Thalia strengthens its cyber defense: why **MXDR** is indispensable for IT managers

The challenge

- Round-the-clock monitoring of all IT
- Managed security service
- Streamlined process for distributing updates

The solution

- G DATA 365 | MXDR (Managed Extended Detection and Response) ↗

The advantages

- 24/7 monitoring of IT systems, 365 days a year
- Immediate response to incidents
- Resource-efficient distribution of updates

Thalia

Sector:
Market-leading omnichannel bookseller in this region

Scope:
6,500 employees in around 380 bookstores in the German-speaking region

Headquarter:
Hagen, Germany

High IT availability is a key prerequisite for commercial success, and not only in online business. Thalia, a traditional bookseller, also relies on high-availability IT for orders. To protect its entire network from cyber attacks and other outages, the family-owned company uses Managed Extended Security Services from G DATA CyberDefense – G DATA 365 | MXDR.

Thalia Bücher GmbH is the leading bookseller in the German-speaking market. Around 6,500 employees work at the key locations in Hagen, Münster, Berlin, Aachen and Linz, as well as in approximately 380 other bookstores. Thalia also has a strong digital presence through its online shop and its own app. Its omnichannel strategy enables the company to let customers shop at any time, across multiple channels. Thalia has established an extensive IT infrastructure to ensure the close integration of traditional book retailing and its digital business. The digital heart of this infrastructure is based in a hybrid data centre and cloud environment. Every order placed in the online shop or in a bookstore, as well as the networking of the cash register systems, converges here. The high availability of the digital environment is a key success factor for Thalia.

"For Thalia, the confidentiality, integrity and availability of information is paramount," says Moundji Merabet, Senior Manager Retail IT at Thalia, who is responsible for IT in the bookstores. "We have to ensure that our systems are available around the clock, and in particular that our customers' data is available." Those responsible are aware that an interruption or failure of the IT infrastructure can have far-reaching consequences for the company – from financial losses to the loss of customers and damage to the company's reputation. The constant growth of the company in recent years has caused the omnichannel bookseller to see an increase in attack attempts as well.

Managed security for greater IT security

SThose in charge quickly realised that more of the same technology alone would not meet the desired aim. So the requirements for a new solution were quickly established - a managed security service with a security team that monitors Thalia's systems 24/7 was needed, able to react quickly and directly in suspicious cases. "We are very much guided by the BSI's baseline protection and ISO 27001 to ensure the protection of our data and processes. However, to secure our IT in the long term, we decided to work with an experienced IT security company that also provides us with the appropriate

resources," says Moundji Merabet. Experts are better at detecting small and inconspicuous anomalies in the network, which can occur as a result of a very wide range of attacks, and to do so more quickly. Security analysts can also identify social engineering attempts and ransomware attacks at an early stage. The first point of contact was G DATA CyberDefense AG, whose security solution Thalia has been using for more than 20 years. "We have a long-standing relationship of trust with G DATA. So it was an obvious first step to ask our partner if they could offer a solution," explains Moundji Merabet. "In addition, our contacts were familiar with our requirements and also with the specifics of the network." In fact, G DATA's Managed Extended Detection and Response offering, G DATA 365 | MXDR, met Thalia's requirements exactly, so those in charge decided to continue to develop their collaboration.

Streamlined update process

DSince the omnichannel bookseller makes only minor changes in the 'frozen zone' between November and January, to ensure system availability and performance during the Christmas season, G DATA and Thalia were able to focus on the project planning and roll-out of new agents. The focus was on one key prerequisite: since all communication in the network and to the shops is via secure connections, resource-efficient distribution of updates for MXDR, which is installed on a total of 6,000 computers, was needed. Normally, each individual agent downloads updates for the application, the signatures or the rules of the protection components directly from the G DATA servers. Specifically, the challenge was to distribute updates without affecting the web traffic of the bookstores or the online shop. Here, G DATA was able to use an existing caching process from

Thalia to distribute updates, for which dedicated servers were provided. This means that each update only needs to be uploaded to the Thalia data centre once. G DATA has therefore stored this alternative data source in the agents. All agents query the defined internal download source, which can respond to the majority of queries from the cache. Download communication with the G DATA servers via the internet is only necessary if a file is not yet in the cache. This solution is based on the open-source software HA-Proxy. "G DATA implemented our request immediately," says Moundji Merabet. "It's very useful that G DATA has developed an distribution solution with us that is integrated into our already established patching processes."

G DATA 365 | MXDR

IT SECURITY IS TEAM PLAY

Roll-out with integrated check-up

The roll-out of MXDR began among more than 6,000 clients immediately after the frozen zone. The software was implemented without any major problems. One of the main reasons for this was G DATA's tried and tested implementation process. In this process, the cyber defense specialist provides customers with a script that checks the compatibility of the systems with the XDR agent. The tool automatically checks whether the computer has a specified patch status. This meant that all systems with old Windows patch statuses could be identified.

Direct contact with support

Six months after the roll-out, Thalia's conclusion is positive. The systems are monitored around the clock by G DATA using a team of experts who react immediately to even minor suspicious cases and disconnect suspicious systems from the network. If the help of employees is required, Thalia receives clear instructions on what to do. "G DATA's security team takes a lot of work off our hands", says Moundji Merabet. "We can concentrate on essential IT tasks, safe in the knowledge that an experienced partner is taking care of our IT security." A major advantage here is the direct contact with G DATA's support team in Bochum. There is no language barrier to communication between G DATA and Thalia, especially in stressful situations.
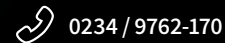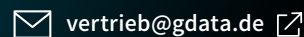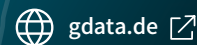
The solution is also used in Austria, because the IT managers are keen to operate a standardised IT landscape. Roll-out in Switzerland is also planned for this reason. In view of the strong cooperation, it is not surprising that Thalia is continuing the long-standing cooperation – true to the motto "Never change a winning team".

Curious how you can secure your business with G DATA?
Find out more here:

🌐 **gdata.de** ↗   ✉ **vertrieb@gdata.de** ↗   ✆ **0234 / 9762-170**

G DATA CyberDefense