ZUSAMMENFASSUNG

Modernisierung des Managements und der Sicherheit von Windows 10 mit VMware AirWatch Unified Endpoint Management

Neue Anforderungen des modernen Arbeitsplatzes

MITARBEITER sind heute mobiler und selbständiger als je zuvor. Der Einsatz von Mobilgeräten nimmt immer mehr zu und Mitarbeiter nutzen eine Vielzahl von Anwendungen, Geräten und cloud-basierten Services. Immer häufiger nutzen sie dasselbe Gerät für Arbeit und Privates und erwarten Wahlfreiheit, Self-Service-Funktionen und Datenschutz. Kann die IT diese Erwartungen nicht erfüllen, leidet die Anwendererfahrung. Die Folgen sind frustrierte Mitarbeiter und die zunehmende Nutzung von Schatten-IT.

Darüber hinaus entsteht in der IT-Organisation selbst eine weitgehende Isolierung zweier Managementwelten: der für Desktops und der für Mobilgeräte. Für das Management von Mobilgeräten kommen moderne EMM-Lösungen (Enterprise Mobility Management) zum Einsatz. Desktop-Geräte hingegen wurden bisher separat mit herkömmlichen PCLM-Tools (PC Lifecycle Management) verwaltet.

Dieses fragmentierte Managementmodell ist jedoch für die IT zu teuer und nicht sicher genug. Bei herkömmlichen PCLM-Tools müssen die Geräte der Domäne und dem Netzwerk des Unternehmens angehören, um mit IT-Richtlinien und OS-Patches aktualisiert werden zu können. Da Mitarbeiter aber nicht mehr an ihre Schreibtische gebunden sind, nimmt das Risiko von Compliance-Verstößen zu und es entstehen mehr Angriffsvektoren für potenzielle Bedrohungen.

Um die Anforderungen moderner Mitarbeiter erfüllen zu können, gilt es als Erstes, Managementsilos abzuschaffen, und es muss ein endpunktübergreifender einheitlicher und anwenderzentrierter Managementansatz gefunden werden. Gartner-Analyst Chris Silver: „Die Zukunft des Endpunktmanagements liegt in der Konsolidierung der Managementtools für herkömmliche PCs und Mobilgeräte in einem gemeinsamen Management-Framework."

Die Einführung von Managementprotokollen für Mobilgeräte in Windows 10 ermöglicht der IT die Zusammenlegung von Managementteams, die Konsolidierung von Tools, die Kostenreduzierung, die Steigerung der IT-Effizienz und die Härtung der Sicherheit im Unternehmen. So können Unternehmen das Management von Anwendergeräten durch die Implementierung einer UEM-Lösung (Unified Endpoint Management, einheitliches Endpunktmanagement) für das Management von Desktops und Mobilgeräten optimieren.

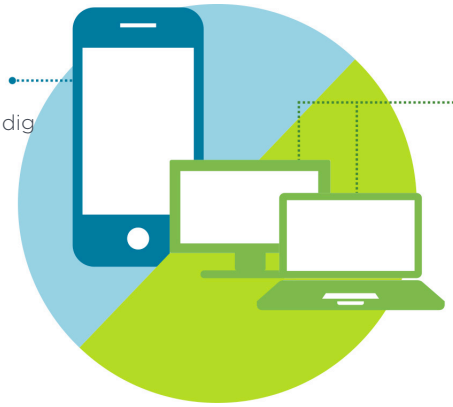
GRENZEN HERKÖMMLICHER ANSÄTZE FÜR DAS PC-MANAGEMENT

Das Hauptziel für IT-Organisationen sollte darin bestehen, Anwendern erstklassige Umgebungen zu bieten, die ein effektiveres und produktiveres Arbeiten ermöglichen. Die Anwendererfahrungen sind bei Mobilgeräten und PCs jedoch oft unterschiedlich, vielfach sogar gegensätzlich. Die Bereitstellung und Konfiguration eines Mobilgeräts erfolgt mittlerweile effizient und unterstützt Self-Service-Funktionen. Die Bereitstellung eines Desktop- oder Laptop-Computers hingegen kann Wochen dauern. Imaging, Konfiguration und Wartung nehmen oft sehr viel Zeit in Anspruch.

Die Kluft zwischen Mobilgeräten mit optimierter Konfiguration und Verwaltung und langwieriger und mit Einschränkungen verbundener PC-Konfiguration frustriert Anwender zunehmend.

Mobilgerät

Mit einem vollständig eingerichteten Smartphone nach Hause gehen



Desktop und Laptop

Wochenlanges Warten, bis das Unternehmensgerät eingerichtet ist

Was muss sich ändern?

1 Betriebssystem

Das Windows-Betriebssystem ist die erste Komponente, die weiterentwickelt werden muss, um den Anforderungen heutiger Mitarbeiter gerecht zu werden. Windows 10 ist ein anwenderzentriertes Betriebssystem mit Funktionen, die Anwendern Wahlfreiheit, Schutz ihrer persönlichen Daten und Mobilität bieten. Aber noch wichtiger bei diesem neuen OS ist die Einführung eines grundlegend anderen Sicherheits- und Managementansatzes, der mehr auf moderne EMM-Lösungen abgestimmt ist. Ein einheitlicher Satz Managementprotokolle für alle PCs, Tablets und Smartphones mit Windows 10 ermöglicht der IT nun, Managementtools zu konsolidieren, einsatzbereite Geräte bereitzustellen sowie Richtlinien und Anwendungen drahtlos aufzuspielen. So können Anwender in kürzester Zeit ihre Arbeit aufnehmen.

2 Managementtools

Legacy-Managementtools für PCs sind für die Anforderungen moderner Mitarbeiter nicht mehr effizient genug. Anwender erwarten, jederzeit, von jedem Ort aus und über jedes Gerät ihre Arbeit erledigen zu können. Sie möchten über alle ihre Geräte gleichermaßen auf Anwendungen und Daten für ihre Arbeit zugreifen können. Diese Erwartungen lassen sich mit herkömmlichen Tools für das PC-Management kaum noch erfüllen. Herkömmliche Tools sind...

- **Teuer** – Legacy-Managementansätze für PCs sind server- und arbeitsintensiv. Sie erfordern mehrere Softwarelösungen und komplexe Methoden für Imaging und Konfigurationsmanagement. Das Management von Softwarepaketen und OS-Patches ist ein mühsamer Prozess und die IT muss sich für beide Managementsilos (Desktops und Mobilgeräte) spezielle Kenntnisse aneignen und regelmäßig auffrischen.
- **Unsicher** – Das Management erfolgt weitestgehend anhand von Gruppenrichtlinienobjekten (GPOs) und ist nur für Geräte möglich, die einem Netzwerk oder einer Domäne angehören. Mit diesem Ansatz kann es Wochen oder sogar Monate dauern, bis die Installation von Sicherheitsrichtlinien, OS-Patches und Anwendungs-Upgrades abgeschlossen ist, und das Unternehmen ist potenziell höheren Sicherheitsrisiken ausgesetzt. Angesichts täglich neuer Formen von Angriffsvektoren wird es für die IT noch schwieriger, sich den nötigen Einblick in Systemzustand und Compliance der Endpunkte zu verschaffen.
- **Einschränkend** – Legacy-Ansätze frustrieren Anwender, da sie die Kontrolle über ihre Geräte einschränken. Die IT kann die erforderliche Sicherheit nur bieten, indem sie die Auswahl an Gerätetypen einschränkt und das Betriebssystem nur für vertrauenswürdige Anwendungen und Updates freigibt. Da bleibt nicht mehr viel Raum für Anpassungen und Anwendern stehen nur wenige oder keine Self-Service-Funktionen zur Verfügung. Diese Einschränkungen sind aufwendig für die IT und verursachen viele Helpdesk-Anrufe selbst für einfache Aufgaben wie die Installation einer Anwendung auf dem Gerät.

DIE LÖSUNG: EINHEITLICHES ENDPUNKTMANAGEMENT

Die Einführung von Management-APIs für Mobilgeräte in Windows 10 schafft ganz neue Möglichkeiten für das Management von PC-Endpunkten in Unternehmen. Anders als iOS und Android sind mit PCs allerdings mehrere spezielle Herausforderungen verbunden. Dazu gehören:

- Unterstützung komplexer Skripts und GPOs muss gegeben sein
- Paketierung und Verteilung klassischer Windows-Anwendungen (Win32)
- Test von OS-Patches, bevor diese für Anwender verfügbar gemacht werden
- Netzwerkeinschränkungen aufgrund der Größe dieser Anwendungen und Updates

Unternehmen brauchen also eine Plattform für einheitliches Endpunktmanagement, die IT und Anwendern die Effizienzen von EMM-Lösungen für Mobilgeräte bietet und gleichzeitig die detaillierten Anforderungen des herkömmlichen PC-Managements erfüllt.

VMware AirWatch Unified Endpoint Management bietet umfassende Funktionen für Windows 10, die Bereitstellung und Konfiguration des Betriebssystems, Verteilung von Anwendungen (einschließlich Win32-Anwendungen) und Updates sowie End-to-End-Sicherheit ermöglichen. Mit einem modernen Cloud First-Ansatz werden Kosten und Aufwand für die IT reduziert und Implementierung sowie Management von Windows 10 werden einfacher und sicherer. Dies ermöglicht Unternehmen Folgendes:

- Umstellung von teuren Imaging-Verfahren auf ein einfacheres Bereitstellungsmodell
- Verteilung von OS-Patches und Software für Geräte, die sich außerhalb der Unternehmensdomäne in einem beliebigen Netzwerk befinden
- Self-Service-Zugriff und Wahlfreiheit bei Funktionen, Geräten und Anwendungen für die Anwender
- Koexistenz von persönlichen und geschäftlichen Daten auf demselben Gerät
- Unmittelbare Transparenz, Sicherheit und Compliance für alle Endpunkte im und außerhalb des Netzwerks

Mit AirWatch UEM ist das Windows-Management auch auf alle Anwendungsbereiche skalierbar. Dazu gehören:

- Bereitstellung von Windows 10 für Remote-Mitarbeiter
- Onboarding mitarbeitereigener Geräte (Bring Your Own Device, BYOD)

Gerätemanagement mit AirWatch UEM – einfacher, sicherer, kostengünstiger

- Implementierung von Unternehmensbereitstellungen in Zweigstellen
- Management eines speziellen Geschäftsbereichs-Terminals

CLOUD FIRST-MANAGEMENT UND -SICHERHEIT FÜR WINDOWS

MDM für Windows

AirWatch unterstützt konsistente Abläufe zur Geräteregistrierung für alle Anwendungsbereiche, z.B. unternehmenseigene Geräte oder BYOD. Dabei spielt es keine Rolle, ob es sich neue oder vorhandene Geräte innerhalb oder außerhalb der Domäne handelt. Mit AirWatch lassen sich generische OEM-Geräte vollständig und ohne Imaging in einen fehlerfreien und einsatzbereiten Zustand versetzen. Dadurch spart die IT Zeit und Kosten. Und neben den von der IT initiierten Abläufen unterstützt AirWatch ebenfalls intuitives Onboarding von Geräten per Self-Service durch die Anwender.

Für BYOD-Anwender und Auftragnehmer ermöglicht AirWatch darüber hinaus eine Step-up-Registrierung für das Management je nach Sensibilität der Anwendungsdaten und Sicherheitsanforderungen. Der Zugriff auf grundlegende Produktivitätsanwendungen kann beispielsweise über einen unternehmensspezifischen Anwendungskatalog basierend auf Anwenderidentität und -berechtigungen erfolgen. Dabei lässt sich der Zugriff auf Anwendungen, die sensible Unternehmensdaten enthalten, auf Geräte beschränken, die ausschließlich über AirWatch verwaltet werden.

Mit AirWatch kann das Management registrierter Windows-Geräte über dieses moderne Mobile-Cloud-Framework erfolgen. Richtlinien lassen sich sofort drahtlos konfigurieren. Mit jedem Upgrade für Windows 10 erweitert Microsoft den allgemein verfügbaren Satz an Managementprotokollen für EMM-Anbieter. Dadurch wird das Management immer mehr an die aktuellen Anwenderprofile und -einstellungen für Mobilgeräte angeglichen. Alle Funktionen zielen auf die Vereinfachung der Betriebssystemkonfiguration und die Verbesserung der Sicherheit ab, zum Beispiel die Durchsetzung von Passcodes, die Einrichtung von E-Mail-Adressen, die Ermöglichung des Zugriffs auf WLAN und VPN des Unternehmens sowie die Durchsetzung von Einschränkungen für Geräte und Anwendungen.

Konfigurationsmanagement

Das Management von Windows-PCs ist für die IT oft mit komplexen Automatisierungsanforderungen verbunden. Im Push-Verfahren sind komplexe Skripts, Richtlinien für Gruppenrichtlinienobjekte und andere Managementeinstellungen für herkömmliche PCs zu verteilen. Beispielsweise möchten Unternehmen ihre Desktops mit einem individuellen Hintergrund versehen, Bloatware entfernen sowie Richtlinien für Firewalls und Virenschutzsoftware festlegen. Mit den Konfigurationsmanagementfunktionen in AirWatch kann die IT „Produkte“ erstellen, die diese Dateien, Anwendungen oder benutzerdefinierten Einstellungen enthalten. Diese Produkte können dann über jedes beliebige Netzwerk auf den Geräten bereitgestellt werden. Sie lassen sich auch komplexeren Aufgabenabfolgen und Installationsbedingungen zuordnen.

Management von Betriebssystem-Patches

Mit „Windows Update as a Service“ verteilt Microsoft drahtlos per Push-Verfahren kumulative Betriebssystem-Updates. Updates, die einen umfassenden Testzyklus durchlaufen haben, werden als Servicing Branch ausgeliefert, der auf die Anforderungen des Business abgestimmt ist. Trotz der Vorteile dieses cloud-basierten Bereitstellungs- und Servicemodells hat die IT nach wie vor Bedenken bezüglich der Kontrolle folgender Punkte:

- Verteilung der richtigen Updates
- Mögliche Beschädigung des Betriebssystems aufgrund von

WLAN | VPN | Zertifikate | E-Mail | Passcodes | Compliance & Einschränkungen | Verschlüsselung | Firewall & Virenschutz | OS-Lizenz-management

AirWatch vereinfacht die drahtlose Konfiguration und Verwaltung von Geräten.

fehlenden umfassenden internen Tests der Updates

- Netzwerkeinschränkungen, da diese Updates mehrere Gigabyte umfassen

AirWatch ermöglicht der IT, Betriebssystem-Updates und -Patches basierend auf Gerätepriorität und Wartungszeitfenstern bereitzustellen oder aber zu verschieben. Bestimmte Update-Gruppen (z.B. „Anwendung“, „Entwickler“ oder „Sicherheit“) lassen sich je nach Anwenderempfindlichkeit für Funktions- und Sicherheits-Updates automatisch genehmigen oder ablehnen. Mithilfe von Peer-to-Peer-Caching ermöglicht AirWatch die Optimierung der Update-Bereitstellung und die Vermeidung von Netzwerkengpässen. Die IT kann für einzelne Windows-Updates eine detaillierte Bestandsansicht aufrufen und Compliance-Prüfungen durchführen. So gehören mit dem Patching außerhalb des Netzwerks verbundene Herausforderungen der Vergangenheit an.

Softwareverteilung

Mit Universal Windows Platform (UWP) hat Microsoft die Anwendungserfahrung auf allen Geräten mit Windows 10 vereinheitlicht. Öffentliche UWP-Anwendungen können nun über den Windows Store (ähnlich wie die Stores auf anderen mobilen OS-Plattformen) oder über einen internen „Business Store“ bereitgestellt werden, der auf die spezifischen Anforderungen eines Unternehmens abgestimmt wird. Zur Optimierung der Bereitstellung dieser modernen Anwendungen ist AirWatch sowohl in den Windows Store als auch in den Windows Store for Business integrierbar.

Der Großteil der Windows-Unternehmenssoftware besteht allerdings immer noch aus klassischen Win32-Anwendungen, deren Paketierung, Bereitstellung und Wartung aufgrund ihrer Größe entsprechend komplex ist. Aus diesem Grund ist die Softwareverteilung eine der größten Herausforderungen beim Management von Windows mit EMM-Lösungen. AirWatch löst diese Herausforderung, indem es die Lücken zwischen dem Lebenszyklusmanagement von UWP- und Win32-Anwendungen schließt.

Mit AirWatch lassen sich das Management mobiler Apps und die Bereitstellung herkömmlicher Win32-Software in einer Verwaltungskonsole konsolidieren. Administratoren können Patches für Anwendungen von Drittanbietern verwalten, Abhängigkeiten im Push-Verfahren ausliefern und sogar Bedingungen oder Eventualfälle für die Anwendungsinstallation definieren.

Mit App Stacks bietet AirWatch einen neuen Ansatz zur Softwareverteilung, mit dem sich die Herausforderungen von Anwendungspaketierung und unzuverlässigen Installationen meistern lassen. Win32-Anwendungen können damit schneller und genauso zuverlässig und einfach wie mobile Apps auf jedem beliebigen Windows-Gerät bereitgestellt werden. Für Anwender bietet AirWatch einen Self-Service-Katalog und eine konsistente Erfahrung mit Single Sign-On (SSO) für alle Windows-Anwendungen, einschließlich native, SaaS- und Remote-Anwendungen.

Client-Systemzustand und -Sicherheit

Für die Herausforderungen moderner Cyber-Security brauchen Unternehmen eine End-to-End-Sicherheitslösung. AirWatch schafft Anwendervertrauen, verbessert den Schutz des Betriebssystems vor neuen Bedrohungen und ermöglicht die Trennung von geschäftlichen und persönlichen Daten, um Unternehmensdaten während der Übertragung, der Verarbeitung und der Speicherung zu schützen.

Managementfunktionen für Win32-Anwendungen

■ **Anwendervertrauen** – Selbst die sichersten Kennwörter können auf unterschiedlichste Arten in falsche Hände geraten, zum Beispiel durch Phishing, Keylogging oder Malware. AirWatch ist in die Identitätsfunktionen von Windows 10 integrierbar und ermöglicht so das Festlegen von Richtlinien für kennwortlose Authentifizierung durch Gesten oder eine PIN. Unternehmen profitieren von einsatzbereiter Mehrfachauthentifizierung und können sich so besser vor Pass-the-Hash-Angriffen schützen.

■ **Verbesserung der OS-Sicherheit** – AirWatch ermöglicht proaktive Sicherheitsmaßnahmen durch Verhinderung des Downloads oder der Ausführung von nicht vertrauenswürdigen oder nicht genehmigten Anwendungen. Geräteintegrität und Compliance werden von AirWatch in Echtzeit überprüft. Erfüllt ein Gerät die Compliance-Anforderungen nicht, wird der Zugriff auf Anwendungen und Services des Unternehmens automatisch gesperrt.

■ **Datensicherheit** – Angesichts der zunehmenden Nutzung von Mobilgeräten, die verloren gehen oder gestohlen werden können, hat der Schutz vor Datenverlust heute oberste Priorität. Darüber hinaus wird immer häufiger dasselbe Gerät geschäftlich und privat genutzt. AirWatch definiert Richtlinien zur Verschlüsselung von Daten, ermöglicht Administratoren und Anwendern, im Fall eines Verlusts die Daten vom betroffenen Gerät remote zu löschen und sorgt für eine saubere Trennung von geschäftlichen und persönlichen Daten. Hierzu nutzt das Tool die Container-Funktionen des Windows-Betriebssystems.

AirWatch UEM ermöglicht Unternehmen die kostengünstige Durchsetzung von End-to-End-Sicherheitsmanagement.

ABSICHERN BELIEBIGER ENDPUNKTE ÜBER EINE EINZIGE PLATTFORM

UEM ist plattformunabhängig und bietet eine zentrale Lösung für das Management jedes Geräts und jedes Betriebssystems in allen Anwendungsbereichen eines Unternehmens. Unabhängig davon, mit welchem Gerät Anwender auf die Unternehmensumgebung zugreifen, sie werden immer dieselbe einheitliche Erfahrung genießen.

AirWatch UEM bietet einen ganzheitlichen, anwenderzentrierten Ansatz für das Management und die Absicherung jedes beliebigen Endpunkts über eine einzige Plattform. Seine mandantenfähige Architektur unterstützt die globale Bereitstellung über eine einzige Konsole für alle Abteilungen, Regionen und Standorte. AirWatch UEM ist mit Unternehmenssystemen integrierbar, sodass vorhandene Investitionen in Infrastruktur genutzt werden können, und macht diese Services für alle Endpunkte zugänglich.

Mit VMware AirWatch UEM lassen sich Prozesse über dynamische und intelligente Richtlinien-Engines für Windows 10-Plattformen automatisieren. Hierdurch werden manuelle Aufgaben reduziert und Self-Service-Funktionen ermöglicht und Unternehmen profitieren von reduzierten Support-Kosten.

Sind Sie bereit zum Umdenken in puncto Endpunktmanagement? Nutzen Sie unser kostenloses 30-tägiges Testangebot, bei dem Sie bis zu 100 Geräte registrieren können. Weitere Informationen finden Sie auf unserer Website.