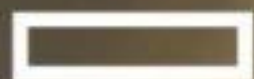


15. BECHTLE IT-FORUM THÜRINGEN

BECHTLE

2024

15. Mai 2024 • STEIGERWALD Stadion ^{Erfurt}



Hewlett Packard
Enterprise



HUAWEI

intel.

Nur gehärtet ist sexy!

Safety First mit M365





Laura Korn

Junior System Engineer

Fachkraft für Datenschutz und -sicherheit (IHK)

M365 Einführung, Compliance, Produktivität



Steffen Höfling

Senior System Engineer

Defender, Intune, Microsoft Security Expert



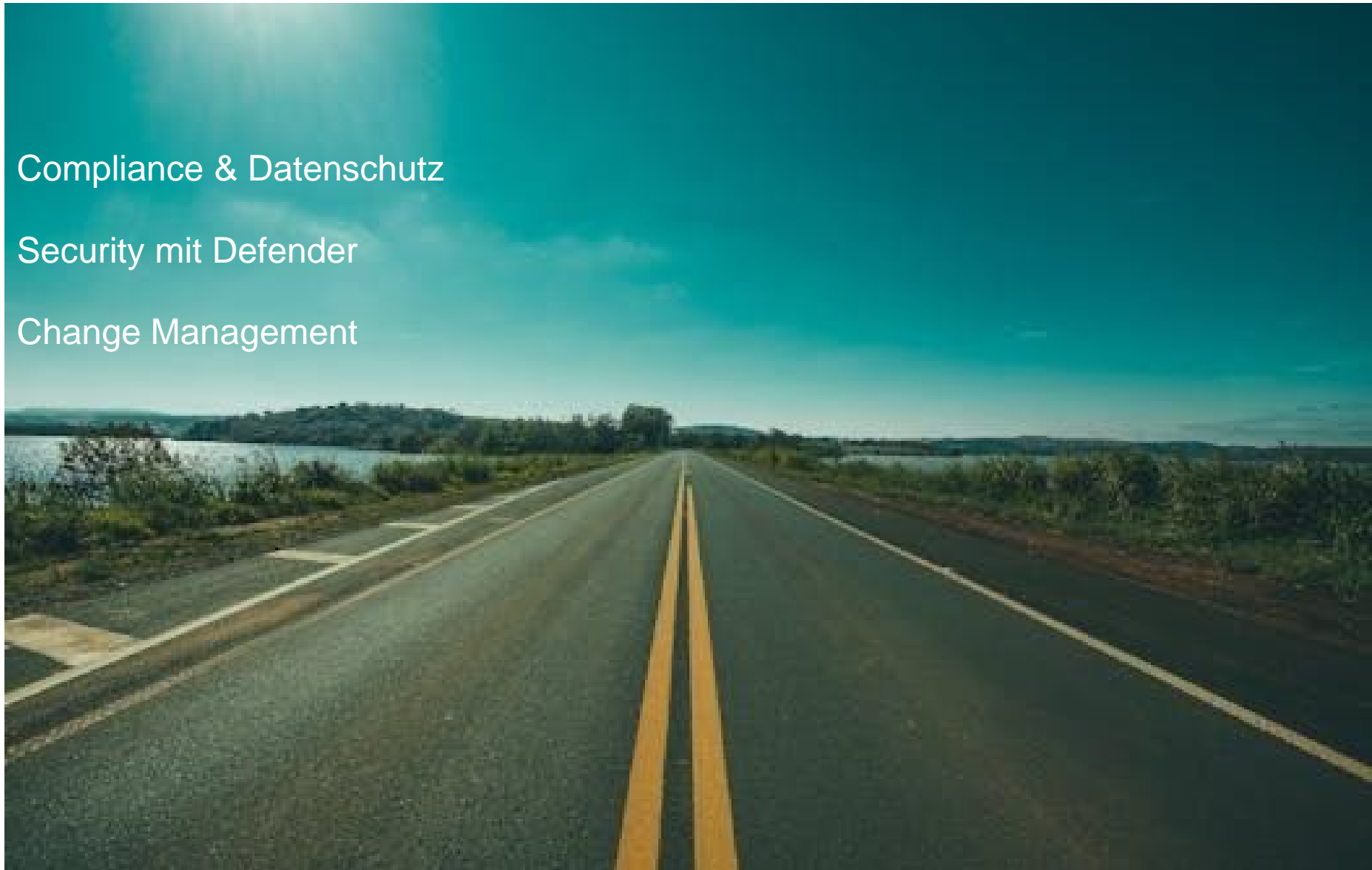


Agenda.

Compliance & Datenschutz

Security mit Defender

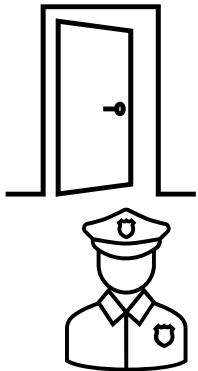
Change Management



Security & Compliance.

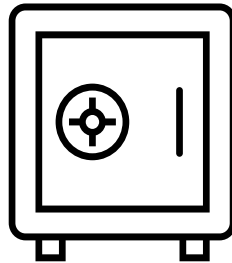
Identitäts- und Zugriffsverwaltung

- Modern Auth
- MFA
- Conditional Access



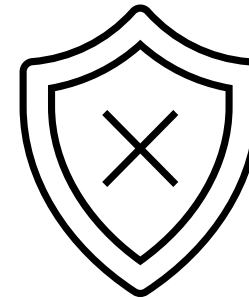
Datensicherheit

- Verschlüsselung
- Aufbewahrung & Archivierung, DLP



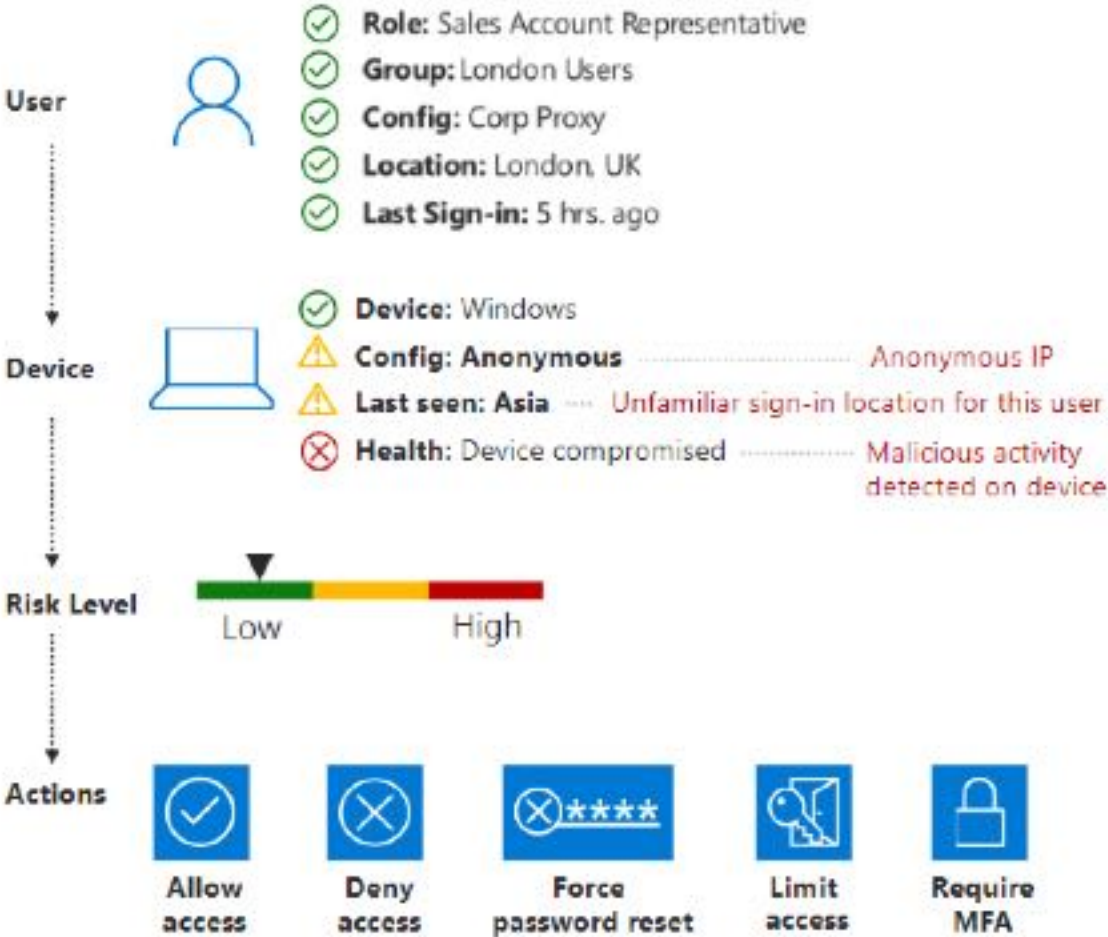
Bedrohungsmanagement

- Erkennung und Abwehr von Malware, Phishing, etc.

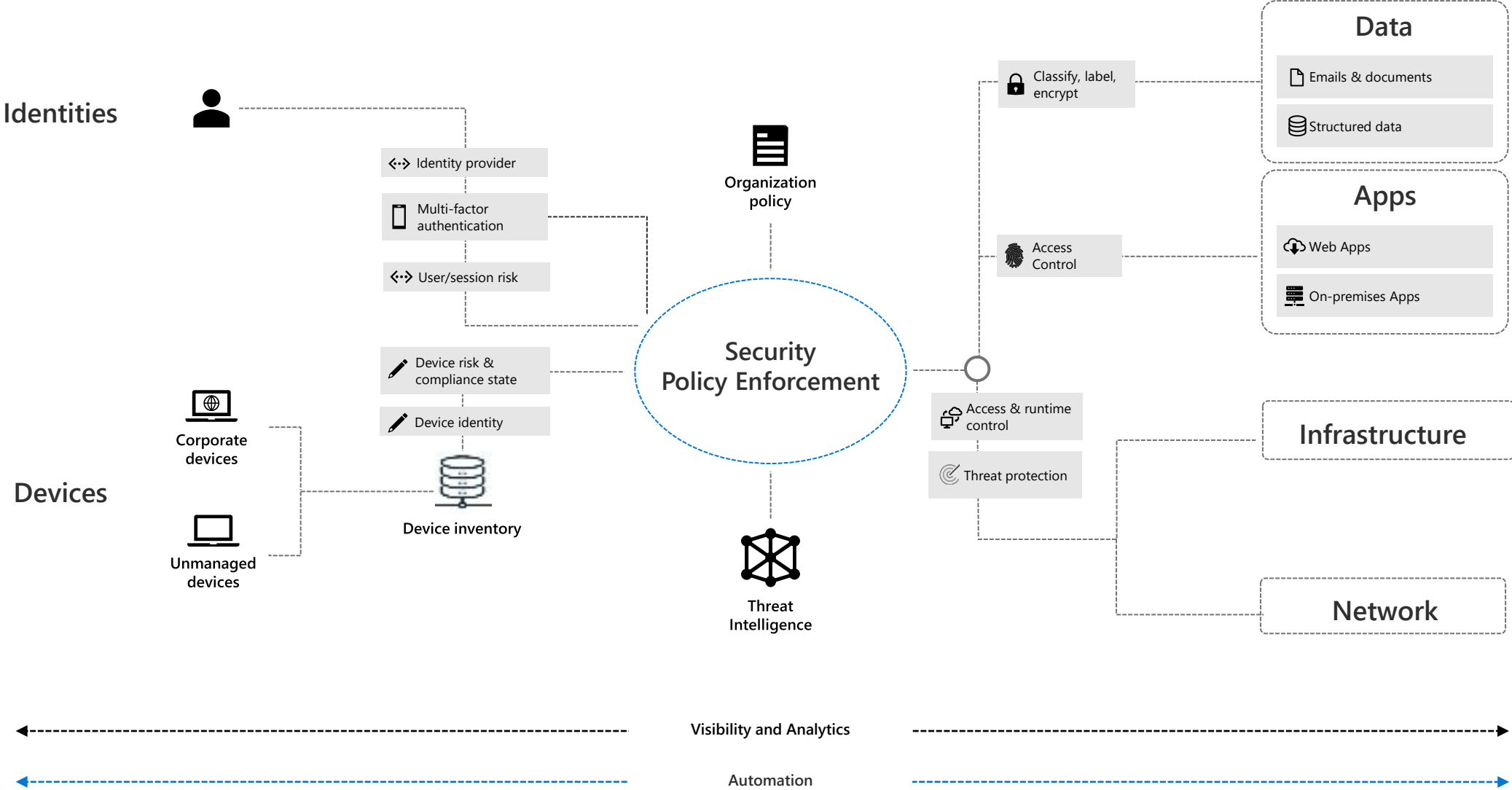


Alle Admin-Center müssen bearbeitet werden!

Conditional Access



Zero Trust



Compliance & Datenschutz

Compliance Manager

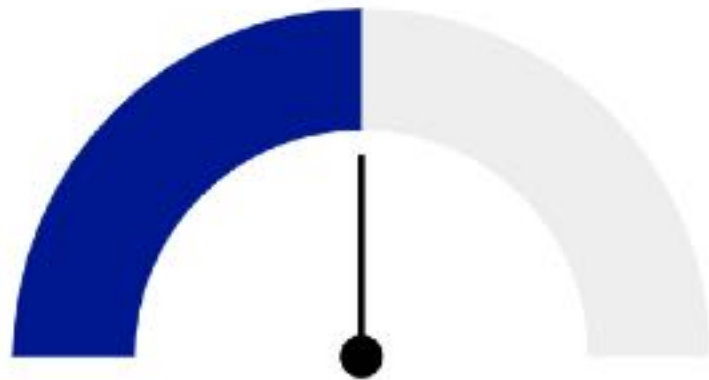


Overview Improvement actions Solutions Assessments Regulations Alerts Alert policies

Compliance Manager measures your progress in completing actions that help reduce risks around data protection and regulatory stand:
[guidance and documentation](#)

Overall compliance score

Your compliance score: 50%



9855/19453 points achieved

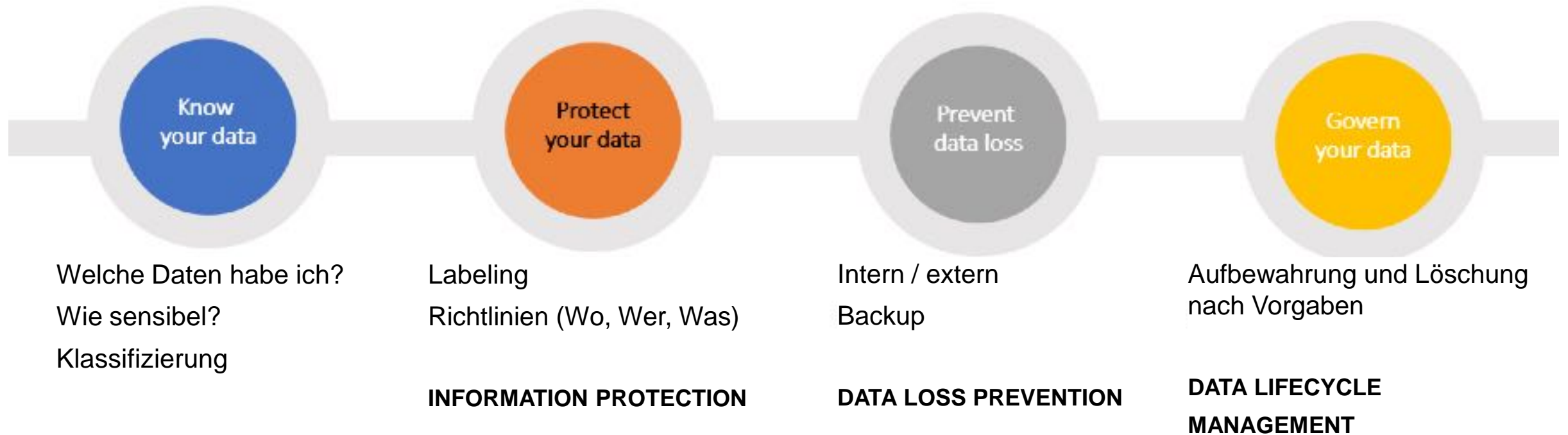
■ Your points achieved ⓘ

Key improvement actions

Not completed **489** | Completed **0** | Out of scope **0**

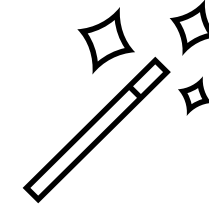
Improvement action	Impact	Test status	Group
Use boundary protection to limit access t...	+27 points	• None	Default Group
Configure VPN integration	+27 points	• None	Default Group
Digitally encrypt secure channel data	+27 points	• None	Default Group
Automate notifications and configure act...	+27 points	• None	Default Group
Block outdated ActiveX controls	+27 points	• None	Default Group
Change your computer account passwor...	+27 points	• None	Default Group

Lösungen



Information Protection

- Labels und Richtlinien
- Verschlüsselung
- Cloud und OnPrem, PDFs



- Wer darf was sehen?
- Dürfen User Labels ändern?
- User Hilfestellungen einbinden
- End-2-End-Verschlüsselung

<input type="checkbox"/>	Personal
<input type="checkbox"/>	Public
<input type="checkbox"/> >	General
<input type="checkbox"/> >	Confidential
<input type="checkbox"/> >	Highly Confidential
<input type="checkbox"/>	Confidential - Finance



Data Loss Prevention – Keep your secrets!

- Templates und Richtlinien
- Sensibilisierung der User



U.S. Financial Data

General Data Protection Regulation (GDPR)

Default policy for Teams

Default policy for devices

- User, der teilen will bekommt Info und Tipps
- User bekommt Inhalt nicht angezeigt
- Admin wird informiert

Content contains any of these sensitive info types: EU-Debitkartennummer, EU Driver's License Number, EU National Identification Number, EU Passport Number, EU Social Security Number (SSN) or Equivalent ID, EU Tax Identification Number (TIN)

Data Lifecycle Management

- Aufbewahrungsrichtlinien

Private

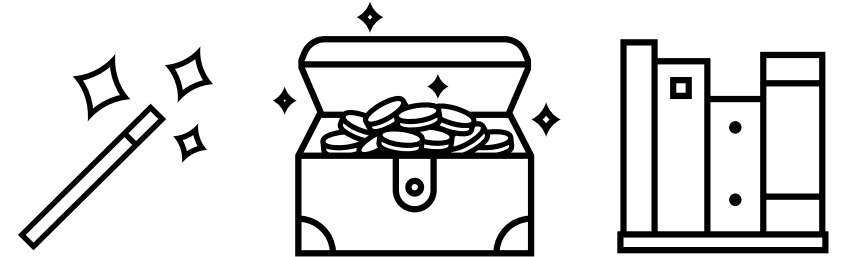
PII Retention Policy

Employee Records

Personal Financial PII

Medical Records Retention Policy

Product Retired



- Wann wird gelöscht?
- Wie ist die Archivierung geregelt?

Security mit Defender XDR

Components of Defender XDR



Microsoft Defender

XDR – Extended Detection and Response Suite

Microsoft 365 Defender

- Microsoft Defender for Identity
- Microsoft Defender for Office 365
- Microsoft Defender for Endpoints
- Microsoft Cloud App Security

Azure Defender

- Azure Defender for servers
- Azure Defender for App Service
- Azure Defender for Storage
- Azure Defender for SQL
- Azure Defender for Kubernetes
- Azure Defender for Resource Manager
- Azure Defender for IoT

Microsoft Defender for Office 365

- Antiphishing
- Antispam
- Sichere Anlagen
- Sichere Links
- Sichere Dokumente
- Schutz für Sharepoint, OneDrive und MS Teams
- Echtzeiterkennungen
- Angriffssimulationstraining



Microsoft Defender for Endpoint

- Automatische Erkennung und Abwehr von Bedrohungen
- Sicherheitsrichtlinienmanagement
- Forensische Untersuchung von Sicherheitsvorfällen
- Plattformübergreifende Unterstützung



Microsoft Defender for Identity

- Risikobasierter Zugriff
- Bedrohungsanalyse
- Passwortüberwachung



Microsoft Defender for Cloud Apps

- Integration mit Microsoft-Tools
- Erkennung und Abwehr von Angriffen
- Compliance-Unterstützung
- Multi-Cloud-Unterstützung



Change Management

