skaylink
Cyber Defense

Security starts here.

it-sa 2024

Let’s go! Dein AI Security Boost startet hier

Skaylink Cyber Defense Team

Oktober 2024

skaylink Cyber Defense

Christian Müller

Cyber Defense Lead
Principal Security Consultant

Seit 10 Jahren beschäftige ich mich bei Skaylink mit dem Thema Microsoft Security. Erst mit Fokus auf AD-Security (Mimikatz lässt grüßen), später erweitert um die Workloads in der Cloud.

Jan Fahrenbach

Cloud Security Architect
FastTrack Consultant

Im architektonischen Design orientiere ich mich stark am Zero Trust Security Framework, welches Ihnen bei der technischen Implementierung skalierbare Vorteile entlang der kompletten Unternehmensstruktur bringt.

skaylink
Cyber Defense

Get started with AI security

1

Manage overprivileged and risky users

Microsoft Entra ID

2

Mitigate Device Risk

Microsoft Intune / Defender for Endpoint

3

Prevent over-exposure of data

Microsoft Purview Information Protection

4

Discover and control the use of AI apps

Microsoft Defender for Cloud Apps

Govern access to Copilot and other Applications
Microsoft Entra ID

1 **Manage overprivileged and risky users**
with Identity and access management

Microsoft Entra ID

2 **Mitigate Device Risk**
with Endpoint management

Microsoft Intune

✓ Login to Microsoft 365 with a single & managed corporate identity.

✓ Evaluate login attempts based on the user or group membership, IP location, device state, application, risk detection.

✓ Decide access level with Conditional Access policies.

- Allow access
- Require MFA
- Limit access
- Password reset
- Monitor access

✓ Monitor critical events and issue access tokens that can be revoked immediately.

Manage device real-estate
Microsoft Intune

1 Manage overprivileged and risky users

with Identity and access management

Microsoft Entra ID

2 **Mitigate Device Risk**

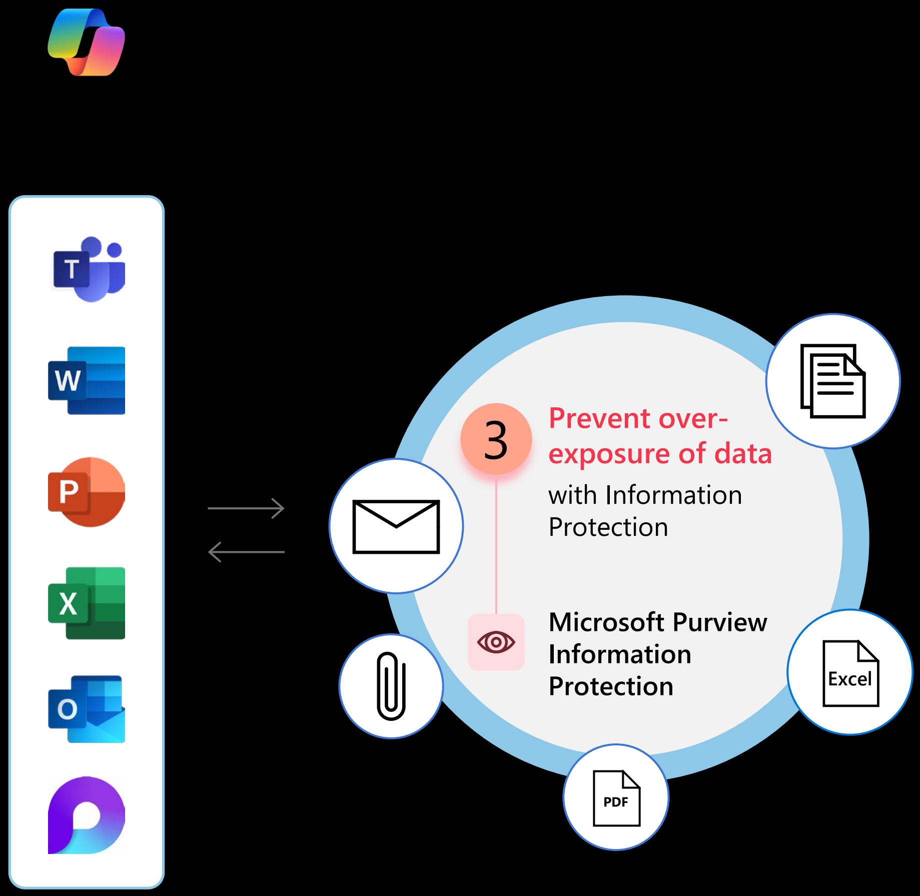
with Endpoint management

Microsoft Intune

- ✓ Ensure the Microsoft 365 apps are securely installed on the user’s device and kept up to date.
- ✓ Limit the use of work apps, including Copilot, on personal devices
- ✓ Implement App protection policies to limit the actions users can take on devices:
  - Save generated files to unsecured apps
  - Restrict copying and pasting to non-work apps
- ✓ Wipe all work content if the device is lost or disassociated with the company or the user.

Protect business information and restrict actions
Microsoft Purview Information Protection

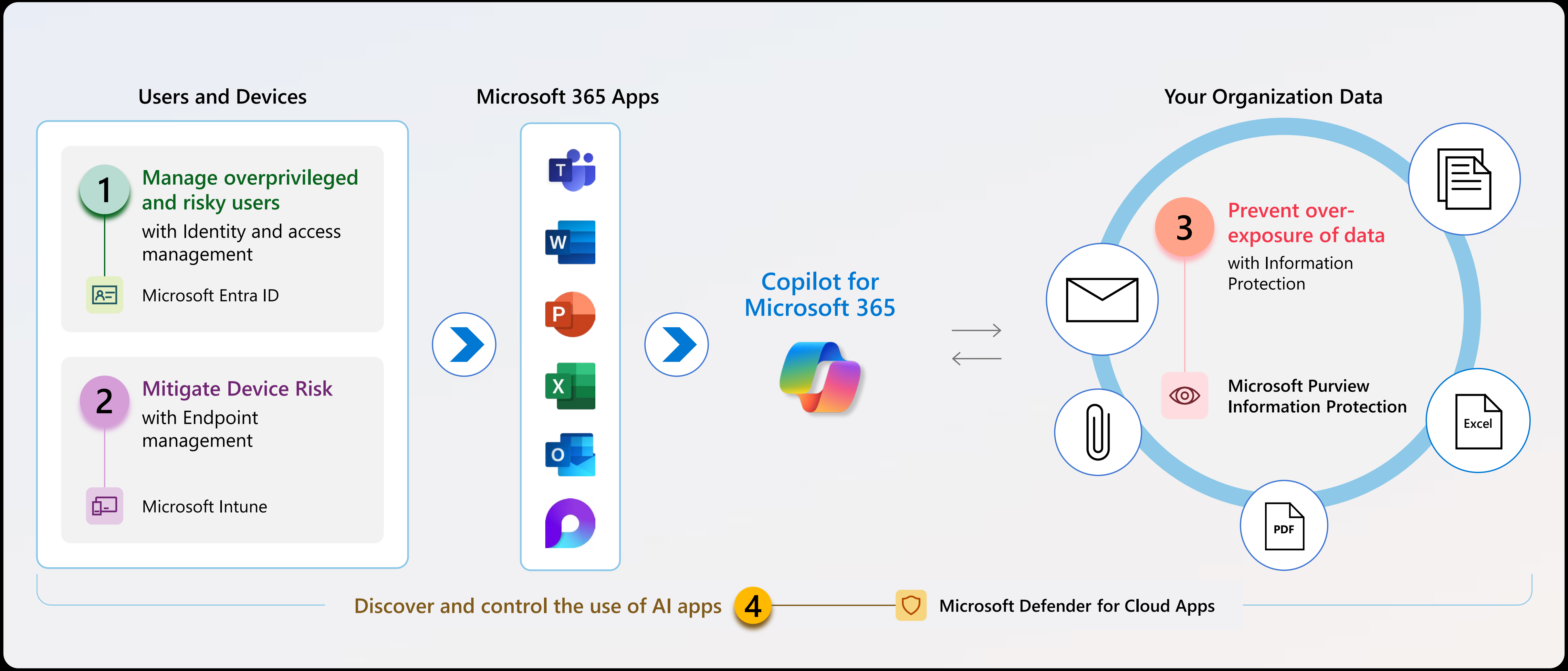
- ✓ Data consumption and processing with Copilot is limited to the user's permissions.
- ✓ Copilot inherits sensitive documents' sensitivity labels and applies them to its output and references.
- ✓ If Copilot generates sensitive data and saves it in Microsoft 365, Data Loss Prevention policies will apply.
- ✓ Interactions with Copilot are logged for auditing purposes and business, or code of conduct violations can be detected.



3 **Prevent over-exposure of data** with Information Protection

Microsoft Purview Information Protection

Security and compliance controls for Copilot for Microsoft 365



Users and Devices

1 Manage overprivileged and risky users with Identity and access management

Microsoft Entra ID

2 Mitigate Device Risk with Endpoint management

Microsoft Intune

Microsoft 365 Apps

Copilot for Microsoft 365

Your Organization Data

3 Prevent over-exposure of data with Information Protection

Microsoft Purview Information Protection

Discover and control the use of AI apps 4

Microsoft Defender for Cloud Apps

Copilot for Microsoft 365
inherits your security, compliance, and privacy policies

1

Manage overprivileged and risky users

Microsoft Entra ID

2

Mitigate Device Risk

Microsoft Intune / MS Defender for EndPoint

3

Prevent over-exposure of data

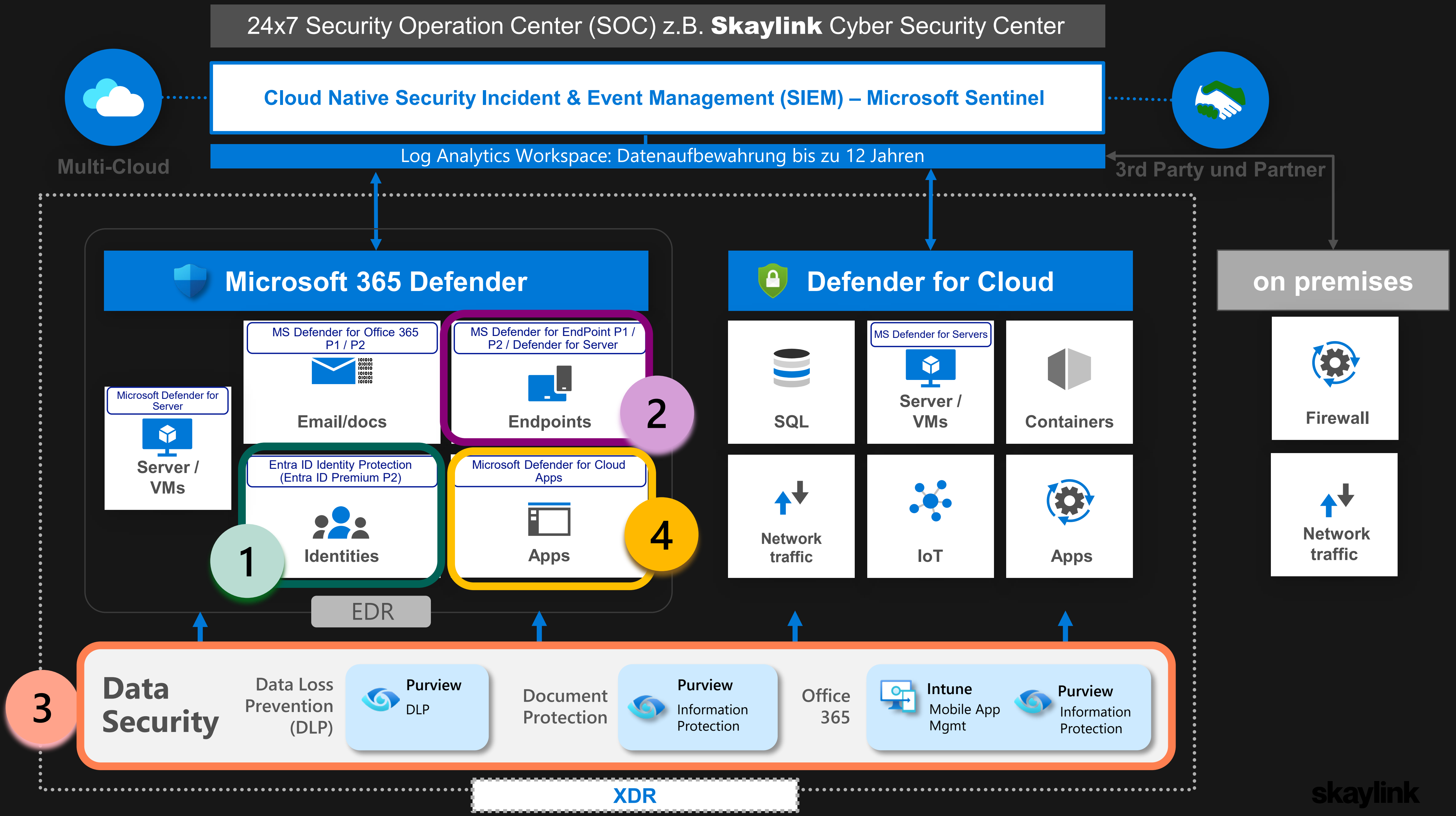
Microsoft Purview Information Protection

4

Discover and control the use of AI apps

Microsoft Defender for Cloud Apps

Skaylink XDR Security Architecture



24x7 Security Operation Center (SOC) z.B. **Skaylink** Cyber Security Center

Cloud Native Security Incident & Event Management (SIEM) – Microsoft Sentinel

Log Analytics Workspace: Datenaufbewahrung bis zu 12 Jahren

Multi-Cloud

3rd Party und Partner

Microsoft 365 Defender

Microsoft Defender for Server

Server / VMs

MS Defender for Office 365 P1 / P2

Email/docs

MS Defender for EndPoint P1 / P2 / Defender for Server

Endpoints

2

Entra ID Identity Protection (Entra ID Premium P2)

Identities

1

Microsoft Defender for Cloud Apps

Apps

4

EDR

Defender for Cloud

SQL

MS Defender for Servers

Server / VMs

Containers

Network traffic

IoT

Apps

on premises

Firewall

Network traffic

3

Data Security

Data Loss Prevention (DLP)

Purview DLP

Document Protection

Purview Information Protection

Office 365

Intune Mobile App Mgmt

Purview Information Protection

XDR

Slides + Follow Up

Thank you very much!

Visit us at hall 6 / booth 6-236

skaylink
Cyber Defense

skaylink

Cyber Defense

Security starts here.

skaylink
Cyber Defense

Security starts here.

it-sa 2024

Let’s go! Dein Security Boost startet hier

Skaylink Cyber Defense Team

Oktober 2024

skaylink Cyber Defense

Christian Müller

Cyber Defense Lead
Principal Security Consultant

Seit 10 Jahren beschäftige ich mich bei Skaylink mit dem Thema Microsoft Security. Erst mit Fokus auf AD-Security (Mimikatz lässt grüßen), später erweitert um die Workloads in der Cloud.

Jan Fahrenbach

Cloud Security Architect
FastTrack Consultant

Im architektonischen Design orientiere ich mich stark am Zero Trust Security Framework, welches Ihnen bei der technischen Implementierung skalierbare Vorteile entlang der kompletten Unternehmensstruktur bringt.

skaylink
Cyber Defense

Low hanging fruits in Microsoft environments are everywhere!

1

Start with best practices known for years

Active Directory

2

Secure identities in the cloud

Entra ID

3

Know your devices and ensure security baselines

Microsoft Intune

4

Centralized security-related signals

Defender XDR / Sentinel