Bitdefender GravityZone Ultra Suite

DESCUBRA Y DETENGA LAS AMENAZAS EVASIVAS CON PRECISIÓN Y AGILIDAD

GravityZone Ultra, con Endpoint Security XDR, destaca sobre los productos especializados de EDR, demasiado complejos y ruidosos, al prevenir, detectar y responder a los ataques sofisticados que eluden el antimalware tradicional. GravityZone Ultra ofrece en una única suite de seguridad unificada lo siguiente:

- Reducción de la superficie de ataque (mediante cortafuego, control de aplicaciones, control de contenidos y gestión de parches).
- Protección de datos (a través del cifrado de disco completo).
- Detección y erradicación de malware antes de su ejecución (mediante el Machine Learning optimizable, la inspección de procesos en tiempo real y el análisis en Sandbox).
- Detección automatizada, fácil investigación y reparación in situ gracias al nuevo registro de eventos de endpoints y al análisis de amenazas de Endpoint Security XDR.

El resultado es una óptima prevención de amenazas, una detección precisa de incidentes y una respuesta inteligente que minimizan la exposición ante las infecciones y detienen las vulneraciones.

Como suite integrada de protección de endpoints, GravityZone Ultra garantiza un nivel constante de seguridad para todo el entorno de TI, de modo que los atacantes no hallen endpoints poco protegidos que utilizar como puntos de partida para acciones maliciosas contra la organización. GravityZone Ultra se basa en una arquitectura sencilla e integrada con administración centralizada para los endpoints y el centro de datos. Permite a las empresas implementar rápidamente la solución de protección de endpoints y requiere un menor esfuerzo de administración después de la implementación.

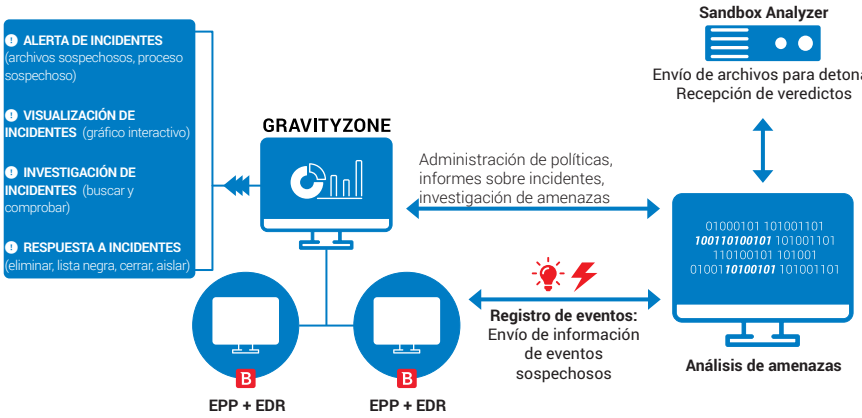


Figura 1. Bitdefender XDR: prevención, detección y respuesta en un solo agente, administrado mediante la consola GravityZone

EDR fácil

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 equipos de seguridad. El nuevo registro de datos de endpoints es una incorporación perfecta al elenco existente de herramientas de protección contra amenazas y plasma un amplio registro de las actividades del sistema (creación de archivos y procesos, instalación de programas, carga de módulos, modificación de registros, conexiones de red, etc.) para contribuir a una visión en toda la empresa de la cadena de eventos involucrados en el ataque.

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.

Beneficios Principales

Endpoint Security XDR, más allá de las funciones tradicionales de EPP, proporciona a los analistas de seguridad y a los equipos de respuesta a incidentes las herramientas que necesitan para analizar actividades sospechosas e investigar y responder de manera adecuada a las amenazas avanzadas:

- Visibilidad de endpoints en tiempo real
- Pone en evidencia las actividades sospechosas
- Investigación con un solo clic
- Protocolo de intervención ante alertas y visualización de análisis de incidentes
- Rastreo de los ataques activos y los movimientos laterales
- Respuesta rápida
- Reduce el tiempo de ocupación con una rápida resolución, contención y reparación

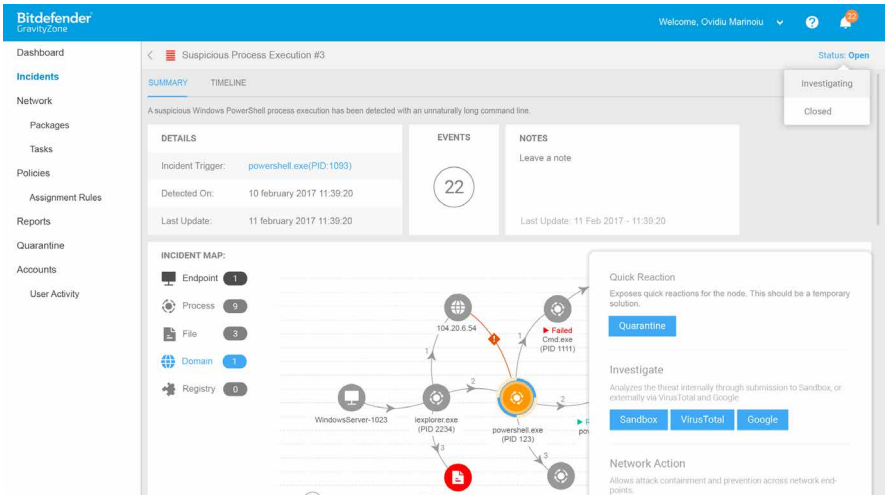


Figura 2. La página de detalles del incidente proporciona una descripción clara del alcance de los incidentes. El profesional puede obtener fácilmente pruebas y responder en consecuencia.

Mejora la visualización de la seguridad. Evita la fatiga ocasionada por las alertas.

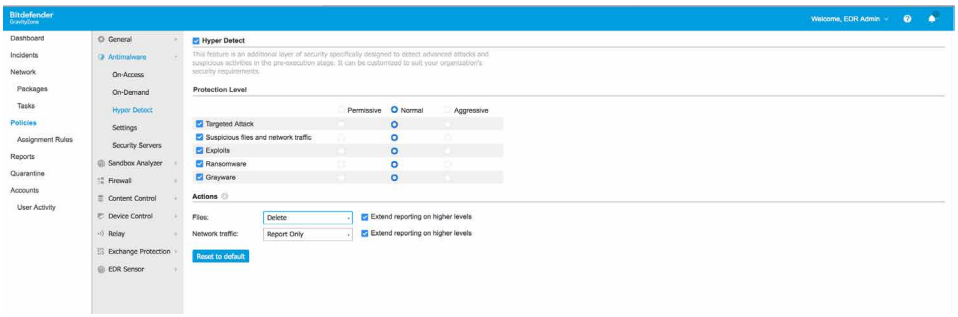
Solo se presentan eventos relevantes, relacionados y con calificación de gravedad para su análisis y resolución manual. Se minimiza el ruido y la información redundante, ya que la gran mayoría de los ataques normales y avanzados se bloquean en la fase de pre-ejecución o al inicio de la ejecución. Las 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:

- Minimice el ruido y la distracción que suponen las falsas alarmas
- 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

Una respuesta inteligente significa una prevención avanzada

Dado que GravityZone Ultra es una solución que cubre todo el ciclo prevención-detección-respuesta, permite una respuesta rápida y una restauración efectiva a un estadio seguro. 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.



Completa plataforma de seguridad de endpoints en un agente y una consola

GravityZone Ultra hereda todo el refuerzo y los controles de prevención de última generación incluidos en Endpoint Security HD y en la suite GravityZone Elite:

- Reduce la exposición con una sólida prevención
- La detección basada en el Machine Learning y el comportamiento atajan las amenazas desconocidas en la fase de pre-ejecución y al inicio de la ejecución
- Detecta y bloquea el malware basado en scripts, sin archivos, escondido y personalizado, con reparación automática
- Protección de memoria para prevenir exploits
- Reduce la superficie de ataque habilitando controles de seguridad TI
- Integrando un cortafuego bidireccional, control de dispositivos, filtrado de contenidos web, control de aplicaciones, gestión de parches y muchas otras características.

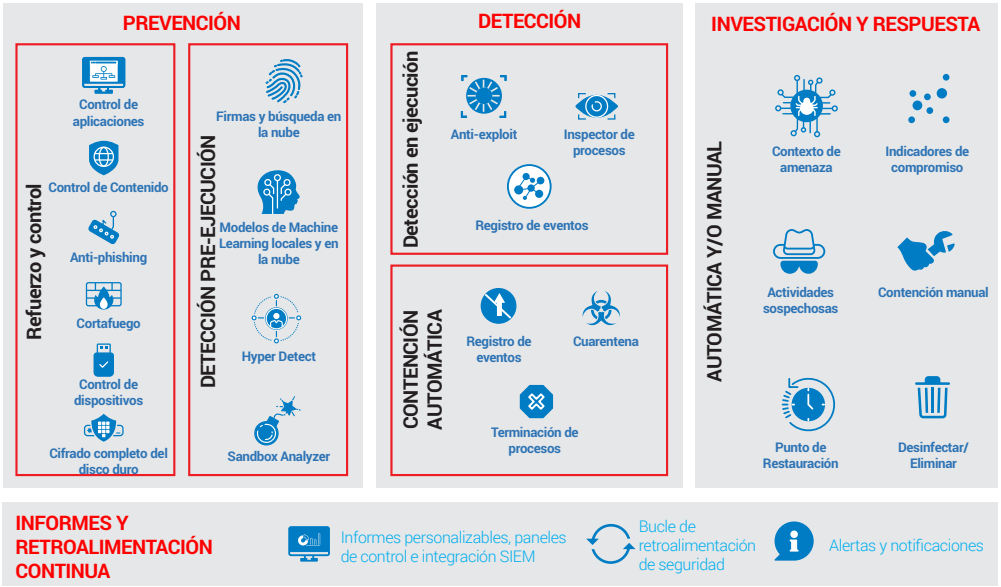
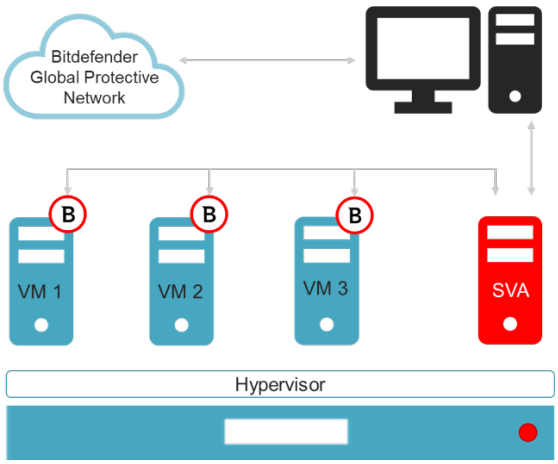


Figura 3. Bitdefender XDR: la plataforma completa de seguridad para endpoints

Protección del centro de datos

Completamente integrado con Bitdefender Endpoint Security XDR, el componente de protección de centros de datos de la suite GravityZone Elite es Security for Virtualized Environments (SVE). Es la solución de seguridad para centros de datos más avanzada del mercado en cuanto a la protección antimalware para máquinas virtuales, optimizando 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.

Beneficios Principales



Agilidad
SVE permite la automatización de la seguridad en todo el ciclo de vida del centro de datos durante la implantación, así como a lo largo de las operaciones de seguridad cotidianas de un entorno virtual muy dinámico. Se integra con VMware (vCenter, vShield, NSX), Citrix XenCenter y Nutanix Enterprise Cloud Platform, y permite el rápido aprovisionamiento automatizado.

Eficiencia Operativa
La consola de administración unificada Control Center de GravityZone simplifica la implementación, el mantenimiento y la actualización de la seguridad, y proporciona una visibilidad centralizada de todas las estaciones de trabajo y servidores físicos y virtuales. Es compatible con la creación centralizada y la administración automática de políticas de seguridad para ayudar a optimizar las operaciones de TI y mejorar el cumplimiento.

Mejor utilización de la infraestructura
El análisis centralizado y un agente muy liviano reducen en gran medida el uso

de memoria, espacio de disco, CPU y actividad de E/S en servidores host, lo que aumenta la densidad de máquinas virtuales y el ROI en la infraestructura TI.

Compatibilidad universal
Compatible con las principales plataformas de hipervisor (VMware ESXi, Microsoft Hyper-V, Citrix Xen, Red Hat KVM y Nutanix AHV), tanto con Windows como con Linux como sistemas operativos de guest.

Escalabilidad lineal ilimitada
Se pueden usar varios SVA para aumentar la capacidad de análisis a medida que crece el centro de datos y se crean más máquinas virtuales. Cuando un SVA existente alcanza un cierto umbral de carga, se pueden implementar otros nuevos para dar respuesta a ese crecimiento. Un beneficio adicional de la implementación de varios SVA es la mejora de la capacidad de recuperación y el reparto de la carga: la carga de un SVA fallido o sobrecargado puede asumirla otro SVA activo o menos cargado.

Defensas por capas de última generación
GravityZone Security for Virtualized Environments incorpora todas las capas de seguridad clave de Endpoint Security, incluyendo HyperDetect, Sandbox Analyzer y métodos de detección de ataques sin archivos para proporcionar una protección líder para los activos digitales de la empresa almacenados o procesados en el centro de datos.

Características

- Diseñado para permitir la transformación del centro de datos: SDDC, hiperconvergencia y la nube híbrida
- Integracion total 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 implementación
- Visibilidad en un único panel y capacidad de administración centralizada de toda la nube híbrida
- Arquitectura eficiente, resistente y escalable basada en SVA compatible con todos los hipervisores
- Densidad de VM maximizada, baja latencia de arranque y rendimiento óptimo de aplicaciones
- Seguridad avanzada por capas con cobertura continua en toda la nube híbrida

GravityZone Control Center

El Control Center de GravityZone es la consola de administración integrada y centralizada que proporciona una única consola para todos los componentes de administración de la seguridad, incluida la seguridad de endpoints, la del centro de datos, la de Exchange y la de los dispositivos móviles. Puede alojarse en la nube o implementarse localmente. El centro de administración de GravityZone incorpora varios roles e incluye el servidor de bases de datos, el de comunicaciones, el de actualizaciones y la consola web. Control Center se suministra como una imagen de appliance virtual y se puede implementar en menos de treinta minutos. En empresas de mayor tamaño, se puede configurar una arquitectura con varios appliances virtuales, con diversas instancias de roles específicos y con balanceador de carga incorporado, para ofrecer una gran escalabilidad y disponibilidad.

Para una lista más detallada de los requerimientos del sistema por favor dirigirse a www.bitdefender.es/business/ultra-security

Bitdefender®

Bitdefender es una empresa de tecnología de seguridad a escala mundial 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

BD-NGZ-Nov.21.2017-Tk#: crea2183
Bitdefender-NGZ-UltraSuite-Datasheet-creat2199-A4-es_ES