WHITE PAPER

BRIAN MADDEN: VOM DESKTOP ZUM DIGITALEN ARBEITSPLATZ

vmware®

Vom Desktop zum digitalen Arbeitsplatz

In den ersten 20 Jahren des End-User Computings (EUC) ging es nur um die Desktop-Computer, die auf den Schreibtischen der Anwender standen. Sie gehörten einer Domäne an und waren im „Besitz" der IT (sowohl im wörtlichen Sinn als auch in Bezug auf die Kontrolle). Die IT nutzte Tools wie Microsoft Systems Management Server (SMS, ein Vorgänger von SCCM), um Software und Patches zu verteilen und zu installieren, Bestände zu erfassen und sie zentral zu verwalten.

Dieses Computing-Modell funktionierte in den meisten Fällen gut genug. Gelegentlich gab es jedoch einen Anwendungsbereich – z.B. eine Client-Server-Anwendung mit langsamer WAN-Verbindung, die serverbasiertes Computing (Server Based Computing, SBC) erforderlich machte. Dabei wurde eine Version von Windows Server für mehrere Anwender in einem Rechenzentrum ausgeführt, um Desktop- und Anwendungssitzungen remote für Anwender bereitzustellen.

Im Zuge der technischen Weiterentwicklung wurde Virtualisierung zur gängigen Praxis und es entstand VDI. VDI kombinierte Hardwarevirtualisierung mit Client-Versionen von Windows und bot im Wesentlichen die Vorteile von serverbasiertem Computing in einem Paket, das dem Management von Windows-Desktops, wie es seit einem Jahrzehnt von den IT-Abteilungen betrieben wurde, eher entsprach.

VDI und RDSH (der Nachfolger von SBC) wurden unter dem Begriff „Desktop-Virtualisierung" zusammengefasst. Es herrschte die einhellige Meinung, dass Desktop-Virtualisierung gegenüber herkömmlichen Desktops und Laptops einige Vorteile bot, u.a. das Potenzial für mehr Sicherheit, Performance und Flexibilität. Das Problem war jedoch, dass die Technologie trotz der großartigen Vorteile der Desktop-Virtualisierung nur begrenzt Anwendung fand. Viele große Unternehmen stellten fest, dass sie problemlos 10 – 20% ihrer Desktops virtualisieren konnten. Das war hervorragend, bedeutete aber auch, dass 80 – 90% der Desktops nicht virtualisiert waren und auf andere Weise verwaltet werden mussten.

Die Unternehmen setzten nun mindestens zwei Tools ein, um ihre gesamte Desktop-Umgebung zu verwalten, zu schützen und zu warten: ein Tool für die virtuellen Desktops und ein weiteres Tool für die physischen Desktops. Die Managementtools für die physischen Desktops hatten sich seit den SMS-Tagen der 90er Jahre nicht nennenswert weiterentwickelt. Auch wenn sich der Name geändert hatte (von Microsoft SMS zu SCCM), folgten die Tools immer noch dem Konzept von Windows-Desktops in einer Domäne mit Netzwerkverbindung zum Rechenzentrum.

Inzwischen dominieren iPhone und Android-Geräte die Szene. Am Anfang behandelte die IT mobile Geräte genauso wie Desktops und entsprechend verhielten sich auch die ersten MDM-Anwendungen: Sie gaben der IT „die volle Kontrolle“ über ein Gerät, einschließlich der Möglichkeit, den gesamten Inhalt – und somit auch die privaten Daten der Anwender – per Fernzugriff zu löschen. Im Laufe der Zeit entwickelte sich MDM zu MAM und schließlich zu EMM. Die IT kann nun die „geschäftlichen“ Bereiche des Geräts verwalten, während die privaten Inhalte der Anwender unangetastet bleiben.

Einer der großen Vorteile von EMM besteht darin, dass ein einzelner IT-Administrator eine Vielzahl von Geräten verwalten kann; unter Umständen sind das bis zu 10.000 Geräte pro EMM-Administrator. Hingegen kann ein einzelner Desktop-Administrator in der Regel nicht mehr als 500 Desktops verwalten.

Diese Diskrepanz blieb den IT-Experten nicht verborgen und sie verlangten von Microsoft, ihnen Tools zur Verfügung zu stellen, mit denen sie Windows-Desktops ähnlich wie mobile Geräte verwalten konnten. Das bedeutete, dass neben einem unkomplizierten Management auch mehr Geräte von einem einzelnen Administrator gehandhabt werden konnten. Microsoft unternahm mit Windows 8 die ersten Schritte in diese Richtung und lieferte dann mit Windows 10 und einer Reihe von Funktionen, dem sogenannten modernen Management, ein umfassendes Konzept.

Einfach ausgedrückt handelt es sich bei den modernen Managementfunktionen von Windows 10 um APIs, über die Windows 10-Geräte auf ähnliche Weise und mit denselben Tools wie mobile Geräte verwaltet werden können. Dadurch ist es möglich, Unternehmensrichtlinien und -konfigurationen sowohl auf unternehmenseigene als auch auf private Windows 10-Geräte anzuwenden. Dies gilt auch für Geräte, die sich nicht in einer Domäne befinden und nicht ständig mit dem Unternehmensnetzwerk verbunden sind.

Apple hat mit dem Release „High Sierra“ vom September 2017 ähnliche Funktionen in macOS hinzugefügt. Das bedeutet, dass Apple-Laptops und -Desktops mit denselben Tools wie iOS, Android und Windows 10 verwaltet werden können.

Diese Entwicklung hat dazu beigetragen, dass sich das Gerätemanagement des End-User Computings heute erheblich von der Situation noch vor einigen Jahren unterscheidet. Für das Management von mobilen Geräten, Windows-Desktops und -Laptops, Macs und virtuellen Desktops werden keine separaten Produkte benötigt, sondern alle Geräte können über eine einzige Plattform verwaltet werden.

Genau das ist das Prinzip von VMware Workspace ONE™, mit dem sich auch Chrome OS und robuste Geräte verwalten lassen. Workspace ONE kann sogar die Lücke zwischen Cloud und interner Umgebung schließen. Beispielsweise können VDI- und RDSH-basierte Desktops und Windows-Anwendungen mit VMware Horizon® intern im eigenen Rechenzentrum oder in Microsoft Azure, Amazon Web Services, IBM Cloud oder bei einem anderen bevorzugten Cloud-Anbieter ausgeführt werden. Die Horizon-Steuerungsebene kann auf Wunsch intern installiert und ausgeführt oder aber als Service abonniert werden. Der entscheidende Vorteil der Workspace ONE-Plattform ist, dass sie für alle Arten von Geräten und Endpunkten eingesetzt werden kann, und zwar unabhängig davon, um welche Geräte es sich handelt oder wo sie sich befinden.

Das Management sämtlicher Umgebungskomponenten mit einem einzigen Produkt wird als „einheitliches Endpunktmanagement“ (Unified Endpoint Management, UEM) bezeichnet und entwickelt sich zum De-facto-Standard in modernen Unternehmen. UEM ist jedoch nicht das Endziel, denn die End-User Computing-Umgebung besteht nicht nur aus Geräten. Die anderen wichtigen Komponenten sind Anwender und Anwendungen, da Anwender in der Lage sein müssen, sich an jedem Gerät anzumelden und auf Anwendungen zuzugreifen.

Einheitliches Endpunktmanagement (UEM) entwickelt sich zum De-facto-Standard in modernen Unternehmen. UEM ist jedoch nicht das Endziel, denn die End-User Computing-Umgebung besteht nicht nur aus Geräten.

Anmeldung und Zugriff werden von VMware Identity Manager™ verwaltet, einer Komponente von Workspace ONE, die Identity as a Service (IDaaS) bietet. VMware Identity Manager übernimmt das Anwendungs-Provisioning und stellt einen Self-Service-Anwendungskatalog, Kontrollen für bedingungsbasierten Zugriff und Single Sign-On (SSO) für alle Geräte und Anwendungen bereit. VMware Identity Manager verwaltet zudem die Anmeldung und Bereitstellung von cloudnativen, SaaS- und Webanwendungen, sodass diese Anwendungen zusammen mit Windows-, Mac-, iOS-, Android- und Chrome-Anwendungen in die EUC-Umgebung integriert werden können. (Und ebenso wie Horizon kann VMware Identity Manager entweder intern bereitgestellt oder als Cloud-Service abonniert werden.)

Mit VMware Workspace ONE und VMware Identity Manager kann die IT jede Anwendung für jeden Anwender auf jedem Gerät jederzeit und überall bereitstellen, verwalten und schützen. Das kann außer VMware bisher kein anderer Anbieter. (Wir reden hier von echten nativen Windows-Anwendungen auf Windows 10-Geräten, nativen Mac-Anwendungen auf MacOS-Geräten, nativen iOS-Anwendungen auf iOS-Geräten usw. Das hat nichts mit der alten Behauptung zu tun, dass alle Geräte unterstützt werden, um dann in einer peinlichen Fußnote die Einschränkung „in Form von Windows-Remote-Anwendungen“ folgen zu lassen.) Das Nirwana, nach dem wir seit den 90er Jahren suchen, wurde endlich Realität.

Aber das ist nur die Grundfunktion. Der wahre Wert zeigt sich, wenn Sie darüber nachdenken, welche Möglichkeiten Ihnen eine einzige Plattform für alle Geräte, alle Anwendungstypen und alle Anwender bietet.

Beispielsweise fasst VMware Workspace ONE Intelligence alle Kennzahlen und Aktivitäten von Workspace ONE-Geräten und VMware Identity Manager-Anwenderaktionen in einem einzigen, Cloud-basierten Datenpool zusammen, korreliert diese und gestattet der IT damit universellen Einblick in die EUC-Umgebung. Auf der Grundlage dieser Informationen können Dashboards, Reports, Analysen, Benachrichtigungen und automatisierte Workflows für alle Anwendungsgeräte und Gerätetypen und von allen Anwendern erstellt werden.

Workspace ONE Intelligence enthält eine Reihe von APIs und ein SDK, mit denen Dritte diese Funktionen erweitern können. Beispielsweise dehnt das Workspace ONE Trust Network die Transparenz von Anwendern, Anwendungen, Geräten und Netzwerken auf externe Sicherheitspartner wie Carbon Black, CrowdStrike, Cylance, Lookout, McAfee, Netskope und Symantec aus. Dadurch ist es ihnen möglich, Bedrohungsdaten im Rahmen von Workspace ONE aufzunehmen, zu verarbeiten, zu teilen und zu korrelieren, sodass ein umfassenderer Schutz als mit Punktlösungen erreicht wird.

Workspace ONE Intelligence umfasst außerdem eine Entscheidungs-Engine und leistungsstarke Automatisierungsfunktionen. (Zusätzlich zu allen Geräten, Anwendungen, Anwendern und Netzwerken, die ihre Daten an Workspace ONE Intelligence übertragen, kann Workspace ONE Intelligence auch Konfigurationsänderungen verteilen.)

Da Workspace ONE dank Konnektivität sämtliche Geräte-, Anwendungs- und Anwenderdaten einsehen kann, sind intelligente, kontextabhängige Aktionen möglich, die Anwendern einfacher und intuitiver als separate Anwendungen präsentiert werden.

Der Service „Workspace ONE Mobile Flows" kann beispielsweise mit jeder beliebigen Business-Anwendung verbunden werden, die über eine API verfügt. (VMware hat bereits Open Source-Konnektoren für beliebte Anwendungen wie Concur, GitHub, Jira, Salesforce und ServiceNow erstellt.) Dort können Entwickler kontextbasierte Aktionen und Benachrichtigungen von diesen Back-End-Systemen im VMware Boxer™-E-Mail-Client für iOS oder Android bereitstellen. Die Schaltfläche **Approve** oder **Deny** kann zum Beispiel direkt in eine E-Mail-Nachricht von Concur übertragen werden, sodass der Anwender schnell aktiv werden kann, ohne die E-Mail-Anwendung zu verlassen.

Mobile Flows mit Aktionskarten für E-Mail-Clients ist aber erst der Anfang. Man stelle sich nur vor, dass sich dieselben Aktionskarten, die so nützlich auf Desktops und Laptops sind, in native Anwendungen und das native Benachrichtigungs-Framework von Betriebssystemen integrieren lassen.

Es ist auch leicht vorstellbar, die verschiedenen Workspace ONE-SDKs und Mobile Flows um eine Sammlung von Mikroservices zu erweitern, die u.a. Authentifizierung, Inhalte, Personen, Genehmigungen, Benachrichtigungen und andere einfache Services verarbeiten. Dadurch wäre es Entwicklern möglich, eigene Anwendungen zu erstellen, die bereits vorhandene Business-Systeme, Inhalte und alle sonstigen Ressourcen, auf die Workspace ONE zugreifen kann, nutzen.

Es lässt sich unschwer erkennen, warum VMware Workspace ONE tatsächlich eine Plattform für digitale Arbeitsplätze ist, die weit über einheitliches Endpunktmanagement, Desktop-Virtualisierung und Mobilitätsmanagement hinausgeht. Durch die Kombination von Management und Kontrolle aller Geräteplattformen, nativen und Cloud-Anwendungen sowie der Anwenderidentität im Rahmen einer einzigen Plattform kann die IT bereits heute mit der Bereitstellung digitaler Arbeitsplätze beginnen, die in den kommenden zehn Jahren das End-User Computing prägen werden.

JETZT STARTEN

Weitere Informationen zur vereinfachten Windows-Bereitstellung >

VMware online:

Über den Autor

Brian Madden ist Technologe im VMware EUC CTO-Büro. Er ist seit mehr als 20 Jahren im Bereich EUC tätig. Er hat BrianMadden.com gegründet und die BriForum-Konferenzreihe ins Leben gerufen. Darüber hinaus hat er sechs Bücher über Desktop-Virtualisierung, VDI und DaaS geschrieben, Tausende von Artikeln und Blog-Beiträgen verfasst und Hunderte von Reden auf der ganzen Welt gehalten.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com Zweigniederlassung Deutschland Willy-Brandt-Platz 2 81829 München Telefon: +49 89 370 617 000 Fax: +49 89 370 617 333 www.vmware.com/de

Artikelnr.: EDW-0914_VM_Brian-Madden-Insights-From-Desktops-to-a-Digital-Workspace_WP_073118_DE
07/18