



WHITE PAPER

Enterprise Mobility Management

Securing mobile endpoints across your organization

CONTENTS

1	Enterprise Mobility Management (EMM)	2
2	Automated security assurance	3
2.1	Enrollment.....	3
2.2	Inventory	5
2.3	Enforce password protection	5
2.4	Remote lock and wipe	5
2.5	Updating device firmware	6
2.6	Block or approve apps.....	7
2.7	Three areas of device management.....	7
2.8	Security through certificates, distribution, and enterprise Wi-Fi	8
2.9	Automated compliance monitoring	8
2.10	End-user self-service capabilities	9
2.11	Apple Volume Purchase Program or Android Enterprise App Distribution	9
3	Comprehensive, efficient, and easy to use	10
3.1	Standalone, integrated, or co-managed: Which is right for you?.....	10
3.2	Implementation, training and usability	10
3.3	The challenge of platform diversity	10
3.4	Transparent management in real time	12
4	Checklist of important functions.....	13
5	Conclusion	14

© 2026 baramundi software GmbH

Statements regarding features and technical functionalities are non-binding and for informational purposes only.
Subject to change without notice.

1 Enterprise Mobility Management (EMM)

As organizations adopt Unified Endpoint Management (UEM) solutions, EMM capabilities for device enrollment, policy enforcement, and compliance monitoring remain central to mobile device management strategies.

Bring-Your-Own-Device (BYOD) has become standard practice at many companies. Employees want to use their personal laptops, tablets, or smartphones to access company data. This improves flexibility and productivity but also increases the risk of cyberattacks or compliance gaps. That's why IT managers need centralized, automated tools to protect mobile devices and company data while maintaining network visibility and an accurate device inventory. Ideally, those capabilities will be integrated into a modern UEM solution to eliminate tool sprawl and provide consistent, policy-based maintenance for all devices on the network.

An increasing number of cyberattacks and malware variants have targeted smartphones, tablets, and PCs. This requires IT teams to apply the same rigor to securing mobile endpoints as to other managed devices. The range of options can make it challenging to select the right solution for your organization. However, asking a few key questions at the start of the process can help you choose the one best suited to your requirements:

- Is it easy to integrate and inventory mobile devices in the management solution?
- Does it provide comprehensive device configuration and security features?
- Does it support platform-specific features such as Apple Business Manager and Android Enterprise?
- Does your environment require a standalone solution or one integrated with other IT management systems?
- Is the solution easy to learn and use?

Use these questions to build your requirements list before evaluating vendors, then validate shortlisted solutions through a proof-of-concept deployment.

2 Automated security assurance

This section covers how EMM/UEM systems automate device integration and security enforcement, enrollment, compliance policies, app management, and OS updates.

2.1 Enrollment

Mobile devices must first be integrated with the EMM solution and registered with the management server. There are several enrollment options available depending on how the device will be used and managed:

- As a fully managed company-owned device restricted to business use (COBO)
- As a company-owned device that also allows personal use (COPE)
- As a user-owned device configured to access company data (BYOD)
- As a company-owned dedicated device (COSU)



2.1.1 Corporate-Owned, Business-Only (COBO) devices

iOS activation with ADE

COBO devices do not allow users to install their own apps or store or access personal data. They provide maximum security but are more cumbersome for users who must carry both a company-owned device and a personal device to keep up with work and stay in touch with family and friends.

2.1.1.1 Apple Automated Device Enrollment (ADE)

With Automated Device Enrollment (ADE), a component of Apple Business Manager (ABM), Apple provides an efficient way to integrate iOS, iPadOS, and macOS devices into EMM or UEM systems. Administrators can centrally manage the process and predefine policies, while end users benefit from simplified, automated activation. This ensures that all company devices remain permanently managed and protected.

2.1.1.2 Android Enterprise Zero-Touch Enrollment

Google provides a similar option for Android Enterprise devices through Zero-Touch Enrollment. This allows Android devices to be automatically integrated into the UEM solution when they are powered on for the first time and provisioned with predefined policies, apps,

and certificates, all without manual intervention by administrators. Companies benefit from scalability, consistency, and immediate security across all company-owned devices.

2.1.2 Corporate-Owned, Personally Enabled (COPE) devices

COPE devices are centrally managed by IT departments but allow personal use by employees. COPE devices are configured with separate company and user partitions. The fully managed company partition enables administrators to secure business data and enforce company policies. The user partition maintains employee privacy by preventing administrators from accessing or viewing users' personal apps and data.

- **iOS/iPadOS:** ADE automatically enrolls the device in the EMM/UEM platform at first power-on. The administrator then configures a *User Enrollment* partition to establish the managed/personal separation. The employee signs in with a Managed Apple ID to activate the personal space.
- **Android Enterprise:** A *Work Profile* provides a secure logical separation between work and personal apps and data, with differentiated policies.

2.1.3 Bring Your Own Device (BYOD): Personal devices for business use

Bring Your Own Device (BYOD) allows users to use their personal devices in the corporate environment. BYOD is convenient for users, but IT teams must clearly separate business and personal apps and data to enforce company policies and protect user privacy.

- **iOS/iPadOS:** The employee enrolls their device by navigating to a sign-in URL or by using a managed Apple ID provided by IT. *User Enrollment* creates a secure managed partition for company apps, accounts, and data, while users' personal data remains private and inaccessible to administrators.
- **Android Enterprise:** A *Work Profile* creates a separate business area that is centrally managed and completely isolated from user apps and data.

2.1.4 Corporate-Owned, Single-Use (COSU) devices

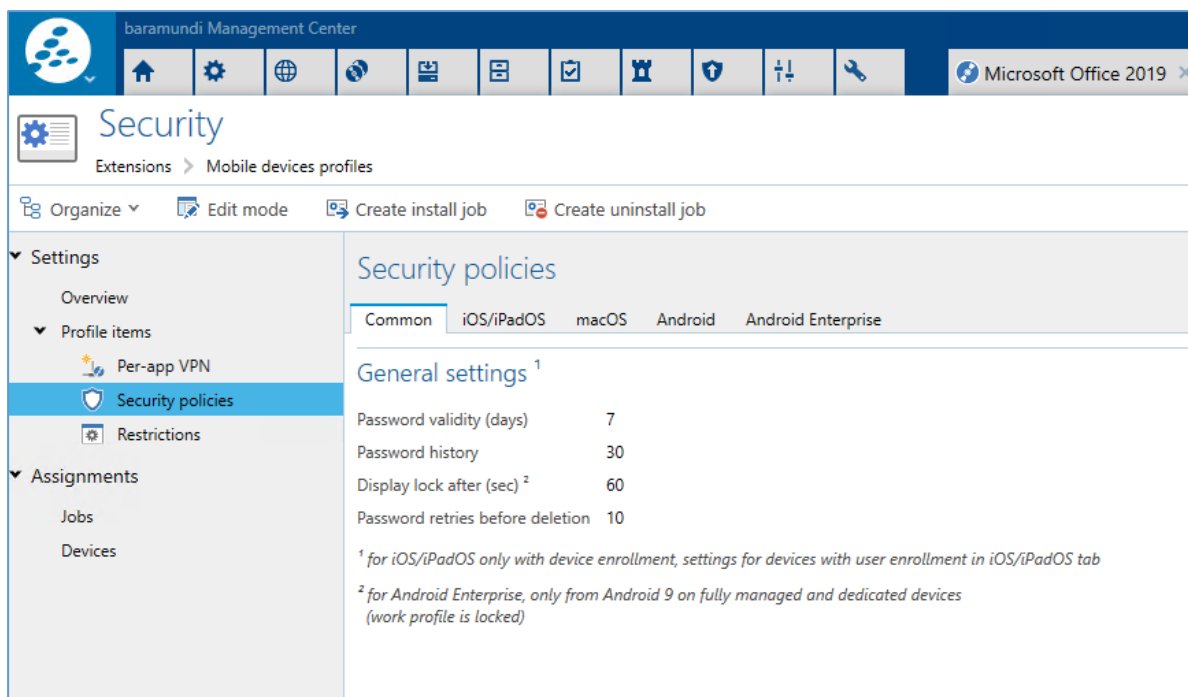
COSU devices are configured for a specific purpose, such as a barcode scanner or a cash register system. They run only predefined apps and do not require user identification. They are ideal for scenarios where devices are shared flexibly among multiple employees. Both Apple (via Kiosk Mode) and Android Enterprise (via Dedicated Device Mode) provide native management options for this.

2.2 Inventory

An EMM/UEM system should provide a comprehensive overview of all registered devices and their status, regardless of whether the device runs iOS, iPadOS, macOS, or Android. This includes hardware details, operating system versions, installed apps, security policies, and certificates. This enables administrators to track the device fleet, compliance, and security status at all times.

2.3 Enforce password protection

To protect valuable company data from unauthorized access, password policies can be enforced across platforms. EMM and UEM systems enable centralized configuration of password complexity and length, as well as activation of additional protective measures such as device encryption and biometric verification. This ensures security policies are enforced consistently across the entire company.



Configuring a security profile

2.4 Remote lock and wipe

If the device is lost or stolen, it can be remotely locked, wiped, and located, depending on the platform. The administrator can remotely reset forgotten passwords, enable Lost Mode (Apple) or Lockdown Mode (Android), or temporarily disable biometric authentication.

2.5 Updating device firmware

Just as important as preventing tampering is updating the firmware in a timely manner. This not only adds new features but also eliminates vulnerabilities.

A capable EMM distributes firmware updates centrally and lets you defer them within a defined window, for example, to validate in-house app compatibility before rollout.

On Apple devices (iOS/macOS), this is handled via Managed Software Updates, with enforcement and deferrals up to 90 days. On Android Enterprise, compliance policies monitor OS versions and automatically trigger updates.

On all platforms, an inventory with rules allows the administrator to remotely monitor firmware versions at any time.

Create new rule

Please define which OS versions are allowed for certain device types

Note: The lines will be checked from top to bottom. As soon as a matching hardware configuration for a device is found, it will be checked if the OS version is in the allowed version range.

Plattform	Hersteller	Modell	Kategorie	Eigentümer	min. Ver	max. Ver
Apple iOS/iPadOS	*	*	*		13.6	*
Android	Google	Nexus 4	*		11.0	*
Android	Google	Nexus 3a	*		10.0	*

Up

Down

Remove condition

Next >

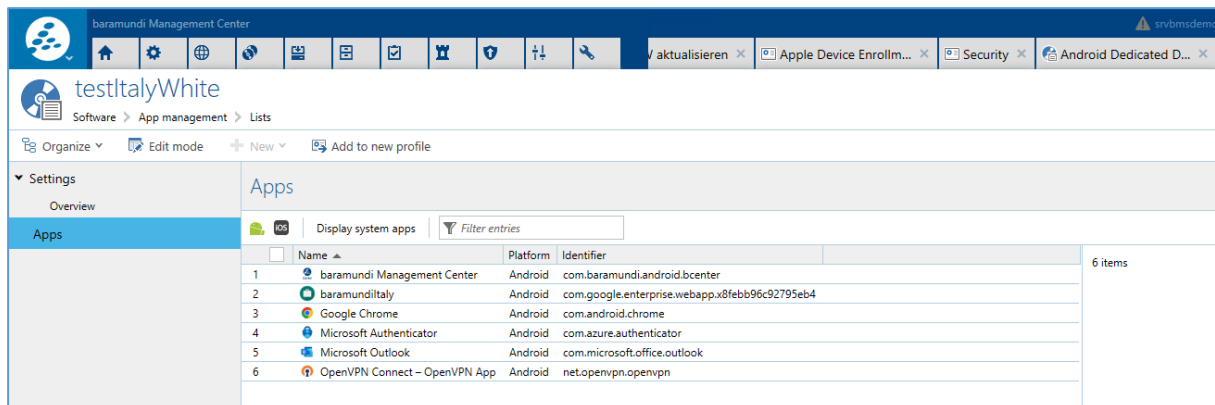
Cancel

Rules for checking operating system versions

2.6 Block or approve apps

The EMM should support blocking or approving apps on managed devices. Blocking prevents the installation or execution of malicious apps, while approval allows only explicitly permitted apps to be installed or launched.

Depending on the circumstances, app approval or blocking can be applied to a specific end device.



App selection for block or allow lists

2.7 Three areas of device management

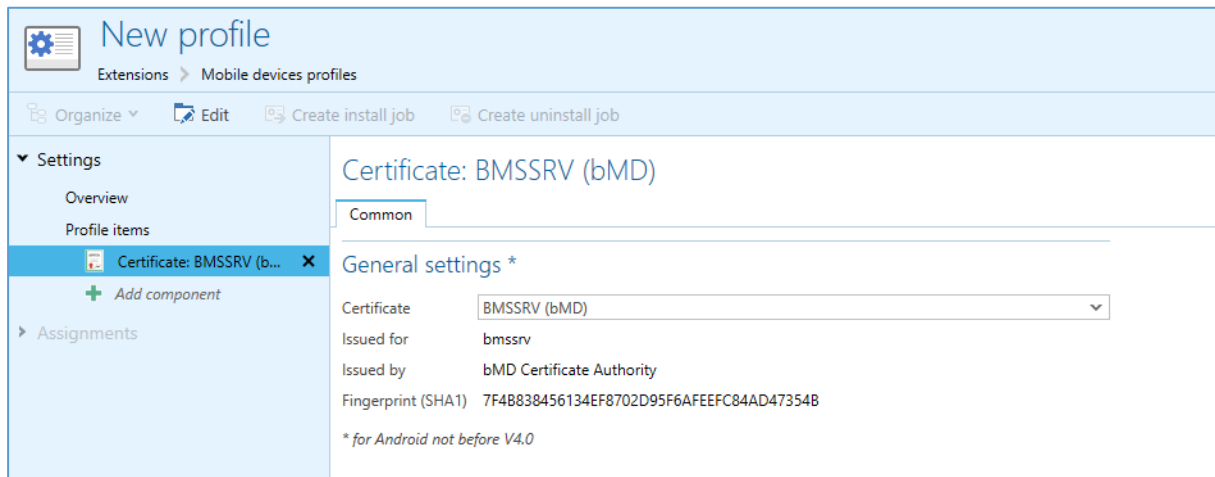
EMM encompasses three areas of mobile device management:

- **Mobile Device Management (MDM):** For system-level device management, including enrollment, inventory, OS updates, passcode and encryption policies, remote lock and wipe, Wi-Fi and VPN configuration, and compliance monitoring.
- **Mobile Application Management (MAM):** Covers app lifecycle management, which apps can access corporate data, policies such as preventing copy-and-paste between managed and unmanaged apps, and selective wipes of data and files.
- **Mobile Content Management (MCM):** Controls the flow of data and files used by managed apps, governs how content can be shared or forwarded, and ensures that corporate files can be opened only in approved apps.

In practice, the three areas overlap and are integrated into modern EMM/UEM solutions.

2.8 Security through certificates, distribution, and enterprise Wi-Fi

An EMM solution should enable the distribution of client enterprise certificates and support the required trust relationships with enterprise services.



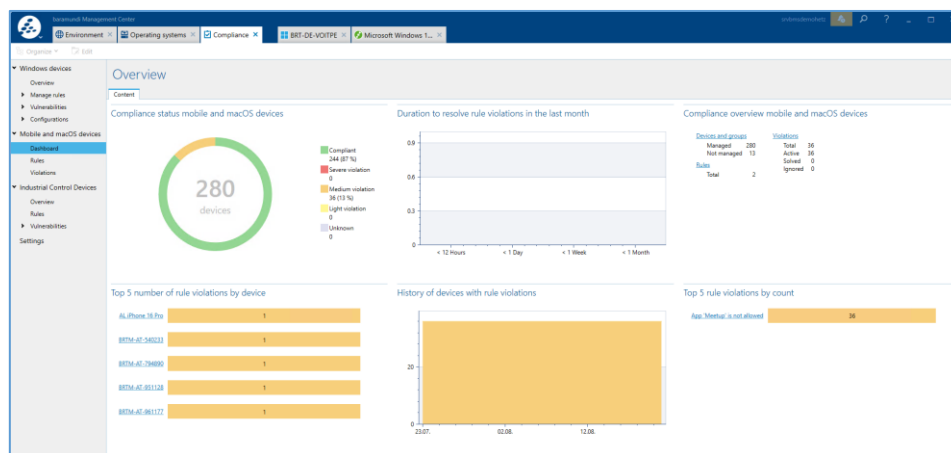
Profile component for client certificates

Certificates can be used to secure access to Microsoft Exchange or to implement secure enterprise Wi-Fi. Both rely on certificate authentication rather than user login.

2.9 Automated compliance monitoring

Compliance with company policies is especially important for mobile devices. In addition to app blocklists, allowlists and tamper detection, missing mandatory apps can be automatically detected and installed.

Compliance information should be clearly displayed on the dashboard, sorted by device or by the severity of violations. This allows the administrator to see at a glance where action is needed. Modern EMM solutions also offer automated measures, ranging from user email notifications to remote deletion in the event of critical violations.



Compliance Monitoring Dashboard

2.10 End-user self-service capabilities

Self-service offers users an elegant way to get immediate support while significantly reducing support requests. Pre-configured apps, password reset functions, and common tasks are available in the portal or in kiosk mode—without any IT intervention.

2.11 Apple Volume Purchase Program or Android Enterprise App Distribution

Both Apple and Android Enterprise provide proven solutions for centralized app license management.

The Apple Volume Purchase Program (VPP) and Android Enterprise app management enable centralized allocation and reuse of paid and free apps. Administrators can deploy apps to devices or users and revoke licenses as needed to reassign them to other devices or users.

Both platforms support flexible, efficient management of the entire app lifecycle—from distribution and updates to license revocation—and help ensure compliance with company-wide policies and requirements.

3 Comprehensive, efficient, and easy to use

This section covers the key selection criteria for EMM solutions: deployment model (integrated vs. standalone), implementation complexity, platform coverage, and operational usability.

3.1 Standalone, integrated, or co-managed: Which is right for you?

A fundamental decision is whether to adopt a standalone EMM tool, use EMM capabilities built into a UEM solution, or take a co-management approach by linking an EMM tool to a UEM system via an API. Integration enables centralized management of all clients through a single interface, while co-management can offer best-of-both-worlds management options. With or without co-management, an integrated solution is particularly suitable for companies with lean IT teams because it maximizes efficiency and productivity.

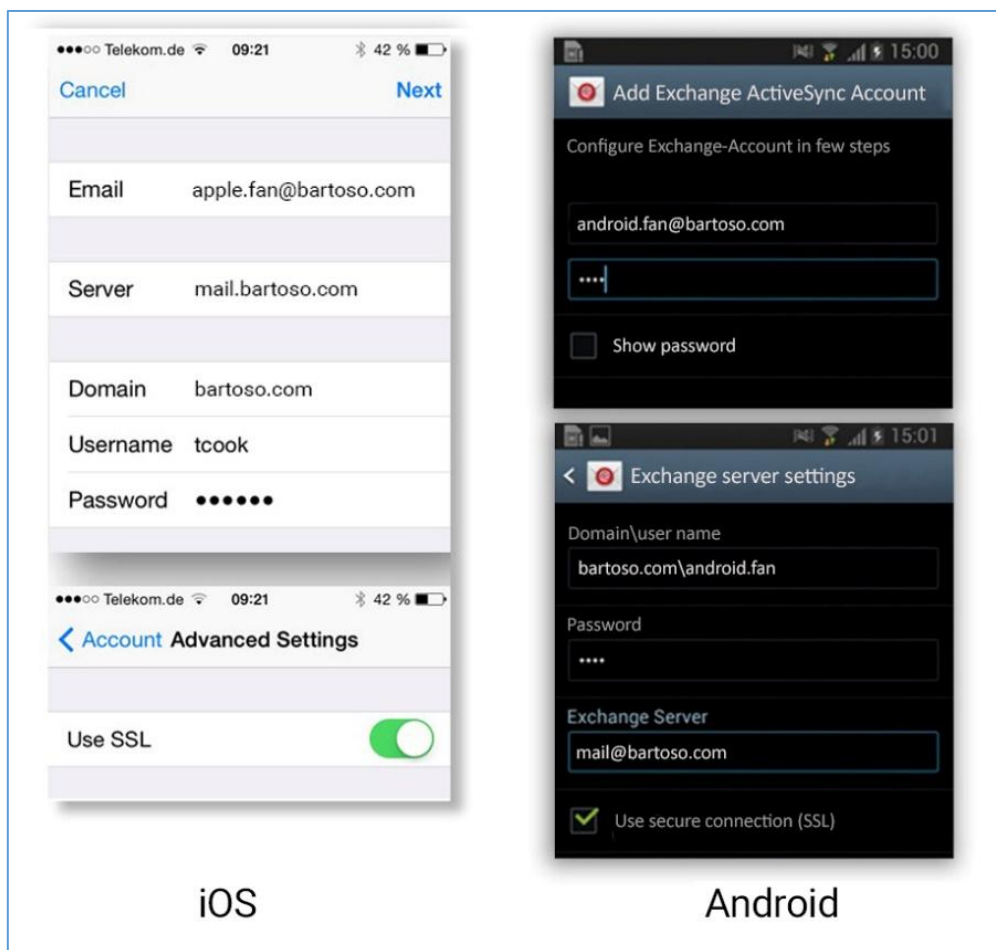
3.2 Implementation, training and usability

When choosing an EMM, administrators should consider the effort required for implementation, deployment, and training. Integration with the existing IT management infrastructure should be straightforward. In addition, an intuitive solution helps new administrators or IT contractors learn and become proficient with the system quickly. This also reduces training and operating costs.

3.3 The challenge of platform diversity

Administrators often have to support multiple mobile platforms, which means they need to understand, configure, and maintain them in detail. This work is complex and time-consuming.

The example of Exchange configuration for email services on Android and iOS shows that identical parameters (name, email address, domain, server, encryption) must be entered in separate dialogs.



Exchange configuration on different mobile platforms

A tool that enables uniform input across all managed devices is both desirable and valuable. A capable EMM that allows administrators to manage all mobile platforms through a single interface reduces configuration errors, shortens onboarding time, and provides consistent visibility across the device fleet.

Exchange account: Exchange

Common iOS Android Windows Phone

General settings *

Component name	Exchange
Display name on device	{RegisteredUser.Mail}
E-mail address	{RegisteredUser.Mail}
User name	{RegisteredUser.UserLogonName}
Domain	{RegisteredUser.Domain}
Exchange server (FQDN)	mail.bartoso.com
Encrypted communication	☒
Certificate selection	None

* for Android only supported by devices with Samsung KNOX or HTC Pro

Cross-platform Exchange configuration using EMM

3.4 Transparent management in real time

An effective EMM solution provides administrators with a continuously updated view of all managed devices, showing current status, compliance posture, and security events, without the need for manual queries. An up-to-date database also forms the basis for creating accurate reports and making informed decisions.

4 Checklist of important functions

	Software distribution and configuration
☐	Distribution Delay of firmware updates
☐	Support for native data separation
☐	Installation of apps with without user confirmation
☐	Uninstalling apps with without user confirmation
☐	Support for Apple Volume Purchase Program (VPP)
☐	Support for Automated Device Enrollment (ADE)
☐	Installation uninstallation with App Store disabled
☐	Installation Uninstallation of self-created company apps
☐	Self-service app: Kiosk
☐	Installation Uninstallation of certificates
☐	Parameterization of settings via variables
☐	Installation of hyperlinks (iOS: web clip)
☐	Deactivation of the camera
☐	Configuring access points (APN)
☐	Secure content distribution (MCM) with encryption
	Inventory
☐	Hardware information
☐	Configured restrictions (e.g., iCloud lock)
☐	Installed profiles
☐	Installed certificates
☐	SIM information
☐	Roaming status
☐	Security settings
☐	Last contact
☐	Device grouping
☐	App usage data and risk scores
	Security
☐	Remote lock Unlock Wipe
☐	Setting PIN/password requirements and complexity
☐	Set device encryption policies
☐	Support Allowlist Blocklist for apps
☐	Deactivation of system apps
☐	Disable Wi-Fi
☐	Deactivation of Bluetooth
☐	Password history Reset Set new password
☐	Allow/deny access to SD card
☐	Allow/deny access to app stores
☐	WLAN auto-connect
☐	Detect jailbreak/rooting
☐	Zero Trust Network Access (ZTNA)
	Compliance
☐	Detect missing required apps
☐	Detection of unwanted app installations
☐	Detection of incorrect configuration
☐	Detect outdated operating system versions
☐	Status and history of rule violations
☐	Automated remediation of violations
☐	Audit logs and compliance reports (e.g., NIST CSF, SOC 2, HIPAA, NIS2(if applicable))

5 Conclusion

Selecting an EMM solution requires aligning technical capabilities with your organization's device mix, compliance requirements, and IT team capacity. It is crucial to precisely define the scope of functions and to supplement this with practical tests of suitable providers. In addition to technology, the operating model and usability play a central role – as does employee acceptance. Without user adoption, even a technically sound deployment will underperform.

As organizations navigate regulatory and security compliance requirements and the realities of hybrid work and AI-assisted automation, IT managers should prioritize a balanced mix of the following elements:

- Company security requirements
- Employee acceptance of managed mobile devices
- Simple, intuitive operation

Only when all three points are considered will the introduction of an EMM solution succeed.

About baramundi software GmbH

As a specialist in unified endpoint management (baramundi Management Suite) and Proactive Endpoint Operations (baramundi Proactive Hub), baramundi software GmbH ensures that companies and organizations can manage work environments and digital workplaces efficiently, securely, and across platforms—both on-premises and in the cloud. baramundi software GmbH is headquartered in Augsburg, Germany. Founded in 2000, the company's products and services are entirely made in the EU and are supported by staff at its U.S. office in Boston and across the country. baramundi successfully collaborates with partner companies worldwide in sales, consulting, and customer support.

More information about baramundi: www.baramundi.com

Would you like to learn more about smart enterprise mobility management with baramundi? Register for the live webinar!

Discover how you can manage smartphones and tablets just as easily and reliably as PCs and notebooks.

<https://www.baramundi.com/en-us/events-trainings/webinars/>

Get in Touch!

We are looking forward to meeting you!



baramundi software GmbH
Forschungsallee 3
86159 Augsburg, Germany
+49 821 56708-380
request@baramundi.com



+48 735 91 44 54
request@baramundi.com



+44 2071 93 28 77
request@baramundi.com



+43 1 928 0136 0010
request@baramundi.com



baramundi software USA, Inc.
30 Speen St, Suite 501
Framingham, MA 01701, USA
+1 508 861 7561
requestUSA@baramundi.com



+41 77 280 49 79
request@baramundi.com



+39 340 8861886
request-italia@baramundi.com



+49 821 56708-390
request@baramundi.com



Making IT Admins Smile