Microsoft Defender for Identity

What is Microsoft Defender for Identity?

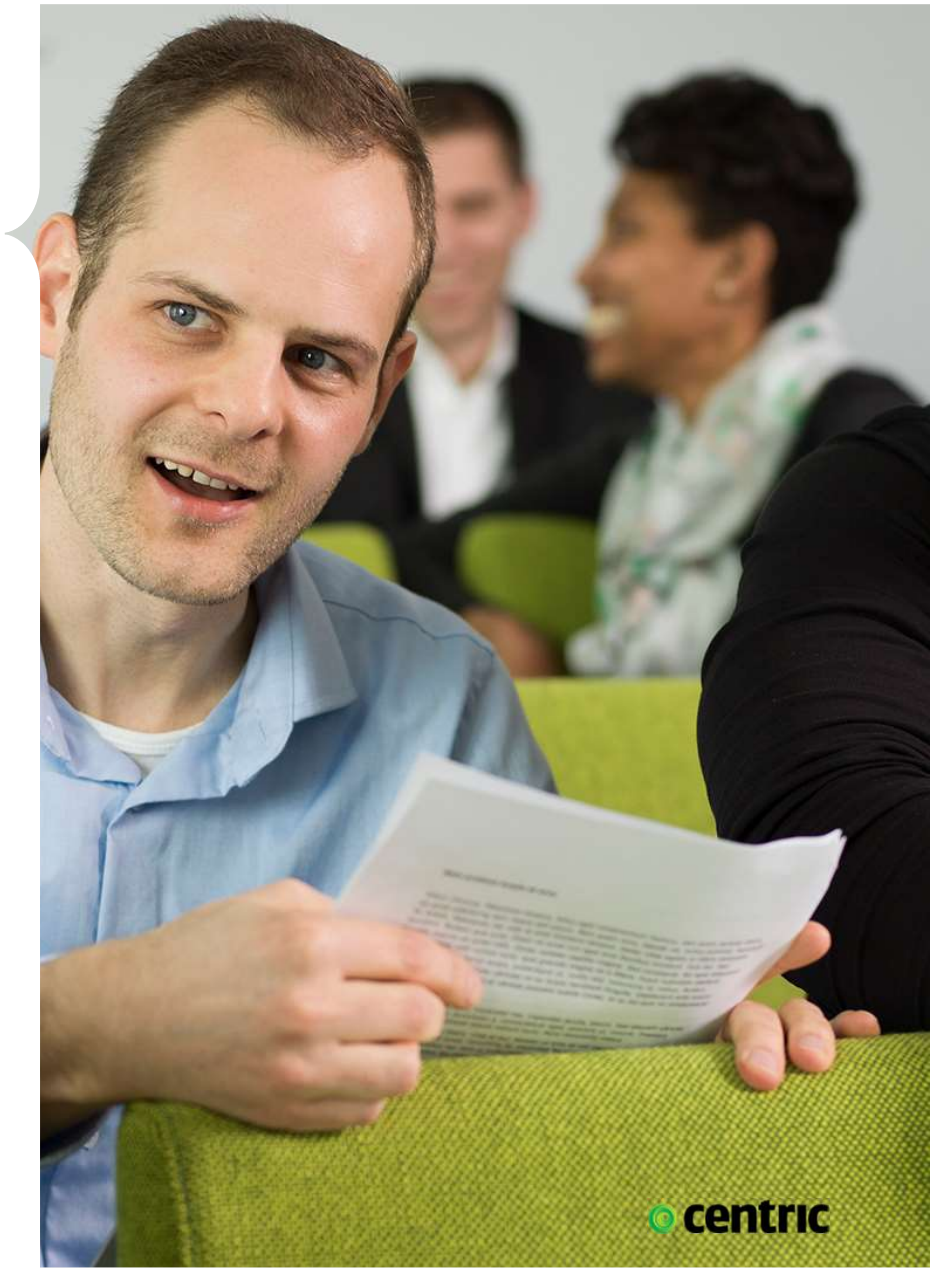
Microsoft Defender for Identity (MDI) is a cloud-based security solution that leverages your on-premises systems to identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions directed at your organization.

Why is Microsoft Defender for Identity important?

MDI Identify suspicious activities and advanced attacks across the cyber-attack kill-chain and provides you invaluable insights on identity configurations and suggested security best-practices.

MDI will help organizations to quickly identify security threats like:

- (Attempts to) compromised user or admin credentials;
- Unsecure or weak network or system configurations;
- Unsecure authentications & authorizations of any account.



The 4-day Microsoft check-up and deployment approach

1

Discover & Design

Analysis Identity environment | Design workshop Microsoft Defender for Identity | Design

2

Configure and Deploy

Configuration of Microsoft Defender for Identity | Deployment of Identity sensors

3

Assess, maintain & handover

Asses | Evaluate discovered threats | Protect Identities

centric

Microsoft check-up and deployment approach

1

Discover & Design

Insight into your identity environment and the possibilities based on an EMS E5 or M365 E5 license.

Based on an interview, we will make a proposal for the implementation of Defender for Identity and the required event & information collection.

2

Configure and Deploy

The previous phase is translated into a technical implementation.

The security signals of the on-premises systems will be forwarded to the Microsoft portals.

Sensors will be installed so events and security signals are collected; This is done together with the security administrators of the internal organization.

3

Assess, Maintain & Handover

After the implementation, the data collected by the sensors will be evaluated with the customer.

Threats which are identified will be addressed and can be managed.

Incidents and alerts will be identified and can be managed and investigated.

centric


centric
connect.engage.succeed.