Microsoft XDR as a Service

More than 70% of cyber attacks start on the end device – either through a website or an email.

Security operations are becoming increasingly difficult due to a growing attack surface, a dangerous threat landscape and the rising use of cloud computing. Preventive security measures like anti-virus software are therefore not enough. By contrast, Microsoft XDR as a Service is able to detect anomalies and protect end users as well as IT infrastructure from attacks.

Microsoft XDR as a Service is based on a uniform platform for identifying and responding to security incidents. The data is automatically collected from multiple security components and sources and then analysed. In the event of an attack, security alerts or incidents are created. Security analysts continuously monitor the dashboard to identify false positives or respond to security incidents.

Your advantages with Microsoft XDR as a Service

Everything at a glance

End-to-end visibility of operations, processes, programs, memory, files across all endpoints, identities, apps, emails, data and cloud workloads. ✓

Comprehensive protection

Protection from file-based and file-less malware, ransomware, attacks and zero day exploits. ✓

Extensive analysis

Collection, analysis and correlation of data from various sources and events. ✓

Relief

Automated checks and alert resolutions help to relieve the security operations team. ✓

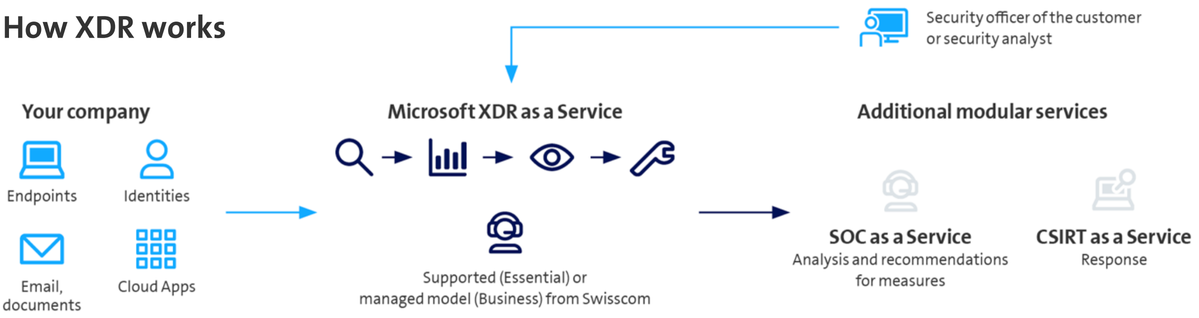
Clear dashboard

The XDR dashboard offers advanced threat hunting and remote remediation capabilities. ✓

Managed service

Swisscom offers the entire Swisscom cyber security portfolio and management, as well as integration into other Swisscom security services. ✓

How XDR works


Security officer of the customer or security analyst
Your company
Endpoints
Identities
Email, documents
Cloud Apps
Microsoft XDR as a Service
Supported (Essential) or managed model (Business) from Swisscom
Additional modular services
SOC as a Service
Analysis and recommendations for measures
CSIRT as a Service
Response

The information in this document does not constitute a binding offer. Subject to changes at any time.

Swisscom (Schweiz) AG Enterprise Customers, Postfach,
CH-3050 Bern, Tel. 0800 800 900, www.swisscom.ch/enterprise

Overview of Microsoft XDR as a Service

Swisscom services	Essential	Business
Project services for onboarding	●	●
Annual Security Policy Assessment	●	●
Tenant management by the customer	–	–
Review and communication of new features and functionalities	–	●
Security policy configuration and agent lifecycle	–	●
Monitoring of operational and health alerts	–	●
Incident management of operational incidents	○	●

XDR components

	Essential	Business
Microsoft Defender for Endpoint (MDE) • Next-Gen Endpoint Protection (EPP) • Endpoint Detection and Response (EDR) • Threat & Vulnerability Monitoring • Attack Surface Reduction • Device Control	–	○
Microsoft Defender for Office (MDO) Protection and monitoring of emails	–	○
Microsoft Defender for Identity (MDI) Protection and monitoring of identities on Active Directory (AD) and AD FS	–	○
Microsoft Defender for Cloud Apps (MDCA) Detects and protects against Shadow IT	–	○

Licences

	Essential	Business
Licences and licence management	–	–

● Standard (included in project price)
○ Optionally available
– Not available

Combinable additional services

Threat Detection & Response – SOC as a Service
With Threat Detection & Response – SOC as a Service, you receive an overview of potential and confirmed security incidents from defined log data in your company via dashboard. Additional analyses with practical action recommendations help you respond to critical security incidents independently.

Threat Detection & Response – CSIRT as a Service
With Threat Detection & Response – CSIRT as a Service, you can call in Swisscom experts to analyse and manage incidents. We carry out the security incident management process remotely or on your premises and support you in documenting evidence and communicating with customers and partners.

Enterprise Workspace, Smart, Connected or Rich Workplace
Enterprise Workspace or Smart, Connected or Rich Workplace: from a smart digital workplace that users can set up themselves without IT, to a holistically managed client workplace, including software distribution, software packeting, asset management and good practice security.

Microsoft 365 Management
Let us handle the management of Microsoft 365 so you can focus on your core business. Management of the customer tenant and the licences are available here.