SOLUTION BRIEF

VERLIEBEN SIE SICH WIEDER IN WINDOWS

Indem Sie es dort betreiben, wo es hingehört: im Rechenzentrum oder in der Cloud

Wenn es um das Thema Endpoint Computing geht, ist Windows längst nicht mehr die einzige Option. Von x86-Betriebssystemen wie MacOS, Chrome OS und Linux bis hin zu vollwertigen mobilen Betriebssystemen wie iOS und Android gibt es heute mehr Möglichkeiten den je für den Zugriff auf Unternehmensanwendungen.

Windows-Desktops werden dennoch bleiben.

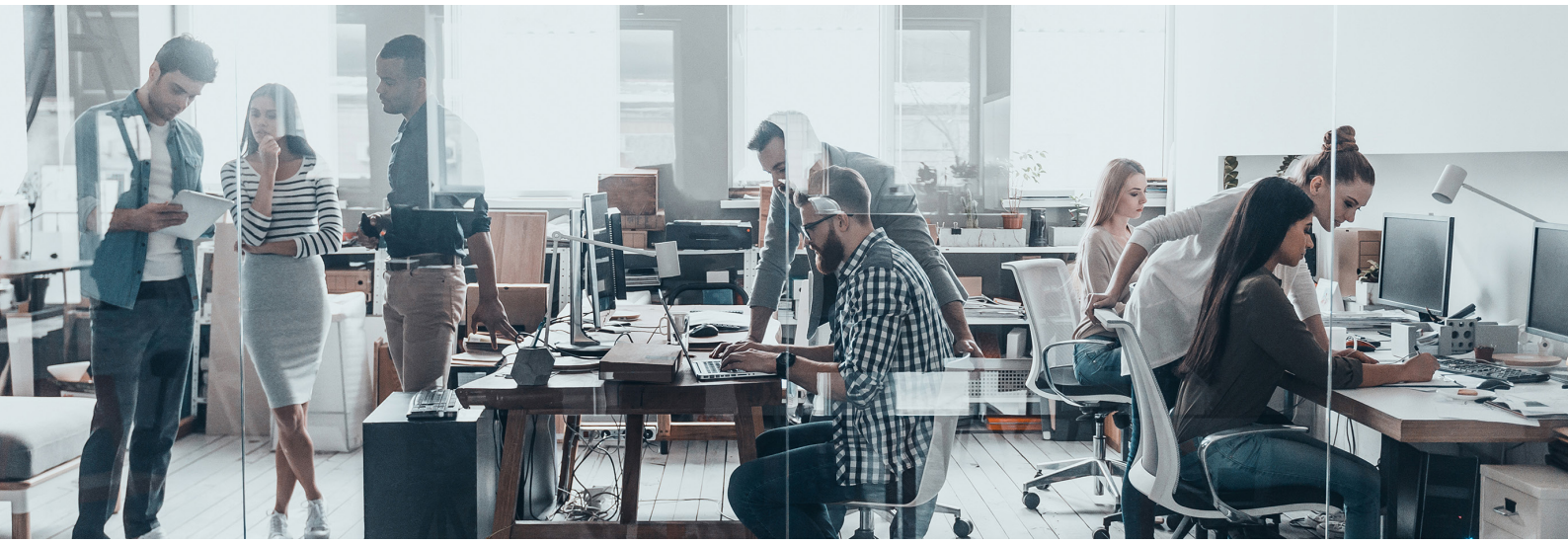
Im April 2019 hielt Windows noch einen Marktanteil von 87 Prozent bei Desktop-Rechnern und Laptops. Und dies liegt nicht nur an der großen Anzahl von älteren Windows-Geräten. Windows 10, die aktuelle Version des Betriebssystems, hat Windows 7 im Dezember 2018 als beliebtestes Betriebssystem der Welt abgelöst.

Aber nicht alles ist perfekt in der Welt der Windows-Desktops. Die breitere Nutzung von Nicht-Windows-Betriebssystemen führt IT-Administratoren immer wieder vor Augen, wie viel Aufwand sie sich im Alltag sparen könnten. Vor allem die Verwaltung und Absicherung der Desktops ließe sich ohne Windows enorm vereinfachen. Man müsste dazu gar nicht komplett auf Windows verzichten, sondern dürfte es nur nicht mehr lokal auf den Endgeräten installieren. Aber das wird von vielen heute noch als unpraktisch empfunden.

Windows ist tief in die Prozesse vieler Unternehmen eingebettet. Zahlreiche spezialisierte Geschäftsanwendungen setzen Windows voraus. Und auch wenn der Support für Microsoft Office auf Nicht-Windows-Betriebssystemen besser geworden ist, sehen viele die Office-Anwendungssuite unter Windows immer noch als überlegen an und setzen sie weiterhin ein.

Zum Glück gibt es eine Möglichkeit, die vielen Vorteile von Windows-Desktops zu nutzen und gleichzeitig die Management- und Sicherheitsprobleme am Endpoint zu beseitigen.

Die Lösung ist, Windows dort zu betreiben, wo es hingehört: ***im Rechenzentrum*** oder alternativ ***in der Cloud***.



Quelle: NetApplications Report, May 2019.

Herausforderungen bei der Verwaltung von Windows-Endpoints

Die Breite der unterstützten Optionen und die hochentwickelten Funktionen machen Windows so nützlich als universelles Betriebssystem für eine Vielzahl von IT-Anwendungen in Unternehmen. Aber dieselben Eigenschaften sind auch der Grund, warum es so schwierig ist, Windows zu aktualisieren und zu warten. Es wird für Microsoft immer aufwändiger, Updates zu erstellen, zu testen und zu verteilen – gleichzeitig stehen IT-Teams vor der Herausforderung, diese Updates zuverlässig und zeitnah auf allen Geräten einzuspielen. Windows 95 erforderte bei seiner Einführung im Jahr 1995 4 MB RAM und 120 MB freien Festplattenspeicher Windows 10 setzt mit 4 GB RAM das 1.000-Fache an Arbeitsspeicher voraus und benötigt mit 16 GB 130-mal mehr Festplattenspeicher. Mit jedem weiteren Update von Windows 10 steigen die Mindestanforderungen an das System weiter an.

Benutzer verlieren Daten durch das Update auf Windows 10

Bei beiden halbjährlichen Feature-Updates von Microsoft für Windows 10 im Jahr 2018 traten erhebliche Probleme auf. Letztlich war Microsoft gezwungen, das Update vom Oktober 2018 zurückzuziehen, nachdem einige Benutzer berichtet hatten, dass Dateien in ihrem Verzeichnis C:/Benutzer/[Username]/Dokumente/ durch das Update gelöscht wurden. Benutzer stießen nach dem Update auch auf Intel-Treiberprobleme und merkwürdige Effekte wie falsche CPU-Auslastungswerte im Task-Manager.

Große Windows-Versions-Upgrades sind besonders für Unternehmen mit vielen Endpoints ernüchternd. Migrationen werden oft zu mehrjährigen Projekten, die erhebliche Ressourcen verbrauchen und gleichzeitig nur einen geringen Wert über die Aufrechterhaltung des Microsoft-Supports hinaus liefern. Microsoft versucht, diese großen Auswirkungen auf die IT-Produktivität zu reduzieren, und hat Windows 10 als "die letzte Version von Windows" bezeichnet. Mittlerweile geht das Unternehmen zu einem interativeren Entwicklungsansatz über. Aber das vergrößert letztlich nur die Welle an Updates, die Unternehmen jeden Monat von Microsoft erhalten.

In Zukunft wird Microsoft neben dem monatlichen "Patch Tuesday" für Sicherheits- und Stabilitäts-Updates, an den sich IT-Teams bereits gewöhnt haben, zwei "Feature-Updates" für Windows 10 pro Jahr veröffentlichen. Durch die zunehmende Dichte an Updates wird der ohnehin schon überfrachtete, zeitaufwändige und arbeitsintensive Aktualisierungsprozess noch komplizierter.

Unabhängig davon, ob die Updates häufig oder selten erfolgen: Die Aktualisierung eines so großen und komplexen Betriebssystems wie Windows ist immer auch anfällig für Fehler und Qualitätsprobleme. In einigen Fällen stammen diese Fehler von Microsoft selbst – in anderen Fällen schlagen Upgrades fehl, weil das IT-Team mit Problemen in der lokalen Infrastruktur kämpft.

Microsoft verdient zwar Anerkennung dafür, dass es den Aktualisierungsprozess mit Windows 10 überdacht hat, aber der neue Prozess ist alles andere als unproblematisch und blockiert nach wie vor viele Ressourcen in Desktop-IT-Teams.

Herausforderungen bei der Sicherheit von Windows

Ein wesentlicher Nebeneffekt des schwierigen Windows-Endpoint-Managements sind anhaltende Sicherheitsrisiken. Viele erfolgreiche Angriffe nutzen bekannte Software-Schwachstellen aus. Die CVE-Datenbank (Common Vulnerabilities and Exposures) der Security-Branche listet 255 verschiedene Windows 10-Schwachstellen auf, die allein im Jahr 2018 entdeckt wurden. Selbst Unternehmen, die sehr erfahren darin sind, Windows-Patches auf ihren Endgeräten einzuspielen, befinden sich schnell in einem nahezu konstanten Zustand der Unsicherheit.

Die meisten Unternehmen versuchen, dieses Risiko durch den Einsatz von Endpoint-Sicherheitsprodukten zu minimieren. Diese Produkte bieten zwar zusätzlichen Schutz, vergrößern aber auch die Komplexität am Endpoint und erhöhen den Verwaltungsaufwand für Desktop-IT-Teams zusätzlich.

Konflikte zwischen Windows Update- und Endpoint-Sicherheitsprodukten führen zu Bootfehlern

Nach der Installation der Microsoft-Updates vom "Patch Tuesday" im April 2019 stellten viele Anwender beliebter Endpoint-Sicherheitsprodukte fest, dass sie ihre Windows-Rechner nicht mehr starten konnten. Sicherheitsanbieter bemühten sich, Workarounds zu kommunizieren, und Microsoft handelte schnell, um zu verhindern, dass Updates auf Systemen mit Konflikten durchgeführt werden. Aber dieses Beispiel zeigt perfekt, welche Probleme bei der Verwaltung eines komplexen Endpoint-Betriebssystems mit Sicherheitsprodukten von Drittanbietern auftreten können. Letztlich ist es ganz einfach: Je mehr Software auf ein Endgerät geladen wird, desto größer ist die Wahrscheinlichkeit, dass etwas schief geht – entweder innerhalb einer einzelnen Softwarekomponente oder beim Zusammenspiel von zwei oder mehr Komponenten. Ganz zu schweigen von der höheren Leistungsbelastung für die CPU dieses Geräts, wenn immer mehr Prozesse (Antivirus, etc) auf dem Endpoint ausgeführt werden.

Unglaublich schnell wachsende Hardware-Anforderungen

Die Verwaltung von Windows-Endgeräten ist aber nicht nur mit operativer Ineffizienz und Sicherheitsrisiken verbunden – Unternehmen müssen sich auch auf steigende Hardwarekosten einstellen, wenn Sie Windows auf Endpoints ausführen. Seit es Windows gibt, werden immer mehr Systemressourcen benötigt, um Anwendern eine akzeptable User Experience am Endpoint zu bieten. Die Art und Weise, wie typische Benutzer ihren Computer verwenden, hat sich in den letzten Jahren kaum verändert. Dennoch müssen Unternehmen laufend in leistungsfähigere Hardware investieren, um die steigenden Anforderungen von Windows zu erfüllen.

Dieser Ressourcenwettlauf ist nicht mehr nur auf neue Betriebssystem-Releases beschränkt. Im April 2019 warnte Microsoft seine Kunden, dass sie bis zu doppelt so viel freien Speicherplatz wie bisher benötigen würden, um ein Major Update zu installieren. Diese ungeplanten Hardwareanforderungen zwingen Desktop-Teams, zwischen dem Kauf neuer Hardware oder neuen Sicherheitsrisiken und Funktionskompromissen wählen zu müssen.

Windows im Rechenzentrum: Das Beste aus beiden Welten

Die oben beschriebenen Herausforderungen mögen wie Argumente gegen die weitere Nutzung von Windows erscheinen – das trifft aber nicht zu. Es spricht allerdings einiges dagegen, Windows weiterhin auf Endpoints einzusetzen, zu verwalten und abzusichern. Seit Jahren betreiben Unternehmen erfolgreich Windows-Desktops und -Anwendungen in ihren Rechenzentren und nutzen dafür Virtual Desktop Infrastructure (VDI)- und Remote Desktop Session Host (RDSH)-Technologien von Anbietern wie Citrix und VMware. Durch Desktop-as-a-Service (DaaS)-Angebote von Amazon Web Services und Microsoft ist es in jüngster Zeit sogar noch einfacher geworden, Windows-Desktops zentral bereitzustellen und zu verwalten.

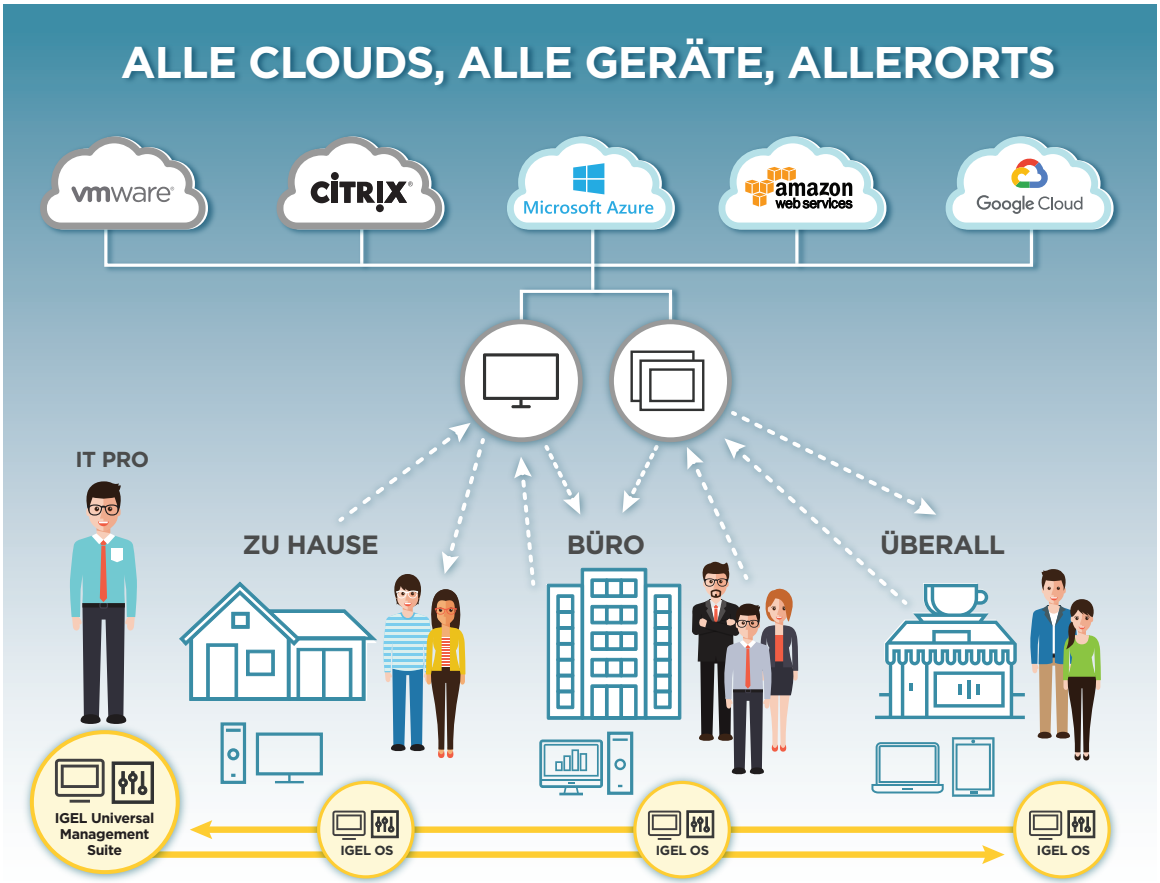
In der Vergangenheit wurde die zentralisierte Desktop-Bereitstellung oft als Nischenlösung angesehen, während die Mehrheit der Benutzer weiterhin lokale Instanzen von Windows auf ihren Endpoints nutzte. Es ist an der Zeit, diese Rollen umzukehren, und zwar aus mehreren Gründen.

Das zentrale Management von Windows mit VDI oder RDSH verbessert die Verwaltbarkeit und Sicherheit erheblich. Virtualisierungsplattformen bieten hervorragende Möglichkeiten, Benutzereinstellungen und Daten vom zugrunde liegenden Betriebssystem zu trennen. Gleichzeitig unterstützen sie erweiterte Funktionen wie nicht persistente Desktops, verknüpfte Klone, Snapshots und Rollback, die sich nur schwer auf Endpoints mit Windows abbilden lassen. Der zentrale Betrieb von Windows auf Servern in einer kontrollierten Umgebung eliminiert viele der hardware- und umgebungsspezifischen Faktoren, die das Patching von Endpoints so kompliziert machen. Zudem verfügen Rechenzentren in der Regel über etablierte Prozesse für die Sicherung von Daten und die Redundanz von Rechenressourcen.

Windows in der Cloud über DaaS geht noch einen Schritt weiter. Unternehmen müssen sich damit auch nicht mehr um das Management des Rechenzentrums und der Virtualisierungsplattform kümmern. Cloud-basierte Software-Angebote wie Office 365 verzeichnen derzeit ein unglaubliches Wachstum. Laut Gartner nutzten im Januar 2019 bereits 91% der Unternehmen Office 365 oder planten, dies zu tun. Das deutet darauf hin, dass es auch im Bereich Windows-Desktops eine ähnliche Entwicklung in Richtung Cloud geben wird. DaaS wäre dann der nächste logische Schritt.

Durch die Verlagerung von Windows in das Rechenzentrum oder in die Cloud können IT-Teams:

- Windows-Arbeitsplätze für Benutzer viel performanter und zuverlässiger bereitstellen,
- die IT-Effizienz erheblich verbessern - durch die Vereinfachung des Windows-Update- und Patches-Prozesses,
- die Sicherheit erhöhen, da Windows-Endpoints nicht mehr remote gepatcht und mit komplexen und kostenintensiven Endpoint-Security-Produkten von Drittanbietern ausgestattet werden müssen,
- Ausgaben für die Aktualisierung der Endgeräte vermeiden oder verschieben und dadurch IT-Budget für strategischere Aufgaben freisetzen.



Minimieren Sie die Komplexität des Endpoint-Managements

IGEL OS wurde als Edge-Betriebssystem der nächsten Generation für Cloud Workspaces entwickelt. Die nahtlose Integration mit der IGEL Universal Management Suite (UMS) ermöglicht ein vollständiges Remote-Management. So lassen sich mit IGEL OS und UMS zehntausende von Nicht-Windows-Endpoints einfach und effizient über eine einzige Konsole verwalten. IT-Teams haben mit IGEL präzise und zentrale Kontrolle darüber, wie Endpoints konfiguriert werden und welche Funktionen und Anpassungen für Endbenutzer verfügbar sind.

Alle erforderlichen Firmware-Updates werden schnell und äußerst zuverlässig bereitgestellt. Dabei kommt ein effizienter "Buddy Update"-Ansatz zum Einsatz, der die Auswirkungen von Bandbreitenengpässen reduziert. Das zentrale Management umfasst sowohl die Endpoints vor Ort als auch Remote-Geräte, die über die IGEL Cloud Gateway (ICG)-Funktion nahtlos bereitgestellt und aktualisiert werden. Updates lassen sich schnell und sicher durchführen - und im Gegensatz zu den meisten anderen Lösungen überprüft IGEL UMS immer, ob die Aktualisierung erfolgreich abgeschlossen wurde.

Der effiziente und zuverlässige Endpoint-Management-Ansatz von IGEL beseitigt in Verbindung mit VDI, RDSH und/oder DaaS die Kosten und Ineffizienz herkömmlicher Imaging-, Patching- und Update-Verfahren für Windows-PCs. IT-Teams haben sofort viel mehr Zeit für strategische Aufgaben – und können nachts besser schlafen.

Ersetzen Sie nicht versehentlich Windows durch Windows

Wenn ein Unternehmen Windows-Desktops in das Rechenzentrum oder in die Cloud verlagert, benötigen die Endanwender immer noch einen Endpoint, um remote auf ihre Desktops zugreifen zu können. Häufig machen Unternehmen den Fehler, ihre Windows-Endpoints durch Thin Clients mit einem "Windows Embedded"-Betriebssystem zu ersetzen. Dabei handelt es sich letztlich auch wieder um Windows-Maschinen – nur in einem neuen Gewand. Dies macht die Vorteile einer Windows-Migration ins Rechenzentrum wieder zunichte. Auch wenn das Thin Client-Betriebssystem einen etwas anderen Namen hat, wie z.B. Windows Embedded oder Windows 10 IoT - es ist immer noch Windows. Das System muss ebenfalls gepatcht und abgesichert werden, ähnlich wie eine lokal ausgeführte Installation von Windows 10.

Überlegene Endpoint-Sicherheit erreichen

Der Wechsel von der großen und anfälligen Angriffsfläche von Windows zu IGEL OS bringt sofortige Verbesserungen in puncto Endpoint-Sicherheit. Das Linux-basierte IGEL OS wird von UMS dynamisch konfiguriert und stellt nur die Funktionen zur Verfügung, die für den jeweiligen Benutzer erforderlich sind. Die zuverlässige Ausführung gewährleistet die Integrität des Endpoints zu jedem Zeitpunkt.

IGEL OS bietet zudem Support für eine Vielzahl von Multi-Faktor-Authentifizierungs- und Single-Sign-On-Technologien und unterstützt allgemeine Security-Best-Practices und branchenspezifische Anforderungen. Darüber hinaus kann ein optionaler sicherer Browser risikoreiche Web-Browsing-Aktivitäten von den primären Computeraktivitäten eines Benutzers in VDI-, RDSH- und DaaS-Umgebungen isolieren.

Die einzigartige UD Pocket-Option von IGEL OS ermöglicht es außerdem, Windows-Desktops zentral für nicht verwaltete und/oder hochmobile "Bring Your Own Device" (BYOD)-Endpoints bereitzustellen. Anwender können dabei IGEL OS von einem USB-Gerät booten, das nicht größer als ein paar Büroklammern ist. So lassen sich Remote-Windows-Desktops sicher auf nicht verwalteten Geräten nutzen – ganz gleich, wo sich der Anwender befindet – ohne dass die IT-Umgebung einem potenziell unsicheren, benutzerverwalteten Betriebssystem ausgesetzt wird.

Unabhängig davon, ob IGEL OS auf einem verwalteten oder nicht verwalteten Gerät läuft: Alle Aktivitäten der Benutzersitzung werden ausschließlich remote ausgeführt – auf Server- und Storage-Ressourcen im geschützten Rechenzentrum oder in der Cloud. Sensible Daten liegen niemals lokal auf dem Endpoint. Dies reduziert die Wahrscheinlichkeit kostspieliger und potenziell rufschädigender Datenschutzverletzungen erheblich.

Verlieben Sie sich wieder in Windows

Der Wandel ist eine Konstante in der Unternehmens-IT. Die meisten erfahrenen IT-Experten kennen die Gefahren radikaler Veränderungen in ihren geschäftskritischen Umgebungen. Ebenso riskant ist es aber, Prozesse und Praktiken beizubehalten, die sich nachweislich nachteilig auf die Effizienz, Sicherheit und Zufriedenheit der IT-Anwender auswirken.

Tatsächlich begrüßt Microsoft selbst die Entwicklung von Windows zu einem zentral verwalteten Betriebssystem. Der bemerkenswerteste Beleg dafür ist die Einführung von Windows Virtual Desktop (WVD), einem Microsoft Azure-basierten DaaS-Angebot, das Anfang 2019 als Preview veröffentlicht wurde. WVD bietet Microsoft-Kunden einen einfachen Migrationspfad zu Windows in der Cloud, einschließlich einer einfacheren Lizenzierung virtueller Desktops und neuer DaaS-freundlicher Funktionen wie Multi-Session Windows 10. Microsoft generiert mit dem neuen Windows-Lizenzmodell kontinuierliche Einnahmen, da Kunden ihre Endpoint-Ressourcen in die Cloud verlagern. Auf Thin Clients wurde Windows bereits von Linux als führendes Endpoint-Betriebssystem abgelöst – so eine Einschätzung von IDC. Und dieser Trend wird sich nicht umkehren. Die Linux-Akzeptanz für VDI-Implementierungen nimmt schnell zu und mit zunehmender Reife der DaaS-Angebote werden Linux-basierte Endpoints immer besser angenommen – siehe Gartner zur WVD-Akzeptanz.

Die Einführung von VDI, Remote Desktop Session Hosts oder DaaS mit dem hocheffizienten und sicheren Endpoint-Managementansatz von IGEL ist eine ideale Kombination. Die Benutzer arbeiten weiterhin an ihrem vertrauten Windows-Desktop und können alle Anwendungen wie gewohnt nutzen. Gleichzeitig werden IT-Teams wesentlich effizienter und können unnötige Hardwarekosten vermeiden. Und schließlich verbessert sich die allgemeine Sicherheitslage des Unternehmens erheblich.

Laden Sie die IGEL Workspace Edition herunter, um noch heute loszulegen.

Sind Sie bereit, Ihre Beziehung zu Windows neu zu starten? **Laden Sie sich die IGEL Workspace Edition kostenlos herunter**, um die einfachste, kostengünstigste und sicherste Methode zur Bereitstellung von Windows-Desktops für Ihre Benutzer zu nutzen.

Der Download der IGEL Workspace Edition beinhaltet 3 IGEL OS-Lizenzen und den vollständigen Zugriff auf die Management-Plattform IGEL UMS. Alle Lösungen können bis zu 90 Tage lang kostenlos genutzt werden.