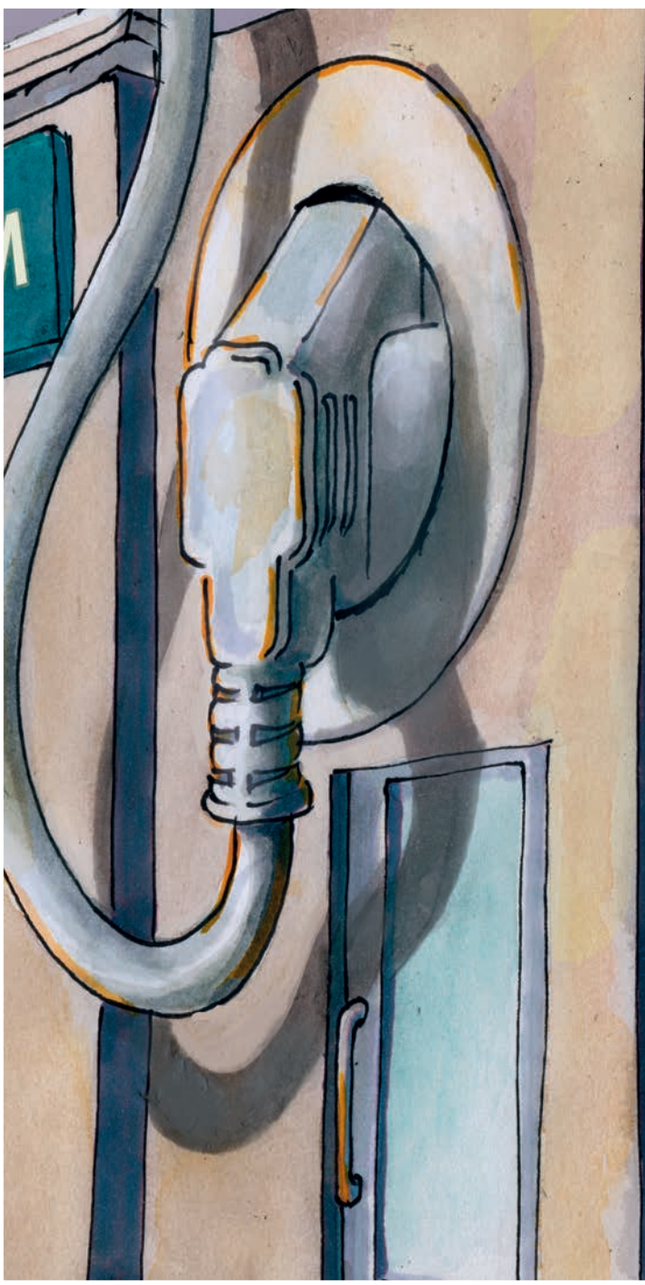
LL03_Sonderdruck_Deskcenter.pdf;S: 1;Format:(210.00 x 297.00 mm);15.Mar 2019 12:05:20

LANline

10,– €
März 2019
26. Februar

IT ▪ Network ▪ Datacenter www.lanline.de



Stromversorgung und Klimatisierung im RZ

Grundlagen der Kühltechnik

Flexible und leistungsfähige USV-Technik

Mit Marktübersicht USV-Anbieter

Sicherheitskonferenz IT-Defense, Stuttgart:
Der Nutzen von Tor und die Risiken von IoT

Im Praxistest Windows Server 2019
Das leistet das neue Server-Betriebssystem

Schwe
End
M

Sonderdruck Deskcenter
IT-Services für alle
Nutzer und
Geräte

März 2019

LL03_Sonderdruck_Deskcenter.pdf;S: 2;Format:(210.00 x 297.00 mm);15.Mar 2019 12:05:20

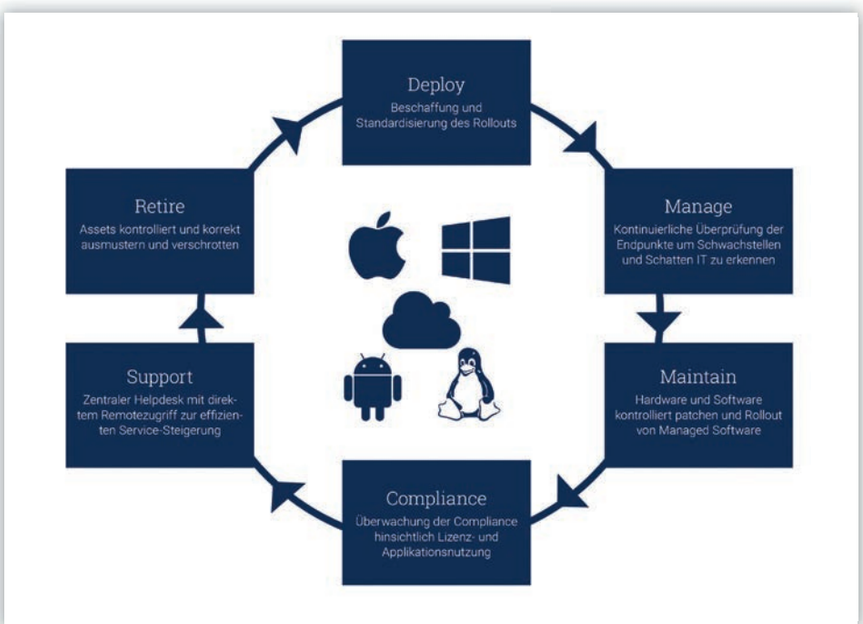
Anforderungen an UEM-Werkzeuge

IT-Services für alle Nutzer und Geräte

Für den Endanwender gehen PC und Mobilgeräte seit Jahren Hand in Hand. Die IT versucht jedoch häufig noch immer, Client- und Mobile-Device-Management mit Insellösungen zu bewerkstelligen. UEM-Anwendungen (Unified-Endpoint-Management) schaffen Abhilfe – vorausgesetzt, es gelingt eine durchgängige Prozessautomation. Dazu müssen neben Security-Features auch Management-Funktionen plattformübergreifend integriert sein.

In Deutschland nutzten 2018 bereits die Hälfte der Anwender beruflich einen Laptop und 75 Prozent ein Smartphone. Das Tablet sehen 50 Prozent der Entscheider als essenziell für den digitalen Arbeitsplatz an – so die Analysten von Crisp Research in einer Umfrage für Samsung. Auch die Forrester-Studie „Forrester Wave Unified Endpoint Management, Q4 2018“ belegt eine starke Zunahme an Endgeräten pro Anwender: Laut den Analysten arbeitet heute jeder fünfte „Information Worker“ wöchentlich mit mindestens drei mobilen Geräten.

Doch die wahren Treiber für das UEM waren 2018 laut Gartner und Forrester Apples macOS, Googles Chrome OS und Microsofts Windows 10 – Plattformen, die sich dank MDM-Bibliotheken (Mobile-Device-Management) gut per UEM-Tool verwalten lassen. Sie legen die technische Basis, um alle Endpunkte samt Anwendungen und Betriebssystemen über eine gemeinsame Oberfläche zu verwalten. UEM-Werkzeuge werden damit zur zentralen Informations- und Entscheidungsplattform.



Eine durchgängige Prozessautomation ist die Voraussetzung für echtes UEM. Bild: DeskCenter Solutions

Service und Sicherheit im Doppelpack

Eine UEM-Lösung sollte es ermöglichen, die hohen Ansprüche der Endanwender zu erfüllen. Denn diese erwarten alle IT-Services zeitnah, anwenderfreundlich und mit hoher Performance – unabhängig vom Endgerät. Dazu gehören auch komfortable Unternehmens-Self-Service-Portale, über die der Anwender Hard- und Software einfach bestellen kann. Durch hinterlegte Workflows mit klar definierten Regeln und Genehmigungsverfahren beschleunigt und sichert die IT hier den weiteren Ablauf.

So kann sie beispielsweise über Sicherheits- und Konfigurationsrichtlinien festlegen, welche Anwendungen und Apps ein Mitarbeiter auf dem Endgerät nutzen darf – und kann diese Nutzung auch überprüfen. Weitere Sicherheitsmaßnahmen sind die Anwendung von MDM-Profilen und einheitliche Richtlinien zur Verhinderung, Erkennung und Behebung von Sicherheitsrisiken für mobile Geräte und PCs.

Dashboard für den Durchblick

Über die Nutzung hinaus gilt es, im laufenden Betrieb alle Endgeräte kontinuierlich zu überwachen, um Schwachstellen und Schatten-IT zu identifizieren, die zur Gefahr für die Sicherheit werden könnten. Dies gelingt mit einer kontinuierlichen Inventarisierung aller Hard- und Software-Assets. Um jedes Endgerät zu erfassen, sind agentenlose wie auch agentenbasierte Methoden notwendig.

Der nächste Schritt ist dann, die Inventarisierungsergebnisse mit einem Software-Erkennungskatalog und der Asset-Management-Datenbank abzugleichen. Entscheidend ist, die Differenzen zum autorisierten Soft- und Hardwarebestand sofort in einem Dashboard sichtbar zu machen. Schatten-IT, mobil oder stationär, lässt sich so identifizieren, prüfen und falls nö-

LL03_Sonderdruck_Deskcenter.pdf;S: 3;Format:(210.00 x 297.00 mm);15.Mar 2019 12:05:20

tig umgehend entfernen. Das UEM-Dashboard muss dazu tagesaktuell Patch- und Release-Stände sowie abgekündigte Versionen auflisten.

Provisionierung automatisiert steuern

Im Idealfall erfolgt aus dem Dashboard heraus direkt die workflowbasierte Softwareverteilung von Updates und Patches – nicht nur für Microsoft-Produkte, sondern auch für PDF-Reader, Browser und weitere Software. Softwarepakete sollte vorab um unerwünschte Toolbars oder Adware bereinigt sein. Eine solches Managed-Service-Angebot, das bereits in die UEM-Lösung integriert ist, liefert in Zeiten von Ransomware & Co. einen wesentlichen Beitrag für die Endpunktsicherheit. Denn standardisierte Prozesse mit ausführlichen Tests vorab stellen sicher, dass die Software frei von Schadcode ist, dass sie auf allen Betriebssystemen läuft und dass bei der Installation alle Einstellungen der Nutzer erhalten bleiben.

Für die grafische, workflowbasierte Softwareverteilung benötigt die IT-Organisation Steuerungsmechanismen, die im Gegensatz zu fehleranfälligen Skripten eine hohe Service-Qualität sicherstellen. Integrierte UEM-Suiten greifen dabei auf Attribute und Informationen aus dem technischen und organisatorischen Asset-Management ebenso zu wie auf das Active Directory mit dessen Organisationseinheiten oder Sicherheitsgruppen. Damit lässt sich eine standortunabhängige und rollenbasierte Verteilung erzielen.

Die Kommunikation zwischen zentralen und dezentralen Verteilungspunkten und Endgeräten erfolgt im Idealfall zertifikatsbasiert und in Echtzeit. Durch die Verwendung unterschiedlicher Protokolle und Deployment-Techniken lassen sich auch selten im Netzwerk angemeldete Geräte zuverlässig über das Internet mit sicherheitsrelevanten Updates und gemanagter Software versorgen.

Windows-10-Deployment

Auch beim OS-Deployment profitiert die IT von UEM. Denn sie kann an unterschiedlichen Stellen des Rollout-Prozesses Aufgaben automatisiert ausführen, um die Betriebssysteminstallation flexibel zu gestalten. Dazu gehören Funktionen wie eine automatische Bereitstellung hardwarespezifischer Gerätetreiber, die Aktivierung von Bitlocker zur Festplattenverschlüsselung oder die Integration von Softwarepaketen direkt in Betriebssystem-Rollouts.

Der Erfolg einer Windows-10-Migration ist immer abhängig von Prüf- und Testszenarien der Applikationen sowie von Hardwaregegebenheiten wie beispielsweise der Prüfung von Systemvoraussetzungen hinsichtlich Architektur, Vorgängerversion oder freiem Festplattenspeicher. Anschließend erfolgt die Verteilung der Daten für die automatische Migration.

UEM hilft darüber hinaus idealerweise auch, Compliance-Anforderungen zu erfüllen: Es stellt eine belastbare Dokumentation für Lizenz-Audits bereit, ermittelt die Gerätenutzung, kontrolliert die Einhaltung von Richtlinien zur Verwendung von Soft- und Hardware und ermöglicht die saubere Trennung privater und beruflicher Daten aus Datenschutzgründen.

Lizenz-Management integrieren

Ein in den Deployment-Prozess integriertes Lizenz-Management steuert und prüft bereits zum Zeitpunkt der Beauftragung oder bei der Softwareverteilung die Verfügbarkeit von Lizenzen der jeweiligen Applikation. Gegen Überlizenzierung hilft Application Metering. Denn um die wirtschaftlichste Lizenzierungsform zu ermitteln, sind Analysen zum Nutzerverhalten erforderlich. Application Metering misst die tatsächliche Nutzung von Software und identifiziert nicht verwendete Software. Auf dieser Basis kann die IT den Lizenzbedarf genau bestimmen und so die Lizenzkosten senken.

Auch für Cloud-Anwendungen wie Office 365 ist im UEM gesorgt. Zwar geben die Hersteller über ein Portal Einblick in die geleasten Produkte, Nutzerrechte und gekauften Lizenzen. Um eine Übersicht für alle Lizenzen eines Unternehmens zu erlangen, ist dies jedoch unhandlich und bedeutet für das laufende Lizenz-Management spürbaren Mehraufwand. Dies verhindert ein UEM-Tool, das laufend Daten aus dem Office-365-Portal ausliest und in ein ganzheitliches Lizenz-Management integriert.

Der Lebenszyklus jeder Hardware endet mit deren Ausmusterung oder Verschrottung. Hier braucht die IT-Abteilung einen integrierten Ausmusterungs- oder „End-of-Life“-Prozess. Dazu gehört, personenbezogene und sensible Unternehmensdaten von Datenträgern so zuverlässig zu löschen, dass eine Wiederherstellung unmöglich ist. Gemäß BSI-Empfehlung sollte ein Tool dazu die Festplatten bis zu sieben Mal überschreiben. Anschließend lassen sich die Altsysteme gefahrlos entsorgen.

Ist auch noch der Helpdesk in das UEM integriert, wirkt sich dies in zwei Richtungen positiv aus: Zum einen wird das IT-Backend spürbar entlastet, zum anderen steigt die Service-Qualität. Dazu sollten Softwareverteilung, Automatisierungsprozesse und Administratoren-Tools wie Fernwartung aus dem Ticket heraus möglich sein. Auch sollte der IT-Support über direkten Zugriff auf alle relevanten Asset- und Anwenderinformationen für jeden Endpunkt verfügen. So kann der Helpdesk-Mitarbeiter aus derselben Ticket-Maske heraus Software- und Patch-Installationen anstoßen. Für fehlgeschlagene Installationen sollte die Software automatisch ein Ticket generieren. Dies geht nur, wenn die UEM-Lösung das gesamte technische Inventar, sämtliche organisatorischen und nutzerbezogenen Informationen sowie alle relevanten Patches und Softwarepakete in einer Datenbank vorhält.

Die Analysten von Gartner weisen zu Recht darauf hin, dass manche UEM-Tools wesentliche Aufgaben der klassischen Windows-Verwaltung nicht abdecken – sie bieten also kein vollumfängliches UEM. Typische Schwachstellen liegen hier beim Patch-Management, der Paketierung von Applikationen oder im Lizenz-Management. Ein echtes UEM gelingt jedoch nur, wenn alle relevanten Disziplinen des IT-Service-Managements integriert sind.

Benedikt Gasch/wg

Benedikt Gasch ist Direktor Produkt-Management bei DeskCenter Solutions, www.deskcenter.com.