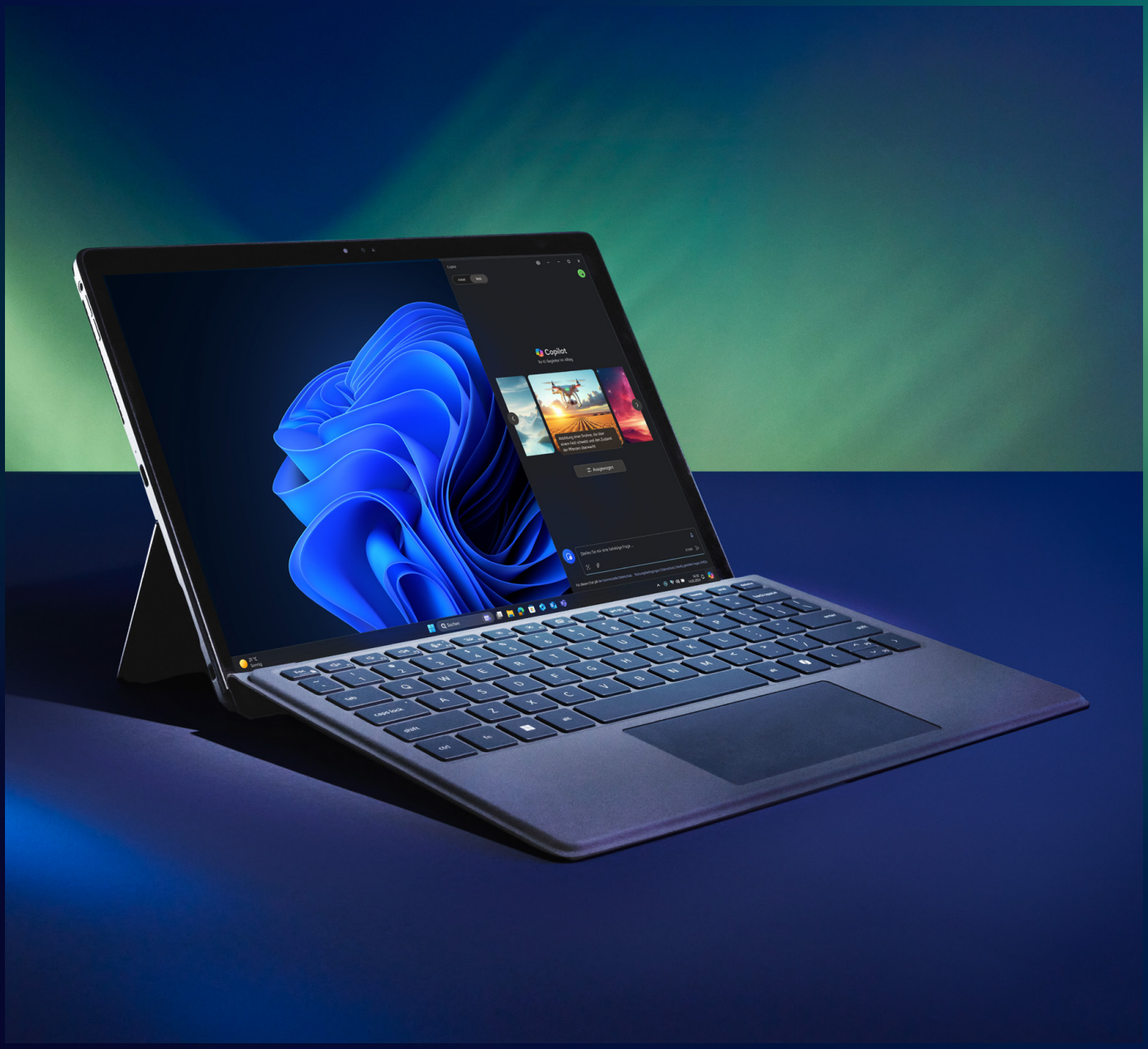


Höchste Maßstäbe für Mitarbeitende und Organisationen

durch standardmäßige Sicherheit

Windows 11 Pro

INHALTSVERZEICHNIS

Beschleunigter Geschäftserfolg dank Always-On-Schutz

Während IT-Führungskräfte neue Technologien nutzen, um das Wachstum voranzutreiben, müssen sie gleichzeitig das Unternehmen vor den sich ständig weiterentwickelnden Sicherheitsbedrohungen schützen. Komplexe Bedrohungen wie z. B. Phishing, Ransomware und DDoS-Angriffe (Distributed Denial of Service) nehmen stetig zu und erfordern eine immer stärkere und proaktive Verteidigung.

Menschliche Fehler erhöhen die Komplexität dieser Herausforderung, denn sie sind die Ursache für 46 % aller Vorfälle im Bereich der Cybersicherheit.[2] Unterschiedliche Arbeitsstile und flexible Arbeitsumgebungen erhöhen das Risiko zusätzlich, da auf diese Weise die Zahl der potenziellen Schwachstellen wächst.

In einem wettbewerbsintensiven Geschäftsumfeld kann die Antwort nicht darin bestehen, ein System komplett abzuschotten. IT-Führungskräfte benötigen Lösungen, die nicht nur den Schutz verstärken, sondern gleichzeitig die Produktivität erhöhen – Geräte, die sowohl auf Sicherheit als auch auf eine Geschäftstransformation ausgelegt sind.

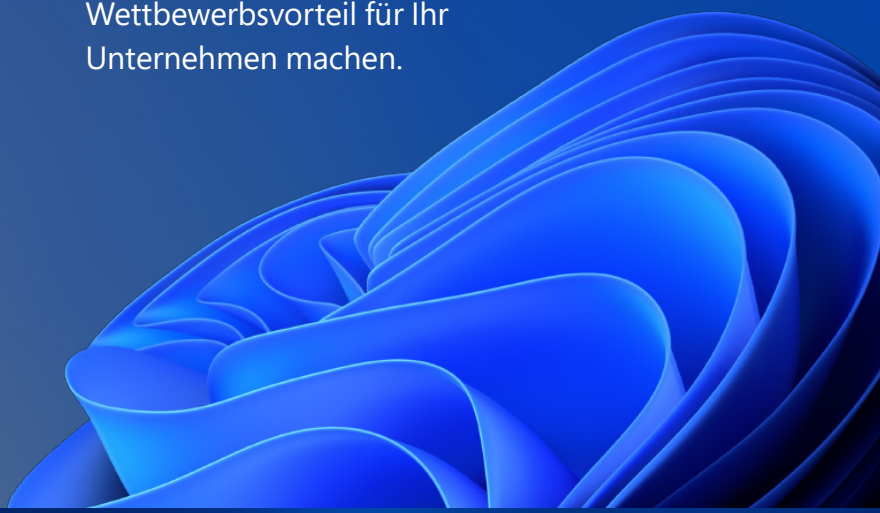
Windows 11 Pro-PCs wurden entwickelt, um Cyberbedrohungen abzuwehren, Innovation und Effizienz zu stärken, Probleme zu lösen und mit weniger Zeit, Aufwand und Kosten mehr zu erreichen.

> Windows 11 Pro verfügt über leistungsstarke Schutzebenen, die Berichten zufolge **Sicherheitsvorfälle um 58 % reduzieren können.**[1]

Systemweite Intelligenz schützt proaktiv vor Bedrohungen, liefert bessere Antworten, verbessert Videokonferenzen, bietet mehr Barrierefreiheit und trägt dazu bei, Ihren CO^2-Fußabdruck zu verringern. Zudem liefert sicherste Windows aller Zeiten die neuesten Feature- und Sicherheitsupdates direkt auf Ihren Desktop.

Und das Beste: Copilot in Windows[3] gehört jetzt zum Lieferumfang von Windows 11 Pro-PCs und sorgt für mehr Erkenntnisse und Effizienz.

Lesen Sie weiter und erfahren Sie, wie Ihre Teammitglieder von standardmäßigem Schutz und KI-Erfahrungen auf Abruf profitieren können. Dank dieser Funktionen können sie jederzeit Höchstleistungen erbringen, ihr volles Potenzial ausschöpfen und ihren Einfallsreichtum zu einem Wettbewerbsvorteil für Ihr Unternehmen machen.



Mehr Innovation, weniger Cyberverbrechen

Die zunehmende Flexibilität der modernen Arbeitswelt schafft ein herausforderndes Umfeld für die Cybersicherheit. IT-Führungskräfte suchen nach Lösungen, um die Produktivität, die Zusammenarbeit und die Innovation zu verbessern und gleichzeitig die Sicherheit der Mitarbeitenden an jedem beliebigen Standort zu gewährleisten. Die gute Nachricht ist: Sie können sich erfolgreich gegen mehr als 99 % der Cyberangriffe schützen, indem Sie einige grundlegende Maßnahmen zur Sicherheitshygiene befolgen: Multi-Faktor-Authentifizierung (MFA), Anwendung von Zero-Trust-Prinzipien, Einsatz von Antischadsoftware und XDR (Extended Detection and Response), Aktualisierung von Firmware, Betriebssystemen und Apps sowie Verwaltung und Schutz von geschäftskritischen Daten.[4]

Viele dieser Maßnahmen sind so einfach zu implementieren wie ein Upgrade Ihrer PCs. Windows 11 Pro-Geräte sind sofort nach dem Auspacken durch mehrere hardwarebasierte Schutzebenen gesichert, was sich Berichten zufolge in einem Rückgang der Sicherheitsvorfälle um 58 % niederschlägt.[1] Mit Windows 11 Pro und Microsoft Intune[5] können Sie problemlos eine moderne Sicherheitsverwaltung in der gesamten Organisation implementieren – auch für Microsoft 365-Apps[6] und Copilot. Darüber hinaus können Sie die Anmeldeinformationen Ihrer Mitarbeitenden mit integrierten Features wie dem erweiterten Phishing-Schutz in Microsoft Defender SmartScreen effizient schützen. Die Anwesenheitserkennung mit den Funktionen „Sperren bei Verlassen" und „Reaktivieren bei Annäherung"[7] trägt ebenfalls dazu bei, Ihre Inhalte und Ihre Privatsphäre zu schützen: Ihr PC wird gesperrt, wenn Sie Ihren Arbeitsplatz verlassen, und wenn Sie sich Ihrem PC erneut nähern, werden Sie über Windows Hello[7] mit Sensoren zur Anwesenheitserkennung sicher wieder angemeldet.

So können Ihre Teams überall ihr Bestes geben – unterstützt durch das sicherste Windows aller Zeiten und mithilfe von branchenführender KI. Und während Copilot in Windows eine Verbesserung der Arbeitsabläufe für fast jeden Mitarbeitenden in Ihrer Organisation ermöglicht, kann Ihr IT-Team mit Copilot für Security zudem Bedrohungen erkennen und maßgeschneiderte Erkenntnisse sowie Informationen zu den nächsten Schritten bereitstellen, um die Reaktion auf Vorfälle zu beschleunigen. Tatsächlich gewinnt die KI in einem zunehmend komplexeren Cyberökosystem eine immer größere Bedeutung und hat das Potenzial, die Sicherheitslandschaft zu verändern, indem sie die Fähigkeiten, die Geschwindigkeit und das Wissen für eine wirksame Verteidigung erweitert und verbessert.

> Der Microsoft-Bericht über digitale Abwehr für das Jahr 2023 zeigt das Potenzial der KI auf, die Sicherheitslandschaft zu verändern, indem sie die Fähigkeiten, die Geschwindigkeit und das Wissen für eine wirksame Verteidigung erweitert und verbessert.
>
> **Bericht herunterladen >**

Die Sicherheitsexperten von Microsoft analysieren mithilfe der KI täglich mehr als 65 Billionen Signale. Tatsächlich investiert Microsoft unter anderem in die Sicherheitsforschung, in Innovationen und in die globale Sicherheitscommunity:[4]

65 Billionen

Signale, die täglich mittels hochentwickelter Datenanalyse und KI-Algorithmen synthetisiert werden

10.000+

Experten für Sicherheit und Bedrohungsanalyse rund um den Globus

4.000

blockierte Bedrohungen in Bezug auf die Identitätsauthentifizierung pro Sekunde

15.000+

Partner mit spezialisierten Lösungen in unserem Sicherheitsökosystem

135 Millionen

verwaltete Geräte mit Erkenntnissen zu Sicherheit und Bedrohungslandschaft

300+

aufgespürte Bedrohungsakteure, darunter 160 nationalstaatliche Akteure und 50 Ransomware-Gruppen

100.000+

entfernte Domänen, die von Cyberkriminellen genutzt werden

Förderung Ihres Geschäftserfolgs durch standardmäßig hohe Sicherheit

Während sich IT-Führungskräfte auf strategische Initiativen konzentrieren, müssen ihre Geschäftsdaten weiterhin geschützt, ihre Endgeräte gesichert und ihre Mitarbeitenden für den Erfolg befähigt werden. Ein Sicherheitsplan muss nicht nur dem Schutz dienen, sondern auch der Produktivität, der Zusammenarbeit und der betrieblichen Effizienz.

Viele Organisationen setzen auf Geräte, die sowohl für die Sicherheit als auch für die Geschäftstransformation entwickelt wurden. Die neuen Windows 11 Pro-PCs sind standardmäßig mit leistungsstarken Schutzfunktionen und KI-Erfahrungen ausgestattet, die es Teammitgliedern ermöglichen, überall bessere Leistungen zu erbringen, ihr volles Potenzial auszuschöpfen und ihren Einfallsreichtum als Wettbewerbsvorteil zu nutzen.

Durch die Bereitstellung von Windows 11 Pro-Geräten können IT-Führungskräfte eine „Secure-by-Default"-Strategie implementieren, um die Angriffsfläche zu minimieren und Bedrohungen zu verhindern, bevor sie entstehen – und das bei einem berichteten Rückgang der Sicherheitsvorfälle um 58 %.[1] Sie können die Vorteile eines modernen Sicherheitsmanagements nutzen, um Richtlinien für Geräte, Apps und die Cloud durchzusetzen. Und dank der leistungsstarken Always-On-Schutzfunktionen müssen sie weniger Zeit für die Reaktion auf Bedrohungen aufwenden und haben mehr Zeit für Wachstum und Innovation.

Windows 11 Pro-PCs: Leistungsstarker Schutz standardmäßig

Höchste Sicherheit für Geschäftsdaten

Windows 11 Pro-Geräte bieten eine End-to-End-Sicherheitsverwaltung, um wertvolle Daten zu schützen und Apps sowie den Zugriff auf Informationen an beliebigen Standorten zu kontrollieren. Der hardwarebasierte Schutz ist eng in die Software integriert und reduziert die Zahl der Firmware-Angriffe Berichten zufolge um das 3,1-fache.[1]

Schutz vor immer neuen Bedrohungen

Böswillige Akteure suchen unermüdlich nach Schwachstellen in Ihrem Netzwerk. Dank der neuesten Schutzmechanismen können Sie auf eine optimale Abwehr von Cyberbedrohungen vertrauen – einschließlich einer berichteten 2,8-fachen Verringerung der Fälle von Identitätsdiebstahl.[1] Außerdem haben Sie die Möglichkeit, Ihre Identitäten und Daten mithilfe von Tokenschutz, erweiterten Windows Hello-Anmeldesitzungen und verbessertem Phishing-Schutz abzusichern. Zusätzlich können Sie Ihre Daten mit der Anwesenheitserkennung von Windows Hello schützen. Diese Funktion verhindert unbefugte Zugriffe, indem Ihr PC beim Verlassen des Arbeitsplatzes gesperrt und bei Annäherung sicher wieder aktiviert wird.[7]

Das sicherste Windows aller Zeiten

Windows 11 Pro-PCs sind bereits mit verschiedenen Sicherheitsebenen ausgestattet, sodass Ihre Teammitglieder von überall aus produktiv werden können – geschützt durch leistungsstarke Cybersicherheit für Hardware, Software, Identitäten und Daten. TPM 2.0 bietet hardwarebasierten Schutz für Anmeldeinformationen und andere vertrauliche Daten, während Windows Hello for Business[7] für eine einfache, sichere und kennwortlose Anmeldung sorgt.

End-to-End-Schutz, leicht gemacht

Mit Intune Endpoint Privilege Management (EPM) können Sie den Zugriff auf Systemressourcen schützen und gleichzeitig die Produktivität aller Mitarbeitenden aufrechterhalten.[8] Und Ihre Teams erhalten mit MAM für Windows auf ihren persönlichen oder BYOD-Geräten über Microsoft Edge sicheren Zugriff auf ihre Arbeits-E-Mails, Teams-Besprechungen und andere Inhalte. Eine optimierte, auf Windows 11 basierende Sicherheitslösung vom Chip bis zur Cloud verbessert die Produktivität von IT- und Sicherheitsteams Berichten zufolge um 25 %.[9]

Einfluss des Arbeitsstils auf die Anforderungen an Geräte und Betriebssysteme

Seit 2020 liefern Untersuchungen von Microsoft wichtige Erkenntnisse über die Rolle neuer Geräte und Betriebssysteme bei der Gestaltung der Zukunft der Arbeit und der Bekämpfung einer sich ständig weiterentwickelnder Bedrohungslandschaft im Bereich der Cybersicherheit.

Flexible Arbeitsformen und -orte setzen sich immer mehr durch und spiegeln einen dauerhaften Wandel in der Beziehung der Mitarbeitenden zu ihrer Arbeit und ihrem Arbeitgeber wider. Mitarbeitende wünschen sich mehr Autonomie und Bequemlichkeit, und viele Organisationen erkennen die Vorteile, die sich aus diesen Veränderungen ergeben, wie z. B. eine höhere Produktivität und Arbeitszufriedenheit.[10]

Diese augenscheinlich tiefgreifende Veränderung in der Arbeitsdynamik führt zu neuen Herausforderungen im Bereich der Sicherheit, insbesondere in flexiblen Arbeitsumgebungen. Die Entwicklung von Arbeit und Technologie geht jedoch Hand in Hand, und bessere Abläufe können die Produktivität steigern. Der Einsatz von KI durch Investitionen in neue Geräte kann nicht nur die digitalen Schulden verringern, sondern auch die Produktivität und die Problemlösung im Allgemeinen verbessern, einschließlich eines größeren Wohlbefindens, einer besseren Work-Life-Balance und einer insgesamt besseren Mitarbeitendenerfahrung.

Die Veränderungen in der Arbeitswelt beschränken sich nicht nur auf den *Arbeitsort*, sondern auch darauf, *in welcher Weise* Arbeitsaufgaben erledigt werden. Genau hier spielt die KI, einschließlich Copilot in Windows und Copilot für Microsoft 365,[6] eine immer wichtigere Rolle bei der Umgestaltung der Arbeitslandschaft. Angesichts der rasanten Zunahme der Erzeugung arbeitsbezogener Daten stellen veraltete Geräte und Betriebssysteme ein echtes Hindernis für die Innovationen dar, die diese Technologien versprechen.

Um in einem sich schnell verändernden Markt erfolgreich zu sein, benötigen Unternehmen die richtigen Tools, die Innovationen fördern und gleichzeitig die Sicherheit bieten, überall erfolgreich zu sein. Mit Windows 11 Pro-Geräten, die standardmäßig über einen leistungsstarken Schutz verfügen, können Organisationen diese Herausforderungen meistern, indem sie die Möglichkeiten der neuen Arbeitsplatztechnologien optimal nutzen.

In diesem Abschnitt gehen wir der Frage nach, wie unterschiedliche Arbeitsstile nicht nur die individuelle Arbeitserfahrung, sondern auch die Dynamik in zusammenarbeitenden Teams, das Unternehmen als Ganzes und sogar das gesellschaftliche Gefüge selbst verändern.

Flexible Arbeit in großem Umfang: Unterschiedliche Demografien verstehen

Auswirkungen auf die Einzelnen

Flexible Arbeitsmodelle ermöglichen eine Kombination aus Remote- und Büroarbeit und bieten den Einzelnen mehr Flexibilität und Autonomie. Die Möglichkeit, von verschiedenen Standorten aus zu arbeiten, kann die Work-Life-Balance verbessern, erfordert jedoch neue Tools, Technologien und Sicherheitsmaßnahmen, die auf unterschiedliche Umgebungen zugeschnitten sind.

Windows 11 Pro bietet den Mitarbeitenden zusätzlich zu einem Produktivitätsschub zahlreiche weitere Vorteile. Mithilfe von Copilot in Windows können sie Aufgaben optimieren und kreativer, innovativer und unabhängiger werden. Und intuitive Benutzerfunktionen wie die PC-Steuerung per Stimme7 sorgen für mehr Teilhabe und ermöglichen es jedem und jeder Einzelnen, mehr zu bewirken.

Auswirkungen auf die Zusammenarbeit im Team

Der Wandel hin zu flexibler Arbeit erfordert ein Umdenken bei der Zusammenarbeit von Teams. Flexibles Arbeiten begünstigt zwar einen vielseitigeren und globaleren Pool von Fachkräften, erfordert aber auch robuste, sichere Plattformen und Tools für die Zusammenarbeit, die eine nahtlose Kommunikation und Koordination unabhängig vom physischen Standort ermöglichen.

Mit Microsoft Teams können Teammitglieder auf den neuesten Windows 11 Pro-Geräten schnell, flexibel und mit Stil zusammenarbeiten. KI-gestützte Empfehlungen ermöglichen es ihnen, nicht nur schneller, sondern auch intelligenter zu arbeiten. Organisationen berichten über eine durchschnittliche Zeitersparnis von 50 % bei Arbeitsabläufen und Zusammenarbeit.[11]

Einfluss auf die Organisation als Ganzes

Organisationen haben mit komplexen Problemen wie teamübergreifender Kommunikation, systemischer Einsamkeit und größeren Personalveränderungen zu kämpfen. Zu den potenziellen Bedrohungen auf Organisationsebene gehören ausgeklügelte Ransomware-Angriffe, die ganze Netzwerke lahmlegen können.

Windows 11 Pro ermöglicht es Unternehmen, Unwägbarkeiten souverän zu handhaben und eine sichere Kommunikation in verschiedenen Arbeitsumgebungen zu gewährleisten. Systemweite Intelligenz schützt proaktiv vor Bedrohungen, liefert die richtigen Antworten, verbessert Videokonferenzen, bietet mehr Barrierefreiheit und trägt dazu bei, Ihren CO^2-Fußabdruck zu verringern.

Auswirkungen auf die Gesellschaft

Die sich wandelnden Arbeitsgeografien und ihre Auswirkungen auf gesellschaftlicher Ebene werden derzeit untersucht. Inmitten dieser umwälzenden Veränderungen können Bedrohungen der Cybersicherheit ganze Sektoren gefährden.

Mit Windows 11 Pro sind Unternehmen in der Lage, sich sicher an diese globalen Veränderungen anzupassen. Es gewährleistet Geschäftskontinuität und Produktivität und bietet gleichzeitig einen robusten Schutz gegen die zunehmenden Bedrohungen der Cybersicherheit.

Drei Risikofaktoren im Zeitalter des modernen Arbeitens

Das Gebot der Stunde für Unternehmen ist klar: Wenn sie die aktuellen und zukünftigen Unwägbarkeiten der Arbeitslandschaft meistern wollen, müssen robuste Cybersicherheitsstrategien und moderne Systeme und Geräte den Kern ihres Betriebskonzepts bilden. Die folgenden drei Risikofaktoren sind in der realen Welt angesiedelt und können – wenn sie nicht proaktiv in Angriff genommen werden – die Sicherheitslage eines Unternehmens und den allgemeinen Geschäftserfolg erheblich beeinflussen.

1. Gebremste Innovation

Durchschnittlich **58 %** mehr blockierte Bedrohungen[1] und damit mehr Zeit für Innovationen.

64 % der IT-Führungskräfte sind der Auffassung, dass sich Bedenken hinsichtlich der Cybersicherheit negativ auf die Bereitschaft ihrer Organisation auswirken, in innovative Technologien zu investieren.[12]

Veraltete Systeme und Geräte können die Fähigkeit einer Organisation beeinträchtigen, innovativ zu sein und sich in einem rasch wandelnden Geschäftsumfeld zu behaupten. Wenn ein Unternehmen den Einsatz von KI zu lange aufschiebt, läuft es möglicherweise Gefahr, von innovativeren Konkurrenten überflügelt zu werden, die den Einfallsreichtum ihrer Arbeitskräfte zu ihrem Vorteil nutzen.

Außerdem sind ältere Systeme fehleranfällig und verursachen störende Ausfallzeiten, die die Produktivität beeinträchtigen und Kundenbeziehungen und geschäftliche Möglichkeiten gefährden. Dies kann sich auch auf die Fähigkeit eines Unternehmens auswirken, Spitzenkräfte anzuziehen und zu halten. Es ist von entscheidender Bedeutung, dass alle Mitarbeitenden mit sicheren und barrierefreien Technologien ausgestattet sind, die es ihnen ermöglichen, sich zu vernetzen und zur Innovationsagenda eines Unternehmens beizutragen.

Überlegungen für Führungskräfte:

- Wie wirkt sich veraltete Technologie auf unsere Innovation und Wettbewerbsfähigkeit aus?
- Wie können wir unsere Teams strukturieren und dazu befähigen, KI als Innovationsbeschleuniger zu nutzen?
- Wie passt unsere derzeitige Technologie zu den verschiedenen Arbeitsstilen innerhalb unserer Organisation?
- Kann unsere Infrastruktur die Fachkräfte anziehen und binden, die für die moderne Arbeitsdynamik benötigt werden?

2. Überlastete IT-Ressourcen

66 % der Mitglieder von Sicherheitsteams **sind bei der Arbeit erheblichem Stress ausgesetzt. 64 %** haben bereits erlebt, **dass Arbeitsstress ihre psychische Gesundheit beeinträchtigt**.[13]

Von den IT- Fachkräften, die in hohem Maße von Burnout betroffen sind, erwägen laut einer Umfrage von Yerbo **42 %, ihr Unternehmen innerhalb der nächsten sechs Monate zu verlassen**. Selbst unter den Mitarbeitenden, die in geringem oder mittlerem Ausmaß unter Burnout leiden, **äußern 25 % den Wunsch, ihr Unternehmen in naher Zukunft zu verlassen**.[14]

Geschätzt bleiben etwa **3,4 Millionen** Stellen für qualifizierte Sicherheitsexperten aufgrund des weltweiten Mangels an Fachkräften unbesetzt.[15]

Ältere Systeme sind wartungsintensiver, belasten oftmals die IT-Ressourcen und lenken den Fokus von strategischen Aufgaben ab. Die Inkompatibilität mit modernen IT-Verwaltungstools erschwert zudem die Aufrechterhaltung einer stabilen Sicherheit und Compliance. Zudem fehlen bei veralteten Systemen häufig die neuesten Sicherheitsupdates, was sie für Cybersicherheitsbedrohungen anfällig macht und zu kostspieligen Datenschutzverletzungen führen kann, die das Kundenvertrauen beeinträchtigen könnten.

Infolgedessen suchen immer mehr IT- Führungskräfte nach einem End-to-End-Schutz, der ihre Mitarbeitenden entlastet. Tatsächlich kann eine optimierte, auf Windows 11 basierende Sicherheitslösung vom Chip bis zur Cloud die Produktivität von IT- und Sicherheitsteams Berichten zufolge um 25 % verbessern.[9]

Überlegungen für Führungskräfte:

- Wie viel Prozent der IT-Ressourcen werden für die Wartung veralteter Geräte aufgewendet, und wie wirkt sich dies auf die strategische Ausrichtung aus?
- Können wir mit Copilot in Windows IT-Ressourcen freisetzen und gleichzeitig eine End-to-End-Verteidigung mit der Geschwindigkeit und Skalierbarkeit der KI implementieren?
- Wie anfällig sind unsere veralteten Geräte für Cybersicherheitsbedrohungen wie Kennwortangriffe und Ransomware?
- Wie hoch sind die potenziellen finanziellen Kosten und die Kosten für den Imageschaden, die durch eine Datenschutzverletzung aufgrund veralteter Sicherheit entstehen?

3. Schwindendes Vertrauen der Mitarbeitenden und sinkende Produktivität

Mitarbeitende sind **230 % engagierter** und **85 % eher bereit**, länger als drei Jahrein ihrem Job zu bleiben, wenn sie das Gefühl haben, dass die Technologie sie bei der Arbeit unterstützt.[16]

60 % der Führungskräfte aus Technik und Management geben an, dass die Verbesserung der Mitarbeitendenerfahrung eine der wichtigsten IT-Prioritäten ist.[17]

Leistungsstarke Unternehmen befinden sich mit fast doppelt so hoher Wahrscheinlichkeit wie alle anderen Organisationen in einem Zustand fortgeschrittener Digitalisierung und haben mit **89 % höherer Wahrscheinlichkeit** die Zufriedenheit ihrer Mitarbeitenden deutlich gesteigert.[18]

Veraltete Geräte können die Produktivität und Zufriedenheit der Mitarbeitenden beeinträchtigen. Eine unzureichende Leistung und die Inkompatibilität mit neuen Tools führen oftmals zu Frustration, was sich auf die Arbeitsmoral und den Gewinn auswirkt. Und natürlich sind ältere Systeme ein leichteres Ziel für Cyberangriffe.

Könnte generative KI am Arbeitsplatz einige oder alle diese Probleme entschärfen? Ein kürzlich veröffentlichter Work Trend Index-Bericht zeigt, dass Early Adopters von Copilot beeindruckende Verbesserungen im Hinblick auf Qualität, Geschwindigkeit, Produktivität und Kreativität verzeichnen konnten, sodass ihnen mehr Zeit für die wirklich wichtigen Aufgaben blieb. Laden Sie den Bericht hier herunter.

Überlegungen für Führungskräfte:

- Können wir das Engagement und die Einbindung der Mitarbeitenden erhöhen, indem wir die Benutzererfahrung mithilfe generativer KI verbessern?
- Wie wirken sich die Leistungsprobleme älterer Geräte auf die Produktivität und Zufriedenheit der Mitarbeitenden aus?
- Sind die Mitarbeitenden in der Lage, die notwendigen neuen Tools zu nutzen, oder wird dies durch Kompatibilitätsprobleme verhindert?
- Wie wird das Vertrauen der Mitarbeitenden durch die erhöhte Gefährdung durch Cyberbedrohungen aufgrund älterer Systeme beeinflusst?

Windows 11 Pro-PCs: Schutz auf mehreren Ebenen für moderne Unternehmen

Entscheidungsträger/innen im Bereich der Sicherheit sind sich einig: Fast 90 % der Befragten sind der Meinung, dass veraltete Hardware die Anfälligkeit für Angriffe erhöht, und dass moderne Hardware für den Schutz in der Zukunft unerlässlich ist.[19] Aufbauend auf den Innovationen von Windows 10 werden mit Windows 11 Pro in Zusammenarbeit mit unseren Fertigungs- und Halbleiterpartnern zusätzliche Hardware-Sicherheitsfunktionen zur Unterstützung der modernen Arbeit und als Reaktion auf die sich entwickelnde Bedrohungslandschaft eingeführt.

Verbesserte Hardware- und Betriebssystemsicherheit

Windows 11 Pro bietet erhöhten Schutz durch hardwarebasierte Sicherheit wie z. B. TPM 2.0, das sensible Daten wie Verschlüsselungsschlüssel und Anmeldeinformationen vor unbefugtem Zugriff und Manipulation schützt. Für einen verbesserten Kernelschutz sind bei Windows 11 Pro Geräten jetzt standardmäßig Isolationstechnologien aktiviert, darunter die virtualisierungsbasierte Sicherheit (VBS) und die hypervisorgeschützte Codeintegrität (HVCI).

Robuste Kontrollen für Anwendungssicherheit und Datenschutz

Viele Unternehmen führen die Anwendungskontrolle als eines der wirksamsten Mittel zur Abwehr von Schadsoftware an, die auf ausführbaren Dateien basiert. App Control for Business[8] (ehemals Windows Defender Application Control) ist die Lösung der nächsten Generation zur App-Kontrolle für Windows und bietet der IT-Abteilung umfassende Kontrolle darüber, welche Anwendungen in Ihrer Umgebung ausgeführt werden. Kunden, die Microsoft Intune[5] zur Verwaltung ihrer Geräte nutzen, können jetzt App Control for Business in der Verwaltungskonsole konfigurieren, einschließlich der Einrichtung von Intune als verwaltetes Installationsprogramm.

Um die Sicherheit von persönlichen und geschäftlichen Daten zu gewährleisten, setzt Windows 11 Pro auf eine mehrschichtige Anwendungssicherheit. Grundsätze wie die Isolation von Anwendungen, Codeintegrität, Datenschutzkontrollen und das Prinzip der geringsten Rechte ermöglichen es Entwicklerinnen und Entwicklern, Sicherheit und Datenschutz von Anfang an zu integrieren. Mit Windows 11 Pro haben Sie außerdem eine bessere Kontrolle über Datenschutzfunktionen wie etwa den Zugriff auf Standort, Kamera und Mikrofon.

Gesicherte Identitäten

Da Cyberkriminelle es häufig auf Kennwörter abgesehen haben, bietet Windows 11 Pro zuverlässigen Schutz gegen den Diebstahl von Anmeldeinformationen. Aktivieren Sie die Multi-Faktor-Authentifizierung und den Schutz von Anmeldeinformationen mit Windows Hello for Business[7] für eine unkomplizierte, sichere und kennwortlose Anmeldung – per PIN, Gesichtserkennung oder Fingerabdruck. Microsoft Defender SmartScreen bietet proaktiven Schutz gegen den Diebstahl von Anmeldeinformationen mit integriertem verbessertem Phishing-Schutz, während die Windows-Anwesenheitserkennung mit den Funktionen „Sperren bei Verlassen" und „Reaktivieren bei Annäherung" dafür sorgt, dass Sie Ihre Geräte beruhigt verlassen können.[7]

Verbindung mit Clouddiensten

Windows Update for Business[20] ist ein kostenloser Clouddienst, der es IT-Administratoren und -Administratorinnen ermöglicht, Windows-Clientgeräte in ihrer Organisation mit aktuellen Sicherheitsfunktionen und Windows-Features auf dem neuesten Stand zu halten, indem sie diese Systeme direkt mit dem Windows Update-Dienst verbinden. Windows 11 Pro verfügt außerdem über integrierte Clients für die Geräteanmeldung und -verwaltung, mit denen Unternehmen Sicherheitsrichtlinien durchsetzen und die Vorteile moderner Geräteverwaltungstools (MDM) wie Microsoft Intune nutzen können.[5] Windows 11 Pro arbeitet mit lokalen und cloudbasierten Verwaltungslösungen zusammen.

Kombinieren Sie Windows 11 Pro mit Microsoft 365 Business Premium, und ebnen Sie damit den Weg zur Cloudverwaltung.[5] Die modernen Windows 11-PCs erfüllen die heutigen Anforderungen an Sicherheit und Flexibilität und sind in Verbindung mit Microsoft 365 Business Premium ein wichtiger Schritt hin zu einer stabileren und effizienteren Arbeitsumgebung.

Wenn Sie mehr erfahren möchten, laden Sie das Windows 11-Sicherheitsbuch herunter.

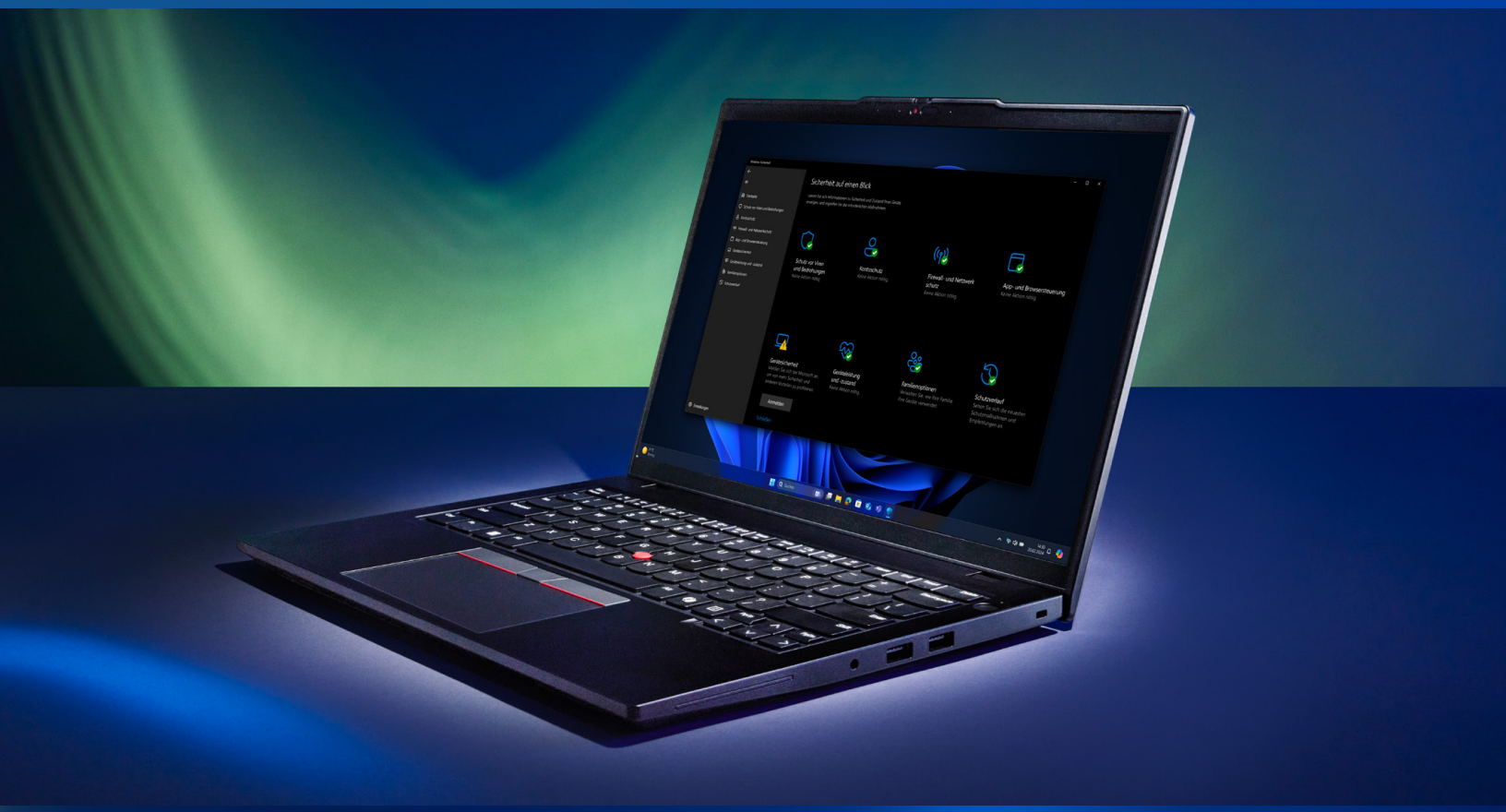
Windows 11 Pro-PCs: Die Arbeitswelt von morgen sichern

Organisationen, die in einer durch KI veränderten Arbeitslandschaft ihren Geschäftserfolg beschleunigen möchten, benötigen eine Plattform, die stabile Sicherheit, eine unkomplizierte Verwaltung und die Unterstützung verschiedener Arbeitsstile vereint. Die Bereitstellung von Windows 11 Pro-Geräten bietet eine fortschrittliche Lösung, die über die traditionelle IT-Sicherheit hinausgeht und nicht nur den Schutz, sondern auch die Produktivität, die Zusammenarbeit und die betriebliche Effizienz berücksichtigt.

Windows 11 Pro-Geräte sind mehr als nur eine Sicherheitsmaßnahme. Sie verbessern die Produktivität und die Zusammenarbeit und ermöglichen die Anpassung an einen sich schnell verändernden Arbeitsplatz.

Diese Anpassung stärkt das Vertrauen der Mitarbeitenden und gleicht einen möglichen Produktivitätsrückgang aus. Durch die Vereinfachung von Bereitstellung und Verteilung entlasten diese Geräte stark beanspruchte IT-Ressourcen, fördern Innovationen und senken die Kosten.

Windows 11 Pro-Geräte legen den Grundstein für die Zukunft. Durch die Umstellung auf cloudbasierte Abläufe und den Einsatz neuer Technologien können Unternehmen Chancen ergreifen, ihre Geschäftsdaten schützen und den entscheidenden Impuls für ihren Erfolg erlangen. Dadurch sind sie bestens gerüstet, um sich in einer sich ständig weiterentwickelnden Geschäftslandschaft zu behaupten.



Zusätzlicher Schutz, wenn Sie ihn brauchen

Windows 11 Pro-Geräte verfügen über eine Reihe von Sicherheitsfeatures, darunter eine optionale hardwarebasierte Root-of-Trust durch den **Microsoft Pluton-Sicherheitsprozessor** und integrierte Elemente wie **BitLocker, Windows Hello for Business**[7] und **TPM 2.0**.

Ein erweiterter hardwaregestützter Stapelschutz kombiniert Software- und Hardwareschutzmaßnahmen gegen Bedrohungen wie Speicherkorrumpierung und Zero-Day-Exploits. Regelmäßige Updates der Root-of-Trust-Firmware sorgen für eine gut abgeschirmte Geräteumgebung.

Organisationen, die Windows 11 Pro-Geräte bereitstellen, können ihre Angriffsfläche drastisch reduzieren, sodass sie Chancen nutzen können, ohne die Sicherheit zu gefährden. Das trägt sowohl zur Anpassungsfähigkeit als auch zum Wachstum bei.

Zentrale Vorteile von Windows 11 Pro

Unternehmen: Eine stabile Sicherheitsgrundlage

Windows 11 Pro kann dazu beitragen, Cyberbedrohungen um bis zu 58 % zu reduzieren.[1] Organisationen können ohne Bedenken Wachstumschancen nutzen, ohne die Sicherheit zu gefährden.

IT-Teams: Zwischenfälle reduzieren und Daten schützen

Vom hardwarebasierten Root-of-Trust bis hin zu integrierten Schutzfunktionen wie BitLocker und Windows Hello[7] – IT-Teams profitieren von den umfassenden Sicherheitsfeatures von Windows 11 Pro.

Mitarbeitende: Sicheres und effizientes Arbeiten

Windows 11 Pro-Geräte erhalten regelmäßige, automatische Firmware-Updates, sodass die Mitarbeitenden darauf vertrauen können, dass ihre Daten geschützt sind und sie sich auf die Produktivität konzentrieren können.

Fortschrittlicher Schutz in einer sich ständig verändernden Bedrohungslandschaft

Windows 11 Pro-Geräte verfügen über moderne CPUs und sind mit standardmäßigen Sicherheitsfeatures wie etwa TPM 2.0 für Hardware-Root-of-Trust, sicheren Start und BitLocker-Laufwerkverschlüsselung ausgestattet, um den Sicherheitsstatus zu verbessern. Bei der Integration in Sicherheitssoftware von Drittanbietern wurde Berichten zufolge eine Reduzierung der erfolgreichen Angriffe auf die Sicherheit um 20 % erzielt.[9]

> Die Wahrscheinlichkeit erfolgreicher Angriffe auf die Sicherheit von Windows 11 Pro-Geräten **sinkt Berichten zufolge um bis zu 20 %.[9]**

Die Integration von TPM 2.0 in neue und aktualisierte Geräte unterstützt Schlüsselfunktionen wie die sichere Speicherung, Verschlüsselung, Schlüsselgenerierung und Integrität des Systemstarts, die die Grundlage für Funktionen wie Windows Hello for Business[7] und die Windows Defender-Systemüberwachung bilden. Dadurch wird eine konsistente Hardware-Root-of-Trust geschaffen, sodass die Voraussetzungen für zukünftige Sicherheitsfunktionen gegeben sind.

Zentrale Vorteile von Windows 11 Pro

Unternehmen: Förderung der Geschäftstransformation

Mit umfassender Sicherheit, die vom Chip bis zur Cloud reicht, können Unternehmen neue Chancen nutzen und die Zukunft ohne Bedenken angehen. Verbesserte Leistung, mehr Sicherheit und KI-Integration ermöglichen es Organisationen, von jedem Standort aus zu operieren und sich ohne Kompromisse weiterzuentwickeln.

IT-Teams: Optimierte Verwaltung und Kompatibilität

Die Kompatibilität mit vorhandener Software und Hardware vereinfacht die Bereitstellung, während moderne Verwaltungsfunktionen es der IT-Abteilung ermöglichen, mit weniger mehr zu erreichen. Windows 11 Pro ist ein Meilenstein bei der Reduzierung von Kosten und Aufwand und ermöglicht eine nahtlose, sichere und effiziente Umgebung für den Unternehmenserfolg.

Mitarbeitende: Voraussetzungen schaffen, um überall Höchstleistungen zu erbringen

KI-gestützte Lösungen, intelligente Workflows und personalisierte Einstellungen ermöglichen es den Mitarbeitenden, nach ihren Wünschen zu arbeiten, und tragen so zu Wohlbefinden und einer höheren Produktivität bei. Windows 11 Pro bietet einen empathischen Ansatz, der über die reine Funktionalität hinausgeht und sowohl die Zufriedenheit als auch die Geschäftsergebnisse im Blick hat.

Entwickelt für Produktivität und Zusammenarbeit

Die neuen Features in Windows 11 Pro haben in Verbindung mit modernen Geräten das Potenzial, die Produktivität der Mitarbeitenden zu steigern und ihnen zu ermöglichen, schneller mehr zu erledigen. Die modernen Windows 11 Pro-Geräte wurden gezielt für das Geschäftswachstum entwickelt und verbinden überragende Leistung mit stabiler Flexibilität. Windows 11 Pro-Geräte sind sicher und direkt einsatzbereit, sobald die Mitarbeitenden sie erhalten. Sie verfügen über einen hardwarebasierten Schutz, der Berichten zufolge zu einer 3,1-fachen Reduzierung von Firmware-Angriffen führt,[1] ohne die Systemleistung oder die Produktivität der Mitarbeitenden zu beeinträchtigen.

> Die befragten Unternehmen konnten ihre Produktivität und Zusammenarbeit im Vergleich zu früheren Windows-Geräten um **50 % steigern.**[11]

Funktionen wie Snap-Layouts ermöglichen eine effiziente Desktoporganisation, fördern die Produktivität und vereinfachen das Multitasking. In Kombination mit KI-Erweiterungen für nahtlose Videokonferenzen werden diese Features durch die hochwertigen Kameras und Lautsprecher, die in die neuen Geräte integriert sind, ergänzt. Die vertraute Windows-Oberfläche sorgt für einen reibungslosen Arbeitsablauf, sodass Projekte im Durchschnitt 42 % schneller abgeschlossen werden können.[11]

Windows 11 Pro-Geräte bieten darüber hinaus Verbesserungen wie eine bis zu 61 % längere Akkulaufzeit,[11,21] reaktionsschnelle Leistung und die Möglichkeit, hochwertige Präsentationen auf mehreren 4K-Monitoren zu unterstützen. Zusätzlich zur herkömmlichen Tastatur und Maus ermöglichen verschiedene durch Peripheriegeräte unterstützte Arbeitsmodi, wie etwa Stift-, Freihand- und Toucheingabe oder Sprachsteuerung[7], eine flexible Arbeitsweise.

Zentrale Vorteile von Windows 11 Pro

Unternehmen: Entwickelt, um das Wachstum anzukurbeln

Windows 11 Pro-Geräte verringern die Anzahl erfolgreicher Firmware-Angriffe und bieten mehr Schutz vor Schadsoftware, ohne die Leistung zu beeinträchtigen.[1] Von der Unterstützung von Präsentationen auf mehreren 4K-Monitoren bis hin zur Steigerung der Produktivität passt sich Windows 11 Pro an Ihre Unternehmensziele an und ermöglicht es Ihnen, Chancen souverän zu nutzen.

IT-Teams: Unerreichte Kontrolle und Sicherheit

Windows 11 Pro-Geräte wurden speziell für eine optimierte Integration entwickelt und bieten nicht nur hardwarebasierten Schutz und reaktionsschnelle Leistung, sondern sind auch mit 99,7 % aller Anwendungen kompatibel[22] und für die Zusammenarbeit mit nahezu sämtlichen Hardwarekomponenten konzipiert, darunter Drucker, Monitore und anderes Zubehör. Mit Windows 11 Pro können sich IT-Teams auf Innovationen konzentrieren, denn sie wissen, dass die Systeme sicher, zuverlässig und einfach zu bedienen sind.

Mitarbeitende: Entwickelt, um sich an jeden Arbeitsstil anzupassen

Snap-Layouts und KI-unterstützte Videokonferenzen sorgen für einfache Zusammenarbeit und Multitasking. Und mit einer bis zu 61 % längeren Akkulaufzeit,[11,21] integrierten hochwertigen Kameras und einer reaktionsschnellen Leistung stellen Windows 11 Pro-Geräte Flexibilität und Komfort für jede Aufgabe in den Vordergrund.

Höhere Produktivität der Sicherheits- und IT-Teams

Laut einem von Microsoft in Auftrag gegebenen Forrester-Bericht[9] bieten Windows 11 Pro-Geräte eine Entlastung für stark beanspruchte IT-Ressourcen. Da die Geräte von Haus aus mit Sicherheitsfeatures wie **virtualisierungsbasierter Sicherheit** (VBS), **hypervisorgeschützter Codeintegrität** (HVCI), **Windows Hello for Business**[7] und **Trusted Boot** ausgestattet sind, müssen sich IT-Teams weniger mit Sicherheitseinstellungen befassen und können sich stattdessen stärker auf strategische Aufgaben konzentrieren.

> **Berichten zufolge ist die** Zahl der Helpdesk-Anfragen innerhalb von drei Jahren um 80 % gesunken.[9]

VBS nutzt die Hardwarevirtualisierung, um einen sicheren, vom Betriebssystem getrennten Kernel zu hosten. Das bedeutet, dass der sichere Kernel selbst dann noch geschützt ist, wenn das Betriebssystem kompromittiert wird. HVCI schützt in Verbindung mit VBS vor Angriffen, die darauf abzielen, den Code im Kernelmodus (z. B. Treiber) zu modifizieren. So wird die Integrität des Codes auf Hardwareebene gewahrt und der Schutz vor unbefugten Änderungen gewährleistet.

Dieses fortschrittliche, proaktive Sicherheitskonzept steigert die IT-Produktivität erheblich. So konnte die Produktivität des Sicherheitsteams in der von Forrester untersuchten gemischten Organisation um 20 % gesteigert werden.[9] Darüber hinaus sind die inhärenten, standardmäßig aktivierten Sicherheitsfeatures der Windows 11 Pro-Geräte mit Self-Service-Funktionen gekoppelt, was zu einer Reduzierung der eingehenden Helpdesk-Anfragen um bis zu 80 % innerhalb von drei Jahren beiträgt.[9]

Zentrale Vorteile von Windows 11 Pro

Unternehmen: Wachstum mit minimalem Overhead

Mithilfe von Sicherheitsfeatures wie der virtualisierungsbasierten Sicherheit (VBS) und der hypervisorgeschützten Codeintegrität (HVCI) können Windows 11 Pro-Geräte dazu beitragen, die Anfälligkeit gegenüber Bedrohungen zu verringern und sensible Daten zu schützen. Diese Systeme führen laut Berichten bei Sicherheits- und IT-Teams zu einer Produktivitätssteigerung von bis zu 20 %.[9]

IT-Teams: Vereinfachung der täglichen Routine

Windows 11 Pro-Geräte bieten eine automatische Aktivierung von Features, wodurch sich der Aufwand für die regelmäßige Problembehandlung verringert und mehr Zeit für proaktive Systemverbesserungen bleibt. In Verbindung mit einer Reduzierung der Helpdesk-Anfragen[9] können sich IT-Teams so auf die Implementierung neuer Technologien und Strategien konzentrieren, anstatt nur Brände zu löschen.

Mitarbeitende: Ein reibungsloserer Arbeitstag

Windows 11 Pro-Geräte bieten eine benutzerfreundliche, sichere Arbeitsumgebung, die sich an jeden Arbeitsstil anpassen lässt. Dank der integrierten fortschrittlichen Sicherheitsfeatures können sich Ihre Mitarbeitenden beruhigt auf ihre Arbeit konzentrieren, da sie wissen, dass ihre Daten und Systeme geschützt sind.

Ein gewaltiger Fortschritt bei der Bereitstellung, Verteilung und Sicherheit

Die Implementierung von Windows 11 Pro-Geräten beschleunigt nicht nur die Bereitstellung und den Bereitstellungsprozess, sondern bietet zudem stabilen Schutz für Geräte und Anwendungen, die für den heutigen Geschäftsbetrieb unerlässlich sind.

Die nahtlose Integration von Hard- und Software reduziert den Bedarf an umfangreichen Hardwareprüfungen und Kompatibilitätsbewertungen. Diese effiziente Bereitstellung erfolgt Berichten zufolge bis zu 25 % schneller.[9]

> **Eine Effizienzsteigerung von bis zu 25 %** bei der Bereitstellung von Windows 11 Pro-Geräten.[9]

Technologien wie **Microsoft Intune**,[5] **Microsoft Entra ID**[23] und **Windows Autopilot**[24] vereinfachen die Gerätebereitstellung, die Konfigurationsverwaltung sowie Softwareupdates in der gesamten Organisation und tragen dazu bei, die Kosten zu senken und die Compliance zu verbessern. Windows Autopilot steigert außerdem die Effizienz, indem es die Zero-Touch-Bereitstellung von vorkonfigurierten Geräten für remote arbeitende Mitarbeitende ermöglicht, was zu erheblichen Zeit- und Kosteneinsparungen führt.

Zentrale Vorteile von Windows 11 Pro

Unternehmen: Die Plattform für geschäftliche Innovation

Durch die Kombination von Windows 11 Pro-Geräten mit moderner Cloudverwaltung können Organisationen die Sicherheit erhöhen, die Effizienz steigern und das Arbeiten an beliebigen Standorten ermöglichen.

IT-Teams: Optimierte Geräteverwaltung

Windows 11 Pro-Geräte vereinfachen die IT-Verwaltung, indem sie zeitaufwändige Hardwareprüfungen und Kompatibilitätsbewertungen überflüssig machen. Durch die Implementierung von Windows 11 Pro-Geräten mit einer MDM-Lösung[5] können IT-Teams den Onboardingprozess beschleunigen und den Bedarf an manuellen Eingriffen reduzieren.

Mitarbeitende: Schnelles Aktivieren und Aktualisieren von Geräten

Windows 11 Pro-Geräte können regelmäßig und schnell aktualisiert werden, was zu einer schnelleren Bereitstellung und einer robusteren Anwendungssicherheit führt. Mit sofort einsatzbereiten Geräten können sich Ihre Mitarbeitenden ohne Verzögerung an die Arbeit machen.

Schutz, der Mitarbeitende befähigt und den Geschäftserfolg beschleunigt

Angesichts des immer größeren Ausmaßes und der zunehmenden Raffinesse von Cyberbedrohungen benötigen IT-Führungskräfte Lösungen, die nicht nur den Schutz, sondern auch die Produktivität erhöhen. Diese Lösungen müssen einfach zu implementieren und mit den vorhandenen Technologien der Organisation kompatibel sein. Kurz gesagt: Ein wirksamer Schutz sollte das Geschäft nicht verlangsamen, sondern es beschleunigen.

Deshalb sind Windows 11 Pro-PCs sowohl für die Sicherheit als auch für die Geschäftstransformation konzipiert. Leistungsstarker, standardmäßiger Schutz und branchenführende KI ermöglichen es den Mitarbeitenden, ihr volles Potenzial auszuschöpfen, ihrer Kreativität freien Lauf zu lassen und von praktische jedem Standort aus erfolgreich zu arbeiten. Und je weniger Zeit IT-Führungskräfte mit der Entschärfung von Bedrohungen verbringen, desto mehr Zeit haben sie für strategische Initiativen.

Wenn Technologie das Unternehmen schützt, jede Mitarbeiterin und jeden Mitarbeiter zu Höchstleistungen anspornt und IT-Teams entlastet, damit sie sich auf Wachstum und Innovation konzentrieren können, gewinnen die Unternehmen.

Beschleunigter Erfolg durch leistungsstarken, standardmäßigen Schutz:

Die Absicherung Ihrer Geschäftsdaten mit End-to-End-Sicherheitsverwaltung sorgt Berichten zufolge für eine **3,1-fache** Verringerung der Firmware-Angriffe.[1]

Der Schutz vor immer neuen Bedrohungen dank neuester Sicherheitsmechanismen sorgt Berichten zufolge für eine **2,8-fache** Verringerung der Fälle von ID-Diebstahl.[1]

Die Einführung des sichersten Windows aller Zeiten mit bereits aktivierten Sicherheitsebenen sorgt laut Berichten für einen Rückgang der Sicherheitsvorfälle um **58 %** .[1]

Die Bereitstellung einer optimierten Sicherheitslösung vom Chip bis zur Cloud steigerte die Produktivität des IT-Teams Berichten zufolge um **25 %.**[9]

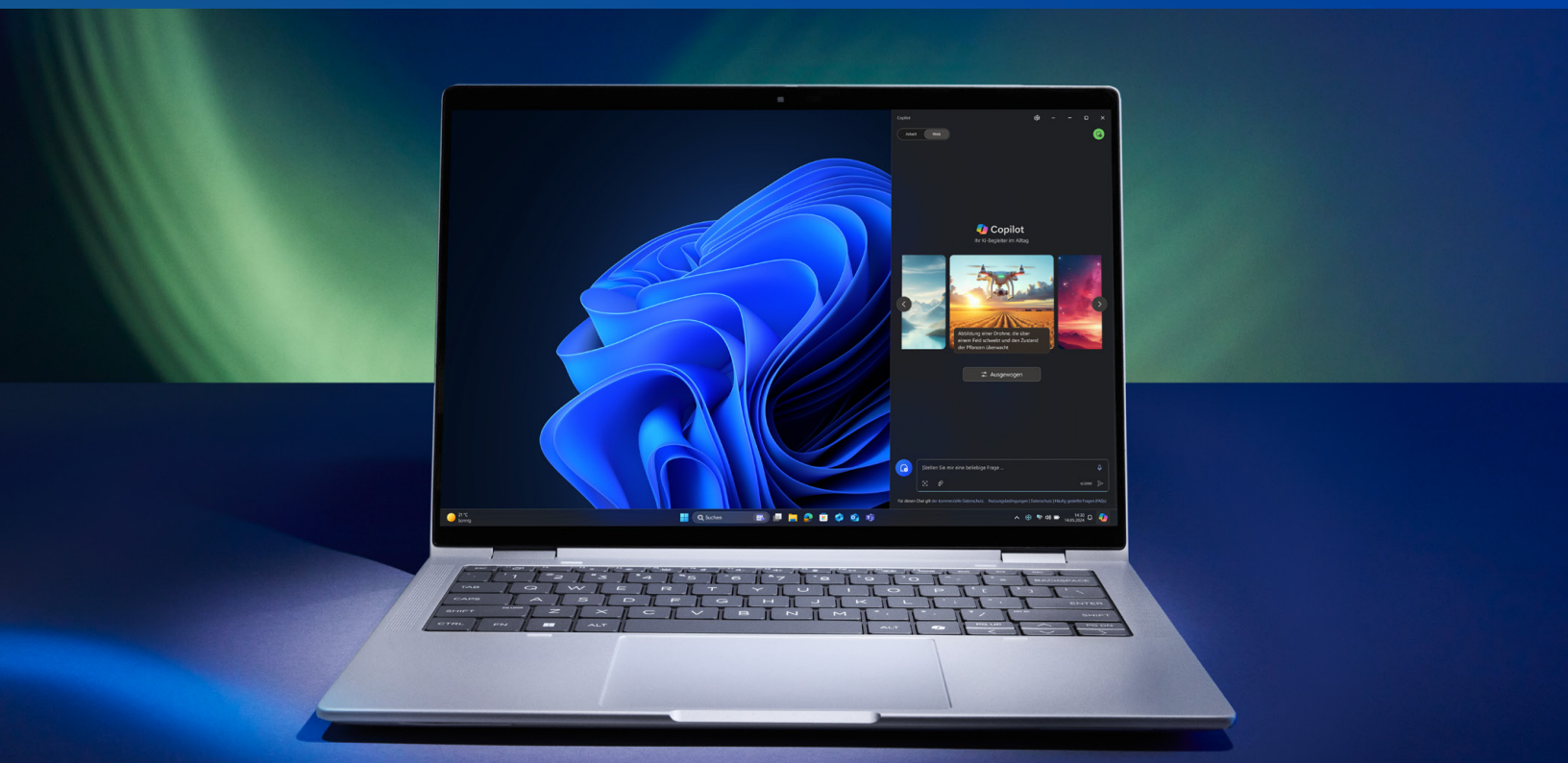
Entdecken Sie die Windows 11 Pro-Geräte

Erkunden Sie die Welt der Windows 11 Pro-Geräte, die auf jegliche geschäftliche Anforderungen zugeschnitten sind. Von innovativen 2-in-1-Geräten über schlanke, leichte Laptops bis hin zu leistungsstarken Workstations – es gibt für jede Rolle in Ihrer Organisation das passende Windows 11 Pro-Gerät. Erfahren Sie, wie Sie mit qualifizierten Geräten noch heute auf Windows 11 Pro upgraden können.

Handeln Sie bald

Veraltete Geräte erhöhen das Sicherheitsrisiko, und der Support für Windows 10 läuft am 14. Oktober 2025 aus.[25] Mit einem Upgrade auf Windows 11 Pro profitieren Sie von den neuesten Sicherheitsfeatures und gewährleisten gleichzeitig, dass Sie Unterstützung erhalten und auf dem neuesten Stand sind. Steigen Sie auf Windows 11 Pro-Geräte um, bevor der Support für Windows 10 am 14. Oktober 2025 ausläuft. Starten Sie noch heute, um die Bereitstellung zu optimieren und von den neuesten Features, einschließlich Copilot in Windows, zu profitieren.

Windows 11 Pro-Geräte anzeigen



Quellen und Danksagungen

1. SMB Windows 11 Survey Report. Techaisle, Februar 2022. Ergebnisse für Windows 11 basieren auf einem Vergleich mit Windows 10-Geräten.
2. Microsoft-Bericht über digitale Abwehr für das Jahr 2022, Microsoft.
3. Copilot in Windows (in der Vorschau) ist in ausgewählten globalen Märkten verfügbar und wird ab Sommer 2024 auf Windows 11-PCs im Europäischen Wirtschaftsraum eingeführt. Copilot mit kommerziellem Datenschutz ist ohne zusätzliche Kosten für Benutzerinnen und Benutzer mit einer Entra ID und einer aktivierten, berechtigten Microsoft 365- oder Office 365-Lizenz verfügbar.
4. Microsoft-Bericht über digitale Abwehr, Microsoft 2023.
5. Separat erhältlich.
6. Microsoft 365-Abonnement erforderlich, separat erhältlich.
7. Hardwareabhängig.
8. Endpoint Privilege Management erfordert Microsoft Entra ID und neben der Microsoft Intune Plan 1-Lizenz eine zusätzliche Lizenz. Sie haben die Wahl zwischen einer Einzelplatzlizenz, die nur EPM hinzufügt, oder einer Lizenz für EPM als Teil der Microsoft Intune Suite. Weitere Informationen finden Sie unter Verwenden der Add-On-Funktionen der Intune Suite.
9. Im Auftrag von Forrester Consulting erstellte Studie, „The Total Economic Impact™ of Windows 11 Pro Devices“, Dezember 2022. Hinweis: Die quantifizierten Vorteile spiegeln zusammengefassten Ergebnisse über einen Zeitraum von drei Jahren in einer einzigen gemischten Organisation wider, die einen Jahresumsatz von 1 Milliarde US-Dollar erwirtschaftet, über 2.000 Mitarbeitende verfügt, ihre Hardware im Vierjahresrhythmus aktualisiert und ihre gesamte Belegschaft auf Windows 11-Geräte umstellt.
10. Microsoft New Future of Work Report 2022, Microsoft.
11. Im Vergleich zu Windows 10-Geräten. Principled Technologies, „Improve your day-to-day experience with Windows 11 Pro laptops“, Februar 2023.
12. Innovation vs. risk: IT leaders share security concerns regarding tech innovation, but can they afford to let risk hold them back? HPE, September 2023.
13. Predictions 2023: Security Pros Face Greater Internal Risks, 2022, Forrester.
14. CIO, Burnout: An IT epidemic in the making, November 2023.
15. Introducing Microsoft Security Copilot: Empowering defenders at the speed of AI, Microsoft, März 2023.
16. In a Hybrid World, Your Tech Defines Employee Experience, 2022, Harvard Business Review.
17. Digital Workplace Trends To Watch Out For In 2023, 2022, Forrester.
18. 2023: Global Employee Experience Trends Report, NTT DATA, Inc.
19. 2022: Windows 11 Security Book: Powerful security from chip to cloud.
20. Windows Update for Business funktioniert mit Microsoft Entra ID (separat erhältlich).
21. Die Akkulaufzeit variiert abhängig von Einstellungen, Nutzung, Gerät und anderen Faktoren.
22. Programmdaten von App Assure.
23. Erfordert eine aktivierte, berechtigte Microsoft 365-Lizenz (separat erhältlich).
24. Erfordert Microsoft Intune und Entra ID (separat erhältlich).
25. Blogbeitrag: Plan for Windows 10 EOS with Windows 11, Windows 365, and ESU. Weitere Informationen.