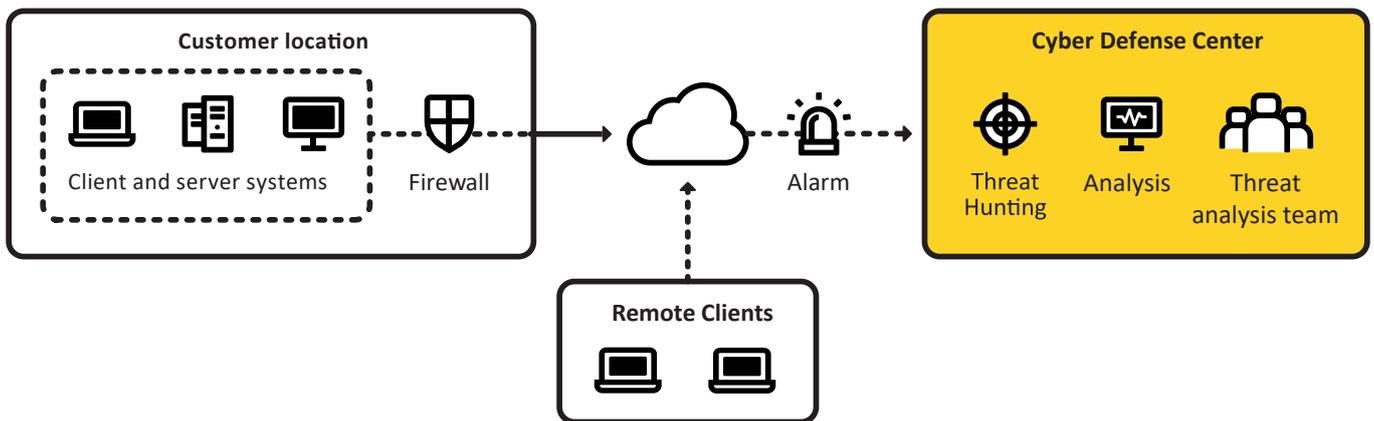


Endpoint Detection Response (EDR) as a Service

Endpoints pose a significant security risk because they are the primary points of attack against your organization’s network. With traditional endpoint technologies unable to detect the latest advanced threats, however, identifying and responding to endpoint attacks has never been more difficult.

Endpoint detection and response



UMB’s EDR as a service significantly improves endpoint attack visibility by providing an experienced team of threat hunters, the latest EDR technology, as well as up-to-date threat intelligence to identify threats that may be overlooked by other monitoring systems.

New level of endpoint security

Endpoint detection and response technologies take endpoint security to a new level by improving threat visibility and coverage beyond the scope of traditional antivirus and network monitoring tools. UMB will detect key system events, such as registry and file changes, on any host where a sensor is installed, and use real-time behavioral monitoring to detect suspicious activity.

The early detection of attacks on endpoints is critical, but without a team of security professionals harnessing

the power of the latest EDR technology while proactively scanning for threats around the clock, your organization is unlikely to achieve the improvements in threat detection you are striving for.

A team of security experts

EDR as a service from UMB eases the challenge of 24/7 endpoint monitoring by offering the latest technology, a 24/7 team of cybersecurity experts and up-to-date threat data as a service.

Benefits from EDR as a Service

Less impact on your daily business

We provide detection, analysis and response to most threats. So you can work in peace.

Optimization of internal security costs and resources

Create the time for your internal IT team to take care of the truly relevant security issues while UMB takes care of protecting your environment.

7x24 Modular and demand-driven security service

Our modular services allow you to optimize your cybersecurity according to your needs - both technically and financially

Shadow IT option - Network scanning without agents

This option is used to scan the connected network for assets, even if they do not have an agent installed. Printers, servers, storage devices, and mobile devices will be detected. If admin rights to these previously unknown devices are available, an agent can be installed. In addition, recommendations are provided to increase the level of protection within the respective network.

Your advantages

- 7x24 threat monitoring
- 7x24 threat analysis & triage
- Concrete recommendation for action for all escalated incidents
- Forensic data collection and analysis of affected end points
- 24x7 hotline to contact the Cyber Defense Center
- Monthly service report

Sounds interesting? Contact us!

We are happy to answer your questions regarding cybersecurity, EDR and more.

Contact

Markus Kaegi
Business Lead Security
markus.kaegi@umb.ch
+41 44 805 14 47
www.umb.ch