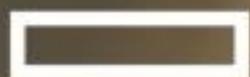


15. BECHTLE IT-FORUM THÜRINGEN

BECHTLE

2024

15. Mai 2024 • STEIGERWALD Stadion ^{Erfurt}



Hewlett Packard
Enterprise



HUAWEI

intel.

Die Zukunft des sicheren Arbeitens mit Windows 11 und den Microsoft Copiloten



Igor Krstin

Sr. Channel Executive – Modernize Endpoints | EMEA

Microsoft

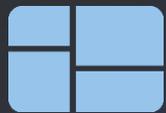


Igor Krstin

Sr. Channel Executive | Modernize Endpoints | EMEA

Mit über zwei Jahrzehnten Erfahrung in der IT-Branche verfügt Igor Krstin über eine Fülle von Wissen und Erfahrung. Ab 1998 arbeitete Igor 18 Jahre lang bei Systemintegratoren wie Computacenter, TSI und HPE (jetzt DXC), wo er verschiedene Rollen innehatte, die von Presales, Implementierung und Lieferung bis hin zur Entwicklung des Serviceportfolios im Bereich Managed Workplace Services reichten. Im Jahr 2016 wechselte Igor zu Microsoft, wo er Führungspositionen im technischen Vertrieb mit Schwerpunkt auf Modern Endpoint und Power Platform innehatte. Seit 2022 arbeitet Igor im Vertrieb von Device Partners, wo er sich auf die Modernisierung von Endpunktbewegungen in Zusammenarbeit mit den OEMs von Microsoft und strategischen Partnern in der EMEA-Region konzentriert.

Eine neue Ära des Hybrides Arbeitens



1985



1995



2001



2009



2015

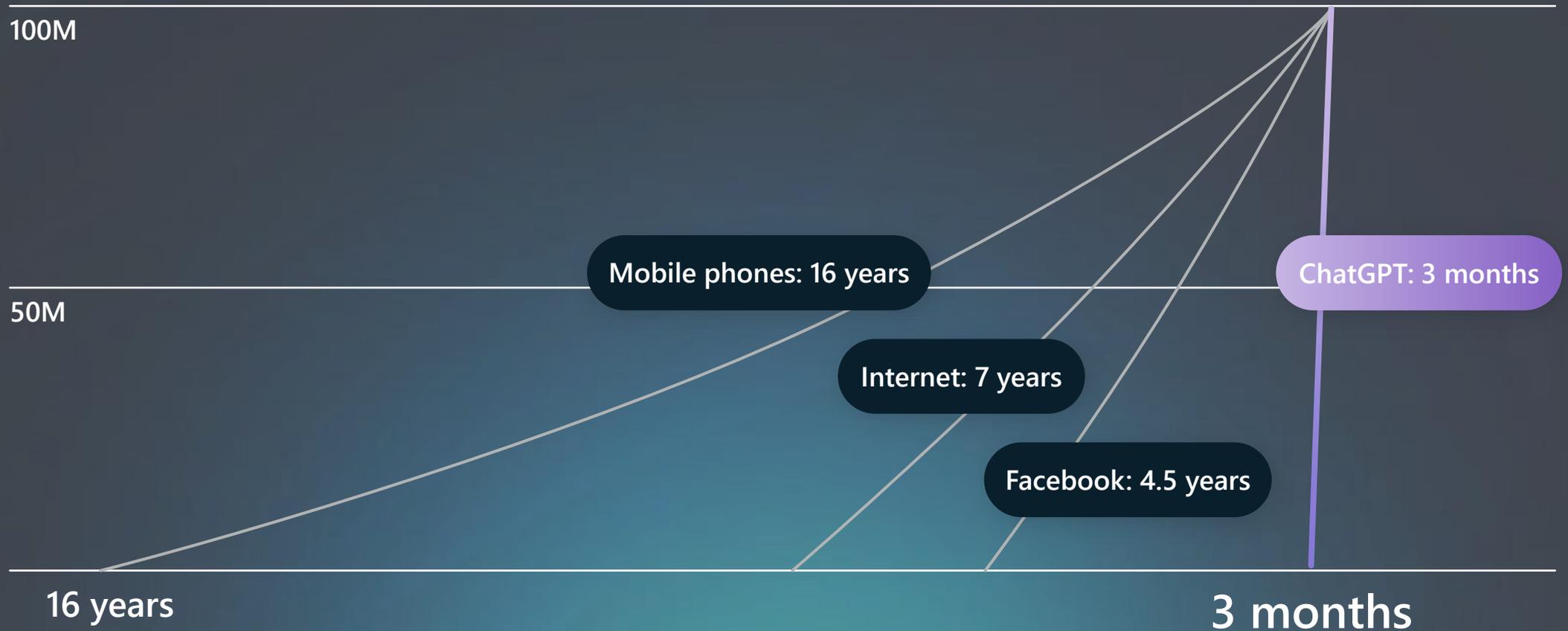


2021

Windows 11

Generative AI technology is here

Time to reach 100M users



Aufbauend auf zwei Jahrzehnten intelligenter Evolution

Windows von 1993 bis 2023

1993	2001	2009	2015	2018	2021	2023
Windows 3.1 Microsoft Agent app	Windows XP Windows Speech Recognition	Windows 7 Windows Sensor & Location Platform	Windows 10 Cortana virtual assistant	Windows 10 Windows Machine Learning platform	Windows 11 launch <ul style="list-style-type: none">• Ink anywhere• Microsoft Search• Microsoft Defender• Intelligent noise canceling any background blur for video conferencing	Windows 11 continuous innovation <ul style="list-style-type: none">• Narrator with natural voices, live captions in multiple languages, enhanced voice access• AI-powered recommendations in File Explorer and Start.• Enhanced phishing protection with Windows Defender SmartScreen• Enhanced capabilities on devices with NPU processors, also known as AI accelerators.• Bing Chat (March 2023)• Bing Chat Enterprise (July 18, 2023)• Copilot in Windows with Bing Chat Enterprise (August 2023 in Preview)• Copilot in Windows¹ (In preview)

"KI ist die wichtigste
Priorität der Technologie"



Satya Nadella

-Chairman and CEO, Microsoft

AI

KI in Windows 11 ist nicht nur der nächste Schritt in der Evolution des PCs. Es ist der nächste Schritt, um den Arbeitsplatz neu zu denken.

1. Timing of feature delivery and availability varies by market and device. Screen simulated, subject to change. Use Copilot with a Microsoft Account or use Copilot with commercial data protection at no additional cost by signing into a work or school account (Microsoft Entra ID) with Microsoft 365 E3, E5, F3, A3 or A5 for faculty, Business Premium, and Business Standard. Coming to more Entra ID users over time.

Die nächste Generation von Windows, entwickelt für KI

Cloud

KI-Integration in alle Windows-PCs



Windows Copilot (Chat), das in Windows integriert ist, sowie optimierte Plug-ins, die es Entwicklern ermöglichen, intensiv mit dem Betriebssystem zu interagieren

Fall 2023

Client

KI-Beschleunigung mit zielgerichteter Hardware



PCs mit NPUs ermöglichen bessere KI-Erfahrungen zusammen mit der Unterstützung durch ein breites ISV-Ökosystem

2024

Are you ready to join the era of AI?

Umstellung auf eine proaktive KI-Strategie (Zugriff, Geräte und Daten)

— Verfügen Sie über umfassende 'Zero-Trust' security?

KI führt neue Vektoren für Sicherheitsrisiken mit Auswirkungen wie Datenschutzverletzungen, finanziellen Verlusten und Reputationsrisiken ein. Zero-Trust mit Anomalieerkennung kann die Zugriffskontrollen verschärfen und Sicherheitsverletzungen minimieren.

— Sind Ihre Endpunkte und Anwendungen einfach zu verwalten??

Ein moderner Tech-Stack ist entscheidend für den Erfolg von KI, damit IT-Teams auf einfache Weise die Kontrollen zum Schutz vor Datenverlust verbessern, eine robuste Data Governance anwenden und Datenaufbewahrungsrichtlinien und Zugriffsrechte durchsetzen können.

— Haben Sie die richtigen Werkzeuge, um die Produktivität zu steigern?

Die richtige Mischung aus Tools kann die Produktivität verbessern, Silos aufbrechen, um die Zusammenarbeit zu fördern, und den Mitarbeitern helfen, mehr Wert aus KI zu ziehen, während gleichzeitig die Sicherheit für das Unternehmen im Vordergrund steht.



How can we protect against 99% of attacks?

While we explore the many dimensions of the cyber threat landscape, there is one crucial point we must emphasize across them all: the vast majority of successful cyberattacks could be thwarted by implementing a few fundamental security hygiene practices.

By adhering to these minimum-security standards, it is possible to protect against over 99 percent of attacks:

- 1 **Enable multifactor authentication (MFA):** This protects against compromised user passwords and helps to provide extra resilience for identities.
- 2 **Apply Zero Trust principles:** The cornerstone of any resilience plan is to limit the impact of an attack on an organization. These principles are:
 - Explicitly verify. Ensure users and devices are in a good state before allowing access to resources.
 - Use least privilege access. Allow only the privilege that is needed for access to a resource and no more.

- Assume breach. Assume system defenses have been breached and systems may be compromised. This means constantly monitoring the environment for possible attack.
- 3 **Use extended detection and response (XDR) and antimalware:** Implement software to detect and automatically block attacks and provide insights to the security operations software. Monitoring insights from threat detection systems is essential to being able to respond to threats in a timely fashion.
 - 4 **Keep up to date:** Unpatched and out-of-date systems are a key reason many organizations fall victim to an attack. Ensure all systems are kept up to date including firmware, the operating system, and applications.
 - 5 **Protect data:** Knowing your important data, where it is located, and whether the right defenses are implemented is crucial to implementing the appropriate protection.

Hyperscale cloud makes it easier to implement fundamental security practices by either enabling them by default or abstracting the need for customers to implement them. With software-as-a-service (SaaS) and platform-as-a-service (PaaS) solutions, the cloud provider takes responsibility for keeping up with patch management.

Implementing security solutions like MFA or Zero Trust principles is simpler with hyperscale cloud because these capabilities are already built into the platform. Additionally, cloud-enabled capabilities like XDR and MFA are constantly updated with trillions of daily signals, providing dynamic protection that adjusts to the current threat landscape.

Fundamentals of cyber hygiene

99%

Basic security hygiene still protects against 99% of attacks.

How effective is MFA at deterring cyberattacks? A recent study based on real-world attack data from Microsoft Entra found that MFA reduces the risk of compromise by 99.2 percent.¹



Enable multifactor authentication (MFA)



Apply Zero Trust principles



Use extended detection and response (XDR) and antimalware



Keep up to date



Protect data

Outlier attacks on the bell curve make up just 1%

Der Weg zu einer neuen Art des Arbeitens

Schaffen Sie eine starke Zero-Trust-Grundlage

Sichern und Verwalten von Identitäten

Abwehr von Bedrohungen auf unterschiedlichen Plattformen

Schutz sensibler Informationen im gesamten Datenbestand

Optimieren Sie die Endpunktverwaltung

Verbessern Sie die IT-Effizienz

Verwalten und schützen Sie jeden Endpunkt

Bieten Sie das beste Erlebnis mit Windows 11



Steigern Sie Produktivität und Zusammenarbeit

Unterstützen Sie Ihre Mitarbeiter mit erstklassigen Produktivitäts Apps

Bringen Sie alle miteinander in Kontakt und arbeiten Sie zusammen

Stellen Sie Ihren Mitarbeitern die Leistungsfähigkeit von KI sicher zur Verfügung

Steigern Sie die Produktivität mit



Copilot for Microsoft 365

Copilot und Windows 11 Pro — Beschleunigen Sie den Geschäftserfolg

Branchenführende KI. Leistungsstarke Cybersicherheit. Entwickelt für Unternehmen.



Steigern Sie Ihre Erkenntnisse und Effizienz

42%

Anspruchsvolle Workloads können im Durchschnitt schneller erledigt werden¹



Leistungsstarker Schutz als Standard

58%

Gemeldeter Rückgang der Sicherheitsvorfälle²



Nutzen Sie Ihren KI-Vorteil

68%

berichteten von einer verbesserten Arbeitsqualität³



Enthält Copilot unter Windows⁴
+86%
der befragten Mitarbeiter würden KI nutzen, um die richtigen Antworten zu finden⁵

1. Compared to Windows 10 devices. "Improve your day-to-day experience with Windows 11 Pro laptops," Principled Technologies, February 2023. [LINK](#)

2. Windows 11 Survey Report. Techaisle, February 2022. Windows 11 results are in comparison with Windows 10 devices.

3. Work Trend Index Report "What can Copilot's earliest users teach us about generative AI at work", November 2023.

4. Timing of feature delivery and availability varies by market and device. Use Copilot with a Microsoft Account or use Copilot with commercial data protection at no additional cost by signing into a work or school account (Microsoft Entra ID) with Microsoft 365 E3, E5, F3, A3 or A5 for faculty, Business Premium, and Business Standard. Coming to more Entra ID users over time.

5. Will AI fix work? Work trend index annual report, Microsoft, May 9, 2023.

Grundlegendes zu Secured-Core-PCs

 Schutz mit Hardware-Vertrauensanker

 Abwehr von Angriffen auf Firmware-Ebene

 Verhindern des Zugriffs auf nicht verifizierten Code

 Schützen von Identitäten vor externen Bedrohungen



FW Virtualization Support Enabled	Memory Access Protection Enabled
Trusted Platform Module 2.0	Enhanced Sign-In Security Capable
UEFI SecureBoot Enabled	Memory Integrity Enabled
Modern Device Servicing	FW Virtualization Support Enabled
	Trusted Platform Module 2.0
	UEFI SecureBoot Enabled
	Modern Device Servicing
STANDARD	ENHANCED

MSFT 3rd Party UEFI CA not trusted by default*
Secured-core PC device identifier
Modern Standby
SMM Protection**
DRTM Protection
Memory Access Protection Enabled
Enhanced Sign-In Security Capable
Memory Integrity Enabled
FW Virtualization Support Enabled
Trusted Platform Module 2.0
UEFI SecureBoot Enabled
Modern Device Servicing
SECURED-CORE



System Management Mode deep dive:
[How SMM isolation hardens the platform - Microsoft Security Blog](#)



Leistungsstarker Schutz als Standard

Schutz von Geschäftsdaten

Schützen Sie Ihre wertvollen Daten und kontrollieren Sie Apps und den Zugriff auf Informationen überall mit einem durchgängigen Sicherheitsmanagement.

Copilot in Windows¹ mit kommerziellem Datenschutz

Intune Endpoint Privilege Management²

Token Protection (in preview) for sign-in sessions

Local Administrator Password Solution (LAPS)

MAM for Windows

Bitlocker

App Control für Business Policy³

Das sicherste Windows aller Zeiten

PCs sind bereits mit aktivierten Sicherheitsebenen ausgestattet, sodass Sie überall mit leistungsstarker Cybersicherheit für Hardware, Software, Identitäten und Daten in die Arbeit eintauchen können.

Microsoft Defender Antivirus

Windows Hello für Business **passwortlos**⁴

Out-of-the-box security mit TPM 2.0

Passkey

Isolationstechnologien: virtualisierungsbasierte Sicherheit, Hypervisor-geschützte Codeintegrität und isolierte Win32-Apps (Entwickler)⁵

Sichere Inbetriebnahme⁶

Schützt vor neuen Bedrohungen

Schützen Sie sich vor Cyberbedrohungen mit den neuesten Sicherheitsvorkehrungen für mehr Sicherheit, einschließlich einer gemeldeten 2,8-mal weniger Fälle von Identitätsdiebstahl ⁷.

Verbesserter Phishing-Schutz mit Microsoft Defender SmartScreen

Sperren bei Abwesenheits-/Anwesenheitserkennung mit Windows Hello⁴

Windows update für business

Liste der anfälligen Microsoft-Treiber⁸

End-to-End-Schutz, vereinfacht

Eine optimierte Chip-to-Cloud-Sicherheitslösung auf Basis von Windows 11 verbesserte die Produktivität von IT- und Sicherheitsteams um 25 %.⁹

Config refresh

Microsoft Intune endpoint privilege management

Windows Firewall¹⁰

Windows Local Administrator Password Solution (LAPS) mit Microsoft Entra ID.

MAM für Windows

Liste der Microsoft-Schwachstellen für Treiber

1. Timing of feature delivery and availability varies by market and device. Use Copilot with a Microsoft Account or use Copilot with commercial data protection at no additional cost by signing into a work or school account (Microsoft Entra ID) with Microsoft 365 E3, E5, F3, A3 or A5 for faculty, Business Premium, and Business Standard. Coming to more Entra ID users over time.

2. Endpoint Privilege Management requires Microsoft Entra ID and an additional license beyond the Microsoft Intune Plan 1 license. You can choose between a stand-alone license that adds only EPM, or license EPM as part of the Microsoft Intune Suite. For more information, see Use Intune Suite add-on capabilities

3. Requires a modern device management (MDM) solution like Microsoft Intune.

4. Hardware dependent.

5. Requires developer enablement. Available in preview.

6. Secure startup is used with a TPM like Microsoft TPM 2.0

7. Windows 11 Survey Report. Techaisle, February 2022. Windows 11 results are in comparison with Windows 10 devices.

8. Vulnerable driver blocklist rules can be enabled and configured using Microsoft Intune, mobile device management (MDM), Microsoft Endpoint Configuration Manager, Group Policy, and PowerShell.

9. Commissioned study delivered by Forrester Consulting "The Total Economic Impact™ of Windows 11 Pro Devices", December 2022. Note, quantified benefits reflect results over three years combined into a single composite organization that generates \$1 billion in annual revenue, has 2,000 employees, refreshes hardware on a four-year cycle, and migrates the entirety of its workforce to Windows 11 devices.

10. Microsoft Intune required; sold separately.

Optimiert für Unternehmen

Windows 11 Pro ist einfach zu bedienen, bereitzustellen und zu verwalten, sodass Sie ganz einfach von den neuesten Fortschritten in der KI für Unternehmen profitieren können.



Optimieren Sie Sicherheit, Datenschutz und Produktivität. Kombinieren Sie Windows 11 Pro mit Microsoft 365 Business Premium oder höher, um die neuesten Office-Apps, moderne Geräteverwaltung und kommerziellen Datenschutz zu erhalten.



App-Kompatibilität und Testbasis für Microsoft 365. Bleiben Sie Problemen einen Schritt voraus, und stellen Sie die Qualität sicher, indem Sie Test Base für Microsoft 365 verwenden, eine Cloudumgebung, um Ihre Apps vor der Bereitstellung anhand von Sicherheits-, Qualitäts- und Funktionsupdates zu überprüfen. Vorhandene Windows-Apps werden wie erwartet mit einer Kompatibilitätsrate von 99,7 % ausgeführt¹.



Beschleunigen Sie die Bereitstellung und das Onboarding von Mitarbeitern. Erleben Sie die Vorteile der Zero-Touch-Bereitstellung mit Windows Autopilot. Stellen Sie Geräte im Durchschnitt 25 % schneller bereit⁴.



Einfache Durchsetzung von Sicherheitsrichtlinien. Stellen Sie sicher, dass Ihr Unternehmen geschützt ist, ohne die Produktivität zu beeinträchtigen. Verwenden Sie die Konfigurationsaktualisierung, um die Geräteeinstellungen automatisch alle 90 Minuten zu aktualisieren, um sie an die Sicherheitsrichtlinien Ihrer Organisation anzupassen.

99.7%

App-Kompatibilität mit Programmen zur kostenlosen Lösung von Problemen¹



1. App Assure program data. Compared to Windows 10 devices.

2. Sold separately.

3. App Assure is available at no additional charge; Test Base for Microsoft 365 sold separately.

4. Commissioned study delivered by Forrester Consulting "The Total Economic Impact™ of Windows 11 Pro Devices", December 2022. Note, quantified benefits reflect results over three years combined into a single composite organization that generates \$1 billion in annual revenue, has 2,000 employees, refreshes hardware on a four-year cycle, and migrates the entirety of its workforce to Windows 11 devices.



Microsoft Copilot



Copilot [in Bing]

(ehemals Bing Chat (Unternehmen))

Erhalten Sie Antworten und Inspiration



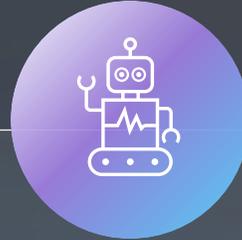
(1) Kostenlos mit Anzeigen für Verbraucher

**Wird zum Trainieren der KI verwendet und hat keinen kommerziellen Datenschutz
Speichert den Chatverlauf**

(2) **Copilot mit kommerziellem Datenschutz**

Kostenlos in Business Standard, Business Premium, E3, E5, A3, A5 oder als Einzelplatzlizenz (kostenlose Entra ID erforderlich)

Generell verfügbar ab 1. Dezember



Copilot unter Windows

Ihr täglicher KI-Assistent



(1) **Copilot**

für Home und Pro basierend auf Copilot mit Bing Chat
Unterstützt Systembefehle in Windows 11

Wird zum Trainieren der KI verwendet und hat keinen kommerziellen Datenschutz

(2) **Copilot mit kommerziellem Datenschutz**

für ein Arbeits-, Schul- oder Universitätskonto auf der Basis von BCE
Speichert nicht den Chatverlauf
Unterstützt Systembefehle in Windows 11



Copilot in Microsoft 365

KI für Ihr Unternehmen

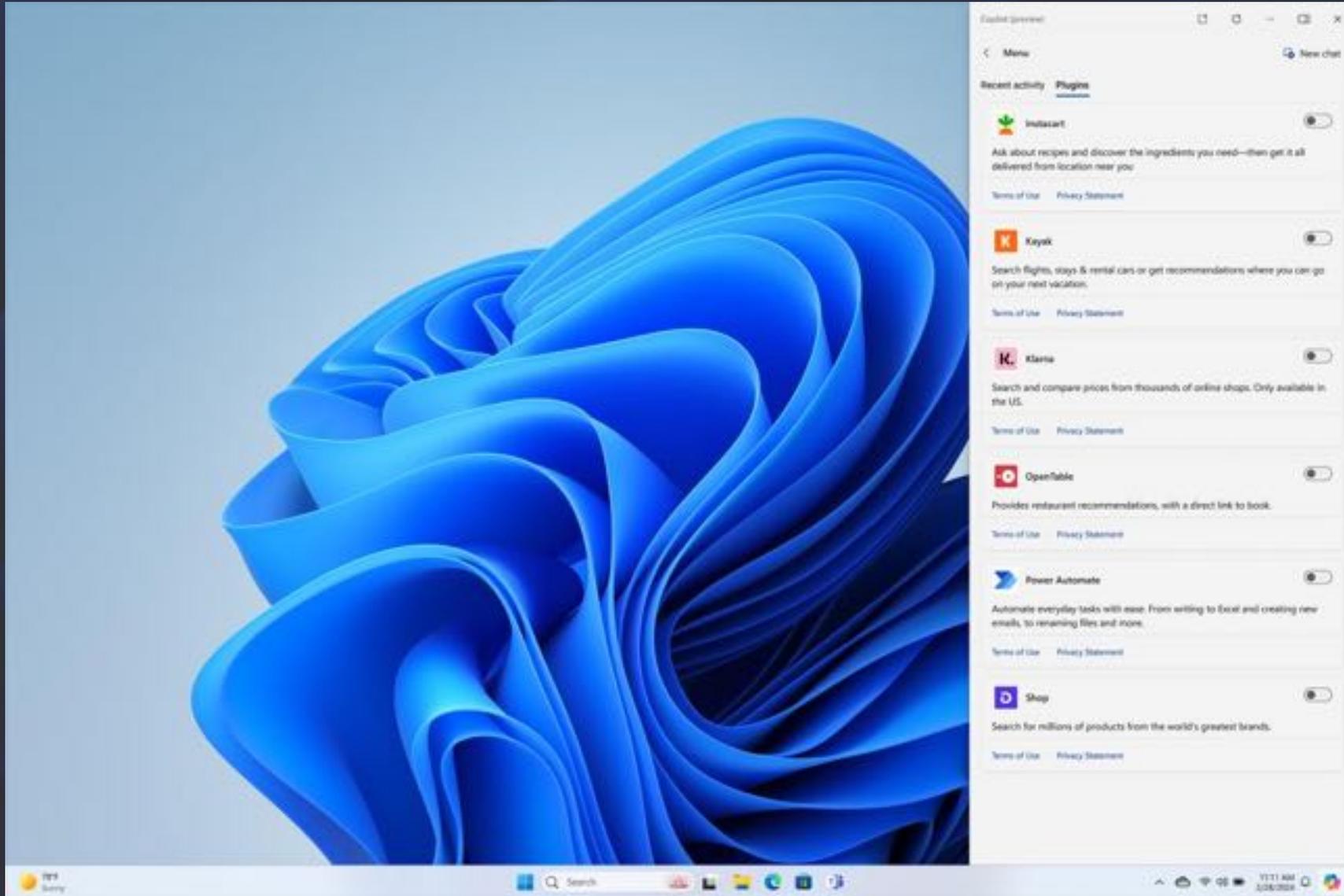
Erstellen, Analysieren und Zusammenfassen



\$30 pro Benutzer/Monat

Business Standard*, Business Premium*, E3, E5

Copilot in Windows 11 (Preview) – Plugins & New Skills^{*1}



New Skills:

•Settings:

- Turn on/off battery saver
- Show device information
- Show system information
- Show battery information
- Open storage page

•Accessibility:

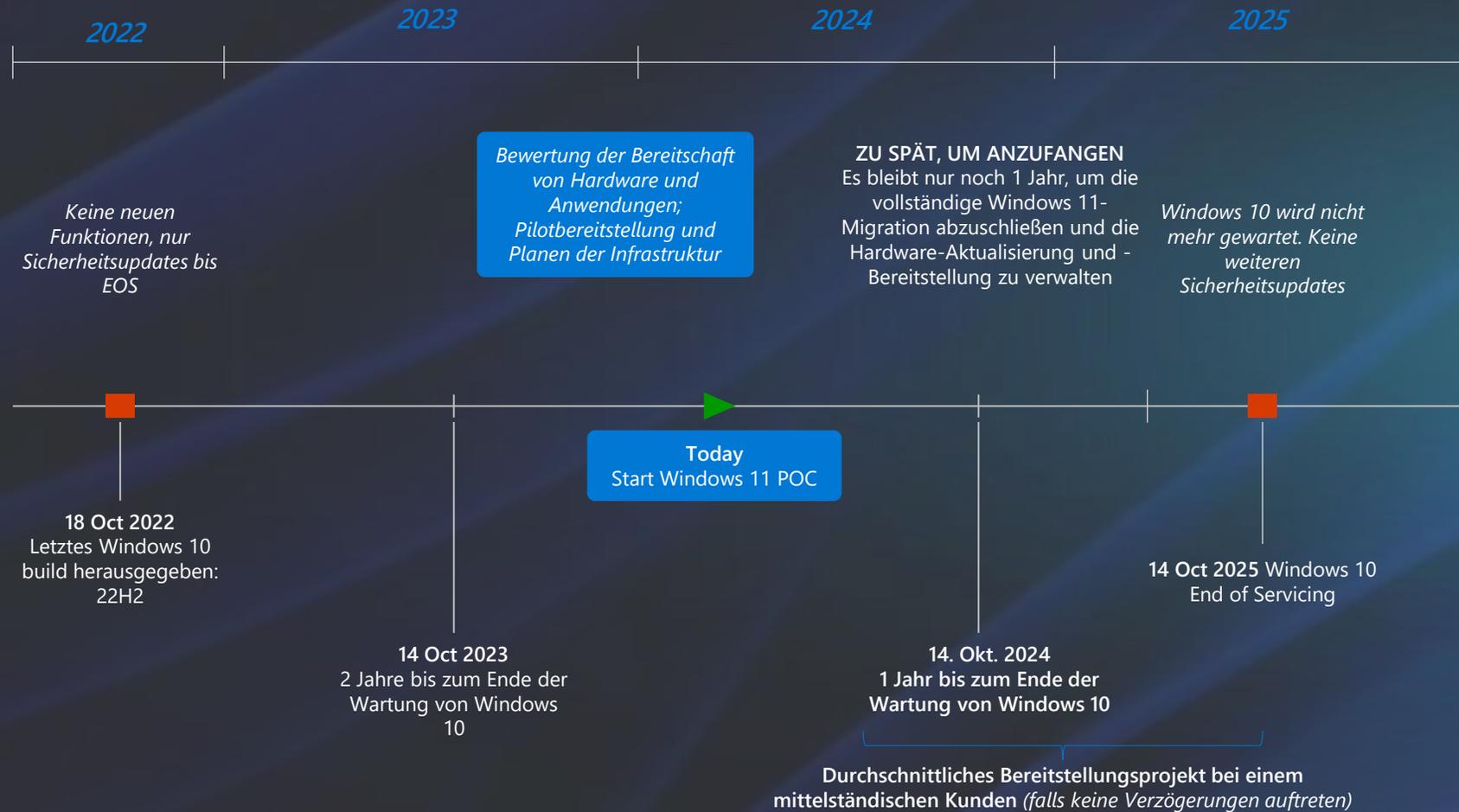
- Launch live captions
- Launch narrator
- Launch screen magnifier
- Open voice access page
- Open text size page
- Open contrast themes page
- Launch voice input

•Device information:

- Show available Wi-Fi network
- Display IP address
- Show available storage space
- Empty recycle bin

Kunden müssen jetzt mit der Aktualisierung beginnen, bevor es zu spät ist

Zeitplan bis zum Ende des Supports für Windows 10



Q: Is it time to move to Windows 11?

A: Yes

"The release of the Windows 11 2022 update signals that it is time for enterprises to introduce Windows 11 into annual update processes."

Gartner

Gartner

Aktivierungsmodelle für die Volumenlizenzierung

5-by-5 activation keys

Verwenden einer beliebigen Updateverwaltungsinfrastruktur. Erfordert eine interne Automatisierung, um Geräte zu aktivieren.

Unterstützt Entra ID Join, Hybrid Join, oder Active Directory-Einbindung.

ESUs werden von Windows Update bereitgestellt, keine Downloads.

Dem Gerät zugewiesene Lizenz.

\$61 pro Gerät und Jahr.

Cloud update management

Verpflichtung zur Verwendung von Windows Autopatch, Intune oder einer Cloud-basierten Lösung für die Verwaltung mobiler Geräte eines Drittanbieters.

Unterstützt Entra ID Join oder Hybrid Join.

ESUs werden von Windows Update bereitgestellt, keine Downloads.

Den Benutzern zugewiesene Lizenz.

45 US-Dollar pro Benutzer und Jahr.
(~25% Rabatt)

Alle Preise sind in US-Dollar angegeben. Die regionalen Preise variieren je nach Wechselkurs zum Zeitpunkt der Bestellung. Es wird Sonderpreise für Bildungseinrichtungen, gemeinnützige Organisationen und akkreditierte Renovierer geben.



Nächste Schritte



Betriebssysteme

Das Ende des Supports für Windows 10 kommt am 14. Oktober 2025¹. Aktualisieren Sie berechnete PCs auf Windows 11 Pro und bereiten Sie sich darauf vor, veraltete Geräte zu aktualisieren.



Geräte

Planen Sie neue Windows 11 Pro-Geräte für die neuesten Funktionen, einschließlich Produktivitäts-, Sicherheits- und Verwaltungsvorteile.



Management

Führen Sie eine Cloud-basierte, moderne Geräteverwaltung ein, indem Sie Windows 11 Pro mit Microsoft 365 Business Premium kombinieren, das auch den Schutz kommerzieller Daten ermöglicht Copilot in Windows².



Endpunkt-Sicherheit

Implementieren Sie eine Strategie für standardmäßige Sicherheit, und verwenden Sie eine gemeinsame Sicherheitsbaseline für alle Geräte und die Cloud.



Wachstumspfad

Führen Sie ein Upgrade auf Windows 11 Enterprise durch, das Teil von Microsoft 365 Enterprise für erweiterte Sicherheit und Verwaltung einschließlich Windows Autopatch ist.

1. [Blog: Plan for Windows 10 EOS with Windows 11, Windows 365, and ESU.](#)
[LINK](#)

2. Timing of feature delivery and availability varies by market and device. Screen simulated, subject to change. Use Copilot with a Microsoft Account or use Copilot with commercial data protection at no additional cost by signing into a work or school account (Microsoft Entra ID) with Microsoft 365 E3, E5, F3, A3 or A5 for faculty, Business Premium, and Business Standard. Coming to more Entra ID users over time.