Trend Micro™

DEEP DISCOVERY INSPECTOR

Detección de ataques dirigidos en toda la red

Los ataques dirigidos y las amenazas avanzadas se personalizan para infiltrarse en su exclusiva infraestructura de TI, evadir las defensas convencionales y permanecer ocultos mientras sustraen sus datos corporativos. Para detectar estas intrusiones criminales, los analistas y expertos en seguridad coinciden en que las organizaciones deben implementar una protección frente a amenazas avanzadas como parte de una estrategia de supervisión de la seguridad ampliada.

Trend Micro Deep Discovery Inspector es un dispositivo de protección frente a amenazas avanzadas que proporciona visibilidad e inteligencia de toda la red, a fin de detectar tanto ataques dirigidos como amenazas avanzadas y responder a ellos. Inspector supervisa todos los puertos y más de 80 protocolos para analizar prácticamente todo el tráfico de red, lo que le brinda la máxima protección disponible. Los motores de detección especializados y el aislamiento personalizado identifican y analizan el malware, las comunicaciones de comando y control (C&C), y las actividades evasivas de atacantes invisibles a la seguridad estándar. La inteligencia de detección en profundidad contribuye a una rápida respuesta y se comparte de forma automática con el resto de productos de seguridad de que dispone, a fin de crear una defensa personalizada en tiempo real frente a sus atacantes.

FUNCIONES PRINCIPALES

Detección de amenazas integral
Supervisa todos los puertos y más de 80 protocolos con el fin de identificar los ataques en cualquier punto de su red.

Malware, C&C y actividad de atacantes
Utiliza motores de detección especializados, reglas de correlación y aislamiento personalizado para detectar todos los aspectos de un ataque dirigido, no solo el malware.

Aislamiento personalizado
Utiliza imágenes que coinciden de forma precisa con sus configuraciones de sistema para detectar las amenazas dirigidas a su organización.

Inteligencia de red Smart Protection
La inteligencia de amenazas global activa la detección y el portal Threat Connect para la investigación de ataques.

Amplia protección del sistema
Detecta ataques contra Windows, Mac OS X, Android, Linux y cualquier otro sistema.

La sencillez y flexibilidad de un único dispositivo
Simplifica la seguridad mediante un único dispositivo disponible con una amplia variedad de funciones e implementable en configuraciones de hardware o virtuales.

Solución de defensa personalizada
Comparte la inteligencia de indicadores de compromiso (IOC) y actualiza automáticamente los productos de seguridad tanto de Trend Micro como de otros proveedores para protegerle de más ataques.

Principales ventajas

Protección frente a ataques dirigidos
Descubre las amenazas invisibles para los productos de seguridad estándar.

Visibilidad y detección integrales.
Supervisa prácticamente todo el tráfico para detectar ataques y revelar su auténtica postura de seguridad.

Análisis y respuesta rápidos
Caracteriza totalmente los factores de amenaza y riesgo para impulsar una respuesta rápida

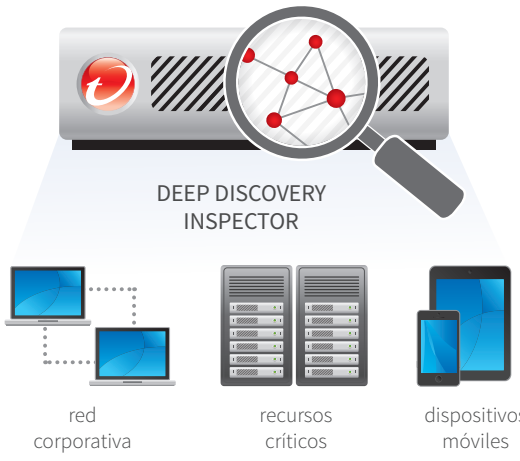
Coste de propiedad más reducido
Simplifica la protección y la gestión con un único dispositivo que reduce el coste total de propiedad.

Piedra angular de una defensa personalizada
Comparte la inteligencia de IOC (indicadores de compromiso, «indicators of compromise») con otras soluciones de seguridad, creando una defensa personalizada, integrada y en tiempo real frente a ataques dirigidos.

NSS LABS RECOMMENDED

Trend Micro™ Deep Discovery
MÁXIMA PUNTUACIÓN
en detección de infracciones

Pruebas de detección de infracciones de 2014 de NSS Labs



Detecta y protege frente a

- Ataques dirigidos y amenazas avanzadas
- Malware de día cero y vulnerabilidades de seguridad en documentos
- Actividad de red del atacante
- Amenazas web, que incluyen vulnerabilidades de seguridad y
- descargas furtivas
- Suplantación de identidad, suplantación de identidad selectiva y otras amenazas por correo electrónico
- Extracción de datos
- Bots, troyanos, gusanos y keyloggers
- Aplicaciones disruptivas

Deep Discovery Inspector proporciona inspección del tráfico, detección de amenazas avanzadas y análisis en tiempo real: está diseñado específicamente para la detección de ataques dirigidos. Utiliza un esquema de detección de nivel 3 para realizar la detección inicial; a continuación, lleva a cabo una simulación de aislamiento personalizado y, finalmente, procede con la correlación de eventos para descubrir actividades de atacantes evasivos.

Los motores de detección y correlación proporcionan la protección más precisa y actualizada, dotada de la inteligencia de amenazas global de Smart Protection Network™ de Trend Micro™ e investigadores de amenazas dedicados. Los resultados muestran tasas de detección elevadas, escasos falsos positivos e inteligencia en profundidad diseñada para agilizar la respuesta ante el ataque.

CÓMO FUNCIONA DEEP DISCOVERY INSPECTOR

Motores de detección de amenazas
Un surtido de motores de detección y reglas de correlación especializados se centran en encontrar malware, C&C y actividades de atacante en prácticamente todo el tráfico de red, más allá del HTTP y el SMTP estándares. Smart Protection Network y los investigadores de amenazas dedicados actualizan continuamente estos motores y reglas.

Analizador virtual
El análisis de aislamiento personalizado, que utiliza entornos virtuales que coinciden de forma precisa con sus configuraciones de sistema, analiza los archivos sospechosos y el contenido web con detenimiento. El aislamiento personalizado detecta de forma precisa las amenazas dirigidas a su organización, frustra las técnicas de evasión y excluye las detecciones de malware irrelevante.

Consola de amenazas en tiempo real
La consola de Deep Discovery Inspector sitúa la visibilidad de amenazas en tiempo real y las funciones de análisis profundo al alcance de su mano. Dispone de widgets de acceso rápido para la información crítica, georrastreo de los orígenes de las amenazas, supervisión mediante lista de vigilancia de los recursos críticos e inteligencia Threat Connect para evaluar las características de los ataques.

Lista de vigilancia
Una pantalla especial proporciona supervisión centrada en los riesgos de las amenazas de gravedad alta y los activos de alto valor. Se puede realizar el seguimiento específico de los sistemas designados en busca de actividades y eventos sospechosos, así como análisis detallados.

Threat Connect
Threat Connect es un portal de información exclusivo que se nutre de la inteligencia global de Smart Protection Network con objeto de proporcionarle la mayor cantidad disponible de datos pertinentes para su ataque. Este perfil incluye evaluación de riesgos; orígenes, variantes y características de malware, IP de C&C relacionadas, perfil de atacante y procedimientos de corrección.

Gestión centralizada, así como de información y eventos de seguridad (SIEM)
Deep Discovery Inspector puede gestionarse de forma independiente a través del centro de inteligencia de amenazas de Deep Discovery o de Trend Micro Control Manager. Asimismo, se integra totalmente con las plataformas de SIEM líderes para admitir la gestión de amenazas en toda la empresa desde una única consola de SIEM.

Uso compartido de información de IOC
Deep Discovery Inspector comparte la información de IOC en nuevas detecciones de aislamiento con otros productos Deep Discovery, Trend Micro y de terceros, creando una defensa personalizada en tiempo real frente a los atacantes.

Implementación flexible y de alta capacidad
Satisface los distintos requisitos de implementación y capacidad con una variedad de dispositivos tanto de hardware como virtuales, desde 100 Mbps hasta 4 Gbps.

CÓMO FUNCIONA LA DETECCIÓN DE DEEP DISCOVERY

Supervisa más de 80 protocolos y aplicaciones en todos los puertos de red

	Detección de ataques	Métodos de detección
Malware avanzado	• Malware de día cero y conocido • Correos electrónicos que contienen vulnerabilidades de seguridad en documentos incrustados • Descargas furtivas	• Descodificación y descompresión de archivos incrustados • Simulación de aislamiento personalizado • Detección de kit de vulnerabilidades de seguridad del navegador • Análisis de malware (mediante firma y heurístico)
Comunicación de C&C	• Comunicación de C&C para todo el malware: bots, gestores de descargas, sustracción de datos, gusanos, amenazas combinadas, etc. • Actividad de puerta trasera por parte del atacante	• Análisis de destino (URL, IP, dominio, correo electrónico, canal IRC, etc.) mediante listas negras y blancas dinámicas • Reputación de Smart Protection Network de todas las URL solicitadas e incrustadas • Reglas de impresiones digitales de comunicaciones
Actividad de atacante	• Actividad de atacante: análisis, fuerza bruta, descarga de herramientas, etc. • Extracción de datos • Actividad de malware: propagación, descarga, envío de spam, etc.	• Análisis heurístico basado en reglas • Correlación de eventos ampliada y técnicas de detección de anomalías • Reglas de impresiones digitales de comportamiento

POR QUÉ EL AISLAMIENTO PERSONALIZADO ES FUNDAMENTAL

Los cibercriminales crean malware personalizado para dirigirse a su entorno específico: los sistemas operativos de sus equipos de sobremesa y portátiles, aplicaciones, navegadores y mucho más. Dado que el malware se diseña para aprovechar estas configuraciones, es posible que el código malintencionado no se ejecute en un espacio aislado genérico. El resultado final: es más probable que no se detecte el malware personalizado en un espacio aislado genérico que no se ajuste a su entorno de TI.

Solo un aislamiento personalizado puede simular su entorno de TI real y permitirle lo siguiente:

- Identificar claramente el malware personalizado dirigido a su organización: su licencia de Windows, su idioma, sus aplicaciones y su conjunto de entornos de escritorio.
- Frustrar las técnicas de evasión de aislamiento basadas en licencias de Windows genéricas, aplicaciones y versiones estándar limitadas, y el idioma inglés.
- Ignorar el malware que no afecta a su organización porque se dirige a versiones del sistema o de aplicaciones que no utiliza.

AMPLÍE SU ESTRATEGIA DE SEGURIDAD

Deep Discovery Inspector es parte de la plataforma Deep Discovery, que ofrece protección avanzada frente a amenazas en los lugares más importantes para su organización: red, correo electrónico, endpoint o integrada. Puede ampliar las capacidades de Inspector añadiendo Deep Discovery Analyzer, Deep Discovery Endpoint Sensor o Deep Discovery Threat Intelligence Center, así como al compartir la inteligencia de detección de IOC de Inspector con otros productos.

Deep Discovery Analyzer es un servidor de análisis de aislamiento personalizado abierto y ampliable. Analyzer puede utilizarse para aumentar la capacidad y la flexibilidad del aislamiento de Inspector, o bien para centralizar el análisis de aislamiento en varias unidades de Inspector. Analyzer también puede utilizarse para aumentar las capacidades de protección de otras soluciones de Trend micro, así como de productos de seguridad de terceros.

Deep Discovery Endpoint Sensor es un monitor de seguridad para endpoints sensible al contexto que registra e informa de las actividades de nivel de sistema en endpoints objetivo de forma detallada. Es especialmente útil para ayudar en la investigación y la corrección de los ataques dirigidos identificados por Inspector. Los datos de IOC hallados pueden utilizase en las búsquedas de Endpoint Sensor para verificar infiltraciones y detectar el contexto completo, la línea de tiempo y la extensión del ataque.

Deep Discovery Threat Intelligence Center proporciona vistas e informes centralizados en todas las unidades de Inspector que implemente. También actúa como punto de distribución para compartir la inteligencia de detección recién descubierta (C&C, otra información de IOC) en las unidades Deep Discovery, productos Trend Micro y también de terceros.

Trend Micro Custom Defense
La plataforma Deep Discovery sirve de base para Trend Micro Custom Defense, lo que le permite detectar, analizar y responder rápidamente a sus atacantes. La detección de Deep Discovery y la inteligencia de IOC se integran con un host de productos de Trend Micro y de terceros para unir su infraestructura de seguridad en una defensa en tiempo real ajustada a medida con objeto de proteger su organización frente a ataques dirigidos.

ESPECIFICACIONES DE LOS DISPOSITIVOS DE HARDWARE DE DEEP DISCOVERY INSPECTOR

	Inspector, modelo 250	Inspector, modelo 500	Inspector, modelo 1000	Inspector, modelo 4000
Capacidad	250 Mbps	500 Mbps	1 Gbps	4 Gbps
Factor de forma	Montaje en bastidor, 1 ud. 48,26 cm (19")	Montaje en bastidor, 1 ud. 48,26 cm (19")	Montaje en bastidor, 1 ud. 48,26 cm (19")	Montaje en bastidor, 2 uds. 48,26 cm (19")
Peso	19,9 kg (43,87 lb)	19,9 kg (43,87 lb)	19,9 kg (43,87 lb)	32,5 kg (71,65 lb)
Dimensiones (An. x Pr. x Al.)	43,4 x 64,2 x 4,28 cm (17,09" x 25,28" x 1,69")	43,4 x 64,2 x 4,28 cm (17,09" x 25,28" x 1,69")	43,4 x 64,2 x 4,28 cm (17,09" x 25,28" x 1,69")	48,2 x 75,58 x 8,73 cm (18,98" x 29,75" x 3,44")
Puertos de gestión	10/100/1000 BASE-T RJ45 1 puerto	10/100/1000 BASE-T RJ45 1 puerto	10/100/1000 BASE-T RJ45 1 puerto	10/100/1000 BASE-T RJ45 1 puerto
Puertos de datos	10/100/1000 BASE-T RJ45 2 puertos	10/100/1000 BASE-T RJ45 4 puertos	10/100/1000 BASE-T RJ45 4 puertos	2 módulos de 10 Gb SFP+ cables de cobre de conexión directa 2 puertos 10/100/1000 BASE-T RJ45
Tensión de entrada (CA):	De 100 a 240 V CA	De 100 a 240 V CA	De 100 a 240 V CA	De 100 a 240 V CA
Corriente de entrada (CA)	De 7,4 A a 3,7 A	De 7,4 A a 3,7 A	De 7,4 A a 3,7 A	De 10 A a 5 A
Discos duros	2 discos duros de 500 GB SATA de 3,5 pulgadas	2 discos duros de 500 GB SATA de 3,5 pulgadas	2 discos duros de 500 GB SATA de 3,5 pulgadas	8 discos duros de 600 GB SAS de 3,5 pulgadas
Configuración RAID	RAID 1	RAID 1	RAID 1	RAID 5
Fuente de alimentación	350 W redundante	550 W redundante	550 W redundante	750 W redundante
Consumo eléctrico (máximo)	385 W	604 W	604 W	847 W (máx.)
Calor	1356 BTU/h máximo	2133 BTU/h (máx.)	2133 BTU/h (máx.)	2891 BTU/h (máx.)
Frecuencia	50/60 Hz	50/60 Hz	50/60 Hz	50/60 Hz
Temperatura de funcionamiento	De 10 a 35 °C (50-95 °F)	De 10 a 35 °C (50-95 °F)	De 10 a 35 °C (50-95 °F)	De 10 a 35 °C (50-95 °F)
Garantía del hardware	3 años	3 años	3 años	3 años

Los dispositivos virtuales Deep Discovery Inspector están disponibles con capacidades de 100, 250, 500 y 1000 Gbps; asimismo, se pueden implementar en VMware vSphere 5 y superiores.

Plataforma Deep Discovery

Deep Discovery Inspector es parte de la familia Deep Discovery de productos interconectados, que brindan protección de red, correo electrónico, endpoint e integrada, de modo que puede implementar protección avanzada frente a amenazas en los puntos que más importan a su organización.

CUSTOM DEFENSE

La plataforma Deep Discovery se halla en el corazón de Trend Micro Custom Defense, que entrelaza su infraestructura de seguridad y le ofrece protección integral a medida para proteger su organización frente a ataques dirigidos.

La detección, inteligencia y controles personalizados de Deep Discovery le permiten lo siguiente:

- Detectar y analizar a sus atacantes
- Adaptar la protección en función del ataque inmediatamente
- Responder con rapidez antes de que se pierdan datos confidenciales

TREND MICRO™

Securing Your Journey to the Cloud