



## ROI of UEM

The Advantages of UEM and Remote Management

## CONTENTS

1	Introduction .....	2
2	Why UEM is critical .....	3
3	UEM – Protecting Against Threats .....	4
3.1	More than just Mobile .....	4
3.2	Product Inventory and License Management .....	4
3.3	IT Staffing Ratios.....	5
3.4	Handling Increasingly Remote Users is impractical without Automation .....	5
3.5	Immediate Benefits of UEM.....	5
4	Achieving ROI with UEM.....	7
5	Picking a UEM – Seven Key Attributes to look for.....	8

© 2021 baramundi software AG

Statements about equipment and technical functionalities are non-binding and for information purposes only.

Subject to change. DocID WP-210628

Authors: Jack Gold, Analyst of J.Gold Associates

William Fendt, Product Manager, baramundi software AG

Franz Braun, PR Manager, baramundi software AG

Board of directors: Graduate engineer (FH) Uwe Beikirch | Dr. Lars Lippert

Chairman of the Supervisory Board Dr. Dirk Haft

Registered office and court of record: Augsburg, HRB No. 2064 | VAT ID DE 210294111

# 1 Introduction

*“Within 3-4 years, we expect 75%-85% of enterprises to have a majority of workers access corporate systems from at least 3-5 different end points, and not just the current traditional ones like PCs, smartphones and tablets. Indeed, as new Enterprise of Things devices become prevalent (e.g., autonomous vehicles, specialty machines, embedded intelligent systems smart personal devices), many with significant compute and user interface capabilities, enterprise users will demand access from any device, at any time, through multiple interfaces (e.g., voice, video, AR/VR) and over any connection. It will become increasingly impossible to have uniformly consistent management, security and user profile capability by installing a unique software component on each device. The only way companies can accomplish this will be through Unified Endpoint Management. Companies not effectively managing this transition will become noncompetitive through user disenfranchisement, lower employee productivity and increased infrastructure costs.”*

*J.Gold Associates LLC.*

Nearly every organization is challenged to keep all endpoint computing assets up to date and secure. Challenges continue to grow because of an expanding array of servers, desktops, laptops, tablets, mobile devices and the new reality of hybrid workforces. The combination of on-site and remote workers also increases the need to create and enforce configuration, usage and security policies for apps and data access.

The most efficient and effective way to enable IT staff to fully support the entire workforce is Unified Endpoint Management (UEM). UEM is a crucial capability that all organizations need to remain competitive by optimizing IT costs, mitigating cybersecurity risks and maximizing IT and user productivity.

This white paper discusses why UEM is so critical for the continued success of businesses worldwide, based on the research of J.Gold Associates, LLC.

## 2 Why UEM is critical

We estimate that the average corporate user has at least 3-5 endpoint devices they use on a regular basis. Even cloud-centric Chromebooks require IT management.

Accordingly, it's imperative that companies manage all endpoints from a consolidated UEM platform and enforces policies uniformly across all devices, apps and users. UEM also helps companies keep IT workloads manageable to maintain productivity and avoid the negative impacts of IT staff burnout, including higher personnel costs and lower quality user experiences that can affect hiring and retention.

Typical UEM features include:

- **Device Asset Management** (inventory, configuration, security, license management, lifecycle control)
- **Multi Device/OS support**
- **Fully Automated Remote Management** (No-touch OS upgrades, application installations, end user setup, remote access)
- **Provisioning/Policy enforcement** (configurations, encryption, device components enabled (camera, etc.), enrollment, network access, VPN)
- **Application Management** (app deployment and monitoring, protected space enablement, updates, user access, license management)
- **Security Management** (data isolation, device encryption, secured browsing, secured email/productivity, LDAP/AD directory interface)
- **Support Services** (remote device access, self-service portals, dashboards, help desk access)
- **Workspace Analytics** (monitoring apps/users, performance alerting, enhanced security enforcement, remediation)





## 3 UEM – Protecting Against Threats

UEM improves overall user and device management and enhances corporate security. Companies that deploy stronger device management and security oversight through enterprise-class UEM services are 25%-35% less likely to have a security breach.

### 3.1 More than just Mobile

With nearly ubiquitous use of mobile devices, a stand-alone MDM solution is no longer cost effective or an efficient use of IT resources. Enterprises must eliminate any existing stand-alone MDM deployments and deploy a UEM solution that universally manages and secures all endpoints.



### 3.2 Product Inventory and License Management

Management transparency is essential for ensuring security, productivity and cost optimization. The growing number of device types and apps means that many organizations don't have a good understanding of existing IT inventory, including:

- A lack of information on the status of warranties, upgrade cycle requirements, disposal of aged assets and the physical location of each device.
- The actual usage of specific application versions, which leads to over or under licensing.

UEM maintains a full and current inventory of all devices and applications, as well as employee usage of applications and licenses. A complete inventory can save companies from 10%-35% of their license costs and eliminates any potential penalties for overuse of application and/or OS licenses.

### **3.3 IT Staffing Ratios**

UEM can significantly increase the number of end users that an IT person can support. The typical ratio of IT-support-people-to-end-users in a non-UEM enabled enterprise is about 1:50. We estimate that UEM can increase the ratio to about 1:100 end users or as high as 1:200 in organizations with less complex computing environments.

This can amount to millions of dollars in savings each year in both hard and soft costs, allowing IT to better allocate resources and enhance user experiences with increased and more responsive IT support.

### **3.4 Handling Increasingly Remote Users is impractical without Automation**

Companies that have a UEM capability in place have had far fewer challenges than those without. It's expected that as much as 50% of workers will continue to work remotely at least part time even after the current pandemic subsides.

The only viable way to manage devices and applications remotely is through an automated system that can configure, update, add policies, enable apps, etc., with zero touch capabilities from IT staff, through scripted workflows and similar mechanisms. This remote management capability is a critical component of any UEM toolset and can provide an advantage for not only remote workers, but also for those organizations that have a distributed office environment.

### **3.5 Immediate Benefits of UEM**

Many companies considering UEM solutions may perceive them as complex, hard to deploy or with delayed benefits. In actuality, there are many immediate benefits even if you don't use all of the functionality available. Even if deployed on a specific project with a singular goal,

such as an OS upgrade, UEM automation offers immediate improvements and returns compared to manual processes.

Benefits include:

- Uniform installation of operating systems and software
- Updating and patching third-party software without losing productivity
- Seamless Windows 10 Upgrade Rollout to all devices
- Automation of routine tasks through scheduling functions
- Modernizing the core infrastructure
- Complete control of the IT support landscape
- Preparing for growth of new users, devices and systems

## 4 Achieving ROI with UEM

Although there are UEM solutions available at little or no cost, for the most part you have to realize: “Free Isn’t Free.” Many enterprises find that after deploying inexpensive tools there are gaps in their management and security capabilities, particularly around the increasing variety of device types and user workloads. Enterprises should evaluate how ROI is affected by specific UEM capabilities, including:



**IT Resources:** Any UEM selected must offer an ability to leverage limited IT resources and make them more efficient and effective. As indicated above, we expect that an optimum UEM tool can improve IT:user staffing ratios from 1:50 to 1:100 or more. Using this as a benchmark, in a typical 5,000-employee company with a burdened IT compensation rate of \$100K per year, a company adopting an effective UEM toolset can save \$5M annually.

**Security Breach Mitigation:** A proper UEM strategy can significantly mitigate cybersecurity risks and potentially save a company from the high cost of a breach, as well as regulatory penalties and loss of customers. It’s imperative that any UEM solution includes a capability to manage any and all end user devices, especially mobile devices, and do so in a complete and optimum fashion.

**Lost Productivity Enhancement:** We estimate that the average end user will have 4-6 calls per year to the help desk for support, with each taking 30-60 minutes to resolve. In a 5,000 employee company, that amounts to 2,500 to 5,000 hours of lost productivity plus IT time to resolve the issues. Assume a blended overhead employee rate of \$100K per year, the overall cost of 5,000 hours of resolving problems is \$240K. We estimate that an effective UEM implementation could cut that time by 25%-50%.



## 5 Picking a UEM – Seven Key Attributes to look for

We recommend that enterprises evaluating UEM solutions look at the following key attributes and assess if products being evaluated will meet the organization's needs:


- 1) Available to manage a variety of device types and OS platforms (e.g., PC, smartphones, Windows, iOS, Android, etc.)
- 2) Ability to integrate with other corporate apps (e.g., through APIs and connects to AD, Security, etc.)
- 3) Single management view across all platforms/devices/apps/infrastructure
- 4) Support enablement through easy to navigate analytics
- 5) Ability to easily deploy new end user services
- 6) A vendor committed to upgrading the UEM capability
- 7) Vendor support to enable customers to fully utilize all UEM capabilities through support, training and application assistance


**We are looking forward  
to meeting you!**


Get in touch!


**baramundi software AG**

Beim Glaspalast 1  
86153 Augsburg, Germany

 +49 821 5 67 08 - 380  
[request@baramundi.com](mailto:request@baramundi.com)  
[www.baramundi.com](http://www.baramundi.com)


 +44 2071 93 28 77  
[request@baramundi.com](mailto:request@baramundi.com)  
[www.baramundi.com](http://www.baramundi.com)

 +48 735 91 44 54  
[request@baramundi.com](mailto:request@baramundi.com)  
[www.baramundi.com](http://www.baramundi.com)

 +49 821 5 67 08 - 390  
[request@baramundi.com](mailto:request@baramundi.com)  
[www.baramundi.com](http://www.baramundi.com)


**baramundi software USA, Inc.**

30 Speen St, Suite 401  
Framingham, MA 01701, USA

 +1 508 808 3542  
[requestUSA@baramundi.com](mailto:requestUSA@baramundi.com)  
[www.baramundi.com](http://www.baramundi.com)

**baramundi software Austria GmbH**

Landstraßer Hauptstraße 71/2  
1030 Wien, Austria

 +43 1 7 17 28 - 545  
[request@baramundi.com](mailto:request@baramundi.com)  
[www.baramundi.com](http://www.baramundi.com)