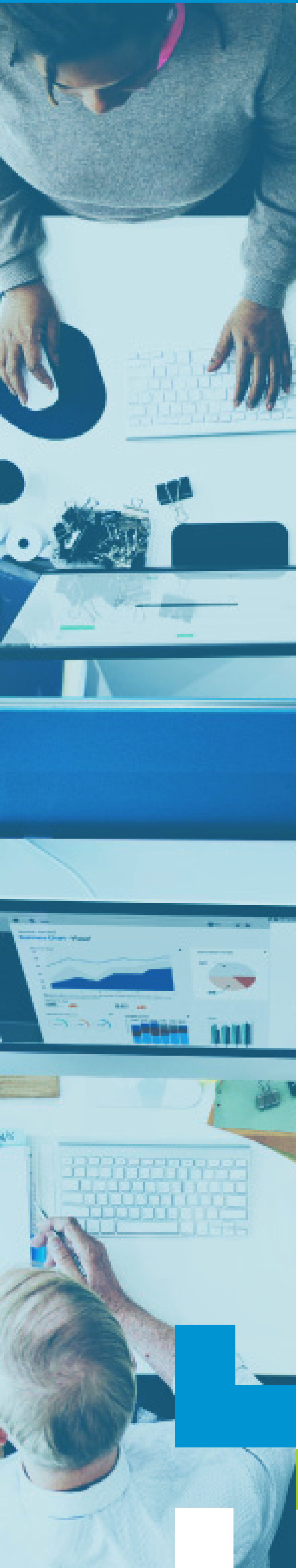
Unified Endpoint Management: the Next Step in the Evolution of Device Management

vmware® airwatch®

CIO
Strategic Marketing Services



First came MDM, then EMM. Now, if you aren’t looking at the world of Unified Endpoint Management, you're falling behind.

Mobile device management (MDM) tools allow companies to connect their employees securely to basic corporate network resources. Enterprise mobility management (EMM) goes a step further by enabling secure mobile versions of business-critical applications and data loss prevention to protect corporate information. But in today's workplace, employees and businesses deal with a vast variety of devices with different operating systems and form factors, from PCs and laptops, to tablets and smartphones, and now, increasingly wearables and Internet of Things (IoT) endpoints. IT has to integrate this heterogeneous mix of devices into critical business operations, secure them from unauthorized use, and manage them so end users enjoy a consistent, productive experience no matter how or where they access the digital workspace. The answer is unified endpoint management (UEM), which enables organizations to take a consistent approach to manage and secure every endpoint, any app and content, and across deployment use cases from a single holistic platform. AirWatch is the first leading platform to unify these endpoints together and the benefits organizations are seeing is tremendous.

The Evolution of Device Management

As soon as the first smartphone hit the market, the bar for productivity and flexibility was raised. Consumers began to take smartphones into their workplace along with heightened expectations of flexibility and productivity. MDM developed as a response to that demand, giving companies a way to configure mobile devices and control their security settings remotely. At first, the functionality was limited to basic resources like email and calendars, but as business-relevant apps grew more sophisticated, EMM evolved to support organizations in giving employees easy, secure mobile access to everything from files to databases to business-critical applications. As organizations began to pursue mobility, new barriers emerged, challenging ITs ability to deliver effective solutions.

Let's face it, mobile operating systems are on the rise and allowing more work to be done on smartphones, but PCs are not going away and still a preferred choice for many knowledge worker tasks. To make things worse, the mobile and desktop interfaces and software differ so significantly that organizations struggle to deliver a consistent end-user experience. All too often, employees face a frustrating process of familiarizing themselves with multiple ways of accessing their work applications, because it can greatly differ across their phone and laptop devices.

Furthermore, the proliferation of devices and operating systems poses an ongoing challenge to IT teams. IT is under relentless pressure to support Windows 10 and Mac laptops, Chromebook notebooks, and Android and iOS mobile devices, and to change configurations and settings fast enough to keep pace with every new device or software release. The more types of devices IT needs to support, the greater the pressure grows.

Finally, IT has traditionally used one set of tools to manage mobile devices and another to manage laptops and desktops. IT needs yet more tools to manage legacy devices, virtual endpoints, wearables, IoT devices and sensors, and so forth. At best, the resulting silos lead to costly, time-consuming duplications of effort. At worst, they create risky inconsistencies and gaps in configurations and security policies.

The Rise of UEM

UEM emerged as a way to address these pain points by extending the concepts of MDM and EMM beyond smartphones and tablets. UEM became a reality with the release of Windows 10, which allowed IT to manage desktops and laptops over the air in the same way we've become accustomed to managing mobile devices. However, UEM is platform-independent by design. It provides a universal platform for managing every device and every operating system across any organizational use case. This ensures that end users have the same consistent experience regardless of what device they use to access the corporate environment.

UEM is user-centric. It allows IT to control and personalize access to specific applications and content based on business processes and business roles, usage history, and context, regardless of whether the device itself is owned by the user or the company. Tying endpoint management to the user rather than the device also simplifies self-service and automatic provisioning.

UEM also allows more granular rules-based device management by location and time. For example, it can push out new configurations only to devices on a specific network, allow only devices in a particular building to use certain applications and data, or shut off network access to certain employees' devices after a certain amount of time to limit the amount of overtime they can accrue.

UEM reduces IT overhead and minimizes potential points of failure. It consolidates the number of management tools in use and limits the amount of integration between device management and back-end systems such as cloud-based applications and virtual private networks. It also minimizes the need to track vendor-service level agreements and product updates, since everything passes through the unified platform. Moreover, UEM consolidates the many processes an IT team needs to learn and follow to successfully support a large, growing, and heterogeneous inventory of devices and operating systems.

“Organizations are spending an average of $7,000 per endpoint per year for a managed PC,” says Blake Brannon, Vice President of Product Marketing for leading enterprise mobility management vendor, VMware AirWatch. "By consolidating your endpoint management operations in a single, consistent platform, UEM can reduce that cost by 30 percent and in some cases more."

"UEM lets organizations introduce rapid, automatic, self-service and on-demand capabilities."

In addition, UEM lets organizations introduce rapid, automatic, self-service and on-demand capabilities for IT. Instead of going through an expensive onboarding process, IT can do a simpler and cheaper provisioning that minimizes a lot of pre-employee-handover steps. IT can push out all the necessary configurations and software via a secure connection to any Wi-Fi network, wherever the employee happens to be. Today's employees expect to unbox a new smartphone, set it up, and be ready to start using it in just a few minutes. Why shouldn't they be able to do that with their work laptop as well? And when the employee leaves, the company can simply wipe and re-provision the device in just a few minutes and hand it to the next employee.

UEM eliminates the disjointed user experience by ensuring that applications and business processes look and function the same, regardless of the endpoint on which end users access them. This allows users to focus on working in whatever way is most convenient for them — which, in turn, drives up application adoption, improves end-user engagement, and ultimately boosts productivity.

By using UEM to automate manual processes, businesses can also realize enormous efficiency gains and even transform their day-to-day operations. A service organization could convert huge paper manuals to digital documents that are easy to carry, search, and share via mobile device. Or a vendor could push out the configurations on a retail kiosk on a daily basis to promote local events. Finally, UEM enables business possibilities

that organizations previously couldn't consider. By bringing IoT devices such as smart glasses and other wearables under a larger management umbrella, it makes adoption of those technologies at scale far easier and faster.

Managing Every Endpoint Across the Lifecycle

The operative word in true Unified Endpoint Management is "unified" — that is, the ability to manage all endpoints from a single platform, regardless of type, user, or use case. It's not enough to be able to manage both Android and iOS, or both Windows and macOS. UEM must be able to scale to include all endpoints, from traditional PCs to modern IoT devices and wearables. Moreover, true UEM needs to function throughout the device lifecycle. When a device first connects to the corporate network, the rules and roles associated with the user's login should trigger the UEM system to launch a seamless onboarding process that automatically installs and configures all appropriate corporate resources and applications. Thereafter, the UEM system should continuously and automatically apply security policies and other relevant business rules and provide authorized users and devices context-driven access to apps and resources. It should also allow IT to provide remote troubleshooting and support, both through proactive monitoring, and in response to end user requests. Finally, when the employee leaves the company or the device is lost, stolen, or retired, UEM should be able to remove all sensitive data from the device and, if necessary, block it from connecting to corporate resources in the future.

UEM does this by extending modern MDM features across all operating systems, every platform maker, and every OEM manufacturer to create a comprehensive IT platform and massive ecosystem of devices and automated tasks the tool can control. A layer of orchestration technology calls and integrates other business systems to push more configuration, control, and security rules to devices. This allows the technology to apply something as abstract as a 802.1X security policy and certificate rotation schedule to every device that might have corporate data on it, from a desktop PC to a smart television in a conference room.

When the UEM platform is provided in the cloud as a service, a company points all of its endpoints to the platform to generate a single dashboard via a browser-based interface that allows it to configure and push out policies and configurations on an individual, group, or company-wide basis.

The browser-based "single pane of glass" includes wizards and screens for manual tasks such as updating and assigning policies or locating individual devices for support or configuration. It also includes automated tasks that draw on other back-end systems to. For example, wipe corporate information from an employee-owned device on the employee's final day or reset that person's corporate-owned laptop for the next user. Role-based contextual dashboards and access controls determine who gets to see and change specific information, from basic configurations at the help desk level to enterprise-wide statistics for IT management.

True Cross-Device Management

The most basic use case for UEM is integrating the management of laptops and mobile devices on a single platform. For many companies, this is also the end goal: a network of Apple, Microsoft, and Google laptops, phones, and tablets operating together to deliver the same consistent, secure experience to employees wherever and whenever they log in.

Increasingly, companies are pushing the boundaries of device management by extending UEM to include other devices, such as vending machines, information kiosks, smart glasses and ruggedized devices for fieldwork and factory floors. By looking beyond knowledge workers to any device used by any employee, organizations can keep an even closer eye on their overall operations.

The Home Depot, for example, has equipped employees in its U.S. stores with a device called the First Phone which combines phone, push-to-talk, and mobile computing functionality. It's equipped with custom line-of-business apps that help employees perform tasks like managing inventory, checking product prices and availability, and completing transactions away from cash registers.

When The Home Depot introduced the latest generation of First Phone, it used AirWatch to onboard all the devices at a central staging facility, then shipped the devices to hundreds of stores a week and remotely configured the applications needed on each one by location. It took the company just a few months to roll out hundreds of thousands of these devices nationwide.

As the Internet of Things expands, UEM will become increasingly important. The more previously "dumb" items become IP-enabled, the more important it will be to manage them, not just for security, but for productivity. Coca-Cola, for example, manages its Freestyle Internet-connected soda dispensing machines with the same platform and in the same ways that it manages other networked devices. UEM lets the company track usage, proactively ship refills of flavor cartridges, and push out software updates that cover everything from pump calibration to new combinations of flavors.

"We migrated more than 30,000 dispensers in the field from old technology to AirWatch," says Chris Dennis, global director of product management for Coca-Cola Freestyle. "We now have a lot more real-time visibility into what's going on, but more than that...we're building profiles for every dispenser and getting to the point where every dispenser in the field can be different."

Conclusion: Accelerating the Move to UEM

UEM is clearly the future for device management, and VMware AirWatch is leading the move to UEM. Unlike vendors whose UEM solutions emerged from a particular OS platform, AirWatch originated in the mobile era of platform heterogeneity, self-service, cloud technology, and it remains vendor-agnostic. It integrates endpoints, configurations, and controls from Apple, Google, Microsoft, Samsung, Zebra, Honeywell, Bluebird and a host of lesser-known hardware and software manufacturers with tools that enable complete lifecycle management and support multiple use cases with management, automation, and self-service tools. AirWatch also provides technologies and services to help organizations migrate to its UEM platform. In addition to consolidation and migration support for organizations currently using other mobile management tools, AirWatch offers a comprehensive Windows 10 solution that assesses a company's current Windows environment, determines the optimal migration path via virtual desktop delivery or physical upgrade, and implements Windows 10 as an initial step toward broader OS and application lifecycle management.

Brannon predicts that as more organizations move to UEM, they will begin to reap additional benefits by tying endpoints together into a business intelligence engine that they can use to better analyze and understand user behaviors and device usage. This will create opportunities to boost user productivity, perform predictive maintenance, and implement intelligent security and threat analysis.

"We migrated more than 30,000 dispensers in the field from old technology to AirWatch"

To learn more about the AirWatch offering and UEM, **visit the website.**

vmware airwatch

CIO
Strategic Marketing Services