WHITE PAPER

BRIAN MADDEN INSIGHTS: FROM DESKTOPS TO A DIGITAL WORKSPACE

vmware®

Virtual Systems

From Desktops to a Digital Workspace

The first 20 years of "end-user computing" (EUC) were really about desktop computers sitting on users' desks. They were domain-joined and IT "owned" them (both literally and in terms of control). IT used tools like Microsoft Systems Management Server (SMS, a precursor to SCCM) to push out software and patches, collect inventories, and centrally manage them.

This model of computing worked well enough in most cases, though there was the occasional use case—like a client/server application that needed to be used across a slow WAN link—that necessitated the use of server-based computing (SBC), where a multiuser version of Windows Server would run in a data center and remotely deliver desktop and application sessions to users.

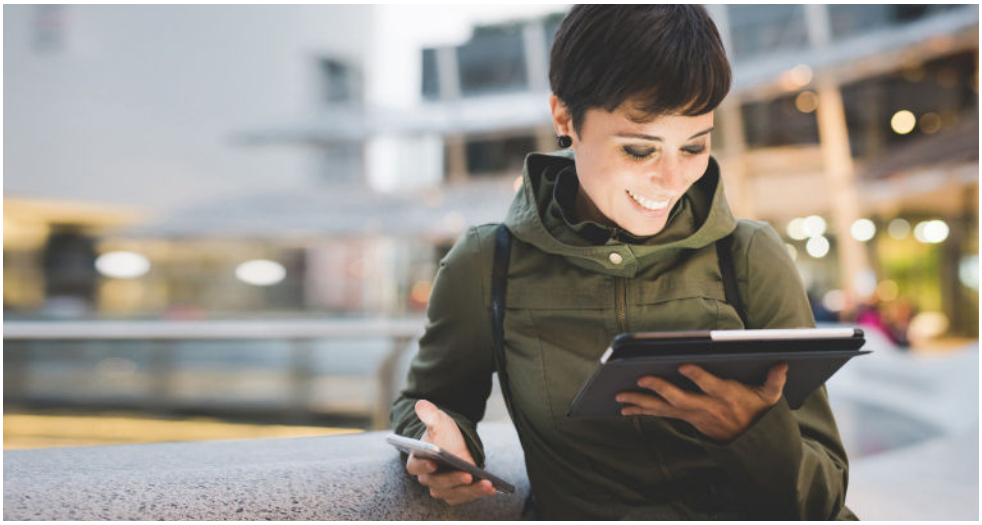
As technology evolved, virtualization became common, and VDI was created. VDI combined hardware virtualization with client versions of Windows, essentially delivering the benefits of SBC in a package that was more consistent with the way IT departments have been managing Windows desktops for a decade.

VDI and RDSH (the successor name of SBC) came to be collectively called "desktop virtualization." Everyone agreed that desktop virtualization had benefits over traditional desktops and laptops, including the potential for increased security, performance, and flexibility. The problem was that no matter how great the benefits of desktop virtualization were, the technology had a limited applicability. Many large organizations found they could easily virtualize 10–20 percent of their desktops, which was great, but that also meant that 80–90 percent of their desktops were not virtualized and had to be managed some other way.

This meant that organizations were now using at least two tools—one for their virtual desktops and another for their physical desktops—to completely manage, secure, and maintain their desktop environments. The physical desktop management tools had not evolved much from the SMS days of the 1990s. While the name had changed (from Microsoft SMS to SCCM), the tools were still built around the concept of domain-joined Windows desktops that maintained a network connection back to the data center.

Meanwhile, the iPhone and Android devices started to flood the scene. IT's initial response was to treat a mobile device just like a desktop, and the early MDM software did just that—essentially giving IT "full control" of a device, including the ability to remotely wipe the entire thing and to have visibility to users' personal content. Over time, MDM evolved into MAM and ultimately EMM—software that allows IT to manage the "work" portions of the device while allowing users to keep their personal stuff private.

One of the amazing things about EMM software is that a single IT administrator can manage a huge number of devices—sometimes this can be something like 10,000 devices per single EMM administrator. A single desktop administrator, on the other hand, can typically manage only 500 desktops.



This disparity was not lost on IT professionals, who demanded that Microsoft help them manage Windows desktops more like mobile devices: with simplicity, and, hopefully, the higher ratio of devices-to-administrators. Microsoft started to respond with Windows 8, and fully responded with Windows 10, via a set of capabilities Microsoft calls "Modern Management."

Put simply, Windows 10 modern management capabilities are a set of APIs that allow Windows 10 devices to be managed in similar ways and using the same tools as mobile devices. This allows corporate policies and configurations to be applied to Windows 10 devices—whether they're corporate-owned or user-owned—even for devices that are not domain-joined and not consistently attached to the corporate network.

Apple has added similar features to the macOS starting with the September 2017 "High Sierra" release, meaning that Apple laptops and desktops can be managed using the same tools as iOS, Android, and Windows 10 devices.

All this means that nowadays, the end-user computing device management landscape is much different than it was a few years ago. Rather than needing separate products to manage mobile devices, Windows desktops and laptops, Macs, and virtual desktops, a single platform can be used to manage them all.

This is what VMware is doing with VMware Workspace ONE,™ which also manages Chrome OS and rugged devices. Workspace ONE can even bridge the cloud and on-premises gap. For example, VDI and RDSH-based desktops and Windows apps, powered by VMware Horizon,® can run on-premises in your own data center, or on Microsoft Azure, Amazon Web Services, IBM cloud, or whatever other cloud provider you prefer. You can choose to have the Horizon control plane installed and running on-premises or you can subscribe to it as a service. The key is that the single Workspace ONE platform can be used for all types of devices and endpoints—regardless of what they are or where they live.

Using a single product to manage everything is referred to as "unified endpoint management" (UEM) and is becoming the de facto standard in the enterprise today. That said, UEM is not the end goal, because the end-user computing environment is more than just devices. The other major components are the users and the apps, since users need to be able to log in to any device and to access their applications.

Unified endpoint management (UEM) is becoming the de facto standard in the enterprise today. That said, UEM is not the end goal, because the end-user computing environment is more than just devices.

VMware achieves this with VMware Identity Manager,™ a component of Workspace ONE that provides Identity as a Service (IDaaS). VMware Identity Manager handles app provisioning, and provides a self-service app catalog, conditional access controls, and single sign-on (SSO) across all devices and apps. VMware Identity Manager also handles sign-on and provisioning of cloud-native, SaaS, and web apps, allowing those apps to be integrated into the EUC environment alongside Windows, Mac, iOS, Android, and Chrome apps. (And, like Horizon, VMware Identity Manager can be deployed on-premises or subscribed to as a cloud service.)

So, with VMware Workspace ONE and VMware Identity Manager, IT can deploy, manage, and secure any app to any user on any device from anywhere at any time. This is something that no one else can do today. (We're talking about actual native Windows apps on Windows 10 devices, native Mac apps on macOS devices, native iOS apps on iOS devices, and so on. This is not the tired old story of "we support all devices" with the awkward footnote "in the form of remote Windows apps.") The nirvana we've been seeking since the 1990s has been realized.

But all this is just the initial baseline functionality. The real value comes when you start thinking about all the additional things you can do when you have a single platform that handles all devices, all app types, and all users.

For example, VMware Workspace ONE Intelligence aggregates and correlates all the metrics and activities from Workspace ONE devices and VMware Identity Manager user actions into a single, cloud-based data lake that gives IT universal visibility into the EUC environment. This can be used to create dashboards, reports, analytics, notifications, and automated workflows across all app devices, all device types, and from all users.

Workspace ONE Intelligence includes a set of APIs and an SDK that allow third parties to extend this functionality. For example, the Workspace ONE Trust Network extends the visibility of users, apps, devices, and networks to third-party security partners, including Carbon Black, CrowdStrike, Cylance, Lookout, McAfee, Netskope, and Symantec. This will allow them to ingest, process, share, and correlate threat data with Workspace ONE in a way that allows for more complete protection than would be possible with point solutions.

Workspace ONE Intelligence also includes a decision engine and powerful automation capabilities. (In addition to all devices, apps, users, and networks pushing their data into Workspace ONE Intelligence, Workspace ONE Intelligence can also push configuration changes back down.)

Since Workspace ONE has connectivity and visibility into all device, app, and user data, it can be used to enable intelligent, context-aware actions that are presented to users in ways that are simpler and more intuitive than separate applications.

For example, the Workspace ONE Mobile Flows service can be connected into any business application that has an API. (VMware has pre-created open source connectors for popular apps like Concur, GitHub, Jira, Salesforce, and ServiceNow.) From there, developers can expose context-based actions and notifications from these back-end systems within the VMware Boxer™ email client for iOS or Android. For example, **Approve** or **Deny** buttons can be rendered directly into an email message from Concur, allowing the user to quickly take action without leaving the email app.

Mobile Flows exposing action cards into email clients is just the beginning. You can imagine the same action cards having value from desktops and laptops, and integrating with native apps and OSs' native notifications framework.

It's also easy to imagine extending the various Workspace ONE SDKs and Mobile Flows with a collection of microservices that could handle things like authentication, content, people, approvals, notifications, and other simple services. This would allow developers to build their own apps that leverage existing business systems, content, and everything else Workspace ONE has access to.

Putting all this together, it's easy to see why VMware Workspace ONE is a true digital workspace platform that is much more than just unified endpoint management, desktop virtualization, or mobility management. By combining the management and control of all device platforms, native and cloud apps, and user identity into a single platform, IT can begin delivering the digital workspace today that will lead the way for the next 10 years of end-user computing.

GET STARTED TODAY

Learn more about simplifying Windows delivery >

Join Us Online:

About the Author

Brian Madden is a technologist in the VMware EUC CTO office. Brian has been in the EUC industry for more than 20 years. He founded BrianMadden.com and created the BriForum conference series. He has also authored six books about desktop virtualization, VDI, and DaaS, thousands of articles and blog posts, and has given hundreds of speeches around the world.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com