



intel.

Verwaltung von Unternehmenstechnik für eine verteilte Belegschaft

Stabile, sichere, skalierbare IT-Plattformen fördern
Mitarbeiterzufriedenheit und Produktivität

IT wirkt sich auf das Mitarbeitererlebnis aus

Wir leben heute in einer Welt, in der man überall arbeiten kann.

In der Corona-Pandemie waren Unternehmen auf der ganzen Welt dazu gezwungen, sich während der Lockdowns rasch auf die Bedürfnisse von Remote-Mitarbeitern einzustellen. Die Verantwortung dafür lag bei den IT-Managern und -Entscheidungsträgern, die sich beeilten, die Mitarbeiter im Homeoffice auszustatten.

Remote-Arbeit wird uns auch nach der Pandemie erhalten bleiben. Die Arbeitnehmer ziehen es vor, Arbeit im Homeoffice und Arbeit vor Ort im Büro flexibel in einem hybriden Modell zu kombinieren, und die Arbeitgeber geben den Bedürfnissen ihrer Fachkräfte oberste Priorität.

Angesichts der Erholung der Weltwirtschaft wird nun erwartet, dass die Bemühungen zunehmen, fähige Mitarbeiter anzuwerben und zu halten. Das bedeutet, dass die Zufriedenheit der Mitarbeiter schnell zu einer wettbewerbsentscheidenden Notwendigkeit wird.

Die Mitarbeiterzufriedenheit hängt wiederum in hohem Maße von der Leistung ihrer Geräte und der unterstützenden Technik ab. Die Verfügbarkeit fortschrittlicher Technik ist zu einem wichtigen Faktor für die Zufriedenheit und Produktivität der Mitarbeiter und für den Gesamterfolg des Unternehmens geworden. Seine Zielsetzung ist klar, aber die Umsetzung kann eine Herausforderung sein.

Für die IT ergibt sich daraus die Erkenntnis, dass die technische Infrastruktur eines jeden Unternehmens sicher, leistungsstark und in der Lage sein muss, zukünftige Workloads, sowohl zentral als auch an allen Endpunkten, zu bewältigen. Es müssen also alle vernetzten Geräte über die Leistung und Funktionalität der Unternehmensklasse verfügen, die nötig ist, damit heute und auch in Zukunft moderne Software darauf laufen kann.

Durch die Zunahme von unbefugten Zugriffen und Cyberkriminalität wird es noch schwieriger, Fernverwaltung zu unterstützen. Sicherheit ist ein wichtiger Aspekt, der das gesamte Netzwerk und jeden Endpunkt betrifft, unabhängig davon, ob die Mitarbeiter im Intranet des Unternehmens, in einer Public Cloud oder am Edge arbeiten.

Leistungsstarke Technik steigert Mitarbeiterzufriedenheit

Eine aktuelle Umfrage von Forrester Consulting¹ hat ergeben, dass die Zufriedenheit und Produktivität der Mitarbeiter direkt von ihren täglichen Erfahrungen mit Technik am Arbeitsplatz abhängen. Wenn ein Unternehmen geeignete Ressourcen bereitstellt, sind seine Mitarbeiter effizient, produktiv und engagiert.

Sich auf die Mitarbeitererfahrung zu konzentrieren, ist mehr als bloß gutes Management – es ist auch gut fürs Geschäft. Forrester hat festgestellt, dass „5 Prozent mehr Mitarbeiterengagement zu 3 Prozent mehr Gewinn führen“. Nicht zufällig haben von den durch Forrester befragten Unternehmen „fast 60 Prozent [...] eine mehr als 10-prozentige Steigerung der Werte im Bereich Mitarbeitererlebnis durch die Verbesserung der Mitarbeiterzufriedenheit mittels Technik erlebt.“¹

Laut IDC „sind 72 Prozent der Unternehmens-IT-Entscheidungsträger der Meinung, dass die Geräteauswahl eine wichtige Rolle bei der Anwerbung und Bindung von Talenten spielt. Die Zufriedenheit der Mitarbeiter muss für die IT eine wesentliche Rolle spielen, aber sie darf nicht zu Lasten der Sicherheit und der Verwaltbarkeit gehen.“²

A man with short brown hair and a beard, wearing large black headphones, is looking down at a laptop screen. He is wearing a dark grey sweater. The background is a blurred office environment with windows and shelves.

60 %

„Fast 60 Prozent [...] haben eine mehr als 10-prozentige Steigerung der Werte im Bereich Mitarbeitererlebnis durch die Verbesserung der Mitarbeiterzufriedenheit mittels Technik erlebt.“¹



IT besitzt Schlüssel zur Mitarbeiterproduktivität

Die Verwaltung von Remote-Nutzern ist aber nicht einfach, ebenso wenig wie der Umgang mit ihrem Verhalten. Zu viele Nutzer machen zu viel auf einmal. Sie nutzen moderne Software, bearbeiten große Datenmengen und wechseln zwischen Dutzenden von geöffneten Browserfenstern, während sie E-Mails abrufen, auf Slack chatten, an mehreren Videokonferenzen teilnehmen oder ähnlichen parallelen Aktivitäten nachgehen.

Drei Jahre alte Laptops können diese Arbeitslast nicht bewältigen. Sie stürzen ab oder funktionieren nicht mehr richtig, was technischen Support oder einen Neustart nötig macht. Das frustriert die Mitarbeiter, beeinträchtigt die Produktivität und vergeudet wertvolle Zeit.



Einschätzung von IT und Mitarbeitern stimmt nicht überein

IT-Manager und Mitarbeiter sind sich zwar „einig, dass PCs schnell, zuverlässig und hochvernetzt sein müssen [...] aber die Mitarbeiter erleben diese Vorteile größtenteils nicht“, so Forrester.¹

Von Forrester befragte Arbeitnehmer:

- **50 %** sind der Meinung, dass ihr PC veraltet oder unzureichend ist
- **44 %** berichten, dass ihr PC regelmäßig abstürzt
- **46 %** merkten an, dass ihre Software häufig nicht richtig funktioniert und dadurch ihre Arbeit stört
- **33 %** gaben an, dass sie mit ihrem aktuellen vom Unternehmen bereitgestellten Laptop sehr zufrieden sind

Die gleiche Umfrage hat ergeben, dass 79 Prozent der IT-Entscheidungsträger ihren Mitarbeitern ermöglichen, auf ein leistungsfähigeres Gerät aufzupgraden, aber nur 49 Prozent der Mitarbeiter glauben, dass ihnen diese Möglichkeit zur Verfügung steht. Die anderen 51 Prozent sind möglicherweise unzufrieden und fühlen sich machtlos, wenn es darum geht, die Arbeitsumgebung und -mittel zu verbessern, auf die sie täglich angewiesen sind.

Wichtigste Erkenntnisse

01

Ein positives Mitarbeitererlebnis erhöht den Wettbewerbsvorteil eines Unternehmens

02

Zufriedenheit mit der Technik verbessert das Mitarbeitererlebnis

03

Nur 33 % der Arbeitnehmer sind mit den von ihren Unternehmen bereitgestellten Geräten zufrieden¹

04

Die Hälfte der Arbeitnehmer glaubt nicht, dass sie upgraden können

Hybride Belegschaft: Die nächste „neue Normalität“

Eine remote oder hybride Belegschaft wird uns erhalten bleiben, da laut einer in *Forbes* zitierten Umfrage „97 Prozent der Arbeitnehmer und Arbeitgeber ein gewisses Maß an Flexibilität zwischen Remote-Arbeit und Arbeiten im Büro bevorzugen“.³

Ebenso gehen die Verantwortlichen in den Unternehmen davon aus, dass ein Großteil der Mitarbeiter auch noch lange nach dem Ende der Pandemie zumindest einige Tage pro Woche remote arbeiten wird. Die „neue Normalität“ wird ein hybrider Arbeitsansatz sein, bei dem die Mitarbeiter einige Tage vor Ort im Büro und einige Tage remote arbeiten, glauben 82 Prozent der von Gartner im Jahr 2020 befragten Führungskräfte.⁴

Das Pandemie-getriebene globale Experiment der Remote-Arbeit hat einige positive Ergebnisse gezeigt. Unternehmen, die schnell geeignete Technik und Geräte anschafften und einsetzten, konnten feststellen, dass ihre Mitarbeiter größtenteils produktiv blieben. Viele Arbeitnehmer fanden sogar, dass sie im Homeoffice zufriedener mit ihrer Arbeit sind.

Hybrides Arbeiten kann zu Spannungen innerhalb der Belegschaft führen, da einige Mitarbeiter im Büro miteinander interagieren, während andere dies nicht tun. Die Führungskräfte eines Unternehmens müssen klare Informationswege schaffen und aufrechterhalten, um ein faires und verantwortungsvolles Miteinander zu gewährleisten.

Das IT-Personal ist dafür verantwortlich, eine Infrastruktur einzurichten, die die Mitarbeiter und das Management in einem solchen dynamischen, flexiblen Arbeitsumfeld unterstützen und miteinander verbinden.



Wichtigste Erkenntnisse

01

Unternehmen führen ein hybrides Modell aus Remote- und Vor-Ort-Arbeit ein

02

Hybride Arbeitsmodelle können den Stress der Beschäftigten steigern

03

IT-Mitarbeiter und Technik müssen die Produktivität und Interaktivität hybrider Arbeitskräfte unterstützen

Verwaltung einer remoten Nutzerbasis

Die IT wird weiterhin mit den Problemen konfrontiert sein, die mit einer verteilten Belegschaft einhergehen. Die IT-Mitarbeiter sind dafür verantwortlich, Hunderte oder Tausende von Client-Geräten zu verwalten und zu unterstützen, während sich die Mitarbeiter außerhalb ihres Arbeitsplatzes befinden, in der Cloud oder am Edge arbeiten, mit oder ohne das Intranet des Unternehmens und den Schutz durch dessen Firewall.

Diese neue Normalität bietet wenige Möglichkeiten, praktische Unterstützung zu leisten oder sogar Dienste über VPN anzubieten. Alles, von routinemäßigen Updates und dem Zurücksetzen von Passwörtern bis hin zur Behebung von Sicherheitsverletzungen und Notfällen, muss per Fernverwaltung erledigt werden.



97 %

97 Prozent der Arbeitnehmer und Arbeitgeber bevorzugen ein gewisses Maß an Flexibilität zwischen Remote-Arbeit und Arbeiten im Büro.⁵

Intel vPro® Plattform unterstützt Fernverwaltbarkeit

Lange bevor die Pandemie die Aufmerksamkeit der Welt auf die Fernverwaltbarkeit gelenkt hat, hatten die vorausschauenden Ingenieure von Intel bereits eine Lösung entwickelt: die Intel vPro® Plattform.

Die Intel vPro® Plattform unterstützt die IT, da sie:

- **die Kosten durch Ferndiagnose und Fernwiederherstellung senkt**
- **der IT die Möglichkeit bietet, infizierte Geräte zu isolieren und ihre Datenträger zu löschen**
- **die Remote-Patch-Verwaltung innerhalb und außerhalb der Firewall optimiert**
- **umfangreiche Implementierungen vereinfacht**

Ein auf der Intel vPro® Plattform basierender Laptop oder Desktop-PC bietet effiziente, hardwarebasierte Sicherheitsfunktionen und Stabilität von Firmengeräten. Auf der Intel vPro® Plattform basierende Geräte sind mit einer Auswahl an Intel® Core™ vPro® Prozessoren in verschiedenen Formfaktoren erhältlich. Die Intel vPro® Plattform bietet der IT verschiedene Optionen, um ihre anspruchsvollsten Benutzer zufriedenzustellen und gleichzeitig ein Höchstmaß an Verwaltbarkeit für alle Firmengeräte zu gewährleisten.

Der IT wird empfohlen, für zusätzliche Kontrolle die Intel® Active-Management-Technik (Intel® AMT) zu aktivieren. Intel® AMT interagiert mit allen Endpunkten über die Hardwareebene unterhalb des Betriebssystems. Intel® AMT ist ausschließlich auf der Intel vPro® Plattform verfügbar und ermöglicht es IT-Fachleuten, Support für Remote-Geräte zu leisten, selbst wenn diese nicht reagieren, ausgeschaltet oder mit Malware infiziert sind.

Was beinhaltet die Intel vPro® Plattform?

Die Intel vPro® Plattform vereint eine Reihe transformativer Technologien, die auf anspruchsvolle Business-Workloads abgestimmt und gründlich getestet wurden. Die IT kann sich darauf verlassen, dass jedes auf der Intel vPro® Plattform basierende Gerät auf Produktivität, Sicherheit, Verwaltbarkeit und Zuverlässigkeit ausgelegt ist.



Erstklassige Leistung

mit der Intel vPro® Plattform, zu der ein Intel® Core™ vPro® Prozessor oder ein Intel® Xeon® Prozessor sowie **Intel® Optane™ Speicher H10** mit Solid-State-Speicher und anderen fortschrittlichen Komponenten gehört



Fernverwaltung

innerhalb oder außerhalb der Firewall mit der **Intel® Active-Management-Technik und dem Intel® Endpoint Management Assistant**



Schnelle, zuverlässige Konnektivität

mit integriertem Intel® Wi-Fi 6 und Thunderbolt™ 4 Technik



Hardwarebasierte Sicherheit

mit **Intel® Hardware Shield** für integrierten Schutz vor unbefugtem Eindringen und Cyberangriffen



Stabilität, Kompatibilität

und langfristige Zuverlässigkeit in einer integrierten, validierten Plattform



Verfügbar in vielen Gerätetypen

einschließlich Desktop-PCs, Laptops, 2-in-1-Geräten und Workstations, von einer Vielzahl an Anbietern weltweit

Wichtigste Erkenntnisse

01

Technischer Support muss remote möglich sein, auch wenn Geräte ausgeschaltet oder nicht mit dem Intranet des Unternehmens verbunden sind

02

Die Intel vPro® Plattform bietet Leistung, Sicherheit, Verwaltbarkeit und Stabilität der Unternehmensklasse

03

Weltweit bauen verschiedenste Anbieter eine Vielzahl von Geräten, die auf der Intel vPro® Plattform basieren

Remote-Arbeit und Sicherheitsrisiken

Remote-Arbeit stellt besondere Risiken für die Sicherheit der Nutzer und Daten eines Unternehmens dar. Ein Bericht von Deloitte⁵ hat festgestellt, dass „47 Prozent der Leute, die im Homeoffice arbeiten, auf einen Phishing-Betrug hereinfallen“. Dadurch sind ihre Unternehmen und deren Netzwerke der Gefahr von unbefugtem Eindringen ausgesetzt. Solche Datenschutzverletzungen kosten laut diesem Bericht durchschnittlich 137.000 US-Dollar pro Vorfall.⁵

Die Arbeit im Homeoffice erhöht auch andere Risiken. Die Mitarbeiter neigen zu menschlichen Fehlern und sind häufiger Ablenkungen ausgesetzt. Möglicherweise verwenden mehrere Familienmitglieder dasselbe Gerät. Zudem könnten ihr privates WLAN oder ihre persönlichen Geräte nicht die Sicherheitsanforderungen des Unternehmens erfüllen.

Laut einem Forschungsbericht von Gartner⁶ „stehen CIOs unter anhaltendem Druck, die Infrastruktur zu skalieren, um die Verlagerung komplexer Workloads in die Cloud und die Anforderungen einer hybriden Belegschaft zu unterstützen“. Dieser Trend dürfte die jährlichen Ausgaben für Cloud-Services bis 2021 um weitere 23 Prozent auf 332 Milliarden US-Dollar weltweit ansteigen lassen, so der Bericht.⁶

Aufgrund der zunehmenden Akzeptanz von remoten und hybriden Arbeitsmodellen muss die IT die Sicherheitsmaßnahmen im gesamten Netzwerk und an allen Endpunkten verstärken.

Softwarebasierte Sicherheitsmaßnahmen, einschließlich Antiviren-Programmen, bieten jedoch keinen ausreichenden Schutz gegen die Cyberkriminellen von heute. Einige der neuesten Ransomware-Angreifer und Hacker haben damit begonnen, Malware direkt in die UEFI/BIOS-Firmware des Geräts einzuschleusen, wo sie von Antiviren-Software häufig nicht erkannt wird.

Unternehmensweite Sicherheit auf der Intel vPro® Plattform

Die hardwarebasierten Sicherheitsfunktionen der Intel vPro® Plattform ermöglichen Profiling und Erkennung von Ransomware sowie anderen Bedrohungen auf BIOS-Ebene, die die Datensicherheit gefährden und die CPU-Leistung verringern können. Die Intel vPro® Plattform schützt alle Geräte eines Unternehmens mit einem mehrstufigen Ansatz. Dazu gehören:

- **Schutz vor Angriffen auf das BIOS auf Firmware-Ebene**
- **Bedrohungserkennung, die Hardwaretelemetrie und Beschleunigungsfunktionen nutzt, um Angriffe und ungewöhnliche Aktivitäten in Echtzeit zu identifizieren**
- **Unterstützung der Endpunktverwaltung, damit IT-Mitarbeiter Geräte remote überwachen, wiederherstellen und patchen können, alle Geräte geschützt sind und die Geräte erreicht werden, die nicht physisch zugänglich sind**

Intel engagiert sich laufend und konsequent für Sicherheit, mit innovativen Lösungen und Support, um Ihr Unternehmen heute und auch in Zukunft zu schützen.



Wichtigste Erkenntnisse

01

Verbesserte Sicherheit ist für eine mobile oder hybride Belegschaft dringend nötig

02

Virenerkennungssoftware bietet keinen ausreichenden Schutz gegen die Cyberkriminalität von heute

03

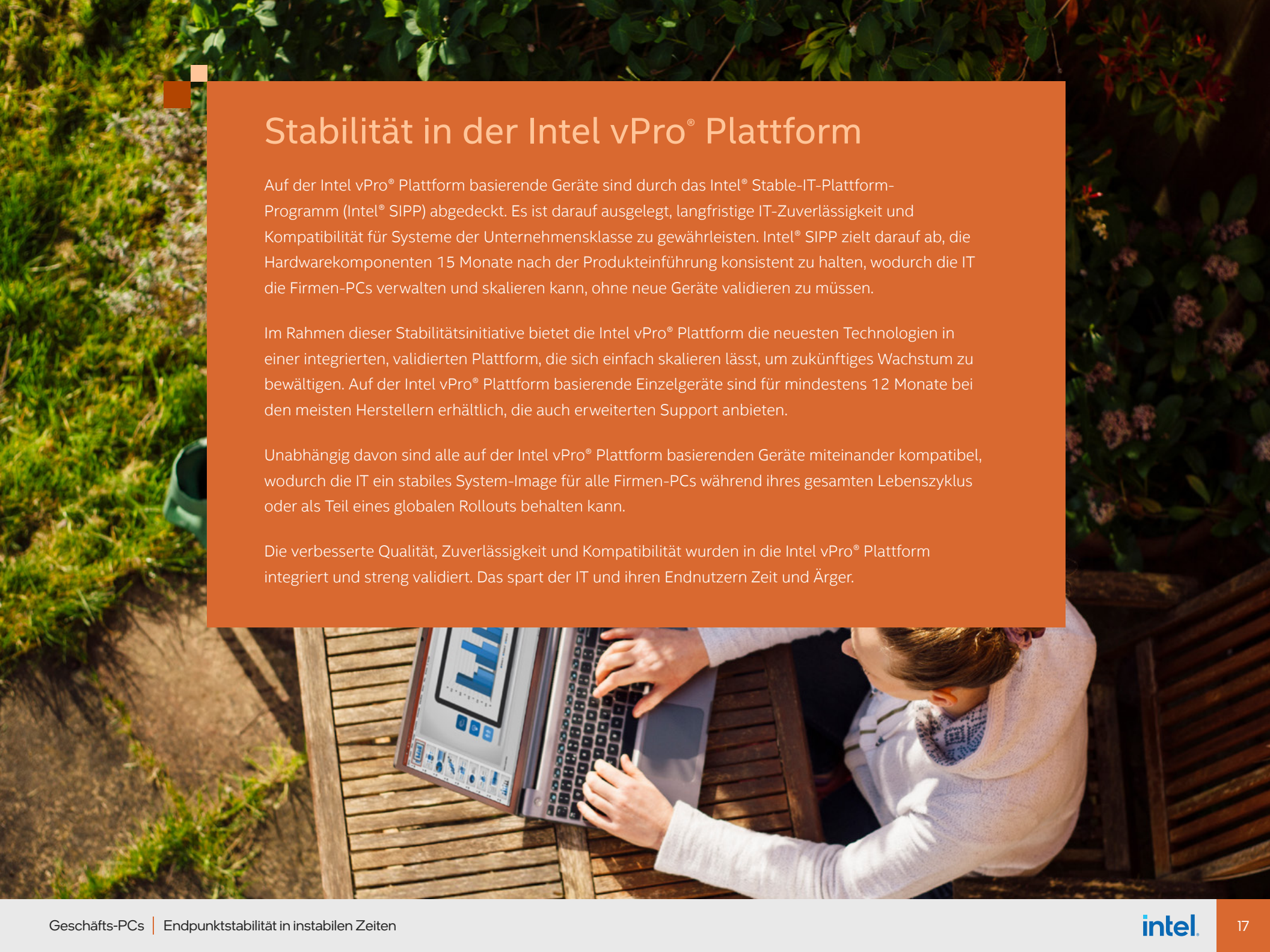
Die Intel vPro® Plattform umfasst hardwarebasierte Sicherheit und Bedrohungserkennung, die Netzwerke und alle Endpunkte schützen

Endpunktstabilität in instabilen Zeiten

Das Management sämtlicher Firmen-PCs ist schon durch den bloßen Umfang der Software-Updates und die Inkompatibilität von Treibern schwieriger geworden. Ein System-Image zu validieren und zu testen kann Wochen oder Monate in Anspruch nehmen. In der Zwischenzeit könnten neue Software- oder Treiber-Updates den Rollout des Images noch weiter verzögern oder eine zusätzliche Implementierung erforderlich machen, die noch mehr Tests und größere Unterbrechungen nach sich ziehen würde.

Durch die Umstellung auf remote oder hybride Arbeit entfällt zudem die Verwaltung vor Ort. Es können außerdem persönliche Geräte genutzt werden, die ursprünglich nicht im Plan enthalten waren. Das gestaltet den Updateprozess noch komplizierter.





Stabilität in der Intel vPro® Plattform

Auf der Intel vPro® Plattform basierende Geräte sind durch das Intel® Stable-IT-Plattform-Programm (Intel® SIPP) abgedeckt. Es ist darauf ausgelegt, langfristige IT-Zuverlässigkeit und Kompatibilität für Systeme der Unternehmensklasse zu gewährleisten. Intel® SIPP zielt darauf ab, die Hardwarekomponenten 15 Monate nach der Produkteinführung konsistent zu halten, wodurch die IT die Firmen-PCs verwalten und skalieren kann, ohne neue Geräte validieren zu müssen.

Im Rahmen dieser Stabilitätsinitiative bietet die Intel vPro® Plattform die neuesten Technologien in einer integrierten, validierten Plattform, die sich einfach skalieren lässt, um zukünftiges Wachstum zu bewältigen. Auf der Intel vPro® Plattform basierende Einzelgeräte sind für mindestens 12 Monate bei den meisten Herstellern erhältlich, die auch erweiterten Support anbieten.

Unabhängig davon sind alle auf der Intel vPro® Plattform basierenden Geräte miteinander kompatibel, wodurch die IT ein stabiles System-Image für alle Firmen-PCs während ihres gesamten Lebenszyklus oder als Teil eines globalen Rollouts behalten kann.

Die verbesserte Qualität, Zuverlässigkeit und Kompatibilität wurden in die Intel vPro® Plattform integriert und streng validiert. Das spart der IT und ihren Endnutzern Zeit und Ärger.

Wichtigste Erkenntnisse

01

Die Wartung von Firmengeräten ist bei einer remoten Belegschaft komplizierter

02

Häufige Updates von Software und Treibern können den Rollout von System-Images stören oder verzögern

03

Intel® SIPP minimiert Updates und ermöglicht es der IT, den PC-Lebenszyklus zu kontrollieren und ein stabiles System-Image zu behalten

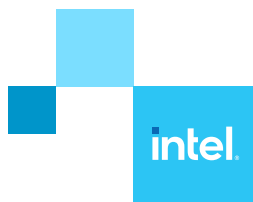
Bewältigung einer hybriden Zukunft

In diesen schwierigen Zeiten haben IT-Verantwortliche mit großem Einsatz Unternehmen am Laufen gehalten und es einer verteilten Belegschaft ermöglicht, erwerbstätig und produktiv zu bleiben. Angesichts der Erholung der Weltwirtschaft bietet sich Unternehmen erneut die Möglichkeit, strategische Lösungen für ein neues hybrides Umfeld zu entwickeln.

Die IT muss die Auswahl der Geräte und Technologien sorgfältig planen und durchführen, da diese die Anforderungen ihres Unternehmens und ihrer Nutzer jetzt und in Zukunft erfüllen müssen. Die Mitarbeiterzufriedenheit hat in der Geschäftswelt einen hohen Stellenwert, und Technik hat einen großen Einfluss auf das Mitarbeitererlebnis. Die IT muss sich darauf konzentrieren, das Nutzererlebnis zu verbessern und gleichzeitig die Herausforderungen in Bezug auf Verwaltbarkeit und Sicherheit zu bewältigen, die sich aus einer mobilen und hybriden Belegschaft ergeben.

IT-Verantwortliche vertrauen darauf, dass die Intel vPro® Plattform die Ziele ihres Unternehmens unterstützt. Diese umfassende, einsatzbereite Plattform unterstreicht, wie sehr sich Intel für die Verwaltungs-, Sicherheits- und Zuverlässigkeitsfunktionen engagiert, die sich in der Praxis bewährt haben – vor, während und nach der Pandemie.

So wie sich der Arbeitsplatz weiterentwickelt, wird sich auch die Intel vPro® Plattform weiterentwickeln und innovative Technologien in einer stabilen, kompatiblen Plattform vereinen, die Unternehmen, ihrer IT und ihren Endnutzern ein optimales Arbeitsumfeld bietet.



Sorgen Sie mit Technik der Unternehmensklasse für mehr Produktivität



Erfahren Sie mehr über die Intel vPro® Plattform

intel.de/vPro

Leistung. Sicherheit. Verwaltbarkeit. Stabilität.

Quellen

1. Forrester, „Invest in Employee Experience (EX), Drive Your Bottom Line Growth“, Oktober 2020. <https://www.intel.com/content/dam/www/public/us/en/documents/white-papers/lenovo-ex-whitepaper.pdf>
2. IDC, „The Importance of the PC in a Data-Centric World“, April 2020. (Von Intel beauftragte Studie). https://plan.seek.intel.com/vProIDC_WhitepaperLPCD.
3. *Forbes*, „5 Statistics Employers Need To Know About The Remote Workforce“, 10. Februar 2021. <https://www.forbes.com/sites/ashiraprossack1/2021/02/10/5-statistics-employers-need-to-know-about-the-remote-workforce/>
4. *Forbes*, „Four Hidden Traps of Managing A Hybrid Workforce“, 12. Mai 2021. <https://www.forbes.com/sites/forbescommunicationscouncil/2021/05/12/four-hidden-traps-of-managing-a-hybrid-workforce/>
5. Deloitte, „Impact of COVID-19 on Cybersecurity“, 2020. <https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html>
6. Gartner, „Gartner Forecasts Worldwide Public Cloud End-User Spending to Grow 23% in 2021“, 21. April 2021. <https://www.gartner.com/en/newsroom/press-releases/2021-04-21-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-grow-23-percent-in-2021>

Hinweise und Disclaimer

Intel® Technik kann entsprechend geeignete Hardware, Software oder die Aktivierung von Diensten erfordern.

Kein Produkt und keine Komponente bietet absolute Sicherheit.

Kosten und Ergebnisse können variieren.

© Intel Corporation. Intel, das Intel Logo und andere Intel Markenbezeichnungen sind Marken der Intel Corporation oder ihrer Tochtergesellschaften.

*Andere Marken oder Produktnamen sind Eigentum der jeweiligen Inhaber.

US/07/2021/PDF/JH/CMD