Cisco Ransomware Defense

Guía de llamadas

Cisco Ransomware Defense

Objetivo

Esta guía de llamadas está diseñada con el fin de presentar un conjunto de preguntas introductorias que lo ayudarán a descubrir oportunidades de Cisco® Ransomware Defense. Puede ayudarlo a planificar y ejecutar un enfoque de clientes potenciales, a adecuarse efectivamente a sus términos y a pasar a la concreción de la venta cuando la oportunidad parezca conveniente.

Su objetivo principal es determinar si debe dedicarle una conversación a un cliente, ya sea ahora o en el futuro. Si percibe una oportunidad inmediata, el resultado que debe buscar es una reunión para comprender los desafíos y oportunidades del cliente.

Organizaciones y público objetivo

La solución Cisco Ransomware Defense está dirigida a pequeñas y medianas empresas comerciales, y a grandes clientes del sector público que necesitan soluciones de seguridad integrales para proteger sus organizaciones de amenazas. Hoy en día, cada organización de cada sector es un blanco de ataque.

Los centros de compra de seguridad también son variados. Los destinatarios principales de Cisco Ransomware Defense son los administradores de seguridad de TI, los directores de seguridad informática, los responsables de brindar una respuesta ante incidentes y el equipo a cargo de la seguridad general de una organización. Sin embargo, dado que ahora la seguridad es un tema de conversación en la sala de juntas y que la seguridad se está implementando de los terminales a la red, usted deberá buscar la participación de otros equipos además del de seguridad. Otros centros de compras incluyen el equipo de escritorio y terminales, el equipo de redes, el director de informática, el gerente de operaciones e incluso el gerente general.

¿Por qué comprometerse?

Consiga clientes nuevos

- Todas las organizaciones necesitan seguridad. Capte nuevas oportunidades compartiendo la propuesta de valor de Cisco Ransomware Defense: Cisco Ransomware Defense reduce el riesgo de infecciones de ransomware mediante un enfoque por capas, de la capa DNS al terminal, el correo electrónico y la web. Cisco ofrece defensas integradas con un enfoque arquitectónico que combina máxima visibilidad con máxima capacidad de respuesta contra el ransomware.

Migre a los clientes

- Migre a los clientes que actualmente estén usando antivirus, firewalls, sistemas de prevención de intrusiones (IPS) y dispositivos de seguridad web y de correo electrónico de competidores como FireEye, Palo Alto Networks, Lastline, Trend Micro, Symantec, McAfee, Check Point y Fortinet, entre otros.
- Migre a los clientes que usan productos de la competencia y que no están satisfechos con su proveedor actual, tienen una suscripción que debe actualizarse, o tienen un producto que está llegando al fin de su vida útil.
- Migre a los clientes que usan productos de seguridad de la competencia y que, a pesar de ello, sufrieron un ataque a la seguridad.

Realice ventas incrementales a los clientes actuales de Cisco

- Realice ventas incrementales de Cisco Ransomware Defense a los clientes que tengan cualquier nivel de productos Cisco en su arquitectura de red, incluso fuera de la seguridad. Cisco crea herramientas de seguridad que se comunican entre sí y con otra tecnología de Cisco para proporcionar seguridad en todas partes mediante diversos vectores de ataque (terminal, red, dispositivo móvil, web, correo electrónico, nube). La implementación de ofertas fragmentadas de diversos proveedores puede causar una disminución de la comunicación entre los productos aislados, retrasar la detección y elevar el costo total para desarrollar, administrar y resolver problemas.
- Venda el valor del enfoque de soluciones optimizadas de Cisco. Nuestras herramientas están integradas, se comunican y comparten información, proporcionan un tiempo de detección más rápido, pueden reducir gastos operativos y son más fáciles de administrar a través de un proveedor confiable. Para obtener más información sobre el enfoque de seguridad en todas partes de Cisco, consulte estos materiales: Perspectivas ejecutivas de Cisco sobre seguridad y el Informe técnico sobre seguridad en todas partes.

Puntos de discusión

La solución comprende los siguientes componentes principales:

- *Cisco Umbrella* protege los dispositivos dentro y fuera de la red corporativa. Bloquea las solicitudes DNS antes de que un dispositivo siquiera pueda conectarse a sitios maliciosos que alojan ransomware.
- *Cisco Advanced Malware Protection (AMP) para terminales* evita que los archivos de ransomware se ejecuten en terminales.
- *La seguridad de correo electrónico de Cisco con Advanced Malware Protection (AMP)* bloquea correos electrónicos no deseados y de suplantación de identidad y adjuntos de correo electrónico y URL maliciosos. La tecnología es la misma que la que se aplica en el terminal, pero se implementa en la gateway de correo electrónico.
- *El firewall de próxima generación de Cisco Firepower con Advanced Malware Protection (AMP) y la tecnología de sandboxing* Cisco Threat Grid detiene las amenazas impidiendo el ingreso de malware conocido y desconocido y bloqueando devoluciones de llamadas de comando y control a hosts de ransomware.
- *Los servicios de seguridad de Cisco* proporcionan una clasificación inmediata en caso de incidentes. También optimizan las implementaciones de AMP, NGFW y demás productos de la solución.

© 2016 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información confidencial de Cisco. Para uso exclusivo de los partners de canal. Se prohíbe su distribución.

Posicionamiento competitivo

- El mercado de seguridad en general está fragmentado, con muchos proveedores de productos puntuales cuyos productos independientes se enfocan en solo una parte de la red, lo que provoca una seguridad dispar.
- Solo Cisco ofrece una arquitectura de seguridad para abordar el desafío de ransomware. Los productos puntuales no son suficientes. Nuestra solución está respaldada por nuestro Grupo de Investigación Talos líder en la industria, el cual realizó una amplia investigación de amenazas de ransomware, alimentando así nuestro efectivo modelo de protección por capas.

Introducción

Hola, [nombre de contacto]: Mi nombre es [su nombre] y llamo en representación de Cisco y [nombre del partner]. ¿Tiene unos minutos para conversar?

Estoy seguro de que ha escuchado historias en los medios sobre el rápido aumento de ataques de ransomware. Solo quería informarle sobre la completa solución de arquitectura de Cisco, Ransomware Defense. ¿Puedo preguntarle [use las preguntas motivadoras a continuación]?

Nuestra solución proporciona [use el correspondiente bloque de texto de soluciones de Cisco a continuación].

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. 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.

© 2016 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información confidencial de Cisco. Para uso exclusivo de los partners de canal. Se prohíbe su distribución.

Tratamiento de las objeciones

Objeción	Cómo responder
Nunca he oído hablar de Ransomware Defense. ¿Cisco es nuevo en este negocio?	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.
¿Es la seguridad una prioridad de Cisco? Solo sé que venden routers, switches, etc.	
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. 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. 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. 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. ¿Puedo preguntarle qué productos ya implementó? (Compare y contraste con la lista de productos de la solución en “Temas de conversación).
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. 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.

© 2016 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información confidencial de Cisco. Para uso exclusivo de los partners de canal. Se prohíbe su distribución.

Ofertas de interés para los clientes

Etapa de compra del cliente	Objetivos	Oferta – Llamado a la acción
Reconocimiento	Establezca relaciones y edúquelos acerca de la tecnología y las soluciones de Cisco.	– Resumen de Ransomware Defense – Infografía de Ransomware
Consideración y evaluación	Evalúe las necesidades, demuestre el valor de la tecnología de Cisco y ayude al cliente a comprender cómo se compara con la competencia.	– Informe técnico “Ransomware: Todo lo que necesita saber” – Descripción general de la solución Ransomware Defense
Diseño	Proporcione los recursos de diseño y ayude al cliente a comprender mejor cómo implementar esta solución.	– Informe técnico “Ransomware: una defensa por capas” – Demostración y Webinar grabados
Compra	Cierre la venta. El cliente está listo para comprar.	– La Id. de la solución Ransomware Defense se encuentra en Cisco Commerce Workspace (CCW).

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)

© 2016 Cisco y/o sus filiales. Todos los derechos reservados. Este documento es información confidencial de Cisco. Para uso exclusivo de los partners de canal. Se prohíbe su distribución.