**✅ 1. Enhance and supercharge IT management with Copilot in Intune**

**Vortragende:** Amit Ghodke, Lavanya Lakshman
**Schwerpunkt:** Einführung und vertiefte Betrachtung der neuen KI-gestützten Copilot-Funktionen in Microsoft Intune zur Unterstützung von IT-Administratoren im Alltag.

**Grundlagen & Prinzipien:**

* **Responsible AI Prinzipien:**
	+ Kundendaten werden **nicht zum KI-Training** genutzt.
	+ Copilot respektiert **Rollen & Berechtigungen** innerhalb von Intune.
	+ Fokus auf **Sicherheit, Datenschutz und Compliance**.

**Hauptfunktionen von Copilot in Intune:**

* **Zusammenfassen** (z. B. Geräte-, Richtlinien-, Konfigurationsübersichten).
* **Antworten & Analysieren** (z. B. konkrete Handlungsempfehlungen, Statusabfragen in natürlicher Sprache).
* **Visualisieren** (z. B. Statusreports, Geräteinformationen).
* **Empfehlen & direkte Handlungsunterstützung** (z. B. Konfliktlösung, Risikoanalysen).

**Detaillierte Use Cases & Beispiele aus der Praxis:**

* **Endpoint Privilege Management (EPM):**
	+ Copilot hilft Admins bei der Bewertung von Apps, die erhöhte Rechte (Elevation) benötigen.
	+ Bewertung erfolgt über eine Hash-Analyse mithilfe von **Defender Threat Intelligence**.
	+ Beispiel: Ein Nutzer möchte eine ZIP-App installieren. Copilot prüft automatisch, ob diese sicher oder risikobehaftet ist, und informiert Admins, die dann entscheiden können.
* **Surface Management:**
	+ Copilot ermöglicht eine einfache, KI-unterstützte Verwaltung von Surface-Geräten.
	+ Beispielsweise Garantieabfragen („Welche Surface-Geräte laufen bald aus der Garantie?“) oder Rollback-Möglichkeiten.
	+ Copilot bereitet automatisch entsprechende Listen auf und ermöglicht einfache Weitergabe an Beschaffungs- oder Support-Abteilungen.
* **Single Device Query:**
	+ KI-basierte Übersetzung von natürlicher Sprache in KQL-Abfragen.
	+ Beispiel: Abfrage des RDP-Ports in der Registry ohne KQL-Vorkenntnisse.
* **Policy Management:**
	+ Automatische Zusammenfassung komplexer Intune-Richtlinien.
	+ Konflikterkennung bei Policy-Einstellungen.
	+ Direkte Hilfestellungen zu Auswirkungen einzelner Richtlinien.
* **Troubleshooting:**
	+ Vergleich von Geräten auf Konfigurations- und Richtlinienebene.
	+ Direkte Unterstützung bei der Ursachensuche, etwa warum eine Policy auf einem Gerät wirkt und auf einem anderen nicht.

**Technische Umsetzung & User Experience (UX):**

* Integration direkt in die Intune-Konsole („Sidecar“).
* Admins behalten stets die Kontrolle und treffen letztendlich alle Entscheidungen – Copilot ist eine unterstützende Instanz.
* Vorgefertigte „Curated Prompts“ erleichtern den Einstieg und die Bedienung.

**Fazit der Session:**

Copilot in Intune führt KI-basierte Automatisierung und Analysen in die IT-Verwaltung ein, reduziert manuelle Aufwände erheblich und steigert gleichzeitig Sicherheit und Kontrolle.

**✅ 2. The path ahead: The roadmap for Windows in the cloud**

**Schwerpunkt:** Strategische Roadmap von Microsoft zur Weiterentwicklung von Windows hin zu einer einheitlichen, cloudbasierten, KI-integrierten und sicheren Plattform.

**Kernstrategie – Windows als Cloud-Erlebnis:**

* Starke Fokussierung auf **Windows 365 Cloud-PCs** und **Azure Virtual Desktop (AVD)**.
* Vereinheitlichung von physischen und virtuellen Geräten unter einem konsistenten Verwaltungskonzept via **Intune**.

**Sicherheitsarchitektur – Security by Design:**

* Geräte (insbesondere Windows 365 Link Geräte) werden standardmäßig sicher ausgeliefert („secure by default“).
* Nutzung sicherer Komponenten: **TPM, Pluton-Chip, Virtualization-based Security (VBS), Hypervisor-protected Code Integrity (HVCI), Secure Boot, BitLocker**.
* Keine lokalen Apps, keine lokalen Userdaten: Komplette Kontrolle & Datenhaltung über die Cloud.

**Hotpatching & Resilienz:**

* Einführung von **Hotpatching** ermöglicht Installation kritischer Sicherheitsupdates **ohne Geräte-Neustart**.
* Verbesserung der Geräte-Resilienz (Fähigkeit zur Selbstheilung), Reduktion der Downtime.

**Copilot+PCs:**

* Neue Geräteklasse mit lokalen KI-Beschleunigungschips.
* Bessere Sicherheitsfeatures wie integrierter Pluton-Chip, Secured-Core PCs.
* Ziel: Mehr lokale Rechenpower für KI-Funktionen und gesteigerte User Experience.

**Verwaltung via Intune und Copilot:**

* Zentrale Verwaltung aller Gerätetypen (physisch, virtuell, hybrid) mittels Intune und Entra ID.
* Nutzung von KI & Copilot für präventive Sicherheit, automatisierte Verwaltung und Problembehebung.

**Fazit der Session:**

Microsofts Roadmap führt Windows konsequent in eine cloudbasierte Zukunft – sicher, automatisiert, KI-getrieben und zentral verwaltet. Ein klarer Fokus liegt auf der Zusammenführung von physischen und virtuellen IT-Landschaften unter Intune und Copilot.

**✅ 3. Achieving update harmony through unified update management**

**Schwerpunkt:** Schaffung einer einheitlichen und robusten Update-Strategie mit Windows Autopatch, um Updates konsistenter, kontrollierter und sicherer über alle Gerätetypen hinweg auszurollen.

**Autopatch und Deployment Rings:**

* Bis zu 15 Deployment-Ringe möglich, wodurch Updates phasenweise, kontrolliert und risikoarm ausgerollt werden.
* Gruppen können dynamisch oder manuell befüllt werden.
* Unterschiedliche Verteilungsmethoden (Scheduled install vs. Deadline-driven install).

**Hotpatching:**

* Windows Updates werden ohne Neustart installiert – wichtige Sicherheitslücken können schneller geschlossen werden.
* Erhöht die Systemverfügbarkeit signifikant, reduziert Wartungsfenster und Downtimes.

**Feature Updates Management:**

* Mehrphasige Feature-Update-Strategien (stufenweiser Rollout).
* Möglichkeit, Windows 11-Upgrades entweder zwingend oder optional anzubieten.
* Automatisierte Rollouts über Autopatch Groups und Intune-Richtlinien.

**Driver & Firmware Management:**

* Zentrale, flexible Treiberverwaltung.
* Wahlweise automatische Genehmigung empfohlener Treiber oder manuelle Freigabe.
* Möglichkeit, problematische Treiber gezielt zurückzuziehen und die Kontrolle zu behalten.

**Reporting und Analytics:**

* Umfassende Reportings auf Geräte-, Gruppen- und Unternehmensebene.
* Geräteübersichten, Statusreports, Update-Compliance-Berichte mit historischen Trends (90-Tage-Reports).

**Fazit der Session:**

Die Einführung eines „Unified Update Management“ erlaubt es Unternehmen, Updates zentral, sicher und skalierbar über alle Gerätetypen hinweg zu orchestrieren. Dabei werden Komplexität reduziert, Risiken minimiert und Reaktionszeiten verbessert. Intune spielt hier eine entscheidende Rolle als zentrales Verwaltungs- und Steuerungstool.

**✅ 4. Untangling this thing called AI in a Windows ecosystem**

**Vortragende:** Aria Hanson
**Schwerpunkt:** Klärung und Differenzierung der verschiedenen KI-Produktangebote von Microsoft (insbesondere rund um Windows und Microsoft 365) sowie deren konkreten Nutzen für Unternehmen.

**Klärung und Übersicht der Microsoft AI-Angebote:**

Die Session adressiert häufige Verwirrungen rund um Begriffe wie „Copilot“ und „KI“ im Zusammenhang mit Microsoft-Produkten. Dabei werden verschiedene KI-basierte Angebote klar abgegrenzt und detailliert beschrieben.

* **Microsoft 365 Copilot:**
	+ KI-Unterstützung direkt in Microsoft-365-Anwendungen wie Word, Excel, PowerPoint und Teams.
	+ Automatisches Erstellen von Meeting-Notizen, Zusammenfassen und Umschreiben von Dokumenten sowie Unterstützung bei E-Mail- und Textverarbeitung.
	+ Integration mit SharePoint und internen Wissensdatenbanken, wodurch deutlich spezifischere, interne Abfragen möglich werden.
	+ Sicherheit & Datenschutz: Daten verbleiben vollständig im Tenant des Kunden und werden nicht zur Modellentwicklung genutzt.
* **Copilot Chat (kostenlose Variante):**
	+ Web-basierte, einfachere KI-Variante, geschützt und ohne Nutzung zur KI-Modellentwicklung.
	+ Weniger leistungsstark als die M365-Variante, aber dennoch nützlich für allgemeine Anfragen und einfache Codereviews.
* **Copilot+ PCs (Hardware mit integrierter KI-Unterstützung):**
	+ Spezielle Hardware (Windows-PCs), ausgestattet mit einem lokalen Neural Processing Unit (NPU).
	+ Leistungsfähige KI-Funktionen direkt auf dem Gerät, u.a. semantische Windows-Suche, automatische Bilderkennung und Übersetzungen in Echtzeit.
	+ Umfassende Sicherheitsfeatures wie Pluton-Chip, Secured-Core-Technologie und Windows Hello Enhanced Sign-in Security (ESS).
	+ Neue Produktivitätsfunktionen wie „Recall“ (ein sicherer Cache für Dokumente), automatisch generierte Bildbeschreibungen und Studio-Effekte für bessere Videokonferenzen.

**Entscheidungshilfe für Unternehmen:**

* Optimale KI-Integration erfordert oft sowohl **Microsoft 365 Copilot** als auch spezielle **Copilot+ PCs**.
* Es ist aber möglich, je nach Anforderung entweder auf reine Hardwarelösungen (KI direkt am Gerät) oder auf reine Cloud-basierte Softwarelösungen (M365 Copilot) zu setzen.
* Langfristig empfohlen wird, bei Hardware-Neuanschaffungen auf Geräte mit NPU von mindestens 40 TOPS zu achten, um zukunftssicher aufgestellt zu sein.

**Fazit der Session:**

Microsoft bietet umfangreiche und differenzierte KI-Produkte, deren Nutzen stark vom konkreten Anwendungsfall abhängt. Klare Positionierung und gezielte Auswahl der passenden KI-Angebote erleichtern Unternehmen den maximalen Nutzen aus den neuen Technologien.

**✅ 5. Understanding security and management on Windows 365 Link**

**Vortragender:** David Wells
**Schwerpunkt:** Detaillierte Erklärung der Sicherheits- und Verwaltungskonzepte von „Windows 365 Link“, einem spezialisierten Gerät, das ausschließlich für den Zugriff auf Cloud-PCs konzipiert wurde.

**Gerätespezifikation und Konzept:**

* Windows 365 Link ist ein speziell entwickeltes Gerät, dessen einziger Zweck der sichere und unkomplizierte Zugriff auf Windows-365-Cloud-PCs ist.
* Kompaktes Hardwaredesign (120x120 mm), Ports für HDMI/DisplayPort (2 Monitore à 4K), USB-A, USB-C, Ethernet, Audio und Wi-Fi 6E.

**Sicherheitsprinzipien:**

* **Secure by Default:**
	+ Kleines, spezialisiertes Betriebssystem „Windows CPC“, das ausschließlich die minimal erforderlichen Funktionen für die Verbindung zum Cloud-PC bietet.
	+ TPM 2.0, Virtualization-based Security (VBS), Hypervisor Protected Code Integrity (HVCI), Secure Boot und BitLocker standardmäßig aktiviert und nicht deaktivierbar.
* **App- und Datenrestriktionen:**
	+ Keine lokalen Anwendungen, keine Speicherung lokaler Daten, keine lokale Nutzerverwaltung möglich.
	+ Strikte Code-Integritätsrichtlinien sorgen dafür, dass nur autorisierte Software ausgeführt wird.
* **Passwordless & Conditional Access:**
	+ Ausschließlich Azure AD Join, keine lokale Anmeldung oder Domain Join.
	+ Unterstützung für Device Health Attestation, wodurch Conditional-Access-Richtlinien effektiv durchgesetzt werden können.

**Verwaltung über Microsoft Intune:**

* Einfache Einrichtung („out-of-box experience“) mit automatischer Azure AD-Registrierung und Intune-Verwaltung.
* Weniger Verwaltungskomplexität durch das minimalistische OS-Konzept.
* Nutzung von Intune-Filtern, um gezielt Richtlinien auf Windows-365-Link-Geräte anzuwenden oder auszuschließen.
* Unterstützt automatische Compliance- und Conditional-Access-Regelungen, die den Sicherheitsstatus des Geräts durchgängig sicherstellen.

**Fazit der Session:**

Windows 365 Link bietet Unternehmen eine optimierte, stark sicherheitsorientierte und einfache Lösung für den exklusiven Zugriff auf Cloud-PCs, bei minimalem Verwaltungsaufwand und maximaler Kontrolle via Intune.

**✅ 6. Achieving sustainability goals with Windows 365 and Cloud PCs**

**Schwerpunkt:** Strategien und Funktionen, wie Windows 365 und Cloud-PCs Unternehmen dabei unterstützen, Nachhaltigkeitsziele (Sustainability Goals) zu erreichen und ihre Umweltbilanz zu verbessern.

**Vorteile von Cloud-PCs im Nachhaltigkeitskontext:**

* Verringerung des Materialverbrauchs und des CO₂-Fußabdrucks durch verlängerte Lebensdauer bestehender Hardware (Thin Clients, ältere PCs etc.).
* Nutzung energiesparender, spezialisierter Geräte (z. B. Windows 365 Link), die weniger Strom verbrauchen als herkömmliche Desktops oder leistungsstarke Notebooks.

**Messbarkeit & Kontrolle des Energieverbrauchs:**

* Windows 365 ermöglicht eine bessere zentrale Kontrolle und Nachverfolgung von Energieverbrauch und Emissionen über die Cloud-Management-Tools.
* Verbesserte Telemetrie und Analysen ermöglichen es Unternehmen, CO₂-Emissionen und Energieverbrauch genau zu erfassen und gezielt zu optimieren.

**Hardware-Auswahl und Recycling:**

* Empfehlung der Nutzung speziell entwickelter, effizienter Hardware wie Windows 365 Link, welche nachhaltig produziert, einfach recyclebar und durch geringe Dimensionen effizient zu transportieren ist.
* Möglichkeiten zur optimalen Wiederverwertung von Geräten und Reduktion elektronischen Abfalls.

**Globale Infrastruktur & Skalierbarkeit:**

* Cloud-PCs sind über eine globale Infrastruktur verteilt, was eine effizientere Auslastung von Serverressourcen ermöglicht (Nachhaltigkeit durch Skaleneffekte).
* Flexibilität bei der Ressourcen-Zuweisung reduziert unnötige Energieverschwendung, da Hardware-Ressourcen bedarfsgerecht bereitgestellt werden.

**Fazit der Session:**

Cloud-PCs und Windows 365 ermöglichen es Unternehmen, ihre Nachhaltigkeitsziele aktiv zu unterstützen. Durch geringeren Hardwareeinsatz, effiziente zentrale Verwaltung und bessere Transparenz über Emissionen und Energieverbrauch tragen diese Technologien entscheidend dazu bei, die Umweltbelastung zu minimieren.

**✅ 7. Managing Windows devices securely and efficiently with Microsoft Intune**

**Schwerpunkt:**
Die Session beschreibt neue und bewährte Methoden, wie IT-Abteilungen mithilfe von Microsoft Intune Windows-Geräte sicher und effizient verwalten können, insbesondere im Kontext von Sicherheit und Automatisierung.

**Zentrale Neuerungen und Funktionen:**

* **Endpoint Security und Intune Integration:**
	+ Tiefe Integration von Microsoft Defender for Endpoint (MDE) und Intune zur verbesserten Erkennung und schnellen Reaktion auf Bedrohungen.
	+ Echtzeitüberwachung und automatische Behebung von Sicherheitsproblemen.
* **Automatisierung durch Policy-Templates:**
	+ Erweiterte Nutzung von Security-Baselines (CIS, Microsoft Security Baselines) direkt in Intune.
	+ Automatische Aktualisierung und Verwaltung von Policy-Templates durch Microsoft, reduziert manuelle Anpassungen und erhöht Sicherheit.
* **Conditional Access und Compliance Policies:**
	+ Feinere Kontrolle durch Conditional-Access-Richtlinien (Gerätezustand, Standort, Nutzerverhalten).
	+ Verbesserte Möglichkeiten für automatische Remediation (z.B. automatische Isolation kompromittierter Geräte).
* **Endpoint Privilege Management (EPM):**
	+ Einschränkung administrativer Berechtigungen bei gleichzeitiger Möglichkeit zur temporären Erhöhung durch Admin-Freigaben (EPM Workflow).
* **Automatische Update-Steuerung:**
	+ Verbesserte Rollout-Kontrolle mit Windows Autopatch.
	+ Nutzung der Unified Update Platform (UUP) für zuverlässigere und kleinere Updatepakete.
* **Cloud-basierte Sicherheit und Intune:**
	+ Vereinfachtes Management hybrider Umgebungen (lokale AD-Domänen + Azure AD).
	+ Neue Intune-Funktionen für die Migration von On-Premises-Richtlinien zu Cloud-nativen Umgebungen.

**Fazit der Session:**

Microsoft Intune bietet IT-Administratoren zunehmend automatisierte und sicherheitszentrierte Werkzeuge, um komplexe Windows-Umgebungen einfacher und sicherer zu verwalten – insbesondere durch die enge Verzahnung mit Defender und Conditional Access.

**✅ 8. Windows Autopilot: Streamlining device provisioning**

**Schwerpunkt:**
Diese Session erläutert ausführlich das Konzept, die Funktionsweise und Best Practices rund um Windows Autopilot, Microsofts Technologie zur automatisierten Einrichtung von Windows-Geräten.

**Grundlegende Prinzipien von Autopilot:**

* Ziel: Geräte schnell, standardisiert und ohne manuelle Eingriffe bereitstellen.
* Geräte direkt vom Hersteller zum Nutzer („Zero-Touch Deployment“).

**Technische Neuerungen und Features:**

* **Autopilot-Geräteregistrierung:**
	+ Vereinfachte Registrierung von Geräten direkt durch OEMs (Dell, HP, Lenovo u.a.).
	+ Möglichkeit der Geräteregistrierung auch nachträglich über CSV-Dateien.
* **Geräteprofilierung und Konfiguration:**
	+ Automatisches Ausrollen von Geräten mittels Intune-Konfigurationsprofilen.
	+ Unterstützung unterschiedlicher Anwendungsfälle: Benutzer-getriebenes Deployment (User-Driven) oder Shared Device Deployment (Kiosk/Meetingräume).
* **Windows Autopilot for pre-provisioned deployment:**
	+ Vorinstallation und Bereitstellung aller Anwendungen und Policies durch die IT-Abteilung vor Übergabe an den Nutzer.
	+ Verkürzt den initialen Setup-Prozess für Nutzer drastisch (Gerät sofort betriebsbereit).
* **Integration mit Windows Autopatch und Intune:**
	+ Autopilot-Geräte können direkt in Autopatch-Gruppen aufgenommen werden.
	+ Erleichtert langfristige Verwaltung und Update-Rollouts über Intune.
* **Reporting und Troubleshooting:**
	+ Verbesserte Statusreports und Fehleranalyse direkt im Intune Admin Center.
	+ Vereinfachtes Troubleshooting über Autopilot Event Logs.

**Fazit der Session:**

Windows Autopilot ist ein wesentliches Werkzeug, um die Einrichtung von Windows-Geräten für IT-Abteilungen enorm zu beschleunigen und gleichzeitig Sicherheit und Standardisierung zu erhöhen.

**✅ 9. Deep dive into Endpoint Privilege Management (EPM) with Intune**

**Schwerpunkt:**
Detaillierte technische Betrachtung von Endpoint Privilege Management (EPM), einer Funktion der Intune Suite, die es IT-Abteilungen erlaubt, administrative Berechtigungen auf Windows-Geräten sicher und flexibel zu steuern.

**Grundprinzip von EPM:**

* Reduzierung von Administratorrechten auf Standardrechte, um Angriffsfläche erheblich zu reduzieren.
* Temporäre Rechte-Erhöhung nach kontrollierter, administrativer Freigabe für notwendige Aufgaben.

**Funktionsweise & technische Details:**

* **Rollen und Verantwortlichkeiten:**
	+ Klare Trennung der Rollen: Nutzer fordern temporäre Rechte an, Admins prüfen und genehmigen über Intune.
	+ Audit-Logs und transparente Dokumentation der Eskalationsprozesse.
* **Copilot-Integration:**
	+ Copilot prüft automatisch, ob angeforderte Anwendungen sicher sind, basierend auf Microsoft Defender Threat Intelligence.
	+ Ermöglicht schnelle Entscheidungshilfen für Admins direkt im Freigabeprozess.
* **Anwendungsfälle:**
	+ Installation von spezifischer Software, Druckertreibern oder Anpassungen der Systemkonfiguration, die erweiterte Rechte erfordern.
	+ Unterstützung unterschiedlicher Zeitlimits für temporäre Berechtigungen (Minuten bis mehrere Stunden).
* **Best Practices für den Einsatz von EPM:**
	+ Klare Definition erlaubter Anwendungen mittels Hash-Analyse und Publisher-Regeln.
	+ Integration in bestehende Sicherheitskonzepte (Conditional Access, Compliance Checks).
* **Berichtswesen und Überwachung:**
	+ Umfassendes Reporting der genutzten Eskalationen und privilegierter Vorgänge in Intune.
	+ Übersichtliche Dashboards für Admins zur schnellen Analyse und Nachverfolgung privilegierter Aktionen.

**Fazit der Session:**

EPM bietet eine innovative Lösung zur Verbesserung der Sicherheit und Flexibilität bei der Verwaltung privilegierter Zugriffe in Windows-Umgebungen, insbesondere durch die Integration von Copilot als Assistenzsystem zur Sicherheitsbewertung und Freigabe-Entscheidungen.

**✅ 10. What's new in Windows 11 24H2 for IT admins**

**Schwerpunkt:**
Ausführliche Vorstellung neuer Funktionen und Verbesserungen in Windows 11 Version 24H2, speziell zugeschnitten auf Anforderungen von IT-Administratoren und Unternehmen.

**Kernfunktionen und Neuerungen in Windows 11 24H2:**

* **Windows Autopatch Integration:**
Erweiterte Möglichkeiten der Update-Verwaltung über Autopatch-Gruppen und dynamische Rollouts, verbesserte Planbarkeit und Kontrolle von Feature-Updates.
* **Verbessertes Sicherheitsmanagement:**
	+ Weiterentwicklung von Pluton-Chip-Integration und Secured-Core-PC-Konzepten.
	+ Neue Optionen für Windows Hello Enhanced Sign-in Security (ESS), um Sicherheit der Benutzeranmeldung zu erhöhen.
	+ Erweiterungen in der Virtualization-based Security (VBS) und Hypervisor-Protected Code Integrity (HVCI).
* **Hotpatching Verbesserungen:**
Erweiterung der unterstützten Szenarien für Hotpatching, ermöglicht kritische Sicherheitsupdates ohne Reboot, reduziert Downtime deutlich.
* **Verbesserte Verwaltung & Reporting über Intune:**
Neue Features im Intune Admin Center, bessere Echtzeitübersichten, verbesserte Telemetrie, und transparentere Status-Reports (Updates, Compliance, Sicherheit).
* **Produktivitätssteigerungen:**
	+ Bessere Multi-Monitor-Unterstützung, effizientere Snap-Layouts.
	+ KI-gestützte Suche und verbesserte semantische Suchmöglichkeiten direkt im Windows Explorer.
* **Sustainability-Einstellungen:**
Neuerungen im Energiemanagement, Geräte können effizienter verwaltet werden, um Stromverbrauch zu reduzieren und Nachhaltigkeitsziele zu unterstützen.

**Fazit der Session:**

Windows 11 24H2 bietet zahlreiche Verbesserungen speziell für IT-Administratoren. Höhere Sicherheit, gesteigerte Produktivität und bessere Verwaltbarkeit durch Intune machen diese Version besonders attraktiv für Unternehmenskunden.

**✅ 11. Modernizing endpoint security with Microsoft Defender and Intune**

**Schwerpunkt:**
Session behandelt, wie Microsoft Defender for Endpoint (MDE) und Intune gemeinsam eine moderne, integrierte Endpoint-Sicherheitslösung bilden, um Geräte umfassend zu schützen und gleichzeitig die Komplexität der Verwaltung zu reduzieren.

**Integrierte Sicherheit mit Defender und Intune:**

* **Automatische Bedrohungserkennung & -reaktion:**
Echtzeit-Erkennung von Sicherheitsvorfällen durch Microsoft Defender, gekoppelt mit automatischen Gegenmaßnahmen über Intune.
* **Zero Trust und Conditional Access:**
Defender liefert kontinuierliche Risikobewertungen, die in Conditional-Access-Richtlinien von Intune genutzt werden, um den Zugriff auf Unternehmensressourcen granular zu kontrollieren.
* **Automatisierte Remediation:**
Bei erkanntem Malware-Befall oder kritischen Sicherheitswarnungen isoliert Intune automatisch betroffene Geräte, um Schäden zu verhindern.
* **Endpoint Security Policies:**
Intune stellt vorkonfigurierte Security Baselines bereit, inklusive Defender for Endpoint-Integration. Automatische Policy-Aktualisierung hält Sicherheitsstandards stets aktuell.
* **Berichterstattung und Analyse:**
Umfangreiche Dashboards und Berichte in Intune zeigen Geräte- und Sicherheitsstatus in Echtzeit, ermöglichen schnelle Diagnose und effektive Reaktion auf Vorfälle.

**Fazit der Session:**

Die tiefere Verzahnung von Defender und Intune ermöglicht Unternehmen, komplexe Sicherheitsherausforderungen effektiv zu managen, Risiken erheblich zu reduzieren und Sicherheitsoperationen zu automatisieren.

**✅ 12. Improving hybrid work productivity with Windows 365 Cloud PCs**

**Schwerpunkt:**
Diese Session beschreibt umfassend, wie Windows 365 Cloud-PCs speziell darauf ausgelegt sind, Produktivität, Flexibilität und Sicherheit in hybriden Arbeitsumgebungen zu erhöhen.

**Produktivität und Benutzererfahrung:**

* **Überall-Zugang:**
Sichere, performante und konsistente Desktop-Erfahrung von jedem Gerät und Ort aus. Mitarbeiter greifen von privaten, Firmen- oder Thin-Client-Geräten zuverlässig auf ihre Cloud-PCs zu.
* **Einfache Skalierbarkeit:**
Schnelle Bereitstellung zusätzlicher Cloud-PC-Ressourcen bei Bedarf. IT-Abteilungen reagieren flexibel auf veränderte Anforderungen der Nutzer.
* **Windows 365 Boot:**
Möglichkeit, physische Geräte direkt in den Cloud-PC zu booten. Vereinfacht Nutzererfahrung und reduziert Komplexität lokaler Verwaltung.

**Sicherheit und Compliance:**

* **Strikte Kontrolle durch Intune:**
Alle Cloud-PCs werden zentral verwaltet, mit automatisierten Richtlinien für Compliance, Conditional Access und Security Baselines.
* **Zero Trust Architektur:**
Windows 365 Cloud-PCs verwenden eine Zero Trust basierte Zugriffssteuerung, um Sicherheitsrisiken zu minimieren und Identitäten wirksam zu schützen.

**Integration und Verwaltung:**

* **Nahtlose Integration in bestehende Strukturen:**
Azure AD, Intune, und Microsoft Endpoint Manager als zentrale Steuerungselemente. Einfache Integration in bestehende Infrastrukturen.
* **Monitoring und Analyse:**
Intune bietet erweiterte Reports zu Gerätenutzung, Performance und Sicherheit, mit detaillierten Telemetriedaten und Warnmeldungen.

**Nachhaltigkeit und Kosteneffizienz:**

* **Nachhaltigkeitsvorteile:**
Weniger Hardwareanforderungen vor Ort reduzieren Umwelteinflüsse und Hardwarekosten.
* **Kosteneinsparungen durch bedarfsorientierte Ressourcen:**
Unternehmen bezahlen nur, was sie tatsächlich nutzen, und können Ressourcen nach Bedarf skalieren, wodurch langfristige Kosten reduziert werden.

**Fazit der Session:**

Windows 365 Cloud-PCs bieten eine umfassende Lösung für moderne, hybride Arbeitsweisen. Sie steigern Produktivität, Flexibilität und Sicherheit erheblich und ermöglichen zugleich nachhaltigere und kostengünstigere IT-Strukturen.

**✅ 13. Enhance and supercharge IT management with Copilot in Intune**

**Schwerpunkt:**
Detaillierte Vorstellung von Copilot in Intune, einer KI-gestützten Lösung, die IT-Administratoren bei der Verwaltung von Endgeräten effizient unterstützt.

**Kernaussagen und Funktionen:**

* **KI-unterstützte Endpoint Privilege Management (EPM):**
Copilot hilft IT-Admins, schneller und sicherer zu entscheiden, ob angeforderte App-Elevationen genehmigt werden sollen. Es nutzt Microsoft Defender Threat Intelligence, um sofort Risiken von Anwendungen zu bewerten, spart Zeit und erhöht die Sicherheit.
* **Surface Geräteverwaltung mit Copilot:**
Einzigartige Eigenschaften von Surface-Geräten (z.B. spezielle Rollbacks, Berechtigungen, Gewährleistungsstatus) können direkt über Copilot abgefragt werden. Admins verwenden einfache natürliche Sprache, um komplexe Daten auszuwerten, wie z.B. Geräte außerhalb der Compliance oder mit bald ablaufender Garantie.
* **Single Device Query mit natürlicher Sprache und KQL:**
Copilot übersetzt einfache, geschäftliche Fragen in komplexe KQL-Abfragen. Ermöglicht eine Echtzeitabfrage kritischer Informationen (z.B. aktueller RDP-Port) ohne tiefe technische Kenntnisse.
* **Richtlinienverwaltung mit Konflikterkennung:**
Copilot analysiert und fasst Sicherheitsrichtlinien zusammen, erkennt automatisch Richtlinienkonflikte und zeigt sie übersichtlich an. Reduziert Fehlerquellen und erhöht Transparenz.
* **Troubleshooting und Gerätevergleich:**
Zusammenfassung und direkter Vergleich von Geräten ermöglicht schnelles Erkennen von Unterschieden in zugewiesenen Richtlinien, Apps oder Fehlerzuständen.

**Fazit der Session:**

Copilot in Intune bietet IT-Administratoren eine leistungsstarke KI-gestützte Unterstützung, die komplexe und zeitintensive Aufgaben deutlich vereinfacht, schnelle Entscheidungen ermöglicht und die Verwaltung großer Geräteflotten effizienter und sicherer macht.

**✅ 14. The hottest way to update Windows 11 and Windows Server 2025**

**Schwerpunkt:**
Vorstellung der „Hotpatch“-Technologie für Windows 11 (24H2) und Windows Server 2025, die ermöglicht, Sicherheitsupdates ohne Neustart zu installieren, was Produktivität und Sicherheit erheblich steigert.

**Kernaussagen und Funktionen:**

* **Hotpatch-Technologie:**
Hotpatching installiert wichtige Sicherheitsupdates direkt im laufenden Betrieb („in-memory“), ohne dass ein Neustart erforderlich ist. Dadurch entfällt die Ausfallzeit für Endbenutzer und Server.
* **Servicing-Strategie:**
Hotpatch-Releases erfolgen achtmal pro Jahr. Quartalsweise (Januar, April, Juli, Oktober) werden Hotpatch-Geräte auf einen gemeinsamen Baseline-Stand gebracht, danach folgen jeweils zwei Monate reine Sicherheitsupdates via Hotpatch.
* **Anforderungen & Management:**
	+ Unterstützt Windows 11 (24H2) sowie Windows Server 2025 Datacenter und Standard Editions (Azure und on-prem via Azure Arc).
	+ Voraussetzung: Virtualization-based Security (VBS) aktiviert.
	+ Verwaltung erfolgt via Autopatch für Windows Clients und Azure Update Manager für Server.
* **Vorteile für Unternehmen:**
Schnellere Absicherung ohne Neustarts reduziert Risiken durch verspätete Neustarts der Benutzer erheblich und verbessert gleichzeitig die Produktivität. Reduziert außerdem deutlich Wartungskosten und Ausfallzeiten.

**Fazit der Session:**

Hotpatching ist eine transformative Lösung für Unternehmen, die Sicherheit und Produktivität kombiniert, indem sie kritische Updates schneller bereitstellt und gleichzeitig Ausfallzeiten vermeidet.

**✅ 15. The path ahead: The roadmap for Windows in the cloud**

**Schwerpunkt:**
Umfassender Überblick über die Roadmap und Neuerungen für Windows 365 und Azure Virtual Desktop, inklusive jüngst veröffentlichter Funktionen und geplanter Erweiterungen.

**Highlights Windows 365:**

* **Verbesserte Sicherheit:**
	+ Microsoft Purview Endpoint DLP und Customer Key Encryption stärken Datenschutz und Compliance nach Zero Trust Prinzipien.
	+ Unterstützung für Intune Endpoint Privilege Management und Scope-Tags sowie Tamper Protection.
* **Benutzerfreundlichkeit und Produktivität:**
	+ Windows 365 Link (neue Geräteklasse) speziell für geteilte Arbeitsplätze wie Hot Desks, Call Center etc.
	+ Windows App als zentrale Schnittstelle für Cloud-PC-Zugriff über mehrere Plattformen (Windows, macOS, iOS, Android).
* **Frontline-Verbesserungen:**
	+ Frontline Shared Mode ermöglicht Cloud-PC-Zugang für mehrere Benutzer auf einem Gerät.
	+ GPU-unterstützte Cloud-PCs für leistungsstarke Anwendungen.
* **Kosten- und Ressourcenmanagement:**
	+ Umfassende Tools zum einfachen Skalieren und Verkleinern der Cloud-PCs, gruppenbasierte Lizenzen, und intelligente Reporting-Funktionen für Kosteneffizienz.

**Highlights Azure Virtual Desktop (AVD):**

* **Verbesserte Nutzererfahrung:**
	+ Optimierte Multimedia- und Teams-Integration (Teams VDI 2.0).
	+ Leistungsverbesserungen wie UDP TURN-Unterstützung für bessere Konnektivität.
* **Erhöhte Sicherheit und Compliance:**
	+ Einführung von 15-Minuten Reauthentifizierung für erhöhte Zugriffssicherheit.
	+ Mobile Application Management (MAM) für iOS und Android-Geräte erhöht die Sicherheit von Remote-Arbeit.
* **Flexible Verwaltung:**
	+ Erweiterte Möglichkeiten der Skalierung und des Session-Host-Managements (z.B. Hibernate-Unterstützung, Autoscale).
	+ Integration mit FSLogix, App-V, VMware Horizon und Citrix zur Vereinfachung der Anwendungsbereitstellung.

**Fazit der Session:**

Windows 365 und Azure Virtual Desktop entwickeln sich kontinuierlich weiter und bieten immer bessere Lösungen für Sicherheit, Flexibilität und Produktivität in modernen, hybriden Arbeitsumgebungen. Die Integrationen mit bestehenden Microsoft-Sicherheitslösungen und neuen Innovationen sorgen für eine zukunftssichere Cloud-Strategie.

**✅ 16. Azure Virtual Desktop: Session host configuration and updates**

**Schwerpunkt:**
Diese Session erläutert umfassend, wie die Verwaltung und Aktualisierung von Session Hosts in Azure Virtual Desktop (AVD) deutlich vereinfacht und standardisiert werden kann.

**Kernaussagen und Funktionen im Detail:**

* **Session Host Configuration:**
	+ Administratoren können jetzt standardisierte Konfigurationsvorlagen definieren, welche automatisch auf alle neuen Session Hosts innerhalb eines Host-Pools angewandt werden. Dies umfasst Einstellungen wie VM-Größe, Image-Typ, Netzwerkoptionen und Disk-Konfigurationen.
	+ Durch Nutzung dieser Templates können Administratoren sicherstellen, dass neue Session Hosts immer konsistent und fehlerfrei erstellt werden.
* **Rolling Updates:**
	+ Ermöglicht die zentralisierte Verteilung von Updates (z.B. neue VM-Images oder VM-Größenänderungen) auf bestehende Session Hosts. Updates werden hierbei schrittweise ausgerollt („rolling“), sodass keine Service-Unterbrechungen entstehen.
	+ Benutzerverbindungen werden auf aktualisierte Hosts umgeleitet, ohne dass es zu Produktivitätseinbußen kommt.
* **Flexibles Image-Management:**
	+ Vereinfachtes Update von Images: Änderungen an Golden Images werden automatisch auf bestehende Session Hosts angewendet.
	+ Admins erhalten Vorschau- und Kontrollfunktionen zur Planung und Steuerung der Rollouts.
* **Erweiterte Verwaltungsmöglichkeiten:**
	+ Geplante Erweiterungen umfassen PowerShell- und ARM-Template-Support, um das Management via Automatisierungstools weiter zu vereinfachen.
	+ Integration mit Microsoft Entra und Azure Key Vault verbessert die Verwaltung von Sicherheitsmerkmalen und Zugangsdaten zusätzlich.

**Vorteile im Überblick:**

* Reduzierung administrativen Aufwands durch Automatisierung.
* Minimierte Fehleranfälligkeit und höhere Konsistenz bei der Bereitstellung.
* Deutlich verbesserte Betriebssicherheit und Kontinuität der Nutzererfahrung.

**Fazit:**

Azure Virtual Desktop bietet nun erheblich erweiterte Funktionen zur Verwaltung und automatischen Aktualisierung von Session Hosts, die den IT-Betrieb vereinfachen, die Nutzererfahrung verbessern und die Ausfallsicherheit signifikant erhöhen.

**✅ 17. Windows 365: Frontline concurrency management & utilization reporting**

**Schwerpunkt:**
Diese Session stellt neue, detaillierte Analyse- und Verwaltungsmöglichkeiten für Windows 365 Frontline Cloud-PCs vor, insbesondere für die gleichzeitige Nutzung („Concurrency“) und bessere Auslastung („Utilization“) der Ressourcen.

**Kernaussagen und Funktionen im Detail:**

* **Concurrency Management:**
	+ Unternehmen können nun exakt nachvollziehen, wie viele Nutzer gleichzeitig mit ihren Frontline Cloud-PCs verbunden sind und für wie lange.
	+ Dadurch wird es einfacher, die maximale Anzahl gleichzeitig benötigter PCs zu bestimmen, Lizenzkosten zu optimieren und Engpässe zu verhindern.
	+ Verwaltung und Kontrolle von Überbeanspruchung einzelner PCs: Möglichkeit, automatisch Sitzungen zu beenden, die ungewöhnlich lange inaktiv sind, um Ressourcen wieder freizugeben.
* **Utilization Reporting:**
	+ Verbesserte Analyse- und Reporting-Funktionalität, die Nutzungsdaten für Zeiträume von 28, 60 oder 90 Tagen bereitstellt.
	+ Identifikation von ungenutzten oder kaum genutzten Cloud-PCs zur besseren Lizenz- und Ressourcenauslastung.
	+ Detailansichten ermöglichen proaktive Optimierung der PC-Zuweisung und Lizenzverteilung.
* **Integration und Automatisierung:**
	+ Die neuen Berichte sind direkt im Intune Admin Center verfügbar und bieten detaillierte Insights zur täglichen Ressourcenauslastung, inklusive Spitzenzeiten und Idle-Zeiten.
	+ Möglichkeit zur automatischen Anpassung von Lizenzzuweisungen anhand der ermittelten Nutzungsdaten.

**Vorteile im Überblick:**

* Signifikante Kosteneinsparungen durch optimierte Lizenzvergabe.
* Verbesserte Nutzerzufriedenheit durch vorausschauende Ressourcenplanung.
* Reduzierte administrative Aufwände durch automatisierte Steuerung.

**Fazit:**

Mit den neuen Concurrency- und Utilization-Funktionen für Windows 365 Frontline erhalten Unternehmen effektive Werkzeuge, um Ressourcen optimal auszunutzen, Lizenzkosten zu senken und gleichzeitig die Verfügbarkeit und Performance der Cloud-PCs sicherzustellen.

**✅ 18. Windows security and resiliency in the cloud**

**Schwerpunkt:**
Diese Session behandelt ausführlich, wie Microsoft die Sicherheit und Resilienz von Windows-Umgebungen in der Cloud (Windows 365 und Azure Virtual Desktop) umfassend verbessert.

**Kernaussagen und Funktionen im Detail:**

* **Zero-Trust-Strategie:**
Stärkung der Zero-Trust-Prinzipien über Identitätsmanagement (z.B. Microsoft Entra ID), Conditional Access, Data Loss Prevention (DLP) und neue Authentifizierungsmechanismen (Passkeys mit Microsoft Authenticator).
* **Erweiterte Sicherheitsfeatures:**
	+ „15-Minuten-Reauthentifizierung“ zur zusätzlichen Absicherung besonders sensibler Cloud-PC-Sitzungen.
	+ Mobile Application Management (MAM) erweitert nun auch auf Android- und iOS-Geräte zum Schutz sensibler Firmendaten.
	+ Einschränkung von Screen Capture und Möglichkeit, Wasserzeichen auf Bildschirminhalten zu setzen, um Datenlecks präventiv entgegenzuwirken.
* **Resilienz und Disaster Recovery:**
	+ Erweiterung von Disaster Recovery-Optionen, darunter Point-in-Time Restore und das Feature Disaster Recovery Plus.
	+ Cross-Region Disaster Recovery ermöglicht schnelle und verlässliche Wiederherstellung von Cloud-PCs aus Snapshots, selbst bei großflächigen regionalen Ausfällen.
	+ Automatische Speicherung von Backups in mehreren Availability Zones, erhöht die Sicherheit und Datenverfügbarkeit erheblich.

**Vorteile im Überblick:**

* Höhere Sicherheit durch umfassende Zero-Trust-Umsetzung.
* Deutlich verbesserte Resilienz und schnelle Wiederherstellungszeiten im Katastrophenfall.
* Umfangreiche Möglichkeiten zur proaktiven Risikominimierung und Datensicherung.

**Fazit:**

Die vorgestellten Sicherheits- und Resilienzmaßnahmen bilden ein umfassendes Paket, das Organisationen dabei unterstützt, ihre Windows-Cloud-Umgebungen sicherer und resilienter zu betreiben und Ausfallzeiten sowie Risiken wirksam zu minimieren.

**✅ Session 19: From admin to standard user with Endpoint Privilege Management (EPM)**

**Vortragende:** Mike Danoski und Don Brown
**Schwerpunkt:**
Detaillierte Einführung und Tipps zur Nutzung von Endpoint Privilege Management (EPM), um Benutzerrechte von Administrator auf Standardbenutzer zu reduzieren und somit das Zero-Trust-Prinzip der geringsten Privilegien („Least Privilege“) effektiv umzusetzen.

**📌 Einführung und Grundlagen zu EPM**

**Was ist EPM?**

* Endpoint Privilege Management (EPM) ist Bestandteil von Microsoft Intune (Intune Suite), das Unternehmen hilft, lokale Administratorrechte auf Endgeräten zu reduzieren.
* Ziel ist es, Nutzer als Standardbenutzer zu betreiben und nur bei Bedarf temporäre, kontrollierte administrative Rechte zu ermöglichen.

**Warum Least Privilege?**

* Reduzierung von Risiken durch weniger Angriffsfläche.
* Weniger Supportanfragen aufgrund von fehlerhaften Konfigurationen durch Nutzer mit ständigen Administratorrechten.

**EPM vs. App Control:**

* EPM kontrolliert speziell die Rechteerhöhung („Elevation“) von Anwendungen, nicht deren grundsätzliche Ausführung.
* Windows App Control ist für generelle Ausführungsrichtlinien gedacht, während EPM gezielt Elevationsanfragen regelt.

**📌 Wichtige Tipps und Best Practices**

**🔑 Tipp 1: Schneller Start mit Audit-Modus**

* **Audit-Modus:**
Schnellster Einstieg ohne Nutzerbeeinträchtigung, indem man zunächst lediglich EPM aktiviert und Elevations-Daten sammelt.
* **Empfohlene Dauer:** Mindestens ein Monat zur genauen Analyse typischer Elevations-Muster in der Organisation.
* **Vorteil:** Kein Risiko für Benutzer, keine Störung der Arbeitsabläufe.

**🔑 Tipp 2: Elevations-Reports effektiv nutzen**

* Reports liefern Daten zu aktuellen Elevations-Vorgängen.
* Regeln lassen sich direkt aus diesen Reports ableiten (z. B. automatische, benutzerbestätigte oder supportbestätigte Elevation).
* Nutzung von Zertifikaten oder Datei-Hashes zur sicheren Identifikation der Anwendungen in den Regeln.

**🔑 Tipp 3: Automatische Elevation für Remote Help Installer**

* Beispiel einer automatischen Regel für die Installation von „Remote Help“ (ebenfalls Teil von Intune Suite).
* Vorteil: Benutzerfreundlichkeit, da Installationen ohne administrativen Eingriff der Nutzer erfolgen können.

**🔑 Tipp 4: Support-Approved Workflow und Security Copilot Integration**

* Elevationen, die nicht automatisch abgedeckt sind, können per Support-Approval abgefragt werden.
* Administratoren erhalten detaillierte Informationen (Dateiname, Benutzer, Geräteinformationen, Hashes etc.) zur Entscheidungsfindung.
* Integration von Microsoft Security Copilot mit Defender Threat Intelligence erlaubt automatisierte Risikobewertung über Datei-Hashes, um Administratoren bei der schnellen, informierten Freigabeentscheidung zu unterstützen.

**Beispiel:**

* Datei wie „InstallPrinter.msi“ könnte harmlos wirken, jedoch eine potenzielle Bedrohung darstellen. Copilot analysiert Datei-Hashes, um schnell Risiken zu identifizieren und Angriffe zu verhindern.

**🔑 Tipp 5: Kontinuierliche Auditierung und Verbesserung**

* Ständiges Auditieren, auch nach initialer EPM-Einführung, um neue, unerwartete Elevations-Vorgänge zu erkennen.
* Unterscheidung zwischen „Managed“ (durch EPM gesteuerte) und „Unmanaged“ (außerhalb von EPM erfolgte) Elevationen, mit dem Ziel, möglichst alle Elevationen unter EPM-Kontrolle zu bringen.

**📌 Weiterführende Empfehlungen und Strategien**

**Granulare Regelgestaltung:**

* Regeln nach Benutzerrollen, Applikationsversionen und Signaturketten definieren, um Sicherheitsrisiken gezielt zu minimieren.
* Verwaltung der Regeln in thematischen Gruppen (z.B. nach Aktionen wie Installation, Deinstallation oder spezifische Benutzergruppen).

**Nutzen aus Reports ziehen:**

* Berichte helfen bei der Identifikation von unerwarteten oder problematischen Anwendungen, veralteten Softwareständen und potenziell gefährlichen Elevationen.

**Benutzerfreundlichkeit und Risikominimierung:**

* Ziel ist eine Balance aus geringer Beeinträchtigung der Nutzerproduktivität und hoher Sicherheitswirkung durch strategische Rechtevergabe und transparente, kontrollierte Elevation.

**📌 Integration zukünftiger Funktionen („Deny Rules“):**

* Geplante Erweiterung im Frühling: Möglichkeit der gezielten Verhinderung („Deny“) von Elevationen für veraltete oder riskante Software-Versionen.
* Hilft, Sicherheitslücken proaktiv zu schließen und klare Richtlinien durchzusetzen.

**📌 Feedback und Nutzerorientierung**

* Kontinuierliches Feedback von Kunden erwünscht, um EPM und die damit verbundenen Workflows beständig zu verbessern.
* Feedback-Kanäle:
	+ Direkt in Intune über die „Send a Smile/Frown“-Funktion
	+ Über direkte Microsoft-Kontakte oder bei Veranstaltungen wie dem Technical Takeoff.

**📌 Zusammenfassung der Vorteile von EPM:**

* Signifikante Erhöhung der IT-Sicherheit durch Minimierung permanenter Adminrechte.
* Reduktion administrativer Belastungen durch automatisierte und KI-unterstützte Entscheidungsprozesse.
* Verbesserte Transparenz und Nachvollziehbarkeit von Elevations-Anfragen.
* Einfache Integration und flexible Anpassung an unterschiedliche Unternehmensanforderungen und Benutzergruppen.

**Fazit der Session:**
Endpoint Privilege Management (EPM) ist ein leistungsstarkes und flexibles Werkzeug, um die Verwaltung von Benutzerrechten effektiv und sicher umzusetzen. Durch intelligente Automatisierung, detaillierte Berichte und die Unterstützung von Security Copilot ermöglicht EPM eine signifikante Verbesserung der Sicherheitslage in Unternehmen bei gleichzeitig minimierter Belastung der IT-Administratoren und Endnutzer.

**✅ Session 20: Managing macOS Updates in Intune**

**Vortragender:** Benjamin Flam (Product Manager, Apple MDM Team bei Intune)
**Schwerpunkt:**
Ausführliche Erläuterung und Demonstration zur Verwaltung von macOS-Softwareupdates in Intune mittels Apples neuer Technologie „Declarative Device Management (DDM)“.

**📌 Einführung in das Declarative Device Management (DDM)**

**Hintergrund und bisherige Herausforderungen:**

* Traditionelles Mobile Device Management (MDM) war ineffizient und verursachte Probleme bei der Verwaltung von macOS-Updates.
* Bisheriger Prozess umfasste mehrere manuelle MDM-Befehle:
	+ Scan nach verfügbaren Updates
	+ Übermittlung verfügbarer Updates
	+ Planung der Installation (Scheduled Updates)
	+ Regelmäßige Statusabfragen (Polling) der Geräte
* Nachteile waren häufige Kommunikationsprobleme, unerwartete Neustarts während Arbeitszeiten und schlechte Nutzererfahrungen durch zu häufige Benachrichtigungen.

**DDM als Lösung:**

* Mit DDM übernehmen die Geräte selbstständig die Steuerung ihrer Updates basierend auf zuvor definierten Regeln (desired state).
* Die Geräte melden proaktiv an den Server zurück, was den aktuellen Update-Status betrifft (proaktives Reporting).
* Administratoren definieren klare, verbindliche Deadlines, und Geräte kümmern sich autonom um die termingerechte Durchführung.

**📌 macOS-Update-Steuerung mit DDM in Intune**

**🔑 Neue DDM-basierte Software-Update-Einstellungen**

Die neuen Funktionen wurden direkt im **Intune macOS Settings Catalog** integriert und ermöglichen eine präzisere Steuerung der Updates:

* **Target Build Version:**
Erlaubt gezielte Auswahl einer spezifischen macOS-Build-Version, z.B. zum Testen von Beta-Versionen.
* **Benutzer-Hilfeseite:**
Möglichkeit, eine benutzerdefinierte Webseite für Hilfestellungen und Erläuterungen zu den Updates zu definieren.
* **Exaktes Installationsdatum und Uhrzeit:**
Erlaubt es, ein genaues Datum und eine präzise Uhrzeit (bis auf die Minute) festzulegen, wann ein Update weltweit installiert werden soll (automatisch in lokaler Zeitzone der Geräte).
* **Target OS Version:**
Dropdown-Liste der verfügbaren macOS-Updates, automatisch gespeist aus dem Apple Software Lookup Service. Administratoren können jedoch weiterhin manuell eine OS-Version eintragen.

**🔑 On-Device Experience mit DDM-Updates**

* Nutzer erhalten Benachrichtigungen über bevorstehende Updates.
* Benachrichtigungsfrequenz erhöht sich stufenweise je näher die Deadline rückt:
	+ 1 Stunde vor dem erzwungenen Neustart erhält der Nutzer sehr häufig Warnungen.
	+ 1 Minute vor Neustart erfolgt eine Countdown-Warnung, bevor das Gerät neu startet und das Update installiert.

**📌 Erweiterte macOS Update-Einstellungen in DDM (ab macOS 15)**

Neue integrierte Einstellungen (vorher auf mehrere Policies verteilt):

* **Allow Standard User OS Updates:**
Erlaubt Standardnutzern, Updates selbst zu installieren (optional).
* **Automatic Actions:**
Steuerung automatischer Update-Downloads und Installationen; Administratoren können dies aktivieren oder vollständig deaktivieren.
* **Deferral Settings (Verzögerungen):**
Festlegung von Verzögerungen, bis wann Nutzer manuell updaten dürfen. DDM-enforced Updates ignorieren diese Verzögerungen.
* **Notification Setting:**
Kontrolle über die Häufigkeit der Update-Benachrichtigungen (täglich oder nur innerhalb der letzten Stunde vor der Deadline).
* **Rapid Security Response:**
Ermöglicht schnellen Rollout dringender Sicherheitsupdates und ggf. deren Zurücknahme (Rollback).

**🔑 Praktische Demo der erweiterten Einstellungen**

* Darstellung in System-Einstellungen > Device Management > Declarations.
* Übersicht über globale Einstellungen: automatische Aktionen deaktiviert, Rapid Security Response deaktiviert, Updates verzögert.
* Klarer Hinweis für Nutzer, welche Version aktuell erlaubt ist.

**📌 Neue Intune-spezifische Funktion: „Enforce Latest OS Version“**

* Intune erkennt automatisch neue macOS-Versionen (via Apple Software Lookup Service).
* Ermöglicht automatisierte Updates der Richtlinien, ohne manuelle Anpassungen.
* Administratoren können eine Verzögerung („Delay“) einbauen, um Updates vor dem automatischen Rollout zu testen.
* Detaillierte Zeitplanung für Installation möglich (24-Stunden-Format).

**🔑 Demonstration der „Enforce Latest“-Funktion**

* Richtlinienerstellung im macOS Settings Catalog gezeigt.
* Konfiguration: Automatische Erkennung der neuesten OS-Version mit optionaler Verzögerung.
* System-Einstellungen zeigen deutlich, wann Updates automatisch installiert werden.

**📌 Troubleshooting von DDM Software Updates**

Empfohlene Vorgehensweise bei Problemen mit DDM Updates:

* **Deklarationen prüfen:**
Kontrolle der Update-Konfiguration direkt auf dem Gerät (System Settings > Device Management > Device Declarations).
* **Software-Update-Ansicht auf dem Gerät:**
Prüfen, ob Gerät das Update bereits geplant (armed) hat.
* **Installations-Log:**
Konsolen-Logs bieten detaillierte Einblicke, ob das Update korrekt geplant wurde, sowie bei auftretenden Fehlern.

**📌 Migration bestehender MDM-Umgebungen auf DDM**

* DDM hat bei Konflikten stets Vorrang gegenüber traditionellen MDM-Richtlinien.
* Sobald DDM aktiv ist, reagieren Geräte nicht mehr auf alte MDM-Befehle.
* Langfristig wird die Unterstützung alter MDM-basierter Update-Richtlinien eingestellt, da DDM von Apple und Intune als zukünftiger Standard gesetzt ist.

**📌 Weiterführende Informationen und Ressourcen**

* **Microsoft Learn Dokumentation:**
Schritt-für-Schritt-Anleitungen zur Konfiguration von macOS Updates via DDM in Intune.
* **Apple Developer Documentation:**
Detaillierte Erläuterungen aller DDM-Funktionen seitens Apple.
* **Apple Plattform Deployment Guides & WWDC Videos:**
Zusätzliche umfassende Informationen und vertiefende Inhalte rund um das Thema DDM.

**📌 Fazit und abschließende Empfehlungen**

* DDM bietet eine signifikant verbesserte Nutzererfahrung durch autonomes Update-Management und proaktive Statusmeldungen.
* Intune bietet mit integrierter DDM-Unterstützung eine hochgradig automatisierte und wartungsarme Verwaltung von macOS Updates.
* Empfehlung: Migration zu DDM frühzeitig planen und durchführen, da alte MDM-basierte Lösungen zukünftig nicht mehr unterstützt werden.

Benjamin Flam empfiehlt allen Admins und IT-Teams, frühzeitig auf DDM umzusteigen, um die Sicherheit, Nutzerfreundlichkeit und Administrations-Effizienz deutlich zu erhöhen und die Zukunft der macOS-Geräteverwaltung optimal zu gestalten.

**✅ Session 21: Windows Autopatch: Your playbook for advanced update management**

**Vortragender:** Ryan Williams, Senior Product Manager (Windows Autopatch Team)
**Schwerpunkt:**
Detaillierte Vorstellung und Demonstration der erweiterten Funktionen von Windows Autopatch für effizientes, sicheres und flexibles Management von Windows Updates, einschließlich Qualität-, Feature-, Treiber- und Edge-Updates.

**📌 Herausforderungen für IT-Admins beim Update-Management**

Die drei zentralen Herausforderungen, denen IT-Administratoren heute gegenüberstehen, umfassen:

1. **Bekannte Sicherheitslücken**:
	* Cybersecurity-Bedrohungen wachsen exponentiell, speziell durch Ransomware.
	* Ungepatchte Systeme zählen zu den häufigsten Angriffsvektoren.
2. **Konkurrierende IT-Prioritäten**:
	* Hybrid-Arbeit erhöht die Komplexität von Update-Management durch unterschiedliche Update-Zyklen und Sicherheitsanforderungen.
3. **Kostendruck**:
	* IT-Budgets stagnieren oder schrumpfen.
	* Administrationsaufwand und Infrastrukturkosten müssen reduziert werden.

**📌 Wie Windows Autopatch diese Herausforderungen adressiert**

Windows Autopatch verspricht „mehr Sicherheit, höhere Produktivität und weniger Aufwand“:

* **Mehr Sicherheit**: Automatische Bereitstellung kritischer Sicherheits- und Zero-Day-Patches.
* **Höhere Produktivität**: Übernahme von Routineaufgaben wie Zeitplanung, Deployment und Monitoring von Updates.
* **Weniger Aufwand**: Zentrale Steuerung und Automatisierung reduziert administrative Komplexität.

**📌 Erweiterte Funktionen und flexible Steuerung durch Autopatch**

**🔑 1. Expedited Quality Updates (beschleunigte Qualitätsupdates)**

* Ermöglicht schnelle, dringende Bereitstellung wichtiger Sicherheitsupdates.
* Ignoriert übliche Verzögerungen und Deadlines.
* Admins können trotz schneller Bereitstellung Neustarts innerhalb eines bestimmten Zeitfensters verzögern.

**Praktische Demo**:

* Einfache Erstellung von "Expedite Policies".
* Nachvollziehbarkeit durch Qualitätsupdate-Report.

**🔑 2. Flexible Steuerung von Feature-Updates (Windows 11)**

* Möglichkeit, Feature-Updates als **optional** bereitzustellen, wodurch Nutzer eigenständig Upgrades durchführen können.
* Automatische Verwaltung von Geräten, die nicht für Windows 11 geeignet sind, indem diese auf die neueste Windows-10-Version aktualisiert werden.

**Praktische Demo**:

* Policies sind flexibel konfigurierbar (optional oder verpflichtend, selektive Gerätezuordnung).
* Fortschritte über den Feature-Update-Report transparent nachvollziehbar.

**🔑 3. Erweiterte Treiberverwaltung (Driver Management)**

* Möglichkeit der manuellen Freigabe und Planung von Treiberupdates.
* Unterstützung von Massenaktionen („Bulk Actions“) für effizientes Management von bis zu 100 Treibern gleichzeitig.
* Flexible Anpassung von Treiber-Rollouts an Updatezyklen (z.B. abgestimmt auf Patch Tuesday).

**Praktische Demo**:

* Gezielte manuelle Genehmigung einzelner Treiber.
* Anpassung des Rollouts für jede Update-Ring-Gruppe.
* Skalierbare Treiberverwaltung durch Mehrfachauswahl.

**🔑 4. Update-Management für Microsoft Edge**

* Verwaltung von Edge-Updates über Autopatch.
* Nutzung von „Stable“ und „Beta“-Kanälen zur kontrollierten Einführung neuer Edge-Versionen.
	+ **Stable Channel**: Breite Bereitstellung alle vier Wochen.
	+ **Beta Channel**: Frühzeitiges Testen und Feedback sammeln vor großflächiger Einführung.

**Praktische Demo**:

* Einfache Aktivierung und Kanalzuordnung.
* Flexible Steuerung und granulare Zuordnung der Edge-Updates.

**📌 Empfehlungen und Best Practices zur optimalen Nutzung von Windows Autopatch**

**🟢 Wichtig zu wissen vor dem Start:**

* **Microsoft Edge**:
	+ Edge-Updates werden automatisch gestaffelt eingeführt.
	+ Im Notfall bietet Microsoft Anleitungen zum Rollback per MSI oder Gruppenrichtlinien.
* **Expedite Updates (Windows 11)**:
	+ Erweiterung auf Nicht-Sicherheitsupdates zur schnelleren Problembehebung.
	+ Keine Abhängigkeit mehr vom "Update Health Tool" ab Windows 11 24H2.
	+ Unterstützung für Long-Term Servicing Channel (LTSC) für kritische Updates.

**🟢 Ausnahmen beim Treiber-Management:**

1. **Plug-and-Play Treiber (PnP)**:
	* Werden automatisch installiert, wenn neue Hardware erkannt wird.
	* Nach Erstinstallation übernimmt Autopatch die weitere Verwaltung.
2. **Extension-Treiber**:
	* Ergänzen Base-Treiber, indem sie neue Funktionen oder Verbesserungen hinzufügen.
	* Werden aktuell nicht von Autopatch verwaltet, erkennbar durch den Begriff „Extension“ im Treibernamen.
3. **Gezielte Treiberbereitstellung (Driver Targeting)**:
	* OEMs und IHVs definieren Attribute (Hardware IDs, Computer Hardware IDs) für Treiber-Verteilung.
	* Computer Hardware IDs (CHIDs) haben Vorrang, um sicherzustellen, dass Treiber kompatibel und OEM-validiert sind.
	* OS-Version beeinflusst ebenfalls, ob ein Treiber angeboten wird.

**📌 Vorteile und Nutzen im Überblick**

* **Vereinfachtes Management** komplexer Update-Szenarien durch Automatisierung und flexible Steuerungsoptionen.
* **Höhere IT-Sicherheit** durch schnelle, gezielte Bereitstellung kritischer Updates.
* **Verbesserte Nutzererfahrung** dank kontrollierter, schrittweiser und optionaler Updates.
* **Optimale Ressourcennutzung** (Zeit und Budget) durch Reduzierung manueller IT-Aufgaben.

**📌 Abschließende Empfehlungen des Vortragenden:**

* IT-Admins sollten frühzeitig die erweiterten Funktionen und Flexibilitäten von Windows Autopatch nutzen.
* Testen und Ausprobieren der Funktionen im eigenen Umfeld empfohlen, um optimale Einstellungen zu finden.
* Feedback erwünscht, um kontinuierliche Verbesserungen der Lösung voranzutreiben.

**Fazit der Session:**
Windows Autopatch bietet IT-Administratoren eine umfassende, sichere und flexible Möglichkeit, komplexe Update-Szenarien effizient zu verwalten. Durch erweiterte Steuerungsmechanismen für Qualitäts-, Feature-, Treiber- und Edge-Updates wird der administrative Aufwand minimiert und gleichzeitig die IT-Sicherheit maximiert.

**✅ Session 22: Unified Security: Intune + Microsoft Defender for Endpoint**

**🎤 Präsentatoren:**

* **Laura Arita**, Produktmanagerin (Intune, Policy und Security)
* **Per Larsen**, Intune Customer Adoption & Enablement

**📌 Überblick zur Unified Endpoint Security Management Lösung**

Microsoft bietet eine **vereinheitlichte Endpoint-Sicherheitslösung**, die es IT- und Sicherheitsteams ermöglicht, eng zusammenzuarbeiten. Im Kern steht die tiefe Integration zwischen **Microsoft Intune** und **Microsoft Defender for Endpoint** (MDE), welche umfangreiche Sicherheitskontrollen und -einstellungen für Geräte ermöglicht.

**📌 Zentrale Funktionen und Vorteile**

* **Tiefe Integration von Intune und Defender for Endpoint** ermöglicht Verwaltung aus beiden Portalen.
* Sicherheitsrichtlinien für Geräteplattformen:
	+ Windows, macOS, Linux Server
	+ Vollständig verwaltete Geräte (MDM enrolled)
	+ Co-managed Geräte (Tenant Attach)
	+ Geräte ohne Intune-Enrollment („Defender Attach“)
* Sicherheitskonfigurationen beinhalten:
	+ Antivirus
	+ Verschlüsselung (Encryption)
	+ Attack Surface Reduction (ASR)
	+ Firewall
	+ Account Protection
	+ Security Baselines

**📌 Unterstützte Managementkanäle**

| **Kanal** | **Geräteplattformen** | **Details** |
| --- | --- | --- |
| **Intune (MDM)** | Windows Desktop, macOS | Vollständig verwaltete Geräte |
| **Tenant Attach (Configuration Manager)** | Windows Desktop, Server | Hybrid-Management (Intune + ConfigMgr) |
| **Defender Attach (ohne Intune-Enrollment)** | Windows Desktop, Windows Server, Linux Server, macOS | Nur Sicherheitspolicies, keine vollständige Geräteverwaltung |

**📌 Technische Details zu „Defender Attach“ (Geräte ohne Intune-Enrollment)**

* Voraussetzung: Defender-Client ist installiert und onboarded.
* Automatische Erstellung eines Geräteobjekts in **Microsoft Entra** (AAD), wenn noch nicht vorhanden.
* Ermöglicht Security-Policy-Zuweisung an Geräte, die nicht vollständig über Intune verwaltet werden.
* Sehr schlanke und flexible Implementierung, speziell für Unternehmen mit komplexer Infrastruktur.

**📌 Demo-Highlights aus Intune Endpoint Security**

Per Larsen zeigte folgende Funktionen aus der **Intune Endpoint Security** Oberfläche:

**1. Antivirus Policies**

* Status-Check auf „unhealthy“ Geräte (z.B. veraltete Virensignaturen)
* Möglichkeit zum Triggern manueller Updates (z.B. AV-Signaturupdates)

**2. Policy-Erstellung & Verteilung**

* Beispiel: Defender-Update-Control-Policy
* Unterschiedliche Deployment-Kanäle (Preview Channel, Current Channel)
* Flexible Gruppen- und Filterzuweisung für Pilottests

**3. Attack Surface Reduction (ASR) & Device Control**

* Verwendung von **Reusable Settings** („wiederverwendbare Einstellungen“) für einfachere Policy-Erstellung
* Kontrolle über externe Geräte (z.B. USB-Medien)
* Möglichkeit, Zugriffsrechte granular zu steuern (Lesen, Schreiben, Ausführen verbieten)

**4. Security Baseline für Defender for Endpoint**

* Sicherheitsbaseline für MDM-verwaltete Geräte
* Einfache Anpassung: Einstellungen können auf „nicht konfiguriert“ gesetzt werden, wenn nicht benötigt

**✅ Session 23: Demo-Highlights aus Defender for Endpoint Portal (MDE)**

Laura Arita demonstrierte die Funktionen im **Defender for Endpoint Portal**:

* Vollständiger Zugriff auf dieselben Policies, die auch über Intune erstellt werden.
* Möglichkeit, Policies direkt aus dem Defender-Portal zu erstellen, bearbeiten, exportieren und löschen.
* Gleiche Policy-Typen (Antivirus, Device Control etc.) wie in Intune, identische Benutzererfahrung.
* Zugriff auf detaillierte Reports und Geräteinformationen direkt im Defender-Portal.
* Nahtloses Arbeiten im Defender-Portal möglich, ohne zwischen Intune und Defender wechseln zu müssen.

**📌 Häufig gestellte Fragen (FAQ)**

1. **Müssen alle Geräte in Intune registriert sein?**
	* Nein. Sicherheitsrichtlinien sind auch via „Defender Attach“ möglich (ohne Intune-Enrollment).
2. **Welche Geräte werden nicht von MDE unterstützt?**
	* Server Core, VDI, Legacy-Betriebssysteme werden aktuell nicht unterstützt.
3. **Conditional Access (CA)**:
	* Erfordert Intune-Enrollment, um Compliance sicherzustellen.
4. **Security Baselines**:
	* Funktionieren nur mit Intune-enrolled Geräten, nicht via Defender Attach.
5. **Schnellere Updates auf Geräte pushen?**
	* Manuelles Anstoßen von AV-Signatur-Updates oder Policy-Synchronisierung ist möglich.
6. **Wie werden Geräte adressiert?**
	* Über Entra-Gruppen (AAD-Gruppen), dynamische oder statische Zuordnung möglich.

**📌 Mehrfach-Managementkanäle & Prioritäten**

Geräte können über mehrere Managementkanäle gesteuert werden (Intune, Configuration Manager, GPO, PowerShell, Dritte). Empfehlungen:

* Priorität auf Intune-basierte Verwaltung setzen, um Konflikte zu vermeiden.
* Detaillierte Infos und Auflösung zur Vorrangigkeit von Richtlinien in der Dokumentation von Microsoft verfügbar.

**📌 Empfehlung der Vortragenden**

* Die einheitliche Verwaltung aus Intune und Defender nutzen, um Sicherheitsrichtlinien effektiv und flexibel zu verteilen.
* Frühzeitig Pilotgruppen einrichten, um Auswirkungen von Policies zu testen.
* Integration von Defender Attach prüfen, wenn nicht alle Geräte direkt via Intune verwaltet werden können oder sollen.

**📌 Fazit**

Die Session vermittelt detailliert, wie Intune und Microsoft Defender for Endpoint zusammenwirken, um umfassende Sicherheit zu gewährleisten und zugleich den administrativen Aufwand zu reduzieren. Durch zentrale Verwaltung, konsistente Benutzeroberflächen und flexible Bereitstellungsmöglichkeiten (MDM, Co-Management, Defender Attach) bietet Microsoft eine ganzheitliche Lösung für die Endpoint-Security.

**✅ Session 24: Effective Prompt Engineering for IT Pros**

**Referenten:**

* **Anur Goel** – Product Manager, Intune Co-Pilot Team
* **Zach Dvorak** – Product Manager, Co-Pilot for Intune
* **Carlos Breo** – Product Manager, Microsoft

**🧠 Ziel der Session:**

IT-Professionals zu zeigen, wie sie **Co-Pilot in Microsoft Intune** und anderen Produkten effektiv nutzen, indem sie **gezielte, strukturierte Prompts (Eingaben)** erstellen – das sogenannte **Prompt Engineering**.

**🚀 Überblick über Co-Pilot in Intune**

**🔍 Aktuelle Funktionen in Public Preview:**

* **Device Insights:** Co-Pilot liefert verwertbare Erkenntnisse zu verwalteten Geräten.
* **Single Device Query:** Abfrage von Echtzeitdaten mit benutzerdefinierten Prompts.
* **Policy Management & Troubleshooting:** Co-Pilot analysiert Richtlinien, erklärt Fehlercodes u. v. m.
* **Enterprise Privileged Management:** Einschätzung von App-Risiken.

**✏️ Zwei Arten von Prompting-Erfahrungen in Intune**

**1. Geleitete Prompts (Scoped Prompting)**

* Vordefinierte, strukturierte Optionen zur Auswahl.
* Beispiel: *Vergleich zweier Geräte* bzgl. Compliance-Policies.
* Benutzer wählt Gerät & Vergleichsbereich – Co-Pilot generiert gezielte Antwort.
* Vorteil: Einfach, benutzerfreundlich, wenig Raum für Fehler.
* Nachteil: Geringe Flexibilität.

**2. Freie Prompts (Open Prompting)**

* Benutzer kann freie Fragen stellen (z. B. zur Registry-Konfiguration).
* Co-Pilot erstellt automatisch eine **Kusto Query (KQL)** basierend auf dem Prompt.
* Beispiel: „Zeig mir den konfigurierten RDP-Port in der Registry dieses Geräts.“
* Vorteil: Maximale Flexibilität.
* Nachteil: Abhängigkeit von der Qualität des Prompts.

**⚙️ Was passiert hinter den Kulissen?**

* Co-Pilot in Intune ist Teil von **Microsoft Security Co-Pilot**.
* Nutzt ein **Plugin-Modell** – z. B. Plugins für Intune, Defender, Entra, Sentinel etc.
* Das **Intune-Plugin** ist für alle Intune-Co-Pilot-Funktionen zuständig.
* Der Kontext aus dem Intune-Portal wird automatisch übermittelt (z. B. Gerätekontext).
* Durch Auswahl von Prompts + Geräten + Datenquellen wird automatisch ein effektiver Prompt konstruiert.
* Vergleich zu Microsoft 365 Co-Pilot:
	+ **Microsoft 365 Co-Pilot:** volle Prompt-Freiheit, aber hohe Verantwortung beim Benutzer.
	+ **Intune Co-Pilot:** eher geführt, aber sicherer und einfacher im IT-Kontext.

**🧩 Einführung in Prompt Engineering (Carlos)**

**Was ist Prompt Engineering?**

* Die Kunst und Wissenschaft, gezielte Prompts zu formulieren, die **präzise und relevante Antworten** von LLMs wie Co-Pilot erzeugen.
* Ziel: Hohe Qualität, Relevanz, Vielfalt und Genauigkeit der Ergebnisse.
* Prompts können Text, URLs, Dateien, Audio, Bilder enthalten.
* **Human-in-the-Loop-Modell**: Mensch gibt kontextualisierte Eingaben → KI antwortet → Mensch bewertet/iteriert.

**🔑 Die 4 Schlüsselelemente eines effektiven Prompts:**

| **Element** | **Beschreibung** | **Beispiel** |
| --- | --- | --- |
| **Ziel (Goal)** | Was will ich erreichen? | „Erstelle eine Liste…“, „Finde…“, „Summarisiere…“ |
| **Kontext (Context)** | Warum brauche ich das? | „Für einen Statusbericht“, „Für eine Urlaubsplanung“… |
| **Erwartung (Expectation)** | In welchem Format? Für wen? | „Als Tabelle für den CIO“, „Bulletpoints für die HR“… |
| **Quelle (Source)** | Woher kommen die Daten? | „Nutze Intune-Daten“, „Greife auf Defender-Logs zu“… |

**📊 Beispiele für gutes vs. schlechtes Prompting**

**Beispiel 1: Nur Ziel**

**Prompt:** „Liste der Feiertage 2025“
➡️ Ergebnis: Allgemeine Liste, lokal basiert, unpräzise.

**Beispiel 2: Ziel + Erwartung**

**Prompt:** „Erstelle eine Liste der US-Feiertage 2025 im Tabellenformat“
➡️ Ergebnis: Tabelle, aber keine Kontext-/Quellenangabe.

**Beispiel 3: Alle 4 Elemente**

**Prompt:**
„Erstelle eine Liste der US-Feiertage 2025 als Tabelle.
Die Daten sind für meine Urlaubsplanung gedacht. Nutze die Feiertage aus der Datei 'company\_holidays.xlsx'.“
➡️ Ergebnis: Präzise, vollständig, korrekt aus der Datei extrahiert.

**💡 Tipps für bessere Prompts**

1. **Spezifisch sein**
	* Bsp.: „Male mir eine Siamkatze, die mit einem Federstab spielt“ statt „Male mir eine Katze“.
2. **Iterieren / Rückmeldung geben**
	* Start: „Gib mir Top-News-Headlines“
	* Dann: „Ohne Sportthemen“ → präzisere Ausgabe
3. **Kontext und Schlüsselwörter verwenden**
	* „Erstelle einen wöchentlichen Paleo-Ernährungsplan <1200 kcal“ statt nur „Ernährungsplan erstellen“

**⚠️ Hinweise zur Nutzung von Co-Pilot & LLMs**

* Antworten können **ungenau** oder **widersprüchlich** sein → **Quellen prüfen!**
* **Antworten variieren** bei gleichen Prompts – aufgrund probabilistischer LLM-Struktur.
* **Verantwortungsvoller Umgang** wichtig: ethisch, legal, respektvoll.
* Microsoft verweist auf eigene **AI Principles & Standards**.

**📚 Weitere Ressourcen**

* Microsoft Learn Artikel zu Co-Pilot
* Prompt Engineering Playbooks
* Dokumentationen zum Microsoft Security Co-Pilot
* Interaktive Leitfäden zum Einstieg in Kusto Queries (KQL)

**🧾 Fazit**

Diese Session ist ein wertvoller Einstieg in das Thema **Prompt Engineering speziell für IT-Professionals**, die Co-Pilot-Funktionen innerhalb von Intune und Microsoft Security besser nutzen möchten. Sie erklärt praxisnah, worauf es bei der Formulierung von Prompts ankommt – sowohl für geführte als auch freie Anwendungsfälle.

**✅ Session 25 Cloud PKI:** Die Session richtet sich an IT-Profis, die Cloud PKI in Microsoft Intune einsetzen oder evaluieren wollen. Sie bietet ein tiefgehendes Verständnis darüber, wie man Cloud PKI optimal konfiguriert, verwaltet und in der Praxis einsetzt – inklusive Tipps, Troubleshooting und Einblicken in zukünftige Entwicklungen.

**🔐 Grundlagen von Cloud PKI**

Cloud PKI ermöglicht die Ausstellung und Verwaltung von Client-Authentifizierungszertifikaten direkt aus Intune – ohne lokale NDES-Server. Es unterstützt:

* Windows, iOS, macOS, Android (Linux nicht unterstützt, da kein SCEP-Profil)
* Vollständiger Lebenszyklus: Ausstellung, Erneuerung, Widerruf
* Verwendung in Ressourcen-Zugriffsprofilen wie Wi-Fi, VPN, E-Mail, Windows Hello for Business
* Zertifikate werden über das cloudbasierte SCEP-Gateway bereitgestellt
* Kein Bedarf mehr an eigener PKI-Infrastruktur oder Firewall-Konfiguration

Besonderheit:

* Für Testumgebungen werden Software-Schlüssel verwendet
* Für Produktivbetrieb kommen Azure Managed HSMs (FIPS 140-2 Level 3) zum Einsatz

**🧹 Löschen einer Cloud PKI CA**

Ein oft gewünschtes Feature war die Möglichkeit, eine CA zu löschen – besonders wichtig bei Umstieg von Test- auf Produktivbetrieb. Seit kurzem können Nutzer:

1. Die CA **pausieren**
2. SCEP-Profile **entsprechen entkoppeln**
3. Alle ausgestellten Zertifikate **widerrufen** (per PowerShell-Skript via Graph API)
4. CA **widerrufen** (unwiderruflich!)
5. CA aus Intune **löschen**

⚠️ Nach dem Widerruf der CA (nicht nur der Zertifikate) gibt es **keinen Weg zurück**.

**🔧 Automatisierung per Graph API**

Es werden zwei Zugriffstypen unterstützt:

* Delegated Permissions: Für interaktive Skripte mit Benutzeranmeldung
* App Permissions: Für Dienste im Hintergrundbetrieb (z. B. Daemons, Dienste)

App Permissions befinden sich derzeit in Entwicklung.

**🔍 Wichtige Besonderheiten beim SCEP-Zertifikatprofil**

* **Subject Alternative Name (SAN)**: URI-Einträge müssen RFC 3986 entsprechen (z. B. ein urn:-Präfix enthalten), sonst schlägt die Ausstellung fehl.
* **SCEP-URL** enthält ein Platzhalter-FQDN ({{CloudPkiFQDN}}), das nicht verändert werden darf. Es dient der intelligenten Lastverteilung im Cloudbackend.
* **EKUs**: Das „Any Purpose“-EKU wird aus Sicherheitsgründen **nicht** unterstützt.

**🛜 Integration mit Network Policy Server (NPS)**

Ein großer Teil der Session widmete sich der Authentifizierung per Zertifikat in Wi-Fi/VPN-Umgebungen via RADIUS (NPS):

* Cloud PKI unterstützt das Microsoft KB5014754-Update (striktere Zertifikatszuordnung via SID)
* SCEP-Zertifikate können automatisch eine SID (Security Identifier) enthalten, wenn sie von Geräten/Benutzern aus AD stammen
* **Entra-only-Geräte (Azure AD joined)**:
	+ **User-Auth** funktioniert, wenn Benutzerobjekt auch in AD existiert
	+ **Device-Auth** funktioniert **nicht**, da kein AD-Geräteobjekt → kein SID
* **Hybrid Join (AD + Entra)**:
	+ Sowohl User- als auch Device-Auth via NPS funktionieren

Wichtig: Der NPS-Server muss der CA (inkl. Root- und Intermediate-Zertifikaten) vertrauen. Dies kann über PKIVIEW.msc eingerichtet werden.

**🧪 Zwei PKI-Topologien im Vergleich**

**1. Cloud-only PKI**

* Root- und Issuing-CA befinden sich komplett in Intune
* Alle On-Prem-Relying-Services (z. B. NPS) benötigen die Cloud-Zertifikatskette als Vertrauensanker

**2. BYOCA (Bring Your Own Certificate Authority)**

* Die Cloud-PKI-CA wird von einer bestehenden ADCS-CA signiert
* Vorteil: Kein zusätzlicher Vertrauensaufbau notwendig, da On-Prem-Dienste die CA bereits kennen

**📈 Verbesserungen und Roadmap**

**Bereits umgesetzt:**

* **Unbegrenzte Anzeige von Zertifikaten** in der Leaf-Zertifikatsliste (vorher max. 1.000)
* Neues UI mit Infinite Scroll in React

**In Planung:**

* Cloud PKI für Government Cloud High (spätere H2 2025)
* Post-Quantum-Kryptographie (PQCrypto) für Zertifikate
* App-Only Permissions via Graph API für vollständige Automatisierung

**🧠 Fazit**

Die Session vermittelt tiefgehendes Know-how über die moderne Zertifikatsbereitstellung mit Cloud PKI. Sie verdeutlicht Vorteile gegenüber klassischen on-prem Lösungen, beleuchtet Integrationsszenarien mit NPS, klärt häufige Stolperfallen (z. B. SAN, EKUs) und bereitet auf künftige Entwicklungen wie PQCrypto und Gov Cloud vor.

**✅ Session 26: Get to know Windows security and resiliency in the cloud“**

**🛡️ Teil 1: Sicherheit in der Cloud mit Windows**

**🔐 Zero Trust – Microsofts Sicherheitsstrategie**

Die vorgestellten Funktionen sind im Rahmen der Zero-Trust-Strategie positioniert. Ziel ist es, Gerätezugriffe unabhängig von Netzwerkgrenzen abzusichern – durch starke Authentifizierung, Gerätesicherheit, Datenkontrolle und minimalen Rechtezugriff.

**🔑 Passkeys mit Microsoft Authenticator**

* **Einfache Konfiguration** in Entra ID: Passwortlose Anmeldung aktivieren und „Authenticator“ auswählen.
* **Funktioniert auf** iOS und Android.
* **Vorteile**:
	+ Keine Hardware-Sicherheits-Keys notwendig.
	+ Kein Merken von Passwörtern.
	+ Nutzer können auf Reisen (z. B. via iPad) über Windows 365 auf ihren Arbeitsplatz zugreifen – sicher, bequem, überall.

**🔄 Hotpatching für Windows 11**

* **Ohne Neustart patchen** – verfügbar auf:
	+ Windows 11 Enterprise
	+ Azure Virtual Desktop (AVD)
	+ Windows 365 Cloud-PCs
* **Voraussetzungen**:
	+ Windows 11 Enterprise, Version 24H2
	+ Microsoft-Subscription mit Intune
* **Aktivierung** über Intune Update-Policy (einfacher Schalter)
* **Vorteile**:
	+ Sicherheitsupdates ohne Neustarts
	+ Erhöhte Verfügbarkeit von Cloud-basierten Workloads

**📱 Sichere Verbindung von BYOD- und Partnergeräten mit MAM (Mobile Application Management)**

* **MAM auf iOS/Android** erlaubt:
	+ Abfrage von OS-Version
	+ Gerätezustand (z. B. Bedrohungsstatus)
	+ Erzwingen von Sicherheitsrichtlinien (z. B. PIN-Eingabe)
	+ Gerätespezifisches Verhalten bei Laufwerksweiterleitungen
* **Demobeispiel**:
	+ Firmengerät: Zugriff mit Weiterleitung erlaubt
	+ Privates iPad: Richtlinien greifen (PIN, keine Laufwerksfreigabe)

**🚫 Screenshots verhindern – Schutz vor Datenabfluss**

* **Bildschirmaufzeichnungsschutz** auf iOS & Android via Intune MAM
* **Windows/Mac**: Empfehlung, systemeigene Mechanismen und App-Richtlinien zu nutzen
* **Konfiguration**: Einfache Richtlinie (z. B. Send org data = None)

**📋 Datenverluste verhindern mit Microsoft Purview**

* **Adaptive Protection mit Entra-Integration**
* Dynamisches DLP – z. B. Blockieren von Copy/Paste mit Optionen:
	+ Komplett blockieren
	+ Auditieren
	+ Block mit Begründung (z. B. geschäftlicher Bedarf)

**🔁 Unidirektionale Zwischenablage**

* **Richtungskontrolle** für Copy/Paste:
	+ z. B. nur vom Cloud-PC ➡️ Lokal erlaubt
	+ Umgekehrte Richtung ❌ blockiert
* **Inhalte definierbar**: Nur Text, keine Bilder/Dateien
* **Unabhängig von Dateiweiterleitungen konfigurierbar**

**🧱 Teil 2: Cloud-Resilienz mit Windows 365 und AVD**

Die Resilienz wird in drei Schichten betrachtet:

1. **Connectivity Platform** (Netzwerkzugriff)
2. **Management Platform** (Verwaltung & Bereitstellung)
3. **Workload Resiliency** (Verfügbarkeit der PCs/Sitzungen)

**🌐 1. Resilienz der Verbindungsinfrastruktur**

* **Azure Front Door** als weltweiter Einstiegspunkt (300+ Edge-Standorte)
* **Automatische Wahl** der schnellsten Region (niedrigste Latenz)
* **RDP Shortpath** für UDP – optimierte Performance
* **Mehrere Instanzen pro Region & Multi-Region-Support**
* **Failover** bei regionalem Ausfall möglich (automatisiert)
* Aktive Infrastruktur in **ca. 40 Azure-Regionen weltweit**

**⚙️ 2. Resiliente Verwaltungsplattform**

* **Verteilt auf mehrere Availability Zones pro Region**
* **Cross-regionale Ausfallsicherheit**
* Unterstützt z. B.:
	+ Azure Network Connection Checks
	+ Windows 365 Managementdienste
* Sichtbarkeit: Deployments in grünen Regionen (Cloud-PCs), Skalierungseinheiten grau

**💻 3. Workload Resiliency – AVD-Sessionhosts**

**✅ Verfügbarkeitszonen (AZs)**

* **Verteilung von Hosts über 3 AZs empfohlen**
* **1 AZ-Ausfall = nur ⅓ der Hosts betroffen**
* **Reduziert Blast Radius**, kein Ersatz für vollständige DR

**🔄 Azure Site Recovery (ASR)**

* **Replikation + automatisierte Wiederherstellung**
* **Kostenpflichtig**, aber starke SLA
* Ideal für kritische Workloads

**⚒️ Alternative: Schnelle Neubereitstellung**

* Per **Infrastructure-as-Code** (z. B. Azure DevOps)
* Voraussetzung: gepflegtes **Golden Image**

**📖 Azure Virtual Desktop Proactive Resiliency Library (APRIL)**

* Teil des **Cloud Adoption Frameworks**
* Enthält:
	+ Best Practices für Hosts, FSLogix, Storage, Netzwerk
	+ Scripts zur **Analyse der Resilienzkonformität**

**🖥️ Workload Resiliency – Windows 365 Cloud-PCs**

**🕒 Point-in-Time Restore**

* **Snapshots alle 4–24 Stunden** (bis zu 10)
	+ 1 Snapshot pro Woche (4 Wochen)
* **Restores durch Admins oder Nutzer** (Self-Service)
* **Erfolgreicher Einsatz bei CrowdStrike-Ausfall** – einfache Rückkehr zum vorherigen Zustand

**🌍 Cross-region Disaster Recovery**

* **Snapshot-Replikation in andere Azure-Region**
* **Wiederherstellung bei Region-Ausfall**
* Snapshot liegt in 3 AZs
* Höhere RPO (Recovery Point Objective), mittlere RTO (Recovery Time)

**⏱️ Windows 365 Disaster Recovery Plus**

* **Snapshots alle 60 Minuten**
* **Replikation in andere Region + laufende Generic Cloud PC Instanz**
* Bei Wiederherstellung: **Disk Swap & Neustart**
* **Sehr niedrige RTO (< 30 Min) & RPO (< 60 Min)**
* **Separate Session „WCX04“ empfohlen**

**🧠 Fazit**

Microsofts Cloud-Strategie für Windows zielt auf:

* **Maximale Sicherheit** für jede Nutzerkonstellation (BYOD, Contractors, Managed Devices)
* **Höhere Verfügbarkeit** durch Hotpatching und Cloud-PC-Backupmechanismen
* **Weltweite Resilienz** auf Netzwerk-, Verwaltungs- und Workloadebene
* **Moderne Wiederherstellungsoptionen**, automatisierbar und benutzerfreundlich
* **Klare Empfehlungen** für AVD- & Windows 365-Betrieb (z. B. 3x AZ, APRIL, ASR)

**✅ Session 27: Windows 11 Kiosks: Cloud Management for the Win**

**Referent:** Steven Hosking (Microsoft)

**Überblick:**

Diese Session beleuchtet die Weiterentwicklung und Verwaltung von Kioskumgebungen in Windows 11 im Vergleich zu Windows 10, insbesondere unter Nutzung von Intune. Sie richtet sich an IT-Administratoren, die Windows-Kioskgeräte bereitstellen und verwalten möchten, sowohl im Single-App- als auch im Multi-App-Szenario.

**1. Grundlagen: Was ist ein Windows-Kiosk?**

Ein Kiosk-Modus ermöglicht es, Geräte für spezifische Zwecke zu sperren, z. B. für Digital Signage, Selbstbedienungsterminals oder eingeschränkte Arbeitsstationen. In Windows 11 basiert der Kioskmodus auf der **Assigned Access CSP**.

**Zwei Hauptszenarien:**

* **Single-App-Kiosk**: Nur eine App (z. B. Microsoft Edge) wird ausgeführt. Ideal für Digital Signage.
* **Multi-App-Kiosk / „Restricted User Experience“**: Mehrere Anwendungen mit stark eingeschränkter Benutzeroberfläche. In Windows 11 wurde das Konzept „Tablet Mode“ entfernt und durch neue Steuerelemente ersetzt.

**2. Änderungen von Windows 10 zu Windows 11**

* Entfernen des **Tablet-Modus**
* Entfernen oder Einschränkung von Systemkomponenten wie:
	+ **Widgets**
	+ **Task View**
	+ **Get Started / Dev Home**
	+ **Desktop-Icons**
	+ **Recycle Bin**
	+ **Edge ohne Einschränkung**
* Umstellung der **Startmenü-Layoutdefinition von XML auf JSON**
* Weiterentwicklung der „Restricted User Experience“ für Multi-App-Kiosks

**3. Single-App-Kiosk in der Praxis**

* Kann über Intune-Vorlage eingerichtet werden.
* Empfehlung: **Auto-Login via Entra ID oder lokales Konto** konfigurieren (z. B. über PsTools).
* Einschränkung: Private-Browsing-Modus in Edge verhindert automatisches Login (gewollt in Zero-Trust-Szenarien).
* Möglichkeit zur Nutzung von Edge in **Kiosk-Fullscreen-Mode** über spezifische CMD-Zeile mit Parametern (--kiosk, --edge-kiosk-type=fullscreen etc.).
* Wichtig: **Startup Boost von Edge deaktivieren**, um volle Kontrolle zu behalten.

**4. Multi-App-Kiosk (Restricted User Experience)**

* Kein klassischer Tablet-Modus mehr, sondern detaillierte Steuerung über **Assigned Access XML**.
* Startmenü kann auf definierte Apps beschränkt werden.
* Erweiterte Steuerung über AppLocker-Regeln:
	+ Welche Prozesse erlaubt sind (z. B. Explorer, PowerShell, Command Prompt)
	+ Welche Startmenüeinträge angezeigt werden
	+ Separate Konfiguration für unterschiedliche Benutzerprofile möglich

**Tipps:**

* **Erst lokal via PowerShell testen**, bevor man Intune nutzt
* Visual Studio Code verwenden, um XML-Fehler zu vermeiden
* XML-Schema beachten (je nach OS-Version)
* Taskbar kann vollständig deaktiviert werden
* Einfache Fehler wie fehlende Kommata in JSON verursachen Komplettversagen der Richtlinie

**5. Sicherheitsmaßnahmen & Einschränkungen**

* Edge kann gezielt entfernt oder deaktiviert werden
* Zugriff auf sensible System-Apps wie Einstellungen oder PowerShell kann unterbunden werden
* **Online-Support-Links im Windows Settings UI** können via Intune blockiert werden
* Breakout-Möglichkeiten lassen sich weitgehend verhindern (z. B. STRG+ALT+ENTF sperren)

**6. Empfohlene Vorgehensweise**

1. **Lokale Tests mit PowerShell & XML-Policy**
2. Nach erfolgreicher Validierung: **Deployment via Intune**
3. Einsatz von **Assigned Access CSP mit Custom XML** für maximale Kontrolle
4. Nutzung von Richtlinien für Startmenüsteuerung, Edge-Verhalten, AppLocker

**7. Fazit & Best Practices**

* Windows 11 bietet umfangreiche, aber komplexe Möglichkeiten für Kiosk-Szenarien
* Microsoft arbeitet aktiv an der Verbesserung der Template-Unterstützung in Intune
* Der Wechsel von XML zu JSON im Startmenü ist technisch herausfordernd, aber notwendig
* **Klares Ziel**: Minimalistische, sichere und unternehmensspezifisch kontrollierbare Benutzeroberfläche

**✅ Session 28: Never trust, always verify: Tips for Zero Trust with Intune**

Diese Session richtet sich an **IT-Profis** und zeigt, wie man **Barrierefreiheitsfunktionen von Windows 11** gezielt **bereitstellt, vorkonfiguriert und verwaltet**, um inklusive IT-Erfahrungen zu ermöglichen – ohne dass betroffene Nutzer\*innen dafür spezielle Anfragen stellen müssen.

**Referenten:**

* *Hajja Dalaal* – Senior Product Marketing Manager
* *Ben W* – Cloud Solution Architect & Accessibility Champion

**🧑‍💻 1. Live Captions & Voice Access: Sprache lokal, ohne Cloud**

**💡 Funktionen:**

* **Live Captions (Windows + Ctrl + L):** Untertitel für Systemaudio, Mikrofon und Medien – **offlinefähig**
* **Voice Access (Windows + Ctrl + S):** Steuerung des PCs mit Sprache (nicht nur Diktieren, auch Navigation und eigene Sprachbefehle)

**🎯 Voraussetzung: Sprachpakete**

* Beide Funktionen benötigen **lokale Sprachpakete**, die **automatisch aus dem Microsoft Store geladen** werden – wenn nicht geblockt oder offline
* Sprachpakete sind meist **zwischen Voice Access und Live Captions gemeinsam nutzbar**, aber:
	+ Live Captions unterstützt mehr Sprachen
	+ **Copilot+ PCs benötigen eigene ARM64-Pakete**

**🧰 Verwaltung:**

* Sprachpakete können per **Intune als Store App** verteilt werden
* Wichtig: Dazu braucht man die **Product ID** der Store-App, die man z. B. über die Store-Download-Historie oder Registry ausliest
* Intune App-Deployment:
	+ App-Typ: *Store-App (neues Erlebnis)*
	+ Installationsverhalten: *System*
	+ Zuweisung: z. B. *an alle Geräte*
	+ *Keine Toast-Benachrichtigungen*, um UX nicht zu stören

**📦 Offlineverteilung:**

* Nur das **englische (US)** Sprachpaket steht als .msix über offiziellen Microsoft-Link zur Verfügung:
aka.ms/windows/speechstorepackages

**🌍 2. Speech Translation Packs auf Copilot+ PCs**

**🧠 Kontext:**

* Copilot+ PCs unterstützen **Live-Untertitel mit automatischer Übersetzung** ins Englische (US)
* Dafür ist ein separates **Speech Translation Pack** notwendig

**🎯 Deployment:**

* Ebenfalls per **Store App mit Product ID** über Intune
* Filtert die Zuweisung auf **ARM64-Geräte** (CPU-Architektur = ARM64)

**🎙 3. Narrator & natürliche Stimmen**

**👓 Funktion:**

* *Narrator* ist der integrierte Screenreader für blinde oder sehbehinderte Personen

**🗣 Natürliche Stimmen (Natural Voices):**

* Bieten angenehmeren, „menschenähnlichen“ Klang für langfristige Nutzung
* Müssen **manuell oder zentral installiert** werden (nicht automatisch vorinstalliert)
* Sprachpakete heißen z. B. Microsoft Windows Voice Sonia

**🔧 Verwaltung:**

* Auch hier über Store-Link → Product ID kopieren → Intune Store-App erstellen
* Kann ebenfalls per Registry und PowerShell analysiert oder entfernt werden

**🔐 4. Voice Access beim Anmeldebildschirm aktivieren**

* Ermöglicht Sprachsteuerung bereits **vor dem Login** (z. B. Eingabe des Passworts)
* Option muss **manuell aktiviert** werden – erfordert **Adminrechte**
* Lösung: Verteilung eines **Registry-Keys** über Intune

reg

KopierenBearbeiten

[HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Accessibility]

"Configuration"="voiceaccess"

➡️ Deployment per **Remediation Script**, PowerShell oder gezielte Intune-Richtlinie

**⚙️ 5. Zugriff auf Barrierefreiheitseinstellungen nicht blockieren**

**⚠️ Problem:**

* In Bildungseinrichtungen, Kiosks oder restriktiven Umgebungen wird oft der **Zugriff auf die App „Einstellungen“ eingeschränkt**
* Viele Barrierefreiheitsfunktionen haben zwar Tastenkombinationen, aber **Detailanpassungen erfordern die Einstellungs-App**

**✅ Lösung:**

* Nutzt den **„Settings Page Visibility“-Mechanismus**, um **nur Barrierefreiheitsseiten** freizugeben

**Beispiele:**

* easeofaccess-display
* easeofaccess-narrator
* easeofaccess-keyboard
* easeofaccess-hearingaids (NEU in 24H2)

➡️ Die vollständige Liste der Sichtbarkeiten kann über ms-settings:easeofaccess-<funktion> getestet werden

**🧩 6. Weitere Empfehlungen**

* **Microsoft Adaptive Accessories**:
	+ Unterstützen alternative Eingabemethoden
	+ **Microsoft Accessory Center App** bereitstellen (Store-App, kein Product ID nötig)
* **Microsoft 365 Accessibility Baseline**:
	+ Im **M365 Apps Admin Center** verfügbar
	+ Optimale Einstellungen für Office-Apps hinsichtlich Barrierefreiheit
* **Kanalwahl**: Am besten *Current Channel* oder *Monthly Enterprise* nutzen, um aktuelle Accessibility-Features zu erhalten

**🫱 Fazit & Call to Action**

* Seid **Allies für Barrierefreiheit**
* Macht Accessibility zur **Standardfunktion**, nicht zur Ausnahme
* Nutzer\*innen sollten nicht erst „anfragen müssen“, um barrierefrei arbeiten zu können
* Verteilt proaktiv:
	+ Sprach- & Voice-Pakete
	+ Natural Voices
	+ Registrierungswerte
	+ Einstellungen über Intune & Store
* Nutzt Microsoft Docs & Blogposts für Updates

**✅ Session 29: Data protection with hardware-based security and Windows 11**

**🧩 Ziel der Session**

Die Session zeigt auf, **wie Windows 11 Daten auf Geräten schützt**, indem es **Hardware-gestützte Sicherheitsfunktionen** nutzt – vor allem:

* **BitLocker** (Volume-basierte Verschlüsselung)
* **Personal Data Encryption (PDE)** (benutzerzentrierte Datenverschlüsselung)
* Einsatz von **TPM** (Trusted Platform Module), **Root of Trust** und **Microsoft Pluton**

**🛡 1. Warum überhaupt Daten schützen?**

* Im *Informationszeitalter* sind Daten wertvoll und angreifbar
* Angriffe zielen auf:
	+ **Offline-Angriffe** (z. B. physischer Zugriff, Geräteaustausch)
	+ **Manipulation des Betriebssystems**
	+ **Speicher- oder Bootkits**
* Ziel: **Schutz von Daten im Ruhezustand** (at rest), nicht Transit oder Cloud (außerhalb des Fokus dieser Session)

**🔐 2. BitLocker – Schutz auf Volume-Ebene**

**📌 Funktion:**

* **Verschlüsselt gesamte Volumes** (z. B. Systemlaufwerk)
* **Verhindert Zugriff auf Daten** bei:
	+ Diebstahl oder Verlust des Geräts
	+ Manipulierten Bootkonfigurationen
	+ Unvollständiger Deinstallation

**🔑 TPM-Integration:**

* Bei Geräten **mit TPM**:
	+ Verifikation der **Bootintegrität**
	+ Entschlüsselung nur bei **unverändertem Systemzustand**
* Bei Geräten **ohne TPM**:
	+ Start mit **Startschlüssel** oder **Kennwort** möglich, aber unsicherer (anfällig für Brute-Force)

**🛠 Deployment:**

* Aktivierbar über:
	+ Intune
	+ Manuelle Aktivierung
	+ Autopilot-Geräteverschlüsselung
	+ **Standardmäßig aktiviert** auf *Copilot+ PCs* (Secure-by-Default-Prinzip)

**🔒 3. Personal Data Encryption (PDE) – Schutz auf Nutzerebene**

**📌 Funktion:**

* Verschlüsselt **Benutzerdaten (Dateien, Ordner)**
* **Zugriff nur bei Windows Hello-Authentifizierung** (PIN, Biometrie)
* Schutz bei:
	+ Direktzugriff auf Speicher (DMA-Angriffe)
	+ Login-Bypass
	+ Festplattendiebstahl

**🔁 Zwei Schutzstufen:**

* **Level 1 (L1)**: Schutz bis zur ersten Authentifizierung nach Login/Neustart
* **Level 2 (L2)**: Schlüssel werden nach Sperrbildschirm automatisch **aus RAM entfernt**

**💾 Technische Basis:**

* Nutzt Schlüssel aus dem TPM, gespeichert in der **NGC-Containerstruktur**
* Wenn **kein TPM vorhanden** → Rückfall auf **DPAPI-Modus** (kennwortbasiert, weniger sicher)

**📦 Verfügbarkeit:**

* Nur in **Enterprise- und Education-Versionen** von Windows 11
* Aktivierbar per **Intune (MDM)**

**🚀 Releases:**

* **Windows 11 22H2**: PDE-API für App-spezifische Nutzung
* **Windows 11 24H2**: PDE für *Known Folders* (Desktop, Dokumente, Bilder)

**🧠 4. TPM – Trusted Platform Module**

**📌 Aufgaben:**

* Hardware-Chip auf dem Mainboard
* Generiert, speichert & schützt **Kryptoschlüssel**
* Unterstützt:
	+ Root of Trust
	+ BitLocker und PDE
	+ Plattform-Messungen (z. B. Hashes von Boot-Komponenten)

**🔁 Messwerte & PCRs:**

* TPM speichert Hash-Werte („Messungen“) in **Platform Configuration Registers (PCRs)**
* Schlüsselfreigabe nur, wenn aktuelle Hashes mit den ursprünglichen übereinstimmen
* Schutz gegen Manipulation der Bootkette (z. B. durch Bootkits)

**🪪 5. Root of Trust & Secure Boot**

**🧩 Problem früher:**

* **Rootkits/Bootkits** starten vor Windows → höchste Privilegien, schwer zu erkennen

**✅ Lösung:**

* Seit Windows 10:
	+ Moderne Hardware verlangt **UEFI Secure Boot**
	+ UEFI + TPM = **Hardwarebasierter Root of Trust**
	+ Nur **authentifizierte Firmware/Software** darf vor Windows starten

**💠 6. Microsoft Pluton – Moderne Sicherheit im Chip**

**🧩 Was ist Pluton?**

* **Sicherheitsprozessor von Microsoft**, in Zusammenarbeit mit **AMD, Intel, Qualcomm**
* Unterstützt oder ersetzt TPM
* Speichert:
	+ **Zugangsdaten**
	+ **Schlüssel**
	+ Bietet **attestierte Kryptografie-Funktionen**

**🔧 Vorteile:**

* Pluton erhält **Firmware-Updates direkt von Microsoft**
* Teil der **Secure Future Initiative**
* **Standardmäßig aktiviert** auf **Copilot+ PCs**

**🔚 Fazit – Zusammenspiel von Hard- und Software**

* **BitLocker** schützt Systemdaten **bis zum Login**
* **PDE** schützt Benutzerdaten **nach dem Login**, gesteuert über Windows Hello
* Beide Technologien **arbeiten unabhängig**, teilen sich aber den **TPM**
* Alles fußt auf:
	+ **TPM-basierter Root of Trust**
	+ **Secure Boot**
	+ **Pluton (neuere Geräte)**

**✅ Session 29: Best practices for Windows Autopilot and device preparation**

**🎯 Ziel der Session**

Diese Session bietet eine umfassende Gegenüberstellung und *Best Practices* zur Fehlerbehebung bei:

* **Windows Autopilot** (klassische Lösung)
* **Windows Autopilot Device Preparation** (neue, modernisierte Lösung)

Ziel: **Fehler vermeiden, reibungslose Bereitstellung sicherstellen** und Klarheit schaffen, **wann welche Lösung** geeignet ist.

**⚖️ 1. Vergleich: Autopilot vs. Autopilot Device Preparation**

| **Aspekt** | **Windows Autopilot** | **Autopilot Device Preparation** |
| --- | --- | --- |
| **Funktionsumfang** | Größere Flexibilität, z. B. Hybrid Join | Vereinfachtes, zuverlässigeres Setup |
| **Zielgruppen** | Beste Wahl bei komplexeren Szenarien (z. B. Hybrid AD Join) | Ideal für **Cloud-native Bereitstellung** |
| **Konfiguration** | Zwei Richtlinien nötig: Deployment Profile + ESP | **Nur eine** Device Preparation Policy |
| **Gruppenzuweisung** | Dynamische Entra-ID-Gruppen | **Enrollment-time Grouping** |
| **App-Bereitstellung** | Einschränkungen bei gleichzeitiger Nutzung von LOB & Win32-Apps | **Serielle, zuverlässige Bereitstellung** inkl. bis zu 10 PowerShell-Skripten |
| **Fehleranalyse** | Eingeschränkt, nicht in Echtzeit | **Umfangreiche Live-Diagnose direkt im Intune-Portal** |

**🔍 2. Troubleshooting: Windows Autopilot**

**🔧 Bekannte Probleme & Empfehlungen**

**a) Registrierung**

* ❌ *Autopilot-Gerät verschwindet aus Intune*: Häufig durch OEM oder Partner gelöscht → **Neu registrieren**
* ❌ *Mainboard-Tausch*: Gerät **vorher deregistrieren**, dann neue Hardware-Hash erfassen und **neu hochladen**
* ❌ *Geräte im Status „pending“ oder „attention required“*: Empfehlung → **neu registrieren**

**b) Enrollment Status Page (ESP)**

* Fehlercode bei Enrollment:
→ Prüfen, ob **MDM Enrollment erlaubt ist** und ob **Enrollment Restrictions korrekt** gesetzt sind
* *Web Sign-In fehlt nach Pre-Provisioning*:
→ Prüfen, ob **Password Policies auf „Not configured“** gesetzt sind
* *Required Apps fehlen nach Autopilot Reset*:
→ **Wird erwartet**, Apps installieren sich **nach dem Login**

**c) Fehler bei Deployment Profile**

* Prüfen, ob Profile **korrekt zugewiesen** wurden (Intune-Portal)
* JSON-Datei in OOBE enthält wichtige Metadaten zur Fehlersuche
* Ereignisprotokolle (Event Viewer) helfen bei Ursachenanalyse

**d) Typische Fehlercodes**

| **Fehlercode** | **Bedeutung** | **Empfehlung** |
| --- | --- | --- |
| **0x80180014** | Hardware-Mismatch (z. B. nach Boardtausch) | Gerät deregistrieren & neu registrieren |
| **0x80180002** | Gerät nicht registriert | Hardware-Hash prüfen & hochladen |
| **0x80180009** | Profil nicht gefunden | Neues Profil zuweisen & neu registrieren |
| **0x8018000a** | Kein Profil zugewiesen | Profil korrekt zuweisen |

**🆕 3. Device Preparation – Neue Lösung im Fokus**

**🔄 Ablauf der Bereitstellung (Schritt für Schritt)**

1. **Vorbereitung (durch Admin):**
	* Erstellen einer Device Preparation Policy mit:
		+ Apps
		+ PowerShell-Skripten
		+ Zielgruppe (Security Group)
	* Apps und Scripts **müssen** der Zielgruppe zugewiesen werden
2. **Voraussetzungen am Gerät:**
	* Kein Autopilot-Eintrag (sonst wird *immer* Autopilot verwendet)
	* Netzwerkverbindung zuverlässig
	* Windows 11 Pro oder Enterprise
	* Nur **Entra Join** wird unterstützt
3. **Ablauf während OOBE:**
	* Benutzer meldet sich an (Azure AD)
	* Entra Join + MDM Enrollment
	* Installation der Intune Management Extension
	* **Serielle Anwendung von:**
		+ Richtlinien, LOB-Apps, M365 Apps
		+ PowerShell-Skripte
		+ Win32 & Store-Apps
	* Kombinierter Reboot
	* Windows Hello Setup
	* Nachbereitende Bereitstellung weiterer Inhalte am Desktop

**🛠 4. Troubleshooting: Device Preparation**

**📊 Diagnose & Monitoring**

* Im Intune-Portal unter **„Device Monitor → Preparation Report“**
* Dort: detaillierter Phasenverlauf & Hinweise auf Fehlerursache

**❗ Häufige Fehler und Lösungen**

| **Problem** | **Ursache** | **Lösung** |
| --- | --- | --- |
| **Gerät nicht eingeschrieben** | Enrollment Restriction greift | Gerät als **„Corporate“** kennzeichnen durch Identifier |
| **ESP erscheint trotz Device Prep** | Gerät ist **noch bei Autopilot registriert** | Autopilot-Eintrag löschen |
| **Policy lässt sich nicht speichern** | Owner-Berechtigung für Gruppe fehlt | Intune Provisioning Client als **Owner** setzen |
| **Apps wurden übersprungen** | - Apps nicht zugewiesen- Installationskontext nicht „System“- Manage Installer aktiviert | App-Zuweisung, Kontext & Richtlinie prüfen |
| **Timeout während Deployment** | Installationsdauer zu lang | Timeout-Wert in Device Preparation Policy erhöhen |

**🧠 5. Wichtige Hinweise & Best Practices**

* **App- und Skript-Fehler lassen sich oft schon im Vorfeld vermeiden**, indem man sie *außerhalb von Autopilot testet*
* **Netzwerkverfügbarkeit und Endpunkt-Erreichbarkeit** sind kritisch
* **Reihenfolge und Zuweisung** der Apps/Skripte beachten
* **Win32 & Winget-Apps** erfordern zusätzliche Prüfung bei aktivierter „Managed Installer“-Policy

**✅ 6. Fazit**

* **Autopilot Device Preparation** ist der empfohlene Weg für moderne, Cloud-native Deployments
* Autopilot bleibt relevant für **komplexere Szenarien**
* **Vermeidung typischer Fehler** durch:
	+ Korrekte Zuweisungen
	+ Vorab-Tests
	+ Nutzung der Intune-Reports
* Ziel: **Stabile und reibungslose Bereitstellungen mit bestmöglichem Endnutzererlebnis**

**✅ Session 30: Intune data platform and Advanced Analytics**

**💡 Zusammenfassung: Intune Data Platform & Advanced Analytics**

**1. Überblick: Device Inventory & Resource Explorer**

* **Ziel**: Bessere Transparenz über Gerätedaten und gezielte Diagnosemöglichkeiten direkt in Microsoft Intune.
* **Device Inventory**: Erfassung detaillierter Geräteinformationen wie CPU, Akku, OS-Version etc. per konfigurierbarem **Properties-Katalog**.
* **Resource Explorer**: Anzeige dieser Daten für einzelne Geräte – **on demand** (innerhalb von 2–24 h), z. B. für Troubleshooting oder Upgrade-Entscheidungen.
* Aktuell nur für **Windows-Geräte**, **Plattformübergreifende Unterstützung** ist in Arbeit.
* In der Intune-Lizenz enthalten, kein Zusatzmodul nötig.

**2. Multi-Device Query (MDQ)**

* **Funktion**: Abfragen über die gesamte Geräteflotte mit **Kusto Query Language (KQL)**.
* Basiert auf den Daten aus „Enhanced Device Inventory“ → vorherige Konfiguration erforderlich.
* Unterstützt **Joins**, Aggregationen und Funktionen.
* **Natural Language to KQL (NL-to-KQL)** mit Copilot: Admins können in natürlicher Sprache Fragen formulieren, die automatisch in KQL umgewandelt werden.

**3. Unterschiede: Single Device Query vs. Multi-Device Query**

| **Merkmal** | **Single Device Query (SDQ)** | **Multi-Device Query (MDQ)** |
| --- | --- | --- |
| Datenquelle | Echtzeit | Cache aus Inventory |
| Zugriff | Pro Gerät | Geräteübergreifend |
| Sensible Daten | Möglich | Eher nicht |
| Zielgruppe | Techniker, die akut Fehler analysieren | IT-Admins, die Flottenanalysen durchführen |

**4. Technische Architektur (MDQ)**

* **Ablauf**: Intune UI → Graph API (intern) → Pivot-Service → AQS-Backend → Inventory Service → Antwort.
* **„device“ als implizites Join-Element**: Wird standardmäßig jeder Abfrage hinzugefügt. Erlaubt einfache Verknüpfung mit der Geräte-ID.

**5. Voraussetzungen & Einschränkungen**

* **Lizenzierung**: Intune Suite oder Advanced Analytics Standalone SKU erforderlich.
* **Berechtigungen**: „Managed devices query“-Recht nötig.
* **Gerätevoraussetzungen**: Windows 10+, firmeneigen, Intune- oder Co-Management.
* **Abfrage-Limitierungen**:
	+ Max. 3 Joins pro Abfrage
	+ Max. 10 Abfragen/Minute
	+ Max. 500.000 Zeilen pro Abfrage (kein Fehler bei Überschreitung im ersten Release)
	+ Max. Laufzeit: 4 Minuten
* **Kein Graph API-Zugriff für MDQ** (noch nicht verfügbar).

**6. Geplante Weiterentwicklungen**

* Timestamps je Entität für bessere **Daten-Freshness**
* **Sample Queries** als klickbare Vorlagen im UI
* Doppelklick auf Properties → Auto-Vervollständigung im Editor
* Aktionen aus Abfragen heraus: Rename, Log Collection
* Erweiterung auf Nicht-Windows-Geräte
* Datenexport (z. B. CSV)
* Automatisierte Skriptausführung bei Query-Ergebnissen
* Abfragen auf App-Ebene (App Inventory)
* Benutzerdefinierte Inventory-Variablen

**✅ Session 30: Intune data platform and Advanced Analytics**

**Enhancing Resiliency with Windows 365 – Zusammenfassung**

**1. Ziel der Session**

Andrej Radinger und Doug Coombs stellen Resilienz-Features von **Windows 365** vor, mit Fokus auf **Business Continuity**, **Disaster Recovery**, **Point-in-Time Restore** und **Cross-Region Disaster Recovery**.

**2. Bedeutung von Resilienz**

* Resilienz ist essenziell für Geschäftskontinuität im Falle von Katastrophen oder Systemausfällen.
* Beispiel: CrowdStrike-Ausfall 2023 → führte zu Bluescreens und Ausfällen.
* Wichtigkeit von Kommunikationsplänen, Wiederherstellungsmöglichkeiten und schneller Fehlerbehebung wurde unterstrichen.

**3. Architektur: Built-in Resilience**

Windows 365 nutzt:

* Globale Azure-Infrastruktur mit regionalen Clustern (keine Single Points of Failure).
* Redundante Dienste: verteilte Storage-Systeme, replizierte Datenbanken, resilient Azure-Komponenten.
* Vollständig verwaltet – kein manuelles Setup von Infrastruktur nötig.

**4. Point-in-Time Restore (PITR) – Wiederherstellung zu früherem Zustand**

* Lässt Admins oder Nutzer einen **Cloud PC** auf einen früheren Zustand zurücksetzen.
* Nützlich bei:
	+ OS-Problemen
	+ Benutzer-/Adminfehlern
	+ Malware
	+ Update-Problemen (z. B. CrowdStrike-Fall)
* 95 % der Kunden nutzen dieses Feature zur Selbsthilfe.

**Konfiguration und Nutzung**

* Konfigurierbar über Intune:
	+ Restore-Frequenz (4–24h)
	+ Nutzer können Restore selbst ausführen (optional).
* Restore auf Einzelgerät oder **Bulk-Restore** für mehrere Geräte gleichzeitig möglich.
* System erkennt Infrastruktur-Ausfall automatisch und migriert Restore in gesunde Zone derselben Region.

**5. Erweiterte DR: Cross-Region Disaster Recovery & Disaster Recovery Plus**

**a. Cross-Region Disaster Recovery (CRDR)**

* Kopie des letzten Restore-Points wird in **andere Region** repliziert.
* Admins wählen Zielregion selbst.
* RTO (Wiederherstellungszeit): **< 4 Stunden**
* RPO (max. Datenverlust): **< 4 Stunden**
* 3 Kopien pro Region → insgesamt 6 Kopien pro Cloud PC.

**b. Disaster Recovery Plus (DR+)**

* Noch höhere Resilienz + Performance:
	+ **RTO: < 30 Minuten**
	+ **RPO: < 60 Minuten**
* Ressourcen werden **vorab reserviert**, nicht erst im Notfall.
* Garantierte Wiederherstellung, unabhängig von Kapazitätsverfügbarkeit.
* Ideal für kritische Bereiche wie **Gesundheitswesen**, **Finanzen** oder **Behörden**.

**6. Verwaltung und Monitoring**

**Konfiguration:**

* DR-Features werden per **Intune Bulk Device Actions** aktiviert/deaktiviert.
* DR-Typ (CRDR oder DR+) wird über User Settings definiert.

**Monitoring:**

* Intune-Reporting zeigt:
	+ Aktivierungsstatus
	+ Aktuelle Restore Points
	+ Zustand von Backup Cloud PCs
	+ Lizenzstatus
	+ Verwendete Region

**7. Empfohlene Strategie („Funnel-Ansatz“):**

* **80 % der Nutzer**: Abdeckung durch Point-in-Time Restore ausreichend.
* **20 % der Nutzer**: Absicherung durch CRDR (z. B. Compliance-Gründe).
* **Kritische Nutzer** (C-Level, Support, Ops): DR+ für garantierte Verfügbarkeit.

**8. Fazit**

Windows 365 bietet ein umfassendes, mehrstufiges Disaster-Recovery-Konzept:

* Eingebaute Resilienz und Selbstheilung.
* Flexible, skalierbare Zusatzlösungen für unterschiedliche Schutzanforderungen.
* Vollständig verwaltet, einfach über Intune konfigurierbar.
* Höchste Sicherheit und Business Continuity – auch bei regionalen Ausfällen.

**✅ Session 31: Delivering like-local Windows experiences from the cloud**

**🎯 Ziel der Session**

Microsoft präsentiert technologische Fortschritte, um Cloud-basierte Windows-Erlebnisse (z. B. mit Windows 365 oder Azure Virtual Desktop) so schnell, reaktionsfreudig und nahtlos wie lokale Geräte wirken zu lassen („like-local experience“).

**🔧 Technische Anforderungen und Qualitätsziele**

* **Verbindungsstabilität:** 99,9 % Verbindungsrate
* **Mittlere Zeit bis zum Verbindungsabbruch (MTTF):** ≥ 8 Stunden
* **Max. Grafikdurchsatz:** 60 Mbps für zwei 4K-Monitore bei 60 FPS
* **Mindestanforderung:** > 0,5 Mbps Bandbreite und < 175 ms Latenz für akzeptables Erlebnis
* **Idealfall:** < 30 ms Latenz für „echtes“ like-local Gefühl

**🚀 Verbesserungen & Innovationen**

**1. Schnellere Verbindungen**

* **Verbindungszeit wurde verkürzt von ca. 30 Sekunden auf unter 7 Sekunden**
* Maßnahmen:
	+ Optimierung von Authentifizierungs- und Token-Prozessen
	+ Caching der RDP-Dateien
	+ Reduktion der Microsoft Graph API-Aufrufe

**2. Streaming & Grafik**

* Einführung des **H.265 (HEVC) Hardware-Encoding** (besseres Kompressionsverhältnis als H.264)
	+ Unterstützt 4K bei 60 FPS mit geringerer Bandbreite
* GPU-beschleunigte Encoding auch für Windows 365 Cloud-PCs verfügbar
* Verbesserte Unterstützung für:
	+ Microsoft Teams / WebEx / Zoom
	+ Single Sign-On mit Entra ID
	+ Multi-Monitor- und Multistream-Szenarien

**3. Netzwerk: Shortpath & Multipath**

* **Shortpath (UDP)**: Direktverbindung mit geringerer Latenz, Nutzung von TURN-Relays
* **RDP Multipath (NEU):** Gleichzeitige Verbindung über mehrere Netzwerkpfade
	+ Automatischer Fallback bei Verbindungsabbruch ohne Reconnect-Screen
	+ Ergebnis: 30 % weniger Verbindungsabbrüche, MTTF auf 8 Stunden erhöht

**4. Peripherie & Redirects**

* **Laufwerks- und Ordnerumleitung stark verbessert**
	+ Neue Caching-Strategie reduziert z. B. Ordnerauflistung von 5 Minuten auf 7,5 Sekunden
	+ Aktivierung über Registry Key auf Remote-Host

**5. Globale Ausweitung & Infrastruktur**

* **TURN-Relays von 14 auf 43 Azure-Regionen erweitert**
	+ Bessere UDP-Verfügbarkeit, geringere Latenz, höhere Ausfallsicherheit
* Einführung von **dedizierten IP-Ranges** für Windows 365 / AVD-Verkehr zur Netzwerkoptimierung & vereinfachtem Firewall-Management

**🔮 In Arbeit / Ausblick**

* RDP-Multipath: weitere Performanceverbesserungen
* Schnellere Verbindung unter 5 Sekunden
* Weitere Caching- und Prefetch-Mechanismen
* Weitere Verbesserungen bei Stifteingaben, Scannern und anderen Peripheriegeräten

**✅ Session 31: Deploying Microsoft Connected Cache for Enterprise at scale**

**📦 Was ist Microsoft Connected Cache (MCC)?**

Microsoft Connected Cache (MCC) ist eine **lokale Software-Cache-Lösung**, mit der Unternehmen **Microsoft-Inhalte (Updates, Apps etc.) effizienter** an große Geräteflotten verteilen können.

**🧩 Anwendungsfall:**

* Viele Geräte ziehen gleichzeitig Inhalte von Microsoft-CDNs (z. B. bei Patch Tuesday) → Netzwerküberlastung.
* MCC speichert Inhalte einmal lokal und stellt sie danach anderen Geräten bereit → **geringerer Bandbreitenverbrauch, schnellere Updates**.

**⚙️ Funktionsweise**

1. **Bereitstellung**:
	* MCC wird auf einem Windows- oder Linux-Host installiert (Server, VM, Desktop).
	* Verwaltung über das Azure-Portal oder CLI.
2. **Ablauf**:
	* Geräte sind via DO (Delivery Optimization) so konfiguriert, dass sie Inhalte zuerst vom MCC-Server anfragen.
	* Falls MCC den Inhalt nicht hat → einmaliger Download vom Microsoft-CDN → dann Weitergabe an alle anderen Geräte im Netzwerk.
	* Geräte validieren heruntergeladene Inhalte per **Hash und Signatur**.
3. **Fallback**:
	* Wenn MCC nicht erreichbar ist, wird automatisch wieder das Microsoft-CDN verwendet.

**🏗️ Host-Anforderungen**

**🔸 Kleine Büros (50–100 Geräte)**

* 4 Cores, 8 GB RAM (4 GB frei), 100 GB Speicher

**🔸 Mittelgroßes Umfeld (100–500 Geräte)**

* 8 Cores, 16 GB RAM (4 GB frei), 500 GB Speicher

**🔸 Große Unternehmen (>500 Geräte)**

* 16 Cores, 32 GB RAM, 2× SSD mit je 200–500 GB
* Mehrere MCC-Instanzen möglich

**🐧 Windows vs. Linux Host**

**Linux (Ubuntu 20.04 / RHEL 8/9):**

* Nutzt Container mit:
	+ **IoT Edge Runtime**, **Edge Agent**, **Edge Hub**, **MCC-Container**

**Windows 11 / Server 2022:**

* Erfordert:
	+ **Windows Subsystem for Linux (WSL)**, **Nested Virtualization**
	+ Deployment eines benutzerdefinierten Ubuntu-Images mit obigem Container-Stack

**🔐 Sicherheit**

* Kommunikation derzeit über **HTTP**, **HTTPS-Support ist geplant**
* Inhalte werden **immer vom DO-Client auf Integrität geprüft**, unabhängig vom Ursprungsserver
* Nur Microsoft-URLs werden vom Cache-Container akzeptiert

**🔁 Updates & Wartung**

* **Automatische Updates über Azure** (Konfiguration über Update-Ring):
	+ **Fast Ring**: direkt nach Release
	+ **Slow Ring**: innerhalb von 5 Wochen
* Fehlerhafte Updates (z. B. >6h Dauer) werden im Azure-Portal gemeldet

**🚀 Skalierung & Deployment**

* **Azure CLI-Unterstützung**:
	+ Skriptbasierte Massenbereitstellung mehrerer MCC-Instanzen
	+ Automatisierung mit Powershell-Skripten
* Beispiel-Demo:
	+ 5 MCC-Instanzen via CLI erstellt und über PowerShell remote auf Windows-Hosts installiert
	+ Zustand der Nodes wird im Azure-Portal überwacht

**🧭 Konfiguration über Intune**

* **Zentrale Policy** in Intune Admin Center erstellen
* Zielplattform: Windows 10 oder höher
* Vorlage: *Delivery Optimization*
* Wichtige Einstellung: DO Cache Hostname
	+ IP-Adresse oder FQDN des MCC-Servers

**🧰 Troubleshooting & Support**

| **Problem** | **Ursache** | **Lösung** |
| --- | --- | --- |
| Deployment schlägt fehl | Firewall blockiert benötigte Endpunkte | Whitelisting lt. [MS-Doku](https://aka.ms/mcc-docs) |
| MCC antwortet nicht | Portweiterleitung nicht aktiv | Port 80 muss an WSL/Container weitergeleitet sein |
| Fehleranalyse | Support-Skript collect-mcc-diagnostics.sh für Windows und Linux |  |

**📚 Weitere Ressourcen**

* 📄 [Blogpost zur Public Preview](https://aka.ms/mcc-blog)
* 📘 [Dokumentation](https://aka.ms/mcc-docs)
* 🔗 [Azure-Portal-Startseite für MCC](https://aka.ms/create-mcc)

**✅ Session 32: Secure corporate data and privacy with Win32 app isolation**

**🧱 Was ist Win32 App Isolation?**

**Win32 App Isolation** ist eine neue Sicherheitsfunktion in Windows 11, mit der klassische **Win32-Anwendungen** (z. B. VLC, Zoom, Skype) **in einer isolierten Sandbox** ausgeführt werden, um sensible Daten zu schützen und Angriffsflächen zu minimieren.

**🚨 Das Problem**

* **Win32-Apps** laufen traditionell mit denselben Rechten wie der Benutzer.
* Dadurch haben sie Zugriff auf Kamera, Mikrofon, Dateisystem etc.
* **Sicherheitslücken** in diesen Apps können ausgenutzt werden, um sensible Daten zu stehlen oder das System zu kompromittieren (z. B. Ransomware über VLC, Kamerazugriff via Skype).

**🛡️ Die Lösung: App-Isolation**

Win32 App Isolation führt einen **Sicherheitscontainer** ein, der einer App **nur minimale Berechtigungen** zuweist. Vorteile:

* Keine automatische Freigabe von Ressourcen wie Kamera oder Dateien.
* Zugriffe müssen **explizit bestätigt** oder per Brokering genehmigt werden.
* Schadsoftware wird in einer Sandbox „gefangen“ – ohne Zugriff auf Benutzerdaten.

**🔍 Technische Komponenten**

1. **App Container Token**
– Isoliert die Anwendung und entzieht unnötige Berechtigungen.
2. **Brokering-Komponente**
– Vermittelt bei notwendigen Zugriffen, z. B. auf Kamera oder Mikrofon, auf sichere Weise.
3. **File & Registry Virtualization**
– Schreibzugriffe auf Dateisystem und Registry werden **in virtuelle Pfade** umgeleitet, ohne echte Daten zu verändern.

**💡 Beispiele aus der Praxis**

| **Situation** | **Ohne Isolation** | **Mit Isolation** |
| --- | --- | --- |
| Ransomware über VLC | Dateien auf Desktop gelöscht, Erpressung | Zugriff auf Desktop blockiert, Benutzer muss zustimmen |
| Kamera-Hack über App | Kamera wird stillschweigend aktiviert | App fragt um Erlaubnis zur Kameranutzung |

**🛠️ Entwicklerfunktionen**

* **Visual Studio Integration** (ab Version 17.10): App-Entwickler können Isolation direkt aktivieren.
* **Single Package Deployment**: Auf Windows 11 24H2+ wird App isoliert ausgeführt, auf älteren Systemen als klassische App.
* **Light Packaging Support**: Auch ohne vollständige MSIX-Verpackung möglich.
* **App Capability Profiler Tool**: Hilft, die benötigten Berechtigungen automatisiert zu erkennen.

**✅ Vorteile für Unternehmen**

* **Erhöhte Sicherheit** bei minimalem Aufwand.
* **Kompatibilität mit Legacy-Apps** bleibt erhalten.
* **Weniger Ausfälle & Datenverluste** bei kompromittierten Anwendungen.
* **Stärkeres Sicherheitsbewusstsein** für Kunden & Partner.

**🏢 Einsatzszenarien**

* Eigene **intern genutzte Apps**: Organisation kann App selbst onboarden.
* **Drittanbieter-Apps**: IT-Abteilung kann App-Hersteller auffordern, Isolation zu unterstützen.

**📘 Ressourcen**

* [Win32 App Isolation auf Microsoft Learn](https://learn.microsoft.com/windows/apps/security/win32-app-isolation/)
* [GitHub-Repo für Feedback & Feature Requests](https://github.com/microsoft/Win32-AppIsolation)
* [Begleitblog zur Session](https://techcommunity.microsoft.com/)

**✅ Session 33: Azure Virtual Desktop hostpool management at scale**

**🎯 Ziel der Session**

Ein umfassender Überblick über **App-Management in Azure Virtual Desktop (AVD)** – mit Fokus auf **MSIX App Attach**, Integration von Drittanbietern, App-Virtualisierung, App-V-Kompatibilität und Monitoring.

**🧩 MSIX App Attach – Aktueller Stand (GA)**

* **Regionale Flexibilität**: Ein einziges App-Image kann in beliebige Hostpools einer Region eingebunden werden.
* **Zuweisung pro Benutzer**: Jeder Benutzer kann eine individuelle App-Kombination erhalten – auch bei gemeinsamem Hostpool.
* **Trennung von Image- & App-Lifecycle**: Keine Anpassung des System-Images nötig → weniger Wartungsaufwand.
* **Support für RemoteApp & Desktop**:
	+ Desktop: direkte App-Zuweisung ohne zusätzliche Gruppen nötig.
	+ RemoteApp: Zuweisung über Application Group erforderlich.

**🔁 App-Update-Prozess**

* App-Update erfolgt durch einfaches Austauschen der .sfs-Datei (schneller als .vhdx).
* Kein Neustart der Session Hosts erforderlich.
* Beim nächsten Login erhalten alle Benutzer automatisch die neue Version.

**🌐 Drittanbieter-Integration**

Microsoft bietet ein App Attach Framework, das Drittanbieter nativ in AVD integriert:

**🔌 Launch-Partner**

1. **Liquidware (FlexApp)**
2. **Numecent (Cloudpager)**
3. **Omnissa (ehemals VMware App Volumes)**

**✅ Vorteile der Integration**

* Einheitliches Management & Monitoring in Azure
* Nutzung von Azure RBAC
* Kombination mit bestehenden On-Premises-Umgebungen möglich (Hybrid-Modell)
* Veröffentlichung und Zuweisung der Apps analog zu MSIX App Attach

**🧰 App-V Integration (Support bis über 2026 hinaus)**

* **End of Life**: Nur die *Server-Komponenten* von App-V (MDOP) werden April 2026 eingestellt.
* **Nicht betroffen**:
	+ App-V Sequencer
	+ App-V Client
* **App-V über App Attach**:
	+ App-V Pakete (inkl. Deployment Config) lassen sich direkt in App Attach integrieren
	+ Keine Konvertierung nötig
	+ Unterstützung von Benutzer- und Systemkonfigurationen

**📊 Monitoring von App Attach**

**🔍 Über Azure Monitor / Log Analytics:**

* Diagnoseevents (z. B. App-Start, Fehler, Nutzungsdauer)
* Filter nach User, VM, App-Name
* Unterstützung von **KQL** (Kusto Query Language)
* Monitoring aller Pakettypen: MSIX, App-V, Drittanbieter

**🗂️ Über Event Viewer:**

* z. B. Apex Deployment Server Events
* Troubleshooting-Logs bei Paketfehlern

**🔧 Framework Packages vorbereiten**

* Viele MSIX-Apps benötigen **Framework-Dependencies** (z. B. Microsoft.VCLibs, .NET Runtime etc.)
* Microsoft stellt ein PowerShell-Skript bereit:
	+ Lädt automatisch alle notwendigen Framework-Versionen herunter
	+ Installiert diese ins Custom Image
	+ Ziel: **Vermeidung von Laufzeitfehlern** bei der Paketbereitstellung

🔗 [GitHub-Link zum Skript von Jim Moyle](https://github.com/jimmoyle/AVDFrameworkPreinstall) (siehe Session-Folie)

**📦 Unterstützte Paketformate für App Attach**

| **Paketformat** | **Unterstützt** |
| --- | --- |
| .msix | ✅ |
| .msixbundle | ✅ |
| .appx | ✅ |
| .appxbundle | ✅ |
| .appv | ✅ (neu) |
| Drittanbieter (z. B. FlexApp) | ✅ |

**✅ Fazit**

Microsoft bietet mit App Attach in AVD ein **flexibles, zentrales App-Delivery-Modell**, das sowohl native als auch virtualisierte Anwendungen unterstützt – inklusive Drittanbieter-Integrationen und modernem Monitoring.

**✅ Session 34: Device management for the frontline: Intune to the rescue**

**🎯 Ziel der Session:**

Verstehen, wie Microsoft Intune speziell für **Frontline Worker** optimierte Gerätemanagementlösungen bietet – von der Bereitstellung über die Nutzung bis hin zur Verwaltung im laufenden Betrieb.

**👷‍♀️ Wer sind Frontline Worker?**

* Mitarbeitende, die **direkt mit Kunden oder Patient:innen** interagieren (z. B. im Gesundheitswesen, Einzelhandel, Produktion).
* Nutzen Technologie **ergänzend**, nicht im Fokus ihrer Arbeit.
* Häufig: **Shared Devices** (mehrere Nutzende pro Gerät), spezielle Apps, hohe Sicherheitsanforderungen.

**🧩 Gerätetypen & Managementmodelle:**

**📱 1. Single-User Devices:**

* Corporate-owned, dauerhaft einem Mitarbeitenden zugewiesen.
* Personalisierung & Zugriff auf verschiedene Apps je nach Rolle.

**🔁 2. Multi-User / Shared Devices:**

* Geräte, die schichtweise zwischen mehreren Nutzenden rotieren.
* Nutzer melden sich per **Entra ID** oder **temporärer Session** an.

**🛒 3. Kiosk Devices:**

* Stationäre Geräte mit **fester App-Auswahl**, z. B. Preisscanner oder Digital Signage.
* Keine Benutzeranmeldung erforderlich.

**📲 Plattformunterstützung:**

**🍏 iOS/iPadOS:**

* **Shared iPad** mit:
	+ Benutzerpartitionen + Managed Apple ID (getrennte App-Daten).
	+ Alternativ: **Temporäre Session** ohne Apple ID (sämtliche Daten nach Logout gelöscht).
* Unterstützt **Entra SSO Plugin**, Single Sign-On für MS-Apps und Safari.

**🤖 Android:**

* **Android Enterprise** für:
	+ Fully Managed, Dedicated, COPE.
* **AOSP Support** für spezialisierte Geräte (z. B. Scanner, VR-Headsets).
* Intune bietet **Microsoft Managed Home Screen** zur Steuerung von UI, App-Zugriff, Branding, Geräteeinstellungen u.v.m.

**🧠 Integriert:**

* Entra Shared Device Mode: Geräte-übergreifendes Login/Logout mit Datencleanup.

**🚀 Produktivitätssteigernde Features:**

**1. Device Staging:**

* IT oder Lieferant bereitet Gerät vor.
* Benutzer muss nur noch schnell via Company Portal anmelden.

**2. Enrollment Time Grouping:**

* Vordefinierte Gruppenzuordnung vor Enrollment → Geräte sofort nach Anmeldung einsatzbereit.
* Reduziert Bereitstellungszeit von **6–8 Stunden auf wenige Minuten**.

**🎛️ Benutzererlebnis steuern:**

* iOS: Home Screen Layout, Wallpaper, Lockscreen Messages.
* Android:
	+ Standard Home Screen oder Kiosk-Modus.
	+ **Multi-App Kiosk** mit Managed Home Screen.
	+ Konfiguration von WLAN, Branding, Quick Settings, Layouts etc.
	+ Verbesserte UX (2024 Redesign): Bessere Übersicht, einfacheres Troubleshooting, Session Pins.

**🛠️ Gerätemanagement im Betrieb:**

**📍 Find/Play Lost Device:**

* Standortbestimmung + Ton abspielen.
* iOS & Android Dedicated Devices.

**🔁 OS-Updates:**

* Apple: Zeitfenster via Declarative Device Management.
* Android: Integration mit Samsung Knox, Zebra LifeGuard, Phoda – inklusive Batteriestatus-Check & WLAN-only Einschränkung.

**🧑‍💻 Remote Help:**

* Fernsteuerung, auch **unattended**.
* Integration in Intune mit Audit Trail & rollenbasierter Zugriffskontrolle.
* Unterstützt Android Dedicated, Samsung & Zebra.

**🔧 Remove Apps & Configuration:**

* Temporäres Entfernen problematischer Apps/Konfigurationen.
* Nach Fehlerbehebung: Wiederherstellung über Konsole.
* Verfügbar für iOS, iPadOS & Android Enterprise.

**📦 Beispiele:**

**🛍️ Einzelhandel:**

* Samsung Tablet als Shared Device.
* Teams Walkie-Talkie, Bezahl-Apps, keine Systemupdates im Weihnachtsgeschäft.
* Nur Store-WLAN erlaubt.
* Umsetzung: Android Dedicated, Shared Mode, Home Screen, OS Update Steuerung.

**🏥 Gesundheitswesen:**

* iPads für Patienten mit Entertainment & Self-Service.
* Geteilt, keine Datenspeicherung zwischen Sessions.
* Branding, WLAN-Beschränkung.
* Umsetzung: Shared iPad mit temporären Sessions, Intune Konfiguration.

**✅ Fazit:**

Microsoft Intune unterstützt eine Vielzahl von **Frontline-Szenarien** durch:

* Flexible Enrollment-Modelle.
* Geräte- & Benutzeroptimierung.
* Schutz sensibler Daten.
* Leistungsfähige Fernwartungs- und Verwaltungsfunktionen.

**✅ Session 35: The latest and greatest in the world of Windows LAPS**

**🛠️ Windows LAPS – Neuerungen in Windows 11 24H2 & Windows Server 2025**

Die Session richtete sich an bereits mit Windows LAPS vertraute IT-Profis und stellte umfangreiche Verbesserungen vor, die in der kommenden Windows-Version und Windows Server 2025 integriert sind.

**🔐 1. Automatisches Account Management (Automatic Account Management)**

* **Top-Feature-Wunsch von Kunden**
* Ermöglicht die zentrale Erstellung und Verwaltung eines lokalen Admin-Accounts durch LAPS – kein Scripting oder Imaging mehr notwendig.
* Verwaltung von:
	+ Built-in Admin Account oder
	+ Benutzerdefiniertem Admin-Account (Name per GPO definierbar)
* **Optionale Konto-Deaktivierung:** Konten können standardmäßig deaktiviert gehalten werden, bis sie gebraucht werden (z. B. via OU-Wechsel aktiviert).

**🔄 2. Name Randomization**

* LAPS kann bei jeder Passwortrotation zusätzlich den Kontonamen zufällig ändern.
* Der neue Name wird in AD mit dem Passwort gespeichert.
* Erhöht die Sicherheit, da der Accountname nicht mehr vorhersagbar ist.

**🔒 3. Erweiterter Accountschutz**

* Für automatisch verwaltete Konten wird nun der komplette Kontozustand geschützt, nicht nur das Passwort.
* Schutz vor Änderungen durch Dritte am Kontoobjekt (lokal oder im AD).

**🧼 4. Sysprep-Kompatibilität**

* Automatisch verwaltete Konten werden bei der Generalisierung durch Sysprep sauber entfernt – keine Reste im Image.

**🔑 Verbesserte Passwortoptionen**

**👁️‍🗨️ 5. Improved Readability für klassische Passwörter**

* Neue Passwortkomplexitätsoption entfernt schwer unterscheidbare Zeichen wie 1/I oder O/0.
* Leicht lesbar, besonders hilfreich beim Vorlesen am Telefon oder bei Remote-Support.

**💬 6. Passphrase Support (NEU!)**

* Unterstützung für **lesbare Passphrasen**, basierend auf EFF Wordlists:
	+ Long words
	+ Short words with unique prefixes
	+ Short words
* Passwortlänge (Anzahl Wörter) konfigurierbar.
* Beispiel: ArborZombieGizmo – einfach zu merken, dennoch sicher (hohe Entropie).

**🧩 7. UI-Verbesserungen & Post-Authentication Actions**

**📋 Neues Monospace-Font für Passwortanzeige**

* In der AD-Snap-In Ansicht (ADUC) jetzt besser lesbar.

**🛑 Neue Option: "Reset + Logoff + Kill Processes"**

* Erweiterte Post-Authentication-Option, um auch **RunAs- oder Hintergrundprozesse** zu beenden, die mit dem LAPS-Konto laufen.

**🌀 8. Rollback Detection via Password Versioning**

* Verhindert "torn state" nach einem OS-Rollback (Backup-Restore).
* Neue AD-Schema-Erweiterung (msLAPS-PasswordVersion) speichert eine GUID bei jeder Rotation.
* Der Client erkennt Abweichungen und rotiert das Passwort sofort neu.
* Nur in AD, nicht in Entra unterstützt.

**🧰 9. Disaster Recovery – LAPS-Passwörter aus AD-Backups extrahieren**

* NEU: Wiederherstellung verschlüsselter LAPS-Passwörter direkt aus AD-Snapshots ohne Domain Controller.
* Ermöglicht vollständige Wiederherstellung in Notfallszenarien (z. B. Domain down).
* Unterstützt alle verschlüsselten Passwörter (inkl. Entra verschlüsselte).
* Funktioniert auf beliebigem Windows-Gerät, sogar in Workgroup.

**🧪 10. Windows Admin Center Integration (Preview)**

* Neues WAC-Extension für Windows LAPS:
	+ Passwortanzeige
	+ Ablaufdatum setzen
	+ Passwortrotation initiieren
	+ Direkt vom Admin Center aus bedienbar

**📚 Weitere Hinweise**

* Neue Dokumentation unter: [aka.ms/laps](https://aka.ms/laps)
* Neue PowerShell-Demos, GPO-Templates, Schemaerweiterungstools
* Feedback-Kanal weiterhin aktiv – viele Features entstanden durch Community-Beiträge

**✅ Session 36: AMA: Cloud native with Microsoft Intune**

**🎯 Ziel der Session**

Ein interaktives Q&A mit dem Customer Experience Engineering Team von Microsoft Intune zur praktischen Umsetzung und Strategie des „Cloud native“-Ansatzes mit Microsoft Intune, insbesondere für Windows-Geräte.

**💡 Was bedeutet „Cloud native“?**

* Geräte werden **direkt in Entra ID (vormals Azure AD)** eingebunden, nicht mehr in eine lokale Domäne.
* Die Geräteverwaltung erfolgt vollständig über **Microsoft Intune**, nicht mehr über GPOs oder andere On-Prem-Tools.
* Dies gilt plattformübergreifend – nicht nur für Windows, sondern auch Android, iOS und macOS.

**🚀 Empfehlungen zur Umstellung auf Cloud-native:**

* **Hybrid Join ist kein Fehler**, sondern oft ein sinnvoller Zwischenschritt.
* Bestehende Geräte können über **Co-Management** migriert werden.
* Ziel: **Entra-Join + Intune-only-Management**.

**🧩 Wichtige Themen & Antworten aus dem AMA:**

**1. 🔁 Richtlinienkonflikte in Intune**

* Intune zeigt Konflikte an, aber nicht immer mit **Ursache**, insbesondere bei älteren Template-basierten Richtlinien.
* Bei **Settings Catalog Policies** wird die Konfliktquelle angezeigt.

**2. 🔒 Remote Lock vs. Remote Wipe**

* **Remote Lock** ist aktuell nicht realistisch für Windows-Geräte (fehlende Always-On-Konnektivität).
* Empfehlung: **Remote Wipe + BitLocker aktivieren**.
* Compliance Policies können **automatische Sperrung bei Inaktivität** erzwingen.

**3. 🧑‍💻 Lokale Adminrechte & Passwortverwaltung**

* Empfehlung: **Windows LAPS (Local Admin Password Solution)** mit Intune verwenden.
* Alternativ oder ergänzend: **Endpoint Privilege Management (EPM)** zur temporären Erhöhung von Rechten.

**4. 🗂 Zugriff auf On-Prem-Ressourcen mit Entra Join**

* **Geräteidentität ≠ Benutzeridentität**
* Zugriff auf Fileshares, Drucker & Co. bleibt mit **hybriden Benutzern** problemlos möglich (über Entra Connect).
* **SSO** funktioniert weiterhin mit Windows Hello for Business.

**5. 🔐 Passwortlose Authentifizierung**

* Funktioniert nahtlos mit Entra Join.
* Viel einfacher umsetzbar als mit Hybrid Join.
* Macht den Alltag für User und IT einfacher (keine Passwort-Resets etc.).

**6. 🧪 Autopilot-Troubleshooting**

* **Vereinfachung der Deployment-Prozesse** ist essenziell – „Lift & Shift“ komplexer Task-Sequenzen ist nicht zielführend.
* **Autopilot-Gerätebereitstellung** wird künftig mit besseren Fehlerreports (z. B. Fehlerphase) ergänzt.

**7. ⚙️ Filter und Zuweisungen**

* **Filters** sind performant und flexibel – sollten bevorzugt genutzt werden.
* Noch nicht überall verfügbar (z. B. Plattform-Skripte), aber auf der Roadmap.

**8. 📡 VPN + Device Certificate Challenges**

* **Device Writeback** hilft nur bedingt – hängt vom verwendeten VPN-Provider ab.
* Besser: VPN-Anbieter mit **Conditional Access**-Unterstützung (z. B. Zscaler, Cisco, Palo Alto).

**🔚 Fazit**

* Cloud native ist ein erreichbares Ziel – mit realistischen Zwischenstationen.
* Fokus: **Vereinfachung, Automatisierung und Nutzung von Cloud-Identitäten**.
* Hilfreiche Tools: Windows LAPS, EPM, Remote Help, Autopilot, Settings Catalog & Filter.

**✅ Session 37: Secure helpdesk support using Intune Remote Help**

**🎯 Ziel der Session**

Ein umfassender Überblick über Microsoft **Remote Help**, eine cloudbasierte Remote-Support-Lösung für IT-Helpdesks, inklusive neuer Funktionen und plattformübergreifender Unterstützung für **Windows**, **Android** und **macOS**.

**🧩 Plattformüberblick**

**🪟 Windows**

* Unterstützung für:
	+ Entra-verwaltete Geräte & nicht verwaltete Geräte
	+ Windows 10 & 11 inkl. ARM64
	+ Windows 365 & **AVD** (Single Session, Multi-Session geplant)
* Features:
	+ **Benachrichtigung direkt vom Intune-Portal** – kein Sessioncode nötig
	+ **View only / Full Control / UAC-Elevation**
	+ **Integration mit Conditional Access und RBAC**
	+ **Annotationswerkzeuge** wie Laserpointer
	+ **Integrierter Chat** (bidirektional, persistent)
	+ **Auto-Updates via Win32-App oder Enterprise App Management**
	+ **Session Reporting** & **Audit Logs**
	+ **Nicht-konformitätswarnungen** für zu helfende Geräte

**🤖 Android**

* Unterstützte Geräte:
	+ **Android Enterprise Dedicated** (v.a. Samsung & Zebra)
* Features:
	+ **View only / Full Control / Unattended Control**
	+ **Benachrichtigungen an den Endnutzer**
	+ **Volle Steuerung via Web-Konsole**
	+ Unterstützung physischer Buttons (Power, Volume etc.)
	+ **Touch- und Tastatureingaben** über Remotehilfe
	+ **Nichtkonformitätswarnungen**, **RBAC**, **starke Authentifizierung**
	+ **Unattended Sessions**, z. B. für Wartung über Nacht
	+ **Session-Timeout bei Inaktivität**
	+ **Session History Reports & Audit Logs**

**🍎 macOS**

* Unterstützte Versionen: **macOS 13–15**
* Architektur:
	+ **Helper** arbeitet über Webbrowser
	+ **Sharer** verwendet native App (PKG oder LOB App)
* Features:
	+ **View only / Full Control**
	+ Funktioniert mit **verwalteten und nicht verwalteten Geräten**
	+ Verbindungsaufbau über **Kurzlink mit Sessioncode**
	+ **RBAC, Conditional Access, starker Authentifizierung**
	+ **Integrierter Chat**
	+ **Session Reporting & Audit Logs**

**🔐 Sicherheitsfeatures (plattformübergreifend)**

* **Multi-Factor Authentication (MFA)** für Helfer & Sharer
* **Conditional Access** zur Absicherung der Remotehilfe-App
* **Benutzerauthentifizierung über Entra ID**
* **Warnung bei Geräten, die Intune-Richtlinien nicht einhalten**
* **RBAC-Rollensteuerung**: Wer darf was (z. B. View vs. Control)

**🧪 Reporting & Überwachung**

* Alle Plattformen unterstützen:
	+ **Session Reports**
	+ **Audit Logs**
	+ Details zu: Gerätename, Seriennummer, Device ID, Helfer, Sessiondauer etc.
* Verwaltung & Analyse im Intune Admin Center

**💡 Praxisbeispiele (aus den Demos)**

**🧑‍⚕️ Windows – Support für Klinikpersonal:**

* Helper startet Session via Intune ohne Codeaustausch
* Benutzer wird via Notification benachrichtigt
* UAC-Elevation durch Full Control möglich
* Diagnostik durch Compliance-Warnung

**🛒 Android – Retail-Szenario:**

* Store Manager wird per Full-Control-Sitzung unterstützt
* Unattended Session wird genutzt, um Gerät nachts zu warten
* Helper kann Tastatur- und Touch-Steuerung remote verwenden

**💻 macOS – Support für Macs im Unternehmen:**

* Helper erzeugt Sitzung und sendet Kurzlink an User
* Support auch für nicht-enrollte Macs
* Gleiches Rechte- & Sicherheitsmodell wie Windows/Android

**🔚 Fazit**

Microsoft Remote Help bietet eine **sichere, skalierbare, plattformübergreifende Remote-Support-Lösung**, die sich tief in Intune, Entra ID und Conditional Access integriert. Die Lösung eignet sich besonders für verteilte oder mobile Arbeitsumgebungen mit unterschiedlichen Endgeräten.

**✅ Session 38: Enterprise Application Management with Microsoft Graph**

**🎯 Ziel der Session**

Die Session demonstrierte, wie Unternehmen **Enterprise Application Management (EAM)** effizienter gestalten können – insbesondere durch den Einsatz von **Microsoft Graph** anstelle der klassischen InTune Admin Center-Oberfläche.

**👥 Sprecher**

* **Joe Lurry** – Microsoft Intune Customer Acceleration Team
* **Danny Gillery** – Product Manager, Enterprise App Management

**🧩 Überblick über Enterprise App Management (EAM)**

EAM wurde eingeführt, um die Komplexität und den Zeitaufwand der Anwendungsbereitstellung drastisch zu reduzieren.

**Vorteile:**

* **Vorgefertigte App-Pakete**: Enthalten Installations-/Deinstallationsbefehle, Detection Rules und Systemanforderungen.
* **Automatische Update-Erkennung**: Neue Versionen werden automatisch erkannt und vorgeschlagen.
* **Guided Upgrade Experience**: Einfacher Upgrade-Prozess für bereits zugewiesene Anwendungen.
* **Katalog mit Hunderten Apps**: Kontinuierlich wachsend, ideal für Windows-Clients.

**🔍 Demo im InTune Admin Center**

Joe zeigte anhand von **WinRAR**, wie man:

* Apps aus dem Katalog auswählt
* Versionen und Sprachen definiert
* Anforderungen prüft und ändert
* Updates durchführt und Pakete ersetzt (Supersedence)
* Apps über Zuweisungen verteilt

**📊 Microsoft Graph: EAM per PowerShell und API verwalten**

Danny demonstrierte, wie man App-Kataloge und -Daten über **Graph-API** automatisiert verwalten kann.

**Key Points:**

* **Alle Graph-Befehle zu EAM befinden sich noch im Beta-Status**
* Nutzung von Invoke-GraphRequest in PowerShell
* Export von Kataloginformationen (inkl. App-ID, Publisher, Versionen etc.) als JSON → Analyse in Excel
* Übersicht der im Tenant installierten EAM-Apps
* Automatisierte Auswertungen z. B. Anzahl der verwendeten Apps, App-Verteilung nach Hersteller
* Möglichkeit, EAM mit anderen Diensten wie Defender, MDE oder Drittanbietertools zu kombinieren

**🔗 Nutzen & Praxisempfehlung**

* **Zeitersparnis**: Kein manuelles Verpacken von Apps notwendig
* **Skalierbarkeit**: Ideal für große Umgebungen mit wiederkehrenden Software-Installationen
* **Integration mit Automatisierungen und Sicherheitslösungen**
* **Feedback wichtig**: Kunden sollen aktiv gewünschte Apps und Funktionen unter [aka.ms/intune-feedback](https://aka.ms/intune-feedback) einreichen

**📌 Weiterführende Ressourcen**

* Microsoft Graph Developer Guide
* Intune Graph API Übersicht auf Microsoft Learn
* Demos & How-To-Videos von Ignite & Tech Takeoff

**✅ Session 39: Windows cloud migration and deployment best practices**

**🎯 Ziel der Session**

Die Session behandelt die Geschichte der Virtualisierung bei Microsoft, die heutigen Optionen für Windows-Cloud-Computing (Windows 365 & Azure Virtual Desktop), typische Anwendungsfälle, Architektur- und Migrationsstrategien sowie neue Entwicklungen wie Windows 365 Link.

**🕰️ Historischer Überblick zur Microsoft-Virtualisierung**

* Beginn in den 1990ern mit **Terminal Services (Windows NT Server)**.
* Weiterentwicklung zu **Remote Desktop Services (RDS)**.
* Übergang zu Azure-basierten Virtualisierungslösungen führte zu:
	+ **Remote Desktop Services on Azure IaaS**
	+ → Weiter zu **Azure Virtual Desktop (AVD)** als vollständig gemanagtes **Cloud-VDI (PaaS)**.
* Entwicklung von **Windows 365** als **SaaS-Lösung für Cloud-PCs**, um Virtualisierung einfacher und breiter verfügbar zu machen.

**💻 Überblick: Windows 365 vs. Azure Virtual Desktop (AVD)**

| **Merkmal** | **Windows 365 Enterprise** | **Azure Virtual Desktop** |
| --- | --- | --- |
| Bereitstellung | SaaS | PaaS |
| Verwaltung | Intune | Azure-Portal |
| Betriebssysteme | Windows 11, 10 | Windows 11, 10, Windows Server |
| Preisstruktur | Fix pro User/Monat | Verbrauchsbasiert |
| Nutzererlebnis | Vollständiger Windows-Desktop | Flexible Desktops und Apps |
| Ideal für | Einfachheit, Planbarkeit | Anpassbarkeit, Flexibilität |

**🧩 Typische Anwendungsfälle für Virtualisierung**

* **Datensicherheit & Compliance**
* **Desaster Recovery**
* **Bring Your Own Device (BYOD)**
* **Hybrides Arbeiten / Reisen**
* **Temporäre / Saisonale Arbeitskräfte**
* **High Performance Computing**
* **Shared Devices (z. B. Callcenter)**
* **Mergers & Acquisitions (M&A)**

**🧱 Architekturvergleich: AVD vs. Windows 365**

**Azure Virtual Desktop:**

* Kundenverantwortung: Identität, Netzwerk, Image Mgmt, Profile, Updates
* Microsoft: Gateway, Brokering, Webzugriff (PaaS)
* Komplexer, aber sehr flexibel

**Windows 365:**

* Microsoft übernimmt mehr: Image Mgmt, Monitoring, DR, Updates
* Intune-native Verwaltung
* Automatische Bereitstellung, Self-Service-Optionen
* Ideal für Intune-zentrierte Organisationen

**🧪 Windows 365 Provisioning via Intune (Demo-Inhalte)**

* Einfache Erstellung von Bereitstellungsrichtlinien über Intune
* Auswahl zwischen Microsoft-gehosteten oder eigenen Netzwerken
* Automatische Zuweisung nach Region oder manuell
* Unterstützung von **Single Sign-On**, **Gallery Images**, **Custom Naming**
* Optional mit **Windows Autopatch** für vereinfachtes Patch-Management
* Automatische Provisionierung nach Lizenz- und Gruppenzuweisung

**🆕 Erweiterungen und Migrationserleichterungen**

**Unterstützung bei Windows 11 Migration:**

* Windows 365 Lizenzen enthalten **Extended Security Updates (ESU)** für Windows 10 bis Oktober 2028
* Option, alte Windows 10 Geräte als Kioske zu verwenden, um Cloud-PCs sicher bereitzustellen

**Windows 365 Link (public preview):**

* Thin-Client-ähnliches Gerät, **speziell für Cloud-PCs**
* Ideal für Shared Use, Callcenter, Hotdesking
* Verwaltung über Intune
* Keine lokalen Daten – nur Cloudzugriff

**🛣️ Migrationsstrategie: Einstiegspunkte**

| **Ausgangssituation** | **Empfehlung** |
| --- | --- |
| Neu in Virtualisierung | Starte mit **Windows 365** |
| Komplexes On-Premises VDI | Migration zu **AVD** oder **Hybrid mit W365** |
| Wunsch nach Vereinfachung & Intune-Nutzung | **Windows 365 mit Intune** |

**🔁 Modernisierungsfelder bei der Cloud-Migration**

* Identität: Entra ID Join + SSO + FIDO
* Netzwerk: Hosted oder On-Prem via ExpressRoute / VPN
* Image Mgmt: Von Golden Images zu Intune Gallery Images
* Updates: Windows Autopatch
* Anwendungen: Von SCCM zu Intune
* Benutzerprofile: Weg von FSLogix, hin zu OneDrive und integrierter Wiederherstellung
* Geräteverwaltung: Intune + Windows 365 + Copilot-Support

**📚 Ressourcen**

* [Interaktive Demos](https://aka.ms/Windows365InteractiveDemo)
* [Christiaan Brinkhoff Blog: Windows 365 Migration Guide](https://aka.ms/W365MigrationBlog)
* [Windows 365 Community](https://techcommunity.microsoft.com/t5/windows-365/bd-p/Windows365)
* [Azure Virtual Desktop Community](https://techcommunity.microsoft.com/t5/azure-virtual-desktop/bd-p/AzureVirtualDesktop)

**✅ Session 40: Windows 10 EOS: Myths, misconceptions, and FAQs**

**🎯 Ziel der Session**

Die Session bereitet Unternehmen auf das **End of Support (EOS)** von **Windows 10** am **14. Oktober 2025** vor. Dabei werden:

* Fakten rund um EOS vermittelt
* Häufige Mythen und Missverständnisse aufgedeckt
* Optionen für Extended Security Updates (ESU) erläutert

**🧾 Fakten zu Windows 10 EOS**

* **Betroffen sind alle Windows 10-Editionen außer LTSC** (Enterprise LTSC & IoT Enterprise LTSC ausgenommen)
* EOS betrifft auch andere Produkte: Office 2016/2019, Exchange, Visio, Project, Skype for Business Server
* Nach EOS:
	+ Keine Sicherheitsupdates mehr
	+ Kein technischer Support
	+ Keine Bugfixes oder Featureverbesserungen
	+ Risiko für Sicherheitslücken und Compliance-Probleme steigt

**❌ Mythen & Missverständnisse (Mythbusting mit Eric Mo)**

1. **„Ich muss alle meine Apps testen“**
	* ❌ Mythos: Windows 10 zu 11 bietet >99 % App-Kompatibilität
	* ✅ Empfehlung: Nur geschäftskritische Apps testen
2. **„Ich brauche Spezialtools für das Upgrade“**
	* ❌ Mythos: Bestehende Tools wie ConfigMgr, Intune, Autopatch reichen aus
	* ✅ Windows 11 wird wie ein Feature Update behandelt
3. **„Ich muss Cloud-native sein, um auf Windows 11 zu migrieren“**
	* ❌ Mythos: Cloud-native ist wünschenswert, aber kein Muss
	* ✅ Cloud-Migration kann parallel erfolgen
4. **„Endnutzer kommen mit Windows 11 nicht zurecht“**
	* ❌ Mythos: Viele kennen Windows 11 bereits von Privatgeräten
	* ✅ Microsoft bietet die „Day One with Windows 11“-Videoserie zur Unterstützung
5. **„Windows 11 benötigt aufwendige Planung“**
	* ❌ Mythos: Kein „großes“ Upgrade wie XP zu 7
	* ✅ Ring-basierte Upgrades, Self-Service möglich (z. B. via Autopatch)
6. **„Windows 11 bringt keinen Mehrwert“**
	* ❌ Mythos: Neue Features wie Hotpatching, Copilot+, KI-Integration
	* ✅ Bessere Sicherheitsfeatures, moderne UX
7. **„Microsoft wird Hardwareanforderungen ändern“**
	* ❌ Mythos: Anforderungen bleiben fix, um Sicherheit zu gewährleisten
8. **„Microsoft wird das EOS-Datum verschieben“**
	* ❌ Mythos: 14. Oktober 2025 ist fix

**💡 Empfehlungen für den Umstieg**

* Nutze **Inplace-Upgrades** (Anwendungen & Daten bleiben erhalten)
* Nutze deine bestehenden Tools
* Berücksichtige Windows Autopatch & Intune
* Starte jetzt, um rechtzeitig fertig zu sein
* Bei Bedarf: **FastTrack-Support** von Microsoft

**🛡️ Extended Security Updates (ESU) mit Jason Lesnak**

**Was sind ESUs?**

* Letzter Ausweg, wenn Migration bis 2025 nicht möglich ist
* **Nur sicherheitsrelevante Updates (kritisch/wichtig)**
* Kein Support für:
	+ Feature-Updates
	+ Bugfixes
	+ Designänderungen

**Voraussetzungen**

* Nur für Windows 10 Version **22H2**
* Laufzeit: max. **3 Jahre**
* Mindestlaufzeit: **1 Jahr**
* Verkauf über **Volumenlizenz** (bereits verfügbar)

**Preise**

* **Jahr 1:** $61 pro Gerät
* **Jahr 2:** $122
* **Jahr 3:** $244
* **25 % Rabatt** bei Nutzung von Autopatch/Intune (Cloud-managed)

**Bezugswege**

1. **Windows 365 Cloud PC**: Automatischer ESU-Anspruch (auch für genutztes Win10-Endgerät)
2. **Azure Virtual Desktop (AVD)**: Nur VM erhält ESU
3. **Physische Geräte**: Aktivierung via MAK-Key & Volume Activation Management Tool

**🔗 Ressourcen**

* [Windows Release Health Dashboard](https://aka.ms/wrh)
* [Windows Servicing Community](https://techcommunity.microsoft.com/)
* Monatliche Q&A: **Windows Servicing Office Hours** (3. Donnerstag im Monat)

**✅ Session 41: Windows 365 Frontline: Frequently asked questions**

**🧭 Ziel der Session**

Beantwortung zentraler Kundenfragen zu **Windows 365 Frontline** – speziell im Hinblick auf die **neue „Shared Mode“-Funktion** und deren Abgrenzung zu **Dedicated Mode**, **AVD** und klassischen VDI-Szenarien.

**🔁 Unterschied zwischen Shared Mode und klassischen VDI-/AVD-Modellen**

| **Kriterium** | **Shared Mode** | **AVD / VDI Multi-Session** |
| --- | --- | --- |
| Sitzungstyp | **Einzelsitzung-VM** (Windows 10/11) | **Multi-Session-VM** (z. B. Windows 10 MS) |
| Nutzung | **Serielle Nutzung**, immer ein User | Gleichzeitige Nutzung durch mehrere |
| Vergleichsmodell | Wie **physisch gemeinsam genutzte Geräte** | Virtuelle Desktop-Infrastruktur |
| Vorteil | Einfachheit, Standardisierung | Flexibilität, Skalierbarkeit |

🟢 Gut geeignet für: Szenarien mit **kurzer, sporadischer Nutzung durch viele User**, z. B. Einzelhandel, Schulungslabore, Spezial-Apps.

**🔄 Unterschied Dedicated Mode vs. Shared Mode**

| **Aspekt** | **Dedicated Mode** | **Shared Mode** |
| --- | --- | --- |
| Nutzerbindung | Feste Zuweisung eines PCs an einen User | Kein personalisierter PC, Nutzung „on demand“ |
| Personalisierung | Benutzer kann Admin sein, Apps installieren, Daten speichern | Immer frischer Zustand, kein Profil bleibt bestehen |
| Verbindung | Kann bis zu 2 Minuten zum Start dauern | Sofortige Verbindung, optimiert für schnelle Nutzung |
| Einsatzszenarien | Wenig genutzte Info-Worker, Callcenter, individuelle Aufgaben | Trainingsumgebungen, Zugriff auf Spezialsoftware |
| Lizenzverbrauch | 1 Lizenz = **3 PCs** in Dedicated Mode | 1 Lizenz = **1 PC** in Shared Mode |

**📌 Nutzungsszenarien für Shared Mode**

* **Retail/Kasse**: Kurze Nutzung einzelner Stationen
* **Trainingslabore**
* **Berater**: Zugriff auf geschützte Umgebungen
* **Spezialsoftwarezugriff**: z. B. Lizenz-gebundene Apps
* **Temporärer Zugriff**: z. B. je 15–60 Minuten pro Tag

**💡 Lizenzierung & Verwaltung**

* **Ein Lizenzmodell** für beide Modi: **Windows 365 Frontline**
* Umstellung zwischen Shared ↔ Dedicated durch Anpassung der **Provisioning Policy**
* **Lizenznutzung reduzieren**:
	+ Dedicated Mode: Entfernen von 3 Usern aus Gruppe (Freigabe von 1 Lizenz)
	+ Shared Mode: Anpassung der Gerätemenge direkt in Policy

**🌍 Regionale Verfügbarkeit**

* Shared Mode nutzt **neue Plattform** → derzeit kleinere Regionenauswahl
* Ziel: **volle Abdeckung** wie bei Windows 365 Enterprise

**⏱️ Sitzungs-Timeout & Benutzerabmeldung**

* Standard-Timeout: **30 Minuten**
* Konfigurierbar: **1 Minute bis 5 Tage**
* Steuerung über: **Intune Richtlinie (Idle Detection Timeout)**

**💾 Persistenz von Daten in Shared Mode**

| **Datentyp** | **Verhalten bei Abmeldung** |
| --- | --- |
| Benutzerprofil | **Komplett gelöscht** |
| Lokale App-Daten (z. B. Outlook) | **Gelöscht** |
| Cloud-konfigurierte Einstellungen (z. B. Edge-Favoriten) | **Persistieren** |

**🧰 Tools & Verwaltung**

* Kein Drittanbieter-VDI-Tool erforderlich
* Verwaltung über **Intune** & Microsoft Admin Center
* **Partnerunterstützung** wird mit GA ausgebaut

**🔄 Autopilot-Support**

* **Aktuell nur in Shared Mode**
* Geplant: Erweiterung auf **Frontline Dedicated** und **Enterprise**

**🔗 Kompatibilität mit Windows 365 Link**

* **Windows 365 Link** (dedizierte Thin Clients für Cloud PCs) ist **voll unterstützt**
* Besonders gut geeignet für **Task Worker**, **geteilte Endgeräte** oder **Hotdesking**

**📊 Kapazitätsplanung & Skalierung**

* Starte mit Anzahl der Cloud PCs analog zur physischen Umgebung
* Beispiel: 30 Geräte im Schulungslabor = 30 Shared Cloud PCs
* **Live-Anpassung** über Provisioning Policy möglich
* **Monitoring & Reports** helfen bei Feinjustierung