Log in

Hoja de datos de Cisco Secure Endpoint

Actualizado: 24 de octubre de 2022

Lenguaje libre de sesgos

Descripción del producto

Cisco® Secure Endpoint integra capacidades de prevención, detección, búsqueda de amenazas y respuesta en una solución unificada que aprovecha el poder del análisis basado en la nube. Secure Endpoint protegerá sus dispositivos Windows, Mac, Linux, Android e iOS a través de una implementación de nube pública o privada.

Cisco Secure Endpoint es una solución de un solo agente que brinda protección integral, detección, respuesta y cobertura de acceso de usuarios para defenderse de las amenazas a sus terminales. La plataforma SecureX™ está integrada en Secure Endpoint, así como las capacidades de detección y respuesta extendidas (XDR). El recientemente presentado Cisco Secure MDR para Endpoint combina las capacidades superiores de Secure Endpoint con la experiencia en operaciones de seguridad para reducir drásticamente el tiempo medio para detectar y responder a las amenazas.

Beneficios

En el mundo del malware en rápida evolución, las amenazas son cada vez más difíciles de detectar. El 1% más avanzado de estas amenazas, aquellas que eventualmente ingresarán y causarán estragos en su red, podrían pasar desapercibidas. Sin embargo, Secure Endpoint ofrece una protección completa contra ese 1 %. Secure Endpoint previene las infracciones, bloquea el malware en el punto de entrada y monitorea y analiza continuamente la actividad de archivos y procesos para detectar, contener y remediar rápidamente las amenazas que pueden evadir las defensas de primera línea.

El recientemente presentado Cisco Secure MDR para Endpoint agrega valor adicional al combinar inteligencia humana y de máquinas, aprovechando un equipo de élite de investigadores de seguridad de Cisco, investigadores y respondedores que utilizan inteligencia de amenazas integrada, investigaciones definidas y manuales de respuesta respaldados por la investigación de amenazas de Cisco Talos.

Podemos identificar y luego detener amenazas, bloquear malware y contener y recomendar acciones de remediación incluso para amenazas avanzadas que evaden las defensas de primera línea las 24 horas del día, los 7 días de la semana, los 365 días del año desde nuestros Centros de operaciones de seguridad (SOC) globales dedicados.

Prevención

Detener las amenazas en el momento más temprano garantiza un daño mínimo a los puntos finales y menos tiempo de inactividad después de una infracción. Secure Endpoint emplea un sólido conjunto de tecnologías preventivas para detener el malware, en tiempo real, protegiendo los puntos finales contra los ataques más comunes de la actualidad, así como también contra las ciberamenazas emergentes.

Reputación de archivos: Secure Endpoint contiene una base de datos completa de todos los archivos que se han visto y una buena o mala disposición correspondiente. Como resultado, el malware conocido se pone en cuarentena de forma rápida y sencilla en el punto de entrada sin necesidad de realizar un análisis intensivo del procesador.

Antivirus: Secure Endpoint incluye motores antivirus basados en definiciones que se actualizan constantemente para puntos finales de Windows y Mac o Linux. Todos los puntos finales se benefician de la detección personalizada basada en firmas, lo que permite a los administradores ofrecer sólidas capacidades de control y hacer cumplir las listas de bloqueo. La base de datos de firmas antivirus reside localmente en cada punto final, lo que significa que no depende de la conectividad en la nube para funcionar. Esto garantiza que sus terminales estén protegidos tanto en línea como fuera de línea.

Detección de malware polimórfico: los actores de malware a menudo escriben diferentes variaciones del mismo malware para evitar las técnicas de detección comunes. Secure Endpoint puede detectar estas variantes o malware polimórfico a través de huellas dactilares sueltas. Las huellas dactilares sueltas buscarán similitudes entre el contenido del archivo sospechoso y el contenido de familias de malware conocidas, y condenarán si hay una coincidencia sustancial.

Análisis de aprendizaje automático: Secure Endpoint está entrenado por algoritmos para "aprender" a identificar archivos y actividades maliciosos en función de los atributos del malware conocido. Las capacidades de aprendizaje automático en Secure Endpoint se alimentan del completo conjunto de datos de Cisco Talos™ para garantizar un modelo mejor y más preciso. Juntos, el aprendizaje automático en Secure Endpoint puede ayudar a detectar malware nunca antes visto en el punto de entrada.

Prevención de exploits: los ataques a la memoria pueden penetrar los puntos finales y el malware evade las defensas de seguridad al explotar las vulnerabilidades en las aplicaciones y los procesos del sistema operativo. La función de prevención de exploits defenderá los puntos finales de los ataques de inyección de memoria basados en exploits.

Protección de secuencias de comandos: Secure Endpoint proporciona una visibilidad mejorada en la trayectoria del dispositivo de las secuencias de comandos que se ejecutan en sus puntos finales y ayuda a proteger contra los ataques basados en secuencias de comandos

comúnmente utilizados por el malware. El control de secuencias de comandos brinda protección adicional al permitir que el motor de prevención de vulnerabilidades evite que algunas aplicaciones de escritorio comúnmente explotadas y sus procesos secundarios carguen ciertas DLL.

Protección del comportamiento: el análisis de comportamiento mejorado de Secure Endpoint monitorea continuamente toda la actividad de los usuarios y puntos finales para proteger contra el comportamiento malicioso en tiempo real comparando un flujo de registros de actividad con un conjunto de patrones de actividad de ataque que se actualizan dinámicamente a medida que evolucionan las amenazas. Por ejemplo, esto permite el control granular y la protección contra el uso malicioso de herramientas de vida fuera de la tierra.

Detección

Si bien las técnicas de prevención de malware son necesarias para una solución completa de seguridad de punto final de próxima generación, combatir las amenazas avanzadas requiere medidas adicionales. Secure Endpoint monitorea continuamente los puntos finales para ayudar a detectar amenazas nuevas y desconocidas.

Protección contra actividades maliciosas: Secure Endpoint monitorea continuamente toda la actividad de los puntos finales y brinda detección en tiempo de ejecución y bloqueo del comportamiento anormal de un programa en ejecución en el punto final. Por ejemplo, cuando el comportamiento del endpoint indica ransomware, los procesos ofensivos se terminan, lo que impide el cifrado del endpoint y detiene el ataque.

Indicadores de compromiso basados en la nube: la organización de inteligencia de amenazas líder en la industria de Cisco, Talos, analiza constantemente el malware para descubrir nuevos tipos de amenazas y crear perfiles forenses y de comportamiento para amenazas emergentes, también conocidos como indicadores de compromiso (IoC). Los datos forenses, como las ubicaciones de los archivos o las modificaciones de los valores de las claves del registro, son todos datos que Secure Endpoint puede usar para ayudar a los administradores a identificar los sistemas que han sido violados.

IoC basados en host: los administradores pueden escribir sus propios IoC personalizados para usarlos en la respuesta a incidentes para buscar indicadores posteriores al compromiso en toda la implementación del punto final. Los IoC personalizados están escritos en un formato estándar abierto (OpenIOC), lo que facilita el aprovechamiento de los datos de cualquier fuente de inteligencia existente.

Vulnerabilidades: para los clientes en Advantage o Premier Tier, Secure Endpoint se integra con Kenna Security para identificar las vulnerabilidades del sistema operativo en su entorno para ayudar a reducir la superficie de ataque. Los endpoints que tienen vulnerabilidades se marcan con una puntuación de riesgo, lo que permite a los administradores priorizar la reparación.

Prevalencia baja: Secure Endpoint identificará automáticamente los archivos ejecutables que existen en cantidades bajas en sus puntos finales y analizará esas muestras en nuestro espacio aislado basado en la nube para descubrir nuevas amenazas. El malware dirigido o las amenazas

persistentes avanzadas a menudo pasarán desapercibidos y comenzarán solo en unos pocos endpoints, pero con una prevalencia baja, Secure Endpoint buscará amenazas automáticamente para ayudar a descubrir fácilmente el 1 % de las amenazas que, de otro modo, habrían pasado desapercibidas.

Caza de amenazas

SecureX Threat Hunting es un enfoque proactivo centrado en el analista para detectar amenazas avanzadas ocultas. Esta capacidad se ofrece exclusivamente como parte del nuevo nivel de licencia Premier dentro de Secure Endpoint. Les dice a los respondedores de incidentes una narración de cómo se detectó un ataque o cómo evolucionó y qué hacer a continuación en términos de respuesta. El propósito es descubrir y frustrar los ataques antes de que causen algún daño. Como efecto secundario de aprovechar una búsqueda de amenazas regular y continua, una organización aumenta su conocimiento de las vulnerabilidades y los riesgos, lo que permite fortalecer aún más su entorno de seguridad.

SecureX Threat Hunting aprovecha la experiencia tanto de Talos como del equipo de investigación y eficacia de Cisco para ayudar a identificar las amenazas que se encuentran en el entorno del cliente. Cisco ofrece búsquedas impulsadas por humanos altamente automatizadas basadas en libros de jugadas que producen alertas de alta fidelidad. El proceso combina de manera única la tecnología Orbital Advanced Search con la experiencia de cazadores de amenazas de élite, con 20 años de experiencia en la industria, para encontrar proactivamente amenazas más sofisticadas.

La licencia Secure Endpoint Premier está disponible para pedidos a nivel mundial en todas las regiones. Sin embargo, la infraestructura SecureX Threat Hunting que procesa la telemetría del cliente y ejecuta búsquedas actualmente solo está disponible en América del Norte.

Respuesta de punto final seguro

A medida que aumenta el número y la variedad de amenazas avanzadas diseñadas para eludir las medidas preventivas, la posibilidad de una infracción debe tratarse como una eventualidad. Con esa mentalidad, se debe implementar un poderoso conjunto de herramientas para ayudar a identificar fácilmente los puntos finales infectados y comprender el alcance de un ataque. Además de múltiples capacidades de prevención y

detección, Secure Endpoint ofrece visibilidad granular de puntos finales y herramientas de respuesta para manejar las infracciones de seguridad de manera rápida y eficiente.

Tableros y bandeja de entrada: los informes no se limitan a la enumeración y agregación de eventos. Los paneles accionables integrados en Secure Endpoint permiten una gestión optimizada y una respuesta más rápida. Los eventos y puntos finales se clasifican por prioridad y se vinculan a flujos de trabajo para realizar un seguimiento del progreso durante la investigación.

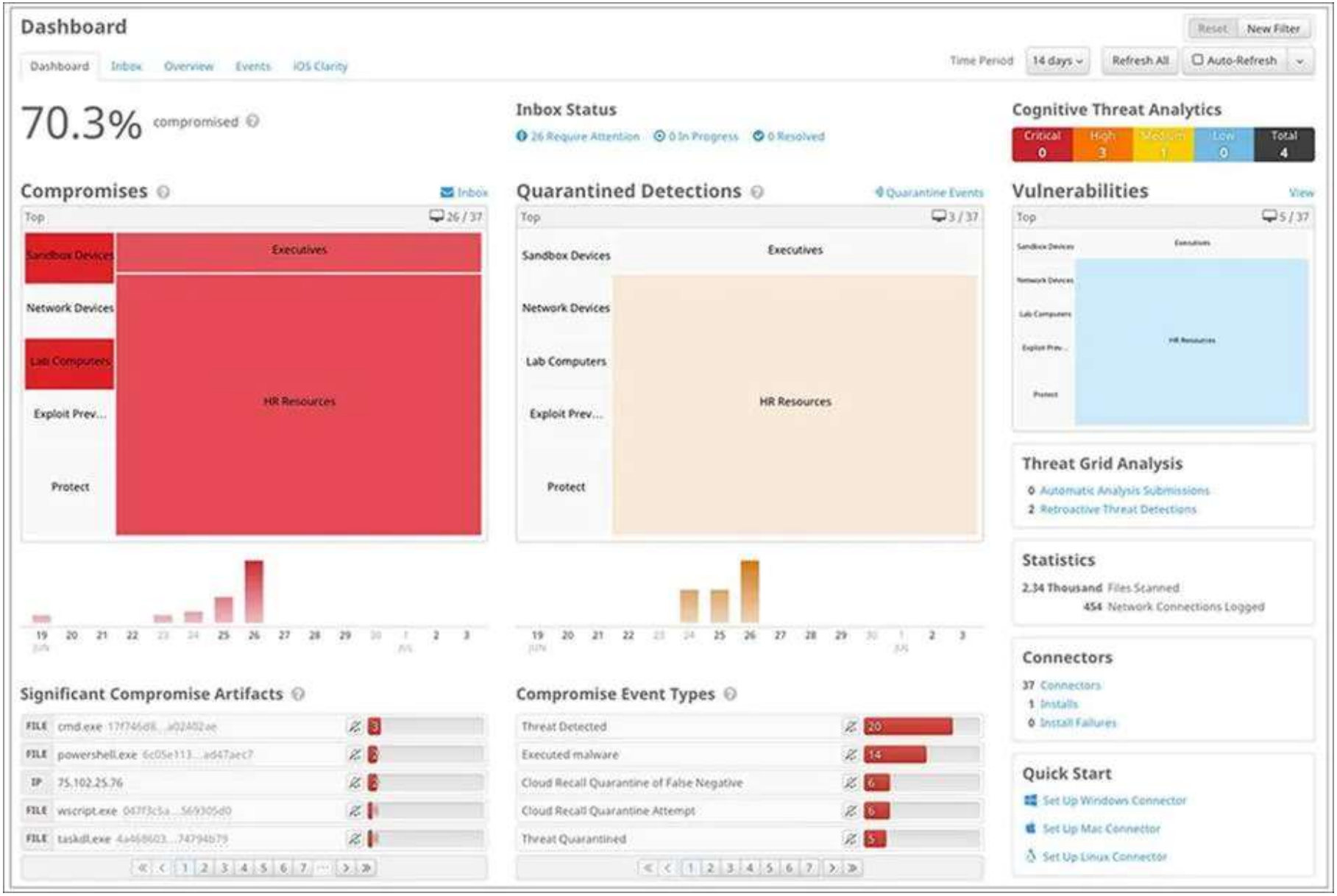

Figura 1.

Panel de control de punto final seguro

Análisis forense de endpoints: potentes herramientas como la trayectoria de archivos y la trayectoria de dispositivos utilizan las capacidades de análisis continuo de Secure Endpoint para mostrarle el alcance completo de una amenaza. Secure Endpoint identifica todas las aplicaciones, procesos y sistemas afectados para identificar al paciente cero, así como el método y el punto de entrada. Estas capacidades lo ayudan a comprender rápidamente el alcance del problema al identificar las puertas de enlace de malware y la ruta que utilizan los atacantes para establecerse en otros sistemas.

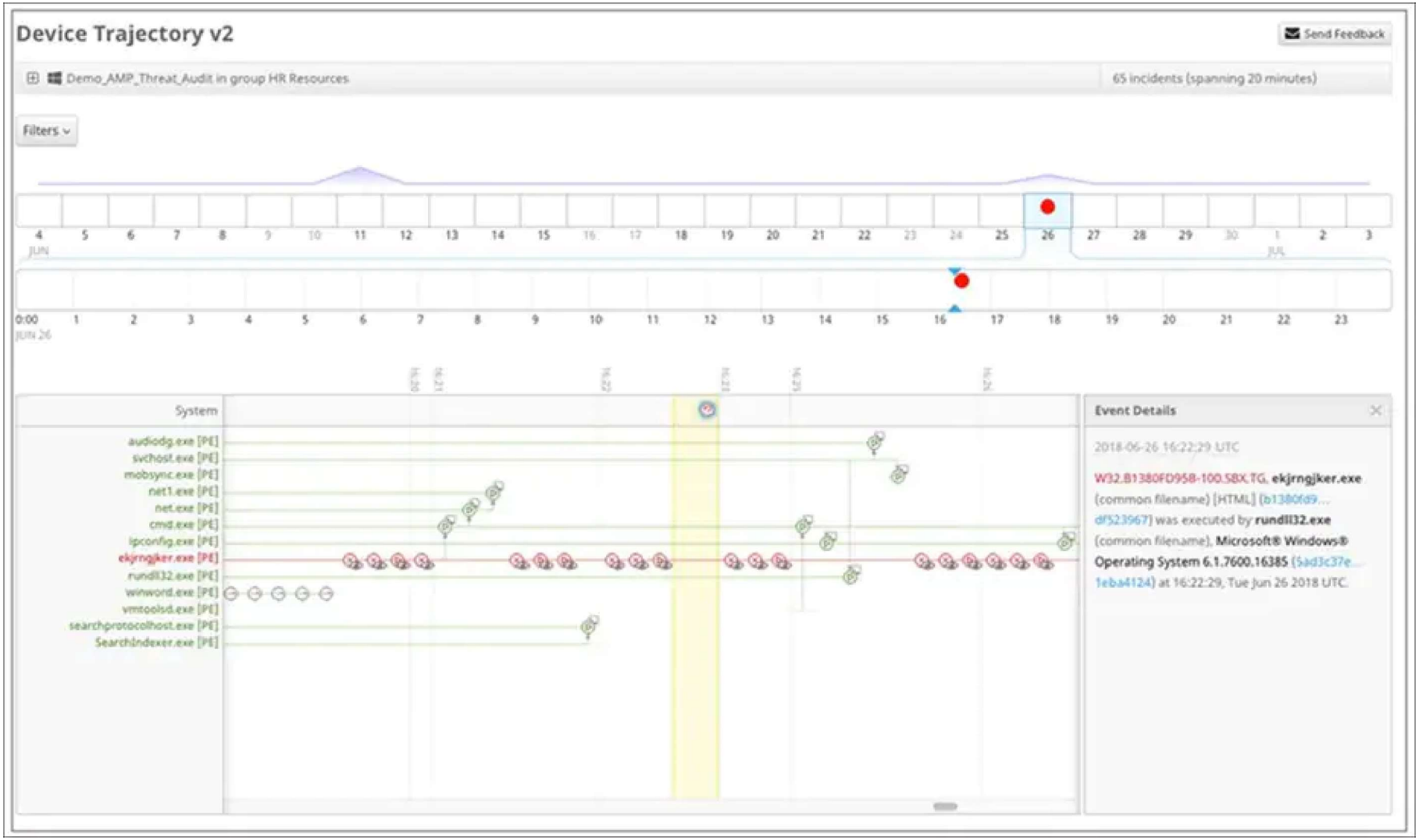

Figura 2.

Trayectoria del dispositivo Secure Endpoint

Análisis dinámico: Secure Endpoint incluye un entorno de sandboxing altamente seguro integrado, con tecnología de Cisco Threat Grid, para analizar el comportamiento de los archivos sospechosos. El análisis de archivos produce información detallada sobre los archivos, incluida la gravedad de los comportamientos, el nombre del archivo original, capturas de pantalla de la ejecución del malware y capturas de paquetes de muestra. Armado con esta información, tendrá una mejor comprensión de lo que se necesita para contener el brote y bloquear futuros ataques.

Seguridad retrospectiva: Secure Endpoint emplea tecnología patentada que descubre automáticamente las amenazas avanzadas que han ingresado a su entorno. Con tecnología de monitoreo continuo, Secure Endpoint correlaciona la información nueva sobre amenazas con su historial anterior y automáticamente pone en cuarentena los archivos en el momento en que comienzan a exhibir un comportamiento malicioso. Esta respuesta automatizada a las últimas amenazas proporciona un tiempo de detección más rápido y reduce en gran medida la proliferación del malware.

Visibilidad de la línea de comandos: Obtener visibilidad de los argumentos de la línea de comandos ayuda a determinar si las aplicaciones legítimas, incluidas las utilidades de Windows, se están utilizando con fines malintencionados. Secure Endpoint puede descubrir comportamientos difíciles de detectar, como el uso de vssadmin para eliminar instantáneas o deshabilitar arranques seguros; Exploits basados en PowerShell; escalada de privilegios; modificaciones de listas de control de acceso; e intenta enumerar sistemas.

Aislamiento de puntos finales: es fundamental aislar los puntos finales que se han visto comprometidos para detener la propagación de amenazas y evitar que se comuniquen con su C&C y, al mismo tiempo, permitir el intercambio de información con recursos confiables, como la nube Secure Endpoint. Endpoint Isolation permite el aislamiento con un solo clic de un punto final infectado junto con la capacidad de incluir en la lista blanca los recursos de red confiables. El punto final se puede desaislar con un solo clic por parte del administrador o a través de un código de desbloqueo por parte del usuario.

Búsqueda avanzada: la búsqueda avanzada es una capacidad avanzada en Cisco Secure Endpoint diseñada para simplificar la investigación de seguridad y la búsqueda de amenazas al proporcionar más de cien consultas preestablecidas, lo que le permite ejecutar rápidamente consultas complejas en cualquiera o todos los puntos finales. Esto le permite obtener una visibilidad más profunda de lo que le sucedió a cualquier punto final en un momento dado al tomar una instantánea de su estado actual. Ya sea que esté realizando una investigación como parte de la

respuesta a incidentes, la búsqueda de amenazas, las operaciones de TI o la vulnerabilidad y el cumplimiento, la Búsqueda avanzada le brinda las respuestas que necesita sobre sus terminales rápidamente.

Cisco Secure MDR para punto final

Secure MDR for Endpoint es un servicio opcional de detección y respuesta administrada de endpoints (EDR) en el que los Centros de operaciones de seguridad (SOC) de Cisco toman todos los eventos de Secure Endpoint, realizan investigaciones, enriquecimientos e inteligencia, y los revisan contra playbooks y casos de uso (con amplia automatización, así como revisión y enriquecimiento humanos). Estos incidentes se priorizan para usted como P1-P4 (P1/P2 acompañados de comunicación directa) con mitigación implementada lo más rápido posible. Cisco monitoreará las alertas de seguridad y responderá apropiadamente minutos después del evento inicial. Esto le permite concentrarse en lo que es importante para su organización.

Tableros y bandeja de entrada: Secure MDR for Endpoint Service Portal es su interfaz principal para el servicio. Todos los incidentes, soporte, comentarios, métricas y más están disponibles allí. Puede ponerse en contacto con el SOC de forma rápida y sencilla directamente a través de un nuevo incidente o un incidente existente. El portal de servicios proporciona widgets en la página de inicio para guiarlo a los últimos incidentes, todos los cuales se enumeran por prioridad. La interfaz Acción de respuesta de aprobación proporciona un portal para el rechazo o

la aprobación de las acciones de remediación recomendadas, así como enlaces a incidentes. También proporcionamos noticias de seguridad, incidentes en espera para que los revisen los clientes y los últimos artículos de la base de conocimientos.

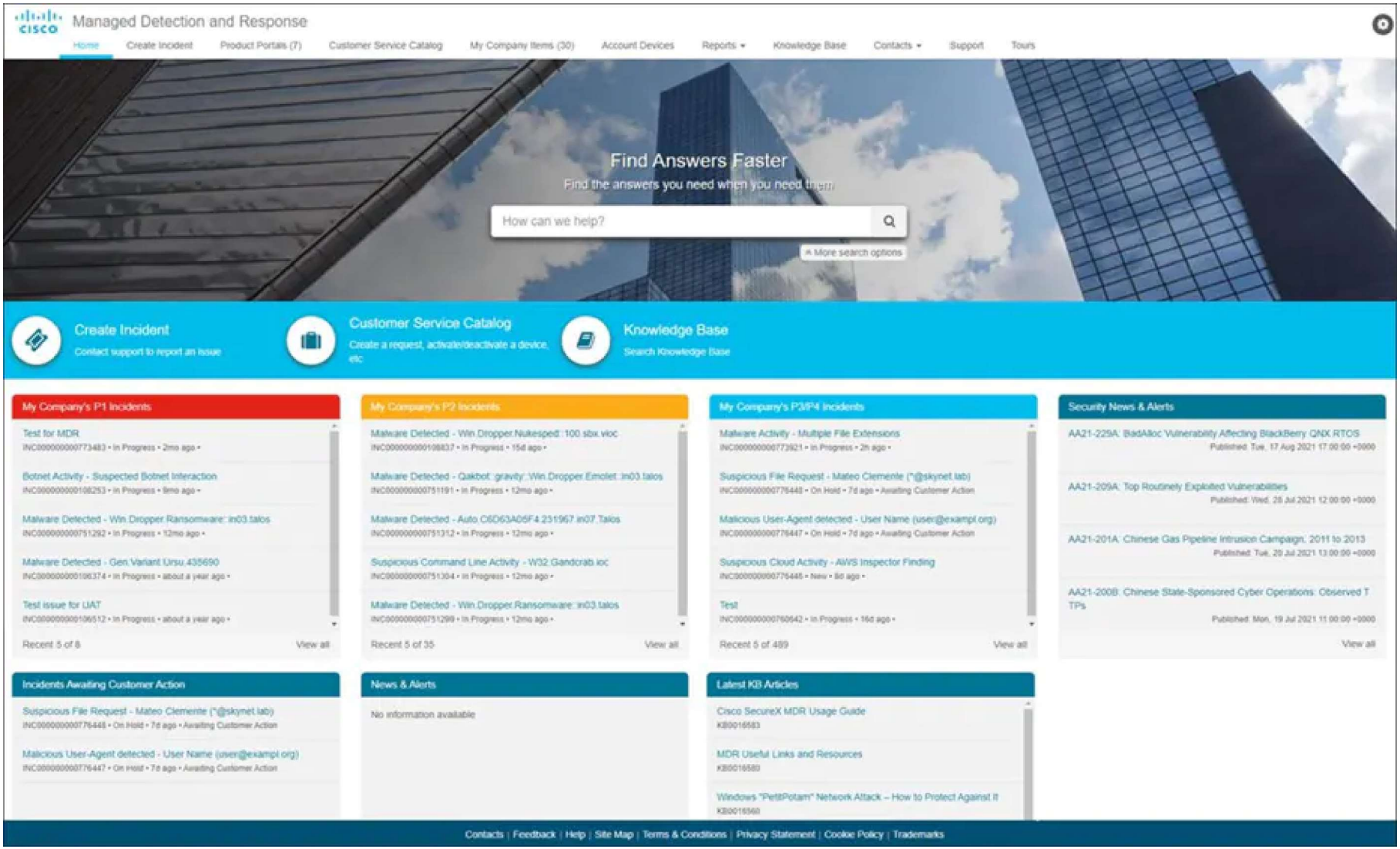

Figura 3.

MDR seguro para el portal de Endpoint

El catálogo de servicios proporciona una forma de dar retroalimentación, solicitar soporte, solicitar informes de inteligencia y más.

La base de conocimiento Secure MDR for Endpoint proporciona varias guías y documentación útiles sobre varios aspectos del servicio y sus productos. Cisco Secure MDR para Endpoint proporciona notas de la versión, guías de productos y servicios, mejores prácticas, información de

administración de licencias y artículos y avisos de inteligencia altamente detallados directamente de nuestro equipo de inteligencia dedicado.

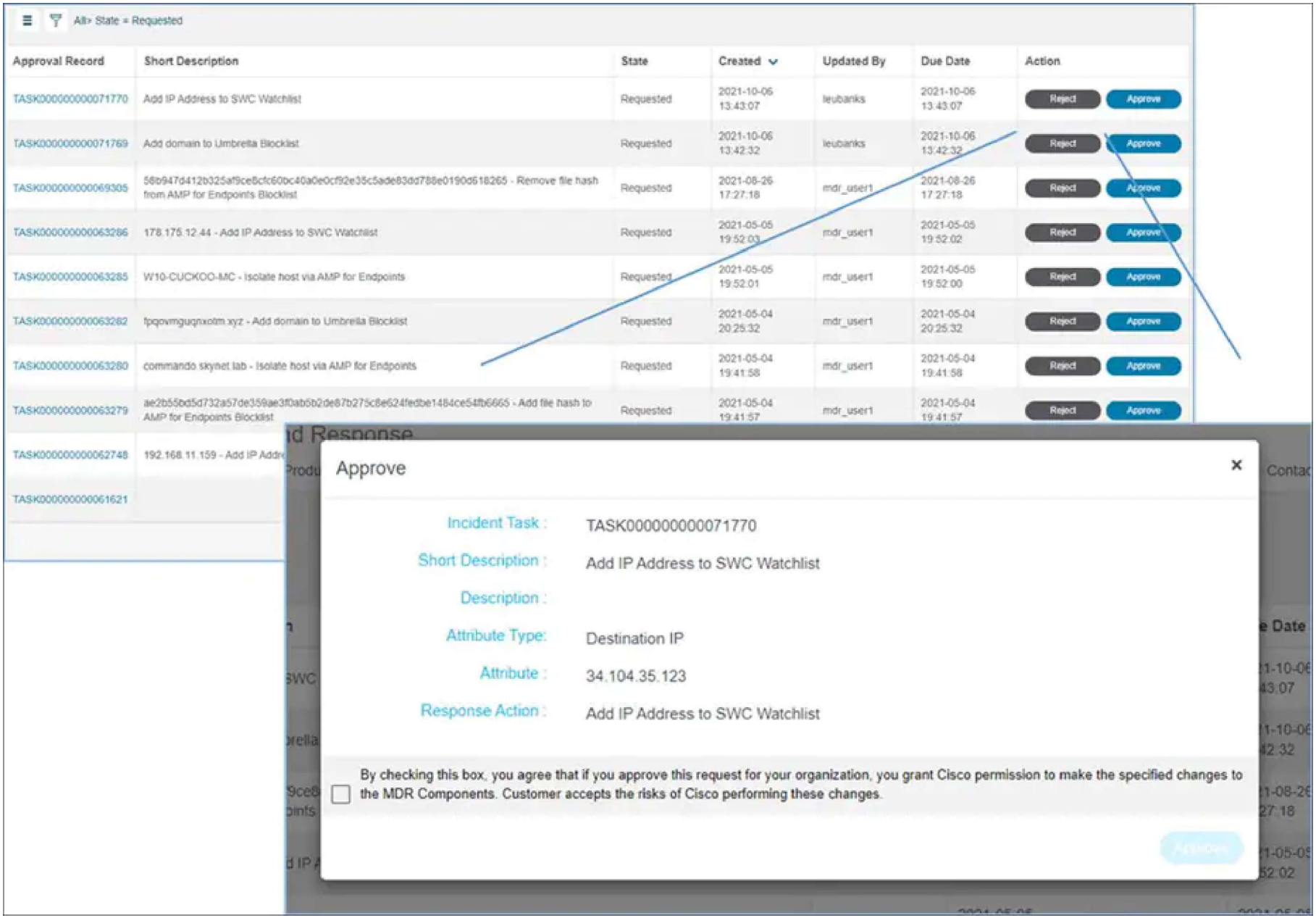

Figura 4.

La interfaz Acción de respuesta de aprobación

Pruebas de terceros independientes de Cisco Secure Endpoint

Soporte y compatibilidad de la plataforma

Secure Endpoint es compatible con los siguientes sistemas operativos:

- Windows (detalles adicionales aquí).
  - Windows 7 (requiere ESU)
  - Windows 8 , 8.1 , 10, 11
  - Windows Server 2008 R2 (se requiere ESU)
  - Windows Server 2012, 2012 R2, 2016, 2019, 2022
- Linux (detalles adicionales aquí)
  - Red Hat Enterprise Linux 6, 7, 8
  - CentOS 6, 7, 8
  - Oracle Linux RHCK (Kernel compatible con Red Hat) 6, 7, 8
  - Oracle UEK (núcleos empresariales irrompibles) 7, 8

- Alma Linux 8
- Rocky Linux 8
- UbuntuLinux 18.04, 20.04
- Amazon Linux 2 - Kernel 4.14 y superior
- SUSE Enterprise Linux 15/openSUSE Leap 15
- Debian Linux 10, 11

- MacOS e iOS (detalles adicionales aquí)
  - macOS 10.13, 10.14, 10.15, 11, 12
  - iOS 14.4 y superior
- androide
  - Android 8.0 (Oreo) y superior

*** Es posible que se apliquen limitaciones a los sistemas operativos heredados**

Información de garantía

Encuentre información sobre la garantía en la página Garantías de productos de Cisco.com .

Sostenibilidad medioambiental de Cisco

La información sobre las políticas e iniciativas de sostenibilidad ambiental de Cisco para nuestros productos, soluciones, operaciones y operaciones extendidas o cadena de suministro se proporciona en la sección "Sostenibilidad ambiental" del Informe de responsabilidad social corporativa (RSC) de Cisco .

Los enlaces de referencia a información sobre temas clave de sostenibilidad ambiental (mencionados en la sección "Sostenibilidad ambiental" del Informe de RSE) se proporcionan en la siguiente tabla:

Tema de sostenibilidad	Referencia
Información sobre leyes y reglamentos sobre el contenido del material del producto	Materiales
Información sobre leyes y reglamentos sobre desechos electrónicos, incluidos productos, baterías y empaques	Cumplimiento de RAEE

Cisco pone a disposición los datos del paquete únicamente con fines informativos. Es posible que no refleje los desarrollos legales más

actuales, y Cisco no declara ni garantiza que sea completo, preciso o actualizado. Esta información esta sujeta a cambios sin previo aviso.

Información sobre pedidos

Encuentre la guía de pedidos aquí .

capital de cisco

Soluciones de pago flexibles para ayudarlo a lograr sus objetivos

Cisco Capital facilita la obtención de la tecnología adecuada para lograr sus objetivos, permitir la transformación empresarial y ayudarlo a mantenerse competitivo. Podemos ayudarlo a reducir el costo total de propiedad, conservar el capital y acelerar el crecimiento. En más de 100 países, nuestras soluciones de pago flexibles pueden ayudarlo a adquirir hardware, software, servicios y equipos complementarios de terceros en pagos fáciles y predecibles. Más información

Para más información

Para obtener más información, visite el siguiente enlace: Cisco Secure Endpoint .

Resources and Legal -

Retroalimentación

Ayuda

Términos y condiciones

Declaracion de privacidad

Galletas

Marcas registradas

Transparencia de la cadena de suministro

mapa del sitio