

Specifications**G DATA XDR****G DATA MXDR****General****Manufacturer's special features**

Holistic manufacturer and provider of IT security solutions and services headquartered in Germany

Software development, support and service from a single source

Compliance with high data protection standards according to GDPR

Data storage exclusively in Germany

Long-standing manufacturer and provider of IT security solutions - inventor of the antivirus in 1987

Service / Support**General**

Support and service are located directly at the headquarters

Support and service have a direct link to the development department

High quality and good availability of support has been proven by independent testing institutes

All product documentation and user guides are available in German and English

Support (Can be upgraded to include 24/7 personal support via the G DATA TAM Service)

Support languages

Yes

Yes

Support is offered in German

Yes

Yes

Support is offered in English

Yes

Yes

Case acceptance - G DATA Support accepts technical queries by phone and e-mail.

Yes

Yes

Case acceptance by phone (Mon-Fri, except public holidays) between 9 a.m. and 4 p.m CET/CEST

Yes

Yes

We respond to email inquiries on the next business day (Mon–Fri, excluding holidays) between 9 a.m. and 4 p.m. CET/CEST

Yes

Yes

Onboarding

Onboarding instructions

Yes

Yes

Instructions for installing the agents in the customer environment

Yes

Yes

Download link for agent setups including parameters required for installation

Yes

Yes

Overview of IP addresses, ports and domains to be released to ensure agent-server communication

Yes

Yes

Agent

Protection and detection mechanisms offer effective threat detection with high detection rates. Detection of complex attack patterns through system-wide behavior monitoring.

Yes

Yes

Agent: System requirements

At least 5 GB free hard drive space

Yes

Yes

At least 2 GB of available RAM

Yes

Yes

A stable internet connection to the G DATA Cloud backend is required for the installation and operation of the agent

Yes

Yes

Windows

Yes

Yes

CPU architecture: x64 with SSE3 instruction set or ARM

Yes

Yes

Specifications**G DATA XDR****G DATA MXDR**

All Windows operating system versions covered by the "Extended Support" from Microsoft. The Windows LTSC versions are only supported as long as they are covered by "mainstream support". Systems with ARM CPU. Systems with ARM CPUs are only supported starting from Windows 11 version 24H2.	Yes	Yes
Linux	Yes	Yes
CPU architecture: x64 with SSE3 instruction set	Yes	Yes
Ubuntu: All Ubuntu LTS versions supported by the manufacturer's 'standard support'	Yes	Yes
Debian: All Debian versions supported by the respective manufacturer's 'LTS Support'	Yes	Yes
SUSE Linux Enterprise Server (SLES): All SLES versions from version 15 onwards that are supported by the respective manufacturer's 'LTSS Support'	Yes	Yes
Red Hat Enterprise Linux (RHEL): All RHEL versions supported by the respective manufacturer through 'Maintenance Support' or 'Extended Update Support' (minor versions)	Yes	Yes
Oracle Linux: All Oracle Linux versions supported by the respective manufacturer's 'Premier Support'	Yes	Yes
macOS	Yes	Yes
CPU architecture: 64-bit Intel or Apple-Silicon (ARM) CPUs	Yes	Yes
The current and the two previous macOS major versions are supported	Yes	Yes
Required: Full disk access for all G DATA services	Yes	Yes
Required: Approval of the G DATA Network Extension to filter network traffic	Yes	Yes
Agent: General functions		
Single Agent - The agent offers comprehensive support for server and desktop systems. Additionally licensed and activated features are automatically downloaded and installed.	Yes	Yes
Available for: Windows, Linux, macOS	Yes	Yes
The agent is provided via a parameterizable setup for all supported operating systems	Yes	Yes
Additionally licensed and activated features are automatically downloaded and installed by the agent in the background	Yes	Yes
Communication with the cloud backend takes place via a limited range of IP addresses and defined domains	Yes	Yes
Automatic updates - The G DATA Agent regularly checks whether new updates are available and installs them automatically in the background	Yes	Yes
Self-protection	Yes	Yes
The agent prevents unauthorized uninstallation	Yes	Yes
Agent: Protection (Prevent)		

Specifications**G DATA XDR****G DATA MXDR**

Static malware protection - The static malware protection includes several powerful functions for combating malware. The agent can scan files for malware infections and move infected files to quarantine. In addition, the agent is able to clean up devices with active malware. To ensure that it is always up to date, the agent downloads the latest signatures for malware detection. Another important component is the on-access scanner, which ensures continuous monitoring. In addition, the agent takes exceptions into account when scanning to avoid false alarms and increase efficiency. For G DATA products with advanced attack detection (see below), the meta information of the objects detected as infected is uploaded to the G DATA Cloud backend in the form of telemetry data.

Yes

Yes

Available for: Windows

Yes

Yes

The detection rate of infected files is similarly high in offline mode as in online mode

Yes

Yes

The agent can check files for malware infections

Yes

Yes

The agent can scan suspicious content for threats using the Antimalware Scan Interface (AMSI)

Yes

Yes

The agent can move files infected with malware to quarantine

Yes

Yes

The agent can clean up devices with active malware

Yes

Yes

The agent automatically updates the latest signatures for malware detection

Yes

Yes

The agent has an on-access scanner

Yes

Yes

The agent takes exceptions into account when scanning

Yes

Yes

Agent: Detection (Detect)

Behavior detection - Behavior detection stores events from various sensor sources and correlates them across endpoints. Complex attacks distributed across multiple processes and sensor sources are reliably detected. Behavioral detection goes beyond static signatures. It ensures that the latest detection rules are available at all times.

Yes

Yes

Available for: Windows, Linux, macOS

Yes

Yes

Behavior monitoring includes process executions in attack detection

Yes

Yes

Available for: Windows

Yes

Yes

Behavior monitoring includes registry events in attack detection

Yes

Yes

Behavior monitoring includes changes to the system configuration in the attack detection

Yes

Yes

Behavior monitoring includes network events in attack detection

Yes

Yes

Behavior monitoring includes file system events in attack detection

Yes

Yes

Behavior monitoring includes dynamically loaded modules in attack detection

Yes

Yes

Behavioral monitoring incorporates Antimalware Scan Interface (AMSI) events into attack detection

Yes

Yes

Agent: Response

Automatic responses

Yes

Yes

Available for: Windows, Linux, macOS

Yes

Yes

Processes and process trees classified as defective can be automatically stopped and terminated

Yes

Yes

Files classified as malicious can be automatically moved to quarantine on execute

Yes

Yes

Available for: Windows

Yes

Yes



Specifications

G DATA XDR

G DATA MXDR

Access to files classified as malicious can be denied on access	Yes	Yes
Entries in the registry database that are classified as malicious can be deleted automatically	Yes	Yes
Live Terminal - Audited remote access tool for G DATA security analysts to carry out remote analyses and measures to manually contain and clean up attacks. All activities carried out by G DATA security analysts via the Live Terminal are logged and made available as an audit log on request or in the web portal. The Live Terminal is used exclusively in connection with products managed by G DATA and only by agreement with the customer.	N/A	Yes
Agent: Local UI		
Available for: Windows	Yes	Yes
Status information	Yes	Yes
The operation of the G DATA Agent is displayed as a tray icon for all logged-in end users, unless configured otherwise	Yes	Yes
Cloud backend		
Central evaluation and processing of threat and system information. Simple configuration of all endpoints and functions. Threats are identified through analysis and assessment of security events and presented as alerts.	Yes	Yes
Web portal		
Secure login procedure with OAuth and Multifactor Authentication (2FA/MFA)	Yes	Yes
Authenticator apps from Microsoft, Google and Duo Mobile are supported for 2FA login	Yes	Yes
Available languages	Yes	Yes
German, English, Polish, Dutch, Portuguese, French, Italian, Spanish	Yes	Yes
Dashboard	Yes	Yes
The dashboard shows the number of managed endpoints as well as their status	Yes	Yes
The dashboard shows the progress over time and the number of detected incidents and their severity as a diagram within a selectable time period	N/A	Yes
The dashboard shows open alerts	Yes	N/A
The dashboard displays an overview of current recommendations for action	N/A	Yes
The dashboard displays statistical information on incident handling by security analysts as well as the number of reports and incidents	N/A	Yes
Endpoints	Yes	Yes
Managed endpoints are displayed in a searchable, filterable and sortable table	Yes	Yes
The current status of all endpoints is displayed in the endpoint overview	Yes	Yes
Currently installed versions of the agents can be viewed via the web portal	Yes	Yes
The configuration of individual endpoints can be viewed	Yes	Yes
Agents can be uninstalled via the web portal	Yes	Yes
Each endpoint can be configured separately	Yes	N/A
Endpoints can be configured collectively across organizational units	Yes	N/A



Specifications	G DATA XDR	G DATA MXDR
Endpoints can be configured so that threats are automatically blocked or simply logged	Yes	N/A
Endpoints can be configured so that a tray icon is displayed or hidden when the agent is running	Yes	N/A
Endpoints can be configured so that users are notified or not notified when a detection occurs on the endpoint	Yes	N/A
Alerts	Yes	N/A
Messages are displayed in a table that can be searched, filtered and sorted	Yes	N/A
In the report overview, additional information can be displayed for each report, such as status, severity or affected endpoint	Yes	N/A
The details of individual reports can be viewed	Yes	N/A
The detailed view of a notification displays all affected artefacts	Yes	N/A
Processes that have been automatically stopped are displayed in the detailed view of a notification	Yes	N/A
The detailed view of a message displays relevant related messages	Yes	N/A
A relevant exception in the detailed view of a report can be added	Yes	N/A
Artifacts can be restored from quarantine in the detailed view of a report	Yes	N/A
Artifacts can be deleted from quarantine in the detailed view of a report	Yes	N/A
In the detailed view of a report, users can leave comments on the report	Yes	N/A
The message graph displays the processes involved in a message as a graph and visually highlights detections	Yes	N/A
Detailed information about individual nodes in the message graph can be displayed, e.g. available file information	Yes	N/A
Exceptions management	Yes	N/A
Exceptions are displayed in a table that can be searched, filtered and sorted	Yes	N/A
In the exception overview, additional information can be displayed for each exception, such as the type, exception value or exception mode	Yes	N/A
New exceptions can be created in the exception management module	Yes	N/A
Details of individual exceptions can be viewed	Yes	N/A
The scope is displayed in the detailed view of an exception	Yes	N/A
An exception can be changed	Yes	N/A
An exception can be deleted	Yes	N/A
Quarantine management	Yes	N/A
Quarantine containers are displayed in a table that can be searched, filtered and sorted	Yes	N/A
In the quarantine overview, additional information can be displayed for each quarantine container, such as the endpoint, artefacts or detections	Yes	N/A
Details of individual quarantine containers can be viewed	Yes	N/A
In the detailed view of a quarantine container, a link is provided to the associated notification	Yes	N/A
In the detailed view of a quarantine container, a link to the associated endpoint is provided	Yes	N/A
In the detailed view of a quarantine container, all artifacts it contains are displayed by name	Yes	N/A



Specifications

G DATA XDR

G DATA MXDR

The artefacts in the quarantine container can be restored on the endpoint	Yes	N/A
A quarantine container can be deleted from the endpoint	Yes	N/A
E-mail notification	Yes	Yes
Notification recipients are displayed in a filterable table	Yes	Yes
The assigned notification events are displayed in the recipient overview	Yes	Yes
The assigned notification languages are displayed in the recipient overview	Yes	Yes
Profile management	Yes	Yes
Contact details for your own profile are displayed and can be changed	Yes	Yes
Display language and design of the web portal are displayed and can be changed	Yes	Yes
The access password can be changed	Yes	Yes
Two-factor authentication can be reset	Yes	Yes
User administration	Yes	Yes
Users and user information are displayed in a searchable, filterable and sortable table	Yes	Yes
Assigned roles and assigned organizational units are displayed in the user overview	Yes	Yes
Individual users can be deactivated	Yes	Yes
Users can each be assigned a role and organizational unit to control access permissions	Yes	Yes
Role management	Yes	Yes
Roles are displayed in a searchable, filterable and sortable table	Yes	Yes
The assigned organizational units are displayed in the role overview	Yes	Yes
Access authorizations for product and functional areas can be assigned to a role	Yes	Yes
Manage organizational units	Yes	Yes
Organizational units are managed hierarchically	Yes	Yes
Incidents	N/A	Yes
Incidents are displayed in a searchable, filterable and sortable table	N/A	Yes
The current status of all incidents is displayed in the incident overview	N/A	Yes
Affected endpoints are displayed in the incident overview	N/A	Yes
The impact of all incidents is displayed in the incident overview	N/A	Yes
Recommendations for action can be viewed per incident, if available	N/A	Yes
The detailed history of individual processes can be viewed	N/A	Yes
All assigned messages and affected artifacts are displayed in the detailed history of an operation	N/A	Yes
The impact, priority and urgency are displayed and described in the detailed history of a process	N/A	Yes
The message graph shows connections to individual messages as a graph and highlights detections visually	N/A	Yes
Detailed information on individual nodes in the message graph can be displayed, e.g. available file information	N/A	Yes
Interactions and activities of security analysts are displayed in the form of a time history	N/A	Yes
Recommendations for action	N/A	Yes

Specifications	G DATA XDR	G DATA MXDR
Recommended actions are displayed in a searchable, filterable and sortable table	N/A	Yes
The current status of all recommendations for action is displayed in the overview of recommendations for action	N/A	Yes
In the recommended action overview, the endpoints affected are displayed for all recommended actions	N/A	Yes
Detailed information on individual recommendations for action can be displayed	N/A	Yes
In the detailed view, meta information, headline and description text for a recommendation for action are displayed	N/A	Yes
There is a link to the linked incident in the detailed view	N/A	Yes
Protocols	N/A	Yes
Executed actions can be displayed in a log overview	N/A	Yes
Support of reporting requirements	N/A	Yes
Preparation of information on incidents on demand, to support reporting obligations	N/A	Yes
Emergency contacts	N/A	Yes
Advanced attack detection		
Complementary to the local protection, detection and automatic response components. Detection of complex attack patterns across the entire geo-fenced customer environment. Detection of attack propagation in the customer environment. Integration and linking of multiple sensor sources to detect complex attacks	Yes	Yes
Advanced attack detection	Yes	Yes
Security events are stored from different sources in the cloud backend	Yes	Yes
Connection of standard SIEM systems	Yes	Yes
Forwarding of detection information from the G DATA cloud backend to standard SIEM systems in CEF or ECS format upon request	Yes	Yes
Availabilities		
Infrastructure	Yes	Yes
The infrastructure for analyzing and evaluating data and for notification and support is at least 99.5% available at the transition point each year	Yes	Yes
Necessary maintenance work that leads to the unavailability of the infrastructure should not exceed eight hours per quarter	Yes	Yes
Upcoming maintenance work will be announced two working days in advance	Yes	Yes
Compliance / Data protection		
Data storage exclusively in Germany and german data center. Strict compliance with high data protection standards in accordance with the GDPR	Yes	Yes
Hosting location (G DATA data center): Bochum	Yes	Yes
Hosting location (Glasfaser Ruhr (GFR)): Bochum, Herne	Yes	Yes
Hosting locations (IONOS): Frankfurt am Main, Berlin	Yes	Yes



Specifications

G DATA XDR

G DATA MXDR

Compliance

ISMS certified according to ISO/IEC 27001

Yes

Yes

G DATA Managed SOC

24/7 SOC service for G DATA Managed Extended Detection and Response. All employees of the Security Operations Center are certified as BSI Vorfall-Praktiker.

N/A

Yes

24/7 Detect Analyst Service

Baseline analysis of monitored devices to detect anomalies

N/A

Yes

The baseline analysis takes place during onboarding for a period of up to six calendar weeks

N/A

Yes

In log-only mode, the agent only records security events

N/A

Yes

Recorded security events are made available in the cloud backend for baseline analysis, automatically normalized, enriched and correlated

N/A

Yes

A profile is created for the customer environment to detect anomalies

N/A

Yes

Exceptions are defined for the customer environment based on the profile created

N/A

Yes

24/7 monitoring and remote analysis

N/A

Yes

Security analysts examine all incoming security messages from all monitored devices

N/A

Yes

Security analysts analyze security messages and incidents remotely via live terminal if necessary and by appointment

N/A

Yes

Security analysts investigate incidents for false positives

N/A

Yes

All activities carried out by security analysts are automatically logged in an audit log

N/A

Yes

24/7 attack notification by e-mail

N/A

Yes

E-mail notification when an incident is detected

N/A

Yes

E-mail notification when the incident status changes

N/A

Yes

Recommendations for action - G DATA security analysts create recommendations for action in the event of a detected attack or if the customer's cooperation is required for handling. The recommendation for action contains information on the detected attack and its classification and describes possible options for action for handling by the customer

N/A

Yes

24/7 Response Analyst Service

Contain the spread of attacks - In the event of an attack, affected endpoints are isolated from the network by G DATA security analysts (for Linux, Windows)

N/A

Yes

Proactive false positive treatment - G DATA security analysts investigate reported incidents for potential false positives and proactively resolve them

N/A

Yes

Scanning of individual files on the host system by security analysts (on-demand scan)

N/A

Yes

Remote cleanup of persistent malware artifacts

N/A

Yes

Security analysts can manually remove malware artifacts identified during the analysis via Live Terminal

N/A

Yes

Security Operations Manager

Direct contact for security requests- Security Operations Manager (SOM)

N/A

Yes



Specifications

G DATA XDR

G DATA MXDR

Dedicated, German and English speaking contacts at the manufacturer who are familiar with the client's environment and processes	N/A	Yes
24/7 Prioritized case acceptance by telephone for security requests	N/A	Yes
24/7 telephone notification in the event of critical incidents, up to five contact attempts within 48 hours if unavailable per incident	N/A	Yes
Response to email inquiries on the next business day (Mon–Fri, excluding holidays) between 9 a.m. and 4 p.m. CET/CEST	N/A	Yes
Incident First Response (4h per quartal)		
Qualification of potential suspected cases	N/A	Yes
Initial IT forensic analysis by certified specialists	N/A	Yes
Risk assessment and information gathering	N/A	Yes
Initial phone consultation in the event of an IT security incident reported by the customer	N/A	Yes
TAM Service (Included as an add-on in the MXDR product or optionally available for purchase as an add-on to the XDR product)		
The G DATA TAM Service provides you with extended, personal support for your G DATA products. Your Technical Account Manager knows your environment, prioritizes your concerns, and actively supports you in reducing risks, resolving disruptions faster, and making optimal use of your security solutions.	Yes (optional)	Yes
After booking it with the XDR product, the G DATA TAM Service includes support for the following G DATA products: XDR, MXDR, Policy Control, Mobile Device Management, and Mail Protection. Without an additional booking, the support covers only the MXDR product.	Yes (optional)	Yes
24/7 Support	Yes (optional)	Yes
24/7 case acceptance by phone	Yes (optional)	Yes
24/7 Prioritized case acceptance by telephone for technical inquiries	Yes (optional)	Yes
Remote support using appropriate remote maintenance software	Yes (optional)	Yes
Personal Remote Onboarding	Yes (optional)	Yes
Personal onboarding through dedicated contacts	Yes (optional)	Yes
Introduction to the product and its operation	Yes (optional)	Yes
Personal email with important information on onboarding and installation	Yes (optional)	Yes
Answering of questions and support through a personal contact	Yes (optional)	Yes
Personal onboarding is offered in German or English	Yes (optional)	Yes
An inventory of the end customer's IT environment is carried out	N/A	Yes
Special features of the IT infrastructure are identified, such as business-critical systems	N/A	Yes
It is agreed to what extent security analysts are allowed to perform remote analyses and responses on individual endpoints	N/A	Yes
Exceptions to the protection components are agreed for individual endpoints	N/A	Yes
There is a risk disclosure in the event of restricted powers of action by security analysts	N/A	Yes
There is a risk disclosure for the case of set exceptions for protection components	N/A	Yes



Specifications

G DATA XDR

G DATA MXDR

Contact persons and contact details for notifications are agreed	N/A	Yes
Contact persons and contact details are agreed for the telephone attack notification	N/A	Yes
A script is provided for uninstalling security solutions that have already been installed	Yes (optional)	Yes
Technical instructions are provided for the deployment of the purchased product	Yes (optional)	Yes
There is a final report with agreements made	N/A	Yes
Product configuration	Yes (optional)	Yes
Adjustments to the product configuration can be requested by e-mail or telephone	Yes (optional)	Yes
The product configuration will be adjusted within two calendar weeks after checking and, if necessary, consultation	Yes (optional)	Yes
Exceptions are defined and rolled out on request by e-mail or telephone after checking and, if necessary, consultation within two calendar weeks	Yes (optional)	Yes
Regular Config Checks (2x per year)	Yes (optional)	Yes
Target/actual comparison of the current product configuration (2x per year)	Yes (optional)	Yes
Comparison of the product configuration against current best practices (2x per year)	Yes (optional)	Yes
Migration	Yes (optional)	Yes
Migration support through Technical Account Managers	Yes (optional)	Yes
Guidance and support when switching from already installed security solutions	Yes (optional)	Yes
SIEM Integration	Yes (optional)	Yes
Support with the integration of standard SIEM systems through Technical Account Managers	Yes (optional)	Yes
Bug and Feature Submission	Yes (optional)	Yes
Prioritization of submitted problems, errors, or bugs	Yes (optional)	Yes
Acceptance of feature requests	Yes (optional)	Yes
Submission via dedicated online forms	Yes (optional)	Yes
Submitting suspicious content for analysis	Yes (optional)	Yes
Prioritized analysis of suspicious submitted content	Yes (optional)	Yes
Submission via dedicated online forms	Yes (optional)	Yes
Fast processing by experienced specialists	Yes (optional)	Yes
Policy Control (Optionally available for purchase as an add-on to the XDR and MXDR products or as a separate licensing solution)		
Device Control		
System requirements	Yes (optional)	Yes (optional)
Windows: CPU architecture: x64 with SSE3 instruction set or ARM	Yes (optional)	Yes (optional)
Windows: All Windows operating system versions covered by the "Extended Support" from Microsoft. The Windows LTSC versions are only supported as long as they are covered by "mainstream support". Systems with ARM CPUs are only supported starting from Windows 11 version 24H2.	Yes (optional)	Yes (optional)
Access control for devices that can be connected to computers	Yes (optional)	Yes (optional)
Available for: Windows	Yes (optional)	Yes (optional)



Specifications

G DATA XDR

G DATA MXDR

Supported devices: Removable storage devices (e.g. USB flash drives), optical drives, floppy disk drives, Windows Portable Devices and webcams

Yes (optional)

Yes (optional)

Mail Protection (Optionally available for purchase as an add-on to the XDR and MXDR products or as a separate licensing solution)

Mail Protection for Microsoft Exchange Online

System requirements

Yes (optional)

Yes (optional)

Active Microsoft 365 Exchange Online or Microsoft Exchange Online account

Yes (optional)

Yes (optional)

Email protection against malware and spam

Yes (optional)

Yes (optional)

Available for: Microsoft Exchange Online

Yes (optional)

Yes (optional)

Mobile Device Management (Optionally available for purchase as an add-on to the XDR and MXDR products or as a separate licensing solution)

Mobile device management for Android and iOS devices

System requirements

Yes (optional)

Yes (optional)

All Android versions supported by the operating system manufacturer

Yes (optional)

Yes (optional)

All iOS versions supported by the operating system manufacturer

Yes (optional)

Yes (optional)

Device management and protection performance

Yes (optional)

Yes (optional)

Available for: Android, iOS

Yes (optional)

Yes (optional)

Mobile devices can be managed centrally in the web portal

Yes (optional)

Yes (optional)

Security settings and policies can be rolled out to all managed mobile devices via the web portal

Yes (optional)

Yes (optional)

Protect sensitive data from unauthorized access: locate, lock or delete mobile devices remotely

Yes (optional)

Yes (optional)

Prevent the use of unwanted apps through blocklisting and allowlisting

Yes (optional)

Yes (optional)

Available for: Android (requirement: supported by manufacturer of operations system)

Yes (optional)

Yes (optional)

Endpoint Security for Android mobile devices. These always receive the latest protection updates thanks to a cloud connection

Yes (optional)

Yes (optional)

Available for: iOS (requirement: supported by manufacturer of operations system)

Yes (optional)

Yes (optional)

Configuration options for the Safari browser for iOS devices for the best possible surfing protection

Yes (optional)

Yes (optional)