Top 4 Unified Endpoint Management Software Vendors in 2024

TechTarget

In this handbook:

Top 4 Unified Endpoint Management Software Vendors in 2024

BRIEN POSEY, MICROSOFT MVP

Unified endpoint management (UEM) products have become necessary in nearly all larger organizations as they incorporate more types of endpoints into their workflows.

While the capabilities vary from one product to the next, UEM products allow organizations to manage and secure various device types, even if those devices are running different operating systems. Explore the four leading UEM products of 2024, chosen for their popularity and appearance in rating reports from Gartner and similar market studies. This list is not ranked and instead appears in alphabetical order.

Compare key UEM tool features and capabilities

When choosing a UEM product, there are several important factors to consider.

- **OS support.** One of the most important considerations is what OSes the tool supports. A UEM product will only be useful if it supports the devices and operating systems the organization uses. If, for example, an organization uses

In this handbook:

Windows PCs and Google Android phones, then the chosen UEM tool needs Windows and Android management capabilities.

- **Security and privacy.** The product's security and privacy features are critical factors to consider. Nearly all UEM products keep managed devices secure, but the actual security capabilities vary from one UEM product to another.
- **Device management and lifecycle.** It's also worth considering a UEM product's device management capabilities. Most UEM products provide a consolidated dashboard, but the similarities end there. As such, it is worth considering the ease with which a UEM product allows IT to manage the registered devices.
- **App and software management.** Most UEM products allow IT to deploy apps to managed devices. However, not all UEM tools support all types of applications.
- **Deployment and enrollment.** Before a UEM product can manage a device, that device needs to be enrolled. IT should closely examine what's involved with the enrollment process, as users will likely register their own devices.
- **Identity and access management (IAM).** Organizations should consider whether a product relies on its own proprietary identity provider or if it can integrate with the existing directory service. It's also important to consider whether a product supports role-based access control (RBAC) and the granularity of permissions.
- **Pricing.** It's important to know what a UEM product costs. UEM tools are typically subscription-based, but ancillary products may be required to realize a UEM product's full potential.

1. IBM Security MaaS360

IBM Security MaaS360 with Watson helps secure and manage various device types, from desktops to wearables. MaaS360 heavily emphasizes helping organizations with their bring your own device (BYOD) efforts. It also uses AI to detect and surface actionable insights.

SUPPORTED OSES

IBM's list of supported operating systems includes the following:

- Apple iOS, macOS and iPadOS.
- Google Android and ChromeOS.
- Microsoft Windows.
- Various ruggedized, wearable and IoT devices.

SECURITY AND PRIVACY

MaaS360 uses an AI-powered tool to identify and generate security insights and detect and remediate threats such as malware, risky device configuration settings and malicious apps. It can also detect when an end-user device has been jailbroken or rooted.

DEVICE MANAGEMENT AND LIFECYCLE

IBM Security MaaS360 is a cloud-based SaaS tool for managing endpoint devices. Like other UEM offerings, MaaS360 provides a dashboard that allows various devices to be managed side by side through a single pane of glass interface.

APP AND SOFTWARE MANAGEMENT

IT can use MaaS360 to create an app catalog to deploy apps to managed devices. The supported app types include the following:

- Internal applications are applications the organization develops for internal use.
- Purchased applications are applications bought from an app store for the organization's use.
- Public apps are those listed in a public app store.

DEPLOYMENT AND ENROLLMENT

IBM Security MaaS360 supports several common types of device enrollment. These include Apple Business Manager, Apple School Manager, Apple Device Enrollment Program (DEP), Android Zero Touch and Samsung KME.

IDENTITY AND ACCESS MANAGEMENT

MaaS360 works with IBM Security Verify, IBM's IAM service, with options for single sign-on (SSO) and conditional access management.

PRICING

IBM uses subscription-based pricing for its MaaS360 software. In addition to a 30-day free trial, the company offers four different pricing plans, each charged per device, per month. The Essentials plan starts at $4, with the price increasing to $5 for the Deluxe plan. IBM's Premier plan starts at $6.25, and the Enterprise plan sells for $9.

2. Ivanti UEM

Ivanti UEM is designed to help organizations with a diverse collection of devices operate at scale. The software allows IT to perform management actions such as policy enforcement or software deployment across many devices with a few clicks. The right reporting capabilities can help admins more easily spot issues needing their attention.

SUPPORTED OSES

Ivanti's ability to manage a device depends on the availability of a management agent for the device's operating system. Ivanti has a long list of supported operating systems but broadly covers the following platforms:

- Apple iOS and macOS.
- Google Android and ChromeOS.
- Microsoft Windows.
- Linux.
- Rugged devices.

SECURITY AND PRIVACY

Ivanti delivers endpoint security through Ivanti Endpoint Security, which is licensed separately. While Ivanti Endpoint Security is probably best known for its patch management and antivirus capabilities, it can do much more. For example, the software can prevent unauthorized applications from running on devices and can even prevent the use of removable media.

It is also worth noting that Ivanti has another tool for protecting mobile devices. Ivanti Neurons for Mobile Threat Defense guards against zero-day threats and protects against more common threats such as phishing attacks and malicious URLs.

DEVICE MANAGEMENT AND LIFECYCLE

Ivanti's preferred tool for device management is Ivanti Endpoint Manager. It provides a single view that shows all managed devices, regardless of type, OS migrations, patch management, software deployment and other similar tasks. The dashboard also includes rich reporting capabilities and a remote control feature that can control remote device troubleshooting.

APP AND SOFTWARE MANAGEMENT

The Ivanti UEM platform deploys AppConnect apps to managed devices. AppConnect apps are containerized apps packaged using the AppConnect SDK, AppConnect Cordova Plugin or App Wrapper for iOS and Android.

DEPLOYMENT AND ENROLLMENT

Ivanti supports common device enrollment types, including Apple's Automated DEP, Google Zero Touch and Samsung Knox Mobile Enrollment. Additionally, Ivanti allows its customers to restrict devices based on enrollment type.

IDENTITY AND ACCESS MANAGEMENT

Ivanti regulates access to its software by using RBAC, which Ivanti refers to as role-based administration. Ivanti allows IT to create custom roles that can restrict administrators based on factors such as geographic location or department. While the software does allow for using local users and groups on Windows machines, IT can also configure it to work with Active Directory users and groups.

PRICING

Ivanti uses a subscription-based licensing model with three plans available -- Secure UEM Professional, Secure UEM Professional Plus and Secure UEM Premium -- but requires potential customers to contact its sales department for a quote. Ivanti is known for an a la carte pricing model, where the overall licensing cost is determined by what tools and features are needed.

3. Microsoft Intune

Intune is Microsoft's cloud-based UEM platform that allows organizations to manage corporate and personally owned devices of various types. Admins can use Intune to apply security policies to devices and manage the apps installed on devices.

SUPPORTED OS PLATFORMS

Microsoft Intune supports a wide range of device operating systems, including the following:

- Apple iOS, macOS and iPadOS.
- Google Android and ChromeOS.
- Microsoft Windows.
- Linux.

SECURITY AND PRIVACY

Microsoft Intune contains an Endpoint Security node that serves as a collection of tools for device security. These tools can check the status of devices or configure devices based on established security baselines. These baselines are collections of security best practices that IT can apply as a policy to devices. The Endpoint Security node can also apply tightly focused policies to devices -- such as antivirus policies and encryption policies. Additionally, these tools allow admins to set user and device requirements through a compliance policy.

DEVICE MANAGEMENT AND LIFECYCLE

Like other UEM tools, Intune provides a consolidated view of managed devices, regardless of type. The management console allows IT to perform various management actions, such as synchronizing the device, resetting its passcode or performing a remote wipe. Notably, some of the available device actions are device-type specific.

APP AND SOFTWARE MANAGEMENT

Microsoft Intune works with five different types of apps. These include apps from the app store, custom apps, built-in apps, web apps and apps from other Microsoft services.

Additionally, numerous Microsoft apps and apps from Microsoft partners are considered Intune-protected apps. IT can apply an even greater level of security to these apps through mobile application protection policies.

DEPLOYMENT AND ENROLLMENT

Microsoft Intune supports several different types of device enrollments. These include Android Zero Touch, Apple Business Manager, Apple School Manager and Apple DEP.

IDENTITY AND ACCESS MANAGEMENT

Microsoft Intune is designed to work with Active Directory and Azure Active Directory and therefore recognizes Active Directory users and groups. Access to Microsoft Intune is provided through RBAC. And while IT can define custom roles, nine built-in roles provide various levels of access.

PRICING MODEL

Microsoft Intune is subscription-based, but Microsoft's licensing options for Intune are somewhat complex. Intune is currently offered in three plans -- Plan 1, Plan 2 and Intune Suite -- with Plan 2 and Intune Suite acting as add-ons to Intune Plan 1 with additional subscription fees. Additionally, Intune is bundled and included in several of Microsoft's other subscription plans, such as Microsoft 365 (E3, E5, F1, F3, A3, A5, G3, G5 and Business Premium) and Enterprise Mobility + Security (E3 and E5).

Microsoft also offers Intune user and device licenses as a standalone subscription. The company also offers device-only licenses, which are useful for managing shared devices not associated with a specific user. Additionally, Microsoft offers remote help capabilities as a premium add-on. Remote Help allows an organization's help desk to troubleshoot managed devices remotely.

4. VMware Workspace One

VMware Workspace One is a UEM tool for managing devices and the apps running on them, regardless of where those devices reside. Workspace One also has security features that make it easy to identify devices that do not comply with an organization's security policies.

SUPPORTED OSES

VMware provides a long and highly version-specific list of supported platforms. The supported operating systems include the following:

- Apple iOS and macOS.
- Google Android and ChromeOS.
- Linux.
- Microsoft Windows.
- Rugged devices.

SECURITY AND PRIVACY

VMware has designed Workspace One to provide a foundation for zero-trust security. In addition to enabling end-to-end security across devices, users and apps, VMware supports conditional access and generates machine learning based on insights and automations.

DEVICE MANAGEMENT AND LIFECYCLE

Like other UEM tools, Workspace One uses a single pane of glass interface to manage devices. This dashboard makes it easy to identify devices suffering from a particular problem. For example, the dashboard shows compromised devices, devices with no passcode and devices that are not encrypted.

APP AND SOFTWARE MANAGEMENT

VMware's tools can manage various application types on managed devices, including internal, purchased and public apps.

DEPLOYMENT AND ENROLLMENT

VMware Workspace One supports several different enrollment workflows. For example, there are two main options for mobile devices. The first option is for users to download the Workspace One Intelligent Hub app from the Android, iOS or Windows app store and then use the app to complete enrollment. The second is an email-based autodiscovery process that completes the enrollment by directing the user to a self-service portal.

IDENTITY AND ACCESS MANAGEMENT

Like other UEM products, VMware Workspace One uses RBAC to manage administrative access. VMware supplies three predefined administrative roles -- super administrator, read-only administrator and directory administrator. These roles cannot be modified or deleted, but VMware does allow organizations to create custom roles.

PRICING

VMware offers Workspace One on a subscription basis, with seven different subscription plans available. There are four Essentials plans -- Employee, Mobile, Desktop and UEM -- that are each meant for a specific use case. For example, UEM

Essentials is geared toward mobile endpoint management and lacks some capabilities found in other Workspace One packages. The three remaining licenses are Standard, Advanced and Enterprise suites, and the total cost is based on the number of devices or user licenses and bills monthly. VMware's Enterprise Suite is the priciest option and costs $10 per device or $15 per user, per month.

Brien Posey is a 15-time Microsoft MVP with two decades of IT experience. He has served as a lead network engineer for the U.S. Department of Defense and as a network administrator for some of the largest insurance companies in America.