Hoja de producto

GravityZone Security EDR Cloud

Detección y respuesta avanzadas en los endpoints

Los delincuentes informáticos son cada vez más sofisticados y los ataques avanzados actuales son cada vez más difíciles de detectar. Mediante técnicas que aisladamente parecen comportamientos rutinarios, un atacante puede acceder a su infraestructura y permanecer sin ser detectado durante meses, lo que aumenta significativamente el riesgo de una costosa vulneración de datos. Cuando su seguridad de endpoints actual no proporciona la detección y respuesta requeridas ante los ataques avanzados, añadir GravityZone EDR Cloud refuerza sus operaciones de seguridad de manera rápida y eficaz.

GravityZone EDR Cloud monitoriza su red para descubrir con prontitud las actividades sospechosas y le proporciona las herramientas que necesita para combatir los ataques informáticos. Al integrar el galardonado Machine Learning de Bitdefender, así como el análisis en la nube y el Sandbox Analyzer, puede detectar las actividades que eluden los mecanismos tradicionales de prevención en los endpoints. Proporciona una visibilidad completa de las técnicas, tácticas y procedimientos (TTP) que se utilizan en los ataques activos, al tiempo que proporciona capacidades integrales de búsqueda de indicadores de compromiso (IoC) concretos, técnicas MITRE ATT&CK y otros rastros que permiten descubrir los ataques con prontitud.

GravityZone EDR Cloud brinda visualizaciones innovadoras y fáciles de entender con un rico contexto e inteligencia sobre amenazas que ayudan al personal del departamento de informática a comprender las rutas de los ataques e identificar las brechas en la protección. Estas visualizaciones agilizan la investigación y la respuesta, lo que alivia la carga del personal de TI. Sandbox Analyzer permite ejecutar automáticamente contenidos sospechosos en un entorno virtual seguro para aislar y neutralizar los archivos sospechosos. Las capacidades de GravityZone EDR Cloud protegen a las organizaciones contra amenazas avanzadas, a la vez que permiten la búsqueda proactiva de amenazas y el análisis de causa raíz.

¿Cómo le ayuda GravityZone EDR Cloud?

- **Detección y respuesta ante ataques avanzados.** Monitoriza su red para descubrir con prontitud actividades sospechosas y proporciona las herramientas para permitirle combatir los ataques informáticos.
- **Cierre de la brecha en las habilidades de seguridad.** Permite que los equipos respondan eficientemente gracias a la priorización automatizada de alertas y la respuesta con un solo clic.
- **Reducción de los riesgos de ciberseguridad.** Analiza continuamente su infraestructura para identificar los riesgos en centenares de factores. Contribuye a mitigar los riesgos por los usuarios, la red y el sistema operativo.
- **Minimización de la carga operativa.** Suministrado a través de la nube y con poco mantenimiento, los agentes son fáciles de implementar e integrar en su arquitectura de seguridad existente y es totalmente compatible con su solución antivirus para endpoints.

Innovación para la eficiencia y la

Bitdefender
BUILT FOR RESILIENCE

En resumen

GravityZone EDR Cloud detecta en tiempo real amenazas avanzadas, incluidos ataques sin archivos, ransomware y otras amenazas de día cero. Su análisis de amenazas y su recopilador de eventos basado en la nube monitorizan continuamente los endpoints y priorizan los eventos de seguridad en una lista de incidentes para su investigación y respuesta. Bitdefender EDR proporciona visualizaciones innovadoras y fáciles de entender con un rico contexto e inteligencia sobre amenazas que ayudan al personal de TI a comprender las rutas de los ataques e identificar las brechas en la protección. Estas visualizaciones agilizan la investigación y la respuesta, lo que alivia la carga del personal de TI.

Principales beneficios

- Detección líder del sector: Detección de amenazas y visibilidad mejoradas que posibilitan las fortalezas de XDR para proteger los endpoints. Capacidades integrales de búsqueda de indicadores de compromiso (IoC) concretos, técnicas MITRE ATT&CK y otros rastros que permiten descubrir los ataques con prontitud.
- Investigación y respuesta focalizadas: La visualización de incidentes a nivel de la organización le permite responder eficientemente, limitar la propagación lateral y detener los ataques en curso.
- Máxima eficiencia: Nuestro agente fácil de implementar y con escasa sobrecarga garantiza la máxima eficiencia y protección con un mínimo esfuerzo. Para disfrutar de una solución totalmente administrada,puede contratar fácilmente los servicios de detección y respuesta administradas (MDR) de Bitdefender.

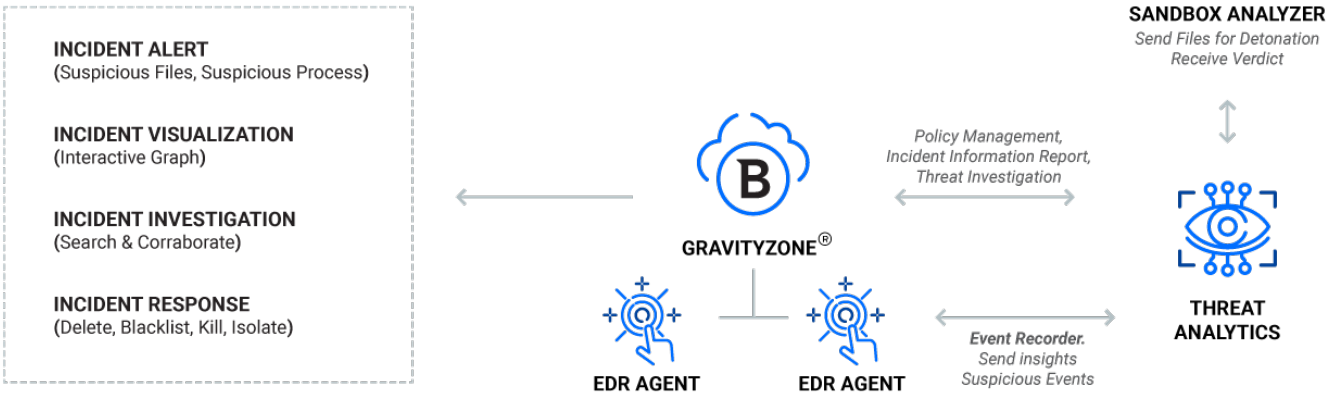
"Las capacidades de EDR de GravityZone nos brindan informes detallados sobre cómo se vieron afectados los procesos durante toda la cadena de los incidentes. Eso nos ahorra una inmensa cantidad de tiempo de investigación, ya que se elimina el trabajo manual".

Sascha Neuhaus, director de seguridad informática de Louis

eficacia

La tecnología de correlación entre endpoints de Bitdefender eleva la capaidad de detección de amenazas y la visibilidad al aplicar funcionalidades específicas de XDR para detectar ataques avanzados que involucran a múltiples endpoints de infraestructuras híbridas (estaciones de trabajo, servidores o contenedores y en varios sistemas operativos). Amplía las capacidades de correlación de eventos, análisis y visibilidad de la EDR más allá de los límites de un solo endpoint, para permitir a los equipos de seguridad lidiar más eficazmente con ataques informáticos complejos que afecten a varios endpoints. Esta tecnología de correlación entre endpoints combina la granularidad y la riqueza del contexto de seguridad de la EDR con el análisis en toda la infraestructura que aporta la detección y respuesta ampliadas (XDR). Al proporcionar visualizaciones de amenazas a nivel de las organizaciones, la XDR les ayuda a centrar sus investigaciones y responder con mayor eficacia.

Cómo funciona



GravityZone EDR Cloud es una solución basada en la nube construida sobre la plataforma de Bitdefender GravityZone XDR. Cada agente de EDR implementado en los endpoints de su organización tiene un registrador de eventos que monitoriza continuamente el endpoint y envía de manera segura la información y los detalles de eventos sospechosos al GravityZone Control Center centralizado. En el Control Center, el motor de correlación de endpoints de Bitdefender recopila y destila los eventos de los endpoints y genera vistas priorizadas de los incidentes de seguridad a nivel de la organización, lo que permite a los administradores investigar con rapidez y responder eficazmente a las amenazas.

Bitdefender
BUILT FOR RESILIENCE

3945 Freedom Circle
Ste 500, Santa Clara
California, 95054, Estados Unidos

Bitdefender es líder mundial en seguridad informática y ofrece las mejores soluciones de prevención, detección y respuesta ante amenazas en todo el mundo. Bitdefender, que vela por millones de entornos domésticos, empresariales y gubernamentales, es uno de los expertos que más confianza inspira en el sector para eliminar amenazas, proteger la privacidad y los datos y facilitar la resiliencia informática. Gracias a sus grandes inversiones en investigación y desarrollo, los laboratorios de Bitdefender descubren más de 400 nuevas amenazas por minuto y procesan diariamente unas 40 000 millones de consultas sobre amenazas. La empresa ha sido pionera en innovaciones revolucionarias en el campo de la seguridad de IoT, antimalware, análisis del comportamiento e inteligencia artificial, y más de 150 de las marcas de tecnología más reconocidas del mundo licencian su tecnología. Fundada en 2001, Bitdefender tiene clientes en más de 170 países con oficinas por todo el mundo.

Para más información, visite https://www.bitdefender.es.

Bitdefender-BSG-GZ-EDRCloud-Datasheet-DEX4610-es_ES
CD-Apr/10/2022 • MD-Apr/10/2022