloquear.
Para eso es necesario una solución como AMP que nos va a permitir hacer un detección y eliminación del malware avanzado, ya que supervisa continuamente la actividad de los archivos revisando cualquier comportamiento anómalo o malicioso, analiza la trayectoria del archivo, logrando identificar el cuándo, dónde y cómo ocurrió un ataque.
Adicional vamos a poder enviar a un análisis de sandboxing esos archivos que están en la zona gris (no tenemos claridad si es un archivo malicioso o no).

## Umbrella

Cisco Umbrella es una solución basada en la nube, es la primera línea de defensa contra amenazas en Internet. La forma de trabajar ha venido cambiando mucho, ahora nuestros usuarios ya no solo trabajan desde la oficina, se conectan de diferentes partes (hotel, casa, café internet) con Umbrella van a poder estar protegidos desde donde estén, sin necesidad de conectarse a un VPN.

Con Cisco Umbrella, vamos a poder detener las infecciones de phishing, malware y callbacks mediante el bloqueo en la capa DNS, Umbrella bloquea las solicitudes de cualquier puerto y protocolo.

## Cloudlock

Cisco Cloud Security permite adoptar la nube de forma segura. Protege a los usuarios de las amenazas cuando acceden a Internet y protege los datos y las aplicaciones en la nube.

CloudLock es una plataforma que se ejecuta en la nube, que tiene diferentes servicios de seguridad.

CloudLock ofrece seguridad en la nube para ayudar a rastrear y controlar el comportamiento del usuario y los datos confidenciales de las aplicaciones SaaS como Office365, Google Drive y Salesforce.

## ISE
(Identity Service Engine)

ISE nos permite autenticar los dispositivos que ingresan a la red. Vamos a tener la capacidad de identificar el contexto: Quién, Qué, Cuándo, En dónde, Cómo, y generar políticas de acesso, perfiles, tener la capacidad de segmentar muy bien la red y controlar los recursos de la red.

## Cisco Web Security

Cisco ofrece una fuerte protección de Web y muy granular.

- Filtrado de URL
- Antimalware
- Reputación de web
- Controles por horario.

## Firepower

Con el FW vamos a controlar lo que nuestros usuarios hacen hacia Internet.

- Controlar aplicaciones.
- Categorías de URL.
- Aplicaciones web.
- Además de servicios de IPS y control del malware avanzado.

El beneficio principal de esta solución es la visibilidad que nos va a dar. Nuestro Firewall de la próxima generación detecta de forma única las aplicaciones y los sistemas operativos del cliente, los tipos de dispositivos móviles y los navegadores que utilizan, las comunicaciones de la máquina virtual y los dispositivos de red, detectando las formas más recientes y avanzadas de malware.

## Stealthwatch
(No solo aplica para el área de Seguridad también a Infraestructura de Red)

Utilizar la red como sensor, la red es muy relevante para la seguridad y quien mejor que Cisco para conocer la red.
Stealthwatch nos permite tener la Visibilidad completa de la red y poder realizar un análisis de la seguridad. Podrá ver todo lo que ocurre en la red y el centro de datos. (Utiliza el protocolo de Netflow).Stealthwatch nos va a permitir detectar cualquier trafico anómalo, o comportamiento anómalo (como un tráfico excesivo de red o comunicaciones entre partes inusuales), lo que nos permite identificar las amenazas en tiempo real.

## Cisco E-mail Security

El correo es uno de los principales vectores de entrada de una amenaza.
Con esta solución vamos a poder analizar los correos tanto entrante como saliente, en el entrante vamos a realizar:

- Filtro de spam.
- Phishing.
- Url maliciosas.
- Reputación de correo.

En el saliente tenemos capacidades de DLP para información confidencial que no deba salir de la organización y cifrado.

# Preguntas motivadoras

Todas las preguntas están formuladas como una introducción al ransomware y la necesidad de un enfoque de seguridad por capas. Después de las preguntas, puede examinar los componentes de la solución y cómo cumplirán con las necesidades del cliente.

| Pregunta motivadora | Solución de Cisco – Con Cisco puede |
|---|---|
| ¿Considera que su seguridad de TI actual lo protege del ransomware? | Cisco cree que para reducir el riesgo de infecciones de ransomware, sus medidas de seguridad requieren un enfoque basado en el portafolio, en lugar de un solo producto.<br><br>El ransomware se debe evitar siempre que sea posible, y se lo debe detectar si obtiene acceso a sistemas y contener para limitar daños.Cisco Ransomware Defense aplica la arquitectura de seguridad de Cisco para proteger empresas mediante defensas que abarcan desde redes, pasando por la capa DNS y el correo electrónico, hasta el terminal. Está respaldado por las investigaciones líderes de amenazas de Talos por la última capacidad de respuesta con ransomware. |
| ¿Sabía que la mayoría de los ataques de ransomware utilizan DNS para obtener acceso a su red? | Las soluciones de Cisco Umbrella bloquean las amenazas de ransomware en la capa DNS e impiden que el ataque obtenga acceso a su red,sistemas y archivos críticos. Cisco Umbrella se instala rápidamente y brinda protección contra la mayoría de los ataques conocidos de ransomware. |
| Si se ve afectado, ¿confía en su tiempo de detección y corrección? | Ransomware Defense consiste en tecnologías que bloquean amenazas, de la capa DNS a la red y la terminal, con Cisco Umbrella, Cisco AMP para terminales, la seguridad de correo electrónico de Cisco y NGFW de Cisco Firepower. También puede segmentar su red implementando políticas de Cisco ISE en la red y utilizando Cisco TrustSec® para contener el ataque para que el ransomware no se pueda propagar lateralmente. Con Cisco AMP integrado en todas partes (en el terminal, en la seguridad de correo electrónico y en la red con nuestro NGFW), las organizaciones pueden reducir el tiempo de detección de días a minutos. Con Ransomware Defense, las organizaciones pueden usar su red como guardián para contener la propagación de ransomware. No será capaz de propagarse tan fácilmente en la red en el peor de los casos de que se produzca una infección. |

# Tratamiento de las objeciones

| Objeción | Cómo responder |
|---|---|
| Nunca he oído hablar de Ransomware Defense. ¿Cisco es nuevo en este negocio?<br>¿Es la seguridad una prioridad de Cisco? Solo sé que venden routers, switches, etc. | Cisco ha invertido significativamente en las mejoras y la postura de sus soluciones de seguridad. La solución de Ransomware Defense es relativamente nueva, pero la necesidad de una defensa ante amenazas integrada no lo es. La solución combina años de avances en investigación y productos en una solución integral que lo protegerá de la red a la capa DNS, el correo electrónico y el terminal. Está respaldado por las investigaciones líderes de amenazas de Talos por la última capacidad de respuesta con ransomware. |
| Tenemos un presupuesto limitado. Analicé Cisco en el pasado, y sus productos de seguridad parecen más costosos que otras soluciones. | ¿Ha pensado en financiar a través de Cisco Capital®? El financiamiento es muy flexible. Puede optar por diferir los pagos para reflejar mejor su retorno de la inversión y comenzar a pagar una vez que la tecnología esté en funcionamiento. Cisco Capital lo ayuda a impulsar sus inversiones en tecnología para fomentar el crecimiento de su negocio y ofrece una solución de financiamiento adaptada a sus necesidades específicas. Cisco Capital puede financiar toda la solución (hardware, software, servicios y equipos complementarios de terceros). Para más información acerca de las opciones de financiamiento visite www.ciscocapital.com. |
| Ya tengo un firewall y otros excelentes productos y servicios de seguridad. ¿Qué diferencia a la solución de Cisco de los productos que me protegen actualmente? | Cisco cree que para reducir el riesgo de infecciones de ransomware, sus medidas de seguridad requieren un enfoque basado en el portafolio, en lugar de un solo producto. Si ya tiene un firewall Cisco o un AMP, puede simplemente agregar el resto de la solución a sus defensas.<br><br>Cisco Ransomware Defense aplica la arquitectura de seguridad de Cisco para proteger empresas mediante defensas que abarcan desde la red, a la capa DNS, el correo electrónico y el terminal. Está respaldado por las investigaciones líderes de amenazas de Talos por la última capacidad de respuesta con ransomware.<br><br>Desde aquí, puede dirigirse a los temas de conversación de productos, incluidos en “Temas de conversación.” |
| Actualmente ya tengo [xx] cantidad de productos de seguridad de Cisco. ¿Me protegerán contra el ransomware? | Sus productos de seguridad existentes sin dudas lo ayudarán a estar protegido. Sin embargo, los ataques de ransomware están evolucionando a un ritmo rápido. Solo sus vectores de ataque aumentan a medida que el malware se vuelve más sofisticado.<br><br>Debido a esto, la solución Ransomware Defense abarca varios productos que le darán la protección en la capa DNS, la red, el correo electrónico, la web y los terminales. Junto con Talos, nuestra investigación de amenazas líder en el sector, implementar la solución completa disminuye sus oportunidades de ataque significativamente. |
| Con el rápido crecimiento de la tecnología de ransomware, aún existe la posibilidad de que pueda estar infectado. ¿Qué sucede luego? | En el peor de los casos de que se produzca una infección, la segmentación dinámica con Cisco TrustSec (a través de una red como sensor y una red como guardián) puede impedir que el ransomware se propague ampliamente una vez dentro de la red. Esto es vital para garantizar que no pueda ejecutarse de manera descontrolada en una red y afectar a la mayoría de los sistemas. Los servicios de protección contra malware de Cisco (AMP mas Threat Grid) proporcionan la capacidad de eliminar el malware retrospectivamente de terminales en donde se lo ha detectado. Esto significa que en el peor de los casos, uno o dos terminales pueden verse afectadas mientras se produce el aprendizaje, y luego el enfoque exhaustivo de defensa elimina el malware de terminales en donde puede permanecer inactivo. |
| ¿Qué sucede con la seguridad para las sucursales? | Para las sucursales que deseen acceso directo a Internet aunque también protección contra ransomware, se puede instalar Umbrella Branch en el router de servicios integrados Cisco (ISR) en las sucursales para una capa inicial de protección.<br>También se puede activar la defensa contra amenazas Cisco Firepower ISR con AMP incluida, lo cual hace que la seguridad de las sucursales sea tan fuerte como la de la oficina principal. Ambas reducen los costos de WAN sin necesidad de devolver tráfico. |