



# Your foundation for digital transformation

Crucial steps toward a successful implementation

## CONTENTS

1	Digital transformation – What’s all the effort for? .....	2
	The advantages of “digital first” .....	3
	Important prerequisites .....	3
2	Laying the foundation – Security, performance and productivity .....	4
	Automation, configuration, patches .....	4
	baramundi delivers .....	5
3	Detailed steps to start the digital transformation .....	8
4	The effort is worthwhile .....	9
5	About baramundi software AG .....	10

© 2020 baramundi software AG

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

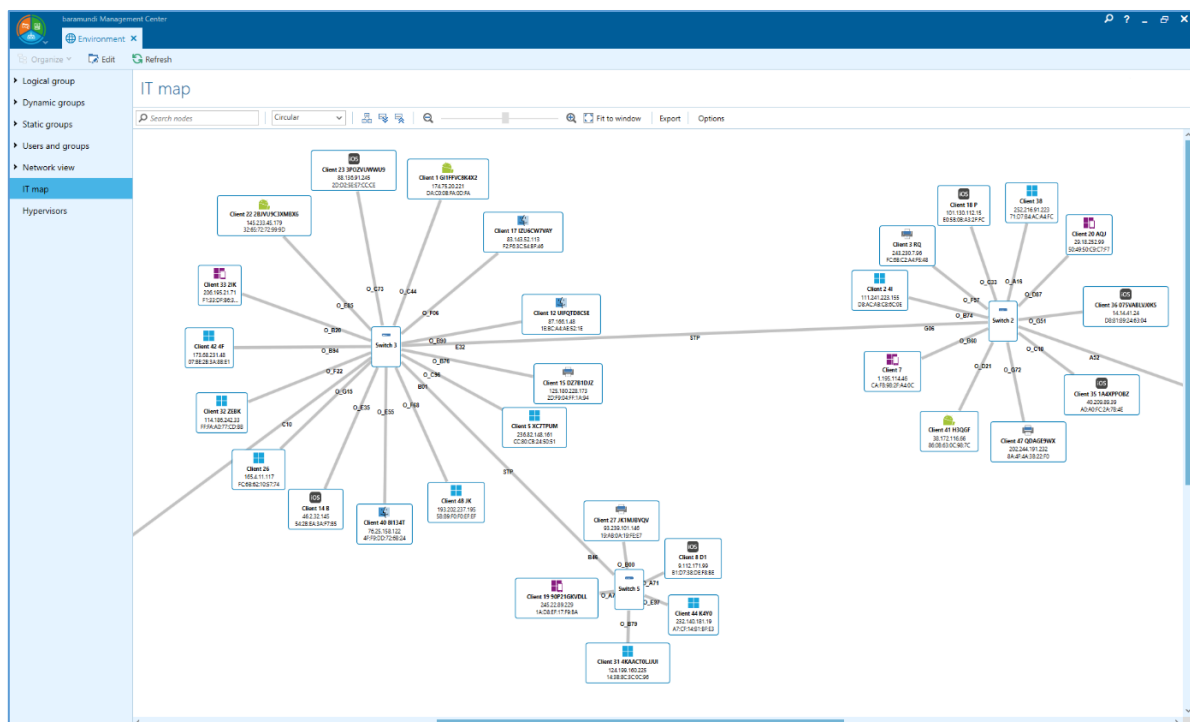
Subject to change. DocID WP-200828

# 1 Digital transformation – What's all the effort for?

The pandemic of 2020 achieved in just a few months what experts worldwide were unable to accomplish over the last 20 years: to encourage companies to actively engage with the possibilities of digitalization.

“Necessity is the mother of invention,” as the saying goes. In this case, however, nothing needed to be invented – the required technology has existed for a long time. Instead, one would need to say that necessity is the mother of *motivation*.

Driven by the need to ensure resilient and flexible operations during a pandemic, many companies have taken the first steps toward digital transformation. However, securing the long-term benefits that digitalization can provide requires a strong foundation for IT infrastructure management. That starts with making meaningful and lasting improvements in the efficiency of essential day-to-day IT operations.





## The advantages of “digital first”

Some companies had planned or already begun to adopt what industry observers call a “digital first” approach to daily operations prior to the pandemic. But for most, the shift to a largely remote and distributed IT environment began dramatically with a massive and often improvised effort by IT departments to equip their users to work safely and productively from home. It was a learning experience for everyone.

One of the immediate insights is that in-person, in-office work is not the necessity or priority that it was long assumed to be. The rapid, at-scale adoption of desktop video conferencing and at-home work demonstrated that a lot of traditional office commutes, meetings and business trips were not really required to retain a high level of productivity. It also showed companies that they could reduce or even eliminate costs of physical office space.

Employees quickly recognized the productivity and lifestyle benefits of not having to get in the car, train, or on an airplane in order to get their work done.

IT teams also quickly began to understand something they knew intuitively but had not yet experienced: shifting to fully or predominantly digital operations involves much more than setting up and deploying laptops and mobile devices and configuring VPNs. In fact, enabling and supporting reliable and secure work environments, processes, communications and information-sharing by IT became dramatically more complex.



Successful implementation of digital transformation requires a high-performance, stable and – especially – secure infrastructure. Building that infrastructure takes time, both for planning and execution. At the same time, IT staff have to keep up with maintaining, upgrading, troubleshooting and securing a wider range of remote and on-premises endpoints over a variety of network connections. On top of that, organizations have in many cases reduced IT headcounts since the start of the pandemic.

The automation, flexibility and real-time management tools found in Unified Endpoint Management (UEM) systems offer a reliable and practical way to address those immediate needs and provide the foundation for the longer-term adoption and management of the new digital infrastructure.

## 2 Laying the foundation – Security, performance and productivity

While it's always been important, network and endpoint security have emerged as both an increasingly complex operational concern and a major stumbling block on the path to digital transformation. Security gaps in IT infrastructure, which could be mitigated or prevented with relative ease behind the safety of enterprise-grade firewalls, have become more challenging with the prevalence of remote work. Consumer-grade internet routers, often provided by the Employee's ISP with just default configurations, and the mix of user- and company-owned devices used by employees on home networks, elevate the risk of exposures and significantly scale up the availability of surfaces for attacks by cyber-criminals. Software used for employee team communication and collaboration can present additional attack vectors for intruders seeking access to company and personal user data.

### Automation, configuration, patches

The human factor remains the biggest security risk. Achieving a balance between security and user productivity is crucial, otherwise employees will bypass safety measures that stand between them and their day-to-day work. Strict access control and security automation offers a viable compromise and a way forward.

Ensuring security is time-consuming, especially on larger networks. However, the most effective measures are relatively simple and compatible with users' needs and preferences:

- proper system configurations
- closing security gaps via patch management
- timely distribution of application updates

The good news is that the majority of this work can be automated with an effective UEM system. Automated packages including proper configurations, updates and patches can be created once then distributed consistently and reproducibly to all target endpoints when and as needed.

## baramundi delivers

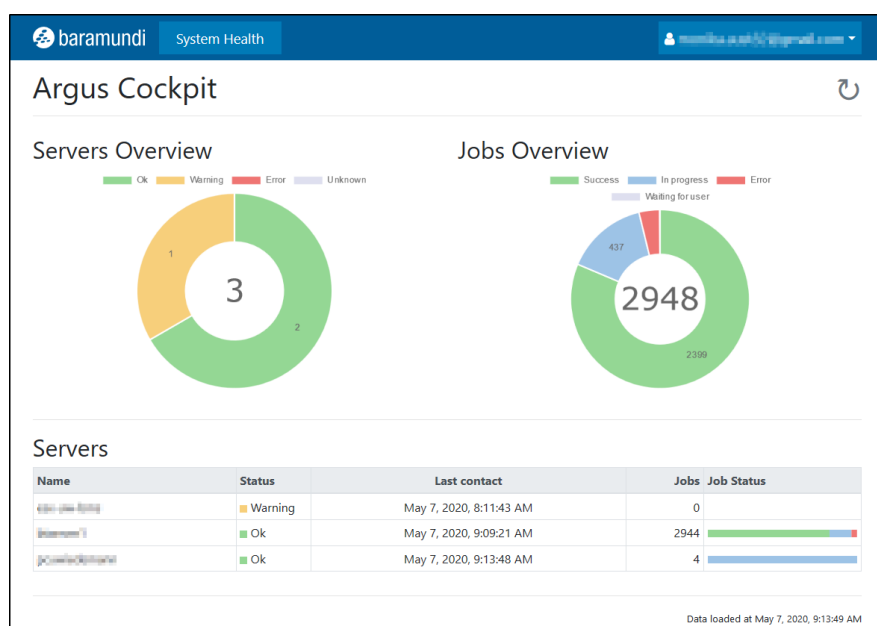
The introduction of baramundi Unified Endpoint Management offers multiple time-saving advantages with functions for automating routine endpoint management of classic desktop clients as well as mobile devices:

### 1. Gather comprehensive insights:

An automated detailed inventory collection of software and hardware provides a quick and current overview of the entire estate. Beyond simply showing what's deployed, inventory data is the cornerstone for the day-to-day management of endpoints and servers, IT budgeting and cost control, and for many aspects of data security.

For example, the License Management module uses inventory data to generate summary and detail reports of current software licensing status. That can help reduce or eliminate unnecessary new license purchases and save time, money and possibly your sanity in the event of a software audit. Inventory reports also make it easier to detect and, if necessary, remove unauthorized applications from user machines with our Deploy module. With baramundi's AUT (application usage tracking) module, the data can also be used to assess user acceptance of new software items or determine if deployed apps are actually being used.

Finally, the cloud-enabled baramundi Argus Dashboard offers a way for authorized IT admins to monitor the system status of one or more baramundi Management Servers via any web browser on any device. That means you don't have to wait until the next morning to see if the after-hours software deployment or patch job that you scheduled completed successfully or if there were errors and exceptions.



## **2. Providing security:**

The automated vulnerability scan provides current and reliable information about exposures and vulnerabilities on all endpoints. It identifies known vulnerabilities on the endpoints using current CVE data from trusted cybersecurity sources, provides easy to read and act upon reports of found vulnerability counts and severity across all devices.

Our MS Patch Management and Managed Software modules can then be used to deploy appropriate and timely remediations for each affected system.

Beyond the typical Microsoft OS and Application stack, the Managed Software module offers ready to deploy patches and updates for third-party applications in the form of tested, fully automated installation packages.

Many companies realized that their current tools for patching and maintaining their environment fell short when it came to managing a large remote workforce as these were often explicitly designed and optimized for LAN use.

baramundi also works for all remote devices that are neither connected via the LAN nor VPN networks, but merely have internet connectivity. This way home or mobile endpoints can be updated or patched securely without having to rely on often unstable and already heavily utilized VPN connections.

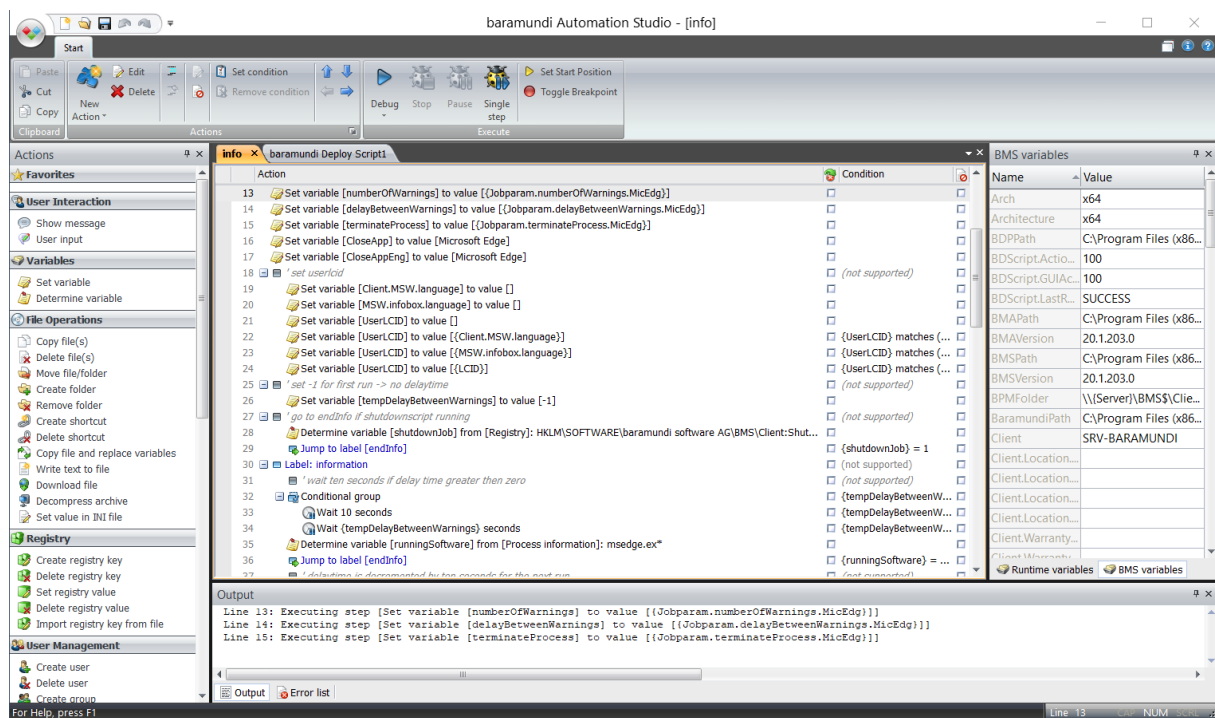
## **3. Making time:**

Automation Studio is a powerful tool that can automate installations and configurations via a drag-and-drop scripting interface that does not require actual coding. Everything from simple administrative processes to more complex installations can be automated, including tasks that normally require manual interaction such as simple mouse clicks, answer dialog boxes or check/uncheck selection boxes.

Since the baramundi Management Suite (bMS) is built around the concept of “jobs,” each automation package once created becomes reusable and can be offered repeatedly, triggered manually or scheduled for execution on as many endpoints as needed.

Via baramundi connect third-party systems can be integrated with baramundi.

An external ticketing system can also be used to trigger such jobs to e.g. reinstall corrupted or damaged applications, wipe local caches, reset local account passwords and/or trigger a remote restart.





### 3 Detailed steps to start the digital transformation

IT admins at many companies have found the following steps to be the most effective for building a solid and secure foundation for digital transformation activities:

1. **Document the current state of the IT estate:**

A clean inventory of all of the elements in your infrastructure is a must before beginning any digital transformation initiative. Inventory data informs strategic and tactical planning, and establishes a baseline. It's also essential for avoiding unpleasant surprises down the road.

2. **Fix security vulnerabilities:**

Just as no one wants to set sail on a boat full of holes, no one should expose a network with security gaps to the outside world. Automated scans and patch rollouts for operating systems and common applications are the first steps toward securing your company's infrastructure.

3. **Ensure proper system configurations:**

Many security and application problems are the result of poor configurations. Anyone who takes the time and effort to create correct OS and system configurations that comply with corporate policies and guidelines can use those as templates for future rollouts.

4. **Script out installations of common apps:**

All applications commonly used within the company can be packaged up as automated installations and rolled out or reinstalled quickly to devices when needed without any additional effort. Role based software that is typically only used by certain groups within the company (Sales, Accounting, Marketing, Production floor) can be layered on top of the basic configuration and corporate standard software as needed on certain endpoints.

5. **Establish user self-service Kiosks:**

Via a self-service interface, any additional and usually optional mobile and Windows application can be offered on demand. That's a valuable time-saving convenience for administrators, the helpdesk and users alike. Such commonly offered on-demand packages can also entail tasks typically performed with help from the service desk, such as disk cleanups, browser cache resets or a local printer installation.

## 4 The effort is worthwhile

From a practical perspective, the initial investment in Unified Endpoint Management yields dividends in a very short time: With colleagues working remotely, times of walking by the office to fix something manually have to some extent passed. Automation saves time and money and increases the efficiency of the IT department. It also frees staff resources for higher-value projects including planning and preparation for digital transformation activities. More broadly, the profound changes required in company operations as a result of the pandemic have cast the role of IT departments in a new light – not as a necessary cost center but as a major factor for business success in the new digital-first world.



## 5 About baramundi software AG

baramundi software AG provides efficient, secure and cross-platform management of workplace environments for organizations of all sizes and in diverse industries worldwide. More than 3,500 baramundi customers benefit from our 20-plus years of experience in endpoint management, our engineering expertise, intuitive solutions and superior customer support. They choose baramundi Management Suite for its holistic, future-oriented approach to Unified Endpoint Management. Client, Mobile Device and Endpoint Security management take place within a common admin interface, in a single database, following uniform standards.

baramundi Management Suite optimizes IT Management processes by automating routine tasks and providing a comprehensive overview of the status of all devices. Our solutions relieve the pressure on IT administrators and ensure that users have the necessary rights and applications on all platforms and form-factors, including PCs, laptops or mobile devices – anytime and anywhere.

baramundi software AG headquarters are located in Augsburg, Germany. Since its founding in the year 2000, baramundi's products and services are 100% Made in Germany. baramundi partners with companies in sales, consulting and user support worldwide.

For more information on baramundi visit [www.baramundi.com](http://www.baramundi.com)

### **Ready to take a closer look at the baramundi Management Suite?**

Find out how you can use the baramundi Management Suite to manage and secure your PC clients, servers and mobile devices by viewing one of our live or on-demand webinars at:

[www.baramundi.com/it-training/](http://www.baramundi.com/it-training/)

# The Full Potential of the baramundi Management Suite

- |   |   |   |
|---|---|---|
|  Inventory Hardware and Software |  Manage Mobile Devices |  Backup and Restore Systems, Data and Settings |
|  Install Operating Systems       |  Smart IT Management   |  Integration with Other Solutions              |
|  Distribute Software Easily      |  Guarantee Security    |   |



## **baramundi Inventory**

Comprehensive Overview of All Hardware, Software and Data



## **baramundi Network Devices**

Detects SNMP Printers, Routers, Switches and Other Devices, and Visualizes Network Topology



## **baramundi AUT**

Finds Unused Software and Helps Reduce Licensing Costs



## **baramundi Energy Management**

Monitor Endpoint Power Consumption to Reduce Energy Costs



## **baramundi License Management**

Comprehensive Overview of Software License Status to Avoid Over- and Under-Licensing



## **baramundi OS-Install**

Install Operating Systems Quickly and Natively



## **baramundi OS-Cloning**

Create and Deploy OS Images



## **baramundi Deploy**

Automated and Flexible Software Deployment



## **baramundi Automate**

Quick and Secure Workflow Automation



## **baramundi Mobile Devices**

Automated Enterprise Mobility Management (EMM)



## **baramundi Mobile Devices Premium**

Secure and Separate User and Company Data on Mobile Devices, and Manage Android Dedicated Devices



## **baramundi Vulnerability Scanner**

Automated Vulnerability Scanning of PCs and Servers and Fulfillment of Security and Compliance Policies



## **baramundi Patch Management**

Reliable, Rule-Based Patch Deployment with Automatic or Customizable Controls



## **baramundi Managed Software**

Provides Updates and Security Patches for 3rd Party Applications as Tested, Deployment-Ready Packages



## **baramundi Defense Control**

Easy and Comprehensive Management of Windows Native BitLocker Encryption



## **baramundi Disaster Recovery**

Accurate Drive Backup and Restoration



## **baramundi Personal Backup**

Efficient Backup and Restore of User Data and Settings



## **baramundi Connect**

SOAP and REST based Interfaces To Helpdesk, License and Asset Management, and Other IT Systems



## **baramundi Argus Cockpit**

Monitor IT system and job status from anywhere at any time via the cloud



## **baramundi Remote Control**

Support for Remote Users and Server Maintenance





# 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)