7 wichtige Verfahrensweisen für End-User Computing mit Windows 10

UBM

Januar 2017

Das Betriebssystem von Microsoft bietet ganz neue Möglichkeiten, um standortunabhängig für Produktivität und Sicherheit zu sorgen. Hier erfahren Sie, wie Sie diese neuen Möglichkeiten optimal nutzen.

Der Arbeitsplatz hat sich grundlegend gewandelt. Um den steigenden Ansprüchen von Beruf und Privatleben gerecht zu werden, greifen Menschen heutzutage netzwerk- und standortunabhängig auf Desktops, Laptops, Tablets und Smartphones zu. Zudem werden immer mehr sich ständig wandelnde digitale Ressourcen eingesetzt, wie etwa traditionelle und cloud-basierte Anwendungen. Darüber hinaus erfordern sowohl Anwendungen als auch Betriebssysteme häufigere Aktualisierungen, um agile und kontinuierliche Ergebnisse liefern zu können.

Herkömmliche Ansätze für Desktop-Management und Mobile Device Management (MDM) sind für diesen neuen digitalen Arbeitsplatz nicht mehr geeignet. Die Unternehmens-IT muss den Anwenderzugriff auf digitale Ressourcen möglichst schnell und umfassend verändern, um eine konsistente Nutzung aller Geräte zu ermöglichen, auch wenn sich Betriebssysteme und Plattformen ständig weiterentwickeln.

Mit Windows 10 können IT-Abteilungen ein einheitliches Endpunkt-management einführen, das den neuen digitalen Arbeitsplatz effektiv unterstützt.

Wenn dieser neue Grundsatz des digitalen Arbeitens nicht mit einheitlichen Verfahrensweisen im Bereich Endpunktmanagement einhergeht, sind Produktionsrückgänge, Sicherheitslücken, Compliance-Verstöße, sinkende Mitarbeitermotivation und geringere Renditen von Technologie-Investitionen unumgänglich.

Glücklicherweise können IT-Abteilungen das Endpunktmanagement mit Windows 10 ab sofort an die neuen digitalen Arbeitsweisen der Anwender anpassen. Insbesondere haben IT-Abteilungen die Möglichkeit, fortan auf einheitliches Endpunktmanagement (UEM, Unified Endpoint Management) zu setzen. Herkömmliche Gruppenrichtlinien werden dank neuer Push-Fähigkeiten und Kontextbewusstsein umfassend erweitert, sodass sie den neuen digitalen Arbeitsplatz noch effektiver unterstützen.

7 wichtige Verfahrensweisen für Windows 10 am Arbeitsplatz

Sieben wichtige Verfahrensweisen können IT-Abteilungen dabei helfen, das neue Microsoft-Betriebssystem wirtschaftlich optimal einzusetzen.

1. Einheitliches Management von Desktop- und Mobilgeräten

Das zentrale Ziel des UEM-Konzepts besteht darin, Desktop- und Mobilgeräte nicht mehr isoliert zu verwalten. Von der Logik und Funktion her bleibt ein Endpunkt ein Endpunkt, unabhängig vom Formfaktor oder der Art der Netzwerkverbindung. Zudem können Anwender unabhängig davon, ob sie sich im Büro oder an einem anderen Ort befinden, dieselben Arbeiten vornehmen. Daher ist es sinnvoll, ihnen geräteübergreifend und einheitlich Zugriff auf sämtliche benötigten Anwendungen und Ressourcen zu ermöglichen.

Verschiedene neue Entwicklungen unterstützen diesen einheitlichen Ansatz. Eine davon ist die Einführung von MDM-APIs als neuer Standard für das Management des Betriebssystems. Mithilfe dieser APIs können IT-Abteilungen vom traditionellen, auf Gruppenrichtlinienobjekten (GPO, Group Policy Object) basierenden Management, das sich hauptsächlich für Geräte in Domänen mit festen Netzwerkverbindungen eignete, auf ein mobiles Cloud-Modell umsteigen. Dieses lässt sich universell auf allen Plattformen und unabhängig von Netzwerken und Domänen einsetzen. Eine weitere Entwicklung ist die Einführung eines einheitlichen API-Pakets (Bestandteil der Windows 10 Universal Applications). Dieses Paket führt eine einzige Codebasis aus und lässt sich bequem auf jedem Windows-Gerät einrichten und verwalten.

Unterstützt von

vmware airwatch

Durch ein besseres Verständnis und die gezielte Nutzung dieser neuen Verwaltungsfunktionen von Windows 10 können IT-Abteilungen den Umstieg auf UEM einleiten. Wenn Unternehmen dieses neue Modell übernehmen, muss die IT-Abteilung zumindest übergangsweise in der Lage sein, diese modernen UEM-Merkmale bei Bedarf über die Cloud mit traditionellen PC-Managementfunktionen zu ergänzen (z.B. GPO-Unterstützung, Skript-Erstellung und Task-Sequenzierung sowie Paketerstellung und Bereitstellung von Win32-Anwendungen). Dies ist eine Win-Win-Situation für das Unternehmen und das für die Endpunkte zuständige Operations-Team.

2. Umdenken beim Onboarding

In der Vergangenheit haben IT-Abteilungen im Vorfeld der Einführung neuer Geräte Images erstellt. Dies hat IT-Ressourcen verbraucht und die Bereitstellung für Anwender verzögert. Ein langsames Onboarding ist heutzutage jedoch nicht mehr akzeptabel. Unternehmen müssen sicherstellen, dass neue Mitarbeiter umgehend produktiv sind. Millennials erwarten von IT-Abteilungen heutzutage ein Servicemodell, mit dem PCs ebenso schnell einsatzbereit sind wie Smartphones. IT-Abteilungen haben zahlreiche weitere Aufgaben, als nur Images auf Geräte zu laden.

Das Betriebssystem Windows 10 verbindet sich sofort, sicher und zuverlässig mit dem Netzwerk und ermöglicht es dann Geräten, drahtlos die entsprechenden Binärdateien, Einstellungen und Berechtigungen abzurufen. Auf diese Weise stellt es eine Umgebung bereit, die die nötigen Voraussetzungen für ein optimiertes Onboarding bietet.

Über ein Repository zum automatisierten Abruf von Arbeitsumgebungen können IT-Abteilungen neue „Produkte“ schneller, häufiger und mit höherer Detailgenauigkeit aktualisieren.

Um dieses effizientere Onboarding-Modell zu nutzen, müssen IT-Abteilungen ihr Konzept grundsätzlich überdenken und von Geräte-Images auf die Bereitstellung von ganzen Arbeitsumgebungen umsteigen. Dies umfasst in der Regel das Erstellen verschiedener Vorlagen für den digitalen Arbeitsplatz, die Anwender basierend auf ihrer Identität, Rolle, Betriebssystemplattform und -version sowie weiteren Kriterien automatisch abrufen können. Über ein Repository zum automatisierten Abruf von Arbeitsumgebungen können IT-Abteilungen neue „Produkte“ für die Umgebung noch schneller, häufiger und mit höherer Detailgenauigkeit aktualisieren als zuvor. Auf diese Weise können sie mit dem schnelllebigen geschäftlichen Umfeld und den technischen Anforderungen besser Schritt halten.

3. Intelligente Definition von Richtlinien für sofortige, standortunabhängige und automatisierte Erweiterungen

Die meisten IT-Organisationen waren bisher nicht in der Lage, ein vollständig auf Richtlinien basierendes Konzept für das Endpunktmanagement zu verfolgen. Dies liegt unter anderem daran, dass einzelne Richtlinienattribute nur auf stark fragmentierte Weise implementiert werden konnten: eine Zugangsgenehmigung für eine SharePoint-Instanz hier, eine Geofencing-Einschränkung da usw. Die Anwendung von Richtlinien wurde dadurch erschwert, dass es sehr lange dauert, diese innerhalb und außerhalb des Unternehmensnetzwerks auf zahlreichen Geräten umzusetzen. Zudem ist ein Neustart dieser Geräte erforderlich, bevor neue oder geänderte Richtlinien in Kraft treten.

Um diese Hindernisse zu überwinden, müssen IT-Abteilungen ein wirklich auf Richtlinien basierendes Endpunktmanagement implementieren, das über modernes MDM und/oder traditionelle GPOs standortunabhängig eine einheitliche und zentrale Steuerung aller Richtlinienattribute ermöglicht. Nur dann haben IT-Abteilungen die Möglichkeit, komplette Richtlinien für Zugriff, Authentifizierung, Verschlüsselung, Whitelisting, kontextabhängige Sitzungssteuerung und vieles mehr festzulegen. Diese gelten für den Einsatz im und außerhalb des Unternehmens sowie auf sämtlichen Windows-Geräten und Geräten mit anderen Betriebssystemen aller Art (z.B. iOS, Android, macOS usw.). Zudem können sie dabei darauf vertrauen, dass diese Richtlinieneinstellungen sofort in Kraft treten.

4. Bereitstellen von kontextabhängigem Self-Service

Durch effektives Richtlinienmanagement können IT-Abteilungen gezielt auf ein Self-Service-Modell umsteigen, mit dessen Hilfe Anwender zugelassene Anwendungen und Ressourcen in ihren digitalen

Arbeitsplatz einbinden können. Denn die Richtlinien sorgen dafür, dass Anwender ausschließlich auf autorisierte Anwendungen oder Ressourcen zugreifen können.

IT-Abteilungen müssen das Self-Service-Modell durch ein einfacheres Erstellen von Anwendungsportalen unterstützen, über die Anwender auf verfügbare und zugelassene Anwendungen zugreifen können. Dies betrifft traditionelle Win32- und neue Windows Store-Apps, kommerzielle Software von Drittanbietern, intern entwickelte Anwendungen, SaaS sowie bereits veröffentlichte Remote-Anwendungen. Der Zugriff muss dabei auf der Identität, Rolle und Zuständigkeit sowie auf dem Standort basieren. Darüber hinaus können IT-Abteilungen eigene Richtlinien für diese Portale erstellen, die durch Wiederverwendung von Lizenzen und Reklamationsmechanismen für Lizenzkonformität sorgen und gleichzeitig die parallele Nutzung optimieren.

Dies hat eine verbraucherorientierte Anwendererfahrung zur Folge, die die Mitarbeiterproduktivität optimiert und zudem den Verwaltungsaufwand der IT-Abteilung reduziert.

5. Aktualisieren des Betriebssystems ohne wöchentliche Patch-Termine

Eine UEM-Lösung, die detaillierte Aktualisierungen des Betriebssystems auf allen Geräten und in allen Netzwerken unterstützt und für einheitliche Endpunkte sorgt, ohne die Anwenderproduktivität zu beeinträchtigen.

Für Sicherheits- und Support-Zwecke ist es wichtig, dass die Betriebssystemversionen der Endpunkte stets auf dem aktuellen Stand sind. Aber das traditionelle Modell mit wöchentlichen Massen-Patches ist lästig und ineffizient. Zudem können IT-Abteilungen bei diesem Modell keine häufigen Aktualisierungen vornehmen, sodass Schwachstellen über längere Zeiträume bestehen und sich die Implementierung neuer Betriebssystemfunktionen verzögert.

Wenn das Unternehmen eine Migration auf Windows 10 vornimmt, erhält die IT-Abteilung die Kontrolle über Aktualisierungsintervalle und kann Richtlinien zur Ausführung von Aktualisierungen flexibler festlegen. Funktionsaktualisierungen können entweder sofort zusammen mit kritischen Sicherheitsupdates („Current Branch“), mit leichter Verzögerung wegen eines vorherigen Einsatztests („Current Branch for Business“) oder bei besonders sensiblen Bereitstellungen, wie z.B. in Medizin- oder Finanzsystemen, zu einem von der IT-Abteilung festgelegten Zeitpunkt („Long-Term Servicing Branch“) erfolgen.

Auch wenn die mit Massen-Patches verbundenen Probleme in Windows 10 einfacher zu lösen sind, da es laufende drahtlose Aktualisierungen ermöglicht, benötigen IT-Abteilungen nach wie vor eine UEM-Lösung, die gezielte Betriebssystemaktualisierungen aller Geräte an jedem Standort und in jedem Netzwerk unterstützt, sobald diese verfügbar sind. So wird ohne Beeinträchtigung der Anwenderproduktivität für einheitliche Endpunkte gesorgt. Zudem werden auch Sicherheitslücken minimiert, da wichtige Fehlerbehebungen sofort aufgespielt werden.

6. Anwenden von Richtlinienautomatisierung und Berichterstattung für einfachere Compliance

Die Compliance wird für IT-Abteilungen zu einer immer größeren Belastung, da die Unternehmensumgebung zunehmend komplex wird. Diese Belastung wird durch manuelle Prozesse verursacht, die sich nicht von allein dokumentieren. Hinzu kommen Endpunktmanagement-Tools, die eine fragmentierte Berichterstattung liefern.

UEM reduziert diese Belastung auf verschiedene Weisen erheblich. Erstens bietet es einen zentralisierten und automatisierten Mechanismus zur ortsunabhängigen Festlegung und Durchsetzung der für die Compliance relevanten Richtlinien. Zweitens liefert es einen einheitlichen Einblick in alle Endpunktgeräte, sodass die IT-Abteilung etwaige Compliance-Unstimmigkeiten mühelos erkennen und auf den betroffenen Geräten automatisch beheben kann.

Und drittens kann die IT-Abteilung mithilfe von UEM verschiedene Compliance-Berichte zusammenfassen, was im Falle eines Compliance-Audits häufig am wichtigsten ist. Dank dieser einheitlichen Berichterstattung kann Auditoren schnell die notwendige Dokumentation vorgelegt werden, damit die IT-Abteilung das Audit besteht. Eine einheitliche Berichterstattung ist für Auditoren im Allgemeinen viel glaubwürdiger, da die verschiedenen Schritte der Datenerhebung wegfallen, die häufig zu Fehlern und Ungenauigkeiten in den Compliance-Dokumenten führen.

7. Implementieren von Datenschutzfunktionen zur gemischten geschäftlichen und privaten Nutzung von Geräten

Die Unternehmens-IT muss sich auf eine gemischte geschäftliche und private Nutzung von Mobilgeräten einstellen. Dies kann durch die Einführung eines offiziellen „Bring Your Own Device"-Programms, durch Leitlinien zur privaten Nutzung von unternehmenseigenen Geräten oder durch eine Kombination dieser beiden Konzepte geschehen. Dennoch erfordert jedes gemischte Nutzungskonzept eine sichere Abstrahierung des digitalen Arbeitsplatzes der Mitarbeiter von der zugrunde liegenden Hardware.

Windows 10 unterstützt diese Abstrahierung, indem für berufliche Zwecke bestimmte Anwendungen, Inhalte und Verbindungskomponenten in Containern abgelegt werden. Das Betriebssystem identifiziert geschäftliche Inhalte nach Attributen wie Ausgangsdateiserver, Mailserver, IP-Adresse und DNS-Adresse. Diese Inhalte können dann automatisch in eigenen Containern gespeichert und ohne Störung der Anwendererfahrung verschlüsselt werden. So können Richtlinien und Verwaltungsmaßnahmen (z.B. Datenlöschung per Fernzugriff) auf Geschäftscontainer angewandt werden, ohne sich auf persönliche Inhalte auszuwirken.

Diese technischen Möglichkeiten sind extrem wertvoll, weil die Grenzen zwischen Berufs- und Privatleben immer mehr verschwimmen. Zudem gewinnt auch der Schutz der Privatsphäre zunehmend an Bedeutung, da die hohe Fluktuation und der wachsende Einsatz von Auftragnehmern die Daten-Governance beeinträchtigen. Darüber hinaus werden sich gesetzliche Bestimmungen wie die Datenschutz-Grundverordnung der Europäischen Union aller Wahrscheinlichkeit nach auf die Verpflichtungen von Arbeitgebern und -nehmern auswirken. Um diese Probleme effektiv zu lösen, müssen IT-Abteilungen alle relevanten Richtlinienparameter ordnungsgemäß definieren und automatisieren.

Der Nutzen von UEM

Die Investition in UEM und Richtlinienautomatisierung zahlt sich aus. Die Arbeitswelt hat sich durch digitale Technologien drastisch verändert. Diese wiederum durchlaufen durch allgegenwärtige Mobilität selbst eine drastische Veränderung. Werden die sieben genannten Verfahrensweisen befolgt, ergeben sich für IT-Organisationen in Unternehmen zahlreiche wichtige Vorteile. Hierzu zählen:

- **Deutlich geringerer Verwaltungsaufwand am Endpunkt.** Aufgrund einer begrenzten Mitarbeiterzahl und eingeschränkten Mitteln können sich IT-Abteilungen keine Endpunkte leisten, deren Kosten unkontrolliert steigen. UEM mit Windows 10 reduziert den Zeitaufwand und die Betriebskosten für das Endpunktmanagement und ermöglicht den Einsatz begrenzter Mittel an anderer Stelle.
- **Eine bessere Anwendererfahrung.** Je schneller die IT-Abteilung auf die Anforderungen der Mitarbeiter reagiert, desto produktiver sind sie. Diese Produktivität führt umgehend zu zufriedeneren Kunden, mehr Innovation und verbesserter wirtschaftlicher Leistung.
- **Mehr Sicherheit für das Unternehmen.** Unzureichend verwaltete Endpunkte stellen eine immense Bedrohung dar. Eine einheitliche und umfassend automatisierte Steuerung von Endpunkten senkt Sicherheits- und Compliance-Risiken deutlich, ohne die Produktivität zu beeinflussen.
- **Höhere geschäftliche Agilität.** Unternehmen können nicht schnell sein, wenn sie Anwendern digitale Fähigkeiten nur langsam bereitstellen. UEM und Windows 10 bieten die notwendige Agilität, indem sie verschiedene Hemmnisse für die digitale Bereitstellung aus dem Weg räumen.

Wayne Gretzky hat einmal den folgenden Rat seines Vaters weitergegeben: „Lauf dahin, wo der Puck hingeht, und nicht dahin, wo er gerade war." Dasselbe gilt für das Endpunktmanagement. IT-Abteilungen müssen die Transformation von Endpunkten vorantreiben oder zwangsläufig mit den Konsequenzen leben, also mit höheren Kosten, häufigeren Sicherheitslücken und frustrierten Mitarbeitern, insbesondere unter den Millennials. Richtig eingesetzt und verwaltet bieten UEM und Windows 10 auf Dauer eine extrem überzeugende Alternative.