Managed Threat Detection

Complemente su actual protección para endpoints de terceros con un servicio totalmente administrado de supervisión y detección 24/7

Conserve su propia protección

Pocas empresas cuentan con las herramientas, las personas y los procesos adecuados para gestionar eficazmente su programa de seguridad las 24 horas. Se depende mucho de la protección para endpoints automatizada pero, ¿qué ocurre si los ciberdelincuentes logran esquivar esta protección? ¿Se dará cuenta alguien antes de que sea demasiado tarde?

Sophos Managed Threat Detection ofrece supervisión y detección de amenazas 24/7 para garantizar que ninguna actividad sospechosa que logre eludir su protección para endpoints pase desapercibida. El servicio está diseñado para ejecutarse en paralelo con productos de protección de endpoints de terceros, lo que significa que las organizaciones pueden seguir utilizando su protección para endpoints existente al tiempo que se benefician de la supervisión por parte de expertos de Sophos.

Detección

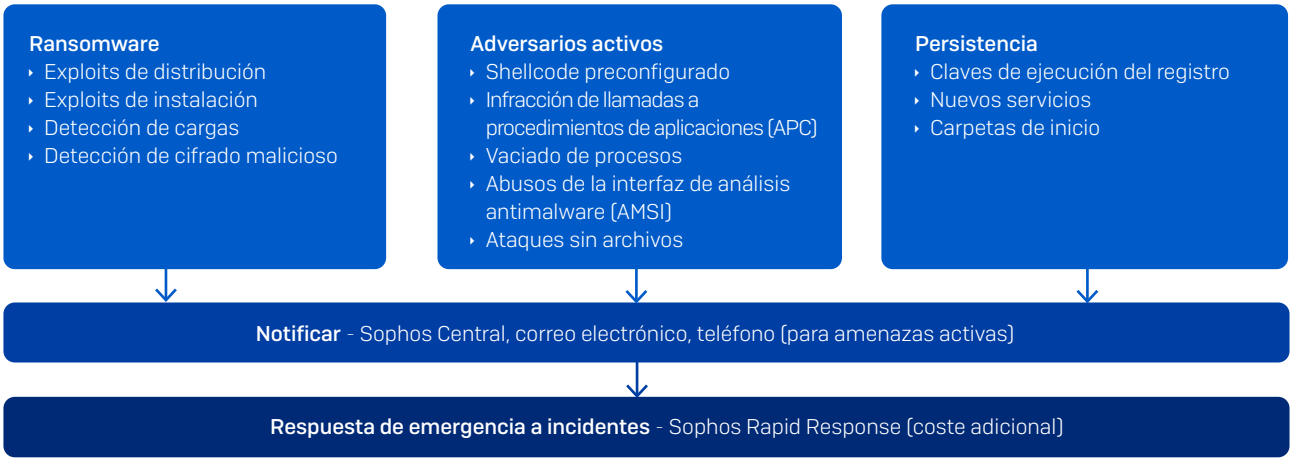
Managed Threat Detection está disponible en el modo de respuesta a amenazas "Notificar". Los clientes reciben alertas si una amenaza de alta gravedad elude su solución de protección para endpoints. Esto incluye varios comportamientos observados habitualmente antes de los ataques de ransomware.

Estos son algunos ejemplos de eventos de detección:

- Shellcode preconfigurado como el que suele encontrarse en CobaltStrike Beacon o Metasploit Meterpreter
- Una nueva tarea programada que ejecuta $PS, incluida la actividad en ubicaciones comúnmente utilizadas para la persistencia por parte del malware y los ciberdelincuentes (como claves de ejecución del registro, servicios o elementos de inicio de Windows)
- Ransomware o comportamientos que otros productos de protección podrían pasar por alto

Aspectos destacados

- Supervisión y detección 24/7 de actividad sospechosa
- Diseñado para ejecutarse en paralelo con productos de protección para endpoints de terceros
- Modo de respuesta a amenazas "Notificar"
- Validación por parte de analistas de todas las detecciones de alta gravedad
- Envío de notificaciones con recomendaciones de remediación
- Sophos Rapid Response está disponible para una respuesta a incidentes adicional



SOPHOS

Notificación y respuesta

Una comunicación clara es totalmente crítica a la hora de ejecutar un programa de operaciones de seguridad. Por esta razón, el servicio Managed Threat Detection proporciona un flujo continuo de información, incluidos informes semanales y mensuales, notificaciones por correo electrónico y un panel de control en Sophos Central.

Los clientes reciben notificaciones por correo electrónico con actualizaciones del estado de los casos. Esto incluye alertas cuando se requiere una acción y cuando los casos se han resuelto. Todos los casos son validados por un analista y las notificaciones incorporan una sinopsis del caso, una lista de dispositivos afectados y recomendaciones de remediación.

Además, se envían comunicados con alertas a los clientes relativas a noticias de última hora con información sobre los descubrimientos más recientes sobre la amenaza, los pasos que está siguiendo Sophos y lo que pueden hacer los clientes para mantenerse protegidos.

Cuando se detecta una amenaza activa en el entorno de un cliente, los operadores de Sophos se ponen en contacto con él por teléfono. Esto garantiza que no haya retrasos de información crítica. Los clientes pueden actualizar la información de su contacto autorizado y sus preferencias de Managed Threat Detection desde el panel de control de Sophos Central en cualquier momento. El panel de control también incluye un resumen de toda la actividad relevante de Managed Threat Detection a fin de proporcionar a los clientes la información más actualizada en cualquier lugar y momento que la necesiten.

Si requiere ayuda para la respuesta a incidentes a fin de resolver una amenaza, tiene a su disposición al equipo de Sophos Rapid Response como servicio adicional. Sophos Rapid Response le proporciona ayuda urgente rápida para investigar y neutralizar amenazas activas. Ya sea una infección, un ataque o un acceso no autorizado que intenta burlar sus controles de seguridad (o que ya lo ha logrado), el equipo lo ha visto todo y lo ha detenido todo. Los clientes de Sophos cuentan con ventaja en cuestión de velocidad, ya que el equipo de respuesta a incidentes de Rapid Response tendrá acceso inmediato a la telemetría y al registrador de datos proporcionados por los agentes de Managed Threat Detection.

	Managed Threat Response (MTR) Standard	Managed Threat Response (MTR) Advanced	Managed Threat Detection
Compatible con protección para endpoints de terceros	✗	✗	✓
Monitorización 24/7	✓	✓	✓
Detección de adversarios	✓	✓	✓
Informes, panel de control	✓	✓	✓
Notificación de amenazas	✓	✓	✓
MTR Connector para Sophos Firewall	✗	✓	✓
MTR Connector para Sophos Cloud Optix	✗	✓	✗
Soporte para múltiples SO	✓	✓	✗ (solo Win10/2012r2 y superior)
Búsqueda de amenazas sin pistas iniciadas por analistas	✗	✓	✗
Estado de seguridad de endpoints de Sophos	✓	✓	✗
Protección en tiempo real	✓	✓	✗
Contención y neutralización	✓	✓	✗
Comunicación por teléfono	✗ (solo amenazas activas)	✓	✗ (solo amenazas activas)

Ventas en España:
Teléfono: (+34) 91 375 67 56
Email: comercialES@sophos.com

Ventas en América Latina:
Email: Latamsales@sophos.com

21-07-13 DS-ES (MP)

SOPHOS