

The background of the slide is a dark blue field filled with a complex network of white lines and dots, resembling a digital or neural network. The lines connect various points, some of which are highlighted with small white circles. The overall effect is a sense of connectivity and technology.

# Webinar

## Grundlagen und Übersicht über Microsoft 365

Wir starten um 10.00 Uhr

The background of the slide is a dark blue color with a complex network of white lines and dots, resembling a digital or social network. The lines connect various points, some of which are highlighted with small white circles. The overall effect is a sense of connectivity and technology.

# Webinar

## Grundlagen und Übersicht über Microsoft 365

Herzlich Willkommen



Linked 



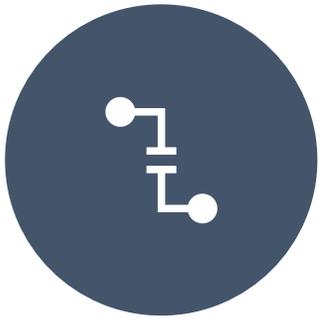
**Ben Bachl-Tanaka**

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



[@benbachltanaka](#)

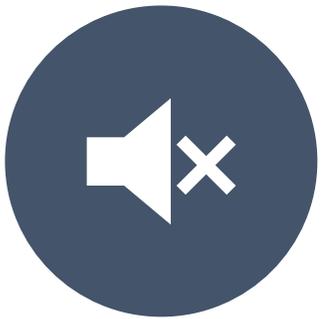
# Regeln



Falls Teams Verbindung unterbrochen sein sollte → dranbleiben



Bei Fragen Chat benutzen oder Mikrofon an (Q&A)



Auf Nebengeräusche achten, Mikrofon stumm schalten



Interaktion und Q&A nutzen



# Inhalte und Ablauf

- **Überblick über Microsoft 365**
- **Security und DLP in Microsoft 365**
- **Sicherer Zugriff via Home-Office und Smartphones**
- **Bereitstellung von Clients mit Autopilot**
- **Q&A**

**Womit sollte ich  
jetzt starten?**



# Unsere Arbeitsweise hat sich verändert



**DAMALS**



**HEUTE**

# **Microsoft Teams & Microsoft 365**

# 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

# Microsoft 365 Business im Überblick

## Premium



### Produktivität

#### Office-Anwendungen

Word, Excel, PowerPoint, Outlook und mehr

#### Onlinedienste

Exchange, OneDrive (1 TB), Teams und mehr

#### Erweiterte Dienste

Exchange Online-Archivierung



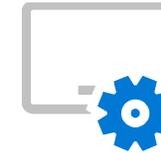
### Umfassende Sicherheit

#### Schutz vor externen Bedrohungen

Office 365 Advanced Threat Protection  
Multi-Faktor-Authentifizierung  
Windows Defender Exploit Guard  
BitLocker-Verschlüsselung

#### Prävention von internem Datenverlust

Data Loss Prevention  
Azure Information Protection



### Geräteverwaltung

#### Geräteverwaltung

Microsoft Intune  
Single Sign-on (SSO) > 10 Apps

#### Unterstützung bei der Bereitstellung

Windows Autopilot  
Automatische Installation der Office-Anwendungen  
Automatische Registrierung bei AAD



### Weitere Vorteile

Konsistente Sicherheitskonfiguration für Windows 10-, MacOS-, Android- und iOS-Geräte

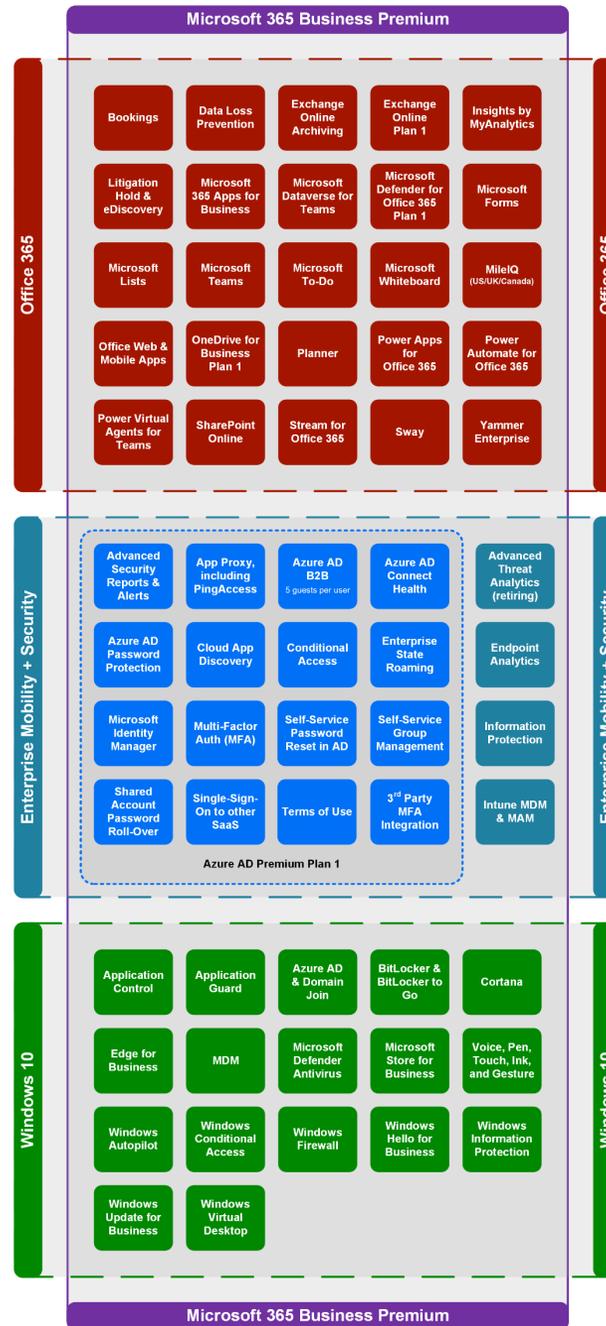
Upgrade von Windows 7 Pro oder Windows 8.1 Pro auf Windows 10 Pro ohne zusätzliche Kosten

Finanziell abgesicherte Verfügbarkeitszusage von 99,9 %; Online- und Telefonsupport 24x7

# Microsoft 365 Business Premium

February 2021

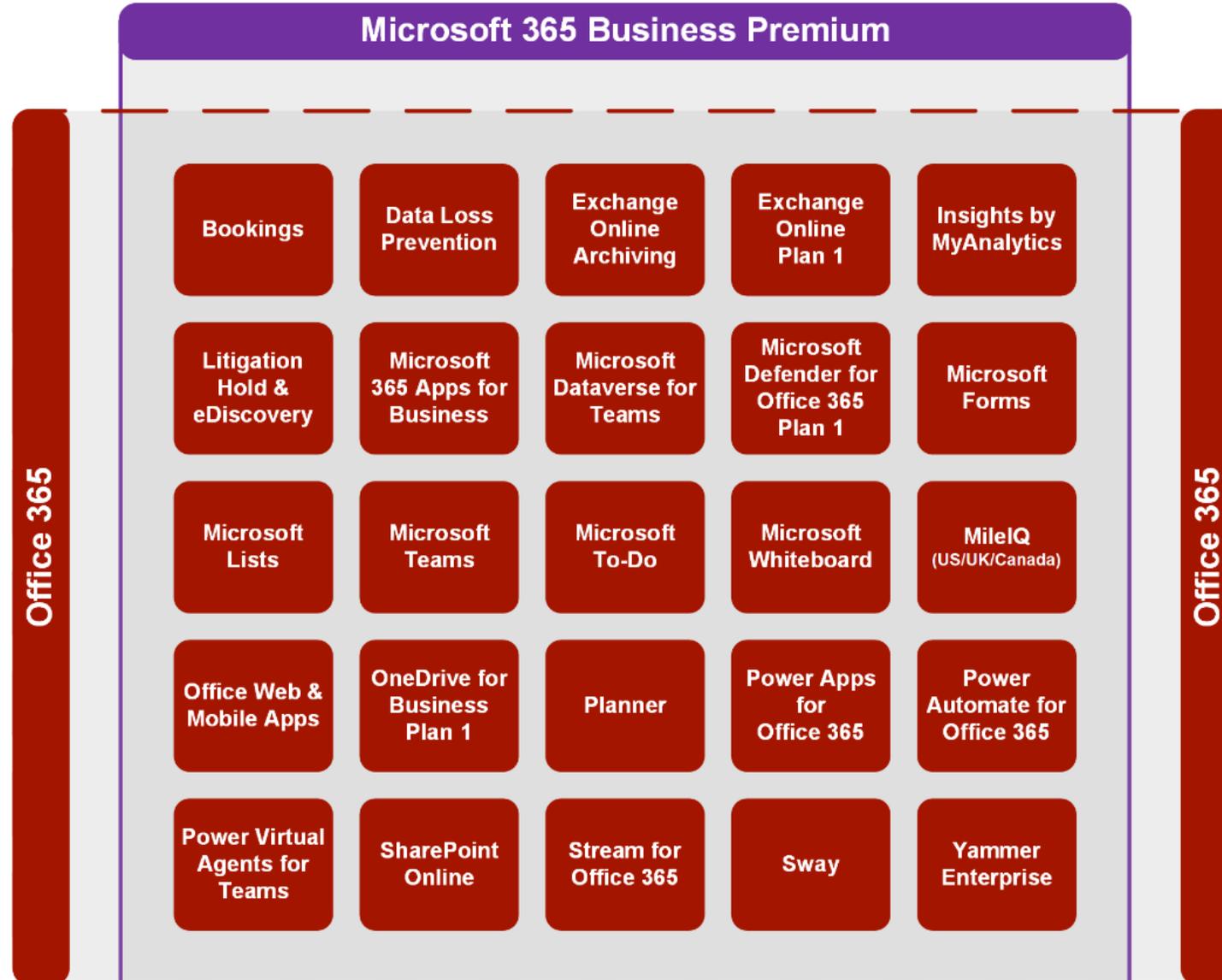
@AaronDinnage



# Microsoft 365 Business Premium

February 2021

@AaronDinnage



Power Virtual Agents for Teams

SharePoint Online

Stream for Office 365

Sway

Yammer Enterprise

Enterprise Mobility + Security

Advanced Security Reports & Alerts

App Proxy, including PingAccess

Azure AD B2B  
5 guests per user

Azure AD Connect Health

Advanced Threat Analytics (retiring)

Azure AD Password Protection

Cloud App Discovery

Conditional Access

Enterprise State Roaming

Endpoint Analytics

Microsoft Identity Manager

Multi-Factor Auth (MFA)

Self-Service Password Reset in AD

Self-Service Group Management

Information Protection

Shared Account Password Roll-Over

Single-Sign-On to other SaaS

Terms of Use

3<sup>rd</sup> Party MFA Integration

Intune MDM & MAM

Azure AD Premium Plan 1

Enterprise Mobility + Security

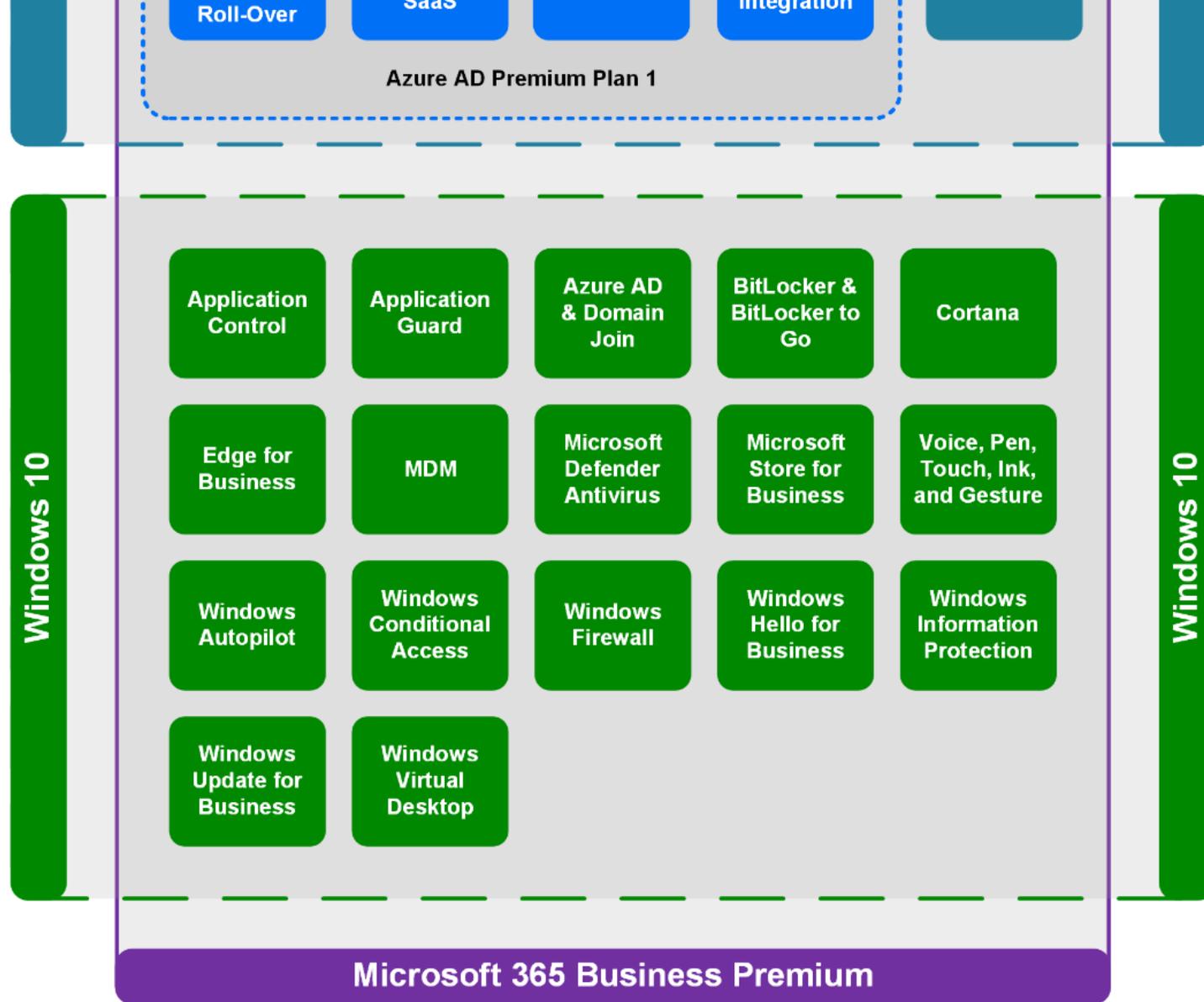
Application Control

Application Guard

Azure AD & Domain Join

BitLocker & BitLocker to Go

Cortana



Interesse an dieser Übersicht und weiteren spannenden Infos? 



# Microsoft 365 Business Standard, Microsoft 365 BP, Microsoft 365 E3 und E5 im Vergleich

Funktionen		M365 Business Standard (O365BP)	Microsoft 365 Business Premium	Microsoft 365 E3	Microsoft 365 E5
	Unverbindliche Preisempfehlung pro Nutzer und Monat in Euro (mit Jahresvertrag)	€ 10,50	€ 16,90	€ 31,46	€ 53,90
	Höchstanzahl der Benutzer	300	300	unbegrenzt	unbegrenzt
<b>Office-Anwendungen</b>	Installation von Office auf bis zu 5 PCs/Macs + 5 Tablets + 5 Smartphones pro Nutzer (Word, Excel, PowerPoint, OneNote, Access), Office Online	Business	Business	ProPlus	ProPlus
<b>E-Mail und Kalender</b>	Outlook, Exchange Online	50 GB	50 GB	100 GB	100 GB
<b>Zusammenarbeit</b>	Chatbasierter Arbeitsbereich, Onlinebesprechungen und mehr in Microsoft Teams	●	●	●	●
<b>Dateispeicherung</b>	OneDrive for Business	1 TB/Nutzer	1 TB/Nutzer	unbegrenzt	unbegrenzt
<b>Social, Video, Sites</b>	Yammer, SharePoint Online, Planner	●	●	●	●
	Stream		●	●	●
<b>Geschäftsanwendungen</b>	Scheduling Apps – Bookings <sup>1</sup> , StaffHub	●	●	●	●
	Business Apps – Outlook Customer Manager, MileIQ <sup>1</sup> , Invoicing <sup>1</sup>	●	●		
<b>Schutz vor Bedrohungen</b>	Microsoft Advanced Threat Analytics, Device Guard, Credential Guard, App Locker, Enterprise Data Protection			●	●
	Office 365 Advanced Threat Protection		●		●
	Windows Defender Advanced Threat Protection				●
	Office 365 Threat Intelligence				●
<b>Identitäts- und Zugriffsverwaltung</b>	Self-Service Passwort-Zurücksetzen für hybride Azure Active Directory-Konten		●	●	●
	Azure AD: Conditional Access, Cloud App Discovery, AAD Connect Health, SSO für mehr als 10 Apps			●	●
	Credential Guard und Direct Access			●	●
	Azure Active Directory Plan 2				●
<b>Geräte- und Anwendungsverwaltung</b>	Microsoft Intune, Windows AutoPilot		●	●	●
	Shared Computer Activation		●	●	●
	Microsoft Desktop Optimization Package, VDA			●	●
<b>Informationsschutz</b>	Office 365 Data Loss Prevention, Azure Information Protection Plan 1		●	●	●
	Azure Information Protection Plan 2, Microsoft Cloud App Security, O365 Cloud App Security				●
<b>On-Premises CAL-Rechte</b>	ECAL Suite (Exchange, SharePoint, Skype, Windows, SCCM, Win. Rights Management)			●	●
<b>Compliance</b>	Unbegrenzte E-Mail-Archivierung <sup>2</sup>		●	●	●
	Advanced eDiscovery, Customer Lockbox, Advanced Data Governance				●
<b>Analytics</b>	Power BI Pro, MyAnalytics				●
<b>Voice</b>	PSTN Conferencing, Cloud PBX				●

[1] Verfügbar in den USA, Kanada, Großbritannien.

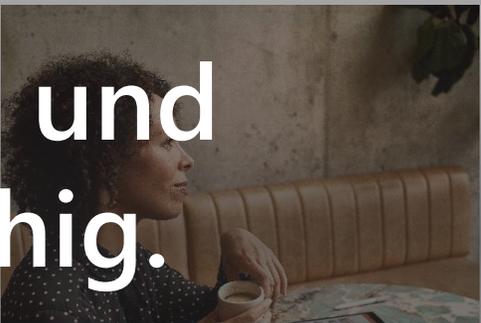
[2] Unbegrenzte Archivierung, wenn Auto-Erweiterung aktiviert wurde.

# Vergleich von Microsoft 365 Business Premium und Office 365 E3

	<b>Funktionen (neue Funktionen in Blau hervorgehoben)</b>	Office 365 E3	Microsoft 365 Business Prem
	Unverbindliche Preisempfehlung pro Nutzer und Monat in Euro (mit Jahresvertrag)	€ 19,70	€ 16,90
	Höchstanzahl der Benutzer	unbegrenzt	300
Office-Anwendungen	Installation von Office auf bis zu 5 PCs/Macs + 5 Tablets + 5 Smartphones pro Nutzer (Word, Excel, PowerPoint, OneNote, Access), Office Online	ProPlus	Business
E-Mail und Kalender	Outlook, Exchange Online	100 GB	50 GB
Chatbasierter Arbeitsbereich, Besprechungen	Microsoft Teams	●	●
Dateispeicherung	OneDrive for Business	unbegrenzt	1 TB
Social, Video, Sites	Stream, Yammer, Planner, SharePoint Online <sup>1</sup> , Power Apps <sup>1</sup> , Flow <sup>1</sup>	●	●
Geschäftsanwendungen	Scheduling Apps – Booking, StaffHub	●	●
	Business Apps – Outlook Customer Manager, MileIQ <sup>1</sup> Business Center <sup>2</sup> , Listings <sup>2</sup> , Connections <sup>2</sup> , Invoicing <sup>2</sup>		●
Schutz vor Bedrohungen	<b>Office 365 Advanced Threat Protection</b>		●
	<b>Windows Exploit Guard Enforcement</b>		●
Identitäts- und Zugriffsverwaltung	Azure Active Directory – SSPR Cloud Identities, MFA, SSO >10 Apps		●
Geräte- und Anwendungsverwaltung	Office 365 MDM	●	●
	<b>Microsoft Intune</b> , Windows Autopilot, Windows Pro Management		●
	Upgrade-Rechte auf Windows 10 Pro für Windows 7/8/8.1 Pro-Lizenzen		●
Informationsschutz	<b>100 GB Exchange Archiving, Office 365 Data Loss Prevention</b>	●	●
	<b>Azure Information Protection Plan 1, BitLocker Enforcement</b>		●
On-Premises CAL-Rechte	ECAL Suite (Exchange, SharePoint)	●	
Compliance	<b>Litigation Hold, eDiscovery, Compliance Manager, Data Subject Requests, Supervision</b>	●	●

[1] Bedeutet, dass die Funktionalität in Office 365 mit Plan 2 und in Microsoft 365 Business mit Plan 1 enthalten ist.

[2] Verfügbar in den USA, Kanada, Großbritannien.



# KMUs sind agil und anpassungsfähig.

## Mitarbeiter

**76 %** Unterstützung und Nutzung von Remote-Arbeitsmodellen

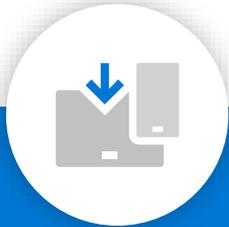
## Werkzeuge

**184 %** erwarteter Anstieg bei videobasierter Zusammenarbeit

## Sicherheit

**11 %** erwartetes Wachstum bei Investitionen gegenüber dem Vorjahr

# Bei unseren KMU-Kunden ganz oben auf der Agenda ...



Wie können wir  
Remote-Arbeit  
optimieren?

Kollegen, die an  
verschiedenen Orten arbeiten



Wie können wir  
die Sicherheit  
gewährleisten?

Vielfalt von persönlichen  
und mobilen Endgeräten

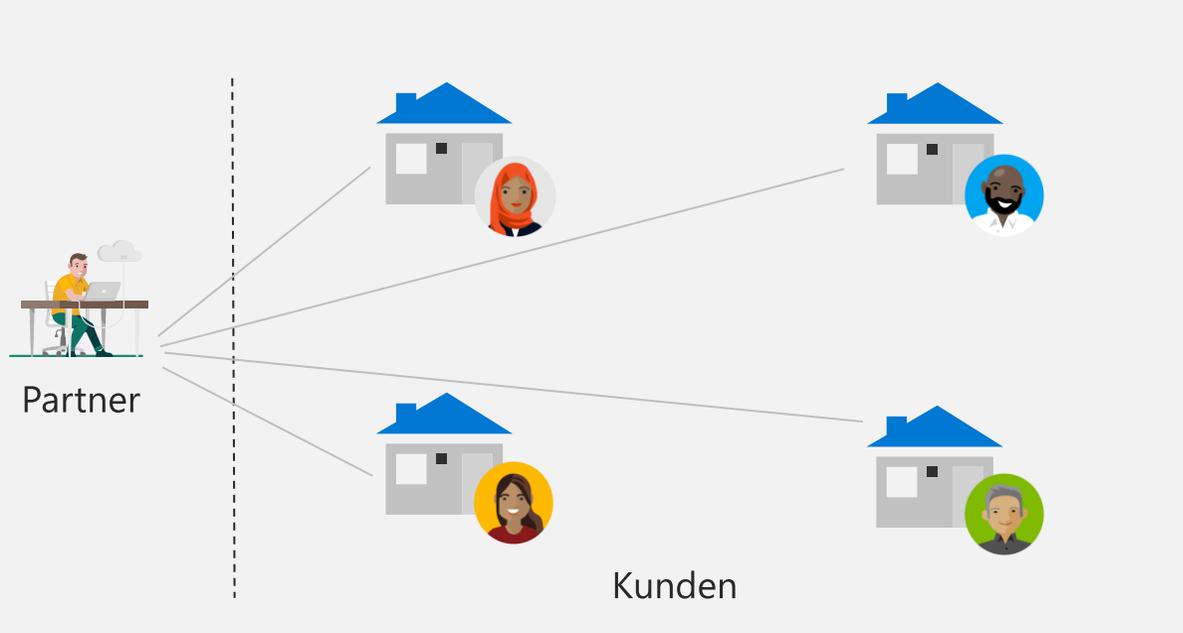


Wie können wir  
unsere Kosten  
senken?

COVID-19-bedingte Zunahme  
von Phishing und  
Ransomware

# Die heutige IT-Umgebung für KMUs ist anspruchsvoll.

Sie als Partner müssen Ihre Kunden dabei unterstützen, in einer Umgebung mit verteilten und Remote-Standorten stets in Verbindung zu bleiben, produktiv zu arbeiten und zugleich ein Höchstmaß an Schutz vor Cyberbedrohungen und Datenverlust für das jeweilige Unternehmen zu realisieren.



Immer mehr Angestellte arbeiten im Homeoffice.



Auf Geschäftsdaten wird mit Heim-PCs und Privatgeräten zugegriffen.



Im Zusammenhang mit COVID-19 entstehen zahlreiche neue Phishing- und Ransomware-Bedrohungen.

# Unterstützung von Unternehmen mit Microsoft 365



Bessere Werkzeuge  
für Remote-Arbeit



Bessere Sicherheit  
bei der Remote-Arbeit



Gelegenheit für die  
Senkung von Kosten

# Bessere Werkzeuge für Remote-Arbeit mit Microsoft Teams

## Integrierte Lösung für ein optimales Anwendererlebnis

Video-  
konferenzen

Gruppen-  
Chat

Einfacher Zugriff  
auf Dateien

Gemeinsame  
Bearbeitung  
in Echtzeit

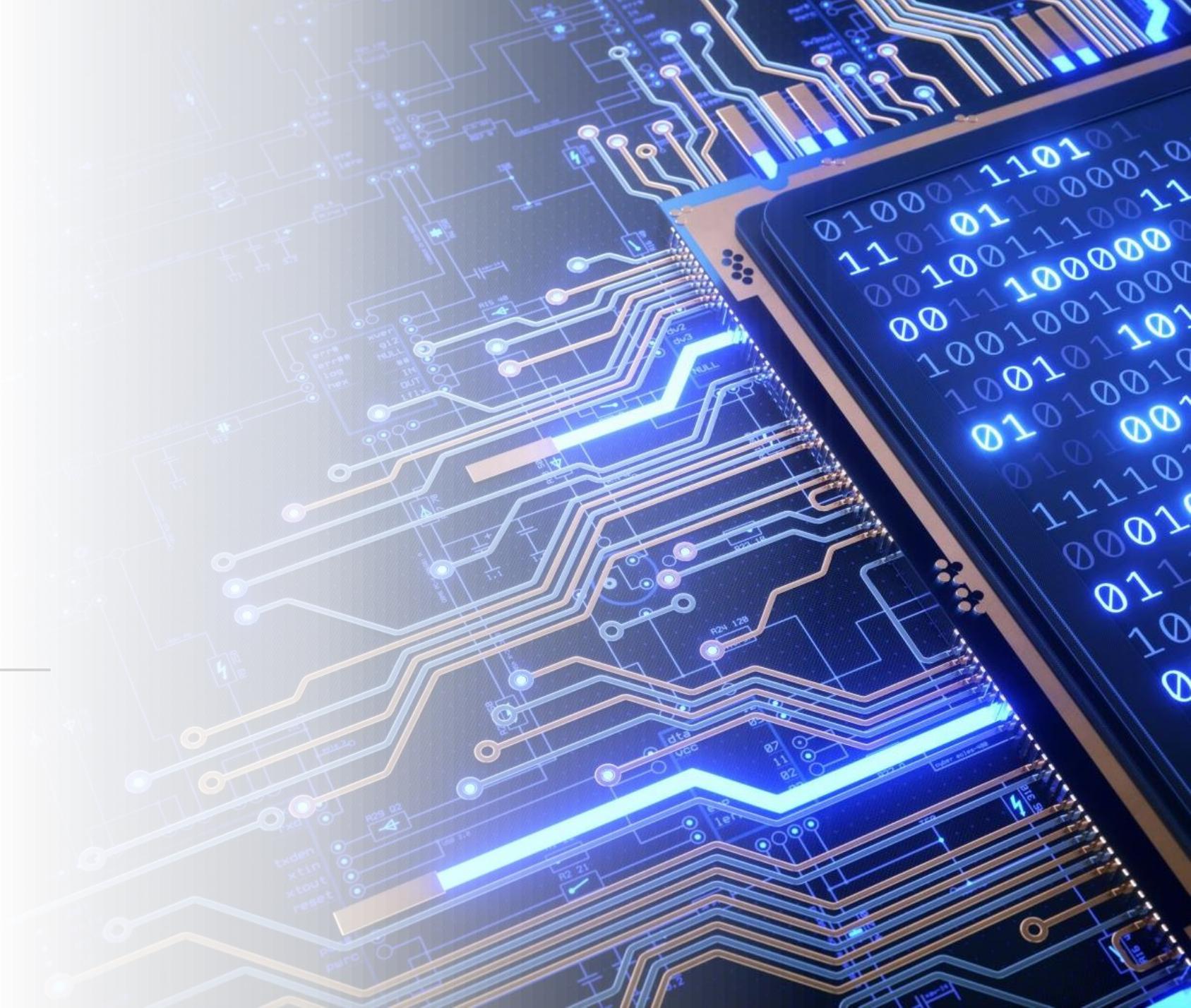
Telefonsystem  
(Microsoft 365  
Business Voice  
Add-on)

Integration  
von Apps



# Enterprise Security in Microsoft365 Business Premium

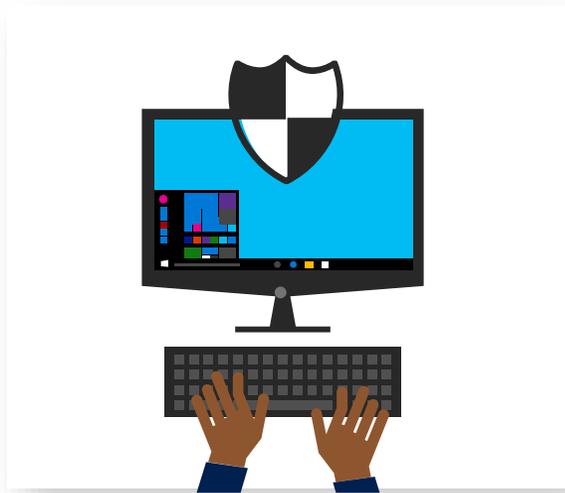
---



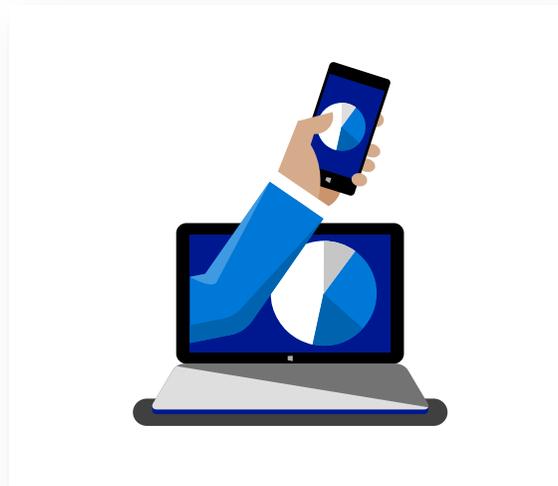
**Sicherheit**

**Aktivierung von Remote-Zugriff  
und Schutz von Identitäten**

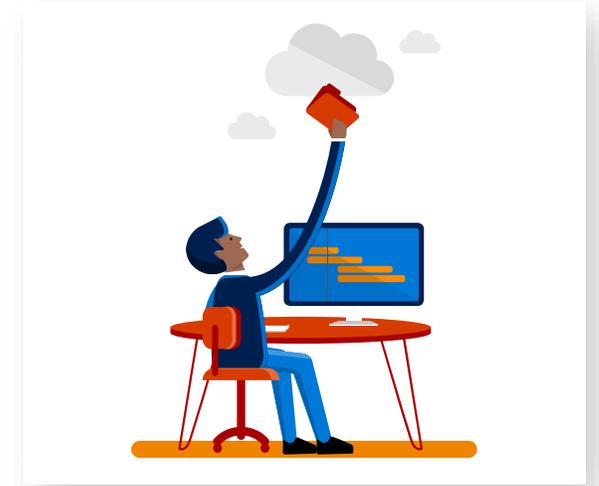
# Die Voraussetzung für Remote-Arbeit: Absicherung von Identitäten und Zugriffsoptionen



Schutz vor Passwort-  
diebstahl und -verlust



Sicherer Zugriff auf  
Arbeitsanwendungen



Bereitstellung von  
Remote-Desktop-Zugriff

# Schutz vor Passwortdiebstahl und -verlust mit MFA

Verifizieren Sie Benutzeridentitäten mit starker Multi-Faktor-Authentifizierung.



Wir unterstützen eine große Bandbreite von mehrstufigen Authentifizierungsoptionen.

## Technologie für passwortlosen Zugriff



Microsoft Authenticator



Windows Hello



FIDO2 Security Key



Biometrie



Push-Benachrichtigung



Soft Tokens OTP



Hard Tokens OTP



SMS, Sprachsystem



Multi-Faktor-Authentifizierung verhindert 99,9 % der Angriffe auf Identitäten.<sup>1</sup>

<sup>1</sup> Quelle: <https://www.microsoft.com/security/blog/2019/08/20/one-simple-action-you-can-take-to-prevent-99-9-percent-of-account-attacks/>, basierend auf einer internen Microsoft-Studie.

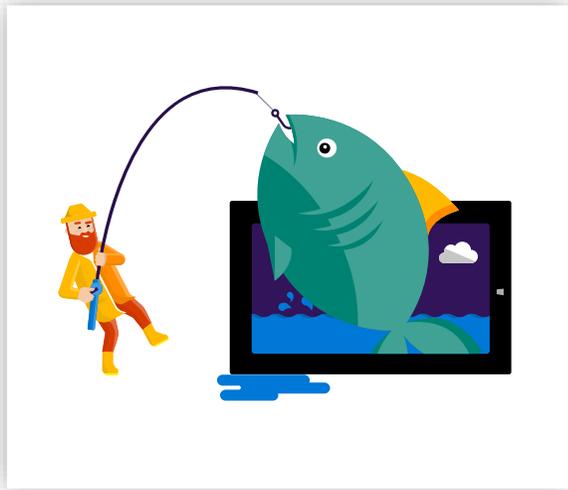
# Bereitstellung von Remote-Desktop-Zugriff mit Windows Virtual Desktop

- Bereitstellung des Windows 10-Erlebnisses mit mehreren Sessions – hochgradig skalierbar und stets auf dem neuesten Stand
- Aktivierung von Optimierungen für Office
- Migration von RDS-Desktops und -Apps sowie Vereinfachung der Lizenzierung und Senkung von Kosten
- Minutenschnelle Bereitstellung und Skalierung sowie Verwaltung auf einer einheitlichen Admin-Oberfläche mit Azure Portal
- Unterstützung aller Endbenutzer-Geräteplattformen, einschließlich Windows, Android, Mac, iOS und HTML 5

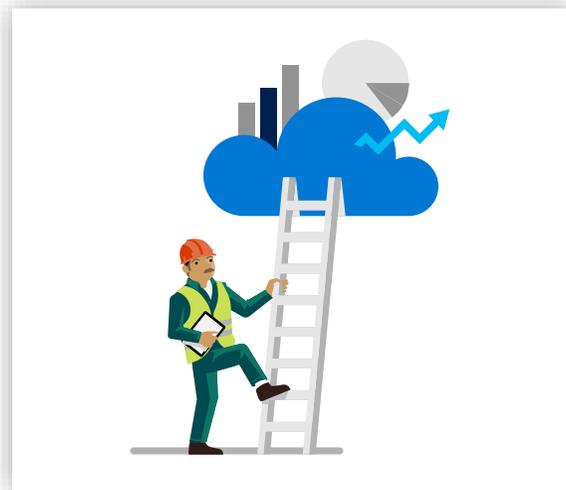


# Schutz vor Cyberbedrohungen und Datenverlust

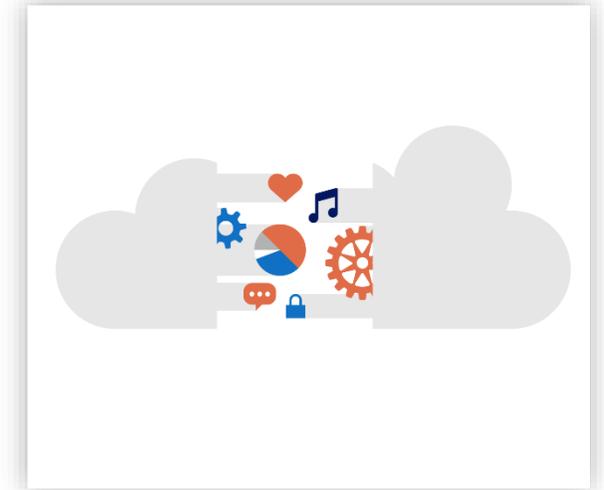
# Verteidigung gegen Cyberbedrohungen und Schutz von Geschäftsdaten



Schutz von Nutzern vor  
Cyberbedrohungen wie  
Phishing



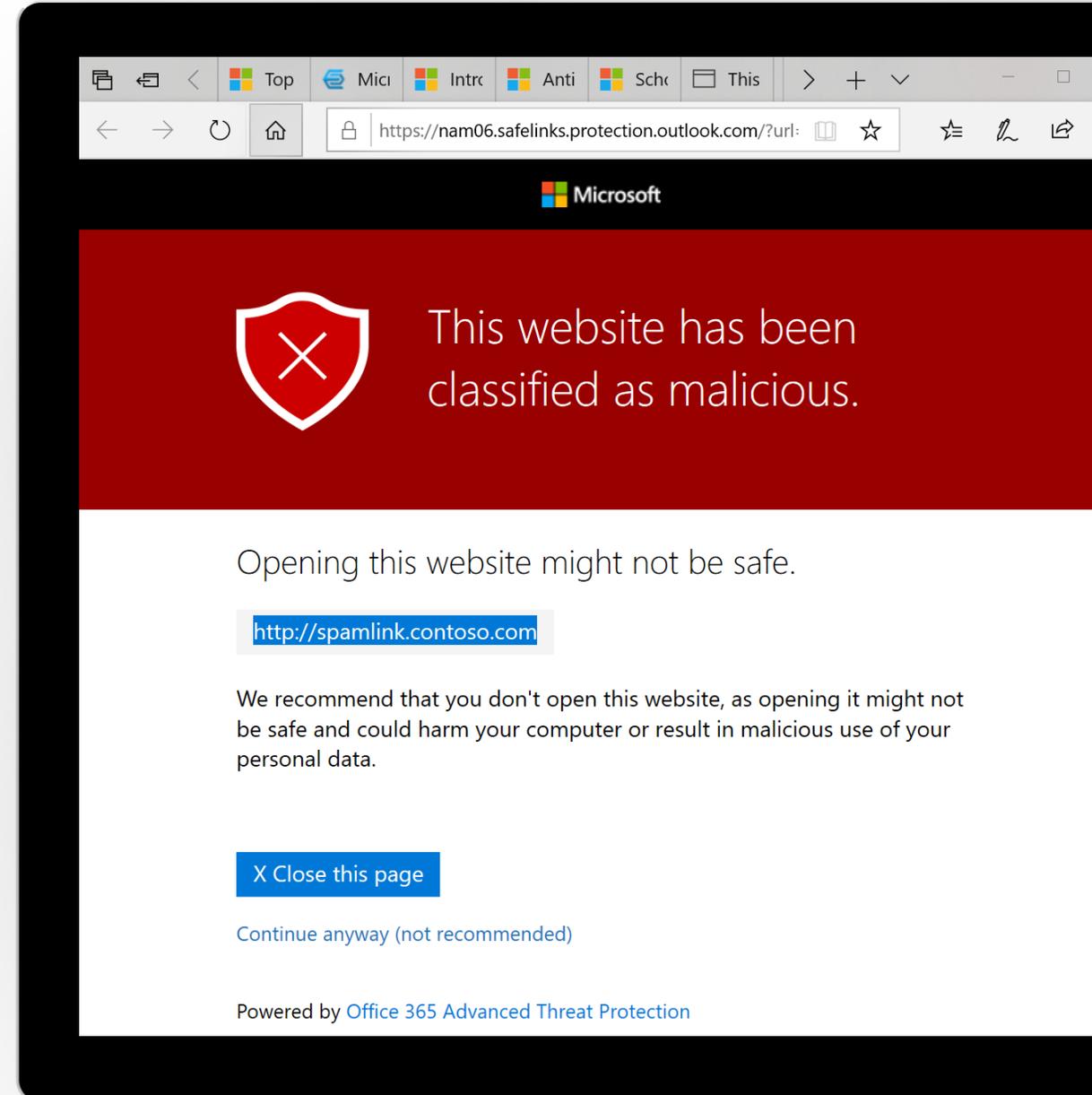
Schutz für vertrauliche  
Geschäftsdaten



Transparenz in der  
Nutzung von Cloud-  
Anwendungen

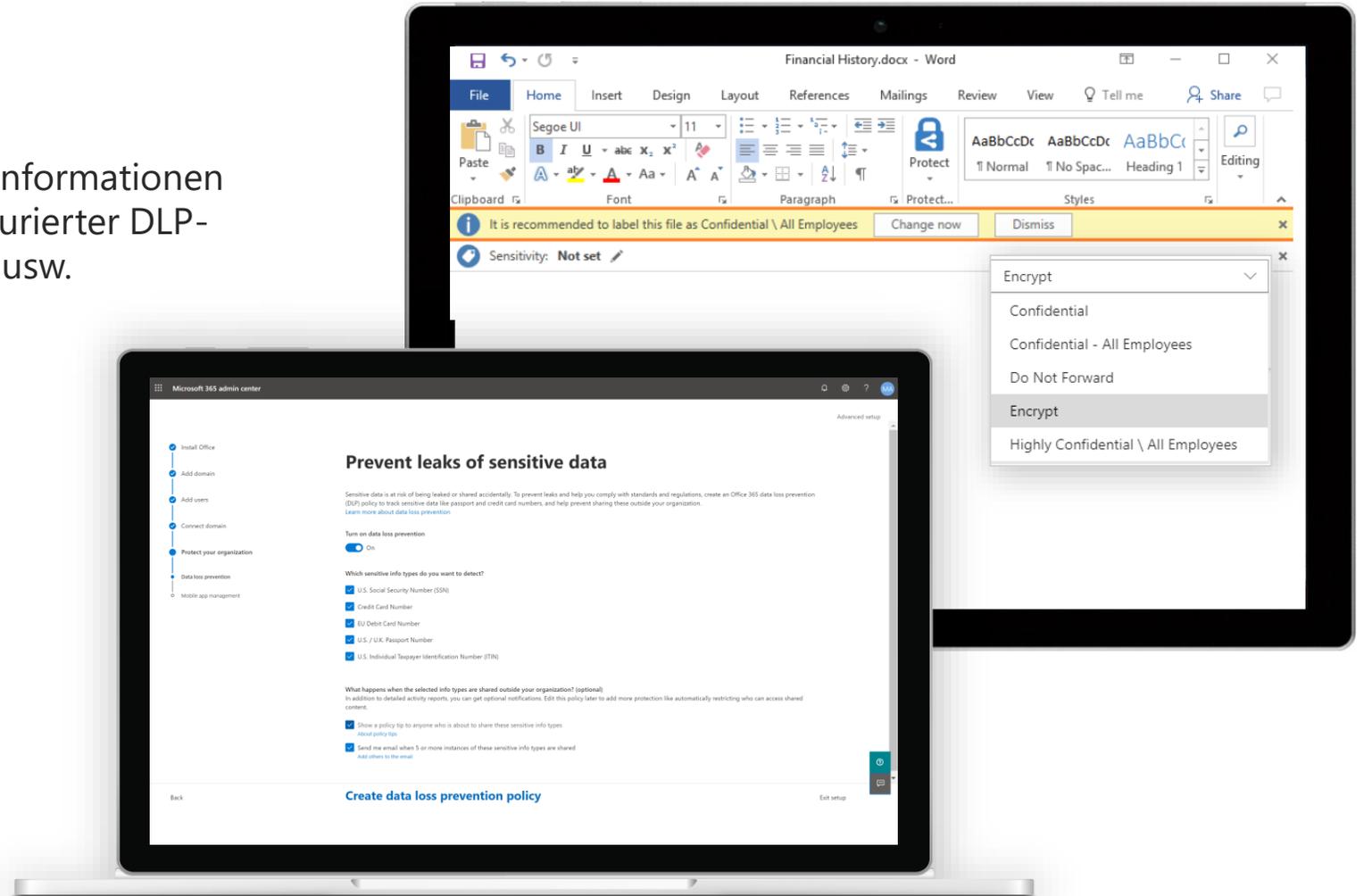
# Schutz von Nutzern vor Cyberbedrohungen wie Phishing mit Microsoft Defender

- Schutz vor bösartigen Links in E-Mails oder Teams mithilfe von Echtzeit-Scans (ATP Safe Links)
- KI-gestützte Malware-Scans für E-Mail-Dateianhänge und Links zu freigegebenen Dokumenten in Teams und OneDrive (ATP Safe Attachments)
- Verteidigung gegen Identitätsbetrug und Spoofing (ATP Anti-Phishing)
- Besserer Schutz auf Windows-Geräten vor verdächtigen Prozessen wie bei Ransomware (Microsoft Defender AV)



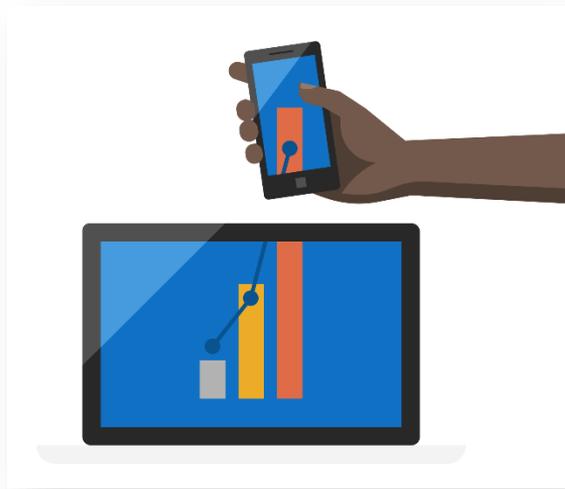
# Schutz für vertrauliche Geschäftsdaten mit DLP und Azure Information Protection

- Unterbindung der Weitergabe vertraulicher Informationen wie Kreditkartennummern mithilfe vorkonfigurierter DLP-Richtlinienvorlagen für HIPAA, PCI-DSS, SSN usw.
- Kontrolle über Aktionen für E-Mails wie Weiterleiten, Drucken oder Anzeigen von externen Nutzern
- Kontrolle über Aktionen für Dateien wie Bearbeiten, Drucken oder Anzeigen von externen Nutzern. Zudem können Sie den Zugriff jederzeit widerrufen.

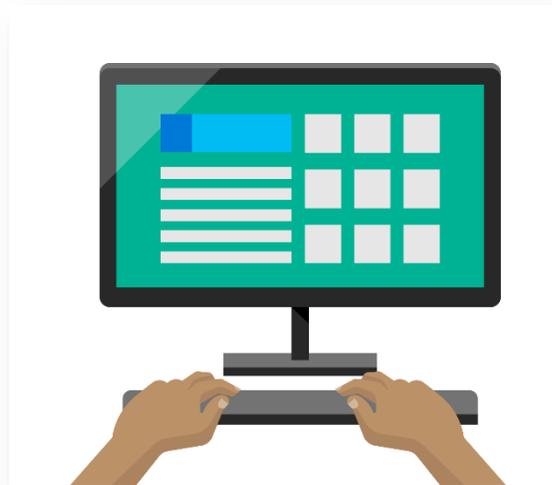


Einfache Absicherung von  
privaten und  
firmeneigenen Geräten

# Absicherung und Verwaltung aller Geräte, die auf Daten Ihres Unternehmens zugreifen



Verwaltung von Arbeitsdaten  
auf Mobilgeräten



Absicherung von  
Windows-Geräten



Automatisierung der  
Bereitstellung mit  
Autopilot

# Verwaltung von Arbeitsdaten auf Mobilgeräten mit Intune



## Mobile Device Management (MDM)

**Bedingter Zugriff:**  
Verwalten Sie den Zugriff auf firmeneigenen Geräten.



Registrierung von Geräten für die Verwaltung



Bereitstellung von Einstellungen, Zertifikaten, Profilen



Reporting und Bewertung der Gerätekonformität



Remote-Löschen von Geschäftsdaten auf Geräten



## Mobile Application Management (MAM)

**Bedingter Zugriff:**  
Steuern Sie, welche Apps für den Zugriff auf geschäftliche E-Mails oder Dateien auf Privatgeräten verwendet werden können.



Veröffentlichung von mobilen Apps für Nutzer



Konfiguration und Aktualisierung von Apps



Durchsetzung von Richtlinien, sodass geschäftliche Daten nicht in persönlichen Apps gespeichert werden können



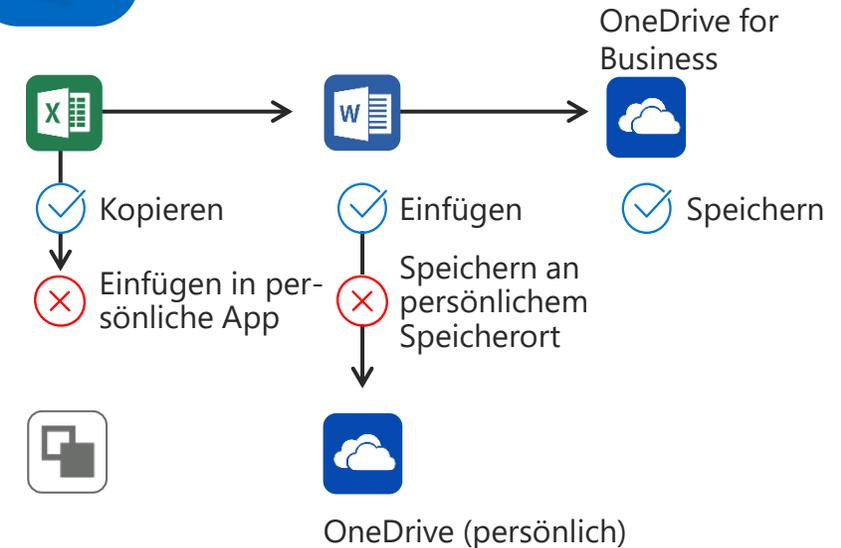
Absicherung und Löschen von Geschäftsdaten in mobilen Apps

# Beispiel: Verwaltung von Arbeitsdaten auf persönlichem Gerät

MAM-Richtlinie,  
um Arbeitsdaten  
abzusichern



E-Mail-  
Dateianhang



Azure Information Protection (AIP) ermöglicht Ihnen, Kontrollwerkzeuge für den Zugriff auf Arbeitsdaten zu definieren.

Trennen Sie die vom Unternehmen verwalteten Apps von persönlichen Apps und definieren Sie Richtlinien, wie über verwaltete Apps auf geschäftliche Daten zugegriffen werden kann.

Intune sorgt dafür, dass Geschäftsdaten nicht kopiert und in persönliche Apps innerhalb des Geräts übertragen werden können.

# Absicherung von Windows-Geräten mit Defender und Intune

- Durchsetzung automatischer Updates auf allen Windows 10-Geräten
- Obligatorische Aktivierung von Microsoft Defender als Schutz vor Schadsoftware
- Obligatorische Nutzung der BitLocker-Verschlüsselung, um unbefugten Zugriff zu verhindern

Microsoft 365 admin center

Setup  
Microsoft 365 Business

Step 1  
Personalize sign-in

Step 2  
Add users

Step 3  
Protect data & devices

## Set Windows 10 device configuration

When a user connects a Windows 10 device to your organization, they'll automatically receive the settings you configure below. You can also make sure that users get the latest version of Office installed on their devices. We recommend that you start with the default settings and adjust your configuration later. [Learn more about configuring Windows 10](#)

Secure Windows 10 devices  On

- Help protect PCs from viruses and other threats using Windows Defender Antivirus  On
- Help protect PCs from web-based threats in Microsoft Edge  On
- Use rules that reduce the attack surface of devices  On
- Protect folders from threats such as ransomware  On
- Prevent network access to potentially malicious content on the Internet  On
- Help protect files and folders on PCs from unauthorized access with BitLocker  On
- Allow users to download apps from Microsoft Store  On
- Allow users to access Cortana  On
- Allow users to receive Windows tips and advertisements from Microsoft  On
- Keep Windows 10 devices up to date automatically  On
- Turn off device screen when idle for  
5 minutes

[Restore default settings](#)

Install Office on Windows 10 devices  Yes

# Conditional Access Example



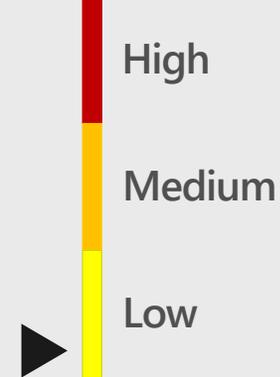
User

- ✓ Role: Sales Account Representative
- ✓ Group: London Users
- ✓ Device: Windows
- ✓ Config: Corp Proxy
- ✓ Location: London, UK
- ✓ Last Sign-in: 5 hrs ago



Device

- ✗ Health: Device compromised
- ✓ Client: Browser
- ⚠ Config: Anonymous
- ⚠ Last seen: Asia



**Block access**  
**Force threat remediation**



Office resource

Sensitivity: Medium

For insights into password spray and other modern attack patterns, see [Your Pa\\$\\$word doesn't matter](#)

- ✗ Malicious activity detected on device
- ⚠ Anonymous IP
- ⚠ Unfamiliar sign-in location for this user

# Automatisierung der Windows-Bereitstellung mit Autopilot

- Direkte Auslieferung von Geräten, die bereits für eine Verwaltung eingerichtet sind
- Signifikante Zeit- und Kostenersparnis bei der Betriebssystembereitstellung
- Praktische Alternative zur klassischen imagebasierten Bereitstellung
- Kontinuierliche Option für die automatisierte Bereitstellung von Apps, Konfigurationen und Benutzereinstellungen
- Komfortables Erlebnis für Endanwender bei neuen Geräten



# Windows Autopilot

## Einfacher Einstieg, schnelle Bereitstellung.

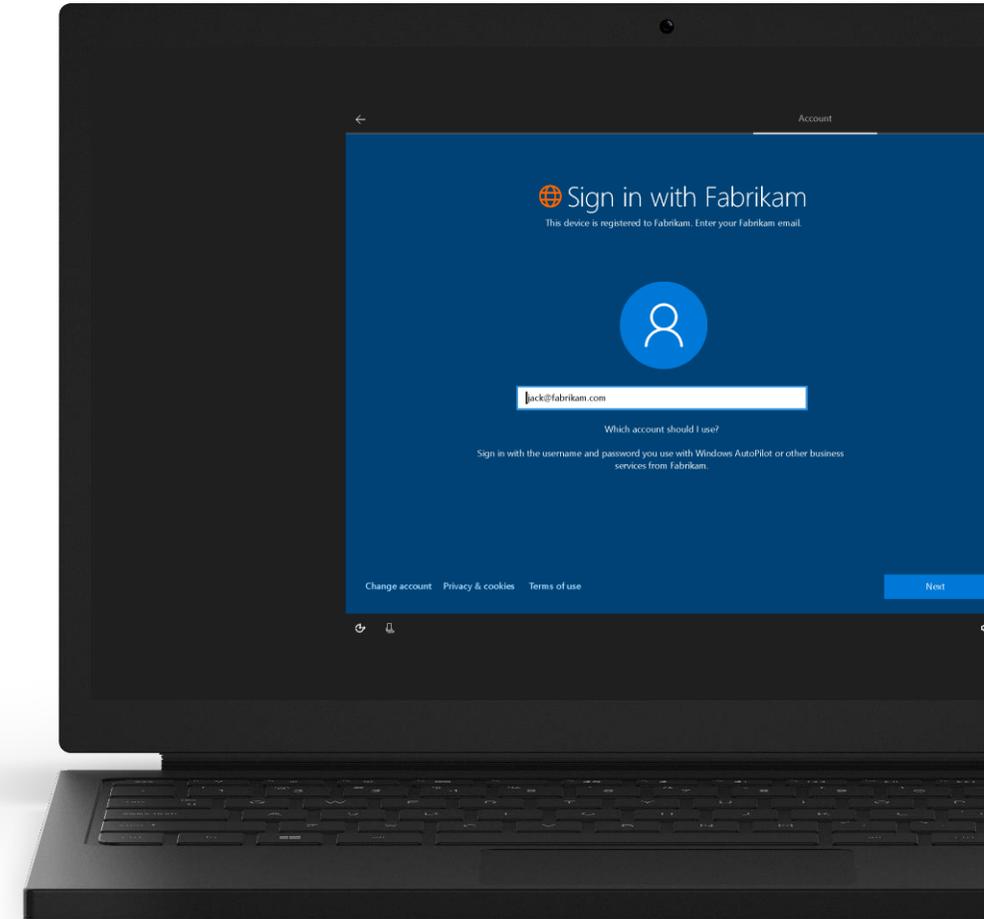
Neue Windows-Geräte können schnell und einfach aufgesetzt und eingerichtet werden. Sobald das Gerät eingeschaltet wird, sorgt Windows Autopilot über die Cloud für die richtige Konfiguration und Verwaltung – ohne Aufwand für Ihre IT-Mitarbeiter.

## 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.

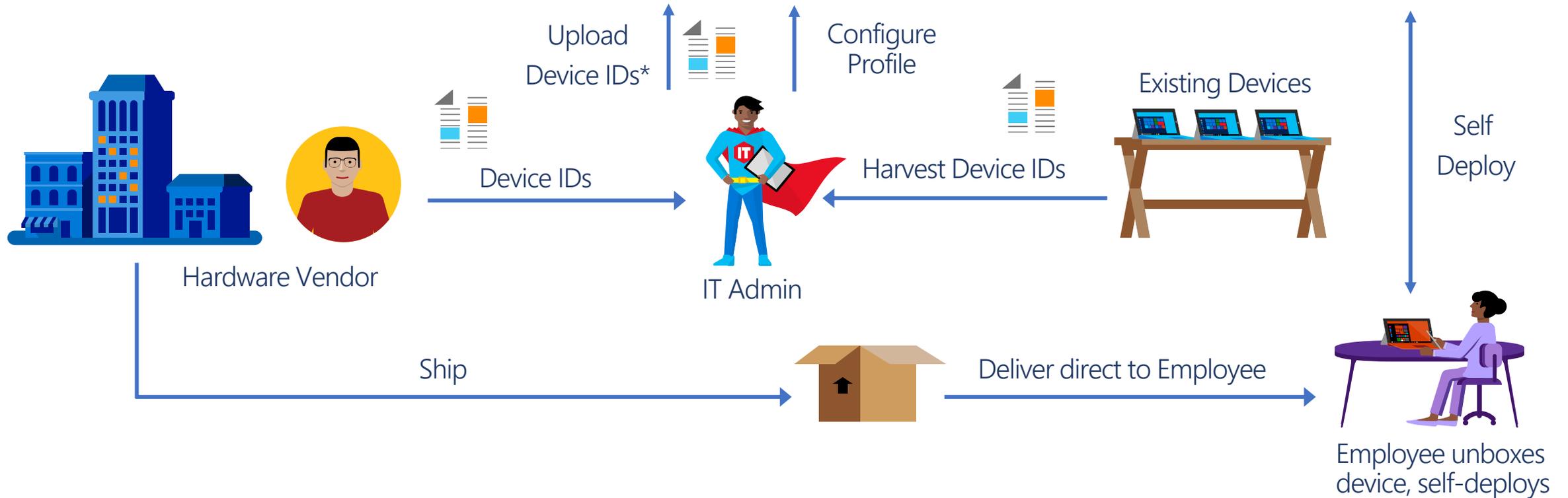
Windows Autopilot unterstützt die weitergehende Personalisierung durch den Nutzer. Office aus Office365 wird auf Wunsch installiert und aktiviert.





# 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>



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!