Inspector de procesos

Informe técnico

Resumen

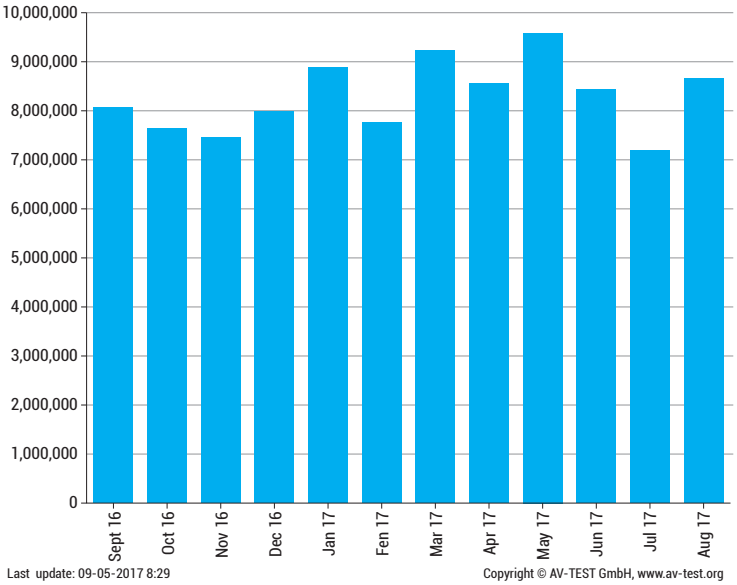
En el panorama actual de la seguridad informática, los autores de las amenazas investigan y cambian constantemente de tácticas, lo que hace que las empresas sean más susceptibles de sufrir incidentes y brotes de malware, trastornos en sus negocios y vulneraciones de datos. La plataforma Bitdefender GravityZone Endpoint Security protege sus endpoints ante todo tipo de ataques informáticos sofisticados con gran eficacia, escaso impacto en el usuario final y baja carga administrativa. Consiste en una serie de capas de protección que levantan obstáculos ante los malhechores para que tropiecen con ellos. Cada una de estas capas está diseñada para frenar tipos concretos de amenazas, herramientas o técnicas y cubren diversas etapas de los ataques.

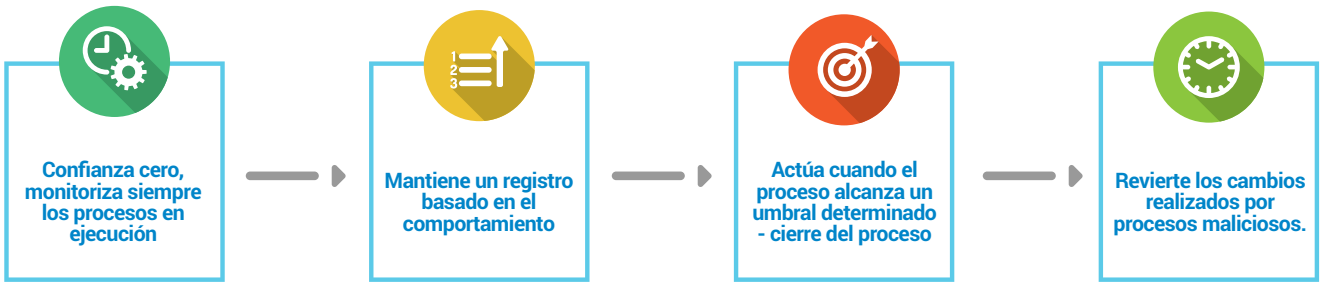
El Inspector de procesos de Bitdefender forma parte de la plataforma GravityZone Endpoint Security. Es una tecnología de detección de anomalías de comportamiento que proporciona protección contra amenazas nunca antes vistas en la etapa de ejecución.

Etapa de detección	Tipo de tecnología	Cobertura de amenazas
Ejecución	Detección de anomalías de comportamiento	Ofuscación de malware, ataques selectivos, malware personalizado, ataques basados en scripts, exploits, malware fragmentado, ataques de memoria, inyección de procesos, escalamiento de privilegios, ataques sin archivos (por ejemplo, uso ilegítimo de PowerShell), ransomware

Comprender la importancia de la tecnología del Process Inspector de Bitdefender

Ante los más de 390 000 nuevos programas maliciosos que se descubren a diario, la necesidad de proteger su entorno contra las amenazas emergentes y de día cero forma parte del día a día de los equipos de seguridad actuales. Process Inspector es una capa de protección en ejecución que amplía las tecnologías integrales de detección previa a la ejecución en la plataforma GravityZone Endpoint Security. Reduce drásticamente el riesgo de que una amenaza nueva o emergente comprometa un sistema. Opera bajo una premisa de confianza cero y monitoriza los procesos que se ejecutan en el sistema operativo utilizando filtros en modo de usuario y kernel. Busca comportamientos específicos del malware y asigna una puntuación a cada proceso basándose en sus acciones y en el contexto. Esto es importante porque los procesos, individualmente, podrían no revelar intenciones maliciosas, pero un análisis colectivo aporta más información. Cuando la puntuación general de un proceso alcanza un umbral determinado, este se identifica como dañino y se adoptan las medidas de reparación apropiadas, lo que incluye la reversión de los cambios realizados en el endpoint por el proceso malicioso.





Características

- Seguimiento de anomalías de comportamiento: las aplicaciones y procesos activos se monitorizan continuamente. Por ejemplo: copiar o mover archivos en carpetas de Windows o del sistema o en ubicaciones de disco de acceso restringido, ejecutar o inyectar código en el espacio de otros procesos para ejecutarse con privilegios mayores, ejecutar archivos que se han creado con información almacenada en el archivo binario, autorreplicarse, crear una entrada de inicio automático en el registro, acceder o ejecutar operaciones ilegales en ubicaciones del registro que requieren privilegios elevados, borrar y registrar controladores, uso ilegítimo de PowerShell (por ejemplo, identificar si se lanza powershell.exe con varios argumentos específicos) y detección específica de ransomware (por ejemplo, eliminación de copias de seguridad de archivos o instantáneas, generación de claves de cifrado, etc.).
- Acción automática: puntúa automáticamente los procesos en ejecución y actúa cuando se detecta una amenaza.
- Reversión o limpieza: mantiene una pista de auditoría de los cambios realizados por el proceso en el endpoint. Cuando se detecta una amenaza, cierra automáticamente el proceso y revierte los cambios maliciosos realizados por este.
- Exclusión de procesos: posibilidad de excluir procesos de la monitorización.
- Realimentación con la red de protección global de Bitdefender (GPN): El Process Inspector informa inmediatamente de las amenazas detectadas a la nube de seguridad de Bitdefender, la red de protección global de Bitdefender (GPN), lo que garantiza que incluso sistemas al otro lado del planeta las detecten.

Beneficios

- Detecta anticipadamente ataques avanzados y evita vulneraciones, además de reducir el coste y el esfuerzo de respuesta ante incidentes.
- Reduce la carga de la persecución de amenazas.
- El Process Inspector aumenta en gran medida la tasa de detección de malware nuevo o evasivo, incluidos los ataques sin archivos, al permitir la monitorización de un proceso durante toda su vida útil y al confiar en las características de comportamiento reales en lugar de en firmas o en huellas binarias o de código.
- Protección contra malware ofuscado, ataques selectivos, malware personalizado, ataques basados en scripts, exploits, malware fragmentado, ataques de memoria, inyección de procesos, escalamiento de privilegios, ataques sin archivos (por ejemplo, uso ilegítimo de PowerShell) y ransomware.
- La reversión automática de cambios maliciosos en el sistema brinda tranquilidad a los equipos de seguridad.
- Está diseñado para funcionar desde un primer momento con una mínima o nula configuración y no requiere activar o escribir reglas complejas.
- La optimización inteligente del rendimiento para la monitorización de aplicaciones y procesos garantiza un bajo impacto en el sistema.
- La información sobre detecciones previas recopilada por el Inspector de procesos se utiliza para mejorar los modelos de aprendizaje automático responsables de la detección previa a la ejecución.
- Forma parte de un único agente de seguridad de endpoint integrado y de una plataforma de administración centralizada, lo que reduce en gran medida la carga administrativa. Los clientes no necesitan implementar una combinación de soluciones de seguridad de endpoints.

Bitdefender es una empresa global de tecnologías de seguridad que ofrece soluciones completas y de vanguardia para la seguridad informática y protección contra amenazas avanzadas a más de 500 millones de usuarios en más de 150 países. Desde 2001, Bitdefender ha desarrollado sistemáticamente tecnologías galardonadas de seguridad, destinadas a usuarios domésticos y empresariales, proporcionando soluciones de seguridad tanto para las infraestructuras híbridas de datacenter, como de protección para los endpoints. Con el apoyo de su I+D, y su red de alianzas y colaboraciones, Bitdefender disfruta del prestigio de ir en la vanguardia de la seguridad y ofrecer una gama de soluciones sólidas y de total confianza. Para obtener más información visite http://www.bitdefender.es

Bitdefender®

Todos los derechos reservados. © 2018Bitdefender. Todas las marcas registradas, nombres comerciales y productos citados en este documento pertenecen a sus respectivos propietarios. PARA MÁS INFORMACIÓN VISITE: www.bitdefender.es/business

BD-NGZ-Jan.30.2018-Tx#:
Bitdefender-2017-TechnicalBrief-ProcessInspector-crea2103-A4-es_ES