

# G DATA 365 | MXDR

Expand your team with our 24/7 service for  
Managed Extended Detection and Response (MXDR)



## Ideal for companies that

- ➔ want to ensure that attacks are stopped quickly - even at night and at weekends.
- ➔ want more IT security without investing in additional specialist staff.
- ➔ need to implement the NIS-2 requirements for attack response.
- ➔ want to be immediately informed about potential threats.



## Your Managed SOC with individual support

### 24/7 Threat Hunting & Response

Proactive protection: Highly specialized SOC analysts monitor your systems 24/7. Thanks to cross-endpoint detection, we always have your entire network in view.

We block out attackers for you.

In case of critical incidents, we will call you directly.

### Best service – right from the start

We have an open ear for all your requirements: Which devices, folders or files are we allowed to respond to and how? And which ones should not be viewed at all?

During onboarding, we advise you in detail and customize Managed XDR for you in the best possible way.

### Close support from experts

Seamlessly expand your security team by having ongoing access to the knowledge of our experts.

Your contacts are based in Bochum, Germany and can be reached 24/7 by telephone - with a direct line to the analysts, who are also based in Bochum.

## Service level G5 and G7

# For your entire IT environment

Are you looking for an MXDR service that covers your entire network?  
Then our G5 and G7 service levels are just right for you.

### Benefits

	G5	G7
	Convenient 24/7 managed security service tailored to your needs for critical incidents	Comprehensive 24/7 managed security service for an increased level of protection and with a direct contact person
Web Console	✓	✓
NextGen Endpoint Agent (Windows, Linux)	✓	✓
24/7 Detection & Response Analyst Service	Incidents classified as critical	All incidents
24/7 support in different languages	✓	✓
Personal support from Technical Account Management		✓
Onboarding Workshop	✓ (one-off costs)	✓ (included)
Regular Config Checks		✓
Incident Compromise Check		✓
24/7 attack notification by telephone		✓
24/7 attack notification by email	✓	✓
Incident Response Retainer Gold/Platinum	optional	optional
365 Mail Protection	optional	optional
Mobile Device Management	optional	optional
Device Control	optional	optional

## Service Level G3

# Especially for servers

An attack is most dangerous when it manages to penetrate your critical servers. This is exactly where our G3 service level comes in. By specifically monitoring your servers, you can contain attacks in good time that could have serious consequences for your company.



Test the full MXDR service for two months  
in your own environment:  
[gdata.de/mxdr-testen](https://gdata.de/mxdr-testen)

