

Webinar

Grundlagen und Übersicht über Microsoft 365

Wir starten um 10.00 Uhr

The background of the slide is a dark blue field filled with a complex network of white lines and dots, resembling a digital or social network. The lines connect various nodes, some of which are highlighted with a bright white glow. The overall effect is one of connectivity and technology.

Webinar

Grundlagen und Übersicht über Microsoft 365

Herzlich Willkommen



Linked 



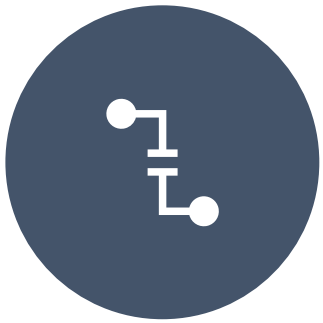
Ben Bachl-Tanaka

Speaker/Trainer/Consultant für Microsoft 365/Office 365,
Hyper-V, Windows Server2019, Cloud Migration, Azure
Metropolregion Nürnberg · [500+ Kontakte](#) · [Kontakt Daten](#)



@benbachltanaka

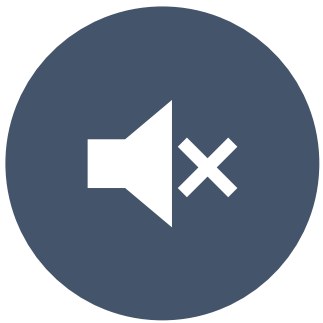
Regeln



Falls Teams Verbindung unterbrochen sein sollte → dranbleiben



Bei Fragen Chat benutzen (Q&A)



Auf Nebengeräusche achten, Mikrofon stumm schalten



Interaktion und Q&A nutzen



Inhalte und Ablauf

- **Überblick über Microsoft 365**
- **Bereitstellung von Clients mit Autopilot**
- **Verwaltung von Clients mit Endpoint Manager**
- **Q&A**

Microsoft 365 Lizenzen

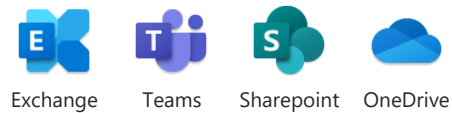
Microsoft 365 for business

Neuer Name, gleicher Preis.

Microsoft 365 Business Basic

Cloud services

€4,20 pro Benutzer/Monat



Microsoft 365 Business Standard

Cloud services und Desktop Apps

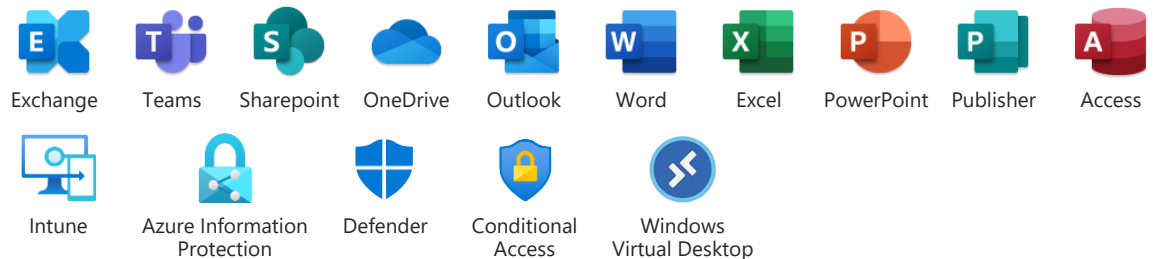
€10,50 pro Benutzer/Monat



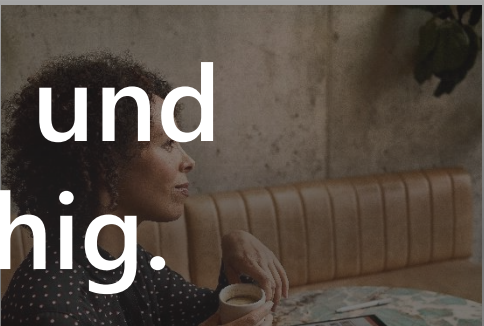
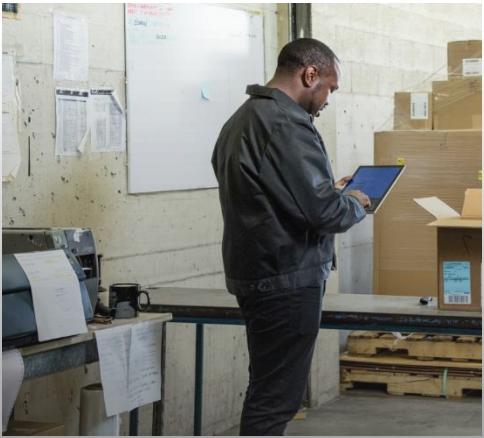
Microsoft 365 Business Premium

Cloud services, Desktop Apps, und erweiterte Sicherheit

€16,90 pro Benutzer/Monat



nicht alle Features werden hier gezeigt



KMUs sind agil und anpassungsfähig.

Mitarbeiter

76 % Unterstützung und Nutzung von Remote-Arbeitsmodellen

Werkzeuge

184 % erwarteter Anstieg bei videobasierter Zusammenarbeit

Sicherheit

11 % erwartetes Wachstum bei Investitionen gegenüber dem Vorjahr

Endpoint Manager

Absicherung von Geräten, die eine Verbindung zu Ihren Daten herstellen

Smartphones

Tablets

Laptops

Desktops



iOS- und Android-Geräte

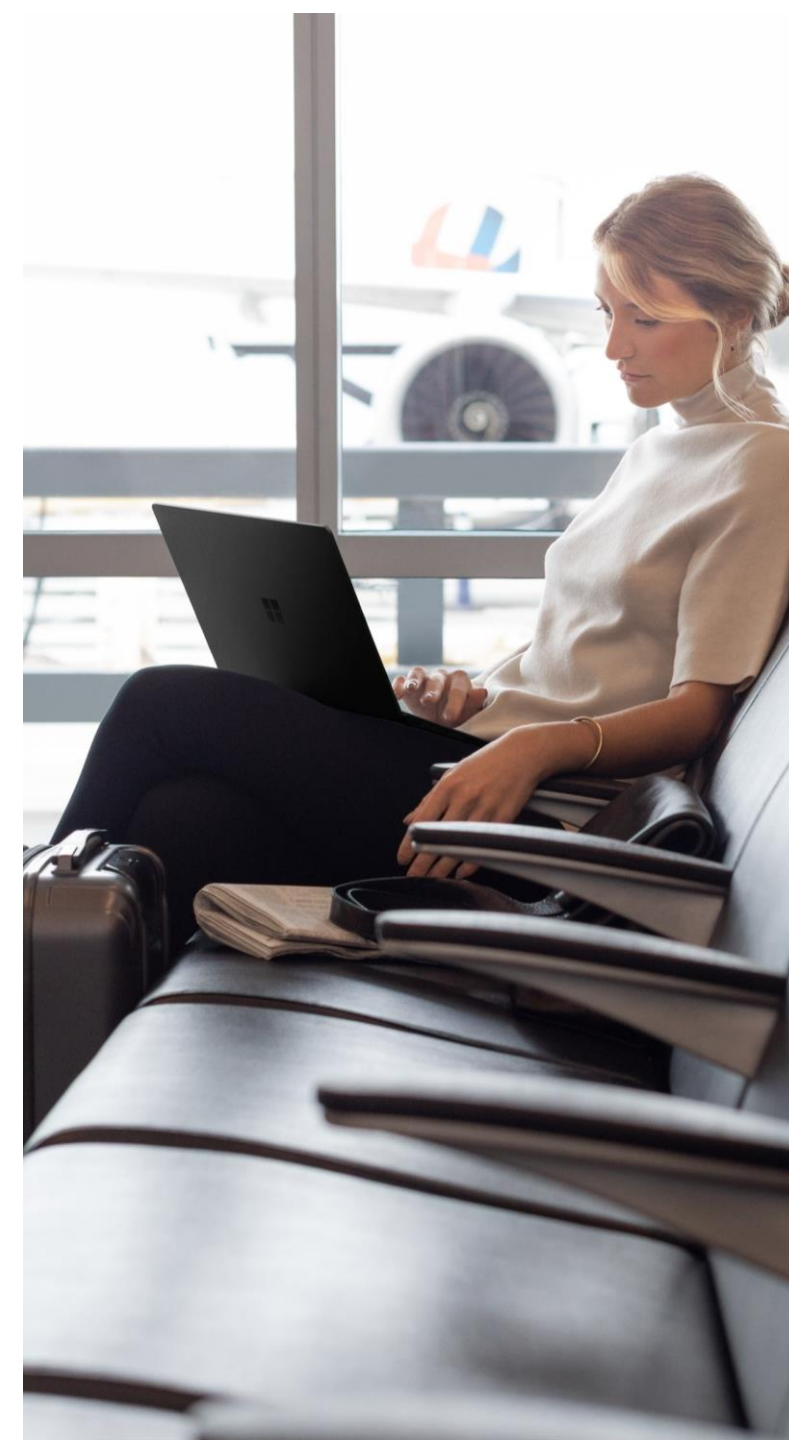
Windows PCs und MAC

Umfassende Lösung für die Geräteverwaltung

Mit dem vollständigen Funktionsumfang von Microsoft Intune

Stellt sicher, dass Geräte und Apps den Sicherheitsanforderungen Ihrer Organisation entsprechen

Bietet Richtlinien, die die Sicherheit Ihrer Geschäftsdaten gewährleisten



Verwaltung von Mobilgeräten – zwei Ansätze



Verwaltung von Mobilgeräten – zwei Ansätze

Mobile Application Management (MAM)

- In der Regel für die Verwaltung von **privaten Geräten** oder **BYOD** (Bring Your Own Device-Szenario) genutzt
- Keine Registrierung (Enrollment) von Geräten erforderlich
- Das Unternehmen verwaltet die Sicherheit nur für die registrierten Anwendungen auf dem Gerät.

Zentrale Funktionen



Absicherung von Geschäftsdaten innerhalb der Apps



Berichte zu App-Verzeichnis und Nutzung



Entfernung von Geschäftsdaten

Administration

Steuerung über Einrichtungsassistenten und eine vereinfachte Oberfläche

Mobile Device Management (MDM)

- In der Regel für die gesamte Verwaltung von **firmeneigenen Geräten** genutzt
- **Registrierung der Geräte erforderlich (Enrollment)**
- Das Unternehmen verwaltet die Sicherheit für das Gerät als Ganzes.

Zentrale Funktionen



Bereitstellung von Einstellungen, Zertifikaten und Profilen



Umfassende Kontrollwerkzeuge für Richtlinien



Berichte und Bewertung der Geräte-Compliance

Administration

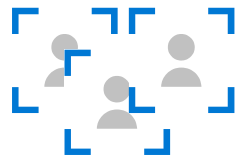
Steuerung über das Intune Admin-Center
Zusätzliche Schritte bei der Einrichtung (Bereitstellung von Zertifikaten usw.)

<https://docs.microsoft.com/de-de/intune/ios-enroll>

<https://docs.microsoft.com/de-de/intune/android-enroll>

Mobile Application Management

App Protection Policies (APP)



Unterstützung für mehrere Identitäten

Richtet sich an Geschäftskonten, nicht privat und „unmanaged“



Conditional Launch

Gerätestatus
Betriebssystemversion
App-Version/SDK
Gerätemodell oder Hersteller



Voraussetzungen für Zugriff

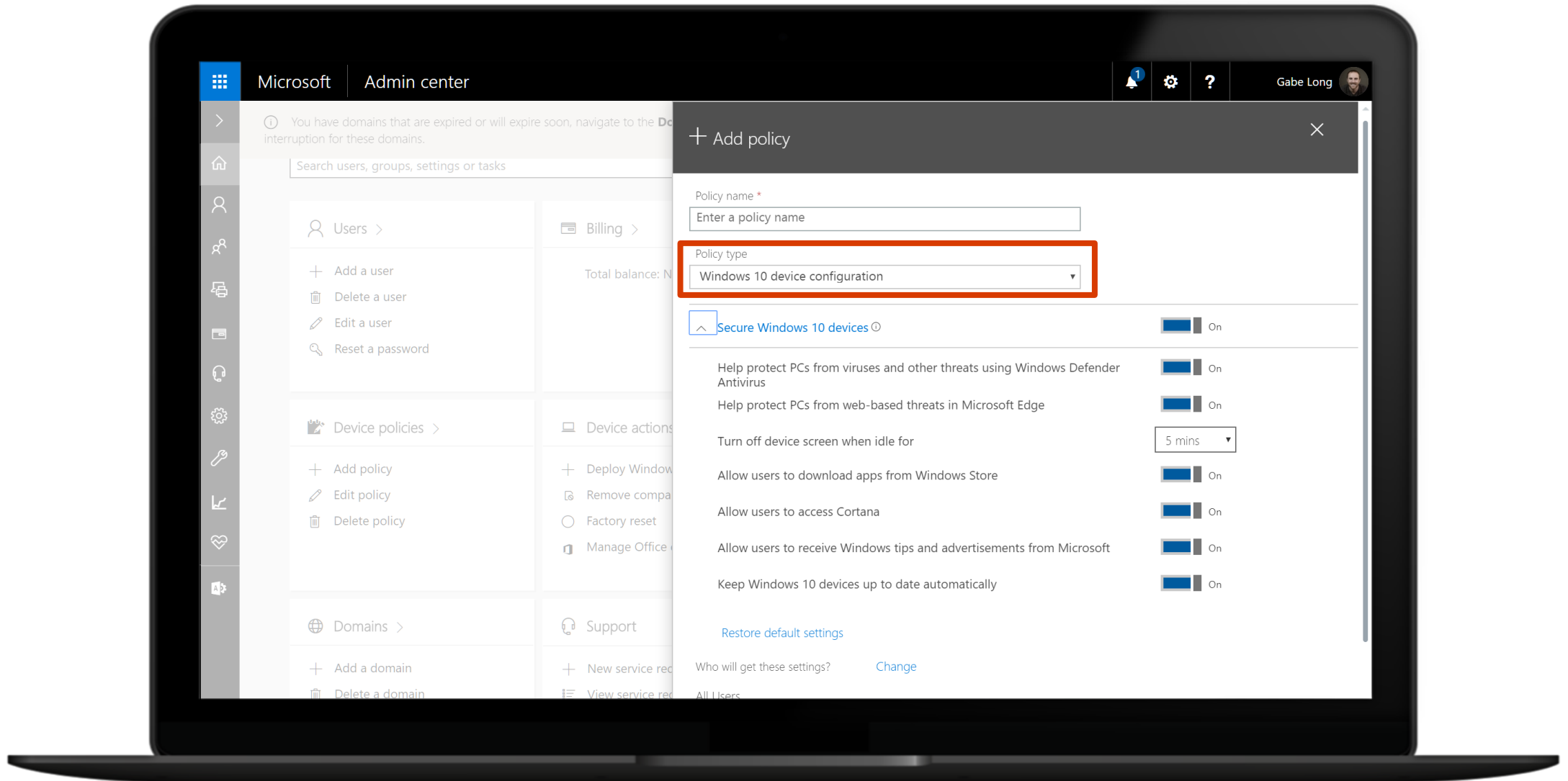
PIN
Biometrische Merkmale
Anmeldeinformationen
Inaktivitäts-Timer



Datenschutz

Zwischen Apps
Verschlüsselung
Übertragung von Webdaten
Selektives Löschen

Verwaltung von Geräterichtlinien



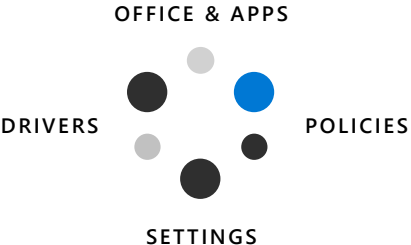
Verwaltung von Geräterichtlinien mit Endpoint Manager

The image displays the configuration of Windows Defender Antivirus settings. On the left, a Microsoft Azure portal interface shows the 'Security Center' section. On the right, a Windows 10 laptop screen shows the 'Windows Defender Antivirus' settings window. A blue dashed line connects the two views, indicating that the settings shown in the Azure portal are being applied to the device.

Setting	Current State	Target State
Real-time monitoring	Enable	Not configured
Behavior monitoring	Enable	Not configured
Network Inspection System (NIS)	Enable	Not configured
Scan all downloads	Enable	Not configured
Scan scripts loaded in Microsoft web browsers	Enable	Not configured
End-user access to Defender	Block	Not configured
Signature update interval (in hours)	Not configured	Not configured
Monitor file and program activity	Not configured	Not configured
Days before deleting quarantined malware	Enter number of days (0-90)	Not configured
CPU usage limit during a scan	Enter CPU % usage (0-100)	Not configured
Scan archive files	Enable	Not configured
Scan incoming mail messages	Enable	Not configured
Scan removable drives during a full scan	Enable	Not configured
Scan mapped network drives during a full scan	Enable	Not configured
Scan files opened from network folders	Enable	Not configured
Cloud-delivered protection	Enable	Not configured

Windows Autopilot

Traditional Windows deployment // The old way



+



=



Build a custom image, gathering everything else that's necessary to deploy

Deploy image to a new computer, overwriting what was originally on it

Time means money, making this an expensive proposition

Modern Windows deployment // The new way



Un-box and turn on
off-the-shelf Windows PC



Transform with minimal
user interaction



Device is ready
for productive use

Windows Autopilot

Einfacher Einstieg, schnelle Bereitstellung.

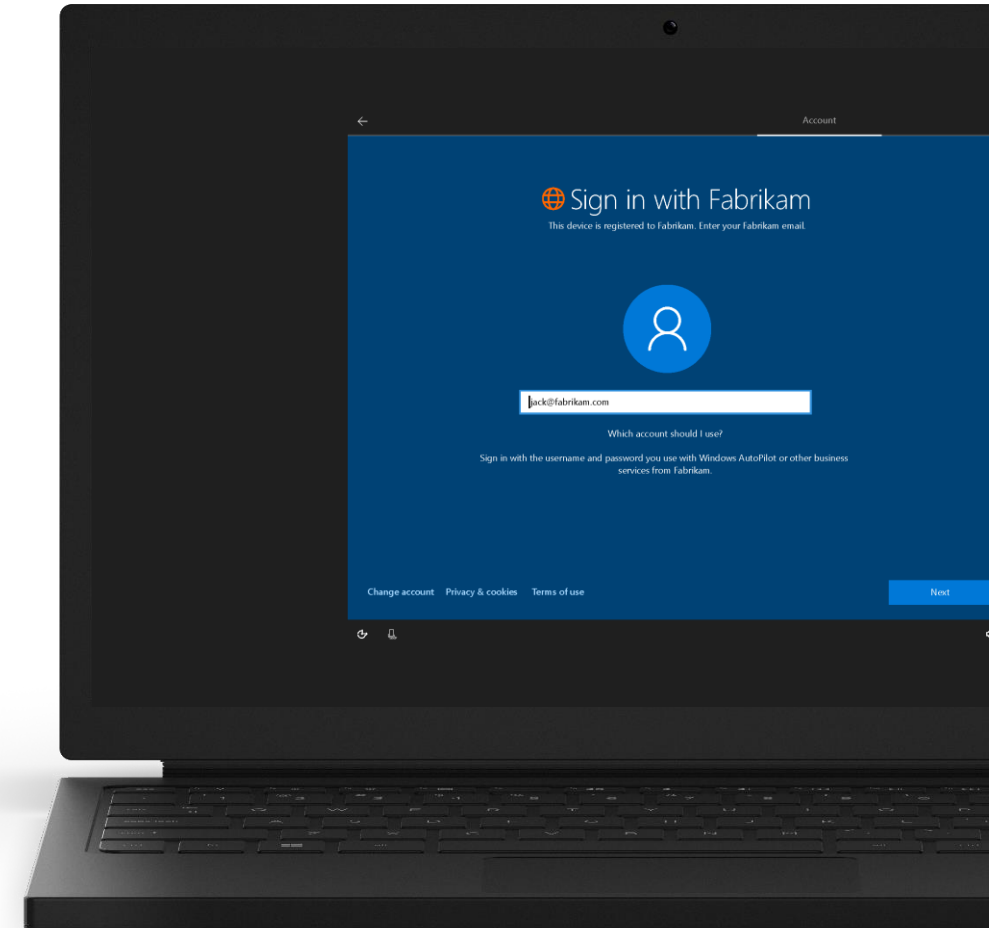
Neue Windows-Geräte können schnell und einfach aufgesetzt und eingerichtet werden. Sobald das Gerät eingeschaltet wird, sorgt Windows Autopilot über die Cloud für die richtige Konfiguration und Verwaltung – ohne Aufwand für Ihre IT-Mitarbeiter.

Traditionell oder modern? Ihre Entscheidung.

Windows Autopilot unterstützt das Hinzufügen von Geräten zu Active Directory, ihre Registrierung in Azure Active Directory und die Einbindung in das Mobile Device Management (MDM).

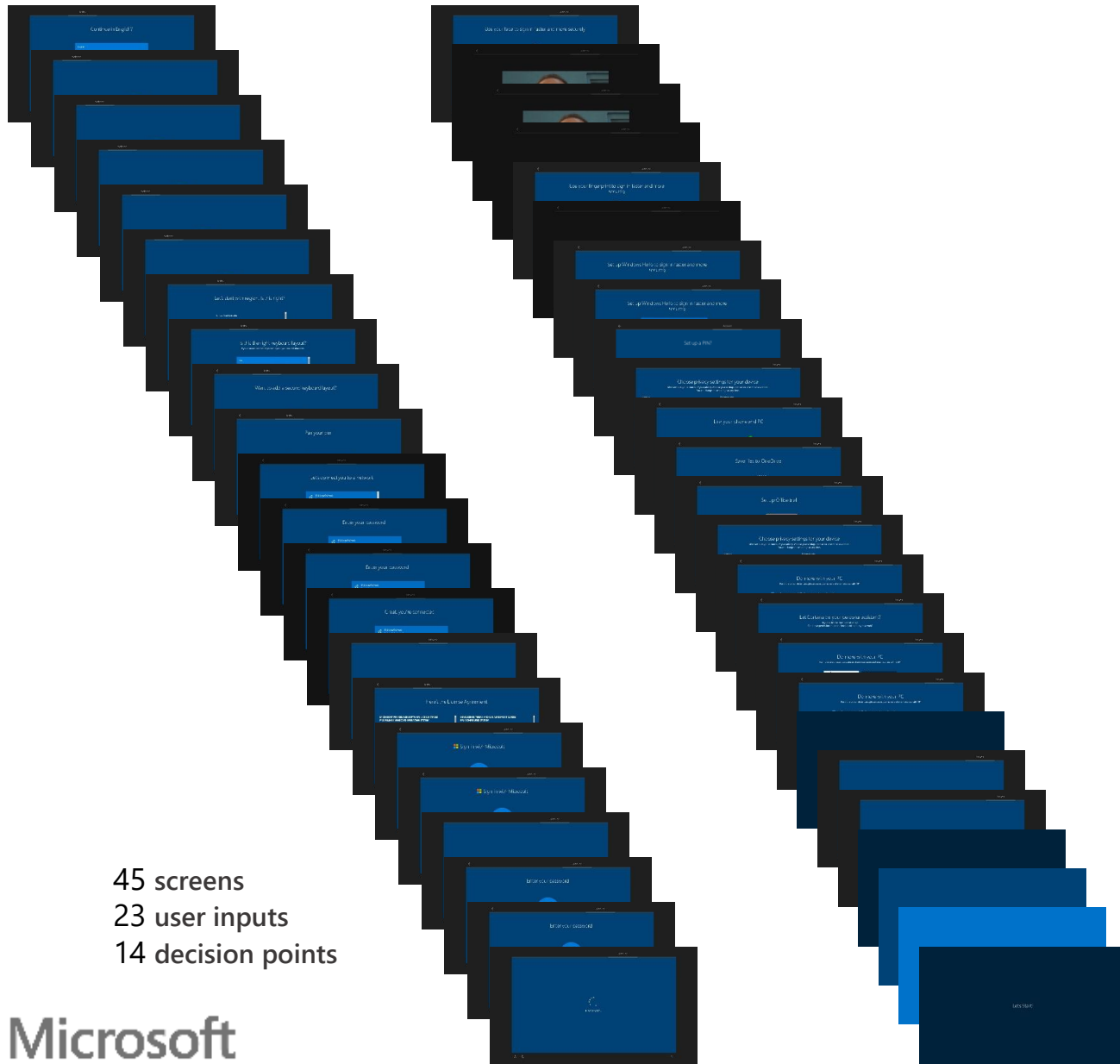
Komfortable Umgebung – von Anfang bis Ende.

Windows Autopilot unterstützt die weitergehende Personalisierung durch den Nutzer. Office aus Office365 wird auf Wunsch installiert und aktiviert.



Default OOB

Power on

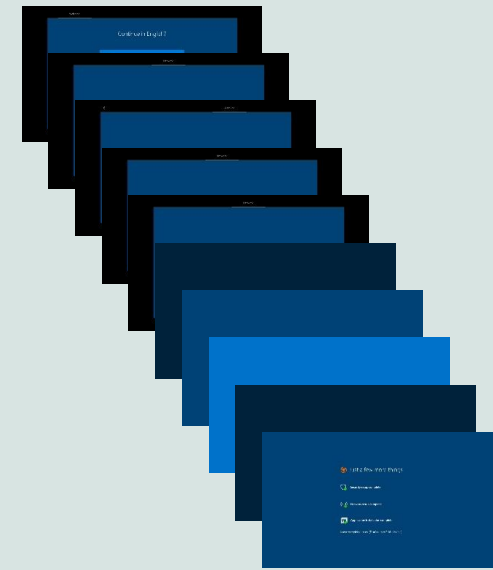


45 screens
23 user inputs
14 decision points



OOBE with Autopilot

Power on



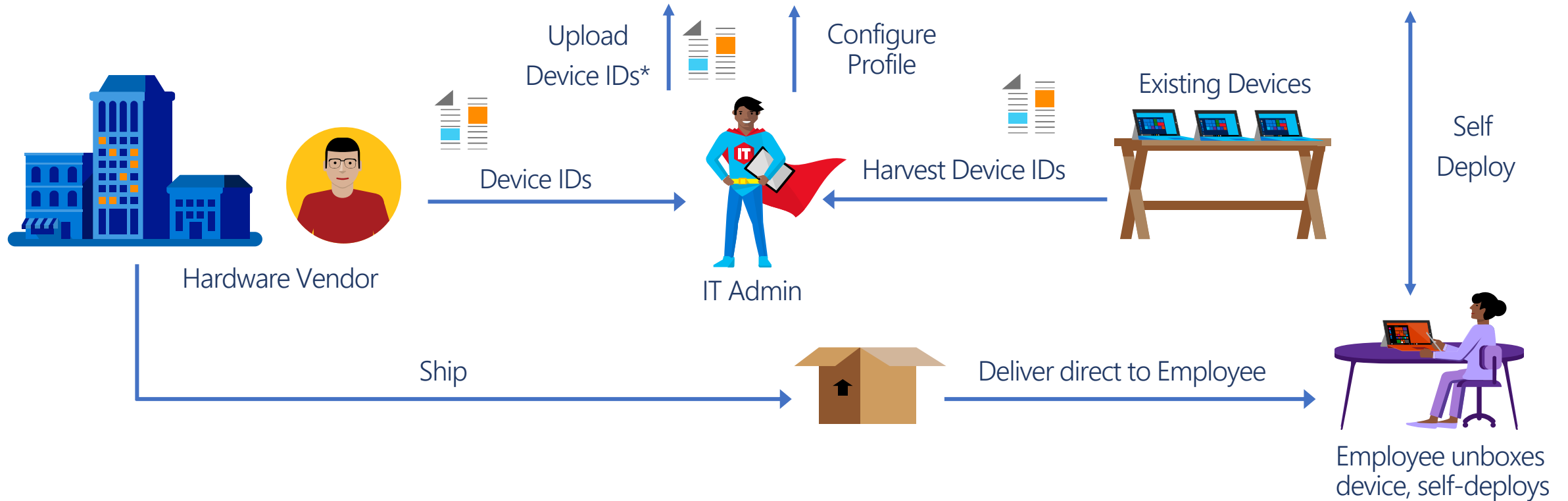
Desktop

10 screens
1 user inputs
1 decision points

Desktop

Windows Autopilot

Windows AutoPilot Deployment Service



*1709 Update - Hardware vendor can deploy configuration profiles. Deployment Profiles can also be applied via the Microsoft Store for Business.

<https://docs.microsoft.com/en-us/microsoft-store/add-profile-to-devices>

How to manually add a device to Windows Autopilot with PowerShell script

Befehle:

- `md c:\\HWID`
- `Set-Location c:\\HWID`
- `Set-ExecutionPolicy -Scope Process -ExecutionPolicy Unrestricted`
- `Install-Script -Name Get-WindowsAutoPilotInfo`
- `Get-WindowsAutoPilotInfo.ps1 -OutputFile AutoPilotHWID.csv`





Q&A



Ben Bachl-Tanaka

Senior IT Consultant - Speaker/Trainer für M365/O365,
Hyper-V, Server2016/2019, Cloud Migration, Azure
Nürnberg und Umgebung, Deutschland

Profilbereich hinzufügen ▼

Mehr ...

LinkedIn



@benbachltanaka



👉 Vernetzen Sie sich mit mir und schreiben Sie mich an für den Link zum Teams Schnellstarthandbuch!



Vielen Dank für die
Aufmerksamkeit!