Microsoft Defender for Office 365 deployment

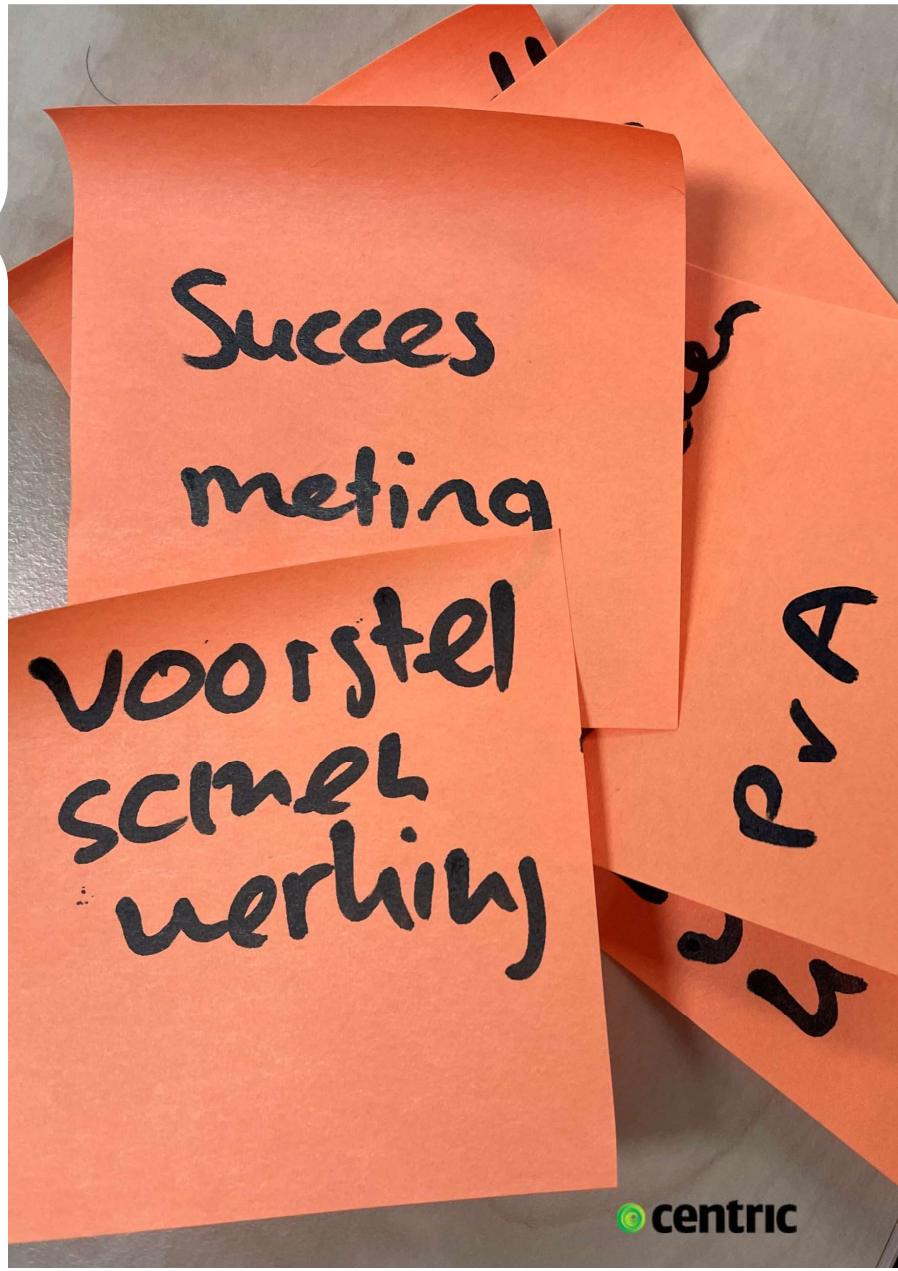
What is Microsoft Defender for Office 365?

Microsoft Defender for Office 365 is a cloud-based email filtering service that helps protect your organization against advanced threats to email and collaboration tools, like phishing, business email compromise, and malware attacks. It enhances the standard scanning process and extends protection beyond Exchange Online, with features such as Safe Links, Safe Attachments, Mailbox Intelligence, and Attack Simulator.

Why is Microsoft Defender for Office 365 important?

Microsoft Defender for Office 365 enhances security in different phases of cybersecurity:

- **More insights (Identify)** where the email is coming from by understanding the source;
- Better **Protection** by providing additional policies that further enhance the protective capabilities provided by built-in security solutions like Exchange Online Protection;
- Faster **Detection** and **Response** with features like Automated Investigation & Response capabilities, as well as the integration with Microsoft 365 Defender for advanced hunting, etc.



The 4-day Microsoft check-up and deployment approach

1

Discover & Design

Analysis Endpoint environment | Design workshop Microsoft Defender for Office 365 | Design

2

Configure and Deploy

Configuration of Microsoft Defender for Office 365 | Deployment to a group of users

3

Assess and Evaluate

Asses | Evaluate policies | Learn to use the extra features

centric

Microsoft check-up and deployment approach

1

Discover & Design

Protection against advanced attacks across email and collaboration tools based on an E3 or E5 license.

Based on an interview, we will make a proposal for the implementation of Defender for Office 365.

2

Configure and Deploy

Your environment can make use of Defender for Office 365. The previous phase is translated into a technical implementation.

Policies will be enrolled into the environment of the customer. This is done together with the security administrators of the internal organization.

3

Assess and Evaluate

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

Detected malicious and suspicious content will be addressed and can be managed.

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

centric


centric
connect.engage.succeed.