Unified Endpoint Management - Market Quadrant 2018


March 2018

Radicati Market Quadrant™ is copyrighted March 2018 by The Radicati Group, Inc. Reproduction in whole or in part is prohibited without expressed written permission of the Radicati Group. Vendors and products depicted in Radicati Market Quadrants™ should not be considered an endorsement, but rather a measure of The Radicati Group’s opinion, based on product reviews, primary research studies, vendor interviews, historical data, and other metrics. The Radicati Group intends its Market Quadrants to be one of many information sources that readers use to form opinions and make decisions. Radicati Market Quadrants™ are time sensitive, designed to depict the landscape of a particular market at a given point in time. The Radicati Group disclaims all warranties as to the accuracy or completeness of such information. The Radicati Group shall have no liability for errors, omissions, or inadequacies in the information contained herein or for interpretations thereof.
## Table of Contents

**Radicati Market Quadrants Explained** ................................................................. 2  
**Market Segmentation – Unified Endpoint Management** ...................................... 4  
**Evaluation Criteria** ............................................................................................ 6  
**Market Quadrant – Unified Endpoint Management Management** .................. 9  
  *Key Market Quadrant Highlights* ........................................................................... 10  
**Unified Endpoint Management - Vendor Analysis** ............................................. 10  
  *Top Players* ........................................................................................................... 10  
  *Trail Blazers* .......................................................................................................... 24  
  *Specialists* .............................................................................................................. 27

Please note that this report comes with a 1-5 user license. If you wish to distribute the report to more than 5 individuals, you will need to purchase an internal site license for an additional fee. Please contact us at admin@radicati.com if you wish to purchase a site license.

Companies are never permitted to post reports on their external web sites or distribute by other means outside of their organization without explicit written prior consent from The Radicati Group, Inc. If you post this report on your external website or release it to anyone outside of your company without permission, you and your company will be liable for damages. Please contact us with any questions about our policies.
Radicati Market Quadrants Explained

Radicati Market Quadrants are designed to illustrate how individual vendors fit within specific technology markets at any given point in time. All Radicati Market Quadrants are composed of four sections, as shown in the example quadrant (Figure 1).

1. **Top Players** – These are the current market leaders with products that offer, both breadth and depth of functionality, as well as possess a solid vision for the future. Top Players shape the market with their technology and strategic vision. Vendors don’t become Top Players overnight. Most of the companies in this quadrant were first Specialists or Trail Blazers (some were both). As companies reach this stage, they must fight complacency and continue to innovate.

2. **Trail Blazers** – These vendors offer advanced, best of breed technology, in some areas of their solutions, but don’t necessarily have all the features and functionality that would position them as Top Players. Trail Blazers, however, have the potential for “disrupting” the market with new technology or new delivery models. In time, these vendors are most likely to grow into Top Players.

3. **Specialists** – This group is made up of two types of companies:
   a. Emerging players that are new to the industry and still have to develop some aspects of their solutions. These companies are still developing their strategy and technology.
   b. Established vendors that offer very good solutions for their customer base, and have a loyal customer base that is totally satisfied with the functionality they are deploying.

4. **Mature Players** – These vendors are large, established vendors that may offer strong features and functionality, but have slowed down innovation and are no longer considered “movers and shakers” in this market as they once were.
   a. In some cases, this is by design. If a vendor has made a strategic decision to move in a new direction, they may choose to slow development on existing products.
b. In other cases, a vendor may simply have become complacent and be out-developed by hungrier, more innovative Trail Blazers or Top Players.

c. Companies in this stage will either find new life, reviving their R&D efforts and move back into the Top Players segment, or else they slowly fade away as legacy technology.

Figure 1, below, shows a sample Radicati Market Quadrant. As a vendor continues to develop its product solutions adding features and functionality, it will move vertically along the “y” functionality axis.

The horizontal “x” strategic vision axis reflects a vendor’s understanding of the market and their strategic direction plans. It is common for vendors to move in the quadrant, as their products evolve and market needs change.

![Radicati Market Quadrant](image-url)
MARKET SEGMENTATION – UNIFIED ENDPOINT MANAGEMENT

This study looks at the Unified Endpoint Management market as comprising one segment:

- **Unified Endpoint Management (UEM) solutions** – provide businesses with the ability to secure, manage and provision mobile devices, desktops, laptops, tablets, applications and content in multi-OS, mixed use environments. Increasingly, UEM solutions will also encompass Internet of Things (IoT) and ruggedized devices for a cohesive single pane-of-glass management experience. Leading vendors in this market include: BlackBerry, Citrix Systems, IBM, Ivanti, Kaspersky Lab, Microsoft, MobileIron, Sophos, SOTI, and VMware.

- UEM solutions are available as on-premises software, cloud-based services, or hybrid solutions.

- UEM solutions bring together several areas of functionality, which include:
  
  - **Mobile Device Management (MDM)** – device level management features such as: remote configuration; remote wipe; selective wipe; remote locking, and more.
  
  - **Mobile Security** – includes features such as encryption of the device storage, SD cards, emails and folders; two-factor authentication; single sign-on; geo-fencing;, and more.
  
  - **Mobile Application Management (MAM)** – includes features such as containerization; app wrapping, app usage analytics, and more.
  
  - **Mobile Content Management** – includes features such as secure email, calendar, contacts, document management software integration, and more.
  
  - **Endpoint Security** – advanced security capabilities for the detection, prevention and possible remediation of zero-day threats and malicious attacks across all protected endpoints. Solutions may include, but are not limited to, threat intelligence, forensic analysis and more.
Integration with PC Management Tools – separate or integrated PC management capabilities through a common management console for PC and mobile management, which includes an integrated app store for both desktop and mobile app deployment.

- Many vendors offer solution components aimed at addressing one or more aspects of Unified Endpoint Management, and there are many pure-play vendors that focus on a single aspect of UEM (e.g. MDM, or PC management). For the purpose of this report, vendors offering solutions that focus only on a single component of UEM are not included.

- While this report focuses mainly on the Unified Endpoint Management market in the context of enterprise business use, Unified Endpoint Management solutions are increasingly extending in scope to include management of Internet of Things (IoT) and ruggedized devices (i.e. for fleet operations).

- Worldwide revenues for the UEM market will total over $2.1 billion by year-end 2018. This figure is expected to grow to over $4.0 billion by year-end 2022. Figure 2, shows the worldwide revenue for the Unified Endpoint Management market from 2018 to 2022.

![Figure 2: Worldwide Unified Endpoint Management Revenue, 2018-2022](image-url)
Evaluation Criteria

Vendors are positioned in the quadrant according to two criteria: Functionality and Strategic Vision.

Functionality is assessed based on the breadth and depth of features of each vendor’s solution. All features and functionality do not necessarily have to be the vendor’s own original technology, but they should be integrated and available for deployment when the solution is purchased.

Strategic Vision refers to the vendor’s strategic direction, which comprises: a thorough understanding of customer needs, ability to deliver through attractive pricing and channel models, solid customer support, and strong on-going innovation.

Vendors in the UEM space are evaluated according to the following key features and capabilities:

• OS Support – support for a variety of mobile and PC platforms, including: Apple iOS, Google Android, Google Android Enterprise, Windows Phone, Windows, macOS, and others.

• Deployment Scenarios – flexible deployment options, including: on-premises, cloud-based, and hybrid models.

• Remote Device Configuration – the ability to configure devices remotely, as well as perform remote device wipe, selective wipe, remote lock, password resets, and more.

• Remote Device Management – the ability to remotely disable the device’s Wi-Fi, camera, Bluetooth connection, and more.

• Device Level Analytics – the richness of usage statistics about device use.

• Encryption – encryption-level protection of device storage, SD card, emails, folders, and more.
• **App Containerization** – the availability of app SDK, app wrapping, block copy/paste between apps or emails, remote app updating, and more.

• **Mobile App Analytics** – the richness of data about app behavior, download stats, and more.

• **Authentication** – including single sign-on, two-factor app/data authentication.

• **Data Loss Prevention** – support for outbound and/or content-aware data loss prevention (DLP).

• **Jailbreak/Rooting Detection** – the ability to identify, report, and block device jailbreak or rooting.

• **Integration with PC Management Tools** – the availability of separate, or integrated PC management tools through a common management console for PC and mobile management, which offers an integrated app store for both desktop and mobile app deployment.

• **Management of IoT and other devices** – the availability of separate or integrated management tool(s) for IoT, printers, servers, ruggedized devices, and more.


• **Partner Ecosystem** – the overall partner ecosystem including carriers, app stores, global partner reach, etc.

In addition, for all vendors we consider the following aspects:

• **Pricing** – what is the pricing model for their solution, is it easy to understand and allows customers to budget properly for the solution, as well as is it in line with the level of functionality being offered, and does it represent a “good value”.

• **Global Support** – 24x7 help desk support. Also, vendors should provide helpdesk automation, which includes a self-service portal that users can access to perform basic MDM functions, such as device wiping, password resetting, and more.

• **Professional Services** – does the vendor provide the right level of professional services for planning, design and deployment, either through their own internal teams, or through partners.

*Note: On occasion, we may place a vendor in the Top Player or Trail Blazer category even if they are missing one or more features listed above, if we feel that some other aspect(s) of their solution is particularly unique and innovative.*
Figure 3: Unified Endpoint Management Market Quadrant, 2018

- Radicati Market QuadrantSM is copyrighted March 2018 by The Radicati Group, Inc. Reproduction in whole or in part is prohibited without expressed written permission of the Radicati Group. Vendors and products depicted in Radicati Market QuadrantsSM should not be considered an endorsement, but rather a measure of The Radicati Group’s opinion, based on product reviews, primary research studies, vendor interviews, historical data, and other metrics. The Radicati Group intends its Market Quadrants to be one of many information sources that readers use to form opinions and make decisions. Radicati Market QuadrantsSM are time sensitive, designed to depict the landscape of a particular market at a given point in time. The Radicati Group disclaims all warranties as to the accuracy or completeness of such information. The Radicati Group shall have no liability for errors, omissions, or inadequacies in the information contained herein or for interpretations thereof.
KEY MARKET QUADRANT HIGHLIGHTS

• The **Top Players** in the Unified Endpoint Management market are *VMware, Citrix Systems, SOTI, Sophos, and BlackBerry*.

• The **Trail Blazers** quadrant includes *Kaspersky Lab*.

• The **Specialists** quadrant includes *MobileIron, IBM, Microsoft and Ivanti*.

• There are **no Mature Players** in this market at this time.

UNIFIED ENDPOINT MANAGEMENT - VENDOR ANALYSIS

TOP PLAYERS

**VMware**

3401 Hillview Ave
Palo Alto, CA 94304
www.vmware.com

VMware, which acquired AirWatch in February 2014, offers mobile security and enablement solutions that include unified workspaces, unified endpoint management, identity management, intelligence, and application mobilization and infrastructure. VMware solutions are deployed by customers in all regions, verticals and sizes; ranging from SMBs to large enterprises.

SOLUTIONS

**VMware Workspace ONE**, is an integrated platform powered by VMware AirWatch technology, which secures and manages any app on any device by integrating access control, application and unified endpoint management. The platform’s unified endpoint management (UEM) capabilities, allow organizations to consistently manage and secure smartphones, tablets, laptops, printers, wearables and IoT devices across operating systems, including Android, Apple
iOS, BlackBerry, Chrome, macOS, QNX, Tizen and Windows, through a single management console.

The UEM technology provides over-the-air provisioning and device lifecycle management from enrollment, profile configuration, security policies and remote support. It also provides application lifecycle management and solutions for app containerization and development. Organizations can choose to deploy Workspace ONE as a multi-tenant SaaS, on-premises or hybrid with perpetual and subscription licensing models.

Key features for Workspace ONE include: consumer-grade self-service access to any app; BYOD or corporate-owned device choice; secure productivity apps such as mail, calendar, docs and social; data security and endpoint compliance; as well as real-time app delivery and automation. Workspace ONE provides apps-based management for end users requiring access to corporate apps without device management through a containerization approach, which separates corporate and personal data. Workspace ONE also features a mobile content management solution that protects sensitive content in a corporate container and provides users with a central application to securely access and collaborate on documents from their mobile devices. It provides mobile users with an aggregated view of corporate content repositories and user content in a single mobile app.

**STRENGTHS**

- VMware Workspace ONE offers comprehensive support for a wide variety of operating systems, including Apple iOS, Android, BlackBerry, Windows, Chrome OS, macOS, QNX and Tizen.

- VMware offers a full PC lifecycle management solution, which allows organizations to fully manage macOS and Windows 10 desktops and applications, alongside smartphones and tablets.

- Non-compliant devices managed with VMware Workspace ONE are not dependent on a network connection to perform a remote wipe, and a local agent on the device enforces policy and security settings whether or not the device has access to the Internet.
• VMware Workspace ONE offers strong integration with enterprise systems and resources, such as an Active Directory synchronization tool and an SDK for integrating security and management features into custom enterprise apps.

• VMware Workspace ONE provides robust support for email access and management, such as Microsoft Office 365 integration, Microsoft Exchange Server integration, and more.

• VMware offers a secure content viewing and collaboration application that integrates with Microsoft SharePoint, network file shares, WebDav, Office 365, OneDrive, Google Drive, Amazon S3 and 30+ CMIS integrations.

• Secure web browsing is available with the VMware Browser application that can authenticate users, apply blacklists/whitelists, and more. The browser is available for Apple iOS, Google Android and Windows.

WEAKNESSES

• VMware offers highly sophisticated feature-rich solutions, however, this may be somewhat overwhelming for customers that are new to UEM. VMware is addressing this through the availability of wizards and templates to help organizations get set-up faster.

• Customers of SaaS installations indicated that the response times for the management console could be improved.

• VMware does not support Linux.

CITRIX SYSTEMS, INC.
851 West Cypress Creek Road
Fort Lauderdale, Florida 33309
www.citrix.com

Citrix offers solutions for server, application and desktop virtualization, networking, software as a service, and cloud computing. Citrix is headquartered in Ft. Lauderdale, Florida and is publicly traded.
**Solutions**

Citrix Workspace Suite, incorporates mobility, virtualization, networking, data, and some cloud services. Citrix Cloud allows the entire solution to be delivered from the cloud. The mobility component of Citrix Workspace - **XenMobile**, includes: *XenMobile Premium Service* (UEM and ShareFile), *XenMobile Advanced Service* (UEM), and *XenMobile Standard Service* (MDM) deployed in Citrix Cloud. For on-premises, Citrix offers *XenMobile Enterprise Edition*, *XenMobile Advanced Edition*, and *XenMobile MDM Edition*.

Citrix also offers a suite of mobile productivity apps, available with both on-premises and SaaS XenMobile deployments, which include:

- **Secure Mail** – secure email client.
- **Secure Web** – secure browser.
- **ShareFile** – secure file sync and sharing application, which allows mobile users to edit and annotate documents directly on the mobile device, with complete audit trails for information access.
- **Secure Notes** – a secure note taking application, with email and calendar integration for streamlined mobile workflows.
- **Secure Tasks** – a secure task management application integrated with email and calendar.
- **QuickEdit** – offline editing capabilities on mobile devices.
- **ScanDirect** – a mobile app that allows convenient document and photo capture directly from the mobile device.
- **Custom Workflows** – available in Citrix Workspace Services, is a secure app for creating, publishing, populating, and storing digitized versions of commonly used forms with no coding required.

Citrix has a strong focus on end user and administrator user experience. For the end users, XenMobile provides a suite of XenMobile Apps that are tightly integrated out-of-the-box for a seamless experience, with support for single sign-on. The XenMobile administrative console offers a unified endpoint management platform for IT administrators to enforce policies on mobile devices, desktops, applications and data using a single pane of glass.

Citrix XenMobile provides a MAM-only, secure and contained environment for enterprise apps and data without requiring MDM (device) enrollment.
**STRENGTHS**

- Citrix offers a comprehensive UEM platform that includes MDM, MAM, and mobile data and content management capabilities, and is available on-premises or in the cloud.

- XenMobile supports all advanced Mobile Application Management (MAM) security features, including local data storage encryption, without requiring MDM enrollment.

- Citrix XenMobile is tightly integrated with other Citrix products, such as XenDesktop and XenApp for virtualized delivery of Windows desktops and apps to mobile devices, NetScaler and ShareFile, as well as mobile collaboration apps like Microsoft Teams (formerly Skype for Business), WebEx, and GoToMeeting.

- XenMobile when deployed as an integrated Citrix Workspace solution provides IT admins with the flexibility to provision end users with single-sign-on onto native mobile, web as well virtual apps and desktops while maintaining a seamless end user experience.

- Citrix offers a strong product portfolio of mobile productivity applications (i.e. Secure Mail, Secure Web and ShareFile).

- One-click live IT support and chat sessions can be initiated directly from a user’s device.

- Granular app policies can be applied across native mobile apps, HTML5 and other Web apps, SaaS apps, and Windows Desktop apps. iOS and Android apps can be wrapped prior to being imported into XenMobile without the need for additional development work.

- Citrix offers comprehensive analytics through its partnership with Aternity. Citrix enables administrators to gather usage and performance analytics for XenMobile and third-party apps.

- Citrix XenMobile supports the Microsoft Intune Graph API for tighter integration into Microsoft Office 365 environments.
WEAKNESSES

• While Citrix XenMobile can be deployed as a standalone solution, its full power is best achieved as part of a unified workspace strategy that may include XenApp, XenDesktop, XenServer and ShareFile.

• Citrix does not support content-aware DLP functionality. Citrix XenMobile can integrate with Microsoft EMS/Intune and leverage DLP provided by Intune App Protection, but this is also fairly basic.

• Customers we spoke with, that have complex needs and integrate with Netscaler, Citrix’s application delivery controller, indicated that troubleshooting issues could be improved.

• Citrix UEM does not support Linux.

• While highly capable Citrix’s UEM solutions are somewhat pricier than competing solutions.

SOTI
5770 Hurontario St.
Suite 1100, Mississauga,
Ontario L5R 3G5, Canada
www.soti.net

SOTI provides a range of solutions to help enterprises manage their mobile and IoT deployments. Founded in 1995, SOTI is headquartered in Ontario, Canada and has regional offices in the UK, Germany, UAE, Australia, and India.

SOLUTIONS

SOTI’s UEM solution, SOTI MobiControl, unifies mobility management from a single management console, removing the complexity of managing a multi OS, multi-vendor, and multi-purpose mobile environment. SOTI MobiControl, supports Apple iOS, Google Android,
Microsoft Windows Mobile devices, as well as Linux-based IoT devices, and Mac and Windows PCs. SOTI MobiControl can be deployed in the cloud, on-premises, or as a managed solution.

The key components of SOTI MobiControl include: mobile device management, mobile security management, mobile content management, mobile application management, mobile email management, telecom expense management, and secure web browsing.

Key integrated features include built-in remote helpdesk tools (including remote control and mobile helpdesk chat), rapid staging and provisioning, content management (including URL filtering), antivirus/anti-malware, remote diagnostics, and more.

The solution provides a single pane of glass for management of smartphones, tablets, laptops, printers, scanners, wearables, digital kiosks, smart watches, vending machines and other connected devices, which helps unify management and support of a growing spectrum of connected endpoints.

SOTI’s UEM capabilities are a key component of the company’s new SOTI ONE platform. In addition to UEM, the SOTI ONE platform includes a rapid mobile application development, as well as a mobile help desk solution. Platform components for IoT management and business intelligence are currently in development.

**Strengths**

- MobiControl is available in different deployment options, including: cloud-based, on-premises, and managed solutions.

- SOTI has a well-established presence in the business-critical mobility market, with its roots in managing traditionally rugged devices. This gives the vendor a clear advantage as these customers transition to Apple iOS, Google Android, Linux, macOS and Windows 10 devices.

- SOTI’s SDK for Apple iOS devices allows organizations to develop iOS apps for additional MAM functionality. Administrators can remotely view the SDK application, as well as conduct two-way chat between user and support administrator.
• SOTI includes content containerization capabilities via its SOTI hub content management app, and via its SOTI surf secure browser app which provides web filtering, and split tunneling capabilities to access corporate intranet sites without the need for a VPN.

• SOTI’s offering in the Windows Desktop space allows mobile Point of Service (POS) devices to deploy kiosk modes that restrict access to only approved applications, without needing to modify the Windows operating system.

**Weaknesses**

• While SOTI offers UEM for a variety of mobile platforms, they are best known for their strong emphasis on Google Android devices.

• SOTI’s focus on business-critical mobility reduces its mindshare with general UEM deployments.

• SOTI does not offer its own app wrapping and containerization solution, instead it relies on native OS containerization solutions, as well as third-party technologies, to containerize email and enterprise apps.

**Sophos**

The Pentagon
Abingdon Science Park
Abingdon OX14 3YP
United Kingdom
www.sophos.com

Sophos provides IT security and data protection products for businesses on a worldwide basis. Sophos is headquartered in Oxford, UK, and is publicly traded on the London Stock Exchange.
SOLUTIONS

Sophos Mobile manages and secures mobile, desktop, and IoT devices in a single console and is available as either standard or advanced offerings. Both are available as a solution in Sophos Central, which provides unified, cloud-based administration interface for all Sophos products, or as a solution for on-premises installation.

- **Sophos Mobile – Standard** provides management and security for iOS, Android (including Samsung, LG and Sony APIs), macOS, and Windows 10 Mobile & Desktop devices. Sophos provides encryption enforcement, password enforcement, device wiping (corporate and full), and complete MDM capabilities. In addition, MAM capabilities include an enterprise app store to distribute internal and public apps securely to individual users or groups along with the ability to whitelist and blacklist apps. Native container solutions include support for all three major management modes in Android Enterprise (formerly Android for Work), Samsung Knox, and iOS. In addition, Sophos Mobile can also manage IoT devices running Android Things or Windows 10 IoT.

- **Sophos Mobile – Advanced** is an extended offering that adds MCM, Sophos Mobile Security, and Sophos Mobile SDK to all the features of Sophos Mobile Standard. Sophos Mobile Advanced includes:
  
  o **Sophos Mobile Security** – antivirus and ransomware protection designed to protect users on Android devices from mobile malware or potentially unwanted/harmful applications that could compromise the performance or the security of the device. In addition, companies or users are protected against malicious web content or can filter webpages with inappropriate content in a number of different categories. Extended mobile threat defense features are planned for later in the year.

  o **Sophos Secure Email** – one of two applications that make up the Sophos mobile container solution. Sophos Secure Email is a Personal Information Management (PIM) application for email, calendar and contacts that helps IT provision corporate email to personal or business-owned mobile devices across iOS and Android.

  o **Sophos Secure Workspace** – provides secure and controlled access to a corporate document container and to corporate websites. Facilitates secure usage of public cloud
services (e.g. Dropbox, Google Drive, Microsoft OneDrive, and various WebDAV-based services) secured by compliance policies. In addition, Enterprise File Share and Sync services are supported including Windows Server, Box, Egnyte, or OwnCloud. Mobile data protection is tightly integrated with the Sophos Safeguard Encryption solution, which lets users access encrypted files on their mobile devices and remain compliant with encryption policy even when cloud storage services are used. Data remains secure via document encryption and Data Loss Protection (DLP) rules that control access, edit rights and enable secure file sharing and collaboration. Sophos Secure Workspace also offers editing of text and Office format files (Word, Excel, PowerPoint), as well as lets users annotate PDF files. A corporate browser within Sophos Secure Workspace offers secure access to company websites and frequently used sites. In addition, support for KeePass format files provides secure management of passwords.

- **Sophos Mobile SDK** – helps companies add security to their applications for mobile access. An extensive list of controls is available including geo-location or time-based policies, additional authentication, and denial of access if jailbreaking or rooting activity is detected.

**STRENGTHS**

- Sophos’ offers a straightforward one user/one license pricing structure. Organizations are charged a license fee based on number of users, regardless of how many devices each employee uses.

- Sophos Mobile provides administrators with an intuitive, web-based user interface, either fully hosted in Sophos Central, or installed on premises. This is essential to enable small to mid-market customers with limited IT resources.

- Sophos includes strong malware and web protection functionality within their UEM solution, and it integrates natively with the company’s next-gen endpoint security platform in Sophos Central.

- Integration with Sophos Safeguard Encryption enables users to access encrypted files on mobile devices and safely utilize cloud storage locations for collaboration. The Sophos Secure Workspace solution allows users to securely add, view and edit encrypted documents.
• Sophos Mobile integrates with Sophos UTM, encryption and endpoint protection solutions for a comprehensive security strategy.

WEAKNESSES

• Sophos offers an SDK for app data protection, but does not support the wrapping of apps.

• Mobile app analytics granularity and reporting could be improved.

• Sophos Mobile supports enrollment of Chromebooks in the container-only management mode.

• While Sophos Mobile offers integrated management of IoT devices running Android Things and Windows 10 IoT, managing and securing servers and Infrastructure as a Service (IaaS) workloads requires a separate license.

BLACKBERRY
2240 University Avenue, East
Waterloo, Ontario
Canada N2L 3W8
www.blackberry.com

BlackBerry, founded in 1984, is a cybersecurity software and services company focused on securing the Enterprise of Things, for organizations of all sizes, ranging from SMBs to very large enterprises. Based in Waterloo, Ontario, Canada the company operates in North America, Europe, Asia, Australia, Middle East, Latin America and Africa. BlackBerry is a publicly traded company.
SOLUTIONS

BlackBerry has completed a significant change of direction choosing to concentrate primarily on the “Enterprise of Things”, by securing all intelligent endpoints in the enterprise. BlackBerry has integrated its acquisitions of Good Technology and WatchDox, into a single Unified Endpoint Management (UEM) platform, called **BlackBerry Enterprise Mobility Suite (EMS)**. BlackBerry builds all its cybersecurity products on the BlackBerry Secure platform, which provides a common foundation for all its security offerings.

BlackBerry EMS enables secure communication, information sharing, document synchronization, user collaboration, and app management for iOS, Android, Windows 10, and macOS. BlackBerry EMS is available in five editions, which allows organizations to choose the set of capabilities that best meet their needs.

Key capabilities and products within these suites include:

- **Multi-Layered Security** – organizations can apply security controls and policy at the user, device, app and content level. Each of these capabilities can be layered with one another, or used in isolation for greater flexibility across use cases. All BlackBerry products and services are controlled via a single UEM console.

- **Unified Endpoint Management (UEM)** – BlackBerry offers MDM and MAM controls through a single point of management. It provides a cross-platform way to set policies across iOS, Android, Windows, Windows Phone, Samsung KNOX, Android Enterprise, macOS and BlackBerry devices. It also offers an attribute-driven, endpoint-permissions model, which gives users and administrators control of devices, applications and data, by-person or by group.

- **App Level Controls and Secure Container** – BlackBerry Dynamics, within BlackBerry EMS, is a secure app platform that enables companies to deploy and maintain a mobile app strategy. It offers a common set of shared services (such as presence), APIs for security, and a common user interface through the BlackBerry Dynamics Launcher to manage BlackBerry’s own apps, ISV partner apps, and custom apps. It includes complete mobile app lifecycle management, from deploying containerized apps, to building custom apps, to the ongoing management and support of apps, devices, and the associated infrastructure.
BlackBerry Dynamics is a widely deployed secure PIM application in government and regulated verticals, and has obtained Common Criteria EAL-4+ certification.

- **Collaboration Apps** – BlackBerry offers a broad portfolio of collaboration apps purpose-built on BlackBerry Dynamics for business. The flagship app is **BlackBerry Work**, which provides an integrated, mobile collaboration experience for email, calendar, contacts, presence status, and documents from multiple repositories. BlackBerry also extends productivity to enterprise IM, notes, tasks, document access, secure access to intranets, web apps, and more. It is available as a cloud, on-premises or hybrid deployment.

- **PC and Mac Management** – BlackBerry UEM manages Windows 10 and macOS devices, through a single endpoint management console for all user devices. In addition, BlackBerry Access, a secure remote browser, provides a lightweight approach to containerizing enterprise data. Employees can connect to enterprise backend data, or cloud services using this secure browser. Employees, partners, or contractors can leverage BlackBerry Access on personally owned, or non-corporate managed Windows 10, or macOS devices, without the need for a VPN, as all network traffic goes thru BlackBerry’s secure network. BlackBerry Access can also be used as an alternative to a Virtual Desktop Infrastructure (VDI), with cost savings and a simpler on boarding process.

- **ISV App Ecosystem** – BlackBerry has an extensive ISV ecosystem with over 100 apps in the BlackBerry Marketplace. The apps can securely interact with each other, as well as BlackBerry’s own apps through the BlackBerry Dynamics Shared Services Framework. These apps are available on common mobile operating systems, including iOS and Android.

- **Content-Level DRM and EFSS** – BlackBerry Workspaces provide secure file-level protections including DRM controls for common documents. It also includes an integrated Enterprise File Sync and Share (EFSS) solution built for mobile, desktop and web. BlackBerry Workspaces, ensures that proprietary information does not leave the enterprise, while users can apply or change DRM policies to documents even after they have been sent outside a corporate firewall.

**STRENGTHS**

- BlackBerry solutions support all deployment models (i.e. cloud, on-premises and hybrid).
• BlackBerry provides UEM support for iOS, Android, Windows, macOS, BlackBerry devices, Windows Phone, as well as extensive support for Samsung KNOX and Android Enterprise.

• BlackBerry delivers multi-layered security including device policies, app controls and containerization, and file-level DRM in a single unified solution. This provides both a high degree of security as well as maximum flexibility.

• BlackBerry delivers comprehensive security and meets Common Criteria EAL 4+ certification for iOS and Android. BlackBerry Dynamics-secured apps (e.g., BlackBerry Work, BlackBerry Access, BlackBerry, Connect, ISV apps, custom-built apps, etc.) provide powerful DLP features, including granular control over open-in, data sharing and cut/copy/paste between apps or to the cloud.

• BlackBerry-secured apps can transparently access behind-the-firewall resources without a VPN, providing a significant benefit to enterprise organizations.

• BlackBerry provides a comprehensive security solution, which includes management servers, the BlackBerry infrastructure, a mobile OS and smartphone devices. This is attractive for organizations looking for complete end-to-end security across all aspects of the mobile experience.

• BlackBerry offers a secure remote browser, BlackBerry Access, for personal computers that enables VPN-less access to corporate resources (including Office 365).

• BlackBerry’s EMM solutions can leverage Microsoft Active Directory to retrieve user profiles and synchronize user groups for streamlined user onboarding, policy creation and application management.

• BlackBerry supports the Microsoft Intune Graph API for tighter integration into Microsoft Office 365 environments.
WEAKNESSES

• While BlackBerry offers highly sophisticated solutions, a full-capability UEM deployment may be somewhat overwhelming for organizations just beginning to deploy mobile security. BlackBerry is addressing this by offering flexible licensing where organizations can choose only the capabilities that they need.

• While highly capable BlackBerry’s UEM solutions are somewhat pricier than competing solutions.

• BlackBerry offers a rich and interesting portfolio of UEM solutions for a wide range of platforms, however, features and functionality are still not the same across all platforms and some integration issues still remain with regards to solution components derived from its Good Technology and WatchDox acquisitions.

• BlackBerry has gone through a major business transformation from mobile phone manufacturer to software and services delivery. The vendor still needs to build greater mindshare in the UEM space.

TRAIL BLAZERS

KASPERSKY LAB
39A Leningradsky Highway
Moscow 125212
Russia
www.kaspersky.com

Kaspersky Lab is an international group, which provides a wide range of security products and solutions for consumers and enterprise business customers worldwide. The company has a global presence with offices in 31 different countries.
SOLUTIONS

**Kaspersky Endpoint Security for Business** is a next generation integrated endpoint threat defense platform, which delivers a broad array of capabilities and technologies to control and protect all endpoint devices. It provides comprehensive security, visibility and manageability of all endpoints – including physical and virtual machines, mobile devices, and file servers.

**Kaspersky Endpoint Security Cloud** is a cloud-based endpoint security solution aimed at small and medium-sized businesses, as well as MSP partners.

**Kaspersky Security for Mobile** is a mobile security and management solution. It is available as an on-premises standalone solution, or bundled with Kaspersky Endpoint Security for Business for on-premise deployment. It is also available as a cloud solution, through Kaspersky Endpoint Security Cloud, aimed at the needs of SMB customers.

The latest version, Kaspersky Security 10 for Mobile, consists of the following key components:

- **Security Agents** – support all popular smartphones and tablets running Android, Windows and Linux. They provide anti-malware and anti-phishing protection through the cloud-based Kaspersky Security Network (KSN) service, anti-theft for remote lock, GPS tracking, mugshot, full or select device wipe, SIM control, applications control for Android, web/safe browsing detection for Android and iOS. Jailbreak/rooting detection checks device compliance in accordance with corporate policies. The security agent can also be deployed on Android devices from third-party EMM solutions (e.g. VMWare AirWatch) and configured via AppConfig’s native OS capabilities.

- **Exchange ActiveSync (EAS)** – the EAS connector supports all popular mobile platforms including Android and iOS. It supports rich controls such as password management, encryption enforcement, camera/Bluetooth usage, application controls and more.

- **Apple MDM** – allows management of iPhones and iPads and supports all Apple MDM features, including device management and configuration controls, device and application usage information and more; it also offers supervised device management.

- **Samsung MDM** – supports Samsung KNOX 2.7+ devices via the Samsung KNOX Enrollment Program, and deeper control and administration of select Samsung devices (e.g.
Samsung Galaxy Tab).

- **Android Enterprise (formerly Android for Work)** – supports Android 5.0+ devices, allowing creation and management of the encrypted working profile.

The **Kaspersky Security Center** delivers centralized security management and control for on-premises Kaspersky Endpoint Security for Business deployments, through a single pane of glass. It allows organizations to identify all endpoint assets (physical, virtual, mobile), conduct fast vulnerability assessments, achieve a real-time hardware and software inventory, and offer actionable reporting. Kaspersky Endpoint Security Cloud includes its own cloud-based centralized management for mobile devices, endpoints, and file servers.

In the UEM space, Kaspersky Lab has chosen to focus on Mobile Threat Defense capabilities that complement EMM platforms. Kaspersky Lab is a member of the AppConfig Community, and has launched go-to-market activities with VMWare AirWatch, and other EMM vendors.

**STRENGTHS**

- Kaspersky’s Endpoint Security for Business Security and Kaspersky Security for Mobile are available on-premises, or as cloud-based solutions through Kaspersky Endpoint Security Cloud for SMB customers (i.e. <1,000 seats).

- Kaspersky Lab provides a single tool to manage, configure and protect mobile devices, endpoints and servers; hybrid and virtual environments, mail and network gateways, encryption and patch management and more.

- Kaspersky offers secure Web browsing as a part of their MDM solution, which enables filtering of Web content based on categories, such as gambling or entertainment, as well as anti-phishing protection.

- Kaspersky includes its own in-house developed anti-malware and anti-phishing protection.

- Kaspersky anti-theft functionality provides the possibility to control mobile device compliance to corporate policies alongside with the ability to alarm, locate, lock or wipe a single device.
WEAKNESSES

• Feature sets across all supported mobile platforms are not identical. Businesses with BYOD environments and several different mobile operating systems within their corporate setting may find some difficulties in managing these devices.

• Kaspersky Lab does not offer Data Loss Prevention (DLP).

• Kaspersky Security for Mobile does not provide mobile app analytics.

• Kaspersky’s cloud solution, Kaspersky Endpoint Security Cloud, is only available to SMB customers (<1,000 seats) or MSP partners.

• Kaspersky’s strategy to augment the capabilities of established EMM vendors with advanced threat protection and analytics is still in its early stages, and depends heavily on the APIs and interoperability framework made available through the AppConfig Community.

SPECIALISTS

MOBILEIRON

415 East Middlefield Rd
Mountain View, CA 94043
www.mobileiron.com

MobileIron, founded in 2007, delivers solutions for endpoint and cloud security. MobileIron is a publicly traded company.

SOLUTIONS

The MobileIron EMM platform enables enterprises to secure and manage operating systems in mixed-use mobile device environments. It incorporates identity, context, and privacy enforcement to set the desired level of access to enterprise data and services. MobileIron secures data-at-rest on the mobile device, in mobile apps, and in cloud storage. MobileIron EMM is
available for on-premises deployments and cloud-based deployments. MobileIron’s solutions are managed from a customizable console. For larger deployments, administration can be delegated based on region, device type, or other factors.

- **MobileIron EMM Platform** – comprises the following components:
  
  o *MobileIron EMM Platform* – integrates with backend enterprise IT systems and enables IT to define security and management policies for mobile apps, content and devices. It offers support for Apple iOS, macOS, Google Android, and Windows 10. It is available in two form factors MobileIron Core for on-premises deployment, and MobileIron Cloud.

  o *MobileIron Sentry* – is an in-line gateway that manages, encrypts, and secures traffic between the mobile device and back-end enterprise systems.

  o *MobileIron Client* – called Mobile@Work, is an app that end users download to automatically configure their device to enforce the configuration and security policies set by their IT department.

- **MobileIron Access** – is a cloud security solution that allows administrators to set granular access control policies based on application, IP address, identity, device posture and other elements. It also assists administrators into gaining more complete insight into user activities.

- **MobileIron Threat Defense** – is a one app solution designed to detect and remediate both known and zero-day attacks on mobile devices. It helps detect device, network and applications attacks and can remediate threats on devices without the need for network connectivity. It offers detailed mobile threat intelligence, which includes forensic reports. It is available for iOS and Android mobile devices.

- **MobileIron Desktop Security** – is a single pane of glass administration solution, which provides management for Windows 10, macOS and mobile devices. It offers encryption, VPN intergration, and certificate deployment to protect corporate data.

MobileIron also offers several Client-side solutions that can be installed on mobile devices to enhance end user productivity. These include:
• **Apps@Work** – is MobileIron’s enterprise app storefront, which lets users download IT approved in-house as well as third party apps. The app storefront experience can be customized by IT administrators, to define which applications are assigned to a given user.

• **Docs@Work** – provides the ability to access, annotate, share, and view documents across a variety of email, as well as on-premise and cloud content management systems, such as SharePoint, Dropbox, OneDrive Pro, Office 365 and Box. It also provides DLP for email attachments by decrypting documents delivered through Sentry.

• **Web@Work** – is a secure browser that lets users access web content within the corporate intranet without requiring the user to go through complex procedures such as starting a device-wide VPN session. It includes data loss prevention (DLP) capabilities.

• **Help@Work** – allows mobile end users to request IT help directly from their iOS devices. It enables IT to support mobile devices more easily and cost effectively.

• **Tunnel** – allows managed applications to access protected corporate data and content behind a firewall through a secure per-app VPN connection without requiring a device-wide traditional VPN solution. It also enables MobileIron’s mobile management software to continuously monitor mobile device security before access is granted to protected enterprise resources.

• **AppConnect** – containerizes apps to protect data-at-rest without affecting personal data. Once integrated, the applications become part of the secure container on the device managed by the MobileIron Client.

• **MobileIron Bridge** – serves to unify mobile and desktop operations for mobile devices and Windows 10 workstations through a single management console.

MobileIron has an extensive partner ecosystem, which includes applications developed by customers as well as third-parties. This serves to increase the number of applications integrated with the MobileIron enterprise mobility management platform.
**STRENGTHS**

- MobileIron offers flexible deployment options, including: cloud-based, on-premises, and virtual solutions.

- MobileIron solutions are simple to deploy and use by IT administrators, as well as by end users.

- MobileIron focuses on preserving the native user experience on mobile devices.

- MobileIron seamlessly integrates with multiple email platforms, such as Microsoft Exchange, Microsoft Office 365, and others.

**WEAKNESSES**

- MobileIron could improve the depth and granularity of its app analytics reporting. The vendor has this on its roadmap for 2018.

- MobileIron does not offer content-aware DLP.

- MobileIron solutions do not support Linux.

- MobileIron started off with a focus on EMM, the vendor is now re-focusing its strategy to deliver endpoint security across PCs, mobile devices and IoT. Being relatively new to the security space it remains to be seen how effective this strategy will be in comparison with established security vendors.
IBM Corporation
1 New Orchard Rd.
Armonk, NY 10504
www.ibm.com

IBM is a global technology company that specializes in computers, IT consulting, messaging and collaboration software, and more. In the mobility space, the vendor’s enterprise mobility management solution is built on technology from its Fiberlink acquisition in 2013.

Solutions

IBM MaaS360 with Watson Mobile Device Management gives visibility and control of iOS, macOS, Android, and Windows devices from one unified cloud platform. IBM MaaS360 includes mobile device management (MDM), mobile application management (MAM), mobile content management (MCM), mobile expense management (MEM), mobile threat management (MTM), mobile identity management (MIM), secure email, secure chat, browser, editors, a full unified endpoint management (UEM) solution and access to network resources with the use of a web gateway.

Delivered as a cloud service, IBM MaaS360 provides streamlined provisioning and configuration, which allows customers to be set up in minutes. Updates and new functionality are provided automatically so customers are always on the latest OS version. MaaS360’s cognitive capabilities based on IBM Watson technology deliver insights, and recommendations as needed to meet evolving threats and vulnerabilities.

App security is provided in several ways: through native app wrapping capabilities within the IBM MaaS360 product; through an App Security SDK, which can integrate security features, such as authentication and copy/paste restrictions into custom-built enterprise apps on mobile devices; as well as through integration with AppConfig, an ISV framework for secure mobile app delivery.
**STRENGTHS**

- IBM MaaS360 provides multiple ways to separate corporate and personal data on mobile devices. This includes containerization, with granular level policy management and data protection controls.

- The IBM MaaS360 Cloud Extender integrates with Microsoft Exchange ActiveSync, Microsoft Office 365, and IBM Verse.

- IBM MaaS360 provides a secure web browser web gateway, which offers organizations access to internal Intranet sites and web application servers without the need for a VPN connection.

- IBM MaaS360 has a secure document sharing application to provide mobile users access to enterprise content. Document access and distribution include the integration of Microsoft SharePoint, NFS, Box, Google Drive, and other third party solutions. Customers also have the option to leverage IBM MaaS360 Doc Cloud, to securely host and distribute files.

- IBM MaaS360 also protects Microsoft Windows and Apple macOS systems, which simplifies protection deployment across mobile devices and workstations.

- IBM MaaS360 brings together mobile security, app development, identity management, and professional services, for a complete mobile enterprise enablement strategy.

- IBM MaaS360 offers even deeper functionality when integrated with other IBM solutions, such as IBM Trusteer and QRadar.

**WEAKNESSES**

- IBM MaaS360 is only available as a cloud solution, which may disappoint customers looking for an on-premises solution.

- Mobile app analytics and reporting could be improved. IBM is working to address this.
• While IBM MaaS360 integrates with BigFix, IBM’s systems management solution for computers and mobile devices, from an administrative standpoint the two solutions are not yet fully integrated.

• IBM MaaS360 is most effective in conjunction with other IBM products (e.g. BigFix, Trusteer, QRadar), which makes it less attractive for smaller customers.

• IBM’s mobile partner ecosystem is not as extensive as other vendors in this space. The vendor is working to address this.

**MICROSOFT**

One Microsoft Way
Redmond, WA 98052-6399
www.microsoft.com

Microsoft delivers products and services to businesses and consumers through an extensive product portfolio that includes solutions for office productivity, messaging, collaboration, and more.

**SOLUTION**

The **Microsoft Enterprise Mobility + Security (EMS)**, formerly Microsoft Enterprise Mobility Suite, comprises several components under a single license, which includes Microsoft Intune, Azure Active Directory Premium, Azure Information Protection, Advanced Threat Analytics and Cloud App Security.

  • **Microsoft Intune** – is a cloud service, which offers MDM, MAM and PC management functionality across Windows, Windows Phone, iOS, Android and macOS devices. It supports selective wiping of apps and data, as well as app wrapping and containerization. Intune can be deployed as a standalone solution, where it is fully cloud based and does not require any on-premises components; or as a hybrid solution, where it integrates with on-premises System Center 2012 Configuration Manager (ConfigMgr). The Intune subscription includes use rights for ConfigMgr, which allows organizations to manage PCs and mobile
devices through a common console. Intune integrates fully with Microsoft Office 365 to manage Office mobile apps on iOS and Android devices. It offers application level authentication, copy/past control, and enforces conditional access policies to Exchange Online, Exchange on-premises, SharePoint Online, and Teams (formerly Skype for Business). Intune also supports multi-identity scenarios where users can use both personal and company accounts in the same Office mobile app. Intune can also be used to manage PCs, through the Intune agent or via MDM. Intune can integrate with ConfigMgr to support advanced PC and server management scenarios. Intune is available as a standalone subscription, or as part of EMS.

- **Azure Information Protection** – is a service that builds on Microsoft Azure Rights Management (Azure RMS) and Microsoft’s acquisition of Secure Islands, which offers data classification and labeling technology.

- **Azure Active Directory Premium** – includes Azure Active Directory Identity Protection for identity rights management, which offers self-service password reset capabilities, group management, group provisioning and access management policy enforcement, synchronization of user identity with on-premises directories, and Multi-Factor Authentication (MFA).

- **Advanced Threat Analytics** – serves to identify known advanced persistent threats and security issues in on-premises deployments.

- **Cloud App Security** – offers granular visibility, control and protection for cloud based application to help identify threats, abnormal use and any other cloud security issues.

Microsoft EMS is available in two plans: E3, which comprises Intune, Azure Active Directory Premium P1, Azure Information Protection P1, and Advanced Threat Analytics; and E5, which includes Intune, Azure Active Directory Premium P2, Azure Information Protection P2, Advanced Threat Analytics, and Cloud App Security. Microsoft EMS is available through the Microsoft Enterprise Volume Purchasing plan.
STRENGTHS

• Microsoft Intune is a strong UEM solution that can be deployed on its own, or as part of the broader EMS service suite.

• Microsoft EMS is a good solution for organizations fully vested in Microsoft collaboration solutions and cloud strategic direction. It allows organizations to deploy a BYOD strategy across all their users, while integrating seamlessly with investments in identity and rights management.

• Microsoft Intune and EMS offer deep integration with Microsoft Office 365, which is the leading cloud based messaging and collaboration suite in use by many enterprises.

• Microsoft EMS is affordably priced to appeal to organizations of all sizes, particularly if they already have Microsoft Enterprise Volume Licensing agreements in place.

• Microsoft EMS was designed from the ground up to fit well into a hybrid Microsoft environment, where a full transition to cloud computing is underway but may still be proceeding in phases.

WEAKNESSES

• Microsoft Intune and EMS are a best fit for Microsoft-centric organizations, which deploy Windows 10, Microsoft Office 365 and broad range of Microsoft solutions. Typically these organizations will benefit from the tight integration of all the above components, and will leverage attractive pricing offered by Microsoft Enterprise Volume Licensing.

• Microsoft Intune and EMS still lag somewhat behind in managing macOS and Chrome systems.

• Microsoft EMS could offer more advanced app analytics reporting.

• Microsoft EMS’s app wrapping and containerization are somewhat basic when compared to other vendors.
Ivanti delivers solutions for security, service management, asset management, systems management and supply chain software. Ivanti was formed in 2017, as result of the merger of Landesk and Heat Software. Ivanti is a privately held company.

**SOLUTIONS**

Ivanti’s **Unified Endpoint Manager (UEM)** integrates and unifies the management of all end user devices including PCs, laptops, servers, tablets and mobile phones. The solution also provides discovery, inventory, remote control, software distribution, patch management and configuration management via MDM and/or profile configuration agent. Discovery includes both active and passive discovery of devices that are network connected. UEM supports Windows, macOS, Linux, Unix, Chromebooks, iOS, Android, Windows Phone, as well as IoT devices based on tvOS and Raspbian. UEM is available as an on-premises solution, a cloud solution, or as a managed service.

Ivanti UEM delivers the following capabilities:

- **Endpoint Management** – the ability to discover, inventory and remotely configure all devices including PCs, laptops, servers, tablets and smartphones.

- **OS provisioning** – simplifies remote imaging of devices allowing organizations to quickly deploy or upgrade users to the latest Windows, Mac or Linux operating systems.

- **Software Distribution** – allows administrators to target specific user groups, as well as delivers an app store experience which allows automatic downloading of software.

- **PC and MAC Remote Control** – allows direct interaction with users to resolve device issues and provide user education.

- **Mobile Device Management** – supports management and MDM functionality for iOS,
Android, Windows, and macOS devices from a central console, which provides easy device enrollment and policy management.

Ivanti also offers UEM-S, an integrated security suite that provides device control, application control, anti-virus, malware detection, device isolation and firewall management. UEM-S supports client management, MDM, patch and security product administration through a single console.

**STRENGTHS**

- Ivanti offers flexible deployment options, including: on-premises, cloud, or managed private cloud.
- Ivanti UEM brings together remote management, inventory control, asset management and software distribution across a broad spectrum of computing devices, mobile phones and IoT devices.
- Ivanti UEM-S further integrates device management with security.
- Ivanti UEM is simple to deploy and use by IT administrators. Ivanti also offers a self-service portal for end users.

**WEAKNESSES**

- While Ivanti UEM offers solid MDM capabilities, it only provides app wrapping and containment management capabilities through integration with third party offerings.
- Ivanti UEM does not provide mobile app analytics reporting.
- Ivanti UEM does not provide single single-on authentication.
- Ivanti does not provide DLP capabilities.
The Radicati Group, Inc. is a leading Market Research Firm specializing in emerging IT technologies. The company provides detailed market size, installed base and forecast information on a worldwide basis, as well as detailed country breakouts, in all areas of:

- Email
- Security
- Instant Messaging
- Unified Communications
- Identity Management
- Web Technologies

The company assists vendors to define their strategic product and business direction. It also assists corporate organizations in selecting the right products and technologies to support their business needs.

Our market research and industry analysis takes a global perspective, providing clients with valuable information necessary to compete on a global basis. We are an international firm with clients throughout the US, Europe and the Pacific Rim. The Radicati Group, Inc. was founded in 1993.

Consulting Services:

The Radicati Group, Inc. provides the following Consulting Services:

- Management Consulting
- Whitepapers
- Strategic Business Planning
- Product Selection Advice
- TCO/ROI Analysis
- Multi-Client Studies

To learn more about our reports and services, please visit our website at www.radicati.com.
MARKET RESEARCH PUBLICATIONS

The Radicati Group, Inc. develops in-depth market analysis studies covering market size, installed base, industry trends and competition. Current and upcoming publications include:

Currently Released:

<table>
<thead>
<tr>
<th>Title</th>
<th>Released</th>
<th>Price*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email Statistics Report, 2018-2022</td>
<td>Mar. 2018</td>
<td>$3,000.00</td>
</tr>
<tr>
<td>Endpoint Security Market, 2017-2021</td>
<td>Oct. 2017</td>
<td>$3,000.00</td>
</tr>
<tr>
<td>Secure Email Gateway Market, 2017-2021</td>
<td>Nov. 2017</td>
<td>$3,000.00</td>
</tr>
<tr>
<td>Enterprise Data Loss Prevention Market, 2017-2021</td>
<td>Nov. 2017</td>
<td>$3,000.00</td>
</tr>
<tr>
<td>Microsoft SharePoint Market Analysis, 2017-2021</td>
<td>Jun. 2017</td>
<td>$3,000.00</td>
</tr>
<tr>
<td>Office 365, Exchange Server and Outlook Market Analysis, 2017-2021</td>
<td>Jun. 2017</td>
<td>$3,000.00</td>
</tr>
<tr>
<td>Corporate Web Security Market, 2017-2021</td>
<td>Jun. 2017</td>
<td>$3,000.00</td>
</tr>
<tr>
<td>Email Market, 2017-2021</td>
<td>Jun. 2017</td>
<td>$3,000.00</td>
</tr>
<tr>
<td>Cloud Business Email Market, 2017-2021</td>
<td>Jun. 2017</td>
<td>$3,000.00</td>
</tr>
<tr>
<td>Advanced Threat Protection Market, 2017-2021</td>
<td>Apr. 2017</td>
<td>$3,000.00</td>
</tr>
<tr>
<td>Enterprise Mobility Management Market, 2017-2021</td>
<td>Apr. 2017</td>
<td>$3,000.00</td>
</tr>
</tbody>
</table>

* Discounted by $500 if purchased by credit card.

Upcoming Publications:

<table>
<thead>
<tr>
<th>Title</th>
<th>To Be Released</th>
<th>Price*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Archiving Market, 2018-2022</td>
<td>Mar. 2018</td>
<td>$3,000.00</td>
</tr>
<tr>
<td>Advanced Threat Protection Market, 2018-2022</td>
<td>Mar. 2018</td>
<td>$3,000.00</td>
</tr>
<tr>
<td>Unified Endpoint Management Market, 2018-2022</td>
<td>Mar. 2018</td>
<td>$3,000.00</td>
</tr>
</tbody>
</table>

* Discounted by $500 if purchased by credit card.

All Radicati Group reports are available online at [http://www.radicati.com](http://www.radicati.com).