G DATA CyberDefense	Leistungsbeschreibung	G DATA XDR	G DATA MXDR
Allgemein			
Besonderheiten des Herstellers			
Ganzheitlicher Hersteller und Anbieter von IT-Security-Lösungen und Services mit Hauptsitz in Deutschland			
Softwareentwicklung, Support und Service aus einem Haus			
Einhaltung hoher Datenschutzstandards nach DSGVO			
Datenhaltung ausschließlich in Deutschland			
Langjähriger Hersteller und Anbieter von IT-Security-Lösungen - Erfinder des Antivirus in 1987			
Support und Service			
Allgemein			
Support und Service sitzen direkt am Hauptsitz			
Support und Service haben direkte Verbindung zur Entwicklungsabteilung			
Hohe Qualität und gute Erreichbarkeit des Supports ist durch unabhängige Testinstitute nachgewiesen			
Sämtliche Produktdokumentation und Anleitungen werden in deutscher und englischer Sprache angeboten			
Support (Erweiterbar auf persönlichen 24/7 Support durch G DATA TAM Service)			
Supportsprachen		Ja	Ja
Der Support wird in deutscher Sprache angeboten		Ja	Ja
Der Support wird in englischer Sprache angeboten		Ja	Ja
Fallannahme - Der G DATA Support nimmt technische Anfragen per Telefon und E-Mail an.		Ja	Ja
Fallannahme per Telefon (Mo.-Fr., außer an Feiertagen) zwischen 9 und 16 Uhr MEZ/MESZ		Ja	Ja
Reaktion auf E-Mail-Anfragen am nächsten Geschäftstag (Mo.–Fr., außer an Feiertagen) zwischen 9 und 16 Uhr MEZ/MESZ		Ja	Ja
Onboarding			
Onboardinganleitung		Ja	Ja
Anleitung zur Installation der Agents in der Kundenumgebung		Ja	Ja
Downloadlink für Agent-Setups inklusive benötigter Parameter zur Installation		Ja	Ja
Übersicht freizugebener IP-Adressen, Ports und Domänen, um Agent-Server-Kommunikation sicherzustellen		Ja	Ja
Agent			
Schutz- und Erkennungsmechanismen bieten eine effektive Bedrohungserkennung mit hohen Erkennungsraten. Erkennung von komplexen Angriffsmustern durch systemweite Verhaltensüberwachung.		Ja	Ja
Agent: Systemvoraussetzungen			
Mind. 5 GB freier Festplattenspeicher		Ja	Ja
Mind. 2 GB freier Arbeitsspeicher (RAM)		Ja	Ja

G DATA CyberDefense	Leistungsbeschreibung	G DATA XDR	G DATA MXDR
	Für Installation und Betrieb des Agents ist eine stabile Internetverbindung zum G DATA Cloud-Backend erforderlich	Ja	Ja
	Windows	Ja	Ja
	CPU-Architektur: x64 mit SSE3 Befehlssatz oder ARM	Ja	Ja
	Alle Windows Betriebssystemversionen, die durch den "Erweiterten Support" von Microsoft abgedeckt sind. Die Windows LTSC Versionen werden nur unterstützt, solange sie vom "Mainstream Support" abgedeckt sind. Systeme mit ARM CPU werden erst ab Windows 11 24H2 unterstützt.	Ja	Ja
	Linux	Ja	Ja
	CPU-Architektur: x64 mit SSE3 Befehlssatz	Ja	Ja
	Ubuntu: Alle Ubuntu LTS Versionen, die durch den “Standard Support” vom jeweiligen Hersteller unterstützt werden	Ja	Ja
	Debian: Alle Debian Versionen, die durch den “LTS Support” vom jeweiligen Hersteller unterstützt werden	Ja	Ja
	SUSE Linux Enterprise Server (SLES): Alle SLES Versionen ab Version 15, die durch den “LTSS Support” vom jeweiligen Hersteller unterstützt werden	Ja	Ja
	Red Hat Enterprise Linux (RHEL): Alle RHEL Versionen, die durch den “Maintenance Support” oder “Extended Update Support” (Minor Versionen) vom jeweiligen Hersteller unterstützt werden	Ja	Ja
	Oracle Linux: Alle Oracle Linux Versionen, die durch den “Premier Support” vom jeweiligen Hersteller unterstützt werden	Ja	Ja
	macOS	Ja	Ja
	CPU-Architektur: 64-Bit Intel oder Apple-Silicon (ARM) CPUs	Ja	Ja
	Die aktuelle und die beiden vorangegangenen macOS Hauptversionen werden unterstützt	Ja	Ja
	Erforderlich: Festplattenvollzugriff für alle G DATA Services	Ja	Ja
	Erforderlich: Freigabe der G DATA Netzwerkerweiterung zum Filtern von Netzwerkverkehr	Ja	Ja
Agent: Allgemeine Funktionen			
	Single Agent - Der Agent bietet umfassende Unterstützung für Server- und Desktop-Systeme. Zusätzlich lizenzierte und aktivierte Features werden automatisch heruntergeladen und installiert.	Ja	Ja
	Verfügbar für: Windows, Linux, macOS	Ja	Ja
	Der Agent wird über ein parametrisierbares Setup für alle unterstützten Betriebssysteme bereitgestellt	Ja	Ja
	Zusätzlich lizenzierte und aktivierte Features werden vom Agent automatisch und im Hintergrund heruntergeladen und installiert	Ja	Ja
	Die Kommunikation mit dem Cloud-Backend erfolgt über einen begrenzten IP-Adressbereich und definierte Domänen	Ja	Ja
	Automatische Updates - Der G DATA Agent prüft regelmäßig, ob neue Updates vorliegen und installiert diese automatisch im Hintergrund	Ja	Ja
	Selbstschutz	Ja	Ja
	Der Agent verhindert unautorisierte Deinstallation	Ja	Ja

G DATA CyberDefense	Leistungsbeschreibung	G DATA XDR	G DATA MXDR
Agent: Schutz (Prevent)			
	Statischer Malwareschutz - Der statische Malwareschutz umfasst mehrere leistungsstarke Funktionen zur Bekämpfung von Schadsoftware. Der Agent kann Dateien auf Malwareinfektionen prüfen und infizierte Dateien in die Quarantäne verschieben. Darüber hinaus ist der Agent in der Lage, Geräte mit aktiver Malware zu bereinigen. Um stets auf dem neuesten Stand zu bleiben, lädt der Agent aktuelle Signaturen zur Malwareerkennung herunter. Ein weiterer wichtiger Bestandteil ist der On-Access-Scanner, der für eine kontinuierliche Überwachung sorgt. Zusätzlich berücksichtigt der Agent Ausnahmen beim Scannen, um Fehlalarme zu vermeiden und die Effizienz zu erhöhen. Für G DATA Produkte mit erweiterter Angriffserkennung (s.u.) werden die Metainformationen, der als infiziert erkannten Objekte, in Form von Telemetriedaten in das G DATA Cloud-Backend hochgeladen.	Ja	Ja
	Verfügbar für: Windows	Ja	Ja
	Die Erkennungsrate infizierter Dateien ist im Offline-Betrieb ähnlich hoch wie im Online-Betrieb	Ja	Ja
	Der Agent kann Dateien auf Malwareinfektionen prüfen	Ja	Ja
	Der Agent kann verdächtige Inhalte mithilfe des Antimalware Scan Interface (AMSI) auf Bedrohungen prüfen	Ja	Ja
	Der Agent kann mit Malware infizierte Dateien in die Quarantäne verschieben	Ja	Ja
	Der Agent kann Geräte mit aktiver Malware bereinigen	Ja	Ja
	Der Agent aktualisiert Signaturen zur Malwareerkennung automatisch	Ja	Ja
	Der Agent hat einen On Access Scanner	Ja	Ja
	Der Agent berücksichtigt Ausnahmen beim Scannen	Ja	Ja
Agent: Erkennung (Detect)			
	Verhaltensüberwachung - Die Verhaltenserkennung speichert Ereignisse verschiedener Sensorquellen und setzt diese endpunktübergreifend miteinander in Beziehung. Komplexe und über mehrere Prozesse sowie Sensorquellen verteilte Angriffe werden zuverlässig erkannt. Die Verhaltenserkennung geht dabei über statische Signaturen hinaus. Dabei ist sichergestellt, dass jederzeit die aktuellen Erkennungsregeln verfügbar sind.	Ja	Ja
	Verfügbar für: Windows, Linux, macOS	Ja	Ja
	Die Verhaltensüberwachung bezieht Prozessausführungen in die Angriffserkennung mit ein	Ja	Ja
	Verfügbar für: Windows	Ja	Ja
	Die Verhaltensüberwachung bezieht Registry-Ereignisse in die Angriffserkennung mit ein	Ja	Ja
	Die Verhaltensüberwachung bezieht Änderungen an der Systemkonfiguration in die Angriffserkennung mit ein	Ja	Ja
	Die Verhaltensüberwachung bezieht Netzwerk-Ereignisse in die Angriffserkennung mit ein	Ja	Ja
	Die Verhaltensüberwachung bezieht Dateisystem-Ereignisse in die Angriffserkennung mit ein	Ja	Ja
	Die Verhaltensüberwachung bezieht dynamisch geladene Module in die Angriffserkennung mit ein	Ja	Ja
	Die Verhaltensüberwachung bezieht Antimalware Scan Interface (AMSI) Ereignisse in die Angriffserkennung mit ein	Ja	Ja

G DATA CyberDefense	Leistungsbeschreibung	G DATA XDR	G DATA MXDR
Agent: Reaktion (Response)			
	Automatische Reaktionen	Ja	Ja
	Verfügbar für: Windows, Linux, macOS	Ja	Ja
	Als schadhaft eingestufte Prozesse und Prozessbäume können automatisch angehalten und beendet werden	Ja	Ja
	Als schadhaft eingestufte Dateien können automatisch in die Quarantäne verschoben werden	Ja	Ja
	Verfügbar für: Windows	Ja	Ja
	Der Zugriff auf als schadhaft eingestufte Dateien kann bei Zugriff verweigert werden	Ja	Ja
	Als schadhaft eingestufte Einträge in der Registry können automatisch gelöscht werden	Ja	Ja
	Live Terminal - Auditiertes Fernzugriffswerkzeug für G DATA Security-Analysten zur Durchführung von Remote-Analysen und Maßnahmen zur manuellen Eindämmung und Bereinigung von Angriffen. Es werden alle von G DATA Security-Analysten über das Live Terminal durchgeführten Aktivitäten protokolliert und auf Anfrage oder im Webportal als Audit-Log bereitgestellt. Das Live Terminal wird ausschließlich im Zusammenhang mit durch G DATA gemanagten Produkten und nur nach Vereinbarung mit dem Kunden eingesetzt.	N/A	Ja
Agent: Lokale UI			
	Verfügbar für: Windows	Ja	Ja
	Statusinformationen	Ja	Ja
	Der Betrieb des G DATA Agents wird für alle angemeldeten Endbenutzer durch ein Symbol in der Taskleiste angezeigt, sofern dies nicht anders konfiguriert ist	Ja	Ja
Cloud-Backend			
	Zentrale Bewertung und Verarbeitung von Bedrohungs- und Systeminformationen. Einfache Konfiguration aller Endpunkte und Funktionen. Bedrohungen werden durch Analyse und Bewertung von Sicherheitsereignissen erkannt und als Meldungen dargestellt.	Ja	Ja
Webportal			
	Sicheres Anmeldeverfahren mit OAuth und Multifaktor Authentifizierung (2FA/MFA)	Ja	Ja
	Authenticator Apps von Microsoft, Google und Duo Mobile werden für die 2FA-Anmeldung unterstützt	Ja	Ja
	Verfügbare Sprachen	Ja	Ja
	Deutsch, Englisch, Polnisch, Niederländisch, Portugiesisch, Französisch, Italienisch, Spanisch	Ja	Ja
	Dashboard	Ja	Ja
	Das Dashboard zeigt die Anzahl verwalteter Endpunkte sowie ihren Status an	Ja	Ja
	Das Dashboard zeigt den zeitlichen Verlauf und die Anzahl erkannter Vorfälle und deren Schweregrad als Diagramm innerhalb eines auswählbaren Zeitraums an	N/A	Ja
	Das Dashboard zeigt offene Meldungen an	Ja	N/A
	Das Dashboard zeigt eine Übersicht aktueller Handlungsempfehlungen an	N/A	Ja
	Das Dashboard zeigt statistische Informationen zur Vorfallsbehandlung durch Security-Analysten sowie die Anzahl an Meldungen und Vorfällen an	N/A	Ja

G DATA CyberDefense	Leistungsbeschreibung	G DATA XDR	G DATA MXDR
	Endpunkte	Ja	Ja
	Verwaltete Endpunkte sind in einer durchsuch-, filter- und sortierbaren Tabelle dargestellt	Ja	Ja
	In der Endpunktübersicht wird der aktuelle Status aller Endpunkte dargestellt	Ja	Ja
	Aktuell installierte Versionsstände der Agents können über das Webportal eingesehen werden	Ja	Ja
	Die Konfiguration einzelner Endpunkte kann eingesehen werden	Ja	Ja
	Agenten können über das Webportal deinstalliert werden	Ja	Ja
	Jeder Endpunkt kann separat konfiguriert werden	Ja	N/A
	Die Konfiguration von Endpunkten kann nach Organisationseinheiten erfolgen	Ja	N/A
	Endpunkte können so konfiguriert werden, dass Bedrohungen automatisch gestoppt oder ausschließlich protokolliert werden	Ja	N/A
	Endpunkte können so konfiguriert werden, dass beim Betrieb des Agenten ein Symbol in der Taskleiste angezeigt oder ausgeblendet wird	Ja	N/A
	Endpunkte können so konfiguriert werden, dass Benutzer bei einer Erkennung auf dem Endpunkt benachrichtigt werden oder nicht	Ja	N/A
	Meldungen	Ja	N/A
	Meldungen werden in einer durchsuch-, filter- und sortierbaren Tabelle angezeigt	Ja	N/A
	In der Meldungsübersicht können für jede Meldung zusätzliche Informationen angezeigt werden, z. B. Status, Schweregrad oder betroffener Endpunkt	Ja	N/A
	Die Details einzelner Meldungen können eingesehen werden	Ja	N/A
	In der Detailansicht einer Meldung werden alle betroffenen Artefakte angezeigt	Ja	N/A
	In der Detailansicht einer Meldung werden automatisch gestoppte Prozesse angezeigt	Ja	N/A
	In der Detailansicht einer Meldung werden relevante zusammenhängende Meldungen angezeigt	Ja	N/A
	In der Detailansicht einer Meldung kann eine passende Ausnahme hinzufügt werden	Ja	N/A
	In der Detailansicht einer Meldung können Artefakte aus der Quarantäne wiederhergestellt werden	Ja	N/A
	In der Detailansicht einer Meldung können Artefakte aus der Quarantäne gelöscht werden	Ja	N/A
	In der Detailansicht einer Meldung können Nutzer Kommentare zur Meldung hinterlassen	Ja	N/A
	Der Meldungsgraph zeigt an einer Meldung beteiligte Prozesse als Graph an und hebt Erkennungen visuell hervor	Ja	N/A
	Detailinformationen zu einzelnen Knoten im Meldungsgraph können angezeigt werden, z. B. verfügbare Dateiinformationen	Ja	N/A
	Ausnahmenverwaltung	Ja	N/A
	Ausnahmen werden in einer durchsuch-, filter- und sortierbaren Tabelle angezeigt	Ja	N/A
	In der Ausnahmeübersicht können für jede Ausnahme zusätzliche Informationen angezeigt werden, z. B. Typ, Ausnahmewert oder Ausnahmemodus	Ja	N/A
	In der Ausnahmenverwaltung können neue Ausnahmen angelegt werden	Ja	N/A
	Die Details einzelner Ausnahmen können eingesehen werden	Ja	N/A
	In der Detailansicht einer Ausnahme wird der Geltungsbereich dargestellt	Ja	N/A

G DATA CyberDefense Leistungsbeschreibung	G DATA XDR	G DATA MXDR
Eine Ausnahme kann geändert werden	Ja	N/A
Eine Ausnahme kann gelöscht werden	Ja	N/A
Quarantäneverwaltung	Ja	N/A
Quarantänecontainer werden in einer durchsuch-, filter- und sortierbaren Tabelle angezeigt	Ja	N/A
In der Quarantäneübersicht können für jeden Quarantänecontainer zusätzliche Informationen angezeigt werden, z. B. Endpunkt, Artefakte oder Erkennungen	Ja	N/A
Die Details einzelner Quarantänecontainer können eingesehen werden	Ja	N/A
In der Detailansicht eines Quarantänecontainers wird die zugehörige Meldung verlinkt	Ja	N/A
In der Detailansicht eines Quarantänecontainers wird der zugehörige Endpunkt verlinkt	Ja	N/A
In der Detailansicht eines Quarantänecontainers werden alle enthaltenen Artefakte namentlich angezeigt	Ja	N/A
Die Artefakte im Quarantänecontainer können auf dem Endpunkt wiederhergestellt werden	Ja	N/A
Ein Quarantänecontainer kann vom Endpunkt gelöscht werden	Ja	N/A
E-Mail Benachrichtigung	Ja	Ja
Benachrichtigungsempfänger werden in einer filterbaren Tabelle angezeigt	Ja	Ja
In der Empfängerübersicht werden die zugeordneten Benachrichtigungsereignisse angezeigt	Ja	Ja
In der Empfängerübersicht werden die zugeordneten Benachrichtigungssprachen angezeigt	Ja	Ja
Profilverwaltung	Ja	Ja
Kontaktdaten zum eigenen Profil werden angezeigt und sind änderbar	Ja	Ja
Anzeigesprache und Design des Webportals werden angezeigt und sind änderbar	Ja	Ja
Das Zugangs-Passwort kann geändert werden	Ja	Ja
Die Zwei-Faktor-Authentisierung kann zurückgesetzt werden	Ja	Ja
Benutzerverwaltung	Ja	Ja
Benutzer und Benutzerinformationen werden in einer durchsuch-, filter- und sortierbaren Tabelle angezeigt	Ja	Ja
In der Benutzerübersicht werden zugewiesene Rollen und zugeordnete Organisationseinheiten angezeigt	Ja	Ja
Es können einzelne Benutzer deaktiviert werden	Ja	Ja
Benutzern können je eine Rolle und Organisationseinheit zugewiesen werden, um Zugriffsberechtigungen zu steuern	Ja	Ja
Rollenverwaltung	Ja	Ja
Rollen werden in einer durchsuch-, filter- und sortierbaren Tabelle angezeigt	Ja	Ja
In der Rollenübersicht werden die zugeordneten Organisationseinheiten angezeigt	Ja	Ja
Einer Rolle können Zugriffsberechtigungen für Produkt- und Funktionsbereiche zugeordnet werden	Ja	Ja
Organisationseinheiten verwalten	Ja	Ja
Organisationseinheiten werden hierarchisch verwaltet	Ja	Ja
Vorfälle	N/A	Ja

G DATA CyberDefense Leistungsbeschreibung	G DATA XDR	G DATA MXDR
Vorfälle werden in einer durchsuch-, filter- und sortierbaren Tabelle angezeigt	N/A	Ja
In der Vorfallsübersicht wird der aktuelle Status aller Vorfälle angezeigt	N/A	Ja
In der Vorfallsübersicht werden betroffene Endpunkte angezeigt	N/A	Ja
In der Vorfallsübersicht wird die Auswirkung aller Vorfälle angezeigt	N/A	Ja
Handlungsempfehlungen können pro Vorfall eingesehen werden, falls vorhanden	N/A	Ja
Der Detailverlauf einzelner Vorgänge kann eingesehen werden	N/A	Ja
Im Detailverlauf eines Vorgangs werden alle zugeordneten Meldungen und betroffenen Artefakte angezeigt	N/A	Ja
Im Detailverlauf eines Vorgangs werden Auswirkung, Priorität und Dringlichkeit angezeigt und beschrieben	N/A	Ja
Der Meldungsgraph zeigt Zusammenhänge zu einzelnen Meldungen als Graph an und hebt Detections visuell hervor	N/A	Ja
Detailinformationen zu einzelnen Knoten im Meldungsgraph können angezeigt werden, z. B. verfügbare Dateiinformationen	N/A	Ja
Interaktionen und Aktivitäten von Security-Analysten werden in Form eines zeitlichen Verlaufs anfgezeigt	N/A	Ja
Handlungsempfehlungen	N/A	Ja
Handlungsempfehlungen werden in einer durchsuch-, filter- und sortierbaren Tabelle angezeigt	N/A	Ja
In der Handlungsempfehlungsübersicht wird der aktuelle Status aller Handlungsempfehlungen angezeigt	N/A	Ja
In der Handlungsempfehlungsübersicht werden betroffen Endpunkte zu allen Handlungsempfehlungen angezeigt	N/A	Ja
Detailinformationen zu einzelnen Handlungsempfehlungen können angezeigt werden	N/A	Ja
In der Detailansicht werden Metainformationen, Überschrift und Beschreibungstext zu einer Handlungsempfehlung angezeigt	N/A	Ja
In der Detailansicht gibt es eine Verlinkung zum verknüpften Vorfall	N/A	Ja
Protokolle	N/A	Ja
Ausgeführte Aktionen können in einer Protokollübersicht angezeigt werden	N/A	Ja
Meldepflichten-Unterstützung	N/A	Ja
Aufbereitung von Informationen zu Vorfällen bei Bedarf, zur Unterstützung von Meldepflichten	N/A	Ja
Notfallkontakte	N/A	Ja
Erweiterte Angriffserkennung		
Ergänzend zu den lokalen Schutz-, Erkennungs- und automatischen Reaktionskomponenten. Erkennung von komplexen Angriffsmustern über die gesamte abgedeckte Kundenumgebung. Erkennung von Angriffsausbreitung in der Kundenumgebung. Einbeziehung und Verknüpfung mehrerer Sensorquellen zur Erkennung komplexer Angriffe	Ja	Ja
Erweiterte Angriffserkennung	Ja	Ja

G DATA CyberDefense — Leistungsbeschreibung	G DATA XDR	G DATA MXDR
Security-Events werden aus unterschiedlichen Quellen im Cloud-Backend gespeichert	Ja	Ja
Anbindung von Standard-SIEM-Systemen	Ja	Ja
Weiterleitung von Erkennungsinformationen aus dem G DATA Cloud-Backend an Standard-SIEM-Systeme im CEF- oder ECS-Format auf Anfrage	Ja	Ja
Verfügbarkeiten		
Infrastruktur	Ja	Ja
Die Infrastruktur zur Analyse und Bewertung von Daten sowie zur Benachrichtigung und Support ist jährlich mindestens 99,5% am Übergangspunkt verfügbar	Ja	Ja
Erforderliche Wartungsarbeiten, die zur Nichtverfügbarkeit der Infrastruktur führen, sollen pro Quartal acht Stunden nicht überschreiten	Ja	Ja
Anstehende Wartungsarbeiten werden zwei Arbeitstage zuvor angekündigt	Ja	Ja
Compliance / Datenschutz		
Datenhaltung ausschließlich in Deutschland und deutschen Rechenzentren. Strenge Einhaltung hoher Datenschutzstandards nach DSGVO	Ja	Ja
Hostingstandort (G DATA Rechenzentrum): Bochum	Ja	Ja
Hostingstandort (Glasfaser Ruhr (GFR)): Bochum, Herne	Ja	Ja
Hostingstandorte (IONOS): Frankfurt am Main, Berlin	Ja	Ja
Compliance		
ISMS zertifiziert nach ISO/IEC 27001	Ja	Ja
G DATA Managed SOC		
24/7 SOC-Service für G DATA Managed Extended Detection and Response. Alle Mitarbeitenden des Security Operation Centers sind mit dem BSI Vorfall-Praktiker zertifiziert.	N/A	Ja
24/7 Detect Analyst Service		
Baseline-Analyse überwachter Geräte, um Anomalien zu erkennen	N/A	Ja
Die Baseline-Analyse findet während des Onboardings für einen Zeitraum von bis zu sechs Kalenderwochen statt	N/A	Ja
Im Log-Only-Modus zeichnet der Agent nur Security-Events auf	N/A	Ja
Aufgezeichnete Security-Events werden im Cloud Backend für Baseline-Analyse bereitgestellt, automatisch normalisiert, angereichert und korreliert	N/A	Ja
Es wird ein Profil für die Kundenumgebung zur Erkennung von Anomalien erstellt	N/A	Ja
Basierend auf dem erstellten Profil werden Ausnahmen für die Kundenumgebung definiert	N/A	Ja
24/7 Monitoring und Remote-Analyse	N/A	Ja
Security-Analysten untersuchen alle eingehenden Security-Meldungen von allen überwachten Geräten	N/A	Ja
Security-Analysten analysieren Security-Meldungen und Vorfälle im Bedarfsfall und nach Vereinbarung remote per Live Terminal	N/A	Ja
Security-Analysten untersuchen Vorfälle auf False Positives	N/A	Ja

G DATA CyberDefense	Leistungsbeschreibung	G DATA XDR	G DATA MXDR
	Alle von Security-Analysten durchgeführten Aktivitäten werden automatisch in einem Auditlog protokolliert	N/A	Ja
	24/7 Angriffsbenachrichtigung per E-Mail	N/A	Ja
	E-Mail-Benachrichtigung bei Vorfallserkennung	N/A	Ja
	E-Mail-Benachrichtigung bei Änderung des Vorfall-Status	N/A	Ja
	Handlungsempfehlungen - G DATA Security-Analysten erstellen Handlungsempfehlungen im Falle eines erkannten Angriffs oder wenn ein Mitwirken des Kunden zur Behandlung notwendig ist. Die Handlungsempfehlung enthält Informationen zum erkannten Angriff und dessen Klassifizierung und beschreibt mögliche Handlungsoptionen zur Behandlung durch den Kunden	N/A	Ja
	24/7 Response Analyst Service		
	Angriffsausbreitung eindämmen - Im Falle eines Angriffs werden betroffene Endpunkte durch G DATA Security-Analysten vom Netzwerk isoliert (für Linux, Windows)	N/A	Ja
	Proaktive False Positive Behandlung - G DATA Security-Analysten untersuchen gemeldete Vorfälle auf potenzielle False Positives und lösen diese proaktiv	N/A	Ja
	Scannen einzelner Dateien auf dem Endpunkt durch Security-Analysten (On-Demand Scan)	N/A	Ja
	Remote Bereinigung persistierter Malwareartefakte	N/A	Ja
	Security-Analysten können per Live Terminal bei der Analyse identifizierte Malwareartefakte manuell entfernen	N/A	Ja
	Security Operations Manager		
	Direkter Ansprechpartner für Security Anfragen - Security Operations Manager (SOM)	N/A	Ja
	Dedizierte, deutsch- und englischsprachige Ansprechpartner beim Hersteller, die mit der Umgebung, den Prozessen und Ansprechpartnern des Auftraggebers vertraut sind	N/A	Ja
	24/7 Priorisierte Fallannahme per Telefon bei Anfragen zur Sicherheit	N/A	Ja
	24/7 Telefonische Benachrichtigung bei kritischen Vorfällen, je Vorfall bis zu fünf Kontaktversuche innerhalb von 48 Stunden bei Nichterreichbarkeit	N/A	Ja
	Reaktion auf E-Mail-Anfragen am nächsten Geschäftstag (Mo.–Fr., außer an Feiertagen) zwischen 9 und 16 Uhr MEZ/MESZ	N/A	Ja
	Incident First Response (4 Std. je Quartal)		
	Qualifizierung von potentiellen Verdachtsfällen	N/A	Ja
	IT-Forensische Erstanalyse durch zertifizierte Fachleute	N/A	Ja
	Risikobewertung und Informationssammlung	N/A	Ja
	Telefonische Erstberatung im Falle eines vom Kunden gemeldeten IT-Sicherheitsvorfalls	N/A	Ja
	TAM Service (Im Produkt MXDR als Add-on inklusive oder als Add-on zum Produkt XDR optional erwerbbar)		
	Der G DATA TAM Service bietet Ihnen erweiterten, persönlichen Support für ihre G DATA Produkte. Ihr Technical Account Manager kennt Ihre Umgebung, priorisiert Ihre Anliegen und unterstützt Sie aktiv dabei, Risiken zu reduzieren, Störungen schneller zu beheben und Ihre Sicherheitslösungen optimal einzusetzen.	Ja (Optional)	Ja

G DATA CyberDefense	Leistungsbeschreibung	G DATA XDR	G DATA MXDR
	Der G DATA TAM Service umfasst, nach Buchung zum Produkt XDR, Support für die G DATA Produkte: XDR, MXDR, Policy Control, Mobile Device Management und Mail Protection. Ohne zusätzliche Buchung umfasst der Support ausschließlich das Produkt MXDR.	Ja (Optional)	Ja
	24/7 Support	Ja (Optional)	Ja
	24/7 Fallannahme per Telefon	Ja (Optional)	Ja
	24/7 Priorisierte Fallannahme per Telefon bei technischen Anfragen	Ja (Optional)	Ja
	Remote-Support über geeignete Fernwartungssoftware	Ja (Optional)	Ja
	Persönliches Remote Onboarding	Ja (Optional)	Ja
	Persönliches Onboarding durch dedizierte Ansprechpartner	Ja (Optional)	Ja
	Einführung in das Produkt und den Betrieb	Ja (Optional)	Ja
	Persönliche E-Mail mit wichtigen Informationen zum Onboarding und der Installation	Ja (Optional)	Ja
	Beantwortung von Fragen und Unterstützung durch persönlichen Ansprechpartner	Ja (Optional)	Ja
	Das persönliche Onboarding wird in deutscher oder englischer Sprache angeboten	Ja (Optional)	Ja
	Es findet eine Bestandsaufnahme der IT-Umgebung des Endkunden statt	N/A	Ja
	Es werden Besonderheiten der IT-Infrastruktur identifiziert, wie z. B. geschäftskritische Systeme	N/A	Ja
	Es wird vereinbart, inwiefern Security-Analysten Remote-Analysen und -Reaktionen auf einzelnen Endpunkten durchführen dürfen	N/A	Ja
	Es werden Ausnahmen der Schutzkomponenten für einzelne Endpunkte vereinbart	N/A	Ja
	Es gibt eine Risikoaufklärung für den Fall eingeschränkter Handlungsbefugnisse durch Security-Analysten	N/A	Ja
	Es gibt eine Risikoaufklärung für den Fall gesetzter Ausnahmen für Schutzkomponenten	N/A	Ja
	Es werden Ansprechpartner und Kontaktdaten für Benachrichtigungen vereinbart	N/A	Ja
	Es werden Ansprechpartner und Kontaktdaten für die telefonische Angriffsbenachrichtigung vereinbart	N/A	Ja
	Es wird ein Skript zur Deinstallation von bereits installierten Security-Lösungen bereitgestellt	Ja (Optional)	Ja
	Es wird eine technische Anleitung für die Verteilung des erworbenen Produktes bereitgestellt	Ja (Optional)	Ja
	Es gibt einen Abschlussbericht mit getroffenen Vereinbarungen	N/A	Ja
	Produktkonfiguration	Ja (Optional)	Ja
	Anpassungen der Produktkonfiguration können per E-Mail oder telefonisch angefragt werden	Ja (Optional)	Ja
	Die Anpassung der Produktkonfiguration erfolgt nach Prüfung und ggf. Rücksprache innerhalb von zwei Kalenderwochen	Ja (Optional)	Ja
	Ausnahmen werden auf Anfrage per E-Mail oder telefonisch nach Prüfung und ggf. Rücksprache innerhalb von zwei Kalenderwochen definiert und ausgerollt	Ja (Optional)	Ja
	Regelmäßige Konfig-Checks (2x pro Jahr)	Ja (Optional)	Ja
	Soll- / Ist-Abgleich der aktuellen Produktkonfiguration (2x pro Jahr)	Ja (Optional)	Ja
	Abgleich der Produktkonfiguration gegenüber aktuellen Best Practices (2x pro Jahr)	Ja (Optional)	Ja
	Migration	Ja (Optional)	Ja
	Begleitung bei der Migration durch Technical Account Manager	Ja (Optional)	Ja

G DATA CyberDefense	Leistungsbeschreibung	G DATA XDR	G DATA MXDR
	Begleitung und Unterstützung bei einem Wechsel von bereits installierten Security-Lösungen	Ja (Optional)	Ja
	SIEM-Anbindung	Ja (Optional)	Ja
	Unterstützung bei der Anbindung von Standard-SIEM-Systemen durch Technical Account Manager	Ja (Optional)	Ja
	Bug- und Feature Annahme	Ja (Optional)	Ja
	Priorisierung bei eingesendeten Problemen, Fehlern oder Bugs	Ja (Optional)	Ja
	Aufnahme von Anfragen zu neuen Produktwünschen	Ja (Optional)	Ja
	Einsendung über spezielle Online-Formulare	Ja (Optional)	Ja
	Einsenden verdächtiger Inhalte zu Analyse	Ja (Optional)	Ja
	Priorisierte Analyse eingesendeter verdächtiger Inhalte	Ja (Optional)	Ja
	Einsendung über spezielle Online-Formulare	Ja (Optional)	Ja
	Schnelle Bearbeitung durch erfahrene Fachleute	Ja (Optional)	Ja
Policy Control (Als Add-on zu den Produkten XDR und MXDR oder als separate Lizenzlösung optional erwerbbar)			
	Device Control		
	Systemvoraussetzung	Ja (Optional)	Ja (Optional)
	Windows: CPU Architektur: x64 mit SSE3 Befehlssatz oder ARM	Ja (Optional)	Ja (Optional)
	Windows: Alle Windows Betriebssystemversionen, die durch den "Erweiterten Support " von Microsoft abgedeckt sind. Die Windows LTSC Versionen werden nur unterstützt, solange sie vom "Mainstream Support" abgedeckt sind. Systeme mit ARM CPU werden erst ab Windows 11 24H2 unterstützt.	Ja (Optional)	Ja (Optional)
	Zugriffskontrolle für an Computer anschließbare Geräte	Ja (Optional)	Ja (Optional)
	Verfügbar für: Windows	Ja (Optional)	Ja (Optional)
	Abgedeckte Geräte: Wechseldatenträger (z. B. USB Sticks), optische Laufwerke, Diskettenlaufwerke, Windows Portable Devices und Webcams	Ja (Optional)	Ja (Optional)
Mail Protection (Als Add-on zu den Produkten XDR und MXDR oder als separate Lizenzlösung optional erwerbbar)			
	Mail Protection für Microsoft Exchange Online		
	Systemvoraussetzungen	Ja (Optional)	Ja (Optional)
	Aktives Microsoft 365 Exchange Online oder Microsoft Exchange Online Konto	Ja (Optional)	Ja (Optional)
	E-Mail Schutz vor Malware und Spam	Ja (Optional)	Ja (Optional)
	Verfügbar für: Microsoft Exchange Online	Ja (Optional)	Ja (Optional)
Mobile Device Management (Als Add-on zu den Produkten XDR und MXDR oder als separate Lizenzlösung optional erwerbbar)			
	Mobile Device Management für Android- und iOS-Geräte		
	Systemvoraussetzung	Ja (Optional)	Ja (Optional)
	Alle Android-Versionen, die vom Betriebssystemhersteller unterstützt werden	Ja (Optional)	Ja (Optional)
	Alle iOS-Versionen, die vom Betriebssystemhersteller unterstützt werden	Ja (Optional)	Ja (Optional)
	Geräteverwaltung und Schutzleistung	Ja (Optional)	Ja (Optional)

G DATA CyberDefense Leistungsbeschreibung	G DATA XDR	G DATA MXDR
Verfügbar für: Android, iOS (Voraussetzung: durch Betriebssystemhersteller unterstützt)	Ja (Optional)	Ja (Optional)
Mobilgeräte können im Webportal zentral verwaltet werden	Ja (Optional)	Ja (Optional)
Sicherheitseinstellungen und Richtlinien können über das Webportal an alle verwalteten Mobilgeräte ausgerollt werden	Ja (Optional)	Ja (Optional)
Schutz von sensiblen Daten vor unerlaubtem Zugriff: Orten, Sperren oder Löschen von Mobilgeräten aus der Ferne	Ja (Optional)	Ja (Optional)
Nutzung unerwünschter Apps durch Block- und Allowlisting verhindern	Ja (Optional)	Ja (Optional)
Verfügbar für: Android (Voraussetzung: durch Betriebssystemhersteller unterstützt)	Ja (Optional)	Ja (Optional)
Endpoint Security für Android Mobilgeräte. Diese erhalten durch eine Cloudanbindung immer die aktuellsten Schutz-Updates	Ja (Optional)	Ja (Optional)
Verfügbar für: iOS (Voraussetzung: durch Betriebssystemhersteller unterstützt)	Ja (Optional)	Ja (Optional)
Konfigurationsmöglichkeiten für den Safari-Browser für iOS-Geräte für bestmöglichen Surfschutz	Ja (Optional)	Ja (Optional)