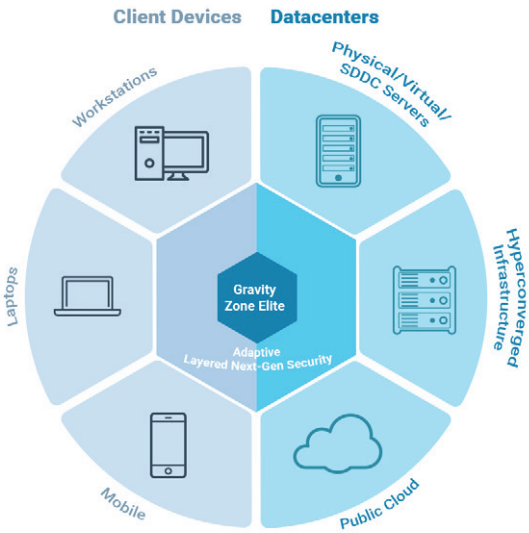
Suite Bitdefender GravityZone Elite

La plataforma de seguridad por capas y de última generación

La suite Bitdefender GravityZone Elite está diseñada para proteger a las empresas contra el espectro completo de sofisticadas amenazas informáticas con rapidez y precisión. Elite combina la probada filosofía de seguridad por capas de Bitdefender con sus herramientas y tecnologías de última generación para proporcionar un rendimiento y protección de alto nivel para todos los endpoints en el entorno empresarial: equipos de escritorio, portátiles, móviles y servidores físicos y virtuales.

GravityZone Elite garantiza un nivel de seguridad consistente para todo el entorno de TI, y limita los endpoints mal protegidos que podrían servir como puntos de partida para acciones maliciosas contra la organización. Se basa en una arquitectura sencilla e integrada con administración centralizada para los endpoints y el centro de datos. Las opciones de consola en la nube y on-premise se adaptan tanto a los entornos preparados para la nube como a los estrictamente regulados.



PUNTOS DESTACADOS

- Detecta y bloquea los ataques de malware sin archivos
- Detenga los ataques basados en scripts
- Descomprime y analiza malware desconocido en la fase previa a su ejecución
- Agente único, pequeña huella con bajo impacto en el sistema
- Consola de administración integrada para endpoints físicos y virtuales

Protección de endpoint

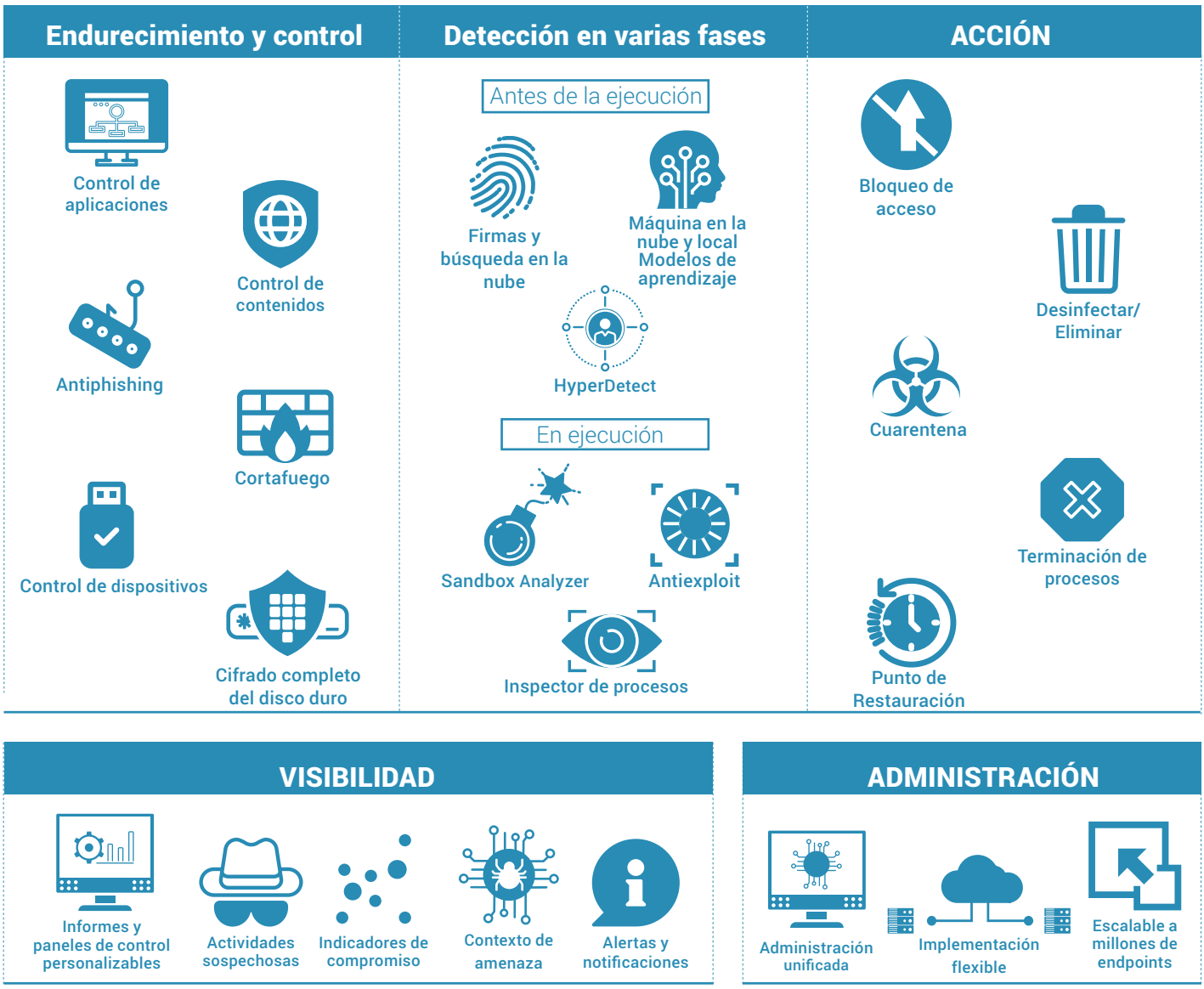
Bitdefender Endpoint Security HD (el componente de seguridad de endpoints de GravityZone Elite) protege a las empresas contra todo tipo de amenazas digitales sofisticadas con rapidez, precisión, escasa carga administrativa y un mínimo impacto en el sistema. Esta solución de última generación elimina la necesidad de ejecutar varias soluciones de seguridad para endpoints en una máquina, al combinar controles preventivos, técnicas de detección sin firmas a varios niveles, y respuesta automática.

Beneficios Principales

Detecta y bloquea todo tipo de amenazas sofisticadas y de malware desconocido
Endpoint Security HD vence el malware desconocido y las amenazas avanzadas que eluden las soluciones tradicionales de protección de endpoints, incluyendo el ransomware. Los ataques avanzados, como los de PowerShell, basados en scripts, los ataques sin archivos y el malware sofisticado, pueden detectarse y bloquearse antes de que se ejecuten.

Detectar y atajar el malware sin archivos
Los ataques de malware sin archivos ejecutan código malicioso directamente en la memoria. Dado que no hay ningún archivo en el disco, la mayoría de las soluciones antivirus diseñadas para el análisis de archivos están ciegas ante este tipo de ataques. Bitdefender aprovecha su Antiexploit avanzado, HyperDetect™ y el Inspector de procesos para detectar, bloquear e interrumpir los ataques sin archivos.

Detener los ataques basados ??en macros y en scripts
En este caso, la amenaza proviene de macros de MS Office de confianza que utilizan herramientas de administración de Windows como PowerShell para ejecutar scripts y descargar código malicioso para ejecutar los ataques. Dado que se trata de herramientas de Windows "de confianza", la mayoría de los productos de seguridad de endpoints, incluidos los llamados proveedores antivirus de última generación, no analizan los scripts, como Powershell, WMI, intérpretes de Javascript, etc. Bitdefender añade técnicas de analizador de línea de comandos para interceptar y dar seguridad a los scripts, al tiempo que alerta a los administradores y bloquea la ejecución del script en caso de que ejecute comandos maliciosos.



Reparación y respuesta automatizada frente a amenazas
Una vez que se detecta una amenaza, Endpoint Security HD la neutraliza de inmediato a través de acciones que incluyen la terminación del proceso, la puesta en cuarentena, la eliminación y la reversión de los cambios maliciosos. Comparte la información sobre amenazas en tiempo real con GPN, el servicio de inteligencia contra las amenazas basado en la nube de Bitdefender, para parar ataques similares en cualquier parte del mundo.

Consiga visibilidad y contexto acerca de las amenazas
La capacidad única de Bitdefender Endpoint Security HD para identificar e informar de actividades sospechosas facilita a los administradores la alerta temprana de los comportamientos maliciosos, como son las acciones dudosas del sistema operativo, las acciones evasivas y las conexiones a centros de comando y control.

Aumente la eficiencia operativa con un solo agente y una consola integrada
El agente unificado, integrado, de seguridad para endpoints de Bitdefender elimina las molestias en escoger y gestionar varios agentes. Su diseño modular ofrece la máxima flexibilidad y permite a los administradores establecer políticas de seguridad. GravityZone personaliza automáticamente el paquete de instalación y minimiza la carga del agente. Diseñado desde el principio para las arquitecturas de seguridad post-virtualización y post-cloud, GravityZone proporciona una plataforma de administración de seguridad unificada para proteger entornos físicos, virtualizados y en la nube.

Características

Machine Learning
Las técnicas de Machine Learning utilizan modelos y algoritmos extensamente entrenados para predecir y bloquear los ataques avanzados. Los modelos de Machine Learning de Bitdefender se basan en 40 000 características estáticas y dinámicas, y se entrenan continuamente con miles de millones de muestras de archivos legítimas y maliciosas recopiladas en más de 500 millones de endpoints de todo el mundo. Así se mejora drásticamente la efectividad de la detección del malware y se minimizan los falsos positivos.

HyperDetect
Este nuevo nivel de protección en la fase pre-ejecución cuenta con modelos locales de Machine Learning y heurística avanzada entrenada para detectar herramientas de hacking, exploits y técnicas de ocultación de malware, con el fin de bloquear las amenazas sofisticadas antes de que se ejecuten. También detecta las técnicas de propagación y los sitios que alojan kits de exploits, además de bloquear el tráfico web sospechoso. HyperDetect permite a los administradores de seguridadajustar la protección para contrarrestar los riesgos

específicos que puede afrontar probablemente la organización. Con la opción de "solo informar", los administradores de seguridad pueden probar y supervisar su nueva política de protección antes de implementarla, para evitar las interrupciones del negocio. Gracias a la combinación de alta visibilidad y bloqueo de amenazas, exclusiva de Bitdefender, los usuarios pueden configurar HyperDetect para que bloquee a nivel normal o tolerante, pero continúe informando en nivel agresivo, para revelar los primeros indicadores de ataques.

Sandbox Analyzer integrado en los endpoints
Este nivel potente de protección contra amenazas avanzadas analiza los archivos sospechosos en profundidad, detona las acciones destructivas en un entorno virtual aislado, alojado por Bitdefender, analiza su comportamiento e informa sobre las intenciones maliciosas. Sandbox Analyzer, integrado con el agente de endpoints de GravityZone, remite automáticamente los archivos sospechosos para su análisis. Al emitir Sandbox Analyzer un veredicto de "malicioso", Endpoint Security HD bloquea automáticamente el archivo malicioso en los sistemas de toda la empresa de forma inmediata. La función de envío automático permite a los administradores de seguridad empresarial elegir el modo de monitorización o de bloqueo, lo que impide acceder a un archivo hasta que se emita un veredicto. Los administradores también pueden enviar manualmente archivos para su análisis. La abundante información forense de Sandbox Analyzer proporciona un contexto claro de las amenazas y ayuda a comprender el comportamiento de estas.

Antiexploit avanzado
La tecnología de prevención de exploits protege la memoria y las aplicaciones vulnerables, como por ejemplo navegadores, lectores de documentos, archivos multimedia y runtime (es decir: Flash o Java). Los mecanismos avanzados observan las rutinas de acceso a la memoria para detectar y bloquear técnicas de exploit como la verificación de llamadas de API, el stack pivoting, la programación orientada al retorno (ROP), etc.

Inspector de procesos
El Inspector de procesos opera en un modo de confianza cero, monitorizando continuamente todos los procesos que se ejecutan en el sistema operativo. Busca actividades sospechosas o comportamientos anómalos de procesos, como por ejemplo los intentos de ocultar el tipo de proceso, ejecutar código en el espacio de otro proceso (secuestro de memoria del proceso para la escalación de privilegios), replicar, descartar archivos, ocultarse a las aplicaciones de listado de procesos, etc. Toma las acciones de reparación apropiadas, incluyendo la terminación del proceso y la reversión de los cambios que haya efectuado. Es muy eficaz a la hora de detectar el malware desconocido, el avanzado y los ataques sin archivos, incluyendo el ransomware.

Antiphishing y filtrado de seguridad web
El filtrado de seguridad web permite analizar el tráfico web entrante, incluido el tráfico SSL, http y https, en tiempo real para evitar la descarga de malware en el endpoint. La protección antiphishing bloquea automáticamente las páginas web fraudulentas y de phishing.

Cifrado completo del disco duro
El Cifrado completo del disco gestionado por GravityZone mediante BitLocker de Windows y FileVault de Mac, aprovecha las tecnologías incorporadas en los sistemas operativos. FDE está disponible como un add-on, con licencia por separado.

Control y refuerzo de los endpoints
Los controles de endpoints basados en políticas de seguridad incluyen el cortafuego, el control de dispositivos con análisis de USB, y el control de contenido web con categorías de URL.

Respuesta y contención
GravityZone ofrece la mejor tecnología de clean-up del mercado. Bloquea o neutraliza automáticamente las amenazas, elimina los procesos malintencionados y revierte los cambios.

Protección del centros de datos

GravityZone Security for Virtualized Environments (SVE) aprovecha las defensas de última generación de Bitdefender Endpoint Security HD para proporcionar a las empresas la mejor seguridad en su clase para las cargas de trabajo de servidor, VDI y nube, al tiempo que maximiza el rendimiento de la infraestructura y la eficiencia operativa. GravityZone SVE es una solución empresarial con un diseño compatible incluso con los centros de datos más grandes.

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, al tiempo que 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 de huella pequeña 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 de TI.

Compatibilidad universal
Al ser compatible con todas las plataformas de virtualización (como VMware® ESXiTM, Microsoft® Hyper-VTM, Citrix® XenServer®, Red Hat® Enterprise Virtualization®, KVM y Nutanix® Acropolis), Microsoft Active Directory y los sistemas operativos guest Windows® y Linux®, GravityZone simplifica la implementación, la detección de endpoints y la administración de políticas.

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.

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.

Seguridad para dispositivos móviles iOS y Android

Esta solución se ha diseñado para permitir la adopción segura del concepto bring-your-own-device (BYOD) y hacer cumplir las políticas de seguridad en todos los dispositivos de los usuarios. Así, los dispositivos móviles se encuentran bajo control y se protege la información sensible que contienen. La carga administrativa se reduce con el estado siempre actualizado de dispositivos conformes y no conformes.

Servidores de Security for Exchange

Proporciona varios niveles de seguridad para el correo electrónico: antispam, antiphishing, antivirus y antimalware con análisis del comportamiento, protección contra amenazas de día cero y filtrado de tráfico de correo electrónico, incluidos archivos adjuntos y filtrado de contenidos. El análisis antimalware se puede transferir de los servidores de correo protegidos a los servidores de seguridad centralizados. Los informes y la administración están centralizados, lo que permite políticas unificadas para los endpoints y el intercambio de mensajes.

GravityZone Control Center

Control Center de GravityZone es una 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 contempla varios roles e incluye el servidor de bases de datos, el de comunicaciones, el de actualizaciones y la consola web. En empresas de mayor tamaño, se puede configurar para utilizar varios appliances virtuales con diversas instancias de roles específicos con equilibrador de carga incorporado, que permite una gran escalabilidad y disponibilidad.

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

BD-NGZ-Nov06.2017-IT#
Bitdefender-NGZ-Elite-Datasheet-creat2088-A4-es_ES