Microsoft

Microsoft 365 Copilot

Schaffen Sie Grundpfeiler für den Einsatz von Künstlicher Intelligenz im Unternehmen

Autoren:
Marina Valtchev (Business Lead M365 Usage)
Alexander Singer (Business Lead Secured Productivity)

Inhalt

Inhalt 2
Einleitung 3
Eine Moderne Sicherheitsarchitektur 6
Checkliste 11
Endpunkte zentral verwalten und schützen 13
Checkliste 17
Microsoft 365 im Überblick: Warum Kollaboration wichtig 19
Checkliste 22
Evergreen IT: Kommunikation mit Bordmitteln 23
Checkliste 26
Mit der passenden Change-Management-Strategie hohe Akzeptanz und Nutzung erreichen 27
Checkliste 28
Steigern Sie Ihre Produktivität mit Microsoft 365 Copilot 29
Checkliste 32
Weitere Ressourcen 33

Einleitung

Künstliche Intelligenz (KI) wird die Art und Weise verändern, wie Sie in ihrem Unternehmen arbeiten werden. Sie werden Zeit einsparen und effizienter sein, Sie werden vor allen Dingen aber auch ein hohes Maß an Arbeitsbelastung an die KI abgeben können. Doch vor dem Start sind ein paar wichtige Schritte vorab zu tätigen.

Dieses E-Book begleitet Sie daher auf dem Weg in die Cloud, denn zur Etablierung von KI in den Arbeitsalltag sind ein paar Hausaufgaben notwendig. Das klingt nach viel Arbeit, doch im Grunde handelt es sich um vier essenzielle Themen. Diese – und somit auch das E-Book – gliedern sich in drei technische Aspekte, sowie eine wichtige organisatorische Maßnahme. Gemeinsam werden wir je Kapitel eine dieser Maßnahmen betrachten und mit Hilfe einer Checkliste weitere Handlungsempfehlungen zum direkten Einsatz in Ihrem Unternehmen/ ihrer Organisation bereitstellen. Am Ende sind Sie somit nicht nur vorbereitet für den Einsatz von Künstlicher Intelligenz in Ihrem Unternehmen, sondern beginnen mit richtungsweisenden Veränderungsprozessen, die Ihr Unternehmen auf dem Weg in die neue Arbeitswelt begleiten.

Wird der Einsatz von Künstlicher Intelligenz im Unternehmen viel verändern? Oder reden wir hier eher über einen Trend, der gerade gehypt wird und dann irgendwann abflacht? Der Wechsel der Plattformen zu KI ist in vollem Gange. Und genauso wie wir Unternehmen bei der Umstellung auf remote und flexibles Arbeiten geholfen haben, wenden sich Kunden an Microsoft, um herauszufinden, wie diese neue Ära der KI die Arbeit noch einmal verändern wird.

Im Rahmen des Work Trend Index 2023 wurden 31.000 Menschen in 31 Ländern befragt und Billionen von Produktivitätsdaten in Microsoft 365 sowie Arbeitsmarkttrends auf LinkedIn analysiert, um zu verstehen, welchen Einfluss KI auf die Arbeitswelt hat. Die Daten zeichnen ein klares Bild: Tempo und Umfang der Arbeit haben exponentiell zugenommen, sodass die Mitarbeitenden mit einer höheren Arbeitslast zu kämpfen haben. Dies kann die Innovationskraft gefährden. Sowohl Führungskräfte als auch Mitarbeitende wünschen sich, dass KI ihnen diese Last abnimmt.

Neue Fähigkeiten für eine neue Art des Arbeitens

49 %

der Menschen haben Schwierigkeiten, Zeit und Energie zu finden, um ihre Arbeit zu erledigen

80 %

Der Führungskräfte sehen einen enormen Weiterbildungsbedarf der Mitarbeitenden zu KI

63 %

Anteil der Personen, die so viel wie möglich an KI delegieren würden, um ihre Arbeitsbelastung zu verringern

40 %

Der Arbeitnehmer haben Sorge, dass durch KI Ihre Arbeitsplätze in Gefahr geraten

Work trend Index Annual Report: Will AI Fix Work? Microsoft. 9 May 2023

Bereits heute haben mehr als die Hälfte der Mitarbeitenden Probleme, das Arbeitspensum in der vorgesehenen Zeit zu erfüllen. Wir alle haben digitale Lasten: Die Menge an Daten, E-Mails und Chats ist größer als unsere Fähigkeit, sie alle zu verarbeiten. Jede Minute, die wir mit der Verwaltung dieser Daten verbringen, ist eine Minute, die wir nicht für kreative Arbeit nutzen können. In einer Welt, in der Kreativität die neue Produktivität ist, ist diese digitale Last mehr als nur eine Unannehmlichkeit – sie wirkt sich auf das Geschäft aus. Genau hier kann KI helfen, doch wird dafür eine neue Allianz zwischen KI und Mitarbeitenden notwendig. Immerhin ist eines der vorherrschenden Argumente im Zusammenhang mit KI die Befürchtung, dass Beschäftigte dadurch ihren Arbeitsplatz verlieren könnten. Während 49 Prozent der Befragten Bedenken hinsichtlich der Arbeitsplatzsicherheit äußern, würden sich immer noch ganze 70 Prozent dafür entscheiden, so viel Arbeit wie möglich an eine KI zu delegieren, um ihre Arbeitsbelastung zu verringern. In Deutschland sind die Bedenken weniger stark als im weltweiten Durchschnitt. Dafür würden 63 Prozent ihre Arbeit an eine KI geben. Kurz gesagt: Für die Mitarbeitenden überwiegt das Versprechen der Entlastung die Bedenken. Sie können sich vorstellen, KI nicht nur für Verwaltungsaufgaben zu nutzen, sondern auch für analytische und kreative Arbeiten.

Künstliche Intelligenz wird zu einem völlig neuen Interaktionsmodell zwischen Menschen und Computern führen und schon bald werden wir uns die Arbeit ohne sie nicht mehr vorstellen können. Ein derartiger Plattformwechsel erfordert neue Qualifikationen – vom Prompt Engineering bis zur Neukonzeption von Arbeitsabläufen mit KI. 80 Prozent der deutschen Führungskräfte und 82 Prozent weltweit gehen davon aus, dass Mitarbeitende im KI-Zeitalter neue Fähigkeiten benötigen werden. Die Beschäftigten sind bereit für diese neue Aufgabe – das Erlernen neuer Fähigkeiten hat für sie oberste Priorität, wofür sie gerne mehr Zeit und Energie aufwenden würden. Auch Führungskräfte sind der Meinung, dass das Erlernen neuer Fähigkeiten die wichtigste Aufgabe ist, für die sie ihren Mitarbeitenden mehr Kapazitäten geben würden.

Sind Sie bereit, in die Ära der KI einzutreten? Hierzu können Sie sich schon jetzt folgende vier Fragen stellen:

- **Verfügen Sie über umfassende "Zero-Trust"-Architektur?**
- **Sind Ihre Endpunkte und Apps einfach zu verwalten?**
- **Sind Ihre Daten einheitlich und leicht zugänglich?**
- **Werden Change-Management und Evergreen Principals in Ihrem Unternehmen gelebt?**

Sie können alle diese Fragen mit „Ja“ beantworten? Super, dann ist Ihr Unternehmen gut aufgestellt für den Einsatz von künstlicher Intelligenz. Wenn nein, keine Sorge – lassen Sie uns in den folgenden Kapiteln gemeinsam daran arbeiten.

Eine Moderne Sicherheitsarchitektur

In der Vergangenheit haben Sie sich im Unternehmen vielleicht darauf konzentriert, den Netzwerkzugang mit Firewalls und virtuellen privaten Netzwerken (VPN) vor Ort zu schützen, in der Annahme, dass alles innerhalb des Netzwerks sicher sei. Heute jedoch, da die Daten nicht mehr nur vor Ort, sondern auch in der Cloud oder in hybriden Netzwerken gespeichert werden, hat sich das Zero-Trust-Sicherheitsmodell weiterentwickelt, um eine ganzheitlichere Reihe von Angriffsvektoren anzugehen.

Das Zero-Trust-Modell geht davon aus, dass nichts sicher ist – auch nicht hinter der Firmenfirewall. Deshalb prüft das Modell jede Anforderung so, als käme sie aus einem offen zugänglichen Netzwerk. Es gilt das Prinzip "Vertrauen ist gut, Kontrolle ist besser" – egal, woher die Anforderung stammt und auf welche Ressource sie abzielt. Bevor der Zugriff gewährt wird, muss eine Anforderung vollständig authentifiziert, autorisiert und verschlüsselt sein. Mikrosegmentierung und das Prinzip der geringstmöglichen Zugriffsrechte tragen dazu bei, die Ausbreitung im System einzudämmen. Hinzu kommen umfassende Business Intelligence und Analytics, um Anomalien in Echtzeit zu erkennen und abzuwehren.

Das Kernstück sind die drei Prinzipien:

Explizite Kontrollen

Prinzip der geringstmögliche Berechtigungen

Was tun Wenn...?

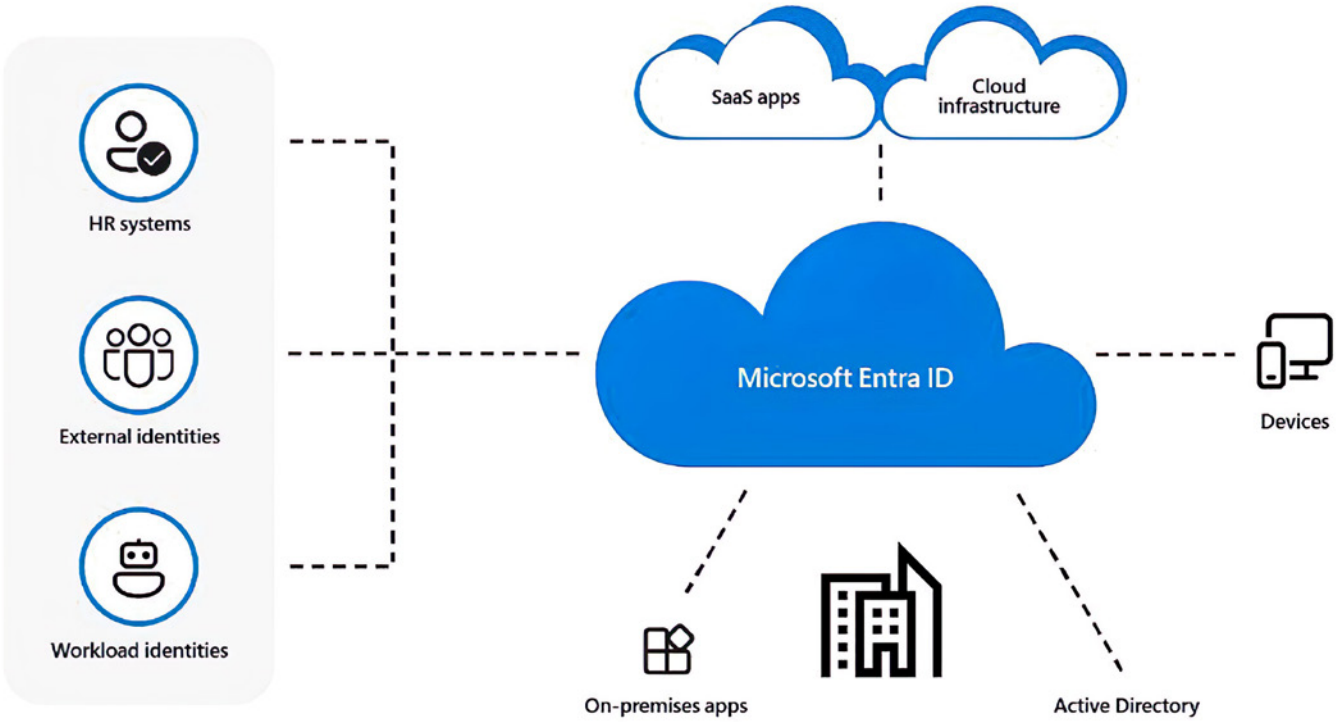
Zero-Trust-Prinzipien [Was ist Zero Trust? | Microsoft Learn]

Diese Prinzipien werden in einer umfassenden Kontrollebene angewendet, um mehrere Verteidigungsebenen zu schaffen. Ein ganzheitlicher Zero-Trust-Ansatz erstreckt sich auf die gesamte digitale Umgebung – einschließlich Identitäten, Endpunkten, Netzwerk, Daten, Anwendungen und Infrastruktur. Die Zero-Trust-Architektur, in der eine umfassende End-to-End-Strategie abgebildet ist, erfordert die Integration aller Elemente.

Identitäten sind die Grundlage der Zero-Trust-Sicherheit. Sowohl menschliche als auch nichtmenschliche Identitäten erfordern eine starke Autorisierung. Die Verbindung mit konformen Geräten erfolgt über persönliche oder firmeneigene Endpunkte, die den Zugriff beide auf der Grundlage strenger Richtlinien und bewährter Zero-Trust-Prinzipien anfordern: explizite Verifizierung, Zugriff mit den geringstmöglichen Berechtigungen und Assume Breach.

Microsoft Entra ID ist eine integrierte Identitäts- und Zugriffsverwaltungslösung in der Cloud und ein führender Verzeichnisdienst. Damit können Sie den Zugriff auf Anwendungen steuern und Identitäten schützen. Mit Microsoft Entra ID verwalten und schützen Unternehmen die Identitäten ihrer Beschäftigten, Partner und Kunden, um Zugriff auf die benötigten Anwendungen und Dienste zu gewähren. Microsoft Entra ID bietet eine Identitätslösung, die sich auf breiter Basis integrieren lässt – von lokalen Legacy-Anwendungen bis hin zu Tausenden führender SaaS-Anwendungen (Software-as-a-Service). So schaffen Sie ein nahtloses Endbenutzererlebnis mit verbesserter Transparenz und Steuerung.

[Cloud]-Identitäten als Grundlage der Zero-Trust-Strategie



https://www.microsoft.com/de-de/security/business/endpoint-management/microsoft-intune

Im Rahmen der durchgängigen Richtliniendurchsetzung fängt die Zero-Trust-Richtlinie die Anforderung ab, verifiziert auf der Grundlage der Richtlinienkonfiguration explizit Signale aus den sechs Grundkategorien und setzt den Zugriff mit den geringstmöglichen Berechtigungen durch. Die Signale beziehen sich auf die Benutzerrolle, den Standort, die Gerätekonformität sowie die Vertraulichkeit von Daten und Anwendungen. Zusätzlich zu den Telemetrie- und Statusinformationen fließt die Bedrohungsschutz-Risikobewertung in das Richtlinienmodul ein, um automatisch und in Echtzeit auf Bedrohungen zu reagieren. Die Richtlinie wird beim Zugriff durchgesetzt und während der gesamten Sitzung kontinuierlich ausgewertet.

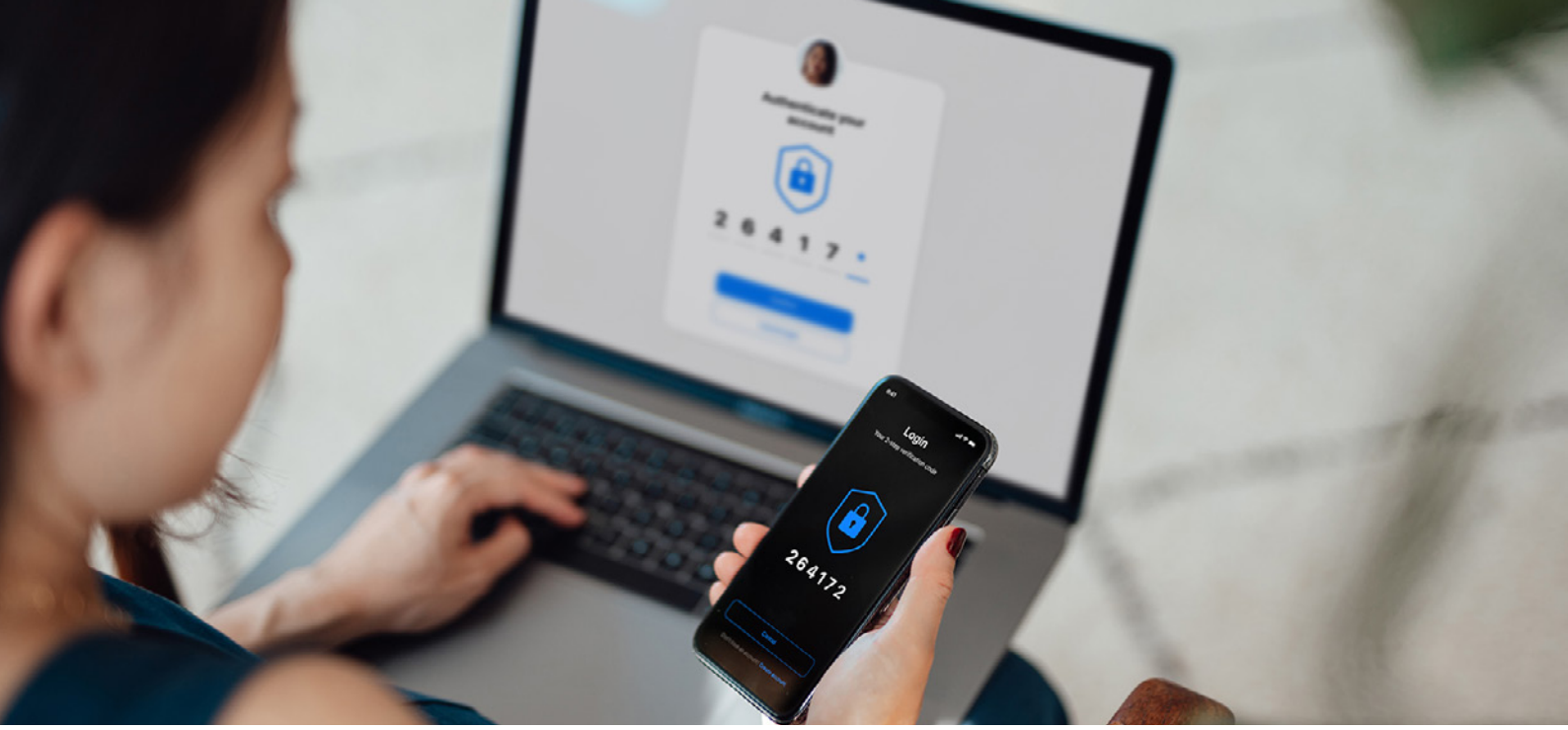
Außerdem wird die Richtlinie durch die Richtlinienoptimierung weiter verbessert. Governance und Compliance sind wichtig für eine erfolgreiche Zero-Trust-Implementierung. Die Bewertung des Sicherheitsstatus und die Produktivitätsoptimierung sind erforderlich, um die Telemetrie in allen Diensten und Systemen zu messen.

Die Telemetrie- und Analysedaten fließen in das Bedrohungsschutzsystem ein. Umfangreiche Telemetrie- und Analysedaten, die mit Threat Intelligence angereichert sind, generieren aussagekräftige Risikobewertungen, die entweder manuell untersucht oder automatisiert werden können. Angriffe erfolgen mit Cloudgeschwindigkeit. Dasselbe muss auch für die Verteidigungssysteme gelten, denn Menschen können nicht schnell genug reagieren bzw. alle Risiken erkennen. Die Risikobewertung fließt in das Richtlinienmodul ein und ermöglicht so den automatisierten Echtzeit-Bedrohungsschutz sowie bei Bedarf eine zusätzliche manuelle Untersuchung.

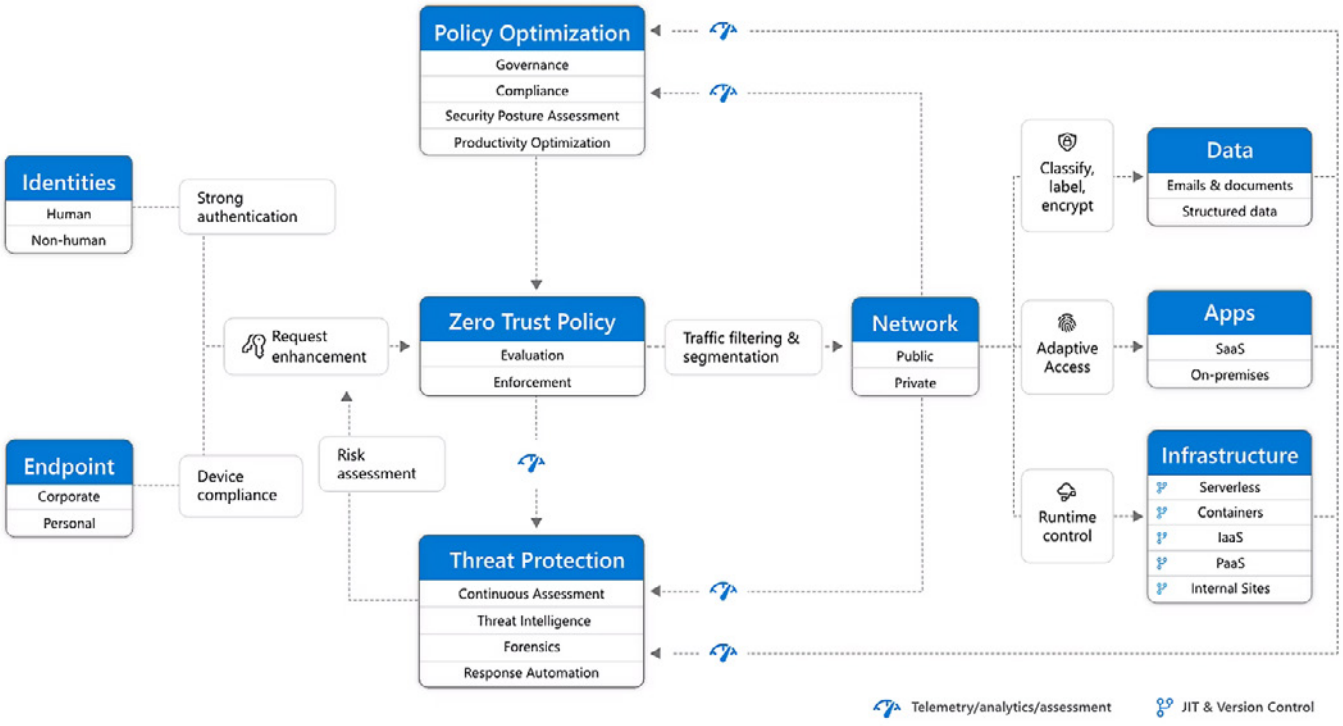
Vor der Evaluierung und Durchsetzung der Zero-Trust-Richtlinie findet die Filterung und Segmentierung des Datenverkehrs statt. Erst danach wird der Zugriff auf ein öffentliches oder privates Netzwerk gewährt.

Klassifizierung, Kennzeichnung und Verschlüsselung von Daten sollten auf E-Mails, Dokumente und strukturierte Daten angewendet werden. Der Zugriff auf Apps erfolgt adaptiv, sowohl bei SaaS- als auch bei lokalen Apps. Die Laufzeitsteuerung wirkt sich auf die Infrastruktur mit serverlosen, containerbasierten, IaaS-, PaaS- und internen Websites aus, wobei JIT (Just-in-Time) und Versionskontrolle aktiv eingesetzt werden.

Zum Schluss werden Telemetrie- und Analysedaten sowie Bewertungen aus dem Netzwerk, den Daten und Anwendungen sowie der Infrastruktur in die Richtlinienoptimierungs- und Bedrohungsschutzsysteme zurückgeführt.



Das Zero-Trust-Modell



Zero Trust Model - Modern Security Architecture | Microsoft Security

Eine Kernfunktion von Azure Active Directory besteht darin, Benutzer zu authentifizieren wenn sie sich bei Anwendungen oder Geräten anmelden. Um diese Anmeldevorgänge zu sichern, sollten Sie die ausschließliche Verwendung von Benutzername und Passwort überdenken. Azure AD Multi-Faktor-Authentifizierung deckt ab, wie man Benutzeranmeldungen sichert, Multi-Faktor-Authentifizierung bereitstellt, und Benutzern die Möglichkeit gibt, ihr eigenes Passwort zurückzusetzen.

Sichere Authentifizierungsmethoden wie z. B. Windows Hello, FIDO2-Sicherheitsschlüssel und die Microsoft Authenticator-App können Ihren Benutzern ein passwortloses Anmeldeerlebnis bieten. Diese starken und sicheren kennwortlosen Methoden reduzieren das Risiko von verschiedenen Arten von Angriffen gegen Ihre Organisation, wie Phishing oder Passwort-Spray.

Bei der Multi-Faktor-Authentifizierung wird ein Benutzer aufgefordert, eine zusätzliche Form der Identifizierung durchzuführen, nachdem er seine Anmeldedaten während einer Benutzeranmeldung eingegeben hat. Diese Anfrage nach einem zusätzlichen Authentifizierungsfaktor hilft, Benutzerkonten zu sichern, indem sie auf mehr als nur eine Methode der Identifizierung setzen. Wenn ein Benutzer sein Passwort vergisst, kann er sein Passwort per Selbstbedienung zurücksetzen. Mit einem beliebigen Webbrowser kann ein Benutzer eine Passwortänderung anfordern. Es besteht keine Notwendigkeit einen Helpdesk oder einen Administrator zu kontaktieren.

Dies spart Zeit und gibt Freiraum für andere Aufgaben. Nachdem ein Nutzer seine Identität mit einer verfügbaren Methode bestätigt hat, kann dieser ein neues Passwort erstellen und weiterarbeiten.

Zur Unterstützung Ihrer geschäftlichen Anforderungen, kann das Zurücksetzen der Passwörter so konfiguriert werden, dass die Änderungen in der Cloud auch direkt in Ihre On-Premise-Umgebung zurückgeschrieben werden.

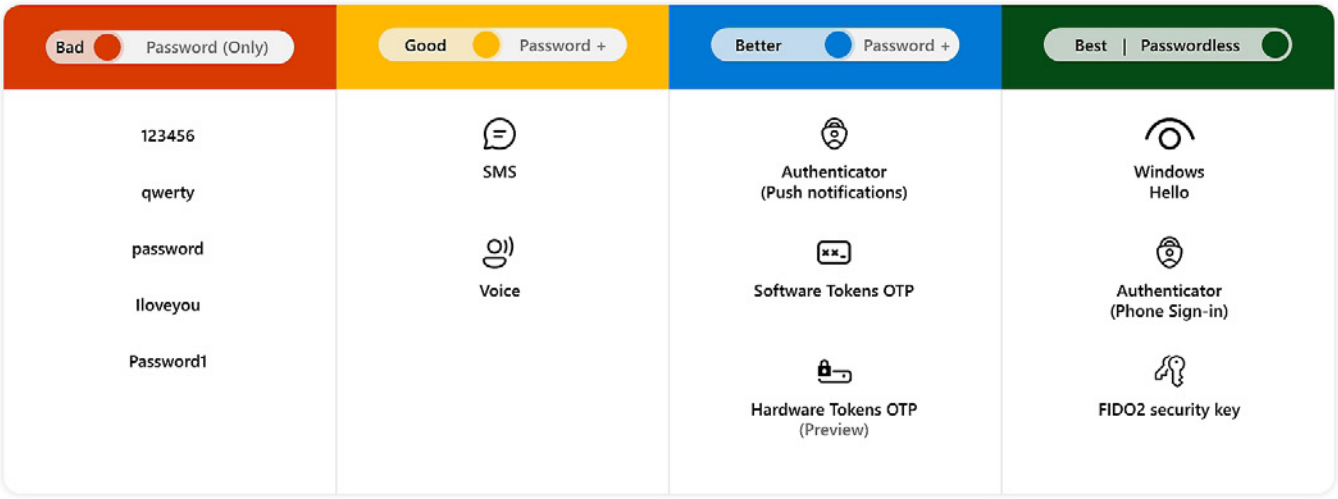
Azure AD-Authentifizierung umfasst darüber hinaus einen Passwortschutz um starke, komplexe Passwörter zu verlangen. Der Kennwortschutz kann auch in einer lokalen Umgebung integriert werden. Unabhängig davon, wo ein Benutzer sein Passwort ändert, sind Identitäten so immer mit dem Azure AD-Kennwortschutz geschützt.

Die Kombination aus Benutzername und Passwort ist in vielen Institutionen noch Standard, um sich bei Netzwerkressourcen anzumelden. Doch die Erfahrung zeigt, dass gerade dieses Sicherheitsverfahren besonders anfällig für Cyberangriffe ist – Stichwort Identitätsdiebstahl. Windows Hello for Business ist ein Sicherheitsfeature, das Ihren Mitarbeiter*innen ermöglicht, ihr Gerät per Gesichtserkennung (Kamera), PIN oder Fingerabdruck zu entsperren. Die Aktivierung von Windows Hello vereinfacht und beschleunigt das Anmelden bei einem Gerät, und es arbeitet nahtlos mit zahlreichen kompatiblen Anwendungen zusammen.

Mit Microsoft Authenticator erhalten die Smartphones Ihrer Nutzer*innen neben ihrer PIN, der Gesichtserkennung oder einem Fingerabdruck einen weiteren Sicherheitsmechanismus. Die Microsoft Authenticator-App unterstützt auch den Industriestandard für zeitbasierte, einmalige Kennungen (auch als TOTP oder OTP bezeichnet), sodass Sie in die Microsoft Authenticator-App weitere Online-Konten einbinden können, die diesen Standard unterstützen.

Funktionen wie die Multi-Faktor-Authentifizierung können die Sicherheit von Unternehmen stärken. Häufig sind die Benutzer jedoch unzufrieden, weil sie sich Kennwörter trotz dieser zusätzlichen Sicherheitsebene merken müssen. Die kennwortlose Authentifizierung ist besonders komfortabel, weil man sich keine Kennwörter merken muss und die Methoden mit den meisten Geräten und Systemen kompatibel sind. Darüber hinaus schiebt sie Phishing praktisch endgültig den Riegel vor.

Vergleich: Sicherheitsniveau von Authentifizierungsmöglichkeiten



https://cdn-dynmedia-1.microsoft.com/is/image/microsoftcorp/image_RE529lh?resMode=sharp2&op_usm=1.5,0.65,15,0&wid=3200&hei=1500&qlt=100&fmt=png-alpha&fit=constrain

Leistungsstarke Werkzeuge für Identitäts- und Zugriffsverwaltung ermöglichen Ihnen, die Identitäten Ihrer Nutzer*innen zu schützen und den Zugang zu wichtigen Ressourcen je nach Risikoniveau durch den bedingten Zugriff zu kontrollieren. Hiermit schaffen Sie ein elementares Grundgerüst für den Einsatz von Copilot in Ihrem Unternehmen.

Checkliste Kurzfristige Bereitstellungsziele

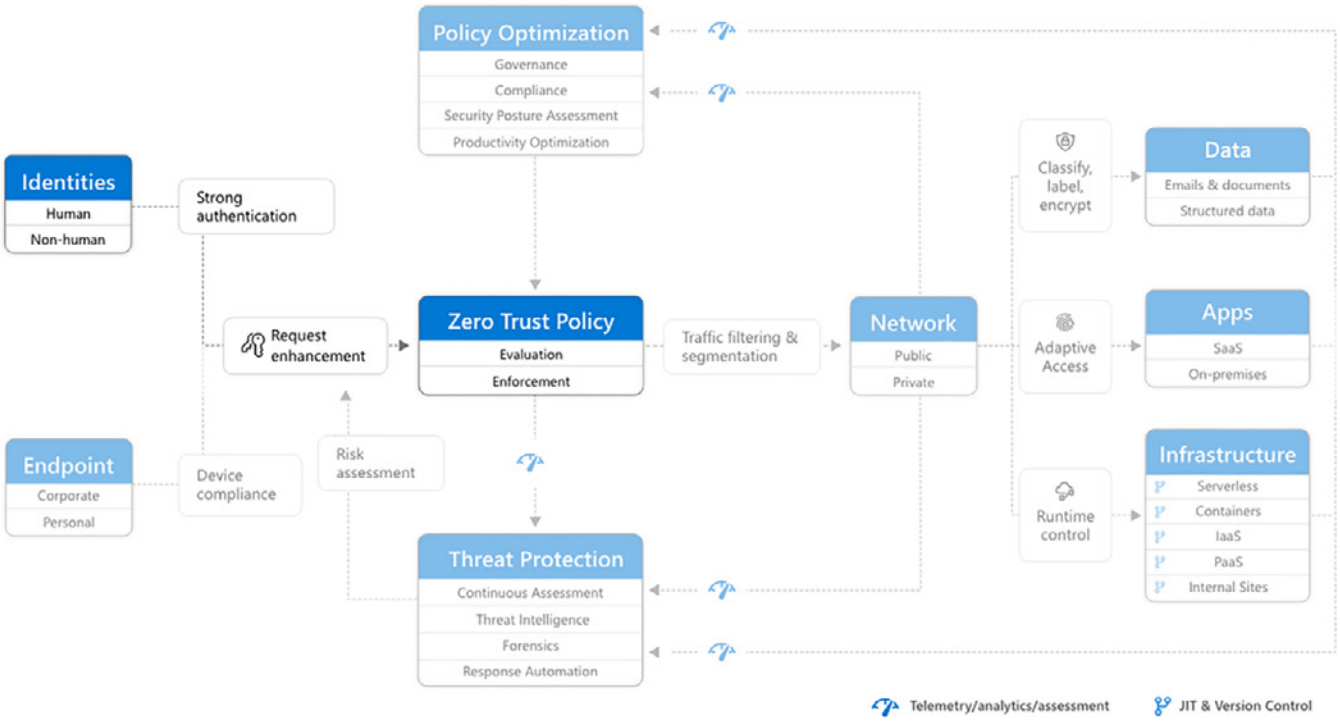
Erfüllen Sie diese Bereitstellungsziele, um Ihre privilegierten Identitäten mit Zero Trust zu schützen:

1. Stellen Sie sicheren privilegierten Zugriff bereit, um Administratorbenutzerkonten zu schützen.
2. Stellen Sie Azure AD Privileged Identity Management (PIM) für einen zeitgebundenen Just-in-Time-Genehmigungsprozess für die Verwendung privilegierter Benutzerkonten bereit.

Erfüllen Sie diese Bereitstellungsziele, um Ihre Benutzeridentitäten mit Zero Trust zu schützen:

1. Aktivieren sie die Self-Service-Kennwortzurücksetzung (Self-Service Password Reset, SSPR), die Ihnen Funktionen zum Zurücksetzen von Anmeldeinformationen bietet
2. Aktivieren Sie Multi-Factor-Authentication (MFA), und wählen Sie die geeigneten Methoden für MFA aus.
3. Aktivieren Sie die kombinierte Benutzerregistrierung für Ihr Verzeichnis, damit Benutzer sich in einem Schritt für SSPR und MFA registrieren können.
4. Konfigurieren Sie eine Richtlinie für bedingten Zugriff, um die MFA-Registrierung zu erfordern.
5. Aktivieren Sie risikobasierte Benutzer- und Anmelderichtlinien, um den Benutzerzugriff auf Ressourcen zu schützen.
6. Erkennen und blockieren Sie bekannte schwache Kennwörter und deren Varianten und blockieren Sie zusätzliche schwache Begriffe, die für Ihre Organisation spezifisch sind.
7. Stellen Sie Microsoft Defender for Identity bereit, überprüfen und minimieren Sie alle geöffneten Warnungen (parallel zu Ihren Sicherheitsvorgängen).
8. Stellen Sie kennwortlose Anmeldeinformationen bereit.

Sie haben nun den Abschnitt Identitäten der Zero Trust Architektur erstellt



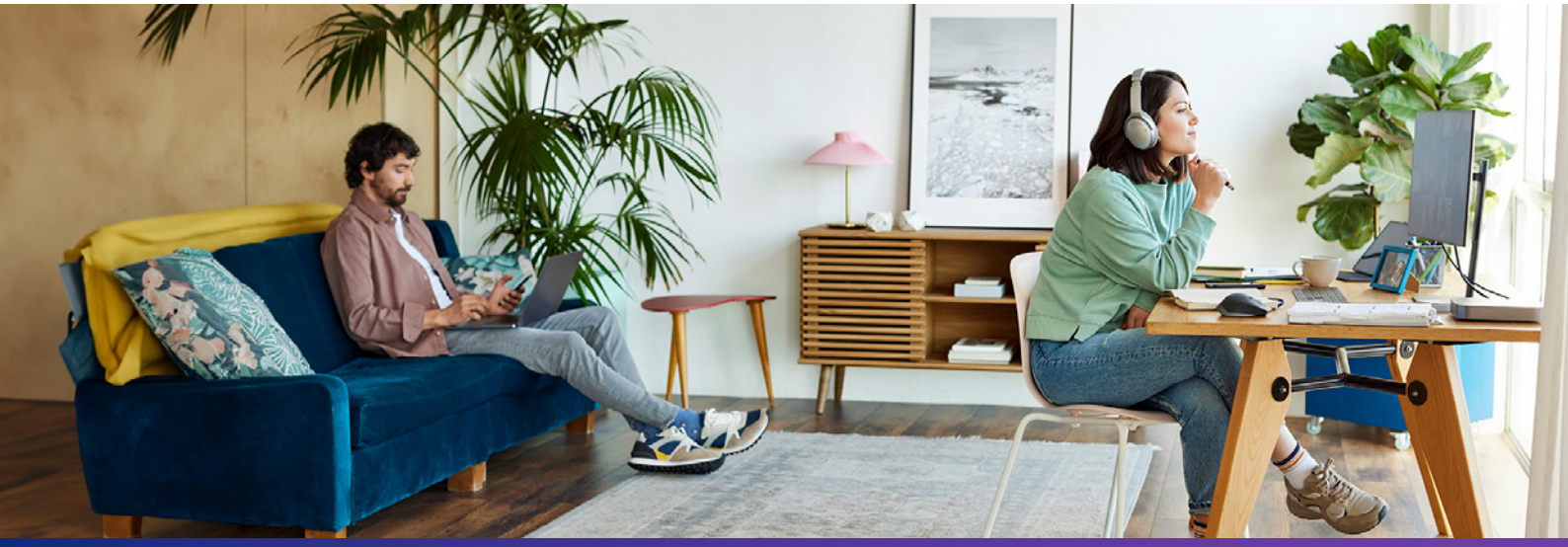
[RaMP-Checkliste – Explizite Überprüfung der Vertrauensstellung für alle Zugriffsanforderungen | Microsoft Learn]

Endpunkte zentral verwalten und schützen

Der heutige Arbeitsplatz spiegelt die jüngsten gesellschaftlichen Veränderungen wider, bei denen hybride und dezentrale Arbeitsformen zur Norm geworden sind.

Die Mitarbeitenden müssen in der Lage sein, überall und jederzeit zu arbeiten. Dies stellt die IT-Verantwortlichen vor neue Herausforderungen, wenn es um die Verwaltung von Endgeräten geht. Die Kosten im Griff zu behalten und gleichzeitig die Sicherheit in dieser komplexen Umgebung zu gewährleisten, birgt Hindernisse. Verschärft wird die Situation dadurch, dass die IT-Abteilung häufig auf einen Flickenteppich von Sicherheitslösungen angewiesen ist, die teuer sein können und ein unzureichendes Sicherheitsniveau bieten. Wie können wir sicherstellen, dass unsere Endgeräte immer auf dem neuesten Stand, sicher und leistungsfähig sind? Wie können wir den Zugriff auf unsere Apps und Daten auf unseren Endgeräten kontrollieren? Wie können wir unsere Endgeräte an verschiedene Arbeitsmodelle und Szenarien anpassen? Und wie können wir die Vorteile von Künstlicher Intelligenz (KI) nutzen, ohne ihre Risiken zu ignorieren?

Die Antwort auf diese Fragen ist Intune, eine cloudbasierte Endpunktverwaltungslösung von Microsoft. Intune hilft uns, unsere Benutzer, Apps und Daten auf unseren vielen Endgeräten zu schützen und zu steuern. Als eine cloudbasierte Lösung, wird keine zusätzliche Hardware oder Software erfordert. Sie können Intune über ein Webportal oder eine mobile App verwalten. Intune ermöglicht es, den Benutzerzugriff und die App- und Geräteverwaltung auf Endgeräten zu vereinfachen. Sie können den Zugriff und die Daten auf organisationseigenen und persönlichen Geräten schützen. Außerdem verfügt Intune über Kompatibilitäts- und Berichterstellungsfeatures, die das Zero Trust Sicherheitsmodell unterstützen.



Microsoft Intune

Was bedeutet Geräteverwaltung?

Welche Geräte und Szenarien kann man mit Intune managen?

Intune unterstützt verschiedene Betriebssysteme wie Windows, Mac, iOS/iPadOS, Android und Linux. Wir können diese Endgeräte verwenden, um mit erstellten Richtlinien sicher auf organisationseigene Ressourcen zuzugreifen. Es ermöglicht Ihnen, verschiedene Szenarien mit unseren Endgeräten zu managen:

- **Hybride Arbeitsmodelle:** Viele Mitarbeitende arbeiten heute teils im Büro, teils zu Hause oder mobil von unterwegs. Dies erfordert eine flexible und sichere Endpunktverwaltung. Mit Intune können Sie Ihre Endgeräte remote einrichten, aktualisieren und unterstützen.

- **Spezielle und gemeinsam genutzte Geräte:** Einige Mitarbeitende verwenden spezielle oder gemeinsam genutzte Geräte für ihre Arbeit in Service und Produktion. Diese Geräte müssen oft bestimmte Anforderungen erfüllen oder eingeschränkt werden. Mit Intune können Sie diese Geräte konfigurieren, sperren und warten.

- **Bring Your Own Device (BYOD):** Einige Mitarbeitende verwenden ihre eigenen Geräte für die Arbeit. Dies bietet ihnen mehr Komfort und Flexibilität, aber auch mehr Verantwortung für ihre Daten. Mit Intune können Sie den Zugriff auf Apps und Daten auf diesen Geräten beschränken oder löschen.

Was sind die wichtigsten Funktionen von Intune?

Intune bietet viele Funktionen für eine effektive Endpunktverwaltung, wie zum Beispiel:

- **Plattformübergreifende Endpunktverwaltung:** Sie können Endpunkte verwalten, die lokal, virtuell, in der Cloud sowie auf Mobilgeräten und dem Desktop eingesetzt werden.

- **Verwaltung mobiler Anwendungen:** Sie können Apps bereitstellen, aktualisieren und entfernen. Sie können auch eine Verbindung mit Apps aus privaten App-Stores herstellen und diese verteilen, Microsoft 365-Apps aktivieren, Win32-Apps bereitstellen, App-Schutzrichtlinien erstellen und den Zugriff auf Apps und deren Daten verwalten.

- **Endpunktanalysen:** Sie können Einblicke in den Gesundheits-, Compliance- und Sicherheits status unserer Endpunkte erhalten. Sie können auch proaktive Empfehlungen basierend auf Microsoft Cloud-Daten erhalten.

- **Integration:** Sie können Intune mit anderen Microsoft-Diensten und -Apps wie Microsoft Entra ID (ehmals Azure AD), Microsoft Defender for Endpoint (MDE) und Microsoft 365 integrieren.

Warum ist Intune mehr als nur Endgeräteverwaltung?

Intune ist mehr als nur Endgeräteverwaltung, weil es nicht nur hilft, Geräte zu konfigurieren und zu verwalten, sondern auch die Benutzer, Apps und Daten. Das besondere an Intune sind u. a. folgende Merkmale:

- **Benutzeridentitäten verwalten und authentifizieren.** Sie können Azure AD verwenden, um Single Sign-On (SSO), Multi-Factor Authentication (MFA) und Self-Service Password Reset (SSPR) zu ermöglichen.

- **Apps schützen und steuern.** Sie können App-Schutzrichtlinien verwenden, um Daten auf App-Ebene zu verschlüsseln, zu isolieren und zu löschen. Sie können auch App-Konfigurationsrichtlinien verwenden, um App-Einstellungen anzupassen.

- **Daten sichern und überwachen.** Sie können MDE verwenden, um Datenverluste zu verhindern, Datenlecks zu erkennen und auf Vorfälle zu reagieren. Sie können auch Audits und Berichte erstellen, um die Einhaltung von Vorschriften zu gewährleisten.

- **Cloud-nativ:** Intune ist eine cloudbasierte Lösung, die Ihnen unbegrenzte Skalierbarkeit und Flexibilität bietet. Sie müssen sich keine Sorgen um die Installation oder Wartung von zusätzlicher Hardware oder Software machen.

- **Künstliche Intelligenz:** Intune nutzt KI, um Bedrohungen zu erkennen und zu verhindern. Sie können auch KI-gestützte Automatisierungsfunktionen nutzen, um Ihre Endpunktverwaltung zu optimieren.

- **Zero Trust:** Intune unterstützt das Zero Trust Sicherheitsmodell, das davon ausgeht, dass kein Benutzer oder Gerät vertrauenswürdig ist. Sie können identitätsbasierte Gerätecompliance und bedingten Zugriff anwenden, um unsere Daten zu schützen.

Warum ist eine Endgeräteverwaltung so wichtig im Zeitalter von KI?

Eine Endgeräteverwaltung ist besonders wichtig im Zeitalter von KI, denn:

- KI ermöglicht neue Möglichkeiten für Innovation und Produktivität, aber auch für Cyberangriffe. KI kann sowohl von Angreifern als auch von Verteidigern genutzt werden, um ihre Ziele zu erreichen. Eine Endgeräteverwaltung hilft, Geräte vor KI-basierten Bedrohungen zu schützen und KI-basierte Abwehrmaßnahmen zu nutzen.

- KI erfordert eine hohe Rechenleistung und Datenmenge, die Geräte belasten können. KI-Anwendungen können Geräte verlangsamen, überhitzen oder beschädigen. Eine Endgeräteverwaltung hilft uns, Geräte zu optimieren, zu aktualisieren und zu warten.

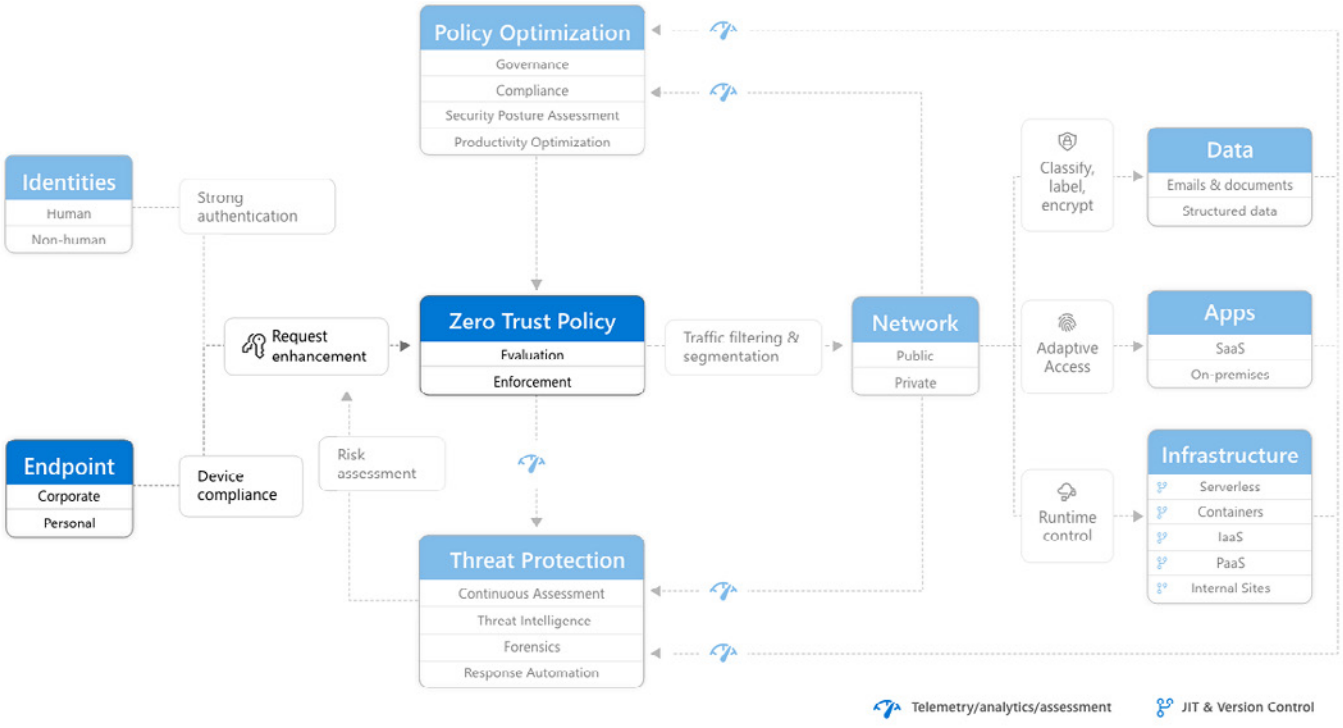
- KI erzeugt ethische und rechtliche Herausforderungen, die Geräte betreffen können. KI-Anwendungen können die Privatsphäre verletzen, Diskriminierung fördern oder Gesetze brechen. Eine Endgeräteverwaltung hilft, Geräte zu überwachen, zu auditieren und zu regulieren.

Checkliste

Erfüllen Sie diese Bereitstellungsziele, um Ihre Endpunkte (Geräte) mit Zero Trust zu schützen:

1. Registrieren Sie Ihr Gerät / Ihre Geräte bei Entra ID.
2. Registrieren Sie Ihr Geräte / Ihre Geräte, und erstellen Sie Konfigurationsprofile.
3. Verbinden Sie Defender für Endpunkt mit Intune (parallel zu Ihren Sicherheitsvorgängen).
4. Überwachen sie die Gerätekonformität und das Risiko für bedingten Zugriff.
5. Implementieren Sie Microsoft Information Protection und integrieren Sie sie in Richtlinien für bedingten Zugriff.

Sie haben nun den Abschnitt Endpunkte der Zero Trust-Architektur erstellt

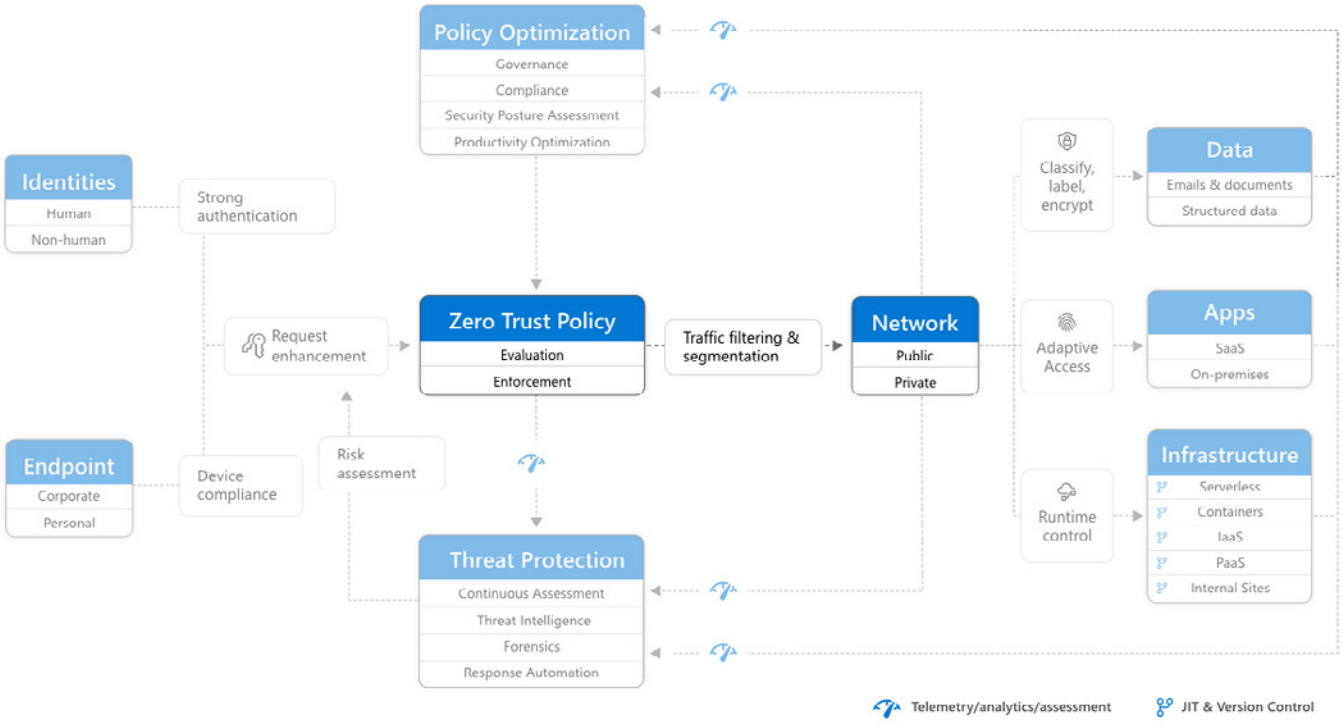


RaMP-Checkliste – Explizite Überprüfung der Vertrauensstellung für alle Zugriffsanforderungen | Microsoft Learn

Erfüllen Sie diese Bereitstellungsziele, um Zero Trust Schutz für Ihre öffentlichen und privaten Netzwerke sowohl für lokalen als auch für cloudbasierten Datenverkehr sicherzustellen. Diese Ziele können parallel durchgeführt werden.

1. Erfordern Sie eine Verschlüsselung für alle Datenverkehrsverbindungen, einschließlich zwischen IaaS-Komponenten und zwischen lokalen Benutzern und Apps.
2. Beschränken Sie den Zugriff auf kritische Daten und Anwendungen durch Richtlinie (Benutzer- oder Geräteidentität) oder Datenverkehrsfilterung.
3. Stellen Sie die lokale Netzwerksegmentierung mit Steuerungen für eingehenden und ausgehenden Datenverkehr mit Mikroperimetern und Mikrosegmentierung bereit.
4. Verwenden Sie die Echtzeit-Bedrohungserkennung für lokalen Datenverkehr.
5. Bereitstellen der Cloudnetzwerksegmentierung mit Steuerungen für eingehenden und ausgehenden Datenverkehr mit Mikroperimetern und Mikrosegmentierung.
6. Verwenden Sie die Echtzeit-Bedrohungserkennung für Clouddatenverkehr.

Nachdem Sie diese Bereitstellungsziele abgeschlossen haben, haben Sie den Abschnitt Netzwerk der Zero Trust-Architektur erstellt



RaMP-Checkliste – Explizite Überprüfung der Vertrauensstellung für alle Zugriffsanforderungen | Microsoft Learn

Microsoft 365 im Überblick: Warum Kollaboration wichtig ist

Microsoft 365 ist eine Cloud-basierte Plattform, die Unternehmen dabei unterstützt, ihre Produktivität, Kommunikation und Zufriedenheit zu steigern. So können Mitarbeitende flexibel von überall arbeiten, ohne dabei an Sicherheit oder Qualität einzubüßen. In diesem Kapitel werden wir erklären, warum Kollaboration ein wesentlicher Faktor für den Unternehmenserfolg ist und wie Microsoft 365 und Teams dies ermöglichen.

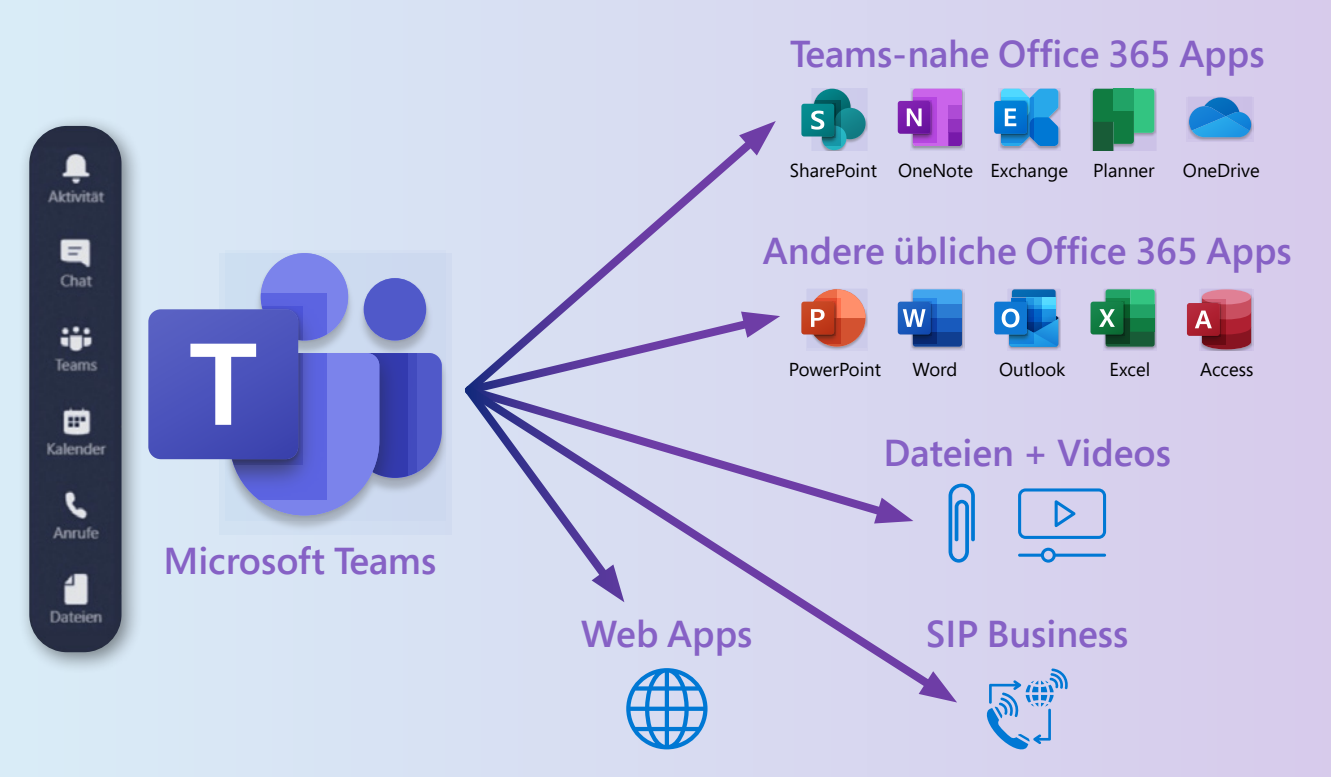
Flexibilität des Arbeitsplatzes und -ortes ist ein unverzichtbarer Treiber des heutigen und zukünftigen Arbeitens, der auch die Intelligenz fördert. Die Pandemie hat gezeigt, dass viele Mitarbeitende in der Lage sind, effektiv von zu Hause oder anderen Orten zu arbeiten, solange sie die richtigen Werkzeuge und Anleitungen haben. Laut einer Studie von Microsoft möchten 73% der Mitarbeitenden auch nach der Pandemie flexibel arbeiten können. Außerdem würden 41% der Mitarbeitenden sogar den Arbeitgeber wechseln, wenn dieser ihnen keine Flexibilität bieten würde. Flexibles Arbeiten bietet nicht nur Vorteile für die Mitarbeitende, sondern auch für die Arbeitgeber. So können sie Kosten sparen, Talente anziehen und halten, die Vielfalt fördern und die Umwelt schonen.

Flexibles Arbeiten erfordert jedoch auch eine Anpassung der Arbeitsweise. Dabei spielen zwei Begriffe eine wichtige Rolle: synchrones und asynchrones Arbeiten. Synchrones Arbeiten bedeutet, dass die Mitarbeitenden zur gleichen Zeit miteinander kommunizieren und zusammenarbeiten, zum Beispiel in einem Meeting oder einem Chat. Asynchrones Arbeiten bedeutet, dass die Mitarbeitenden unabhängig voneinander arbeiten und sich später austauschen, zum Beispiel über E-Mail oder ein Dokument. Beide Formen haben ihre Vor- und Nachteile. Synchrones Arbeiten ermöglicht eine schnellere Abstimmung und eine stärkere Bindung, kann aber auch zu Unterbrechungen und Stress führen. Asynchrones Arbeiten ermöglicht eine höhere Autonomie und Flexibilität, kann aber auch zu Missverständnissen und Isolation führen. Die folgende Tabelle zeigt einige Unterschiede zwischen synchronem und asynchronem Arbeiten:

Synchrones Arbeiten	Asynchrones Arbeiten
Zur gleichen Zeit	Zu unterschiedlichen Zeiten
Direkte Kommunikation	Indirekte Kommunikation
Hohe Koordination	Geringe Koordination
Schnelle Rückmeldung	Verzögerte Rückmeldung
Hohe Bindung	Hohe Autonomie

Um flexibel arbeiten zu können, müssen die Mitarbeitenden in der Lage sein, sowohl synchron als auch asynchron zu arbeiten. Dabei müssen sie einige Faktoren berücksichtigen, wie zum Beispiel den Zweck, die Dringlichkeit, die Komplexität und die Präferenz der Kommunikation oder Zusammenarbeit. Außerdem müssen sie klare Erwartungen, Regeln und Grenzen festlegen, um eine gesunde Balance zwischen Arbeit und Privatleben zu finden.

Microsoft Teams: Übersicht von Funktionen



Erfahren Sie mehr über Microsoft Teams: Videokonferenzen, Besprechungen, Anrufe | Microsoft Teams

Um die Mitarbeitenden bei der flexiblen Kommunikation und Zusammenarbeit zu unterstützen, bietet Microsoft 365 eine Cloud-basierte Plattform an, die verschiedene Funktionen und Anwendungen integriert. Die zentrale Drehscheibe dieser Plattform ist Teams, eine Anwendung, die Chats, Besprechungen abhalten, telefonieren, Dateien teilen und gemeinsam bearbeiten ermöglicht. Mit Teams können Mitarbeitende nahtlos zwischen synchronem und asynchronem Arbeiten wechseln, ohne dabei Teams als zentrale Plattform im Arbeitsalltag verlassen zu müssen. Neben den Kernbereichen von Teams haben die Mitarbeitenden auch Zugriff auf ihre gewohnten Produktivitätswerkzeuge wie Word, Excel oder PowerPoint direkt in Teams und voll integriert. So können sie gemeinsam an Projekten und Dokumenten arbeiten und sich von überall aus beteiligen. Außerdem können sie auch Geschäftsprozesse oder eigene Apps in Teams integrieren, um ihre

Arbeitsabläufe zu optimieren. Teams bietet somit eine einheitliche und vielseitige Plattform für Kollaboration, die die Produktivität, Kommunikation und Zufriedenheit der Mitarbeitenden erhöht.

Als cloudbasierte Plattform bietet Microsoft 365 viel mehr als man vielleicht denkt. So kann nicht nur mit den bekannten Produktivitätsanwendungen wie Word, Excel oder PowerPoint gearbeitet werden, sondern auch von intelligenten Cloud-Diensten profitiert werden, die Sicherheit, Verwaltung und Zusammenarbeit verbessern. Einer dieser Cloud-Dienste ist Copilot, Ihr künstlicher Intelligenz-Assistent für die Arbeit. Copilot kann helfen, schneller und einfacher Aufgaben zu erledigen, indem er relevante Informationen, Vorschläge und Aktionen anbietet. Sie können Copilot einfach per Sprache oder Text in Microsoft Teams oder anderen Microsoft 365 Apps aktivieren und ihm Fragen stellen oder Anweisungen geben. Zum Beispiel können Sie Copilot bitten, eine Präsentation zu erstellen, eine E-Mail zu schreiben oder eine Besprechung zu planen. Copilot versteht Ihre Absicht und liefert passende Ergebnisse oder führt die gewünschte Aktion aus.

Um diese intelligenten Antworten und Aktionen zu bieten, nutzt Copilot den Semantic Index, eine fortschrittliche Karte Ihrer individuellen und unternehmensbezogenen Daten. Der Semantic Index versteht die Bedeutung und den Zusammenhang der Daten und kann sie mit Ihren Anfragen abgleichen. Zum Beispiel, wenn Sie Copilot nach dem "März-Umsatzbericht" fragen, sucht er nicht einfach nach Dokumenten mit diesen Wörtern im Dateinamen oder im Text. Stattdessen versteht er, dass "Umsatzberichte von Kelly aus dem Finanzteam erstellt und in Excel gespeichert werden". Und er nutzt dieses konzeptuelle Verständnis, um Ihre Absicht zu bestimmen und für Sie das zu finden, was Sie brauchen.

Der Semantic Index ist nicht nur für Copilot wichtig, sondern auch für die allgemeine Suche in Microsoft 365. Er verbessert die Suchergebnisse für Microsoft 365 E3 und E5 Kunden – egal, ob sie Copilot nutzen oder nicht. Mit dem Semantic Index können Sie schneller und einfacher auf Daten zugreifen und sie nutzen.

Im Vergleich zu einer On-Premise-Lösung bietet Ihnen Microsoft 365 viele Vorteile. Sie müssen keine teure Hardware, Installation oder Softwarelizenzen kaufen oder verwalten. Sie können von überall aus auf Daten und Anwendungen zugreifen und sie mit anderen teilen. Sie profitieren von regelmäßigen Updates und Innovationen ohne zusätzliche Kosten. Und Sie haben Zugriff auf fortschrittliche Sicherheits- und Compliance-Funktionen, die Ihre Daten schützen.

Microsoft 365 ist also mehr als nur Office 365 in der Cloud. Es ist eine integrierte Plattform, die hilft, produktiver, kreativer und sicherer zu arbeiten – mit Copilot als Ihrem persönlichen Assistenten.

Checkliste

- Prüfen Sie die Grundvoraussetzungen für Microsoft 365, wie z. B. die Netzwerkverbindung, die Gerätekompatibilität, die Lizenzierung und die Sicherheitsanforderungen.
- Definieren Sie Ihre Vision und Strategie für die digitale Transformation mit Microsoft 365. Was sind Ihre Geschäftsziele und wie können Sie diese mit Microsoft 365 erreichen?
- Erstellen Sie einen Projektplan für die Einführung von Microsoft 365. Legen Sie den Umfang, den Zeitplan, das Budget, die Rollen und Verantwortlichkeiten, die Kommunikation und das Change Management fest.
- Wählen Sie die geeigneten Microsoft 365 Apps und Dienste aus, die Sie in Ihrer Organisation nutzen möchten. Zum Beispiel Teams, SharePoint, OneDrive, Outlook, Word, Excel, PowerPoint, Copilot usw.
- Konfigurieren Sie Ihre Microsoft 365 Umgebung und migrieren Sie Ihre bestehenden Daten und Anwendungen in die Cloud. Nutzen Sie die verfügbaren Tools und Ressourcen von Microsoft, um Ihnen bei diesem Prozess zu helfen.
- Schulen Sie Ihre Mitarbeitenden in der Nutzung von Microsoft 365. Bieten Sie ihnen verschiedene Lernformate an, wie z. B. Online-Kurse, Webinare, Videos, Handbücher oder persönliche Workshops. Ermutigen Sie sie, Fragen zu stellen und Feedback zu geben.
- Messen Sie den Erfolg Ihrer Microsoft 365-Einführung. Verwenden Sie quantitative und qualitative Indikatoren, um den Nutzen, die Akzeptanz und die Zufriedenheit Ihrer Mitarbeitenden zu bewerten. Identifizieren Sie mögliche Verbesserungsbereiche und passen Sie Ihre Strategie entsprechend an.

Evergreen IT: Kommunikation mit Bordmitteln

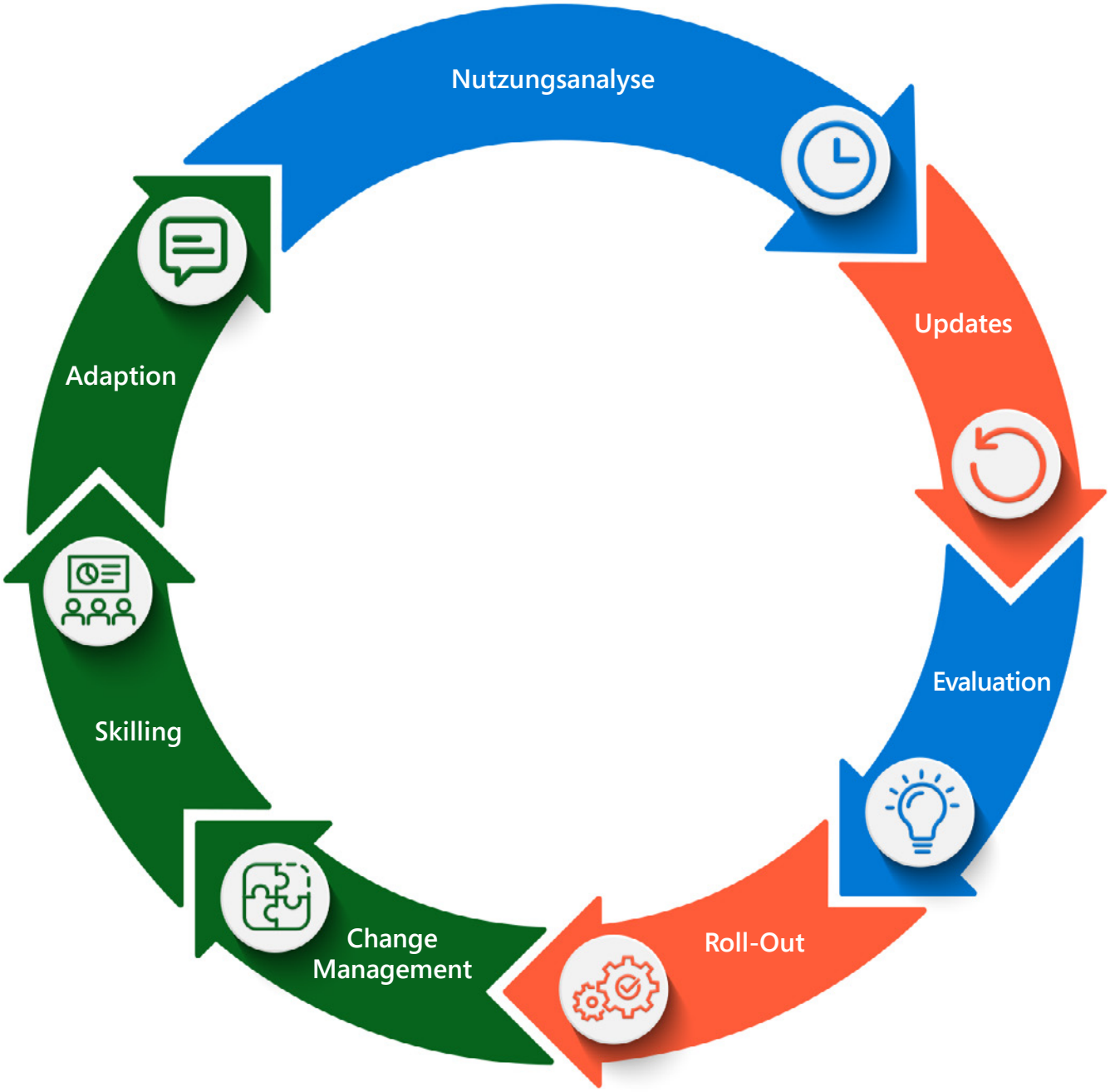
Ein wichtiger Aspekt, der den Weg in die Cloud mitgestaltet, ist das Thema Evergreen und die Etablierung eines Evergreen Prozesses bei Microsoft 365, mit dem die Cloud-Umgebung immer aktuell bleibt. Denn Evergreen IT ist ein Konzept, das darauf abzielt, die IT-Systeme eines Unternehmens kontinuierlich auf dem neuesten Stand zu halten, indem regelmäßig Updates, Patches und Verbesserungen eingespielt werden. Das hat viele Vorteile, wie zum Beispiel eine höhere Sicherheit, eine bessere Performance, eine einfachere Integration und schließlich eine höhere Zufriedenheit der User.

Für viele Organisationen ist das aber immer noch ein neuer und ungewohnter Ansatz, der sich sehr vom traditionellen Prinzip für Anwendungen und Server Produkte unterscheidet. So hatte man für das Ausrollen neuer Funktionen im klassischen Office Paket einen Dreijahreszyklys etabliert, sodass es dazwischen sehr gelegentlich reine Sicherheitsupdates gab. Dadurch hatte man alle drei Jahre ein aufwendiges Migrationsprojekt mit vielen Veränderungen und Schulungen, sowie danach für drei Jahre erstmal eine gewisse Kontinuität, bis die neue Version kam.

Mit der Einführung von Windows 10 und vielen Clouddiensten wie Microsoft Teams wurde dieses Prinzip verabschiedet und ein kontinuierlicher Prozess der Anpassung und Verbesserung mit regelmäßigen neuen Funktionalitäten ohne einen vordefinierten Zeitraum etabliert. Dies erfordert zu Beginn auch einen gewissen Aufwand für die Einführung des neuen Dienstes, ist das Evergreen-Prinzip einmal aufgesetzt und eingespielt, reduziert sich der Aufwand und die Veränderungen bleiben minimal. Im Beispiel von Windows 10 konnte sichergestellt werden, dass jede Sicherheitslücke rechtzeitig geschlossen wird und dass damit das Fundament für alles, was danach kommt in Form von Clouddiensten stabil und sicher ist. Genauso wichtig ist es, mit den aktuellen Entwicklungen rund um KI, die M365-Dienste als Basis dafür stets aktuell zu halten. Entscheidend ist hier die Fähigkeit, eine schnelle Feature Bereitstellung anzubieten. Genau das bietet die Evergreen IT.

Der Umstieg vom klassischen auf das Evergreen Prinzip erfordert eine Veränderung der IT-Strategie und -Kultur eines Unternehmens, was auch Herausforderungen mit sich bringt. Zum einen muss insbesondere die IT-Abteilung die Balance zwischen Kontrolle der Umgebung und der schnellen Bereitstellung spannenden neuer Features halten. Zum anderen sind vor allem die Akzeptanz und das Engagement der Nutzenden ausschlaggebend für eine erfolgreiche Cloudeinführung und Aktualisierung.

Für die IT bietet Microsoft zahlreiche Tools und hilfreiche Resourcen wie z. B. die M365-Roadmap oder die Monthyl Technical Briefings, um auf dem Laufenden zu bleiben und vorzeitig für die Einführung/Aktualisierung zu planen und vorzubereiten. Für den detaillierten Plan schauen Sie in den Evergreen/Change-Management-Prozess im Anschluss.



Von der IT bis zu den Fachbereichen: In sieben Schritten wichtige Veränderungen bei der hybriden Arbeit verstehen und optimal darauf reagieren

Checkliste zum Thema Evergreen/Updatemanagement:

1. Durchführen einer Bedarfs- und Nutzungsanalyse
   Microsoft 365 Admin Center-Aktivitätsberichte - Microsoft 365 admin | Microsoft Learn
2. Mehr Klarheit zu aktuellen Upgrades und Updates sowie kommenden Funktionen
   - Microsoft 365 Roadmap - See What's Coming | Microsoft 365
   - Message center: In the admin center, go to Health > Message center.
3. Evaluation der Veränderungen mit Use Cases
   Microsoft 365-Änderungshandbuch - Deploy Office | Microsoft Learn

Mit der passenden Change-Management-Strategie hohe Akzeptanz und Nutzung erreichen

Mit jedem Evergreen-Konzept sollte bestenfalls eine Change-Management-Strategie einhergehen, denn das Change-Management schafft als Bindeglied zwischen der IT-Abteilung und den Fachbereichen eine klare Vision und Strategie für die Veränderung. Das bedeutet eben auch, dass die IT-Abteilung enger mit den Fachbereichen zusammenarbeiten muss, um deren Bedürfnisse und Use Cases zu verstehen und zu erfüllen.

Ganz wichtig ist die transparente und frühzeitige Kommunikation über die kommende Veränderung. Denn für die Nutzenden ist eine beispielsweise verbesserte Benutzerfreundlichkeit nicht immer sofort ersichtlich, sondern eine Veränderung, die sie zunächst in ihrem gewohnten Arbeitsablauf eventuell verlangsamt, weil sie sich mit der neuen Funktionalität oder Design vertraut machen müssen. Genau an dieser Stelle ist das Thema Transparenz und Kommunikation entscheidend, also das Verständnis vermitteln, welche Ziele, Nutzen und Ablauf mit der Veränderung einhergehen.

Die Beteiligung ist ebenfalls entscheidend. Nutzende sollten in den Prozess einbezogen werden, indem man ihnen zum Beispiel Pilotgruppen anbietet, Umfragen durchführt oder Workshops veranstaltet. Also sicherstellen, dass die Benutzer*innen engagiert und nicht überfordert sind, was wiederrum die Veränderungsmüdigkeit und vor allem auch die Abneigung gegenüber einer Veränderung minimieren kann. Wichtig dabei ist auch, verschiedene Kanäle zu nutzen bzw. neue Kanäle zu schaffen, um vor allen auch Gruppen zu erreichen, die überwiegend zu Hause arbeiten.

Regelmäßige Schulungen sind ein weiterer wichtiger Faktor, in denen Tipps und Tricks zu neuen Funktionen und Möglichkeiten vermittelt werden können. Eine gewisse Guidance, wie man die neuen Funktionalitäten einsetzt, kann hilfreich sein. Letztlich geht es um Zusammenarbeit und Kollaboration und da sollte, wenn möglich, ein gemeinsames Verständnis geschaffen werden. Ein gemeinsamer Nenner kann hilfreich sein, gerade weil Kolleg*innen oft unterschiedliche Arbeitsweisen haben.

Jedes Unternehmen hat, je nach Kapazität, Unternehmenskultur und Größe des Projektes eine andere Herangehensweise an ein Change-Management-Projekt., Zum Beispiel mit einem interdisziplinärem Projektteam aus Unternehmenskommunikation, Bildung, Personalentwicklung und IT und einem Mentorenprogramm oder mit frühzeitiger Einbindung des Betriebsrates über Schulungspläne und der passenden Kommunikationsstrategie.

Checkliste

Bewährte Methoden für Change Management für Microsoft Teams:

1. Identifizieren Ihrer wichtigsten Beteiligten, Pioniere und Benutzerprofile
2. Identifizieren ausgewählter Geschäftsszenarien
3. Durchführen eines Pilotprojekts mit Geschäftsbenutzern, Pionieren und IT-Spezialisten
4. Entwerfen, Starten und Verwalten Ihrer Einführungsinitiative. Laden Sie als Ausgangspunkt unser Customer Success Kit herunter. Eine sinnvolle Einführungsinitiative umfasst Folgendes:
   a. Interne Informationsmaterialien wie beispielsweise Poster, digitale Beschilderung und Veranstaltungen
   b. Zentral verfügbare Selbsthilfe- und Schulungsinformationen
   c. Einen definierten Feedbackmechanismus
   d. Vordefinierte Erfolgskennzahlen (Einführung der Lösung, Aufrufe von wichtigen Materialien, Teilnahme an Kursen)
5. Einrichten eines Pionierprogramms parallel zur Bereitstellung des Diensts
6. Bereitstellen einer Standardmethode für Feedback
7. Messen des Einführungs- und Freigabeerfolgs
8. Anpassen Ihrer Kommunikation und Ihrer Methoden auf der Grundlage des Feedbacks, Wiederholen

Die Einführung von KI-Funktionalitäten zum Beispiel in Form des M365 Copilot bringt sehr viele Chancen aber auch ganz neue Herausforderungen an das Change-Management, denn dabei ist es besonders wichtig, dass der Wandel gut überlegt gestaltet und kommuniziert wird, damit das Vertrauen und die Akzeptanz in die KI gestärkt werden.

Unternehmen, die Evergreen IT leben und bereits ein gut funktionierendes Change-Management-Konzept verinnerlicht haben, werden es leichter haben, KI-Funktionalitäten einzuführen und deren enormen Nutzen im Kontext des hybriden Arbeitens auch wirklich geltend zu machen.

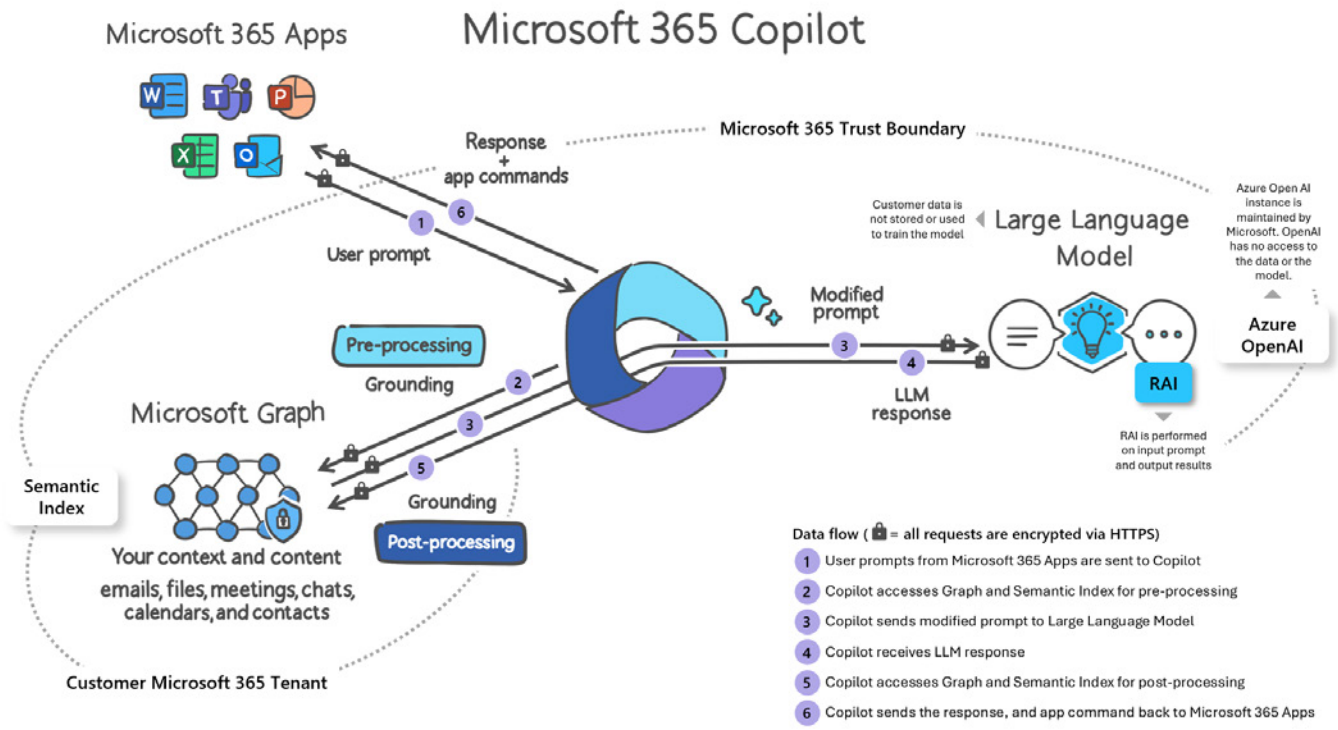
Steigern Sie Ihre Produktivität mit Microsoft 365 Copilot

Warum führen all die angesprochenen Themen dazu, dass Sie Ihr Unternehmen für die Zukunft der Arbeit aufstellen werden? All die bisher angeschauten Maßnahmen bilden das Grundgerüst, um Microsoft Copilot in Ihrem Unternehmen einzuführen.

Basierend auf dem umfassenden Ansatz von Microsoft für Sicherheit, Compliance und Datenschutz ist Copilot auf Microsoft 365 aufgebaut und in dieses integriert. Diese Integration ermöglicht es Ihnen, die Vorteile der vorhandenen Microsoft-Lösungen für Sicherheit, Compliance und Datenschutz zu nutzen, die Sie bereits in Ihrem Unternehmen eingesetzt haben, sowie andere Kontrollmechanismen, die zur Verfügung gestellt werden können, um die Verwendung von Copilot entsprechend den Anforderungen Ihres Unternehmens zu konfigurieren.

Das folgende Diagramm zeigt eine visuelle Darstellung der Funktionsweise von Microsoft 365 Copilot:

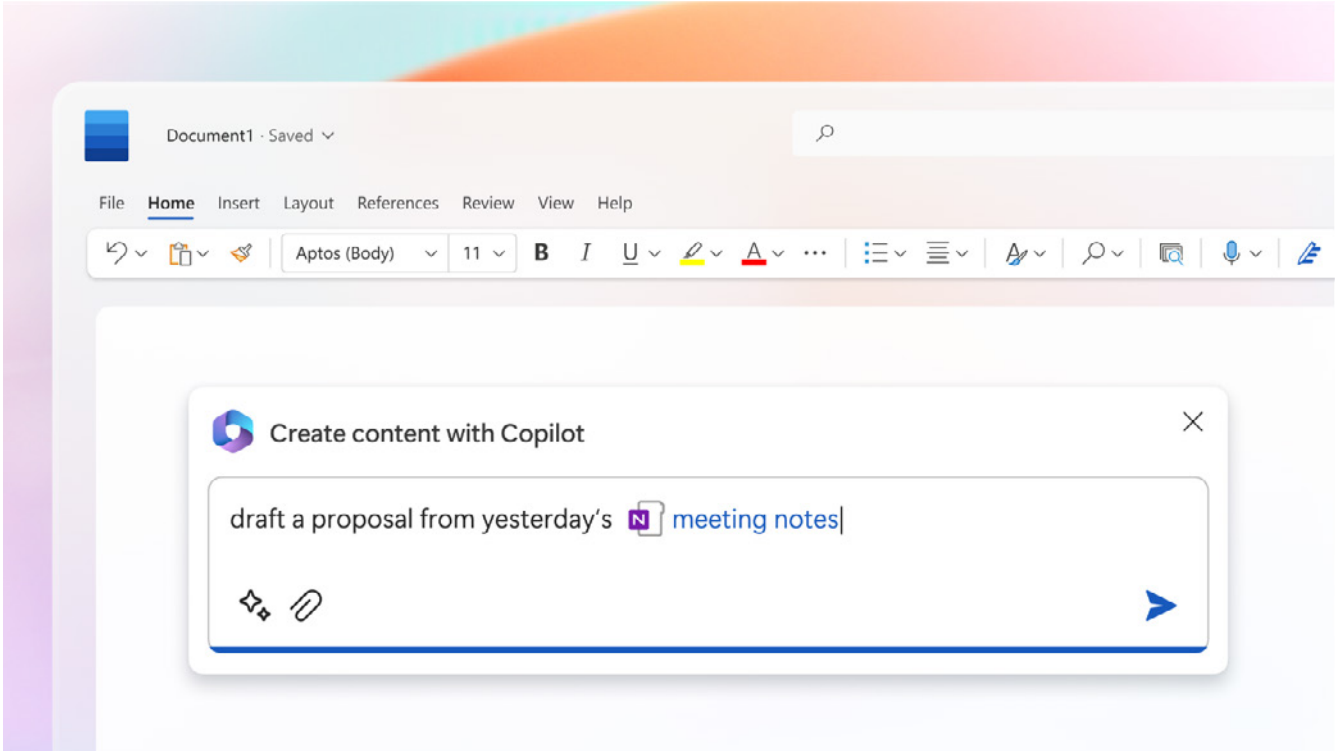
Die Funktionsweise von Microsoft 365 Copilot



https://learn.microsoft.com/en-us/deployoffice/images/privacy/microsoft-365-copilot-flow.png

Copilot ist in Microsoft 365 auf zwei Arten integriert: Er arbeitet nebenher, eingebettet in die Microsoft 365 Apps, die Anwender*innen täglich nutzen, wie Word, Excel, PowerPoint, Outlook, Teams, und mehr, um kreativ zu arbeiten, ihre Produktivität zu steigern und persönliche Fähigkeiten auf ein neues Level zu bringen. Wir stellen heute außerdem ein völlig neues Erlebnis vor: Business Chat. Business Chat arbeitet über das LLM, die Microsoft 365 Apps und die Daten von Nutzer*innen (wie Kalender, E-Mails, Chats, Dokumente und Kontakte) hinweg und kann auf diese Weise Aufgaben abnehmen. Anwender*innen können per Sprache mit dem System kommunizieren, zum Beispiel: „Kannst du bitte unserem Team erklären, wie wir die Produktstrategie überarbeitet haben", und es generiert automatisch ein Update basierend auf den kürzlich abgehaltenen Meetings, E-Mails und Chatverläufen.

Copilot in Word: Erstellen Sie Dokumente schneller als je zuvor

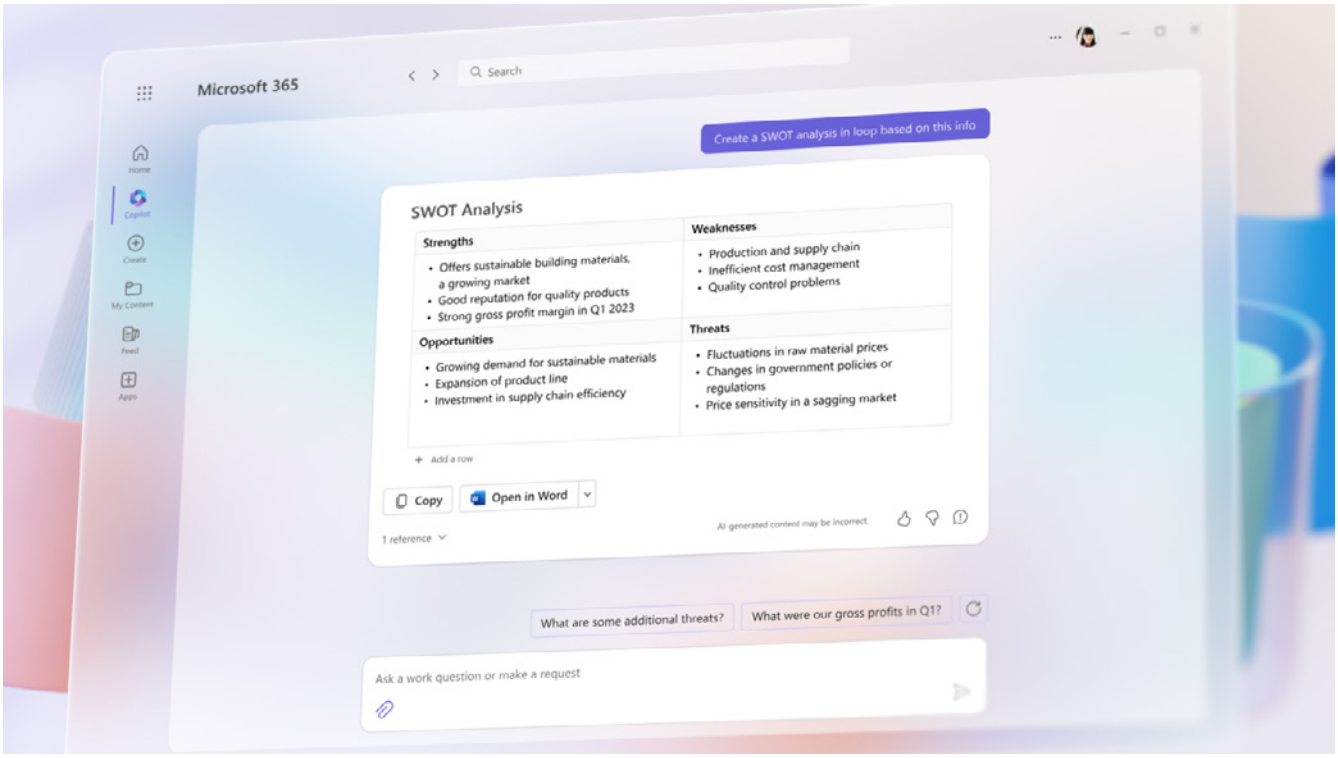


Erfahren Sie mehr zu Copilot unter: [Microsoft 365 Copilot – Microsoft Adoption]

Mit Microsoft 365 Copilot in Word bekommt der kreative Schaffungsprozess eine Starthilfe, sodass Nutzer*innen nie wieder mit einem unbeschriebenen Blatt beginnen müssen. Copilot gibt ihnen einen ersten Entwurf zum Überarbeiten und zum Finalisieren – was viele Stunden an Schreibarbeit, Recherche und Korrekturzeit spart. Copilot in PowerPoint hilft, ansprechende Präsentationen mit einem einfachen Befehl zu erstellen und relevante Inhalte aus Dokumenten hinzuzufügen, die Nutzer*innen beispielsweise letzte Woche oder letztes Jahr erstellt haben. Und mit Microsoft 365 Copilot in Excel können sie Trends analysieren und Daten innerhalb von Sekunden professionell visualisieren lassen.

Wir alle wollen uns auf die 20% der Arbeit konzentrieren, auf die es wirklich ankommt – 80% unserer Zeit wird jedoch für unwesentliche Tätigkeiten verschwendet. Copilot nimmt einem diese Last ab. Von Zusammenfassungen langer E-Mail-Threads bis hin zu schnellen Antwortentwürfen: Copilot in Outlook hilft dabei, den Posteingang in Minuten aufzuräumen anstatt in Stunden. Und jedes Meeting ist mit Microsoft 365 Copilot in Teams produktiv. Er kann Schlüsselpunkte der Diskussion zusammenfassen – unter Berücksichtigung dessen, wer was sagt und an welchen Stellen Personen zustimmen oder nicht übereinstimmen – und schlägt nächste Schritte in Echtzeit, noch während des Meetings, vor. Mit Microsoft 365 Copilot in Power Plattform kann Jede*r wiederkehrende Aufgaben automatisieren, Chatbots erstellen und eine Idee bis zur fertigen App innerhalb von Minuten entwickeln.

Copilot in PowerPoint: Erwecken Sie Ihre Ideen zum Leben



Erfahren Sie mehr zu Copilot unter: [Microsoft 365 Copilot – Microsoft Adoption]

Copilot hilft den Anwender*innen, besser in den Dingen zu werden, die sie bereits beherrschen, und Fähigkeiten zu meistern, die sie noch lernen wollen. Durchschnittlich verwenden Nutzer*innen nur eine Handvoll an Anweisungen – so wie „animiere die Folie" oder „füge eine Tabelle ein" – aus tausenden verfügbaren über Microsoft 365 hinweg. Ab sofort ist dieses weite Spektrum an Funktionen durch die Nutzung natürlicher Sprache verfügbar. Und dies ist nur der Anfang. Copilot wird von Grund auf ändern, wie Menschen mit KI und KI mit Menschen arbeitet. So wie bei jedem neuen Arbeitsmodell gibt es eine Lernkurve, aber diejenigen, die sich diese neue Art der Arbeit zu Eigen machen, werden einen Schritt voraus sein.

Copilot übernimmt automatisch alle relevanten Sicherheits-, Compliance-, und Datenschutzrichtlinien und -prozesse. Zwei-Faktor-Authentifizierung, Compliance-Richtlinien und mehr machen Copilot zu einer KI, der Unternehmen vertrauen können. Wir wissen, dass sich unsere Kunden um Datenlecks sorgen. Copilot LLMs werden nicht mit Tenant-Kommandos trainiert. Innerhalb des Tenants sichert unser lange erprobtes Berechtigungsmodell, dass Daten nicht nutzergruppenübergreifend geteilt werden.

Checkliste

Bevor Sie auf Copilot zugreifen können, müssen Sie die folgenden Anforderungen erfüllen:

1. Prüfen Sie, ob Sie eine Microsoft 365 E3 oder E5 Lizenz, Business Standard oder Business Premium haben oder erwerben können.
2. Microsoft 365 Apps for Enterprise müssen für Ihre Nutzer*innen bereitgestellt werden, die nahtlos in Microsoft 365 Copilot und Anwendungen wie Word, Excel, PowerPoint, Outlook und Teams integriert werden können. Informationen zu den ersten Schritten mit dem Implementierungsprozess finden Sie im Bereitstellungshandbuch für Microsoft 365 Apps.
3. Um Microsoft 365 Copilot verwenden zu können, benötigen Sie ein Azure Active Directory-basiertes Konto. Weitere Informationen finden Sie unter Azure Active Directory.
4. Sie benötigen ein OneDrive-Konto für mehrere Features in Microsoft 365 Copilot, z. B. das Speichern und Freigeben Ihrer Dateien. Weitere Informationen finden Sie unter Anmelden oder Erstellen eines Kontos für OneDrive.
5. Für die nahtlose Integration von Microsoft 365 Copilot in Outlook müssen Sie das neue Outlook für Windows verwenden, das sich derzeit in der Vorschauphase befindet. Sie können zu Outlook Mobile wechseln, um auf die neue Outlook-Benutzeroberfläche zuzugreifen. Weitere Informationen finden Sie unter Erste Schritte mit dem neuen Outlook für Windows.
6. Um Microsoft 365 Copilot mit Microsoft Teams zu verwenden, müssen Sie den Teams-Desktopclient oder -Webclient verwenden. Sie können den Desktopclient hier herunterladen oder sich unter bei https://teams.microsoft.com der Web-App anmelden. Sowohl die aktuelle als auch die neue Version von Teams werden unterstützt. Weitere Informationen finden Sie unter Microsoft Teams-Desktopclient.
7. Um Copilot in Microsoft Loop verwenden zu können, muss die Schleife für Ihren Mandanten aktiviert sein. Weitere Informationen zum Aktivieren von Loop finden Sie unter Erste Schritte mit Microsoft Loop.
8. Ihre Benutzer müssen sich im aktuellen Kanal befinden, um auf Copilot zugreifen zu können. Weitere Informationen finden Sie unter Aktualisieren von Kanälen für Microsoft 365 Apps.

Weitere Ressourcen

Zero Trust

Was ist Zero Trust? | Microsoft Learn
Zero Trust Rapid Modernization Plan | Microsoft Learn
Zero Trust Bereitstellungsplan mit Microsoft 365 | Microsoft Learn
Multi-Faktor-Authentifizierung (MFA) | Microsoft Security
Kennwortlose Authentifizierung | Microsoft Security
Azure Multi-Factor Authentication- Adoption Kit

Intune

Microsoft Intune – Endpunktverwaltung | Microsoft Security
Was ist Microsoft Intune | Microsoft Learn
Kostenlos testen Microsoft Intune | Microsoft Learn

Copilot

Erste Schritte mit Microsoft 365 Copilot - Microsoft 365 admin | Microsoft Learn
Daten, Datenschutz und Sicherheit für Microsoft 365 Copilot - Deploy Office | Microsoft Learn
How Microsoft 365 Copilot works - YouTube

Change Management

Erstellen einer Change-Management-Strategie - Microsoft Teams | Microsoft Learn
Become a Champion – Microsoft Adoption

Microsoft Deutschland GmbH, Walter-Gropius-Straße 5, 80807 München