Changelog

Changelog 15.2

New features

New: Extended analysis information in the security events, including: Sha 256, last write and last access of the file, owner and size of the file, and name of the calling process.

New: Changes to client settings are logged in the infrastructure logs. This means that changes can now be tracked. Exceptions to this are changes in the spam settings.

Modified system supports

Removed: Support for CentOS 8 is discontinued.

New G DATA Linux Client: Ubuntu 22.04 is supported.

New G DATA Linux Client: Debian 11 is supported.

New G DATA Linux Client: RHEL 8 is supported.

New G DATA Linux Web Security Gateway: Ubuntu 22.04 is supported.

New G DATA Linux Mail Security Gateway: Ubuntu 22.04 is supported.

New G DATA Linux Web Security Gateway: Debian 11 is supported.

New G DATA Linux Mail Security Gateway: Debian 11 is supported.

General modifications

New: The certification of G Data files has been switched to the latest Microsoft Azure Code Signing (ACS) procedure.

Optimized: The sometimes confusing "data status" time information has been removed both in G DATA Administrator and on the client tray icon. Timestamps now refer exclusively to the signature version.

SIEM

New: The update provides ready-to-use preconfigured telegraf.config files for Graylog, Splunk and Syslog. Future updates will not overwrite the files used.

Fixed: Data transfer issues between G DATA ManagementServer and the Telegraf service have been fixed.

Removed: The "Telegraf (Gdmms)" service is no longer created automatically.

G DATA Administrator

New: The version number of the additional security components loaded on G DATA ManagementServer is also displayed in the ManagementServer view, in the Update/Signature Updates module.

New: The version number of the additional security components loaded on the individual client is now also displayed in the Client view, in the Client Settings / Overview module.

New: The "Messages by staged distribution" feature has been added to the alert messages.

Enhanced: Windows 11, Windows Server 2022, and Windows 10 21H2 operating systems are now displayed in the system information for the client.

Optimized: Sorting of the object tree.

Fixed: Problems with setting an exception for the AntiRansomWare module were fixed.

Fixed: Problems with logging in with the "Portable Admin" were fixed.

Fixed: Problems with opening the client settings / guards in the module menu were fixed.

Updates

New: Insufficiently patched systems do not receive automatic program updates. The "Update program files automatically" feature is disabled. Notes are written to the infrastructure logs. See also Update status of your operating systems. (Warning) This does not apply to G DATA SubnetServers. These cannot be intercepted. Therefore, before updating, please make absolutely sure that the systems are patched.

Optimized: Optimization of storage space requirements of signature updates by deleting obsolete signature packages.

Optimized: Failed client program updates are repeated.

Optimized: The update for MAC client program updates has been changed to an improved update procedure. As a result, clients receive their program updates directly from the G DATA management server.

Fixed: Problems with the client loading signature updates (additional security components) from the Internet have been fixed.

Fixed: Causes that caused G DATA ManagementServer to stop performing automatic virus signature updates have been fixed.

Fixed: Linux clients, with the Perform program updates automatically feature enabled, no longer perform the update after each contact with G DATA ManagementServer.

Removed: The outdated signature update cycles "Weekly" and "On Internet update" have been removed.

ManagementServer

New: Alert message when the G DATA ManagementServer hard disk is running full. (Configurable in the config.xml file: PercentageThresholdFreeSpace).

New: If computer names have been swapped in Active Directory, synchronization problems occur between G DATA ManagementServer and Active Directory. The problem is documented in the infrastructure logs with the name of the causing clients.

Clients

New: Security events of the monitor and the scan jobs are written to the Windows event displays (application and service logs) of the affected client.

Optimized: Client-specific monitor and scanner exceptions are preserved when moving to another group.

Fixed: Clients load again in peer-to-peer update mode when this feature is enabled.

MAC

New: The status of program updates is now also displayed in G DATA Administrator for MAC clients.

G DATA Exchange Mail Security

Optimized: Temporary files created during mailbox scanning are completely deleted after the scan is completed.

PatchManagement

Optimized: The product has been revised in terms of performance.

Added: Missing browser updates have been added.

PolicyManager

Optimized: The web content control categories have been updated.

Logs

Optimized: Logs do not report web browser plugin messages when the browser is updated. Logs are created just when the plugin is activated and deactivated in the web browser.

Synchronisation

Fixed: Changed settings of device control in G DATA Administrator, are correctly applied by G DATA Security Client again.

Fixed: When using comments in the logs, synchronization problems of G DATA SubnetServer with G DATA ManagementServer (Main) no longer occur.

Android

Fixed: The link to G DATA ManagementServer is again correctly displayed / transmitted in the email for the installation of G DATA Android Client.