Resumen de Intercept X for Server, XDR y MTR

SOPHOS

Administrado con Sophos Central

	Características	Intercept X Essentials for Server	Intercept X Advanced for Server	Intercept X Advanced for Server with XDR	Intercept X Advanced for Server with MTR Standard	Intercept X Advanced for Server with MTR Advanced
ADMINISTRACIÓN	Múltiples políticas		✓	✓	✓	✓
	Actualizaciones controladas		✓	✓	✓	✓
REDUCCIÓN DE SUPERFICIE DE ATAQUE	Control de aplicaciones		✓	✓	✓	✓
	Control de periféricos		✓	✓	✓	✓
	Control web / bloqueo de URL basado en categorías		✓	✓	✓	✓
	Listas blancas de aplicaciones (bloqueo de servidor)		✓	✓	✓	✓
	Reputación de descargas	✓	✓	✓	✓	✓
	Protección web	✓	✓	✓	✓	✓
ANTES DE QUE SE EJECUTE EN EL DISPOSITIVO	Detección de malware con Deep Learning	✓	✓	✓	✓	✓
	Escaneado de archivos antimalware	✓	✓	✓	✓	✓
	Live Protection	✓	✓	✓	✓	✓
	Análisis de comportamiento previo a la ejecución (HIPS)	✓	✓	✓	✓	✓
	Bloqueo de aplicaciones no deseadas	✓	✓	✓	✓	✓
	Sistema de prevención de intrusiones (IPS)	✓	✓	✓	✓	✓
DETENER LA AMENAZA EN EJECUCIÓN	Prevención de pérdidas de datos	✓	✓	✓	✓	✓
	Análisis de comportamiento en tiempo de ejecución (HIPS)	✓	✓	✓	✓	✓
	Interfaz de análisis antimalware (AMSI)	✓	✓	✓	✓	✓
	Detección de tráfico malicioso (MTD)	✓	✓	✓	✓	✓
	Prevención de exploits (detalles en la página 5)	✓	✓	✓	✓	✓
	Mitigaciones de adversarios activos (detalles en la página 5)	✓	✓	✓	✓	✓
	Protección contra archivos de ransomware (CryptoGuard)	✓	✓	✓	✓	✓
	Protección del registro de arranque y disco (WipeGuard)	✓	✓	✓	✓	✓
	Protección contra Man-in-the-Browser (Navegación segura)	✓	✓	✓	✓	✓
	Bloqueo de aplicaciones mejorado	✓	✓	✓	✓	✓

Más funciones en la página siguiente

Resumen de Intercept X for Server, XDR y MTR

SOPHOS

Administrado con Sophos Central

	Características	Intercept X Essentials for Server	Intercept X Advanced for Server	Intercept X Advanced for Server with XDR	Intercept X Advanced for Server with MTR Standard	Intercept X Advanced for Server with MTR Advanced
DETECTAR	Live Discover (consultas SQL en toda la infraestructura para la búsqueda de amenazas y la higiene de las operaciones de seguridad TI)			✓	✓	✓
	Biblioteca de consultas SQL (consultas ya escritas totalmente personalizables)			✓	✓	✓
	Almacenamiento de datos en disco de rápido acceso (hasta 90 días)			✓	✓	✓
	Fuentes de datos entre productos (p. ej. Firewall, Email)			✓	✓	✓
	Consultas entre productos			✓	✓	✓
	Sophos Data Lake (almacenamiento de datos en la nube)			30 días	30 días	30 días
	Consultas programadas			✓	✓	✓
INVESTIGAR	Casos de amenazas (Análisis de causa raíz)		✓	✓	✓	✓
	Análisis de malware con Deep Learning			✓	✓	✓
	Información sobre amenazas avanzada de SophosLabs a demanda			✓	✓	✓
	Exportación de datos forenses			✓	✓	✓
SOLUCIONAR	Eliminación de malware automatizada	✓	✓	✓	✓	✓
	Seguridad sincronizada con Security Heartbeat	✓	✓	✓	✓	✓
	Sophos Clean	✓	✓	✓	✓	✓
	Live Response (Acceso remoto al terminal para realizar investigaciones adicionales y tomar medidas)			✓	✓	✓
	Aislamiento de servidores a demanda			✓	✓	✓
	"Limpiar y bloquear" en un solo clic			✓	✓	✓
VISIBILIDAD	Protección de cargas de trabajo en la nube (Amazon Web Services, Microsoft Azure, Google Cloud Platform)	✓	✓	✓	✓	✓
	Control de aplicaciones sincronizado (visibilidad de aplicaciones)	✓	✓	✓	✓	✓
	Gestión de la posición de seguridad en la nube (supervise y proteja hosts en la nube, funciones sin servidor, buckets de S3 y más)		✓	✓	✓	✓

Resumen de Intercept X for Server, XDR y MTR

SOPHOS

Administrado con Sophos Central

	Características	Intercept X Essentials for Server	Intercept X Advanced for Server	Intercept X Advanced for Server with XDR	Intercept X Advanced for Server with MTR Standard	Intercept X Advanced for Server with MTR Advanced
CONTROL	Caché de actualización y repetidor de mensajes	✓	✓	✓	✓	✓
	Exclusiones de escaneado automático	✓	✓	✓	✓	✓
	Monitorización de integridad de archivos		✓	✓	✓	✓
SERVICIO GESTIONADO	Búsqueda de amenazas a partir de pistas 24/7				✓	✓
	Comprobaciones del estado de seguridad				✓	✓
	Retención de datos				✓	✓
	Informes de actividades				✓	✓
	Detección de adversarios				✓	✓
	Neutralización y remediación de amenazas				✓	✓
	Búsqueda de amenazas sin pistas 24/7					✓
	Responsable del equipo de respuesta a amenazas					✓
	Soporte telefónico directo					✓
	Gestión proactiva de la posición de seguridad					✓

Comparación de funciones entre sistemas operativos

SOPHOS

	CARACTERÍSTICAS	WINDOWS	LINUX*
ADMINISTRACIÓN	Múltiples políticas	✓	✓
	Actualizaciones controladas	✓	✓
REDUCCIÓN DE SUPERFICIE DE ATAQUE	Protección web	✓	
	Reputación de descargas	✓	
	Control web / bloqueo de URL basado en categorías	✓	
	Control de periféricos	✓	
	Control de aplicaciones	✓	
	Listas blancas de aplicaciones (bloqueo de servidor)	✓	
ANTES DE QUE SE EJECUTE EN EL DISPOSITIVO	Detección de malware con Deep Learning	✓	✓
	Escaneado de archivos antimalware	✓	✓
	Live Protection	✓	✓
	Análisis de comportamiento previo a la ejecución (HIPS)	✓	
	Bloqueo de aplicaciones no deseadas	✓	
	Sistema de prevención de intrusiones (IPS)	✓	
DETENER LA AMENAZA EN EJECUCIÓN	Prevención de pérdidas de datos	✓	
	Análisis de comportamiento en tiempo de ejecución (HIPS)	✓	
	Interfaz de análisis antimalware (AMSI)	✓	
	Detección de tráfico malicioso (MTD)	✓	Véase la nota
	Prevención de exploits (detalles en la página 5)	✓	
	Mitigaciones de adversarios activos (detalles en la página 5)	✓	
	Protección contra archivos de ransomware (CryptoGuard)	✓	
	Protección del registro de arranque y disco (WipeGuard)	✓	
	Protección contra Man-in-the-Browser (Navegación segura)	✓	
	Bloqueo de aplicaciones mejorado	✓	

Más funciones en la página siguiente

Comparación de funciones entre sistemas operativos

SOPHOS

	CARACTERÍSTICAS	WINDOWS	LINUX*
DETECTAR	Live Discover (consultas SQL en toda la infraestructura para la búsqueda de amenazas y la higiene de las operaciones de seguridad TI)	✓	✓
	Biblioteca de consultas SQL (consultas ya escritas totalmente personalizables)	✓	✓
	Almacenamiento de datos en disco de rápido acceso (hasta 90 días)	✓	✓
	Fuentes de datos entre productos (p. ej. Firewall, Email)	✓	✓
	Consultas entre productos	✓	✓
	Sophos Data Lake (almacenamiento de datos en la nube)	✓	✓
	Consultas programadas	✓	✓
INVESTIGAR	Casos de amenazas (Análisis de causa raíz)	✓	
	Análisis de malware con Deep Learning	✓	
	Información sobre amenazas avanzada de SophosLabs a demanda	✓	
	Exportación de datos forenses	✓	
SOLUCIONAR	Eliminación de malware automatizada	✓	
	Seguridad sincronizada con Security Heartbeat	✓	Véase la nota
	Sophos Clean	✓	
	Live Response (Acceso remoto al terminal para realizar investigaciones adicionales y tomar medidas)	✓	✓
	Aislamiento de servidores a demanda	✓	
	"Limpiar y bloquear" en un solo clic	✓	
VISIBILIDAD	Protección de cargas de trabajo en la nube (Amazon Web Services, Microsoft Azure, Google Cloud Platform)	✓	✓
	Control de aplicaciones sincronizado (visibilidad de aplicaciones)	✓	
	Gestión de la posición de seguridad en la nube (supervise y proteja hosts en la nube, funciones sin servidor, buckets de S3 y más)	✓	✓
CONTROL	Caché de actualización y repetidor de mensajes	✓	
	Exclusiones de escaneado automático	✓	
	Monitorización de integridad de archivos	✓	

Comparación de funciones entre sistemas operativos

SOPHOS

	CARACTERÍSTICAS	WINDOWS	LINUX*
SERVICIO GESTIONADO	Búsqueda de amenazas a partir de pistas 24/7	✓	✓
	Comprobaciones del estado de seguridad	✓	✓
	Retención de datos	✓	✓
	Informes de actividades	✓	✓
	Detección de adversarios	✓	✓
	Neutralización y remediación de amenazas	✓	✓
	Búsqueda de amenazas sin pistas 24/7	✓	✓
	Responsable del equipo de respuesta a amenazas	✓	✓
	Soporte telefónico directo	✓	✓
	Mejora proactiva de la posición de seguridad	✓	✓

*Linux incluye dos opciones de despliegue. 1) El despliegue de Sophos Protion for Linux da acceso a las funciones indicadas en la tabla. 2) El despliegue de Sophos Anti-Virus for Linux incluye: antimalware, Live Protection, detección de tráfico malicioso y Seguridad Sincronizada. Tenga en cuenta que las dos opciones de despliegue no se pueden utilizar juntas.

Funciones de Sophos Intercept X

SOPHOS

Detalles de las funciones incluidas en Intercept X

	Características	
EXPLOIT PREVENTION	Aplicación de la prevención de ejecución de datos	✓
	Selección aleatoria del diseño del espacio de direcciones obligatoria	✓
	ASLR de abajo a arriba	✓
	Página NULL (Protección de desreferencia NULL)	✓
	Asignación de pulverización del montón	✓
	Pulverización dinámica del montón	✓
	Eje de la pila	✓
	Ejecución de la pila (MemProt)	✓
	Mitigaciones de ROP basadas en pilas (Autor de llamada)	✓
	Mitigaciones de ROP basadas en ramas (Asistidas por hardware)	✓
	Sobrescritura del controlador de excepciones estructurado (SEHOP)	✓
	Filtrado de tabla de direcciones de importación (IAF)	✓
	Carga de bibliotecas	✓
	Inyección de DLL reflectiva	✓
	Shellcode	✓
	Modo Dios de VBScript	✓
	Wow64	✓
	Syscall	✓
	Vaciado de procesos	✓
	Secuestro de DLL	✓
	Omisión de AppLocker Squiblydoo	✓
	Protección de APC (Double Pulsar / AtomBombing)	✓
	Aumento de privilegios de procesos	✓
	Protección shellcode dinámica	✓
	EFS Guard	✓
	CTF Guard	✓
	ApiSetGuard	✓
MITIGACIONES DE ACTIVE ADVERSARY	Protección contra robos de credenciales	✓
	Mitigación de cuevas de código	✓
	Protección contra Man-in-the-Browser (Navegación segura)	✓
	Detección de tráfico malicioso	✓
	Detección de shell Meterpreter	✓

	Características	
ANTI-RANSOMWARE	Protección contra archivos de ransomware (CryptoGuard)	✓
	Detección automática de archivos (CryptoGuard)	✓
	Protección del registro de arranque y disco (WipeGuard)	✓
BLOQUEO DE APLICACIONES	Navegadores web (incluido HTA)	✓
	Complementos de navegadores web	✓
	Java	✓
	Aplicaciones multimedia	✓
	Aplicaciones de Office	✓
PROTECCIÓN CON DEEP LEARNING	Detección de malware con Deep Learning	✓
	Bloqueo de aplicaciones no deseadas (PUA) con Deep Learning	✓
	Supresión de falsos positivos	✓
RESPONDER INVESTIGAR ELIMINAR	Casos de amenazas (Análisis de causa raíz)	✓
	Sophos Clean	✓
	Seguridad sincronizada con Security Heartbeat	✓

Managed Threat Response (MTR)

Sophos Managed Threat Response (MTR) es un servicio totalmente administrado prestado por un equipo de expertos que ofrece funciones de búsqueda, detección y respuesta a amenazas 24/7. Los clientes de MTR también reciben Intercept X Advanced for Server with XDR.

Sophos MTR: Standard

Búsqueda de amenazas a partir de pistas 24/7

Las actividades o artefactos maliciosos confirmados (indicios sólidos) se bloquean o detienen automáticamente, lo que libera la carga de trabajo de los analistas de amenazas para que puedan realizar búsquedas a partir de pistas. Este tipo de búsqueda de amenazas implica agregar e investigar eventos causales y adyacentes (indicios débiles) para descubrir nuevos indicadores de ataque y de peligro que antes no podían detectarse.

Comprobación del estado de seguridad

Mantenga el máximo rendimiento de sus productos de Sophos Central, empezando por Intercept X Advanced for Server with XDR, con exámenes proactivos de sus condiciones operativas y mejoras de configuración recomendadas.

Informes de actividades

Los resúmenes de las actividades de los casos facilitan la priorización y comunicación para que su equipo sepa qué amenazas se han detectado y qué acciones de respuesta se han llevado a cabo dentro de cada periodo del informe.

Detección de adversarios

La mayoría de los ataques eficaces dependen de la ejecución de un proceso que puede parecer legítimo para las herramientas de supervisión. Mediante técnicas de investigación patentadas, nuestro equipo determina la diferencia entre un comportamiento legítimo y las tácticas, técnicas y procedimientos utilizados por los atacantes.

Sophos MTR: Advanced *Incluye todas las funciones de Standard, más lo siguiente:*

Búsqueda de amenazas sin pistas las 24 horas

Aplicando data science, la información sobre amenazas y la intuición de experimentados detectores de amenazas, combinamos el perfil de su empresa, sus activos de alto valor y usuarios de alto riesgo para anticiparnos al comportamiento de los atacantes e identificar nuevos indicadores de amenazas.

Telemetría optimizada

Las investigaciones de amenazas se complementan con la telemetría de otros productos de Sophos Central que van más allá del endpoint para ofrecer una imagen completa de las actividades del adversario.

Mejora proactiva de la posición de seguridad

Mejore de forma proactiva su posición de seguridad y refuerce sus defensas con una guía prescriptiva para corregir las carencias de configuración y arquitectura que merman sus capacidades generales en materia seguridad.

Responsable de respuesta ante amenazas dedicado

Cuando se confirma un incidente, se le asigna un responsable de respuesta ante amenazas dedicado para que colabore directamente con sus recursos locales (equipo interno o partner externo) hasta que se neutralice la amenaza activa.

Soporte telefónico directo

Su equipo tiene acceso telefónico directo a nuestro centro de operaciones de seguridad (SOC). Nuestro equipo de operaciones de MTR está disponible las 24 horas y cuenta con el apoyo de equipos de soporte en 26 lugares de todo el mundo.

Detección de recursos

Desde datos sobre recursos que incluyen versiones de sistemas operativos, aplicaciones y vulnerabilidades hasta la identificación de activos gestionados y no gestionados, proporcionamos información valiosa durante las evaluaciones de impacto, las búsquedas de amenazas y como parte de las recomendaciones para la mejora proactiva de la posición de seguridad.

SOPHOS