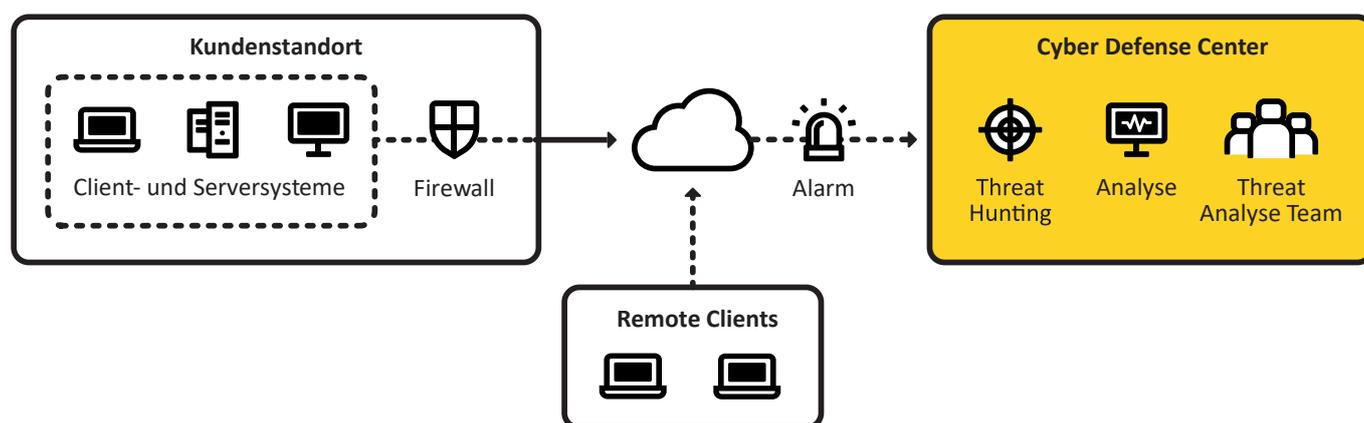


# Endpoint Detection Response (EDR) as a Service

Endgeräte stellen ein erhebliches Sicherheitsrisiko dar, da sie die wichtigsten Angriffspunkte auf das Netzwerk Ihres Unternehmens sind. Da herkömmliche Endpunkt-Technologien jedoch nicht in der Lage sind, die neuesten fortschrittlichen Bedrohungen zu erkennen, war es noch nie so schwierig, Angriffe auf Endpunkte zu identifizieren und darauf zu reagieren.

## Endpoint Detection and Response



Mit EDR as a Service von UMB verbessern Sie die Sichtbarkeit von Angriffen auf Endgeräte erheblich, indem Sie ein erfahrenes Team von Bedrohungsjägern, die neueste EDR-Technologie und aktuelle Bedrohungsdaten bereitstellen, um Bedrohungen zu identifizieren, die von anderen Kontrollen übersehen werden können.

### Neue Stufe der Endpunktsicherheit

Endpoint Detection and Response-Technologien heben die Endpunktsicherheit auf eine neue Stufe, indem sie die Sichtbarkeit von Bedrohungen und die Abdeckung über den Umfang herkömmlicher Antiviren- und Netzwerküberwachungstools hinaus verbessern. Auf jedem Host, auf dem ein Sensor installiert ist, erfasst UMB wichtige Systemereignisse wie Registrierungs- und Dateiänderungen und nutzt Echtzeit-Verhaltensüberwachung, um verdächtige Aktivitäten zu erkennen. Die frühzeitige Erkennung

von Angriffen auf Endpunkte ist von entscheidender Bedeutung, aber ohne ein Team von Sicherheitsexperten, das die Leistungsfähigkeit der neuesten EDR-Technologie nutzt und rund um die Uhr proaktiv nach Bedrohungen sucht, wird Ihr Unternehmen wahrscheinlich nicht die angestrebten Verbesserungen bei der Erkennung von Bedrohungen erreichen.

### Team von Sicherheitsexperten

EDR as a Service von UMB erleichtert die Herausforderung der 24/7-Endpunktüberwachung, indem es die neueste Technologie, ein rund um die Uhr verfügbares Team von Cybersicherheitsexperten und aktuelle Bedrohungsdaten als Service anbietet.

## Nutzen durch EDR as a Service

---

### Weniger Auswirkungen auf Ihr Tagesgeschäft

Wir sorgen für die Erkennung, Analyse sowie die Reaktion auf die meisten Bedrohungen. Damit Sie in Ruhe arbeiten können.

### Optimierung interner Sicherheitskosten und -Ressourcen

Kreieren Sie Ihrem internen IT-Team die Zeit, sich um die wirklich relevanten Sicherheitsfragen zu kümmern, während UMB den Schutz Ihrer Umgebung übernimmt.

### 7x24 modularer und bedarfsge-rechter Security-Service

Unsere modularen Services erlauben es Ihnen, entsprechend Ihrem Bedarf Ihre Cybersecurity zu optimieren - sowohl technisch wie auch finanziell.

## Option Shadow-IT - Netzscanning ohne Agenten

---

Mittels dieser Option wird in jeweilig verbundenen Netz nach Assets gescannt, auch wenn diese keinen Agenten installiert haben. Damit werden Printers, Server, Storage-Devices und auch Mobile Devices erkannt. Sollten Adminrechte zu diesen bisher unbekanntes Devices vorhanden sein, kann ein Agent installiert werden. Zudem werden Empfehlungen, um das Schutzlevel innerhalb des jeweiligen Netzes zu erhöhen, bereitgestellt.

## Ihre Vorteile

---

- 7 x24 Threat Monitoring
- 7x24 Threat Analyse & Triage
- Konkrete Handlungsempfehlung bei allen eskalierten Incidents
- Forensische Datensammlung und Analyse von betroffenen End Points
- 24x7-Hotline zur Kontaktaufnahme mit dem Cyber Defense Center
- Monatlicher Servicebericht

# Klingt interessant? Kontaktieren Sie uns!

---

Gerne beantworten wir Ihre Fragen zum Thema  
Cybersecurity, EDR und mehr.

### Kontakt

---

Marc Rudin  
Sales Consultant  
marc.rudin@umb.ch  
+41 58 510 18 07  
www.umb.ch