Bitdefender GravityZone Ultra Suite

Unificación de la prevención, detección, respuesta y análisis de riesgos en los endpoints

GravityZone Ultra, con más de treinta capas de tecnologías de protección, es la primera solución en ofrecer la defensa más eficaz del mundo integrada con una EDR con escasa sobrecarga y Análisis de riesgos en los endpoints en un solo agente con arquitectura de consola única. Esto reduce drásticamente la superficie de ataque en los endpoints, lo que ayuda a las empresas de cualquier tamaño a evitar vulneraciones, simplificar la administración de la seguridad y reducir drásticamente el coste de las operaciones de protección. GravityZone Ultra proporciona lo siguiente:

- **La protección de endpoints más eficaz del mundo** que encabeza regularmente las pruebas de prevención independientes.
- **Detección y respuesta en los endpoints con escasa sobrecarga,** lo que facilita que cualquier organización de TI adopte la EDR, mejore el tiempo de respuesta y reduzca los gastos de personal que conlleva la EDR.
- **El Análisis integrado de riesgos en los endpoints** analiza constantemente sus endpoints en busca de configuraciones incorrectas y efectúa recomendaciones para reducir la superficie de ataque.
- **Una consola única con agente único** para todas las características, incluyendo administración de parches, cortafuego, cifrado, control de aplicaciones, control de contenido, etc.
- Los módulos complementarios opcionales de **Administración de parches,** , **Seguridad avanzada de correo electrónico** y **Protección de datos** agilizan los procesos de seguridad y reducen el tiempo de respuesta ante incidentes.
- El resultado es una **óptima prevención de amenazas, una detección precisa de incidentes y un endurecimiento inteligente** que minimizan la exposición ante infecciones y detienen las vulneraciones.
- **Bloquea la mayoría de los ataques en la fase previa a la ejecución,** antes de que afecten a su sistema, gracias a la inspección de procesos en tiempo real con aprendizaje automático y al análisis automatizado en espacio aislado.
- Una sola solución que cubre implementaciones **físicas,** , **virtuales** y en la **nube** desde una sola consola
- Solución opcional de **Network Threat Analytics** que proporciona información sobre IoT y posibles amenazas de red.
- Protección para entornos complejos y heterogéneos: GravityZone Ultra, como conjunto integrado de protección de endpoints, le garantiza un nivel constante de seguridad en todas sus plataformas, desde Windows™ hasta macOS, Linux, VMware™ iOS, Android o AWS™. El resultado de ello es que los atacantes no pueden encontrar brechas en la protección que poder aprovechar. GravityZone Ultra se basa en una arquitectura sencilla e integrada con administración centralizada para los endpoints y el centro de datos. Permite a las

Beneficios Principales

GravityZone Ultra, la principal suite de seguridad de Bitdefender, proporciona a los analistas de seguridad y a los equipos de respuesta ante incidentes las herramientas que necesitan para analizar actividades sospechosas e investigar y responder de manera adecuada a las amenazas avanzadas:

- Líder mundial en prevención de amenazas
- Detección en tiempo real y reparación automática
- Rápida priorización de incidentes, investigación y respuesta
- Detección de actividades sospechosas
- Análisis de riesgos de configuración
- Respuesta ante incidentes con un solo clic
- Endurecimiento automático
- Búsqueda de datos actuales e históricos para la localización de amenazas
- Etiquetado de eventos MITRE

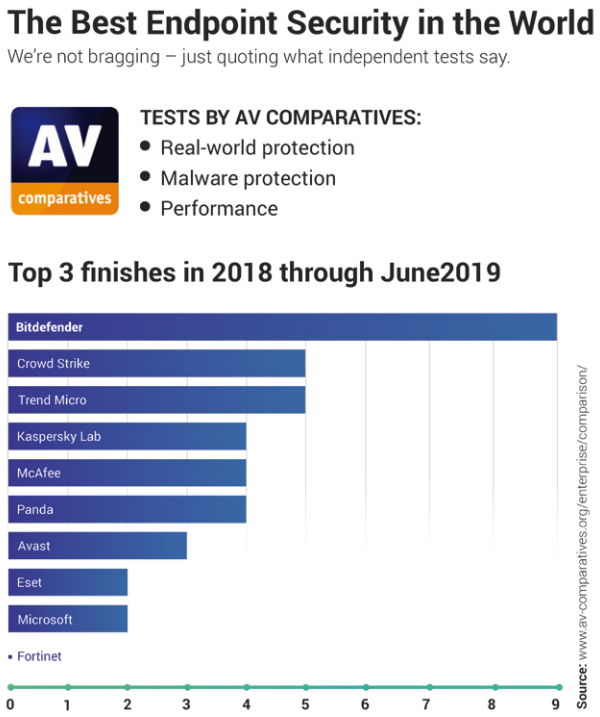
empresas implementar rápidamente la solución de protección de endpoints y requiere un menor esfuerzo de administración después de la implementación.

La protección de endpoints más eficaz del mundo

Para la defensa de extremo a extremo contra violaciones de la seguridad

Más de treinta tecnologías de protección desarrolladas a lo largo de 18 años por los investigadores, matemáticos y científicos de datos de talla internacional de Bitdefender dan como resultado una protección superior cuya licencia utilizan actualmente más del 38 % de los productos de seguridad de TI.

- **Aprendizaje automático local y basado en la nube:** Bitdefender incorporó por primera vez el aprendizaje automático en 2009, con el resultado de una mayor detección de amenazas con escasos falsos positivos y la posibilidad de detener amenazas desconocidas en la fase previa a la ejecución y a lo largo de esta.
- **HyperDetect, aprendizaje automático optimizable- Permite a los equipos de TI optimizar la protección en servicios empresariales sensibles que corren el mayor riesgo.**
- **Defensa contra anomalías:** Tecnología avanzada de aprendizaje automático que determina los servicios normales del sistema y los monitoriza para detectar técnicas de ataque sigiloso. Es capaz de proteger aplicaciones personalizadas frente a ataques maliciosos.
- **Entorno de pruebas basado en la nube:** 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 con la adopción de medidas de reparación basadas en el veredicto proporcionado.
- **Network Attack Defense:** Detecta y bloquea nuevos tipos de amenazas al principio de la cadena de ataque, como ataques de fuerza bruta, ladrones de contraseñas o movimientos laterales
- **Defensa contra exploits:** Varios motores de prevención de exploits protegen la memoria y bloquean los ataques antes de que se aprovechen de los sistemas, lo que reduce los esfuerzos de priorización.
- **Defensa contra ataques sin archivos:** Detecte y bloquee malware basado en scripts, sin archivos, ofuscado y personalizado, con reparación automática.
- Cortafuego integrado, control de dispositivos, filtrado de contenidos web, control de aplicaciones y muchos más modulos en el mismo agente.
- **Módulos complementarios:** Seguridad de correo electrónico, Cifrado de disco completo y Administración de parches.



Bitdefender ha alcanzado el primer puesto en las pruebas de protección de AV-Comparatives™ más veces que ningún otro proveedor

GRAVITYZONE ULTRA TECHNOLOGY MAP

GravityZone Ultra es lo último en protección, detección, respuesta y análisis de riesgos avanzados, diseñado para abordar todo el ciclo de vida de la amenaza. Con GravityZone Ultra, puede reducir el número de proveedores a la vez que disminuye el tiempo necesario para responder a las amenazas a través de una pila de seguridad integrada.

EDR fácil y con escasa sobrecarga

Completas herramientas de investigación pensadas para organizaciones de cualquier tamaño.

Gracias a una clara visibilidad de los indicadores de compromiso (IOC) y los flujos de trabajo de respuesta a incidentes e investigación de amenazas en un solo clic, GravityZone Ultra reduce los recursos y las habilidades necesarias para los miembros de los equipos de seguridad.

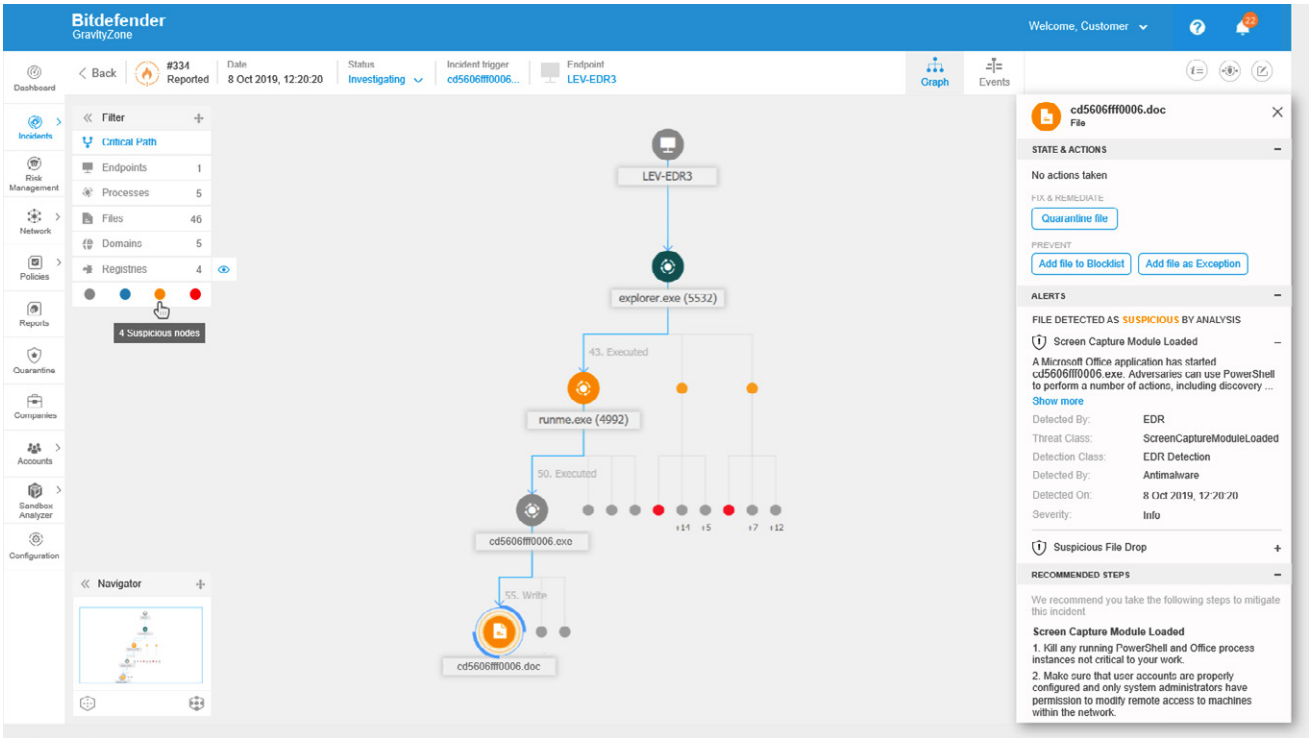
El módulo de análisis de amenazas trabaja en la nube y filtra continuamente los eventos de comportamiento en las actividades del sistema para crear una lista priorizada de incidentes merecedores de investigación y respuesta adicionales.

Una respuesta adecuada habilitada por una prevención avanzada

Dado que GravityZone Ultra es una solución integrada de prevención-detección-respuesta, le permite responder rápidamente y restaurar los endpoints a una situación anterior. Aprovechando la información de inteligencia sobre amenazas recopilada desde los endpoints durante el proceso de investigación, una única interfaz proporciona las herramientas para ajustar de inmediato la política y parchear las vulnerabilidades para evitar incidentes futuros y mejorar la seguridad de su entorno.

Ultra cumple con los requisitos de EDR convencionales:

- Detección y visualización de actividades sospechosas
- Detección de anomalías
- Análisis de causa raíz
- Etiquetado de eventos MITRE
- Puntuación de confianza respecto a la amenaza
- Indicadores de ataque
- Shell de comandos remotos
- Investigación guiada de incidentes
- Opciones avanzadas de contención de amenazas
- Análisis de Sandbox
- Servicio opcional de detección y respuesta administradas

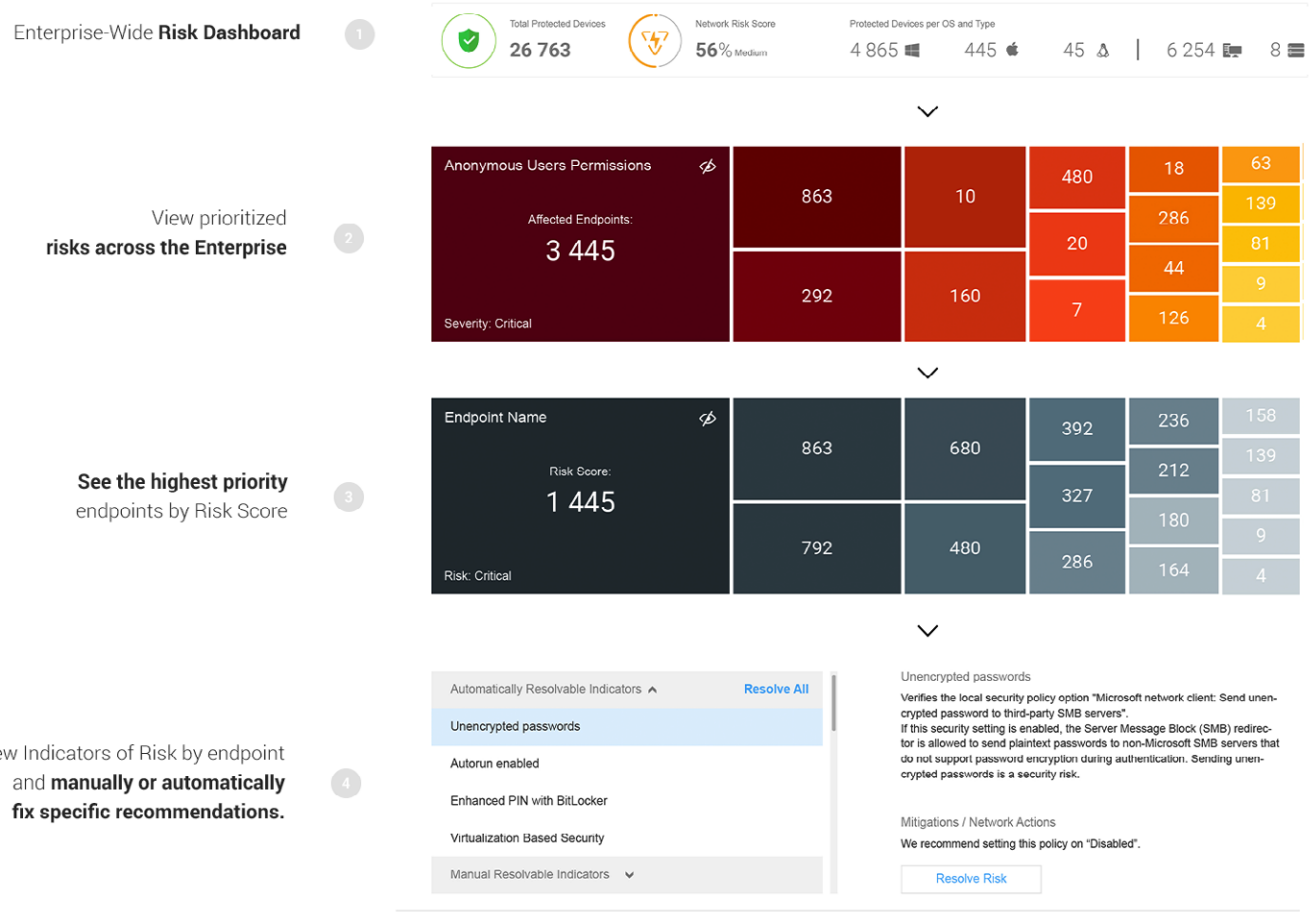


La detección y respuesta avanzadas muestran con precisión cómo funciona una amenaza potencial y el contexto en su entorno. Las técnicas de ataque MITRE y los indicadores de compromiso brindan información actualizada al minuto sobre las amenazas identificadas y sobre cualquier otro malware que pueda estar implicado. Las guías visuales fáciles de entender resaltan las rutas de ataque críticas, lo que alivia la carga del personal de TI.

Análisis de riesgos en los endpoints para una gestión continua de la superficie de ataque

Permite procesos activos de endurecimiento del sistema en toda la empresa

El motor de análisis de riesgos en los endpoints de Bitdefender permite a las organizaciones evaluar, priorizar y endurecer continuamente los ajustes y configuraciones erróneas de seguridad en los endpoints gracias a una lista de prioridades fácil de entender. Gracias a análisis de riesgos únicos, se produce una reducción continua de la superficie de ataque.



Aborde la escasez de habilidades de seguridad y evite la fatiga por las alertas

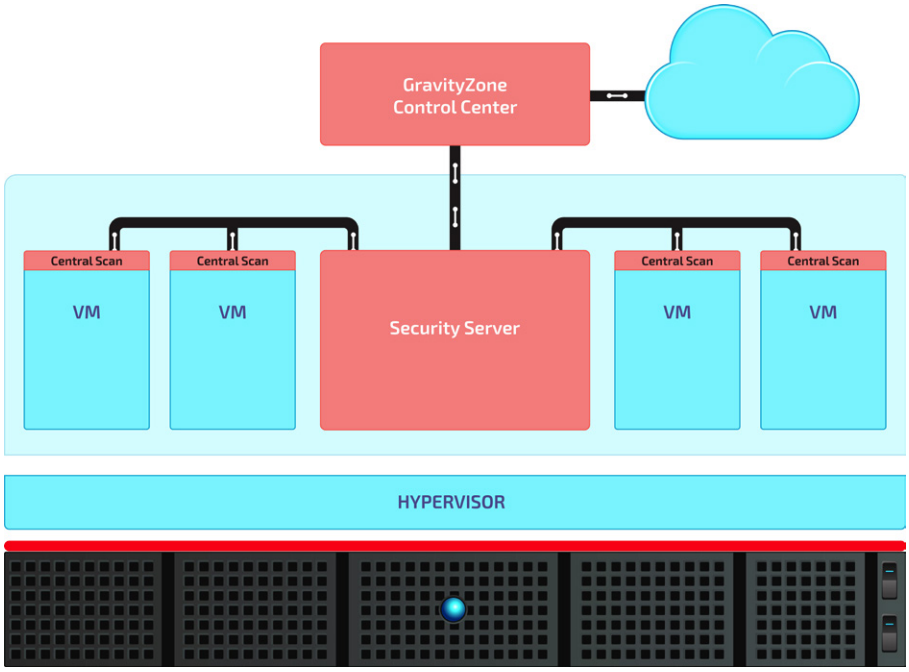
Solo se presentan eventos relevantes, relacionados y con calificación de gravedad para su análisis y resolución manual. Se minimiza el ruido y la información redundante, ya que la gran mayoría de los ataques normales y avanzados se bloquean en la fase de pre-ejecución o al inicio de la ejecución. Las amenazas evasivas, incluido el malware sin archivos, los exploits, el ransomware y el malware escondido, se neutralizan gracias a las altamente eficaces tecnologías de prevención por capas y de última generación para endpoints y al inspector de procesos basado en el comportamiento durante la ejecución. La respuesta y reparación automáticas eliminan la necesidad de intervención humana en los ataques bloqueados.

La detección, altamente fiable, permite que el personal de seguridad se centre solo en incidentes y amenazas reales:

- Disminuye el ruido y la distracción que suponen los falsos positivos
- Reduzca el volumen de incidentes con una prevención eficaz de amenazas
- Olvídese de la reparación manual de los ataques bloqueados gracias a la reparación automática

Protección del centro de datos

Desde la arquitectura unificada de Ultra, es posible administrar y proteger por completo las plataformas de centros de datos con escasa sobrecarga informática. . Se incluye GravityZone Security for Virtualized Environments (SVE), que es la solución de seguridad para centros de datos virtualizados más avanzada del mercado en cuanto a protección antimalware para máquinas virtuales y que optimiza no solo los ratios de consolidación, sino también los costes operativos. GravityZone SVE es una solución empresarial compatible incluso con los centros de datos más grandes. La integración en un entorno de producción es sencilla y pueden beneficiarse de esta tecnología entornos virtuales de cualquier tamaño.



- Visibilidad en una sola consola y capacidad de administración centralizada en arquitecturas de nube híbrida.
- Densidad de VM maximizada, baja latencia de arranque y rendimiento óptimo de aplicaciones
- Diseñado para permitir la transformación del centro de datos: SDDC, hiperconvergencia y la nube híbrida
- Integraciones totales con VMware, Nutanix, Citrix, AWS y Microsoft para proteger su inversión, automatizar la implementación y administrar inventarios y licencias.
- Compatible con varios entornos de virtualización y cloud con una sola instancia de implementación
- Arquitectura eficiente, resistente y escalable basada en SVA compatible con todos los hipervisores

Administración de GravityZone Ultra: control y escalabilidad de nivel corporativo

El centro de administración de GravityZone, probado con implementaciones de más de 120 000 endpoints, es una consola de administración integrada y centralizada que proporciona una visibilidad en una sola consola de todos los componentes de administración de la seguridad, incluida la seguridad de endpoints, la seguridad de centros de datos, la administración de parches, el análisis de riesgos, la generación de informes y mucho más. La administración de políticas basadas en roles de GravityZone, alojado en la nube en los centros de datos de alta seguridad de Bitdefender, admite múltiples políticas y roles anidados.

Para conocer los requisitos detallados del sistema, consulte https://www.bitdefender.com/business/gz-ultra.html

Integración de partners del ecosistema de terceros

Admite la integración con sus herramientas de operaciones de seguridad existentes (incluyendo Splunk) y se ha optimizado para tecnologías de centros de datos, incluidos los principales hipervisores.

Para más información, visite https://www.bitdefender.com/business/enterprise-products/ultra-security.html

O póngase en contacto con su partner local de Bitdefender.

esta página se ha dejado en blanco intencionadamente

Bitdefender

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 de seguridad galardonadas, 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 estar 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

BD-NGZ-Nov.12-2019-TM-new2.tdt
Bitdefender-NGZ-UltraSuite-Datasheet-CREA T3989-A4-v-es_ES