Generalidades:

Origen: Alemania

Fabricante: G Data Cyberdefense AG

AvTEST Approved corporate endpoint protection: APPROVED

AV Comparatives malware protection test (marzo 2020): Blocked: 100% Compromised: 0% User dependent: 0% Posición: Primer lugar

Garantía anti-espionaje: ITSMIG - Bundesverband IT-Sicherheit eV (TeleTrusT)

El compromiso incluye:

- Ofrecer exclusivamente soluciones de seguridad TI sin posibilidades ocultas de acceso para terceros.
- Fabricar únicamente productos que no conlleven la transmisión de claves criptográficas o partes de claves ni identificaciones de acceso.
- Cerrar los puntos vulnerables o métodos de elusión de sistemas de control de acceso lo más rápidamente posible tras ser puestos en conocimiento.

Licenciamiento

- Licenciamiento por dispositivo
- Suscripción anual
- Multiplataforma. cambio flexible y sin costo entre sistemas operativos

Administración

- Consola de administración portable instalable on-premise, cloud o híbrida.
- 100% en español
- Instalación de múltiples consolas de administración sin costo adicional
- Repositorios locales opcionales gratuitos
- Sistema de actualizaciones P2P autogestionado

Cliente

- Instalable desde consola para todos los sistemas operativos soportados
- Excepciones de análisis de archivos o procesos totalmente configurables
- Presencia configurable del icono de systemtray (ver/ocultar)
- Fuente de actualizaciones de firmas de virus configurable (internet, servidor de actualización, P2P)
- Periodicidad de las actualizaciones totalmente configurable
- Permite RollBack de las últimas 2 actualizaciones aplicadas
- Permite o bloquea los escaneos por parte de los usuarios
- Permite o bloquea la descarga de actualizaciones por parte de los usuarios
- Permite o bloquea la configuración de opciones para correo y vigilante
- Permite o bloquea el acceso a la cuarentena local

- Es posible bloquear la configuración mediante contraseña
- Permite definir acciones automáticas (registrar, desinfectar, enviar a cuarentena o borrar)

Cliente ligero para entornos virtuales

- Compatible con Microsoft HyperV® y VMware vSphere®
- Incluye todas las funciones de protección reactiva y proactiva
- Virtual Remote Scan Server (VRSS) incluído sin costo adicional
- Virtual Remote Scan Server (VRSS) gestionado desde la misma consola de administración
- Protege infraestructuras de escritorio virtual (VDI) y servidores virtualizados

Funciones de protección

- Incluye tecnología de fingerprinting que evita analizar elementos ya marcados como seguros
- Permite elegir la ejecución de vigilancia al escribir, leer o ejecutar elementos, esto con el fin de adaptarse a equipos con pocos recursos y minimizar el impacto en las operaciones de lectura/escritura sobre discos duros mecánicos
- Posee funciones avanzadas de análisis heurístico
- Analiza la conducta de archivos e informa claramente la ruta, hash y acciones que generan sospecha
- Permite elegir entre informar, esperar acción de administrador o ejecutar una acción automática en caso de detección de comportamiento sospechoso
- Permite definir límites de tamaño para el escaneo de archivos comprimidos
- Permite definir si analizar o no archivos PST
- Permite habilitar el escaneo automático al iniciar el sistema
- Permite definir si se debe notificar o no al usuario cuando se detectan amenazas
- Cuenta con tecnología de hibrida mediante 2 motores de fabricantes diferentes, adaptables y complementarios
- Todos los módulos y tecnologías son adaptables, permitiendo proteger con funciones básicas dispositivos con muy pocos recursos
- Cuenta con tecnología de escaneo en modo reposo que detecta cuando el usuario no usa su equipo y aprovecha esos momentos para hacer análisis profundos
- Cuenta con módulo especial de protección anti-troyanos bancarios
- Cuenta con módulo de inventario de hardware y software
- Cuenta con tecnología anti-exploit que evita la explotación de aplicaciones vulnerables
- Cuenta con sistemas de aprendizaje de máquina (DeepRay) capaces de detectar malware camuflado, ataques dirigidos y fileless
- Cuenta con tecnología basada en AI (DeepRay) para detectar malware evasivo
- Cuenta con funciones de EDR libre de gestión (BEAST) capaz de detectar con base en IOC, conexiones sospechosas y a C&C
- Cuenta con registro gráfico de actividades (BEAST) capaz de correlacionar amenazas con procesos y revertir cambios maliciosos post-ejecución

Funciones de MDM (mobile device management)

- Permite proteger y gestionar dispositivos Android y iOS dentro de la misma consola
- Permite detectar dispositivos rooteados y prohibirlos
- Permite forzar el cifrado de los dispositivos
- Permite prohibir el uso de la cámara

- Cuenta con control de aplicaciones mediante lista negra, blanca y protección por contraseña administrativa
- Cuenta con directorio telefónico sincronizable con AD con posibilidad de establecer filtros de llamadas entrantes y salientes
- Cuenta con funciones antirrobo para dispositivos android (ubicar, restablecer, bloquear, cambiar contraseña remotamente)

Funciones de control de usuarios

- Permite especificar si las reglas se aplican a usuarios o a usuarios y administradores
- Firewall inteligente con funcionalidad de Piloto Automático y políticas adaptables en el interior o exterior del perímetro
- Control de aplicaciones mediante lista negra y blanca
- Control de dispositivos
- Control de URLs independiente del navegador y por categorías
- Control del tiempo de acceso a internet
- Permite supervisar los horarios de uso de internet
- Permite bloquear el uso de cámara web, medios ópticos o dispositivos USB
- Los medios de almacenamiento se pueden bloquear a nivel de lectura, escritura o total
- Los usuarios pueden reportar en tiempo real páginas y aplicaciones bloqueadas y solicitar autorización de acceso
- Los administradores pueden recibir notificación de las solicitudes de desbloqueo de los usuarios, autorizarlas o negarlas e informar al usuario desde el mismo panel

Funciones de reporte

- El panel de reportes se actualiza en tiempo real con los eventos de toda la red
- Es posible filtrar los eventos por tipo, equipo, servidor, fecha y hora, remitente, hallazgo, usuario, detalles
- Los informes estadísticos permiten obtener rápidamente indicadores del estado de los equipos (Actualizados, activos, conectados)
- Los informes permiten determinar las amenazas detectadas y las más frecuentes

Funciones de administración de parches y actualizaciones

- Permite obtener y desplegar parches mínimo de fabricantes como Microsoft, Adobe, Oracle, Apple, VMWare, Autodesk, Google, Novell y Sun
- Garantiza que los parches han sido probados antes de ponerlos en el repositorio
- Comprueba automáticamente o por demanda la aplicabilidad de parches en los equipos de la red
- Permite ordenar la aplicación de parches a grupos o equipos individuales
- Permite programar la verificación y aplicación de parches
- Permite aplicar parche en entornos de prueba antes de aplicarlos en producción
- Permite hacer rollback de los parches aplicados en caso de causar problemas
- Permite obtener informes para verificar el progreso de la aplicación de los parches
- La interfaz gráfica muestra información sencilla que incluye los equipos, fabricantes y productos con más parches pendientes

- Permite visualizar parches por estado, prioridad, fabricante o producto y obtener detalles de su compatibilidad y propósito
- Permite poner parche en lista negra para no aplicarlos en caso de detectar problemas
- Es posible localizar parches específicos y ordenar su despliegue inmediato en caso de ser necesario
- Los usuarios pueden opcionalmente visualizar y solicitar parches
- Es posible informar a los usuarios sobre el despliegue de parches

Exchange Mail Security

- Compatible con Microsoft Exchange Server 2007 SP1/2010/2013/2016
- Se ejecuta como plugin en todos los servidores Exchange que ejecutan el Mailbox Role o el Hub Transport Role
- Escaneo antimalware con dos motores de detección
- Acciones automáticas configurables
- Análisis heurístico avanzado de adjuntos
- Análisis configurables de archivos comprimidos
- Avanzada protección anti-spam
- Clasificación (sospechoso, probable, muy probable) configurable
- Listas blancas y negras

Requisitos de sistema

G DATA Management Server		
General:	min. 1 GB RAM, 1 CPU und 5 GB HDD	
When using G DATA Management Server with Local Microsoft SQL Database Server:	4 GB RAM, multicore CPU	
Supported Operating Systems	32-bit	64-bit
Windows Server 2019		☑
Windows Server 2016		☑
Windows Server 2012 (R2)		☑
Windows Server 2008 (R2)	☑	☑

Windows 10	☑	☑
Windows 7 (min. SP1)	☑	☑

G DATA Administrator / G DATA Web Administrator / G DATA Mobile Administrator

Supported Operating Systems	32-bit	64-bit
Windows Server 2019		☑
Windows Server 2016		☑
Windows Server 2012 (R2)		☑
Windows Server 2008 (R2)	☑	☑
Windows 10	☑	☑
Windows 7 (min. SP1)	☑	☑

G DATA Security Client (Microsoft Windows)

Supported Operating Systems	32-bit	64-bit
Windows Server 2019		☑
Windows Server 2016		☑
Windows Server 2012 (R2)		☑
Windows Server 2008 (R2)	☑	☑

Windows Server 2008	☑*	☑*
Windows 10	☑	☑
Windows 7 (min. SP1)	☑	☑
Windows XP	()* **	()* **

G DATA Security Client (macOS)

Operating Systems	Support
macOS Mojave 10.14	☑
macOS High Sierra 10.13	☑
macOS Sierra 10.12	☑
OS X El Capitan 10.11	☑

G DATA Security Client (Linux)

Operating Systems	Support
Debian 8	☑
Debian 9	☑
OpenSUSE Leap 42.3	☑
SLES 11 SP4	☑

SLES 12	☑
SLES 15	☑
RHEL 5.11	☑
RHEL 6.6	☑
RHEL 7.0	
Ubuntu 14.04.1	☑
Ubuntu 16.04	☑
Ubuntu 18.04	☑
CentOS 6.6	☑
CentOS 7.0	☑
Fedora 27	☑
Fedora 28	☑
Fedora 29	☑

G DATA Mail Security for Exchange

Microsoft Exchange Version	Support
Microsoft Exchange Server 2019	☑

Microsoft Exchange Server 2016	☑
Microsoft Exchange Server 2013	☑
Microsoft Exchange Server 2010	☑

G DATA Mobile Device Management for Android

Operating System	Android 4.2 or newer

G DATA Mobile Device Management for iOS

iOS Version	Support
iOS 9	☑
iOS 10	☑
iOS 11	☑
iOS 12	☑

G DATA Mail Security Mail Gateway

General:	min. 1GB RAM, 1 CPU und 1GB HDD	
Supported Operating Systems	32-bit	64-bit
Windows Server 2019		☑

Windows Server 2016	☑	☑
Windows 10		☑
Windows Server 2012 R2	☑	☑
Windows 7 (min. SP1)	☑	☑
Windows Server 2008 R2	☑	☑
Windows Server 2008	☑	☑
Windows XP SP3		

G DATA Web-Extension

Browser	Version or newer
Microsoft Edge (Chromium-based)	79.0
Microsoft Edge (EdgeHTML-based)	11.0.117763
Mozilla Firefox	57.0
Mozilla Firefox ESR	63.0
Google Chrome	65.0

* not available as a Light Agent
** limited feature set