The Forrester Wave™: Unified Endpoint Management, Q4 2018

The 12 Providers That Matter Most And How They Stack Up

November 20, 2018

By Andrew Hewitt, **Chris Sherman** with Christopher Voce , Robert Perdoni , Diane Lynch

Why Read This Report

In our 28-criterion evaluation of unified endpoint management (UEM) providers, we identified the 12 most significant ones — BlackBerry, Cisco, Citrix Systems, IBM, Ivanti, Jamf, Kaspersky Lab, Matrix42, Microsoft, MobileIron, Sophos, and VMware — and researched, analyzed, and scored them. This report shows how each provider measures up and helps infrastructure and operations (I&O) professionals make the right choice.

Key Takeaways

VMware, MobileIron, IBM, Microsoft, And Citrix Systems Lead The Pack

Forrester's research uncovered a market in which VMware, MobileIron, IBM, Microsoft, and Citrix Systems are Leaders; Sophos, BlackBerry, and Matrix42 are Strong Performers; Ivanti, Jamf, and Cisco are Contenders; and Kaspersky Lab is a Challenger.

I&O Pros Are Looking For Comprehensive Management And Security Across All OSes

The UEM market is growing because more I&O professionals see UEM as a way to consolidate and modernize their approach to endpoint management and security. I&O pros increasingly see UEM providers as partners in helping them provide a better experience for employees while maintaining security and compliance.

OS Support, Identity, And Threat Detection Are Key Differentiators

As employees continue to adopt a greater set of devices and apps, user-focused management and security capabilities become differentiators. Vendors that can provide management, identity, and threat capabilities across a broad set of employee devices and apps position themselves to successfully deliver secure, user-friendly UEM experiences to their customers.

UEM IS A CRITICAL TOOL TO BALANCE EMPLOYEE EXPERIENCE AND SECURITY

Providing a great technology experience for employees requires anytime, anywhere access to task-critical information on whatever device or application they prefer. Today, nearly one in five global information workers uses at least three devices per week to complete their work, but I&O teams frequently employ separate tools to manage and secure these devices: enterprise mobile management (EMM) for mobile devices and

client management tools (CMTs) for PCs. (see endnote 1) Over the past year, these two siloed management systems have come together to form the UEM market. Forrester defines UEM as:

Products that provide a centralized policy engine for managing and securing employee laptops and mobile devices from a single console.

Driven by Microsoft's simplification of Windows 10 management, 47% of global infrastructure technology decision makers say they're implementing, have implemented, or are expanding/upgrading implementation of UEM (see Figure 1). (see endnote 2) Why? UEM helps companies:

- **Support a better employee experience (EX).** A great employee experience hinges on employees' ability to get work done every day — and their technology has an outsized impact. (see endnote 3) I&O teams frequently use UEM to grant access to enterprise resources to employees off the company network, whether through granular policy control on devices and apps or through contextual authentication capabilities that deliver access based on a variety of criteria (i.e., conditional access). UEM is also a critical capability for delivering PC and mobile applications to users, often via a self-service enterprise app store or through automation capabilities such as Google's Zero Touch Provisioning or Windows Autopilot. (see endnote 4)

- **Maintain security and compliance.** While technology teams must provide better employee experiences, they must also protect their businesses. In addition to providing a common baseline of device protections through mobile device management (MDM) profiles, UEM offers I&O teams a unified approach to prevent, detect, and respond to security threats on mobile and PC endpoints. Data-centric protections such as full-disk encryption (FDE), secure sharing tools, or data loss prevention controls provide an additional layer of security. We've often seen clients deploy UEM for compliance reasons, such as improving audit readiness, easing access to device usage telemetry, or ensuring proper separation of work and personal data for privacy considerations.

Figure 1: Windows 10 Enhancements Drive The Move Toward UEM

Today's Leading UEM Providers Differentiate Themselves In Four Ways

This Forrester Wave™ evaluation reveals four key differentiators in the UEM market. Today's leading vendors:

- **Support both traditional and modern management techniques.** Leading UEM providers enable customers to move to cloud-based, modern management practices at a comfortable pace. While they offer traditional capabilities for PC and mobile (such as patching, software distribution, and mobile OS containerization), they also support modern approaches that leverage MDM APIs, automation, and conditional access. In addition, they provide a path to help customers make the transition from traditional to modern management with tools such as automated PC life-cycle migration, peer-to-peer (P2P) distribution, and application compatibility testing for Windows 10.

- **Offer contextual identity and access management (IAM).** Conditional access and risk-based authentication (RBA) methods improve security and user experience. While most UEM providers support conditional access based on one or two criteria like device posture, leading vendors have greater breadth and look at additional variables, such as location, network risk, and user behavior. If a user's context doesn't meet certain criteria, the solution can require multifactor authentication (MFA) for access. RBA uses machine learning algorithms to assign a risk score to employees and dynamically adjust their access levels based on the level of risk. Both of these approaches increase security without sacrificing end user productivity.

- **Use analytics to help guide decision making.** UEM tools typically collect abundant device usage and behavioral data. Leading solutions then apply analytics to this data to build more context around alerts to inform admins about potential operational or security issues. Some go even further and suggest potential remediation actions or policy changes, such as blocking a compromised device from accessing the corporate network or updating a vulnerable application to protect it from an active exploit seen in the wild. This requires integration with external sources of intelligence to learn from other environments and prevent potential issues early on. Vendors typically conduct most of this analysis automatically, with policies to dictate when remediation actions can automatically happen without admin input.

- **Serve the needs of highly regulated customers.** Some industries have unique compliance needs that will dictate which UEM solutions will end up on their shortlists. Leading vendors will have multiple certifications that give them the flexibility for deployment in a number of environments, such as Common Criteria MDM V2, ISO 2700, and FedRAMP. Highly risk-adverse organizations and federal agencies also expect multitenant options for cloud-based management consoles and features such as derived credentials to replace traditional smart card authentication solutions to achieve a better balance between security and usability.

UNIFIED ENDPOINT MANAGEMENT EVALUATION OVERVIEW

To assess the state of the UEM market and see how the vendors stack up against each other, Forrester evaluated the strengths and weaknesses of top UEM vendors. After examining past research, user need assessments, and vendor interviews, we developed a comprehensive set of evaluation criteria. We evaluated vendors against 28 criteria, which we grouped into three high-level categories:

- **Current offering.** Each vendor's position on the vertical axis of the Forrester Wave graphic indicates the strength of its current offering. Key criteria for these solutions include OS support, update management, enterprise app store, application security, data security, network security, IAM, privacy, analytics, management console, and certifications.

- **Strategy.** Placement on the horizontal axis indicates the strength of the vendors' strategies. We evaluated product vision, road map execution, revenue growth, commitment to innovation, supporting products and services, and partner ecosystem.

- **Market presence.** Represented by the size of the markers on the graphic, our market presence scores reflect each vendor's customer count, devices under management, and revenue.

Evaluated Vendors And Inclusion Criteria

Forrester included 12 vendors in the assessment: BlackBerry, Cisco, Citrix Systems, IBM, Ivanti, Jamf, Kaspersky Lab, Matrix42, Microsoft, MobileIron, Sophos, and VMware (see Figure 2). Each of these vendors:

- **Meets revenue and general availability requirements.** Evaluated vendors have at least $50 million in annual revenue from the UEM product. The product had to be generally available on October 1, 2018. We didn't factor any functionality added after this date into this evaluation.

- **Had the ability to provide customer references.** We asked evaluated vendors to supply three customer references that are using the UEM product, at least one of which is using the product for both mobile and PC management and one of which is using UEM to displace traditional endpoint security functionality (e.g., antivirus).

- **Supports both mobile and desktop endpoints.** Each vendor in the evaluation can enroll and set policy for both mobile (Android or iOS) and desktop (Windows 10 or macOS) devices.

- **Has mindshare among Forrester's enterprise clients.** These offerings appear frequently in Forrester client inquiries, shortlists, consulting projects, and case studies.

Figure 2: Evaluated Vendors And Product Information

VENDOR PROFILES

We intend this evaluation of the UEM market to be a starting point only and encourage clients to view detailed product evaluations and adapt criteria weightings to fit their individual needs through the Forrester Wave Excel-based vendor comparison tool (see Figure 3 and see Figure 4). Click the link at the beginning of this report on Forrester.com to download the tool.

Figure 3: Forrester Wave™: Unified Endpoint Management, Q4 2018

Figure 4: Forrester Wave™: Unified Endpoint Management Scorecard, Q4 2018

Leaders

- **VMware combines UEM with strong identity and digital workspace capabilities.**Over the past year, VMware has invested heavily in helping customers embrace modern management for Windows 10 with its Workspace ONE product. The solution's differentiated AirLift feature automates migration of SCCM collections, devices, and app packages to Workspace ONE. It excels in IAM, with features like single sign-on (SSO) to the Workspace ONE app and support for dozens of conditional access policies. This vendor continues to satisfy the needs of regulated customers by achieving high levels of security certifications and offering capabilities like Derived Credentials. Workspace ONE doesn't yet support behavioral analytics for anomaly detection, and customers cited frustrations with the complexity of VMware's licensing.

- **MobileIron's UEM solution is a good fit for highly regulated customers.** MobileIron's Unified Endpoint Management offering includes several security and compliance certifications, such as Common Criteria MDM PP V2, FedRAMP, and NIAP Protection Profiles, which has enabled it to win several

large US government customers in the past year. MobileIron has a fully integrated mobile threat solution that uses machine learning algorithms to detect device, network, and application-level attacks without requiring the device to have network connectivity. The solution's Access product also includes a newly released Authenticator app that enables passwordless authentication to cloud services. MobileIron's macOS management and analytics capabilities are not as advanced as some of the other solutions in this evaluation.

- **IBM's MaaS360 is the only fully cloud solution to offer PCLM and modern APIs.** The solution offers deep management and application delivery capabilities across a wide variety of endpoints, notably ChromeOS and Windows 7. IBM has also integrated IAM capabilities into the platform, with support for risk-based authentication, Derived Credentials, and third-party identity provider (IdP) integration with OKTA, Ping, and others. MaaS360 embeds IBM Trusteer to offer threat prevention, giving customers support for threat prevention and behavioral analysis. It has robust industry and use case wizards to help customers with UEM policy generation and can surface actionable insights from anonymized customer data and third-party sources to improve user experience or security posture. The solution lacks capabilities for P2P distribution on Windows 10 and has less mature file and data-level security capabilities than others in this evaluation.

- **Microsoft offers a path for customers to embrace modern management using Azure.** Enterprise Mobility + Security (EMS) is a bundle of Microsoft products that includes Advanced Threat Analytics, Azure AD Premium, Azure Information Protection, Cloud App Security, Intune, and System Center Configuration Manager (ConfigMgr). Microsoft's release of co-management in late 2017 has bolstered the company's ability to serve advanced Windows 10 management use cases and provides a flexible path for customers to test out modern management. Additionally, EMS has some of the strongest security capabilities in this evaluation, including native vulnerability management on Windows 10, file-level encryption, data-loss prevention (DLP), and malicious app behavior detection. The solution doesn't offer the comprehensive OS coverage, automation, and third-party integration flexibility that other solutions provide.

- **Citrix Systems enables employees with access to a broad set of applications.** Citrix System's Endpoint Management (formerly XenMobile) is well integrated with the company's recently released Workspace App, which combines device management with application access and identity management. The solution has one of the best app store experiences in this evaluation, with comprehensive app support, self-service features, and access to all content repositories, whether on-premises or in the cloud. Citrix Systems offers strong identity management and file-level encryption capabilities and now supports risk-

based authentication based on user behavior through integration with Citrix Analytics. The company's Windows 10 and macOS capabilities are maturing but lag the competition, with notable gaps in support for PC life-cycle management migration on Windows, legacy app delivery on macOS, and threat detection capabilities across mobile and traditional endpoints. The solution will support native mobile SSO by the end of 2018.

Strong Performers

- **Sophos offers tightly integrated security and management capabilities.** Sophos' UEM solution, Sophos Mobile, is especially suited for security-minded small and medium-size businesses with limited technology management resources. The product provides strong security capabilities and integrates with Sophos Central, a cloud-base suite of endpoint protection, server protection, encryption, phishing education, web and email filtering, and firewall products. Sophos is one of the only vendors in this evaluation to provide threat detection and remediation capabilities for both macOS and Windows 10. The solution also has robust data security capabilities, including support for FDE, file-level protections, and DLP. Sophos' device and identity management capabilities aren't as granular as some other products and include gaps in areas such as custom app distribution and conditional access.

- **BlackBerry delivers management and security support for a wide range of devices.**BlackBerry Unified Endpoint Management offers many advanced device and app management features for mobile devices, including secure OS containerization and SSO capabilities. Customers frequently cite the security benefits of BlackBerry's Secure Connectivity service as well as the strong app and data-level security features included with the platform. The UEM product is one of the most mature solutions for managing internet-of-things (IoT) devices and can support advanced IoT use cases such as fleet management. BlackBerry's Access solution enables employees to access enterprise resources on Windows 10 and macOS through a secure browser, but the solution lacks granular management, software delivery, and security capabilities for these platforms.

- **Matrix42 supplements its strong management capabilities with endpoint security.**Unified Endpoint Management is part of Matrix42's larger Workspace Management suite, which includes connectors to its IT service management (ITSM), software asset management, IAM, and endpoint security solutions. The company has aggressively expanded the scope of its offering in the past year and now includes capabilities for DLP through its acquisition of EgoSecure as well as a personal information management (PIM) containerization through partnership

with SyncDog. Matrix42 offers one of the most robust enterprise app stores in this evaluation, with strong license, asset, and service management integrations. It includes malware and exploit protection across all device form factors, with a strong vision for future security capabilities. While Matrix42 has integrated identity management into the UEM platform, the vendor's conditional access capabilities lack the granularity of other solutions in this evaluation.

Contenders

- **Ivanti offers granular management and security capabilities for traditional endpoints.** Ivanti is the result of a merger between Heat Software and Landesk in January 2017. Unified Endpoint Manager (formerly Landesk Management Suite) represents a blended agent and MDM-based approach to endpoint management. Ivanti offers strong client management capabilities for Windows 10 and notably includes malware, ransomware detection, and integration with Microsoft Autopilot to enable out-of-the-box provisioning for employee onboarding. The vendor also provides a strong app store experience featuring tight integration with the company's service and management products. While Ivanti has an identity management and governance product that integrates with UEM, the solution doesn't support more advanced identity management capabilities, such as SSO. Ivanti declined to participate in our research. Scores are based on Forrester estimates.

- **Jamf delivers a best-of-breed solution for managing Apple devices.** It services some of the world's largest macOS deployments and has grown revenues by more than 40% in the past year. The solution offers advanced macOS management capabilities such as third-party patch management, granular scripting, and local caching functionality for the efficient delivery of large software packets. Jamf's newly released self-service portal helps users download preferred applications, install printers, run maintenance scripts, and submit IT help desk requests. Although the company recently acquired NoMad, an IAM solution for Macs, Jamf Pro currently lacks integrated identity features but does integrate with third-party IdPs and can leverage Microsoft Intune for conditional access. (see endnote 5) The solution doesn't support Android or Windows devices and lacks native threat detection, prevention, and remediation capabilities on iOS and macOS.

- **Cisco takes a network-based approach to UEM.** Cisco's Systems Manager is part of the larger Cisco Meraki product line, a collection of cloud-based networking and security products. This allows administrators to monitor how devices are interacting with the network and take remediation actions if necessary. The solution has a visually appealing UI that lets administrators create

device, policy, and user "tags," eliminating the need for manual policy creation. Its integration with Cisco Advanced Malware Protection and the Cisco Security Connector enables Systems Manager to detect remediate malware infection on all supported endpoints, which include Android, ChromeOS, iOS, macOS, and Windows 10. The solution has some gaps in key areas, such as lack of support for mobile app isolation, SSO, and Windows Autopilot.

Challengers

- **Kaspersky Lab offers basic management capabilities with strong threat protection.**The solution supports malware detection and app reputation-based block on Android. It has strong data security capabilities, including FDE, DLP, and file-level encryption. Kaspersky supports a baseline of MDM APIs for management of Android, iOS, macOS, and Windows 10 but has some major gaps in functionality, such as no support for Apple Device Enrollment Program (DEP) or Windows Autopilot. The solution lacks strong identity management capabilities and can't enable SSO. Kaspersky provided incomplete information for this evaluation. Some Forrester scores are based on estimates.

SUPPLEMENTAL MATERIAL

Online Resource

The online version of Figure 3 is an Excel-based vendor comparison tool that provides detailed product evaluations and customizable rankings. Click the link at the beginning of this report on Forrester.com to download the tool.

Data Sources Used In This Forrester Wave

Forrester used a combination of three data sources to assess the strengths and weaknesses of each solution. We evaluated the vendors participating in this Forrester Wave, in part, using materials that they provided to us by October 1, 2018.

- **Vendor surveys.** Forrester surveyed vendors on their capabilities as they relate to the evaluation criteria. Once we analyzed the completed vendor surveys, we conducted vendor calls where necessary to gather details of vendor qualifications.

- **Product demos.** We asked vendors to conduct demonstrations of their products' functionality. We used findings from these product demos to validate details of each vendor's product capabilities.

- **Customer reference calls/survey.** To validate product and vendor qualifications, Forrester also conducted reference calls and fielded a survey with three of each vendor's current customers.

The Forrester Wave Methodology

We conduct primary research to develop a list of vendors that meet our criteria for evaluation in this market. From that initial pool of vendors, we narrow our final list. We choose these vendors based on: 1) product fit; 2) customer success; and 3) Forrester client demand. We eliminate vendors that have limited customer references and products that don't fit the scope of our evaluation. Vendors marked as incomplete participants met our defined inclusion criteria but declined to participate or contributed only partially to the evaluation.

After examining past research, user need assessments, and vendor and expert interviews, we develop the initial evaluation criteria. To evaluate the vendors and their products against our set of criteria, we gather details of product qualifications through a combination of lab evaluations, questionnaires, demos, and/or discussions with client references. We send evaluations to the vendors for their review, and we adjust the evaluations to provide the most accurate view of vendor offerings and strategies.

We set default weightings to reflect our analysis of the needs of large user companies — and/or other scenarios as outlined in the Forrester Wave evaluation — and then score the vendors based on a clearly defined scale. We intend these default weightings to serve only as a starting point and encourage readers to adapt the weightings to fit their individual needs through the Excel-based tool. The final scores generate the graphical depiction of the market based on current offering, strategy, and market presence. Forrester intends to update vendor evaluations regularly as product capabilities and vendor strategies evolve. Vendors marked as incomplete participants met our defined inclusion criteria but declined to participate in or contributed only partially to the evaluation. For more information on the methodology that every Forrester Wave follows, please visit on our website.

Integrity Policy

We conduct all our research, including Forrester Wave evaluations, in accordance with theposted on our website.

Survey Methodology

The Forrester Analytics Global Business Technographics® Infrastructure Survey, 2017, was fielded in July and August 2017. This online survey included 3,923 respondents in Australia, Brazil, Canada, China, France, Germany, India, New Zealand, the UK, and the US from companies with two or more employees.

Forrester Anaytics Business Technographics ensures that the final survey population contains only those with significant involvement in the planning, funding, and purchasing of business and technology products and services. Research Now fielded this survey on behalf of Forrester. Survey respondent incentives include points redeemable for gift certificates.

Please note that the brand questions included in this survey should not be used to measure market share. The purpose of Forrester Analytics Business Technographics brand questions is to show usage of a brand by a specific target audience at one point in time.

ENDNOTES

1. Source: Forrester Analytics Global Business Technographics Workforce Benchmark Survey, 2018.

   "Back to text"

2. Base: 1,296 global infrastructure technology decision makers whose firms prioritize personal device technology initiatives. Source: Forrester Analytics Global Business Technographics Infrastructure Survey, 2017. Microsoft has embraced MDM management for Windows 10 devices using APIs. For more information on the impact of this on traditional endpoint management and PC life-cycle management, see the Forrester report " **Unified Endpoint Management (UEM) Finally Arrives.** "

   "Back to text"

3. See the Forrester report " **The Employee Experience Imperative.** "

   "Back to text"

4. Apple's Device Enrollment Program (DEP) is another example of this type of automation, although it's been on the market for a number of years.

   "Back to text"

5. Jamf also acquired NoMAD, a macOS identity and access management solution, at the end of September 2018. Source: "Jamf Acquires NoMAD, the Leading Solution for Streamlining Mac Authentication and Account Management," Jamf press release, September 19, 2018 (https://www.jamf.com/resources/press-releases/jamf-acquires-nomad-the-leading-solution-for-streamlining-mac-authentication-and-account-management/).