

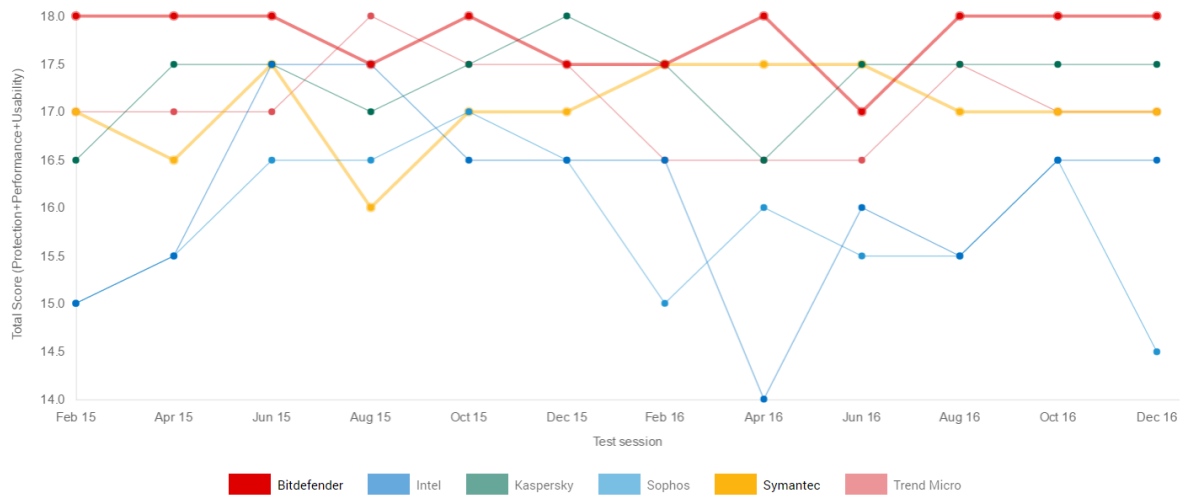
Bitdefender

1.- Security for EndPoint:

Bitdefender Business proteger los endpoints: Aprovechando las debilidades de los endpoints y la negligencia de los usuarios, los delincuentes a menudo tienen éxito al atacar los endpoints. Movidos por el lucro, desarrollan continuamente malware nuevo y más sofisticado, y buscan nuevas formas de violar la protección existente de los endpoints.

Si su organización ha sido víctima del ransomware o de otros ataques informáticos, es hora de buscar una protección mejor. A pesar de llevar mucho tiempo en el mercado, las plataformas de protección de endpoints difieren significativamente en cuanto a su capacidad para prevenir las vulneraciones sin disminuir la velocidad para los usuarios ni afectar a la facilidad de uso y de administración.

Bitdefender demuestra sistemáticamente su superioridad en pruebas independientes. En 2016, 2015 y 2014, Bitdefender obtuvo la puntuación más alta por su protección, rendimiento y facilidad de uso en las pruebas de AV-Test sobre protección de endpoints.



Soluciones de bitdefender para la protección de endpoints:

Ante el cambio en el panorama de la TI que han supuesto el BYOD, la nube y la virtualización, cada vez es más difícil mantener la protección en diferentes entornos con soluciones tradicionales de endpoint.

Bitdefender GravityZone, ha sido diseñado de abajo arriba para la nube, la virtualización, y proporciona una única consola para la administración de la seguridad de estaciones de trabajo física y virtual, servidores, dispositivos móviles y correo electrónico.

Las pequeñas y medianas empresas pueden eliminar costes de infraestructura de seguridad y utilizar la versión de consola alojada en la nube de Bitdefender. A diferencia de las soluciones de otros proveedores, las de Bitdefender incluyen -- sin cargo adicional-- todos los módulos de seguridad esenciales: antivirus y antimalware, cortafuego con IDS/IPS (sistema de detección y evitación de intrusos), filtrado web, control de contenidos y control de dispositivos.

2.- Security for Virtualized Enviroments:

BitdefenderGravityZone Security for Virtualized Environments:

Servicio de seguridad para máquinas virtuales, centros de datos virtualizados e instancias de nube proporcionado por la consola on-premise de GravityZone.

La mejor protección para máquinas virtuales Windows y Linux; permite el análisis en tiempo real de sistemas de archivos, procesos, memoria y registro. El mejor rendimiento demostrado en centros de datos: hasta un 20% de mejora en comparación con los proveedores de seguridad tradicionales funciona en cualquier plataforma de virtualización: VMware, Citrix, Microsoft Hyper-V, KVM, Oracle y otras bajo demanda seguridad sin agente para VMware NSXSistema de licenciamiento flexible por servidor virtual, por VDI o por CPU para centros de datos consolidados.

Beneficios Principales:

Mejor rendimiento en entornos virtuales:

Según las exigentes pruebas de rendimiento de Login Virtual Session Indexer (Login VSI), GravityZone – SVE presenta el menor impacto en las aplicaciones que se ejecutan en entornos virtualizados entre las soluciones de seguridad para la virtualización.

Reducción de costes a través de una consolidación más alta del servidor:

GravityZone Security for Virtualized Environments mejora la consolidación del servidor hasta un 20% en comparación con el antimalware tradicional, reduciendo las necesidades de hardware y el consumo energético.

Mínima carga administrativa:

Combina la administración simplificada con los potentes motores antimalware y las políticas de seguridad para ayudar a simplificar las operaciones de TI a la vez que se mejora el cumplimiento.

Sencillo y fácil de implementar, reduce el tiempo y los costes de implementación:

Proporcionado como un appliance virtual reforzado autoconfigurable Linux Ubuntu, se integra con VMware vCenter, Citrix XenServer y Active Directory.

Seguridad escalable y con capacidad de recuperación:

Elimina el único punto de fallo y las tormentas AV, crece orgánicamente clonando dispositivos virtuales y automatizando la implementación con imágenes maestras

Cobertura multiplataforma:

Protección optimizada en todos los hipervisores conocidos: VMware vShield VMware ESXi, Citrix Xen, Microsoft Hyper-V, Red Hat KVM, Oracle VM, etc.

3.- Security for Mobile:

BitdefenderGravityZone Security for Mobile:

Seguridad unificada para minimizar la sobrecarga administrativa. La tecnología antimalware número uno*Protege y administra dispositivos móviles iOS y Android.

Beneficios Principales:

Seguridad unificada para minimizar la sobrecarga administrativa:

La solución de Bitdefender se ha diseñado para soportar la adopción segura del concepto bring-your-own-device (BYOD), haciendo 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.

Tecnología antimalware con la mejor valoración:

Se incluye análisis antimalware bajo demanda para dispositivos Android con el fin de asegurar que están libres de código malicioso. El análisis se inicia automáticamente siempre que se conecta una unidad de almacenamiento extraíble o cada vez que se instala una nueva aplicación. El análisis detecta malware de Android y evita que los usuarios de dispositivos móviles distribuyan archivos infectados a otros usuarios dentro o fuera de la organización.

El fenómeno bring-your-own-device (BYOD):

Bitdefender soporta iniciativas BYOD con la administración de políticas de seguridad centralizada para dispositivos Android, iPhones y iPads con acciones predefinidas para dispositivos no conformes, tales como la denegación de acceso a los servicios de la empresa, el bloqueo permanente del dispositivo o incluso el borrado del mismo en caso de que haya sido robado y rooteado.

Impone un sencillo pero efectivo bloqueo de pantalla y autenticación:

Los usuarios de dispositivos móviles puede que encuentren que el bloqueo de pantalla con autenticación entorpece su uso del teléfono móvil o tablet, pero nadie pondría en duda la necesidad de una contraseña en su portátil. Bitdefender simplifica aplicar políticas de seguridad consistentes en todos los dispositivos de los usuarios y evita el acceso no autorizado a teléfonos o tablets sin vigilancia. Dado que la seguridad no puede ser una opción del usuario final, las políticas administradas centralizadamente permiten hacer cumplir fácilmente las opciones de seguridad en dispositivos móviles, incluyendo el bloqueo de pantalla tras cierto tiempo o el uso de contraseñas complejas con un número límite de errores al introducirlas.

Evita el uso de dispositivos perdidos o robados:

Bitdefender mejora los actuales sistemas operativos Apple iOS y Android con las características de seguridad más necesarias y empleadas por las empresas. Una de estas características clave es la administración centralizada de dispositivos perdidos o robados para evitar que la información privada caiga en manos equivocadas. La información confidencial en dispositivos móviles va desde las comunicaciones por correo electrónico hasta la información médica y fotos personales. Bitdefender evita el uso de dispositivos móviles perdidos o robados bloqueándolos remotamente y localizándolos para tener la posibilidad de recuperar tanto los datos como los dispositivos en sí. Si no fuera posible recuperar el dispositivo, la información puede simplemente borrarse para minimizar el riesgo de uso no autorizado de los datos.

Se adapta a las necesidades de seguridad para el uso profesional y personal:

Bitdefender tiene en cuenta los requisitos de seguridad de los dispositivos móviles tanto en la vida profesional como en la personal. Aplicable tanto a dispositivos móviles propiedad de la empresa como a dispositivos Bring-Your-Own-Device (BYOD), permite a los usuarios cambiar rápidamente de perfiles para cubrir ajustes de conectividad y cifrado (VPN) en función de cuáles sean los servicios que necesite el usuario. La administración remota de los perfiles también permite aplicar más políticas de seguridad, incluso para las horas de acceso Web predefinidas en los dispositivos Android.

4.- Security for Exchange:

GravityZone Security for Exchange:

Servicio de seguridad para servidores de correo de Microsoft Exchange proporcionado por la consola GravityZone on-premise..

- La mejor protección antispam para servidores de correo demostrado.
- Garantiza un entorno de colaboración y mensajería seguro.
- Protege servidores de correos físicos y virtuales.

Beneficios Principales:

- La mejor protección antispam para servidores de correo: ganadora del premio Golden SPAM+ de Virus Bulletin durante dos años consecutivos.
- Se instala en minutos.
- Antimalware, antivirus, antiphishing y antispam en tiempo real basados en Bitdefender Global Protective Network
- Cubre todos los protocolos de transferencia de correo electrónico utilizados en Exchange.

Características:

- Múltiples capas de seguridad para mensajería: antispam, antiphishing, antivirus y antimalware con análisis del comportamiento y protección contra amenazas de día cero.
- Filtrado del tráfico de correo electrónico, incluyendo adjuntos y filtrado de contenidos.
- El análisis antimalware se puede transferir de los servidores de correo protegidos a los servidores de seguridad centralizados.
- Análisis antimalware bajo demanda del Almacén de información de Exchange.
- Soporte para Grupos de disponibilidad de base de datos
- Integración con Active Directory, VMware vCenter y Citrix XenServer para la implementación remota.
- Protocolos de transferencia de correo electrónico cubiertos: SMTP, Microsoft Exchange (MAPI) y Exchange ActiveSync.
- La protección antimalware incluye el sistema de archivos de los servidores que alojan Exchange.

SISTEMAS Y PLATAFORMAS PROTEGIDOS:

Servidores de Correo:

- Exchange 2016, 2013, 2010, 2007.
- Servidores físicos y virtuales.
- Roles: perimetral, concentrador o buzón.
- Protocolos: SMTP, MAPI, Exchange ActiveSync.