Compliments of

IBM **MaaS360**

Unified Endpoint Management

for dummies®

A Wiley Brand

Manage mobile devices, laptops, and IoT

Deploy and secure apps

Protect content and proprietary data

IBM Limited Edition

Ken Hess

Unified Endpoint Management

IBM Limited Edition

by Ken Hess

for dummies®
A Wiley Brand

Unified Endpoint Management For Dummies®, IBM Limited Edition

Published by
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

ISBN: 978-1-119-37964-5 (pbk); ISBN: 978-1-119-37963-8 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

Publisher's Acknowledgments

Some of the people who helped bring this book to market include the following:

Project Editor: Carrie A. Burchfield
Editorial Manager: Rev Mengle
Acquisitions Editor: Steve Hayes
Business Development Representative: Sue Blessing
Production Editor: Vasanth Koilraj

Introduction

Today's devices are more powerful than enterprise-level servers were ten years ago. They help you multitask, communicate, compute, and mobilize — making security a more complicated issue than ever before. Users enjoy continuous connectivity through their devices — to the Internet, other personal devices, the corporate network, and everywhere in between. Now with anytime, anywhere accessibility, today's employers expect their workers to be productive around the clock, whether at home, onsite, or in the field.

In addition to traditional desktop and laptop computers, smartphones, tablets, wearables, and even the Internet of Things (IoT) present enterprise IT teams with challenges they never encountered before. Chief among these problems are users violating corporate standards, data leakage occurrences — especially from enterprise apps — and the prevalence and evolution of malware and other advanced threats. Not only do enterprises want their users to be accessible and productive, but also they want them to be secure. Ever-evolving device technology has led enterprises to seek out management options to ensure security without overburdening the user, especially in bring your own device (BYOD) scenarios.

Because devices continue to advance, employees come and go, and the security landscape is in constant flux, IT leadership must rise to the challenge of managing a disparate and growing number of devices, operating systems, and platforms. The only efficient method of managing and securing all endpoints, their users, apps, content, and data is to implement and deploy a unified endpoint management (UEM) solution that changes and adapts with new technology, more skilled users, and increasingly sophisticated attacks by hackers. Ultimately, workers want the freedom to use the endpoints of their choosing, and enterprises want to secure those endpoints to protect their proprietary data.

About This Book

The purpose of this book is to provide an overview of UEM, why it's necessary, how it addresses complex problems encountered in the modern enterprise, and where IT can turn for help. *Unified Endpoint Management For Dummies,* IBM Limited Edition, gives you the

information you need to move forward with a management solution that gives the business owner, IT manager, CIO, CISO, or other responsible party an informed point-of-view from which to draw.

Icons Used in This Book

To enhance your experience, while reading this book, the following icons make it easier to grasp complex information, to emphasize key points, and to point out areas that might prove difficult along the path to accomplishing your goals in setting up and implementing technologies explained in the text.


TIP

Reference these items to save yourself time and effort.


REMEMBER

These key takeaway points reinforce your learning.


WARNING

Watch for potential pitfalls, roadblocks, and detours on your journey.


TECHNICAL STUFF

Information to help you explore certain topics in greater detail.

Beyond the Book

This book can help you discover more about UEM, but if you want resources beyond what this book offers, take a look at the following:

- IBM MaaS360 is a comprehensive UEM platform. Learn more at `www.ibm.com/maas360`.
- Find out how IBM's global strategy helps keep your endpoint data secure. Visit `https://ibm.biz/BdrT6L`.
- Find out how Microsoft's Windows 10 operating system will affect your enterprise security and device management. Go to `https://ibm.biz/BdsaJ3`.

IN THIS CHAPTER

- Defining unified endpoint management
- Transitioning to the modern enterprise
- Beginning the unified endpoint management process

Chapter 1
Understanding Unified Endpoint Management

IT organizations have traditionally managed network security with firewalls, virtual private networks (VPNs), complex passwords, antivirus software, and computers imaged and deployed from within corporate walls. But, today's devices generally fall outside the scope of most IT shops, posing a significant threat to enterprise security and creating complexity for those in charge of their management. Devices are now a part of everyday life and thus a part of everyday business. Such devices are no longer optional because they exist irrespective of corporate policy, and for this reason, bring your own device (BYOD) policies have become commonplace. An agile workforce depends on collaboration and communication across devices regardless of platform, ownership, and security.

This chapter focuses on the ability to identify, manage, and effectively tame the "Wild West" that is the modern enterprise. You're introduced to some new terminology, some new concepts, and some new ideas for transitioning your current enterprise into a more agile and accommodating version of itself.

What Is Unified Endpoint Management?

A quick search for *unified endpoint management* (UEM) displays hundreds of topics and multiple definitions, but they all agree that UEM redefines end-user devices as "endpoints" and that the management of those endpoints is centralized, or unified, into a single application or a single application suite. Endpoints are desktop computers, laptops, tablets, smartphones, ruggedized devices, wearables, the Internet of Things (IoT), and any other computing device used by an employee or guest to access network resources. Network resources can range from connecting to an unsecured Wi-Fi access point to complete administrative access for IT staff members and everything in between for regular users, contractors, and casual guests.

But UEM is much more than simply allowing or denying access to network resources; it's single sign-on (SSO) management, user management, device management, device health checks, update management, resource management, device security, access control, and app delivery.

REMEMBER

Using a UEM solution transforms your business from chaos to calm by keeping your network resources and your business assets secure, while still providing the freedom your users need to creatively solve business problems with as few roadblocks as possible.

Untangling the Alphabet Soup That Is MDM, EMM, and UEM

UEM didn't appear overnight or out of thin air; it evolved with personal computing technology that becomes more mobile and more powerful with each new generation's release. Evolving technologies evoke evolving language to describe them, including an array of jargon, abbreviations, and three-letter acronyms (TLAs).

UEM began life as mobile device management (MDM), which many users viewed as "heavy handed" in its approach to security. MDM worked in environments where the company owned and controlled every device. Security was tight and often users felt that either they had to work around security or to use their own devices to have the freedom and flexibility they required to remain agile and competitive in the marketplace.

This consumerization of IT trend led to the modern-day phenomenon of BYOD. MDM suites evolved into enterprise mobility management (EMM) to encompass those devices owned by employees but used somewhat less heavily handed management by their employers. With a plethora of mobile apps to choose from, new ways to collaborate, and anytime, anywhere access to enterprise resources, the focus began to shift from device visibility and control to maximizing employee productivity while preserving data security. EMM further evolved to include services such as mobile app and content management. It also began to support a greater variety of devices beyond smartphones and tablets — extending to e-book readers and some traditional computing devices as well.


TECHNICAL STUFF

Mobile life cycle management includes device deployment, configuration, security, monitoring, and support. IBM MaaS360 also provides container solutions to protect corporate data and BYOD privacy settings to uphold the privacy of the user's personal information (PII).

UEM suites are the latest incarnations of software applications that manage and monitor every user device through the entire mobile life cycle. Users enjoy the freedom of using their own devices and companies enjoy knowing that employees securely access and use corporate data, assets, intranet sites, apps, and other resources.


REMEMBER

Publications, industry leaders, and reporters use EMM and UEM interchangeably, but UEM is a solution that covers a wider range of devices, operating systems, and services. EMM is a subset of UEM, and the terms aren't equivalent. Technology changes so quickly that it's difficult to stay current.

The Modern Enterprise

The days of users marching into an office, sitting down, logging into a desktop PC, and working all day from a single place are in the past. The contemporary enterprise is on the go. Today's backpacks are loaded with laptop computers, tablets, and smartphones. Many also carry e-book readers and hybrid laptops, and their devices may have different hardware manufacturers, running on separate platforms with distinct operating system versions.

THE LOGIC BEHIND UEM

Both enterprise mobility and the adoption of BYOD programs have forced companies to look for management solutions. Businesses do not, however, want to support two or even three separate solutions in the enterprise: one or two that cover laptops and desktops, the other for smartphones and tablets. They're seeking a solution that unifies end-users, endpoints, and everything in between.

An end-user's tendency to use one type of endpoint for a specific task doesn't rule out the possibility that a separate one could be used at any given time. No matter which one chosen to use on the spur of the moment, IT needs a way to keep track of it — and UEM makes it possible to do so from the same platform. Here are the most common platforms:

- **PC/laptop:** 91 percent of Internet users browse the Internet with a PC/laptop.
- **Smartphone:** 80 percent of Internet users own a smartphone.

Businesses can use UEM to deliver secure apps to devices that unify the user experience. A CRM app, for example, delivered by the UEM, behaves the same on PCs and Macs as it does on iOS, Android, and Windows devices. This unified experience makes troubleshooting and end-user support much easier and much less expensive for the company. Businesses can deliver an app to any device with the knowledge that the user experience will be the same, regardless of the device or the platform used.

The modern enterprise is not only mobile and diverse but also dynamic. Users are pushing the boundaries by requiring faster access, creating larger documents, using more resources, and using more data than ever before. This paradigm shift has caught many companies and CXOs off guard, leaving IT staff and security professionals scrambling for answers and management options.

UEM Security: Keeping a Close Watch on Mobile Access

Lack of strict device control scares many business owners and executives away from BYOD programs and away from a more

mobile workforce. Security doesn't have to be a resource drain nor does it have to be a limiting factor in mobilizing users. Security is manageable. It's true that if everyone left his mobile phone, computer, and tablet at the office, there would be far fewer security issues, but then, the contemporary workforce would suffer significant competitive setbacks.

WARNING

Users and their unsecured devices are major threats for businesses. Malware, data leaks, and onboard cameras can have detrimental effects on a business's reputation, intellectual property, and profits.

The solution is to enforce security in such a way that it's transparent to users, but powerful enough to protect a company's assets. UEM provides security across all devices, platforms, operating systems, apps, content, and their users in a consistent manner. And policies can be as strict or as relaxed as the company chooses. IT staff and security personnel can apply broad policies to all users, while restricting others to a very high degree.

For example, apps that access corporate information can require a VPN secured connection to the company network — on a per-app basis. This means that a user's personal email operates outside of the secured apps' VPN and the data between the two apps never mix with each other. This "containerization" protects the user's personal privacy and the company's proprietary data. It's the best of both worlds in that it preserves absolute transparency for end-users while upholding the best interests of the organization.

TECHNICAL STUFF

Containerization can take many forms, from simple isolation to the setup of security boundaries or partitions between business applications and personal applications. In the strictest and most secure situations, a user's mobile phone will essentially become two devices — one business and one personal.

The user's device isn't locked down in such a way as to prevent the user from enjoying social media, games, personal email, or personal messaging, but all corporate data and transmissions are separated by encrypted storage and encrypted communications. Additionally, and at the discretion of the company, a user's corporate data and apps may be removed at any time without affecting the user's device or personal applications.

The Need for a Unified Front

The real "secret sauce" in UEM is the centralized or unified management feature. Any IT professional can tell you that trying to manage all endpoints with multiple tools is a big problem:

- There's the lack of competency with the use of several different tools. Too many tools lead to sprawl and costly mistakes because administrators can't thoroughly train themselves on multiple, disparate systems.
- There's the upkeep of the tools themselves that can prove problematic. Can you see yourself efficiently updating and maintaining ten different security tools for managing user accounts and permissions?
- Having to do everything (provisioning, operating system maintenance, security, and decommissioning) manually leads to staffing bloat. A UEM solution can allow an IT department to perform more efficiently and allow management to significantly reduce IT staff numbers and lower the costs associated with endpoint maintenance.

UEM provides labor-saving functionality to IT staff

UEM centralizes your endpoint management under a single software suite that not only streamlines, but automates tasks that traditionally require labor-intensive manual manipulation and a lower IT staff to endpoint ratio. For endpoints and for users, UEM tools provide the following functions:

- **Provisioning:** UEM suites configure users, devices, and applications for deployment and manage updates, upgrades, and decommissioning.
- **Auditing, tracking, and reporting:** IT staff can accurately track endpoint inventory, audit devices, and produce reports on endpoint policy compliance.
- **Loss prevention:** Endpoint theft, data access, endpoint lockdown and lockout, remote wipe, and application wrapping are a few of the security-focused functions available.

- **Endpoint support:** UEM suites assist IT staff in trouble-shooting problems through inventory, analytics, and remote-access activities.

The five core features of a UEM solution

Although terminology differs among UEM vendors, the functionality of the offerings remains relatively consistent. These core features of a UEM suite are important to consider when selecting an endpoint management solution. The most advanced UEM suites contain all five features:

- **MDM:** MDM includes endpoint life cycle management, endpoint onboarding, provisioning, decommissioning, remote wipe, remote access, inventory, and operating system management.
- **Mobile application management (MAM):** MAM applies policies and controls to applications, includes the ability to whitelist or blacklist applications, provides bulk distribution options, and makes them available to enrolled devices and users via an Enterprise App Store. Corporate or private apps that were developed in-house and deployed and controlled by MAM can be isolated from other business and personal applications and protected through mobile application security.
- **Mobile content management (MCM):** MCM rules and policies apply to access to documents and other content resources from devices. These rules and policies are very fine-grained down to the individual file level and provide extreme security and auditing trails for sensitive content. Organizations can set up Enterprise Document Catalogs to aid in making the right content available to the right users.
- **Identity and access management:** Identity and access management focuses on endpoints and users — ensuring that only trusted entities can gain secure access to corporate information. Service managed by identity management are app code signing, single sign-on (SSO), certificate management, and authentication. Business transactions that have increased security risk factors will benefit by implementing context-based access. Context-based access improves security during authentication and authorization by associating registered devices with user credentials and calculates

risk based on a user's behavioral patterns to grant or to deny access to a resource.

- **Containment:** UEM administrators can separate business apps and data from personal apps and data through password protected pre-configured apps or through application extensions, and prevent sensitive data from leaking externally.

GARTNER: MAAS360 A UEM LEADER

MaaS360 is a good fit for organizations interested in an easy-to-deploy [UEM] product and comprehensive mobile security. MaaS360 app management and distribution capabilities have proven large-scale deployments.

IBM has a strong UEM offering through long-standing MaaS360 client management capabilities and improved integration with IBM BigFix.

MaaS360's integration with QRadar enables administrators to create automated mobile device actions (for example, selective wipe), based on security events or newly discovered vulnerabilities.

MaaS360 [UEM] manages the three popular mobile OSs: iOS, Android and Windows Phone, in addition to systems based on Windows 7/8/10 and [macOS]. Often sold individually or as part of a larger bundle, customers consistently report MaaS360 to be an easy-to-use [UEM] tool. MaaS360 is a complete [UEM] suite offering all five functional areas.

IN THIS CHAPTER

- Getting new endpoints securely connected to your network
- Addressing unified endpoint management security concerns
- Figuring out which devices to allow and which to exclude

Chapter 2
Keeping Track of Endpoints, End-Users, and Everything in Between

This chapter gives you an overview of the endpoint enrollment process. It also deals with vetting your endpoints, managing many different types of devices, physical security, and addressing malware threats.

Enrolling Devices as Endpoints

Enrolling devices into your unified endpoint management (UEM) only requires a few mouse clicks and keystrokes. Of course, you can configure a host of advanced features, but enrolling devices is a simple process.


TECHNICAL STUFF

Apple devices need special treatment prior to enrollment. Apple requires you to have an Apple Push Notification service (APNs) certificate. To obtain this certificate, IBM recommends that you use a corporate Apple ID rather than an individually owned one.

WARNING

Using a personal Apple ID puts the company at risk of losing the certificate if the individual leaves the organization. When a new Apple ID is used for device enrollment, all Apple devices will have to be reenrolled.

Biting into your first Apple enrollment

Apple devices require a special process to request, process, acquire, and upload an Apple Push Notification Service (APNs) certificate into your UEM before you can begin enrolling them as endpoints.

Some devices can be enrolled using Apple's Device Enrollment Program (DEP) if the devices were purchased by an organization directly from Apple or an authorized DEP provider. Using DEP will streamline your enrollment process and give administrators more control over endpoints.

TECHNICAL STUFF

The UEM administrator creates the enrollment request and sends it to the user. The user accepts the enrollment request and allows the UEM app to install. Once the UEM app installs onto the device, the new endpoint sends data to the UEM. A properly enrolled endpoint participates in two-way communications with the UEM solution. UEM administrators can then enforce security policies, create notifications, and control how data flows into and out of any UEM-managed apps, data, and resources.

Enrolling all other device types

The other major mobile OS platforms don't require certificates such as APNs; you can begin enrolling Android, Windows, and other devices as soon as you open your UEM solution.

Submitting a request to add a device (or devices) normally requires a device owner's username, the user's email address, a domain, and optionally a phone number. Simple requests can be delivered to users over the air (OTA) via messaging services or email.

The enrollment request contains an enrollment URL (which can be customized and is a special IBM MaaS360 feature) and a one-time passcode. As soon as the user completes the enrollment process, by installing the UEM app, administrators can view the device and its information.

Using a comprehensive UEM is easy and straightforward. Once enrolled, users can enjoy business resource access, enhanced security and protection, and can perform self-service actions from their endpoints by using the end-user portal.

Enrolling Windows 10 Laptops, Tablets and Smartphones

Windows 10 is here, and either you're currently involved in a migration plan or you soon will undertake one. Now, with Windows 10, you can enroll laptops over the air (OTA) just as simply as with your other mobile devices. MaaS360 provides full visibility and full control over your Windows 10 laptops, tablets, and smartphones.

Once enrolled, the Windows 10 endpoint security is very strong. You can secure your endpoints with extreme granularity. Require complex passcodes, enforce internal storage encryption, enable/disable SD card use, and require VPN connectivity to the Internet.

You can also place restrictions on

- Camera
- Cortana
- Location and telemetry data
- Bluetooth
- Hotspotting
- Non-Windows store apps

REMEMBER

If you have yet to update your entire environment to Windows 10, you are not alone. Rest assured, MaaS360 offers additional support for Windows XP SP3, Windows Vista, Windows 7, and Windows 8+. And keep in mind that your migration will take time; the transition from Windows 7 to Windows 10 is a process that can't be accomplished overnight or even over a weekend. Until you've transitioned, you can take advantage of consistency of information and actionable intelligence across all your Windows devices with MaaS360.

TIP

You can also enroll your Mac computers OTA and deliver policies, authentication requirements, email configurations, and network connectivity. Administrators can take remote actions on MaaS360-managed endpoints, such as device locking, corporate data wiping, changing security policies, and removing device control.

Managing a Diverse, Multi-Platform Environment

If you're old enough to remember the 1980s and 1990s, you know that there were desktop PCs and a few very expensive laptops. Managing a homogenous environment still had its challenges, but compare those days to today and you'll admit that the number of device possibilities approaches overwhelming without the right tools at your disposal.

Bring your own device (BYOD) programs introduce multitudes of disparate device types into the corporate environment. Then consider the diverse assortment of operating systems, operating system versions, and applications. These factors combined draw up an entirely new meaning for the term *device diversity.* Ponder the entire range of security issues associated with those devices, operating systems, and applications. The increased complexity that these devices bring to a corporate setting is enough to make even the most seasoned veterans in IT security cringe.

MaaS360 combines the management of users, devices, apps, and content with strong security to simplify your approach to mobile. You can monitor for threats and automate compliance to maximize security without compromising the user experience. MaaS360 supports several device types and operating system versions.

UEM suites collect this device menagerie into a manageable list of tamed endpoints. UEM solutions manage security, operating systems, patches, applications, and hardware for you, and they reduce the complexity of ever-expanding device diversity.

Visit IBM Marketplace at https://ibm.biz/BdsTPn to see MaaS360's full assortment of UEM solutions and their associated editions.

Automating Enforcement of Policies and Restrictions

UEM administrators can enforce policies and restrictions without ever touching an endpoint and without requiring the endpoint to have corporate connectivity. Administrators can modify passcodes and passcode restrictions, setup automatic app download, enforce operating system patches and updates, force all web traffic through a proxy server, and much more.

And endpoint management doesn't stop with enforcing security on employee devices — it can extend to any enrolled device, such as those owned by guests and contractors. You can uphold the safety and security of your network and then remove control after your protection is no longer required.

REAL-TIME POLICY ENFORCEMENT

"MaaS360 filled all of our requirements. It is cloud-based, which allows us to instantly push apps and monitor policy compliance. It offers the right security and document management capabilities. And it's easy to use, which is important for non-IT users," says Adam Berr, Assistive & Instructional Technology team manager at Bancroft.

"MaaS360 is great in that it allows us to view the compliance state of devices at a glance and also alerts us via email if there is anything that requires our immediate attention."

And, adds Adam, "When students bring their own iPads, we're able to push Bancroft-approved apps onto their devices to use while enrolled, and we can remotely wipe the apps once they leave."

Identifying Compromised Devices Pre- and Post-Deployment

UEM solutions can also detect and take action on jailbroken (iOS) and rooted (Android) devices. Because they aren't considered secure, devices determined to be jailbroken or rooted during enrollment can be automatically quarantined via policy configuration, refusing its access to the corporate network. A factory reset usually restores a device to its original condition, which is then allowed to enroll as a managed endpoint.

MaaS360 also contains advanced mobile threat detection and remediation capabilities, which is a feature not offered by all UEMs. For those that do offer similar functionality, third-party partners provide it. If the UEM identifies a device as malware-infected, the environment administrator can prohibit it from completing its enrollment until the end-user has removed the infected app.

Administrators can configure policies to ensure automated steps are taken to address enrolled devices that have violated their corporate standards. If administrators choose to follow best practices, their users who jailbreak or root their devices after enrollment would trigger deauthorization by the UEM in accordance with their corporate policy. The same action would apply to devices infected with malware.

BANCROFT: INCREASED SECURITY FOR CONFIDENTIAL INFORMATION

For clinical staff, maintaining the confidentiality of their records is essential. "Because of HIPAA issues regarding personal student information and records, the ability to remotely lock and wipe any lost devices provides an added layer of security to iPads used in therapy and other clinical settings," says Beth Greer, Assistive & Instructional Technology Specialist and Special Education Teacher, of MaaS360. "We feel confident knowing that our devices are secure at all times."

You can view the public press release about Bancroft's use of MaaS360 at `https://www-03.ibm.com/press/us/en/pressrelease/44734.wss`.

Subsequent actions are up to the UEM administrators, but their options consist of application-level wipe, container-level wipe, selective wipe, control removal, or a full factory wipe. Several factors determine which action the UEM takes, such as device ownership, automated policy rules, and remote compliance rules. Administrators may also choose to respond manually.

Addressing Lost and Stolen Devices

With the capability to remotely wipe corporate data and enterprise apps, MaaS360 UEM is fit to handle lost, stolen, and otherwise compromised endpoints. Administrators can also lock endpoints, shut down endpoints, and find an endpoint's last known location.

Data breaches cost companies millions of dollars in lost revenue, reputation damage, and lost data. In a 2016 Ponemon Institute study, the average consolidated total cost of a data breach grew from $3.8 million to $4 million. The study also reported that the average cost incurred for each lost or stolen record containing sensitive and confidential information increased from $154 to $158.

Strict policy enforcement via a UEM can significantly reduce costs associated with endpoint loss by using remote wipe, remote lockout, remote shutdown, and geolocation.

REMEMBER

Based on Kensington's research concerning lost and stolen devices, the firm recommends five practices for securing mobile devices:

- Implement a security policy.
- Invest in physical security.
- Never leave devices logged into networks, email, or websites.
- Encrypt all data and secure networks.
- Authenticate users and always know who has access.

UEM addresses four out of five of these recommendations. Unfortunately, no UEM solution can enforce physical security on endpoints. Physical security requires an investment in security accessories, such as locking laptop cables, secure enclosures for tablet computers, and USB port locks. That said, the use of an auto-wipe policy tied to geolocation or Wi-Fi profile geolocation can in specific use cases.

It isn't enough to write a security policy; you must enforce it by placing restrictions and policies onto the devices themselves. Implementing a security policy means enforcing passcodes, timeout values, logout policies, and re-authentication rules. UEM administrators can set timeout values on applications and devices so that idle applications and endpoints don't add to security risk. Leaving an endpoint logged into email, a website, a corporate network, or to the device itself are all major security risks for an unattended endpoint.

Device and data encryption are UEM-controlled features. Administrators should elect to encrypt all corporate data in transit and at rest on the device. Optionally, administrators can enforce full device encryption to secure an endpoint's data.

Network, app, and device authentication are UEM features that administrators can use to verify that the user of an endpoint is legitimate. Multi-factor authentication further ensures that the user is authorized to access corporate resources.

Physical security and encryption are two powerful deterrents to data loss and device theft. Written corporate security policy should clearly identify physical security methods and encryption requirements.

IN THIS CHAPTER

- Controlling access to sensitive data
- Protecting your organization against data theft
- Enforcing endpoint security policies

Chapter 3
Protecting Content and Proprietary Data

This chapter is all about data security as it relates to user devices as managed endpoints. Users want to know that their personal data is private from prying corporate eyes or remote wipe events, and businesses want their data secure and separate from user data. Without a unified endpoint management (UEM) solution, the clear separation of personal and corporate data isn't possible to achieve. For these reasons, many bring your own device (BYOD) programs fail.

WARNING

Corporate policy writers and UEM administrators need to be aware that users who feel that their privacy is violated or that endpoint management is too restrictive will find ways to work around security measures or to abandon BYOD altogether.

Preserving User Data and Privacy

An effective BYOD program allows employees to work with technology that they own and feel comfortable using, while using it efficiently within their organizational role. The problem is that users want the freedom to choose their own technology in the workplace — all without extreme restrictions on personal functionality, spying, or the possibility of their data being wiped out by

an overzealous administrator. A heavy-handed approach to personal devices causes BYOD to fail. However, there is a solution that preserves and protects user data, yet also provides a comfortable security scenario for corporate data and apps: a device dual persona.

A dual persona separates a device into two zones: one preserving end-user privacy and the other protecting corporate, proprietary data. The UEM solution provides a high level of security to corporate-owned information on the endpoint — managing the data, apps, and security inside the corporate persona — giving employees the freedom to use their personal apps and data at will. There are two major approaches to dual persona: containment and data stripping.

Containment

Containment is set up by the UEM to provide end-users with a separate security zone. The container is a type of sandbox that only allows certain types of data to enter and leave. Only activities allowed by the UEM take place inside the container. For example, a corporate email client used in the corporate container can't access personal mail accounts and personal accounts won't have access to corporate email.


TIP

If a user reads an email within the container, policy can prohibit her from copying and pasting text elsewhere on the device — in an instant messaging application for example. This is the primary advantage to containerizing corporate data. UEM administrators can implement very tight security policies without the possibility of cross-contamination with personal data. A company can be as heavy-handed as necessary with the corporate container or containerized app without disruption to personal apps, data, or communications. Containerized apps are the least intrusive approach to dual persona or to freedom in BYOD implementations.

Data stripping

The second, and perhaps least desirable approach to data separation is data stripping. *Data stripping* is a security implementation that strips corporate data from common applications and redirects it to secure applications. The reason that this approach is undesirable to many is that it presents the end-user with more steps than they'd normally have to take to undertake regular tasks.

For example, an employee uses the native mail client on a smartphone for personal and corporate email. The user receives a business email but sees no content until the user opens the secure app to which the email has been directed.

Providing Secure Access to Sensitive Data

A UEM can protect sensitive data through enforced authentication and authorization controls. Each time an endpoint attempts a connection to a network resource, the UEM authenticates the endpoint through its device ID. The UEM checks the device for security compliance and allows the device to connect if all policies pass.

User authentication, shown in Figure 3-1, is the next layer of security for sensitive data access. The user's credentials must be authenticated and then check for authorization to access the resource. If any part of device authentication or user authentication/authorization fails, the user can't access the resource.

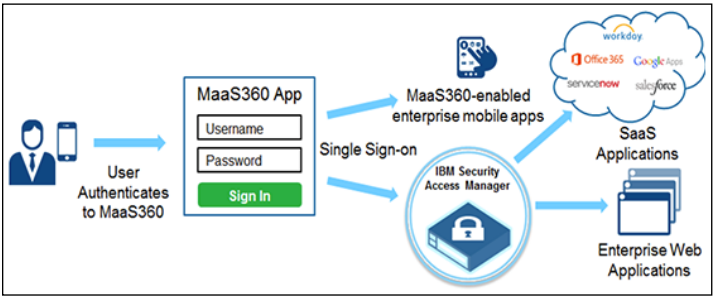

FIGURE 3-1: A UEM can provide secure access to resources without productivity barriers and minimal authentication friction.

Knowing the difference between authentication and authorization is important. *Authentication* is the process of verifying one's credentials to a resource. *Authorization* is the process of verifying that the resource allows the connection to complete. Authentication occurs first to verify credentials and then the resource checks for authorization. A user can have authentic credentials on a domain but not have resource authorization.

Facilitating Secure, Fast, and Efficient Communications

To ensure that communications to and from the corporate network begin and remain secure throughout the session, best practices dictate that apps should only connect via VPN, which

encrypts the entire communications session between the endpoint and the network. In-app VPN communications are transparent to the user — making communications faster, secure, and more efficient than the more traditional method of connecting to a VPN and then launching an app to communicate over the encrypted link.

For example, the IBM MaaS360 Gateway for Browser allows you to login to your corporate intranet and access all web applications and network resources without the use of a device-level VPN session. The Gateway for Browser encrypts all transmitted data, features data leak controls, and enables faster access to corporate resources without multiple steps to initiate connectivity.

Similarly, the IBM MaaS360 Gateway for Documents and the IBM MaaS360 Gateway for Apps provide seamless access to internal content and applications, respectively. Through in-app VPN tunnels that require no extra user intervention, Gateway for Apps ensures that data that is transmitted to and from the corporate network is always secure.


TIP

Users may forget to manually connect via VPN before opening apps; therefore, UEM administrators should require in-app VPN connectivity to secure sensitive data in-flight between the endpoint and the network.

GARUDA INDONESIA: NATIONAL AIRLINE ENABLES DIGITAL TRANSFORMATION WITH COMPREHENSIVE UEM

"MaaS360 provided the features we needed," says Sulistyo Nugroho, Operation Publication Control Coordinator at Garuda Indonesia. "For example, it makes it very easy to distribute or update a file or an app with one click to the Aircraft iPad. We can also easily monitor the last update for Aircraft Document and Performance database in the Aircraft iPad, to make sure that pilots have the latest information, and it helps us track the last location of the iPad and last activity in case of loss."

"Productivity increased by nearly 50 percent for our pilots and 30 percent for Operations staff. Pilots can find the information and perform calculations in 5 minutes that before might take 10-50 minutes."

Upholding Data Leakage Prevention (DLP)

Data leakage is the unauthorized transfer of private, secret, or classified information from a computer to individuals outside of the intended audience. Data leakage isn't necessarily done with malicious intent. The transfer of information can be accidental through conversations, email, or device loss.

In a February 2015 Ponemon Institute research report, "The State of Mobile Application Insecurity," 61 percent of the respondents agreed or strongly agreed that the real risk to mobile apps is data leakage.

The answer to DLP is containerized apps. Containerization of apps involves wrapping apps with security controls such as in-app VPN tunneling, single sign-on (SSO) access, real-time alerting for compliance violations, copy and paste controls, data backup prevention, associated application whitelists, and strict authentication controls.

Enforcing Security Policy Compliance

There are two types of security policies — those that affect devices and those that affect users. The UEM solution is the enterprise's first line of defense for employees who remotely access corporate resources. UEM must strictly enforce this perimeter-based security to protect corporate assets, resources, secrets, and sensitive information. Allowing devices and users to enter an external portal into the network introduces risks. Security policy enforcement and compliance reduces those risks.

Device compliance

Device compliance begins with determining which types of devices you'll allow your UEM to enroll as endpoints. You should decide how to handle devices that are jailbroken, rooted, or don't otherwise meet compliance restrictions for enrollment.

After enrollment, endpoints submit to regular compliance checks to remain updated with security fixes, operating system updates, patches, anti-malware signatures, and any updated security information from the network, such as new resource access.

REMEMBER

The UEM suite contains a mobile device management (MDM) module that handles the heavy lifting for device compliance and enforcement. The UEM manages user compliance in other modules.

User compliance

Before a user can connect and use network resources, the endpoint must meet security policy compliance rules. After the endpoint has passed its compliance tests, the UEM tests the user's security compliance for password complexity, login restrictions, and authorized usage.

Securing Docs and Content Repositories

MaaS360 handles document access and content repositories through its mobile content management (MCM). The MCM provides the following features and benefits:

- **Enterprise document catalog:** The document catalog gives users a safer method of accessing and viewing documents.
- **Document life cycle management:** Managing the entire document life cycle provides a more consistent and streamlined workflow approach for end-users.
- **Compliance and enforcement:** MCM protects documents and files. This module also prevents data leakage by restricting actions users can take regarding documents.

The UEM gives administrators a central location from which to manage documents and to distribute documents. Administrators can set expirations for documents to change access rules. To further protect sensitive information shared with users, administrators can restrict document sharing, printing, copying, and pasting outside of the secure container.

IN THIS CHAPTER

- Delivering catalogued apps to endpoints
- App acceptance, deployment, and denial
- Dealing with malware-infected apps

Chapter 4
Deploying and Securing Apps

It isn't enough to secure documents or other network resources if the apps that connect to and use them aren't equally protected. To secure enterprise applications (apps) that fall outside of IBM MaaS360, unified endpoint management (UEM) administrators can wrap them with MaaS360 security code. Application wrapping secures enterprise apps with a layer of protection afforded by corporate polices with zero reliance on developers for any code changes. This app wrapping process is carried out as follows:

1. **The app is uploaded to MaaS360 portal.**
2. **The app is then wrapped via a configurable security layer.**
3. **The app is then available for download on the enterprise app store.**
4. **After the user elects to download the app, he can deploy it to his device.**
5. **A user-specific policy is then applied to the app on his device.**

Developers who create apps from their own code can use the MaaS360 software development kit (SDK) to add containerization controls natively to their apps. The advantage to integrating MaaS360 app security into your own apps is that UEM administrators can more effectively manage security, updates, and other advanced features for users.

This chapter covers the processes involved with creating and deploying secure apps to users, securing apps, and maintaining app security throughout the entire app life cycle.

Pleasing the Masses with an Enterprise App Catalog

Device users spend most of their time using apps. When managed properly, this behavioral trend can result in massive productivity boosts that benefit organizations. However, when workers are left to their own devices, their apps can pose significant threats to enterprise network security. This is largely due to non-secure data storage practices, malware infections, unauthorized access, lack of data or transmission encryption, and data leaks during syncing.

Millions of apps are right at the fingertips of end-users — a large percentage of which are unsafe for work and even personal use. The enterprise app catalog has answered the organizational need to ensure the right apps can be made available to the right users at any given time, while answering questions surrounding app security and approval for corporate use.

Enterprise app catalogs function much like public app stores, only they're company-managed. All enterprise app catalog apps have been secured and pre-approved for corporate use from any compliant endpoint that is enrolled in the UEM platform.

Users appreciate the enterprise app catalog because it provides a central location where they can download and use apps without obtaining approvals or exceptions. MaaS360 provides an intuitive user experience — mimicking the workflows that users are familiarized with on public app stores — so there is no associated learning curve or need for training.

Surveying App Deployment Options

UEM administrators have several choices for deploying apps to enterprise users. The standard practice is to push a few selected apps to all endpoints so that users have a consistent experience across devices. Enterprise app catalogs are optional but a strongly recommended option for users who would like a list of approved, secure apps that can be downloaded and used at will.

UEM administrators can selectively whitelist, blacklist, and require some apps from third parties, such as vendor app stores or manufacturer app stores. Another option is to push optional apps to the endpoints. Users, however, aren't always on board with more than the small list of required apps pushed onto their devices. Space and power constraints on a user's device are the two main issues users have against administrators pushing these optional apps.

Enterprise app catalog

The enterprise app catalog contains a list of enterprise-built and enterprise-approved apps from which users may choose at will and on-demand as needed. The vendor app store has the familiar look and feel that allows users to intuitively browse and select from all available apps, or those that have been packaged for specific groups or job functions. Users need not worry about selecting any app from the app catalog because the apps contained in it are secure, approved, and ready for deployment. If an administrator finds that an app has a security problem, the administrator can remove it from endpoints and the catalog.

Apps presented in the enterprise app store also contain fewer superfluous functions and features than their vendor app store and third-party counterparts do. They generally have a singular purpose for use in the workplace. Functions such as geolocation, push notifications, always on, and other power-draining, resource intensive features do not exist in these apps. Apps delivered from the catalog are also maintained by the UEM and its administrators. The UEM handles all updates, configurations, and optional features.

ARIZONA CHEMICAL FINDS THE SOLUTION

The people of Arizona Chemical like the MaaS360 app catalog because they no longer need to search and choose from twenty different apps that are basically all doing the same thing. From the expense management and CRM apps to independent apps from its preferred travel vendors, everything is immediately available in the app catalog once a new device is enrolled.

Vendor app stores

UEM administrators may optionally require apps available through vendor app stores, such as the Google Play Store or the Apple App Store. This option is less desirable than creating your own enterprise app catalog because you have no control over quality control, security, malware infections, or optional app features that you don't want enabled for corporate use. However, using strict rules in the UEM's mobile application management module, administrators can manage optional features for public apps to comply with corporate security policy.

If your security policy denies access to vendor app stores, your UEM administrators can list public apps in the enterprise app catalog or push public apps to endpoints.

Push deployments

Pushing apps to devices is a cinch, so long as it's understood by end-users that the UEM will be able to do so upon successful enrollment. As a best practice, users should be informed, prior to the push, how much space and other resources these apps will consume on their personal devices.

Administrators can identify vendor app store apps that have received approval for installation on endpoints without having to connect to the vendor app store, which security policy might prohibit. In either case, the user can install public app store apps that UEM administrators have vetted and approved for use in the corporate network.

Protecting Apps by Enforcing Authentication and Securing Data

The MaaS360 UEM uses a multi-layered approach to app and data security and its functionality is almost entirely transparent to the user, while still providing enterprise-level security for endpoints.

REMEMBER

App protection does the following:

- Enforces data file protection to reduce data leakage risks
- Prevents access from compromised devices
- Uses data leakage prevention (DLP) controls, such as no copy/paste or data backups
- Provides authentication before users access apps
- Sets timeout values for single sign-on (SSO) across all apps
- Enforces on-device access controls
- Automatically delivers updates over-the-air (OTA) to all endpoints
- Wraps apps in security code prior to deployment
- Containerizes apps to separate personal from business functions

Only a multi-layered security approach works for enterprises and devices that are constantly under pressure from advanced threats and ever-evolving malware exploits.

Blacklisting and Whitelisting Apps

When UEM administrators blacklist an app, it is an explicit denial to download and install that app. If there are dozens of prohibited apps that employees shouldn't download, it's more effective to whitelist the few that the company allows and then deny all the others. Administrators employ whitelists and blacklists to allow or deny access to specific apps from an app store or some other public access point.

Administrators can also selectively blacklist and whitelist apps. For example, UEM policy blacklists social media apps

company-wide except for the marketing team who uses Twitter, LinkedIn, and Facebook to promote the company brand to potential customers and to keep current customers updated on breaking company news.

Detecting and Remediating Malware-Infected Apps

IBM MaaS360 Mobile Threat Management (MTM) detects, analyzes, and remediates malware. It also provides advanced jailbreak, root, and hider detection with over-the-air updates for security definitions.

Using MTM, all devices are scanned for malware from a continually updated database and are either remediated automatically, manually by the user, or denied access. Apps pass through a similar vetting process that scans them for malware infections. This is especially important for third-party apps, such as those from vendor app stores and other independent sources.

ARROW INTERNATIONAL (NZ) LTD IMPROVES SECURITY AND WORKFORCE PRODUCTIVITY

"One of the key reasons we picked MaaS360 was because of the anti-malware capability," says Wayne Broekhals, IT Manager, Arrow International (NZ) Ltd. "Other products we tested didn't have that all-around capability to protect against viruses and malware in a single solution. "We discussed the need to not only know where our devices are, but also protect them — that was the key message in gaining executive approval."

IN THIS CHAPTER

- Learning how to properly vet endpoints
- Enabling agility through single sign-on
- Granting secure access to enterprise resources

Chapter 5
Preventing Unauthorized Access

When operating on a corporate network, versus working at home on their private systems, users don't always understand the risks they impart to company resources. For example, malware-infected devices can pose threats to corporate security. After a malicious program or virus has infiltrated a complex network, it is very hard to remove completely. In dealing with Trojan horses and other delayed-release malware types, users can experience related infections for months.

Some malware programs allow the originator backdoor access into infected systems with elevated privileges, which can be extremely difficult to detect and to remove. The perimeter is the best place to stop malware by stopping it before it enters the network.

Unified endpoint management (UEM) solutions monitor the devices requesting access to your network and work hand in hand with your network access control (NAC), to selectively allow or deny their connectivity based on several compromise checks. This chapter examines those checks, why they exist, and what's done by the UEM to protect your data, your network resources, your employees, and their devices.

Remediating Jailbroken, Rooted, and Non-Compliant Devices

IBM MaaS360 UEM allows administrators to detect, analyze, and remediate malware on associated endpoints. Compliance policies determine options for remediation or denial of compromised devices and endpoints. Administrators can automate remediation of jailbroken (Apple iOS), rooted (Google Android), and malware-infected devices, endpoints, and apps. In addition, administrators can monitor the compliance state of enrolled macOS and Windows 10 devices, and act to ensure all endpoints stay in accordance with corporate policies.

After the administrator has enabled the applicable policies, it isn't possible for users to bypass jailbreak and root detection. Though they may attempt to use apps, workarounds, and various instructions to "fool" the UEM system, MaaS360 will detect their jailbroken/rooted device or endpoint and can subsequently restrict access to secure apps. Administrators will receive alerts of detected device jailbreaks and roots, plus a current list of all non-compliant endpoints, giving them the context needed to take appropriate actions.

CDW BOOSTS EMPLOYEE EFFICIENCY AND FREEDOM OF CHOICE

Steve Staines, Manager of Enterprise Collaboration at CDW, stated that its employee efficiency and freedom of choice were boosted with MaaS360. "One of the major benefits of MaaS360 is that we've been able to move from an IT-driven enrollment process to an employee-driven one. When a user tries to connect a new device to the network, MaaS360 automatically quarantines the device and the user is prompted to enroll the device with just three pieces of information: email, username and password. The process takes less than five minutes."

Quarantining and Approving Devices

Using MaaS360's auto-quarantine feature, all discovered devices are placed into quarantine and denied access to Microsoft Exchange, Office 365, IBM Lotus Notes, or other enterprise systems. The user may not access the enterprise network until an administrator approves enrollment. Administrators can also automatically release the device from quarantine, if it enrolls by passing all security and device requirements.

Other than network quarantine, administrators may choose to quarantine any device, enrolled or not, that deviates from policy. Quarantine might include disabling Wi-Fi, disabling VPN (inside or outside of apps), and disabling email as previously discussed. Optionally, quarantined devices may be wiped selectively or in full (back to the factory default settings).

Enforcing Authentication and Single Sign-on

Single sign-on (SSO) is an authentication process that allows a user to access all containerized apps with one set of credentials. SSO is common in enterprises where users may have access to hundreds of systems, websites, and resources that all require a username and password or other credential combination.

TIP

SSO has many advantages over individual credentials for each resource:

- Eliminates the need for users to redo their authentication, therefore improving productivity
- Improves security because it prevents users from writing down passwords in effort to remember them
- Improves compliance through a centralized credential database
- Allows for extensive access reporting

SSO removes the barriers often associated with device use in an enterprise where IT and security administrators manage access with a mobile device management (MDM), a mobile application

management (MAM), or a mobile content management (MCM) solution. SSO removes the typical heavy-handedness of a strictly enforced MDM suite. MaaS360 enforces authentication security without the baggage of overhead for the users.

Securing Access to Enterprise Resources

For today's end-users, obtaining on-the-go access to enterprise resources must be a quick and intuitive process; the inability to do so could be detrimental to productivity in countless scenarios.

Per-app or in-app VPN takes the pain and potential grief out of secure app access. Apps maintained by MaaS360 use in-app VPN connectivity. In other words, if a user opens the email app, the app initiates a VPN connection and will not operate until one is established. The whole process is transparent to the user. The user opens the app, enters login credentials, and the rest is business as usual.

Device-level VPN also consumes a lot of bandwidth because every app the user opens during a VPN session sends its information over the VPN link and through your network. Sure, the VPN encrypts the data, but there's a lot more data flowing through your VPN and your network than is necessary. An app with built-in VPN connectivity only sends its data to your VPN gateway and across your network. There's absolutely no mixing of traffic between business apps and personal apps.

What about apps connected directly to your network? You don't have a need for in-app VPN and the unnecessary traffic going outside and then back inside your network. The app senses that it is inside your protected network and doesn't use the VPN, making app use and network use far more efficient.

MaaS360's Gateway for Browser, Gateway for Apps, and Gateway for Documents each alleviate the need for a device-level VPN. The features available through each of these modules ensure seamless and secure access to enterprise resources without the need for additional user intervention.

Users can view and share content with other SharePoint users, with other Box users, and with other Windows file share users. Per-app VPN ensures that all traffic between the app and its destination (your network) gets there and back encrypted.

IN THIS CHAPTER

- Getting a handle on UEM
- Focusing on app, data, and device security
- Getting started with a UEM solution

Chapter 6
Five UEM Takeaways

The five takeaway points in this chapter are action items for you to use when selecting, implementing, and using your unified endpoint management (UEM) suite. They include best practices, implementation advice, tips, and notes that help you on your way to a successful and secure UEM experience.

Bridging the Mobile Endpoint Gap

Enterprise mobility management (EMM) software is yesterday's news. Mobility management is only part of the equation. A UEM combines mobile device management (MDM) and all other computing endpoints into a single application. To the UEM, all devices are endpoints, and it manages them uniformly.

And if you're transitioning to Microsoft Windows 10 from legacy platforms such as Windows 7, which you should be doing, a UEM makes the management process simple and secure. Only with IBM MaaS360 you can you complete your migration all from the same platform. You can set strong security policies; access robust device views; take enforcement actions; configure device, app, doc, and data security settings; enforce internal storage encryption; configure ActiveSync settings; and disable external storage devices. You can also treat your Windows 10 endpoints the same

way you do your other standard and mobile endpoints by making policy changes, locating devices, and performing selective or full device wipes.


REMEMBER

Enrolling your Windows 10 devices over-the-air (OTA) is simple. You can place restrictions on the use of device cameras, Cortana, location and telemetry data, Bluetooth usage, hotspots, and non-Windows Store apps.

Finding the Right Solution to Meet Your Needs

Most business environments have many different types of devices at multiple patch levels and with varying degrees of security compliance. The UEM brings these disparate devices under control for patching, malware protection, device-level security, app-level security, and user security. MaaS360 uniformly manages device, content, user, and app security across all devices, including laptops, desktops, smartphones, and tablets.

You might ask the legitimate question, "What makes MaaS360 the right solution for me and my business?" The answer is simple: MaaS360 allows you to enroll and to protect your endpoints and their users all in one platform. It is a UEM suite that enables administrators to place adequate restrictions on devices, apps, content, and data — while upholding privacy and giving the user enough space and resources to work in an unencumbered manner.

For example, when a user needs to open a protected network document, the app automatically and transparently opens an encrypted VPN connection to that resource for the user. No user intervention is required — only a need to access the protected document from corporate storage.

MaaS360 also allows administrators to restrict access to apps from a corporate app catalog. Users may opt to install apps from this protected environment, ensuring that those apps are malware free and VPN-enabled. And MaaS360 supplies these protected apps to every enrolled device.

Taking to the Cloud for Ease, Speed, and Savings

If you've ever endured the process of procuring, deploying, imaging, managing, and paying for hardware, you know that it's a slow, tedious, and costly process. Cloud-based or Software as a Service (SaaS) offerings remove the complexity, the red tape, maintenance and expenses associated with on-premise hardware.

SaaS-based offerings like MaaS360 are easy to financially justify. With a free, full production trial offering, no hardware purchase requirements, no scale-up or scale-back issues, no overprovisioning, no wasting of capacity, no customer data center housing, and no hardware managing, it's easy to forget about the advantages of an on-premise solution.


TIP

Your SaaS-solution provider can deliver recurring, no-impact software upgrades throughout the year. These updates deliver new functionality that's intended to enhance the customer experience. No on-premise solution can offer that kind of uptime or smooth transitioning. In fact, most require ongoing maintenance by customers themselves to stay up to date with the latest technology.

Another major advantage to SaaS is that you will never have to deal with obsolescence of your hardware, your platform, or any software. You'll never have to migrate from a legacy solution to a contemporary one. Even if you're in it for the financial savings, you should also consider the other long-term, non-financial benefits of a SaaS solution.

Delivering Consistent Support, Policies and Restrictions

At present, you probably have one client management solution you use to configure policies and enforce restrictions on your enterprise PCs and Macs. And you have another mobile device management (MDM) or enterprise mobility management (EMM) solution you use to manage your smartphones, tablets, and other endpoints such as ruggedized devices (not to mention their apps, docs, and data). And now you have to find a whole new solution to

manage the Internet of Things (IoT). As if juggling multiple solutions wasn't exhausting enough, you're also losing precious time and incurring unnecessary costs.

What if you could consolidate your endpoint support, policy configuration, and restriction enforcement all from the same place? As part of the definition of UEM, you can. The MaaS360 UEM solution integrates, manages, and secures all endpoints, end-users, and everything in between from a single platform.

If you want to restrict the use of external storage, you can easily distribute that rule to all applicable devices. You don't have to swap from platform to platform to accomplish this (for example, one for your Mac computers and another for your Androids). Instead you have one platform for all your endpoints.

And that's just the tip of the iceberg. You can distribute the same authentication requirements across all devices. Grant secure, seamless access to corporate resource. Ensure that all devices meet your security standards by either staying up to date on the latest software or maintaining the latest anti-malware signatures. Update apps across all your devices regardless of platform, operating system, or hardware vendor.

All the while, you'll enjoy the same level of visibility and support across all of your endpoints.

Preserving a Positive End-User Experience

So, what does MaaS360 look like to the end-user? Think more native-like, and less learning curve. Whether MaaS360 is used to send an email, chat with a colleague, create and share a doc, or download an enterprise app — the experience shouldn't seem any different from normal, everyday device use.

No amount of text-based dialog can convey the ease of use the way a live demonstration can. Visit MaaS360's website and request a demo to quickly see how easy it is to self-enroll a new device, to install the MaaS360 application, and begin reaping its productivity benefits. See how simply UEM administrators can remove their control over a device, effectively turning a personal device into a

business device and then back into a personal device, all in less than three minutes.

The user requires no training in order to self-enroll a device and no intervention is required to remove a device from its corporate enrollment. Enrollment only requires the installation of a single app onto the device. When an administrator removes a device from enrollment, only the MaaS360 app, its protected data, and any MaaS360-controlled apps are removed completely from the device. No global changes are made to the enrolled device. The user's personal device is still personal but can be used for corporate work and connectivity without the mixing of data or security compromise either for the user or for corporate data.

For more information about MaaS360 and to start your free 30-day trial, visit `http://ibm.com/maas360`.

IN THIS CHAPTER

- Embracing the future of endpoint computing
- Gaining cognitive insights and actionable intelligence
- Meeting the demands of the contemporary regulatory climate

Chapter 7
Ten Emerging Trends That Impact Your Business Transformation

Not since the introduction of the IBM PC in 1981 has any technological advance captured the world's attention like mobile computing. The ability to work from any location, on any device, at any time has increased efficiency, improved business processes, and yielded tremendous productivity boosts. Never have so many people had so much power right in the palm of their hands.

The ten emerging trends in this chapter help shape the path for your business transformation and expand the ability to stay connected to both work and each other. They allow you to gather more information about everything in a shorter amount of time. This revolution is the current version of the 20-year-old Internet revolution that promised to save time, but actually did the opposite. Together these trends will keep you better informed, maintain a watch on your health, and make you more efficient information gatherers.

Unified Endpoint Management

Of course, I know that this book is about unified endpoint management (UEM), but what you don't know is that UEM is very young, but rapidly gaining ground in some very interesting places. Think about the Internet of Things (IoT). Now think about UEM. Are you seeing a connection? You should. As IoT matures, the need for "thing" management will grow in demand. Organizations will increasingly rely on their UEM to enroll, monitor, manage, and protect millions of their things, all from one automated console.

UEM is a broad-spectrum control and protection solution for all endpoints. Its goal is to simplify management of diverse device types and to streamline their security. It includes mobile device management (MDM), mobile application management (MAM), and mobile content management (MCM), and a number of other controls to detect and remediate malware and other advanced threats to protect associated devices.

Most organizations continue to support legacy Microsoft devices, such as Windows 7-based laptops. IBM MaaS360 UEM allows for a simple, seamless transition to Windows 10, eliminating the need to phase out old management tools and replace them with new ones. Thanks to Microsoft APIs for Windows 10, organizations can use MaaS360 to effortlessly migrate from traditional agent-based device management to API device management.

Malware and Advanced Threats

According to a survey conducted by the Federal Reserve Board's Division of Consumer and Community Affairs (DCCA), 87 percent of the U.S. adult population owns a mobile phone, and 77 percent of those are smartphones. The survey also showed that 53 percent of smartphone owners had used mobile banking. One-third of the survey respondents use some type of anti-malware software to protect their devices, but only 2.3 percent of those surveyed have a concern about malware being installed on their phones.

Despite this level of apathy predominantly exhibited by these end-users, no one device type is completely invulnerable. And even the most popular mobile platforms have had their share

of scares. Take Pegasus spyware for example; it threatened the security of the same iPhones and iPads that are among the safest available on the market. The three zero-day vulnerabilities that made Pegasus possible have been patched, but it shows that no device or platform is off the malware radar.

Malware and other advanced threats can be stopped. MaaS360 protects against malware by detecting risks and managing those threats before they compromise your data by analyzing apps before you deploy them to users. Administrators can set and apply granular policies and usage controls in near real time to automate remediation of threats.

Cognitive Computing

Have you ever heard of Watson? Yes, Watson was the computer that won Jeopardy, but it's much more than just a trivia whiz kid; it's the future — and the future is cognitive computing.

Cognitive computing allows its users to interact with information in natural language. You believe that you're interacting with a computer or an Android, but in actuality, you're interacting with information and a very clever information retrieval system.

App developers are tapping (pun intended) into the power of Watson through APIs that allow them to build cognition into their apps and their products. How valuable would it be to ask, "How likely is it that Customer X will purchase our technology solution today"? The answer might force you to revise your sales strategy with that particular customer.

Cognitive computing allows you to ask the important questions in language that both you and your computer can understand. The answers might not be what you want them to be, but they'll be accurate, fast, and relevant.

TIP

With Watson, MaaS360 UEM delivers cognitive intelligence to customers in several flavors: descriptive (what is happening?), predictive (what will happen?), and prescriptive (what should I do?). And with cloud-sourced benchmarking capabilities, administrators can see how they compare to organizations just like them — or those of different sizes from different industries — for better decision making. They don't have to consult a peer, attend

an event, or browse the web to obtain this actionable intelligence; it's instantaneously available from the platform with the click of a button.

Big Data and Analytics

Big Data and Analytics are hot business topics these days. In the near future, you'll draw on both for market predictions, for measuring sales campaign successes, and for gauging customer sentiment. Numbers are just numbers, but the difference in the future's big data and analytics is that those numbers will take seconds, instead of weeks or months, so that you can make strategic changes in real time.

Internet of Things

Internet of Things (IoT) is one of the most popular buzzwords of the past two years, but its implications reach far beyond the imagination. IoT began humbly in oil fields, weather stations, and in industrial complexes to monitor switches, gauges, flaps, pressure tanks, and temperatures. The IoT of the future will provide feedback on every aspect of your business in observable real time.

IoT devices will measure and automatically control gadgets and "things" from the most mundane to the very elaborate. IoT devices measuring the temperature inside a pressure vessel to monitoring an actuator that dispenses medicine to receiving notification that the refrigerant inside the space shuttle needs to be replaced are a few of the future IoT applications. And somewhere will be a cluster of computers gathering, compiling, and reporting on this data.

Software-as-a-Service

Software-as-a-Service (SaaS) isn't new, but what *is* new is that mobile computing will increase the number of SaaS offerings so that users can enjoy an in-office experience with any application, on any device, in an app that's tied to a SaaS backend.

Additionally, the increased numbers of SaaS offerings will make it easier on UEM administrators to secure data transmitted to and from SaaS-enabled apps.

Hybrid Laptops

A hybrid laptop is a tablet computer that also has an attachable keyboard that basically converts it into a standard, but highly portable, laptop computer. The tablet part of the computer features a touch screen that allows its use whether or not you have the keyboard attached. The future implications for business range from taking handwritten notes in a meeting, when the clackety-clack of a keyboard isn't appropriate to participating in online conference meetings that include interactive presentations using mouse, keyboard, touchscreen, and other peripherals.

Hybrid laptops are also UEM suite manageable. Pre-installed apps, security policy enforcement, and remote wipe capability at a UEM administrator's fingertips. Business users will enjoy the flexibility of the hybrid laptop platform and can adjust to a variety of situations with it.

Wearables

Wearables are the current rage for those who want to count steps or to check email, but the wearables of the near future are going to change business forever. Imagine wearables that not only connect to your corporate email, corporate instant messenger service, and your corporate calendar, but also can be used to provide constant feedback during presentations or for up-to-the-minute information delivered by big data analytics-based apps.

The wearables market has historically focused on personal physical performance, but start-ups are currently creating business apps that take wearables into every technological aspect, such as system monitoring, service notification, and password management.

Identity and Access Management

As hacks, breaches, and identity theft incidents continue to rise, companies will concentrate their security efforts on identity and access management as a primary defense against data theft. The problem that many businesses will face is the enormous amount of data generated from the level of monitoring, logging, and alerting required by Identity and Access Management (IAM) solutions.


TIP

MaaS360 UEM gives users quick, seamless access to enterprise apps and cloud services with a single sign on (SSO) experience. Administrators can implement and enforce conditional access controls to enforce stronger security. They can also set granular policies for specific apps that take the device compliance state into account — blocking access for non-compliant devices. Contextual attributes such as resources accessed and network information can be assessed to make more intelligent, risk based decisions that increase security while preserving end-user transparency.

Rising Regulatory Requirements

The rise of regulatory requirements in preserving data privacy and protecting individual's personally identifiable information (PII) means that businesses will have to spend more money and more time on security efforts. Regulations such as HIPAA and the European Union's (EU) General Data Protection Regulation (GDPR) return control of PII to the information's owner.

The GDPR extends and replaces the EU's data protection directive. It also extends the scope of the data protection law to all foreign companies that process EU resident's personal data.

Failure to comply can result in serious sanctions and fines. In response to GDPR, IBM's Privacy Consulting Services can help organizations adhere to the new sets of data protection rules that cover all companies that sell to customers in the EU.

What to look for in a unified endpoint management solution

Devices are advancing, employees are coming and going, and the security landscape is in a constant state of flux. These factors are forcing businesses to deploy an efficient and cost-effective method to manage and secure all endpoints, their users, apps, content, and data. This solution is unified endpoint management (UEM). Adapt to new technology, more skilled users, and increasingly sophisticated attacks by hackers — all with UEM.

Inside...

- Understand UEM
- Track endpoints, end-users, and more
- Grant secure access to resources
- Five UEM takeaways
- Ten emerging UEM trends
- Get started with a UEM solution
- Migrate from legacy laptop platforms

IBM **MaaS360**

Ken Hess is a system administrator, systems analyst, virtualization administrator, author, blogger, columnist, technology journalist, and podcaster. With 20+ years of IT experience, he writes on a variety of topics. Ken loves watching and exposing film, creating video, and attempting to create art.

for dummies®
A Wiley Brand

ISBN: 978-1-119-37964-5
Part #: WGW03288USEN-00
Not for resale

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.