Sandbox Analyzer
Informe técnico

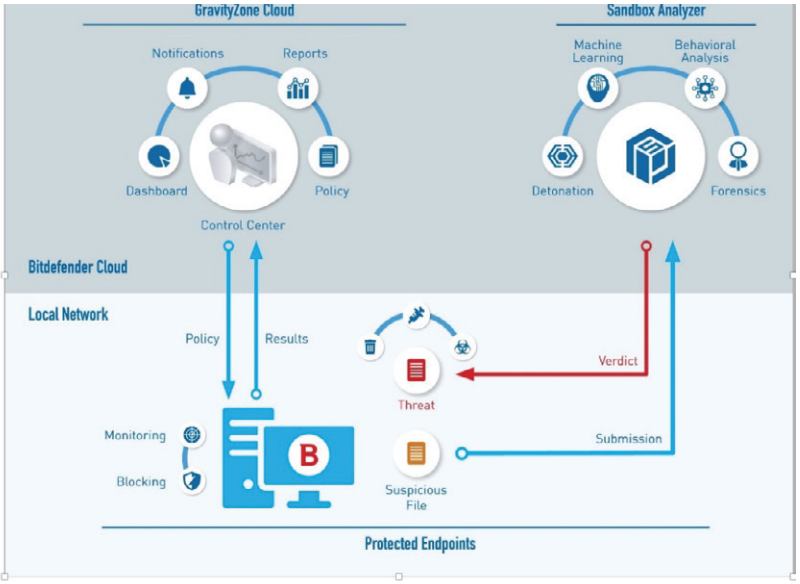
Resumen

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.

Bitdefender Sandbox Analyzer forma parte de la plataforma GravityZone Endpoint Security. Aporta detección previa a la ejecución contra ataques avanzados mediante el envío automático de archivos que requieran un análisis más detenido a un espacio aislado en la nube y la adopción de medidas de reparación basadas en el veredicto proporcionado.

Etapa de detección	Tipo de tecnología	Cobertura de amenazas
Pre-ejecución	Detonador (Sandbox)	APT, ataques selectivos, técnicas de evasión, malware ofuscado, malware personalizado, ransomware

Comprender la importancia de Sandbox Analyzer



Los autores de las amenazas toman una ya existente e introducen pequeñas modificaciones en su código para tratar de eludir las defensas del cliente basadas en firmas. Actualmente, muchas herramientas de seguridad han evolucionado para detectar al menos algunas de las amenazas polimórficas. No obstante, los atacantes más decididos, pacientes y hábiles invertirán tiempo y dinero en crear una amenaza completamente nueva. Estas amenazas podrían orientarse concretamente a una industria o a una organización o, en algunos casos, incluso a un individuo. Las organizaciones siempre corren el riesgo de sufrir brotes y vulneraciones a causa de estas amenazas evasivas. Sandbox Analyzer está diseñado para detectar y detener estas amenazas evasivas y evitar las vulneraciones anticipadamente, antes de que el archivo malicioso pueda incluso ejecutarse en el endpoint (detección previa a la ejecución). Esto se logra a través de la tecnología de espacios aislados basados en la nube. Cada vez que un usuario final accede a un portable ejecutable (PE) desconocido, Bitdefender aplica primero el Machine Learning y la tecnología HyperDetect para determinar si el archivo es malicioso. Luego, Bitdefender enviará automáticamente los archivos que requieran un análisis adicional al Sandbox Analyzer. En este Sandbox estudiará el archivo con algoritmos avanzados de Machine Learning, señuelos y técnicas antievasión, antiexploit y análisis de comportamientos agresivos. Dado que el archivo se analiza en un espacio aislado en lugar de en el endpoint, Bitdefender GravityZone puede realizar un estudio en profundidad sin preocuparse por el rendimiento y eliminar el riesgo de permitir que un archivo potencialmente malicioso se ejecute en el endpoint. Bitdefender permitirá o bloqueará la ejecución del archivo en el endpoint en función de la política administrativa. Si el veredicto es malicioso, Bitdefender también actualizará su red de protección global (servicio de inteligencia de amenazas en la nube de Bitdefender). Esto permitirá que todos los clientes de Bitdefender puedan recibir protección contra esta nueva amenaza sin que haya que volver a detonar el mismo archivo nuevamente.

Características

- Envío automático de archivos sospechosos desde el endpoint para el análisis en el Sandbox Analyzer. Las capas de prevención adicionales de Bitdefender GravityZone (detección de amenazas basada en el Machine Learning e HyperDetect) garantizan que solo se envíen al espacio aislado los archivos que requieran un análisis adicional.
- Reparación automática basada en el veredicto: bloqueo de las amenazas recién detectadas en toda la empresa y a nivel global.
- Hace uso de algoritmos avanzados de Machine Learning, análisis de comportamientos agresivos, técnicas antievasión y comparación de instantáneas de memoria para detectar amenazas.
- Cubre una amplia gama de tipos de archivos, entre los que se incluyen Microsoft Office, applets de Adobe Flash, Adobe Reader, applets de Java y archivos portables ejecutables (PEF).
- Alerta al usuario final cuando se realiza un análisis en el Sandbox.
- Admite los modos de monitorización y bloqueo.
- Posibilidad de enviar archivos manualmente.
- Obtención de una visibilidad anticipada con valiosos indicadores de compromiso (IOC).
- Proporciona informes detallados sobre el comportamiento del malware.
- Compatibilidad con endpoints físicos y virtuales: Bitdefender GravityZone - Security for Virtualized Environments (SVE).

Beneficios

- Detecta anticipadamente ataques avanzados y evita vulneraciones, además de reducir el coste y el esfuerzo de respuesta ante incidentes.
- Reduce la carga que supone la persecución de amenazas.
- Sandbox Analyzer aumenta en gran medida la tasa de detección de amenazas evasivas en la etapa previa a la ejecución, incluidas las APT, ataques selectivos, técnicas de evasión, malware ofuscado, malware personalizado y ransomware.
- El envío automático de los PE desde los endpoints a un servicio de espacio aislado basado en la nube reduce drásticamente la carga administrativa asociada habitualmente con la tecnología de espacios aislados.
- Las sólidas tecnologías de detección de comportamiento y de Machine Learning de Bitdefender garantizan que solo se envíen al espacio aislado los archivos que requieran un análisis más cuidadoso.
- Los informes detallados brindan al administrador de seguridad visibilidad del comportamiento del malware.
- Los modos de monitorización y bloqueo dotan al administrador de seguridad de la flexibilidad necesaria.
- 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.

BD-NGZ-Jan 30 2018-1-ar
Bitdefender-2017-TechnicalBrief-SandBoxAnalyzer-creat2103-A4-es_ES