



Der neue Kollege

DIE BESETZUNG

Drei Figuren, eine Geschichte



SABINE · Vertrieb
Will Tempo, kein Risiko.



COPI · Der Neue
Liest alles. Fragt nie.



ROBIN · Angreifer
Will nur Ihre Daten.

Wer nutzt Copilot im Unternehmen?

**Copilot sicher nutzen:
Best practices für den Unternehmenseinsatz**
Continuum x FREICON – 25. Heimspiel

Thomas Schuster
Business Development Manager Microsoft Security @ Arrow ECS



The background of the slide is a vibrant, stylized illustration of a modern office. On the left, a massive, towering stack of papers and documents dominates the foreground, with several papers floating in the air around it, some glowing with blue light. In the center, a small, white and blue robot with a friendly face and glowing eyes is gesturing towards the papers. To the right, a woman with long brown hair, wearing a blue blazer over a white top, stands with one hand on her hip and the other holding a blue mug, looking at the robot with a smile. The office has large windows in the background showing a city skyline with skyscrapers under a blue sky. The overall atmosphere is one of productivity and technological advancement.

KAPITEL 1

Ein Neuer fängt an

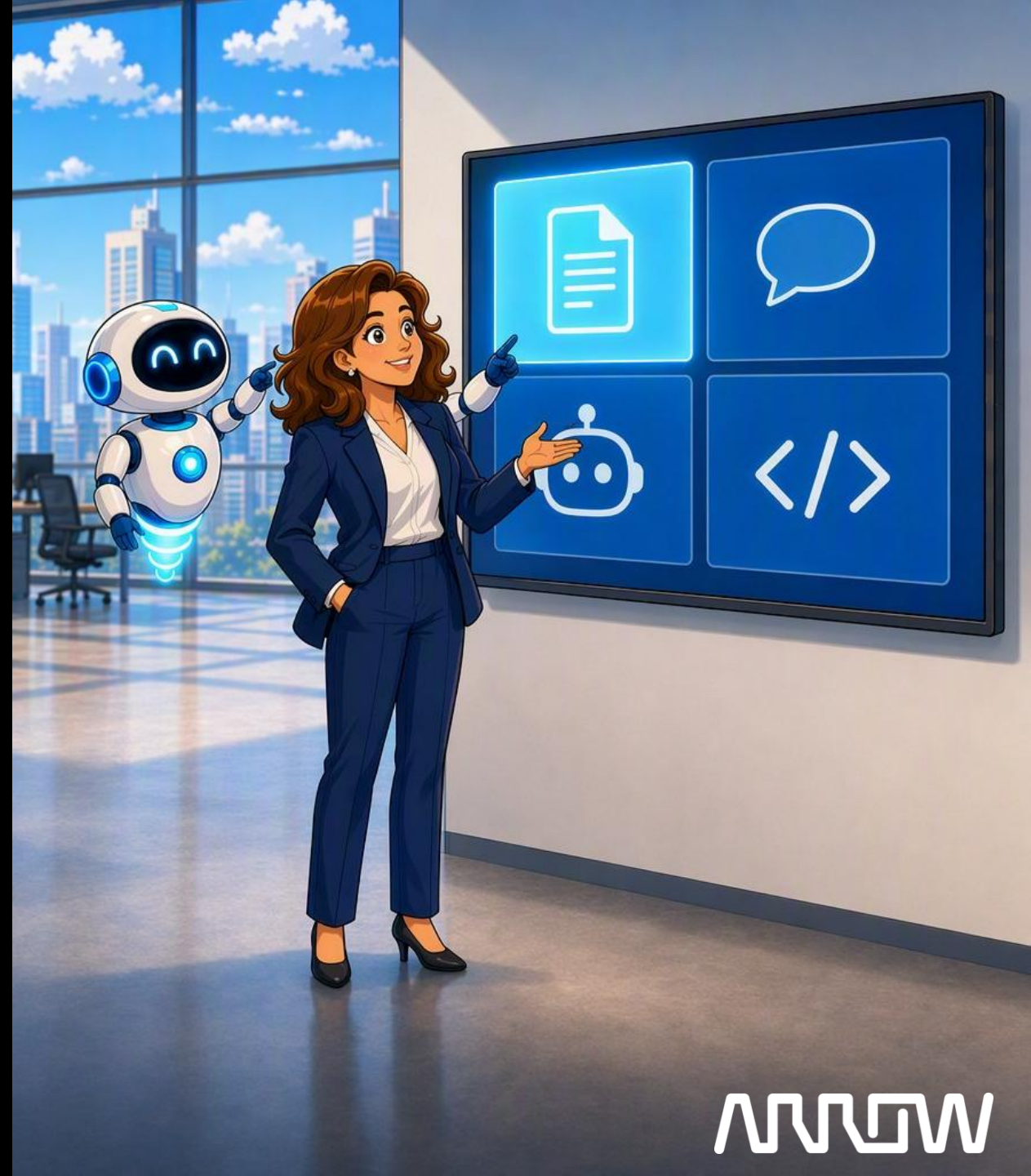
Er liest in einer Minute, wofür ein Mensch zwei Wochen braucht. Er heißt Copi.

DIE LANDKARTE

Vier Produkte, ein Name

M365 COPILOT · In Word, Excel, Outlook, Teams
COPILOT CHAT · In M365 enthalten, ohne Firmendateien
COPILOT STUDIO · Eigene Agenten, nach der Einführung
GITHUB COPILOT · Entwicklung

Vier Produkte. Eine Frage: welcher?



Hallo, wie kann ich helfen?

+ Nachricht an Copilot senden



Vorgeschlagen

Dateieinblicke

Posteingangstriage

Personensuche



FLEX ROUTING

Wenn die Rechenlast ausweicht

Bei Spitzenlast: Verarbeitung in USA, Kanada oder Australien.
Gespeicherte Inhalte bleiben in der EU-Datengrenze.
Verschlüsselte Übertragung zur Verarbeitung
Abschaltbar im Microsoft 365 Admin Center.

Bitte prüfen, ob aktiv!

Die Berechnung darf ausweichen,
Ihre gespeicherten Inhalte nicht.



DER GEWINN

Was der Neue wirklich bringt

30 Minuten weniger E-Mail-Zeit pro Woche und Kopf.

12 % schneller fertig bei Dokumenten.

66 % haben mehr Zeit für wertvolle Arbeit.

Nur 40 % nutzen ihn regelmäßig.

Microsoft Research: Early Impacts of M365 Copilot · Work
Trend Index 2026



DAS PROBLEM

**Längst da, nur eingestellt
hat ihn keiner**

42 % Der Unternehmen vermuten private KI-Nutzung.
23 % haben Regeln für die Nutzung von KI
20 % hatten schon eine Panne mit KI.

Bitkom 2025 · IBM/Ponemon 2025 · Europäische Kommission

An illustration of a woman with brown hair, wearing a dark blue blazer over a grey top, standing in a cluttered office. She has a thoughtful expression, with her hand to her chin. To her left is a small, white, rounded robot with blue eyes and a blue antenna. The robot is emitting a bright blue beam of light that passes through a large, disorganized pile of papers and folders. The office is filled with stacks of papers, folders, and a desk lamp. A window in the background shows a city skyline under a blue sky with clouds.

KAPITEL 2

Der Aktschrank

Copi ist nicht das Problem. Zwanzig Jahre ungeordnete Ablage sind es.

SENSIBLE DATEN

Wertvoll, aber nicht zu erkennen

Personaldata, Verträge, Preise, Entwürfe.
Ohne Bezeichnung sieht jede Datei gleich aus.
Purview zeigt, was noch nie geprüft wurde.

Unerkannt heißt ungeschützt.

**Copi kann keinen Unterschied machen, den
vorher niemand gemacht hat.**



OVERSHARING

Einmal geteilt, für immer offen

Links für „jeder in der Organisation“.
Copi nutzt genau die Rechte, die da sind.
Die Datenrisikobewertung zeigt es auf.

KI verstärkt das Problem.

**Microsoft sagt es selbst:
KI verstärkt übermäßiges Teilen.**

Microsoft Learn: Datensicherheitsstatus-Management für KI



KI-DATENABFLUSS

Wenn Daten in fremde KI wandern

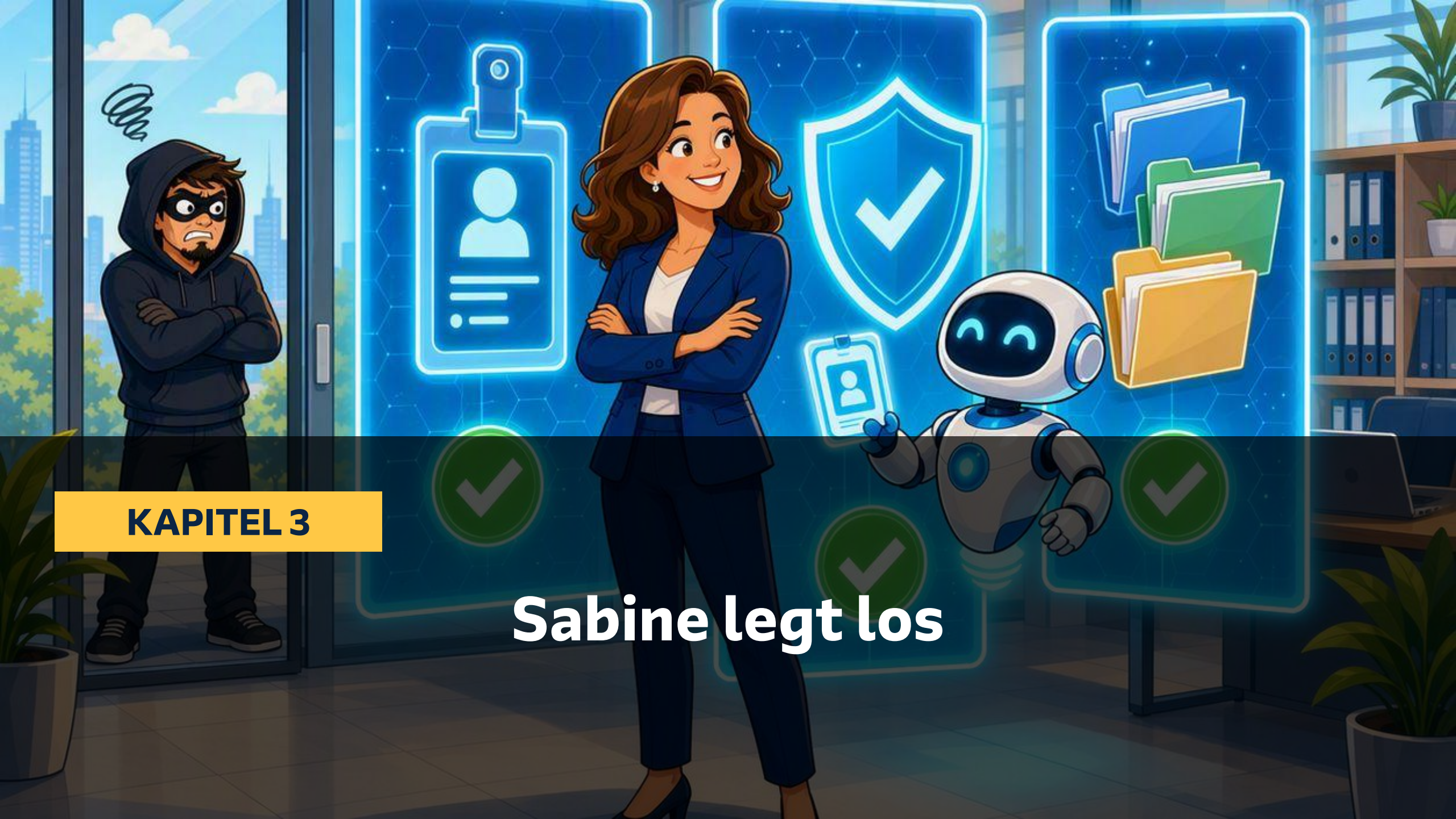
Vertrauliches wandert in fremde KI-Seiten.
Im Browser, in Apps, über Schnittstellen.
Purview erkennt es, auch in Copilot.

20 % hatten schon eine Panne.

Der Abfluss passiert im Browser, nicht im Rechenzentrum.

Microsoft Learn: DSPM für KI · IBM/Ponemon 2025





KAPITEL 3

Sabine legt los

DREI SÄULEN

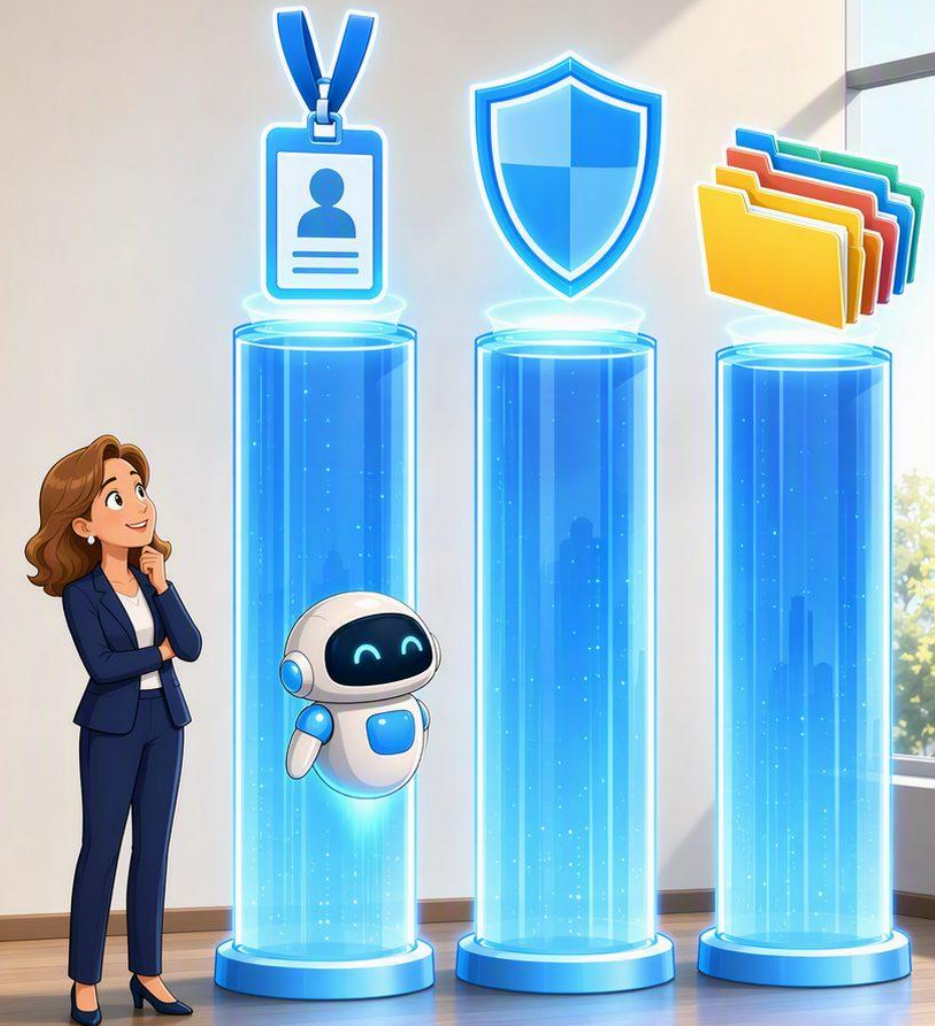
Ausweis, Werkschutz, Aktenordnung

ENTRA · Wer darf überhaupt herein?

DEFENDER · Was, wenn doch jemand reinkommt?

PURVIEW · Was darf mitgenommen werden?

Drei Fragen, drei Werkzeuge.



Drei Säulen, ein Fundament

Microsoft Entra
Identität & Zugriff

Microsoft Defender
Bedrohungen erkennen & stoppen

Microsoft Purview
Daten schützen & steuern

Serverschutz: Defender for Servers, for Endpoint Server, for Business Servers

Sentinel: SIEM & zentrale Überwachung **Intune:** Geräte & Applikationen verwalten

SCHATTEN-KI

Sichtbar machen, was schon läuft

Welche KI-Dienste nutzen Ihre Leute wirklich? Jeder Dienst bekommt eine Risikobewertung. Uploads vertraulicher Dateien gezielt stoppen.

Nicht verbieten. Anbieten.

Wer keine sichere KI nutzt, bekommt eine unsichere im Browser nebenan.

Microsoft Defender for Cloud Apps



PURVIEW

Microsoft Purview, die Aktenordnung

Die Frage: Was darf gesehen, kopiert und mitgenommen werden?

Was folgt:
Bezeichnungen für Dateien und Schutz vor Datenabfluss

Hier entscheidet sich alles für Copi.

**Copi hält sich an jede Regel,
wenn es eine gibt.**



DIE ORDNUNG

Jede Akte bekommt einen Stempel

Vier Stufen genügen zum Start.
Der Stempel bleibt an der Datei, auch beim Kopieren.
Copi sieht ihn und hält sich daran.

Vier Stempel reichen zum Start.

**Was einen Stempel hat, lässt sich schützen.
Was keinen hat, nicht.**

Microsoft Purview – Sensitivity Labels



DIE PFORTE

Kontrolle beim Hinausgehen

Kontonummern und Kundenlisten werden erkannt.
Greift in E-Mail, Teams und in KI-Eingaben.
Start beobachtend: volle Sicht, keine Störung.

Hinweis statt Rüge.

Microsoft Purview - DLP



KEY ASSETS

Welche Kronjuwelen betroffen sind

Ordner mit Personal- und Finanzdaten.
Postfächer und Ablagen der Führung.
Adminkonten, Notfallzugänge, KI-Agenten.

Drei Bereiche, nicht alles.



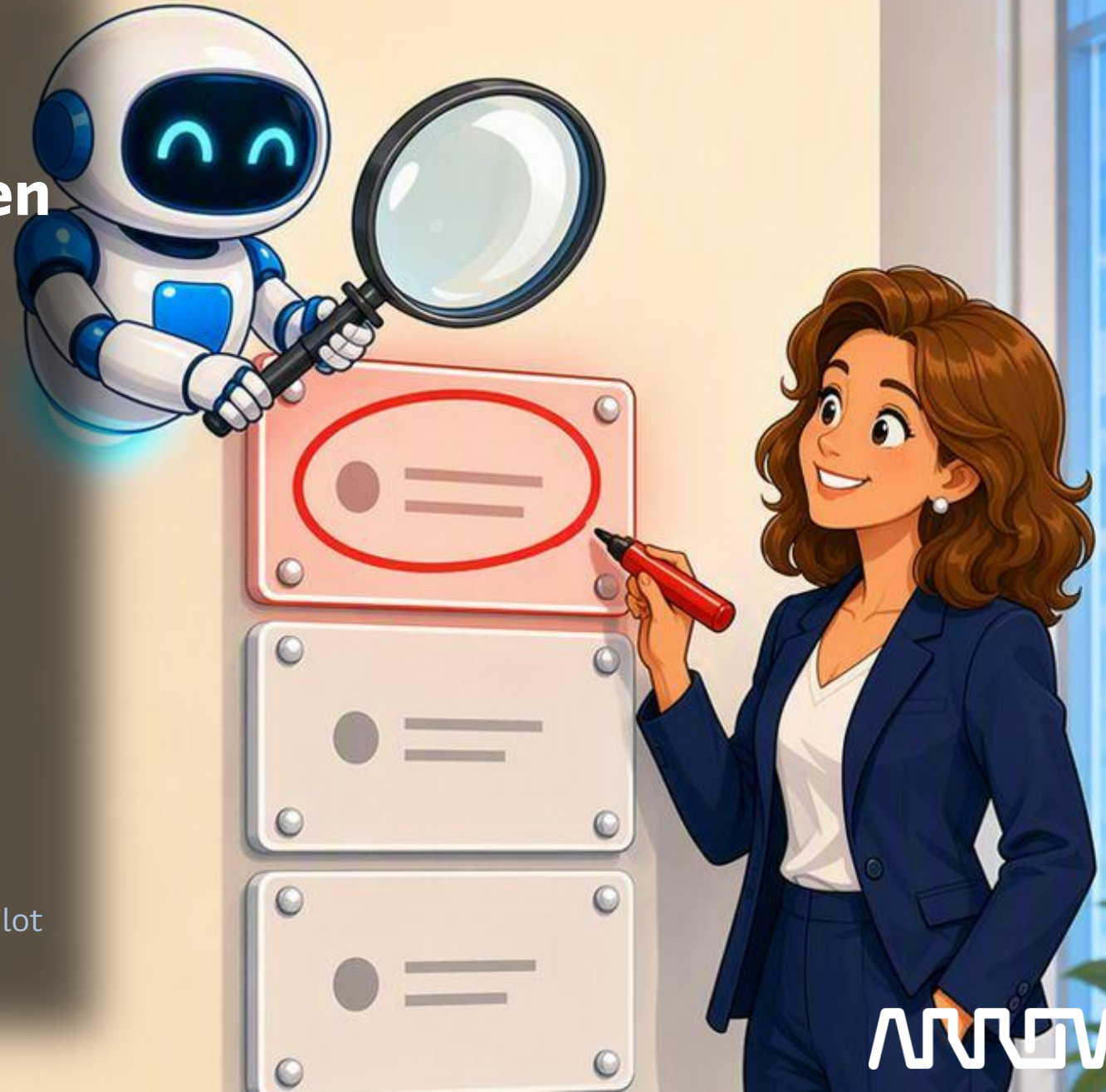
WAS ZUERST?

Womit wir anfangen sollten

1. Zu breit geteilte Inhalte einsammeln.
2. Dauerhafte Adminrechte abschaffen.
3. Bezeichnungen und Ausgangskontrolle.

Übermäßiges Teilen zuerst.

Microsoft Learn: Sichere Grundlage für Microsoft Copilot





KAPITEL 4

Adoption

Was man für eine sinnhafte Nutzung umsetzen muss.

DER BAUPLAN

Vier Kapitel, in dieser Reihenfolge

1. GOVERNANCE: Rechte, Sensivity Labels, DLP.
2. IMPLEMENTATION: Use Cases, Lizenzen, Pilot.
3. ADOPTION: Schulung, Champions, Wave-Rollout.
4. SUPPORT: Betrieb, Monitoring, Update-Zyklus.

Governance first.



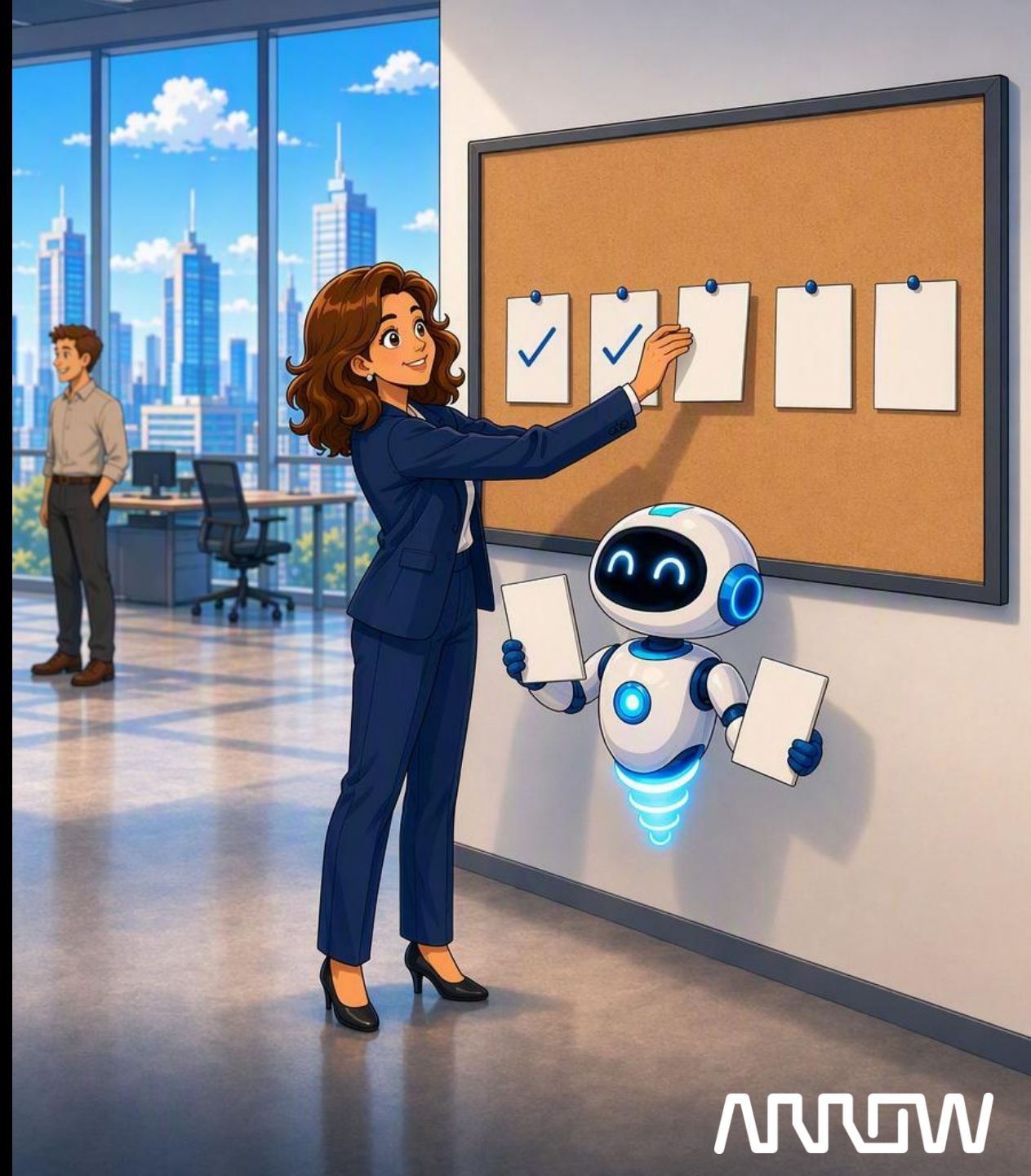
DAS PLAYBOOK

Fünf Hebel für echte Nutzung

1. Pilot-Phase mit Telemetrie, messen statt hoffen.
2. Champions statt Zwang.
3. Schulung der Enduser an eigenen Use Cases.
4. Change & Communication, Erfolge sichtbar machen.
5. Wave-Rollout, nicht alle Nutzer auf einmal.

Niemand wurde überredet.

**Wir haben nicht überzeugt,
wir haben es leicht gemacht.**



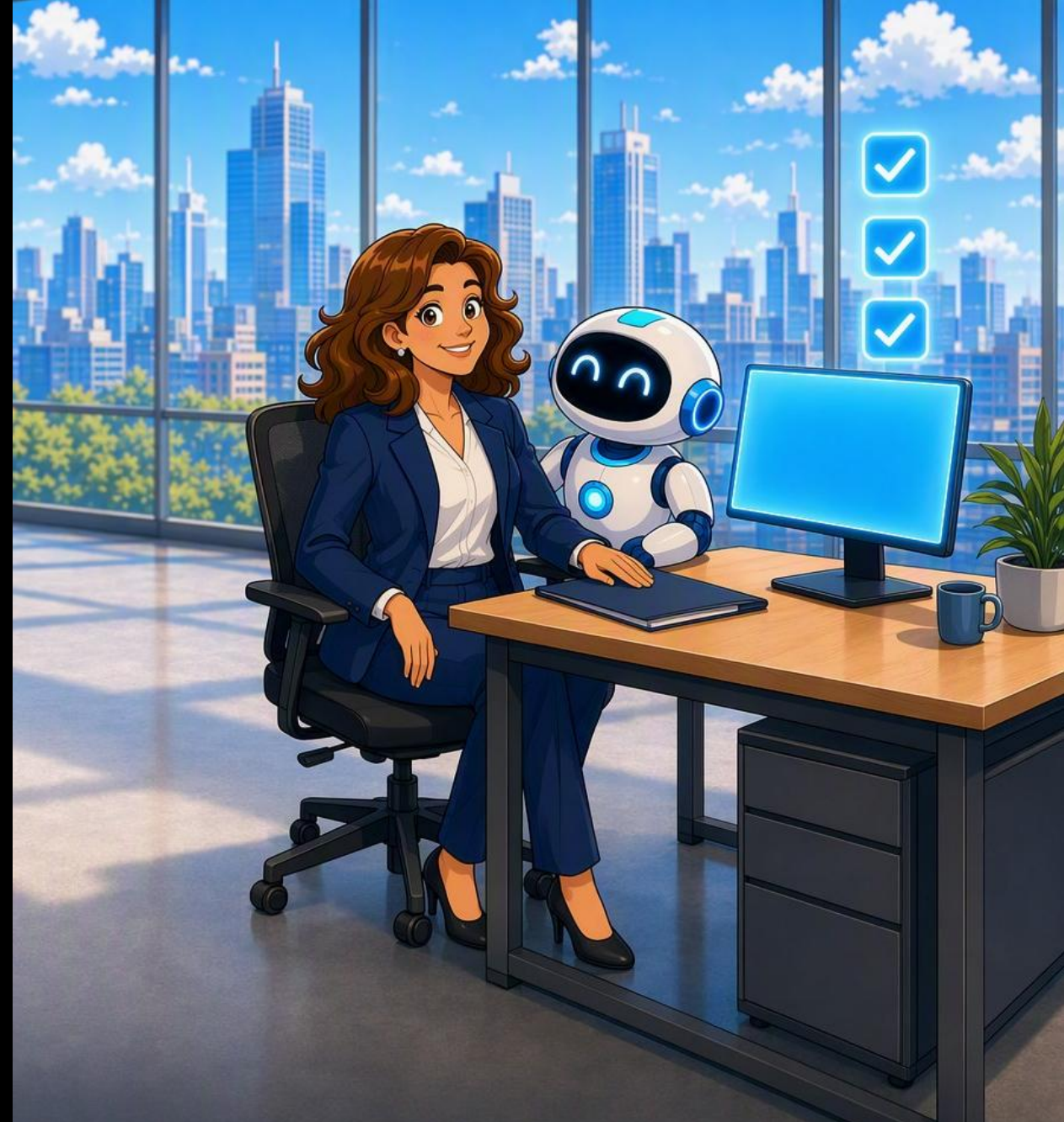
DAS FAZIT

Drei Sätze, die bleiben

1. Kaufen ist der Anfang, nicht das Ziel.
2. Enablement ist Bedingung, nicht Reihenfolge.
3. Governance ist Fundament, nicht Bremsklotz.

Die Lizenz schafft nur Möglichkeit.

Wer Enablement ans Ende schiebt,
bekommt tote Lizenzen.



Danke. Fragen?

Thomas Schuster

Business Development Manager Microsoft Security

