



Automatisierung im Endpoint Management

*Routineaufgaben optimieren –
von OS-Deployment bis NIS2-Compliance*

Inhalt

1 Steigende Anforderungen an IT-Abteilungen	03
2 Routinearbeiten automatisieren	04
2.1 Betriebssysteme und Anwendungen verteilen	04
2.2 Schwachstellen erkennen und Updates automatisieren	06
2.3 Hardware und Software inventarisieren, Lizenzen managen	07
2.4 Intelligent automatisieren: Zeitsteuerung und Self-Service	09
2.5 Integration in die bestehende Infrastruktur	10
3 Schnittstellen und Co-Management	11
4 Mobilgeräte managen	12
5 Datensicherheit und Datenschutz	15

© 2026 baramundi software GmbH | Aussagen über Ausstattung und technische Funktionalitäten sind unverbindlich und dienen nur der Information. Änderungen vorbehalten.



1 Steigende Anforderungen an IT-Abteilungen

Die Entwicklung der IT schreitet immer rascher voran. Von Zuses Z1 zu den ersten PCs vergingen Jahrzehnte, heute sorgen KI-Technologien und monatliche Revolutionen in Hardware und Software für Tempo. Mit der Leistungsfähigkeit und Vielfalt der Geräte wachsen auch die Anforderungen an die IT. Es bietet sich daher an, die Verwaltung aller Endgeräte in einer Lösung zu bündeln. Damit lassen sich einheitliche Standards durchsetzen und ein umfassender Überblick über den Zustand des Netzwerks und aller Endgeräte gewinnen.

Routineaufgaben automatisieren

Mit einem Endpoint Management System können zudem Routineaufgaben automatisiert und somit effizienter, schneller und einfacher erledigt werden. Das sorgt für die nötige Übersicht und erhöht gleichzeitig die Sicherheit des Unternehmensnetzwerks. Dieses Dokument gibt einen Überblick über Administrationsaufgaben, die auf jeden Fall automatisiert werden sollten.

The screenshot displays the Ivanti Management Center 2026 R2 interface. On the left, a navigation pane shows a hierarchical tree of logical groups, including 'Cologne' and 'Frankfurt'. The main area is divided into a table of devices and a detailed view of a selected device.

Name	Last contact	Comment
BRT-DE-352308	18 months ago	Automatically created by ACSync from LDAP://CN=BRT-DE-352308.Ou=Cologne.Ou=Germany.Ou=barco
BRT-DE-354180	17 months ago	Automatically created by ACSync from LDAP://CN=BRT-DE-354180.Ou=Cologne.Ou=Germany.Ou=barco
BRT-DE-359176	18 months ago	Automatically created by ACSync from LDAP://CN=BRT-DE-359176.Ou=Cologne.Ou=Germany.Ou=barco
BRT-DE-371295	18 months ago	Automatically created by ACSync from LDAP://CN=BRT-DE-371295.Ou=Cologne.Ou=Germany.Ou=barco
BRT-DE-375175	18 months ago	Automatically created by ACSync from LDAP://CN=BRT-DE-375175.Ou=Cologne.Ou=Germany.Ou=barco
BRT-DE-381081	17 months ago	Automatically created by ACSync from LDAP://CN=BRT-DE-381081.Ou=Cologne.Ou=Germany.Ou=barco
BRT-DE-387640	18 months ago	Automatically created by ACSync from LDAP://CN=BRT-DE-387640.Ou=Cologne.Ou=Germany.Ou=barco
BRT-DE-395643	17 months ago	Automatically created by ACSync from LDAP://CN=BRT-DE-395643.Ou=Cologne.Ou=Germany.Ou=barco
BRT-DE-397209	18 months ago	Automatically created by ACSync from LDAP://CN=BRT-DE-397209.Ou=Cologne.Ou=Germany.Ou=barco
BRT-DE-417224	17 months ago	Automatically created by ACSync from LDAP://CN=BRT-DE-417224.Ou=Cologne.Ou=Germany.Ou=barco
BRT-DE-419896	17 months ago	Automatically created by ACSync from LDAP://CN=BRT-DE-419896.Ou=Cologne.Ou=Germany.Ou=barco
BRT-DE-420383	17 months ago	Automatically created by ACSync from LDAP://CN=BRT-DE-420383.Ou=Cologne.Ou=Germany.Ou=barco
BRT-DE-428920	17 months ago	Automatically created by ACSync from LDAP://CN=BRT-DE-428920.Ou=Cologne.Ou=Germany.Ou=barco
BRT-DE-428957	17 months ago	Automatically created by ACSync from LDAP://CN=BRT-DE-428957.Ou=Cologne.Ou=Germany.Ou=barco
BRT-DE-429937	18 months ago	Automatically created by ACSync from LDAP://CN=BRT-DE-429937.Ou=Cologne.Ou=Germany.Ou=barco
BRT-DE-434680	18 months ago	
BRTM-DE-371295	17 months ago	
BRTM-DE-381081	17 months ago	
BRTM-DE-395643	18 months ago	
BRTM-DE-403183	17 months ago	
BRTM-DE-409937	17 months ago	
BRTX-DE-419896	18 months ago	

The detailed view on the right shows the following information for device BRT-DE-354180:

- Group: Logical group/Germany/Cologne
- Domain: barco.local
- Host name: BRT-DE-354180
- Registered user: stefan.wester@barco.local
- User is logged on: Yes
- Operating system: Windows 8
- OS version: 6.2.9200
- Release ID: --
- Display Version: --
- Reinstallation allowed: No
- Primary IP: --
- Primary MAC: 883268667935
- UUID: --
- Last channel: LAN
- Tenant name: --
- Autopilot: No
- Co-management: No
- Modem Management: Not managed
- Last contact: 17 months ago (3/27/2025 3:17 PM)
- Local time: 3:58 PM (UTC+01:00 Europe/Berlin)
- Risk level: No scan is for
- Serial number: 0CKGB3AMJ7N
- Comment: Automatically created by ACSync from LDAP://CN=BRT-DE-354180.Ou=Cologne.Ou=Germany.Ou=barco on 25.04.2019 10:38

Einheitliche Übersicht über alle Gerätetypen/Plattformen

2 Routinearbeiten automatisieren

In diesem Kapitel erfahren Sie, wie automatisierte OS- und Softwareverteilung, Patch-Management, Inventur, Self-Service und API-Integrationen Schwachstellen schließen, Compliance sichern und den Endpoint-Alltag entlasten.

2.1 Betriebssysteme und Anwendungen verteilen

Ein neuer Mitarbeiter wird eingestellt. Für die IT-Abteilung heißt das: Ein PC-Arbeitsplatz und/oder ein Notebook müssen bereitgestellt werden. Die Neuinstallation mit Betriebssystem und allen benötigten Anwendungen (z. B. via Autopilot und Co-Management) nimmt – inklusive aller nötigen Neustarts, der Auswahl der passenden Treiber etc. – schnell mehrere Stunden in Anspruch. Mit einer Managementlösung schrumpft dieser Aufwand auf wenige Mausklicks zusammen.

Anstatt von Hand oder per Skript ein Setup ablaufen zu lassen, wird das neue Gerät automatisch im Netzwerk erkannt. In einem Durchgang wird die Festplatte vorbereitet und es werden die nötigen Treiber zugeordnet. Intelligente Lösungen nutzen die native Installationsmethode des OS-Herstellers und erhalten so den vollen Gewährleistungsanspruch. Per Wake-on-LAN können Rechner sogar über Nacht neu installiert werden.

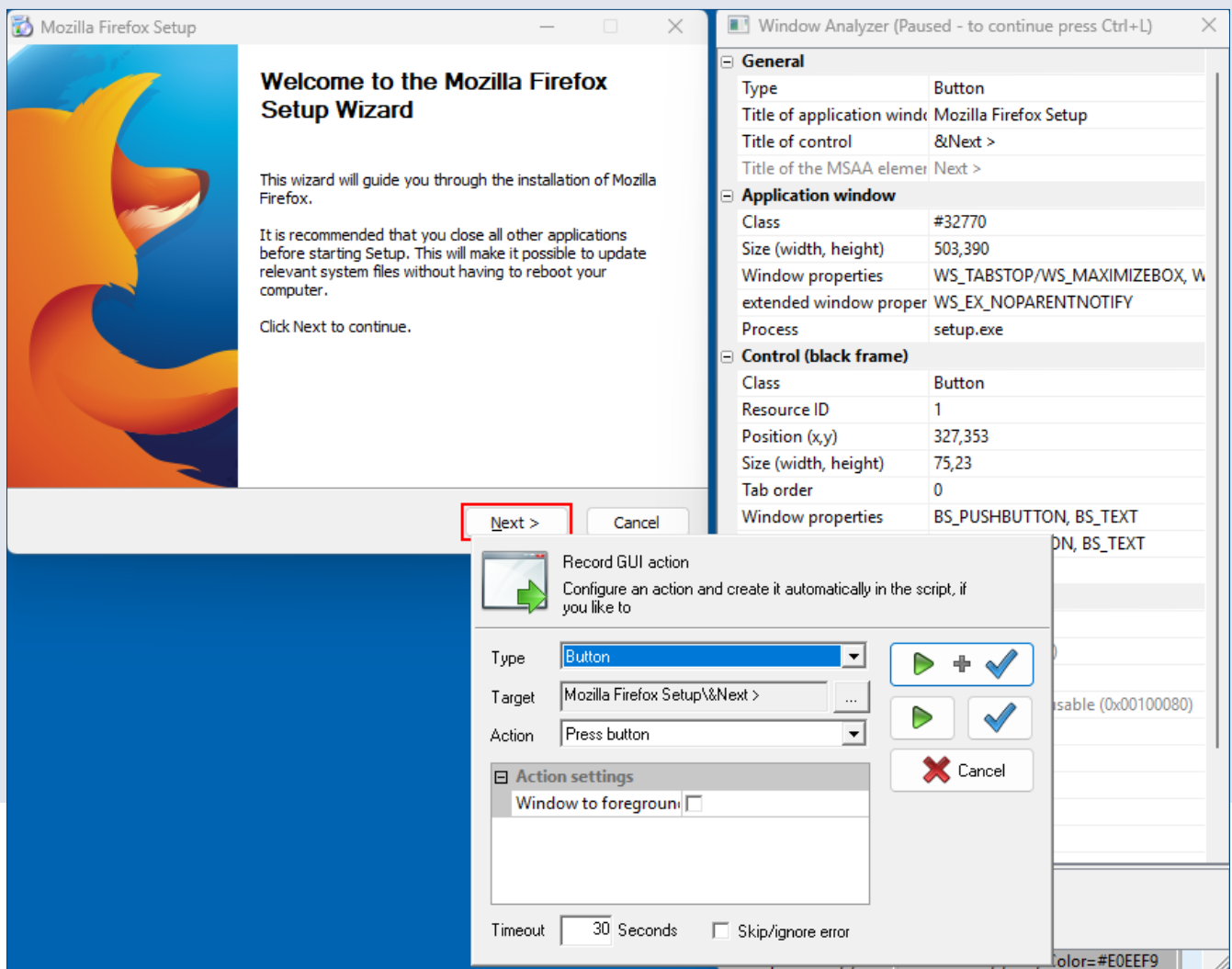
Anwendungssoftware automatisch verteilen

Die automatisierte Softwareverteilung entlastet IT-Abteilungen und schafft durchgängig standardisierte Systemumgebungen. Für jedes Einsatzprofil wird eine definierte Standardausstattung hinterlegt, die sich bei Bedarf per Mausklick auf einzelne oder mehrere Geräte parallel ausrollen lässt – inklusive Neustarts, Statusrückmeldungen und Fehlerprotokollierung. Bereits konfigurierte Verteilungsaufgaben können jederzeit wiederverwendet werden, etwa bei neuen Mitarbeitenden oder Gerätewechseln. Das sorgt für konsistente Installationen und minimiert manuelle Aufwände sowie Fehlerrisiken.

20 % kosten 80 % der Zeit

Software ohne standardisierte Installationspakete wird seltener ein Problem. Die benötigten Skripte zur Oberflächenautomatisierung lassen sich mit integrierten Tools gängiger Managementlösungen einfach und intuitiv erstellen. Selbst problematische Setups werden so zentral und automatisiert mit dem vom Softwarehersteller vorgesehenen Setup-Verfahren installiert – die Herstellergarantie bleibt erhalten.

Über eine Managementsoftware lassen sich Anwendungen aber nicht nur verteilen, sondern auch vom Client entfernen. Bei der Auswahl einer Lösung sollte darauf geachtet werden, dass dies auch für Programme möglich ist, die nicht über die Managementsoftware installiert wurden. Auf diese Weise lassen sich beispielsweise Applikationen, die Anwender unerlaubt auf ihren Rechner aufgebracht haben, effizient entfernen.



Oberflächenautomatisierung per Wizard mit baramundi Endpoint Automation

Die zentrale, automatisierte Installation von Anwendungen und Betriebssystemen hat zudem einen positiven Nebeneffekt für IT-Administratoren und Endanwender: Im Fall von Performance-Problemen und hartnäckigen Fehlern kann der Arbeitsplatz in weniger als zwei Stunden komplett neu aufgesetzt werden, anstatt aufwendig nach der Ursache zu suchen. Auf diese Weise steht bei minimalem Zeitaufwand schnellstmöglich wieder ein voll funktionsfähiges Gerät zur Verfügung. Auch die Migration einer großen Zahl von Arbeitsplätzen, zum Beispiel auf ein neues Betriebssystem oder eine neue Office-Version, lässt sich so automatisiert abwickeln – inklusive nahtloser Co-Management-Synchronisation mit Microsoft Intune.

2.2 Schwachstellen erkennen und Updates automatisieren

Einmal installiert und fertig? Leider nein. Laufend erscheinen Updates für Anwendungen und Betriebssysteme. Diese müssen schnellstmöglich auf allen Rechnern eingespielt werden. Dabei geht es nicht nur um neue Features, sondern vor allem um die Sicherheit: Patches schließen Sicherheitslücken, über die potenzielle Angreifer ins Unternehmensnetzwerk eindringen und großen Schaden anrichten könnten. Die Konsequenzen reichen vom Imageschaden über die Offenlegung von Firmeninterna bis zu juristischen Folgen, wenn Kundendaten gestohlen werden und Verstöße gegen Gesetze und Richtlinien wie die DSGVO oder NIS2 vorliegen.

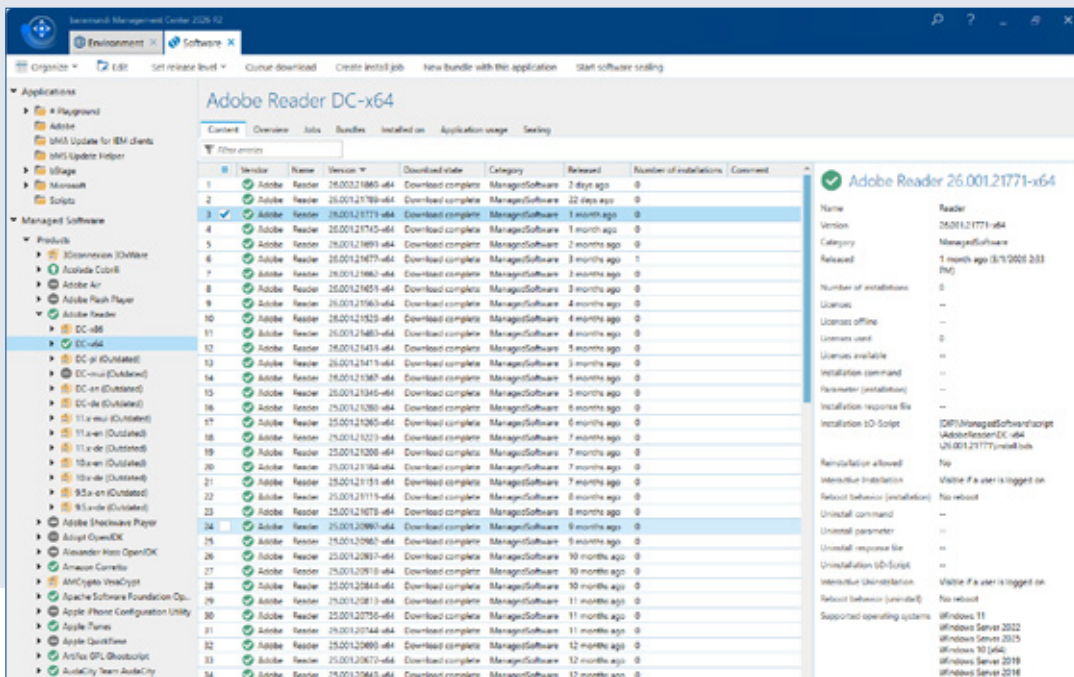
Einfallstor Nr. 1: Ungepatchte Schwachstellen

Firewall und Virens Scanner sind zwar unabdingbare Bestandteile eines wirksamen Sicherheitskonzepts, aber gegen Angriffe über nicht gepatchte Schwachstellen weitgehend wirkungslos. Bei einem sogenannten Reverse-Shell-Angriff wird der Rechner eines Mitarbeitenden unter Ausnutzung einer Schwachstelle dazu gebracht, eine verschlüsselte Verbindung mit dem Kontrollserver des Angreifers aufzubauen – die Firewall greift hier in der Regel nicht ein, da der Kontakt über Standardkanäle aus dem Unternehmen herausläuft. Es ist daher unabdingbar, Schwachstellen auf jedem Endgerät im Blick zu behalten und je nach Gefährdungsgrad schnellstmöglich zu schließen.

Doch jede Woche werden über 900 neue Schwachstellen erkannt und dokumentiert, wie Statistiken der National Vulnerability Database (NVD) von NIST zeigen. Hier kann die Managementsoftware den IT-Admin durch einen automatisierten, regelmäßigen Scan aller Clients und Server unterstützen. Als Ergebnis erhält er übersichtliche Listen, z. B. der gefährlichsten Schwachstellen im Unternehmensnetzwerk oder der Clients mit den meisten Sicherheitslücken. So kann er priorisieren und gezielt die Lücken schließen.

Schwachstellenscanner und Update Management

Verfügt die Lösung neben dem Schwachstellenscanner auch über ein Update Management, lassen sich erkannte Lücken auch gleich zentral und automatisiert schließen. Neben Microsoft-Patches sollte die Managementlösung grundsätzlich auch Updates für häufig genutzte Anwendungen wie Adobe Reader, Chrome oder Firefox zentral und automatisiert verteilen, die aufgrund ihrer großen Verbreitung bei Angreifern besonders beliebt sind. Aktuelle Softwarepakete für zahlreiche Anwendungen sind dabei auch als Managed Software vom UEM-Hersteller verfügbar. Diese können für die produktive Nutzung oder zum Test nach eigenen Richtlinien für freigegeben werden.



Verteilte Softwarepakete mit unterschiedlichen Freigabe Leveln

Für ein wirksames Schwachstellenmanagement genügt es aber nicht, von einer Lücke zu wissen und die Installation eines Patches anzustoßen. Essenziell ist auch das Wissen darüber, ob das sicherheitsrelevante Update tatsächlich auf allen Clients angekommen ist. Installationen können fehlschlagen, vom Benutzer blockiert werden oder ein Notebook kann im Außeneinsatz nicht erreichbar sein. Die eingesetzte Lösung muss daher eine Rückmeldung zum Installationsstatus sowie zu etwaigen aufgetretenen Fehlern geben, um sicherzustellen, dass tatsächlich alle Lücken geschlossen werden.

2.3 Hardware und Software inventarisieren, Lizenzen managen

Ein umfassender Überblick ist nicht nur wichtig, um Schwachstellen zu erkennen und Sicherheit zu garantieren. IT-Verantwortliche müssen auch den Einsatz von Hard- und Software berichten oder im Fall eines Lizenzaudits durch einen Softwarehersteller die korrekte Lizenzierung nachweisen können. Unter Kostengesichtspunkten ist es wichtig, ungenutzte Software zu erkennen, die auf Clients schlummert und teure Lizenzen bindet.

Compliance durch Automatisierung

Die automatisierte Inventur einer Managementlösung zeigt präzise und schnell, welche Hard- und Software im Unternehmensnetzwerk im Einsatz ist. So steht jederzeit eine aktuelle Datenbasis für fundierte, managementfähige Auswertungen bereit. Besonders bei Volumen- und Upgrade-Lizenzen geht der Überblick leicht verloren. Ein integriertes Lizenzmanagement schafft hier Klarheit und sichert Compliance.

Zusätzlich kann die tatsächliche Nutzung einer App erfasst werden, um unnötige Kosten zu vermeiden. Dazu wird der Start einer Anwendung auf den einzelnen Endgeräten protokolliert. Dies zeigt, auf welchen Endgeräten ein Programm in einem vorgegebenen Zeitraum ungenutzt bleibt und welche Lizenzen daher eingespart werden können, z. B. bei SaaS-Modellen. Wichtig: Die eingesetzte Lösung muss dabei die aktuellen europäischen Datenschutzvorgaben einhalten und darf keine Überwachung des individuellen Userverhaltens zulassen.

The screenshot displays the 'baramundi Management Center 2025 R2' interface. The left sidebar contains navigation menus for 'Settings', 'Assignments', 'Inventory', 'Microsoft Defender Antivirus', and 'Compliance'. The main area is titled 'Software' and shows a table of installed software. The table has columns for Name, Vendor, Version, Last found, Category, and License key. The right sidebar shows details for the selected '.Net Framework' entry.

Name	Vendor	Version	Last found	Category	License key
1 .Net framework	Microsoft	3.5.1-en	17 months ago	ManagedSoftware	
2 .Net framework	Microsoft	4.7.2-en	17 months ago	ManagedSoftware	
3 Chrome	Google	51.0.2704.136-x64	17 months ago	ManagedSoftware	
4 Firefox	Mozilla	10.0.2-de	17 months ago	ManagedSoftware	
5 iTunes	Apple	12.9.4.102-usb	17 months ago	ManagedSoftware	
6 Java JRE	Oracle	6.30-x64	17 months ago	ManagedSoftware	
7 Management Suite	baramundi	barsDP	17 months ago	ManagedSoftware	
8 Notepad++	Notepad++ Team	5.9.5-x64-de	17 months ago	ManagedSoftware	
9 SumatraPDF	Krzysztof Kowalczyk	1.8	17 months ago	ManagedSoftware	
10 Thunderbird	Mozilla	45.2.0-de	17 months ago	ManagedSoftware	
11 Updates	Windows	Root Certificates november2011	17 months ago	ManagedSoftware	
12 Visual C++ Redistributable	Microsoft	2010-SP1-x64	17 months ago	ManagedSoftware	
13 Visual C++ Redistributable	Microsoft	2010-SP1-x86	17 months ago	ManagedSoftware	
14 VLC	Videolan	2.2.4-x64	17 months ago	ManagedSoftware	

.Net Framework Details:

- Vendor: Microsoft
- Version: 4.7.2-en
- Category: ManagedSoftware
- License key: --
- Type: Application
- Comment: --
- Installed: 7 years ago (1/9/2019 6:00 PM)
- Last found: 17 months ago (4/1/2025 4:37 PM)
- Software detection rule: --

Managed Software Summary:

- Status: Up-to-date
- Name: .Net Framework
- Installed version: 4.7.2-en
- Latest version released: 4.7.2-en
- Latest version released for testing: 4.7.2-en
- Latest version available: 4.7.2-en

Auflistung der installierten Software

Vorteil für IT-Support

Auch der IT-Support profitiert von der automatisierten Inventur: Integrierte Helpdesk-Lösungen erlauben es den Supportmitarbeitern bei Anfragen schnell die Hard- und Softwareausstattung des betreffenden Arbeitsplatzes zu erfassen. Korrekte Daten des betreffenden Endgeräts sind essenziell, um das Anliegen des Nutzers schnell und kompetent bearbeiten zu können.

2.4 Intelligent automatisieren: Zeitsteuerung und Self-Service

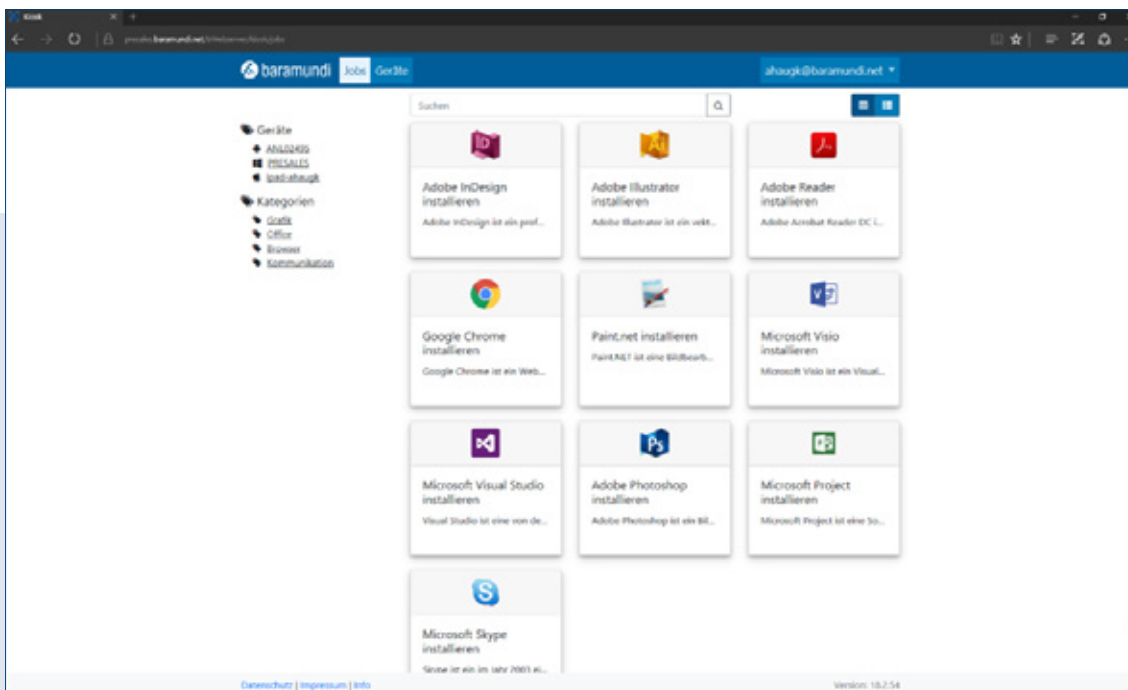
In vielen Unternehmen sind Wartungszeitfenster definiert, in denen administrative Aufgaben auf bestimmten Endgeräten ausgeführt werden dürfen. Moderne Managementsoftware stellt dafür zeitgesteuerte Aufgaben bereit. So lassen sich Patch-Installationen gezielt innerhalb eines festgelegten Zeitfensters auf einzelnen oder mehreren Endgeräten ausführen.

Störungsfreies Arbeiten

Ereignisgesteuerte Aufgaben entlasten den IT-Admin bei der Reaktion auf definierte Ereignisse. Wird beispielsweise während einer Inventarisierung unerwünschte Software auf einem Client entdeckt, kann diese automatisch entfernt werden. Der Admin muss nicht mehr bei jedem Fund manuell eingreifen, sondern erhält nur noch einen Report über die automatisch durchgeführte Deinstallation.

Self Service

Komfortabel für IT-Admins und User ist die Möglichkeit, vorbereitete Installationsabläufe in einem Self-Service-Kiosk bzw. Unternehmens-App-Store bereitzustellen. So lassen sich Standardanfragen – etwa die Installation eines Browsers oder zusätzlicher Tools – schnell und unkompliziert erledigen, genau dann, wenn Nutzende sie benötigen. Gleichzeitig sinkt das Supportaufkommen, da diese Installationen vollständig automatisiert ablaufen. Der Admin behält über Dashboards und Berichte jederzeit den Überblick über alle Self-Service-Installationen.



Self-Service-Kiosk für die Anwenderinnen und Anwender

Leistungsfähige Managementsoftware bietet darüber hinaus die Möglichkeit, Anwender in Installationsabläufe mit einzubeziehen, ohne als Administrator die Kontrolle aus der Hand zu geben. Zum Beispiel kann dem Nutzer das Recht eingeräumt werden, eine Patch Installation, die einen Neustart erfordert, innerhalb eines vorgegebenen Zeitfensters zu verschieben. So werden die Kollegen nicht in ihrem Arbeitsfluss gestört und die Installation läuft während einer Kaffeepause ab. Gleichzeitig ist sichergestellt, dass die Verteilung eines kritischen Patches nicht zu weit hinausgeschoben werden kann.

2.5 Integration in die bestehende Infrastruktur

Die Managementsoftware sollte nahtlos in die bestehende Infrastruktur eingebunden und nicht als isolierte Insellösung gesehen werden. Moderne APIs ermöglichen eine nahtlose Integration über moderne Schnittstellen. Nur so lassen sich auch weitere organisatorische Prozesse automatisieren. So ist es etwa möglich, dass nach der Erfassung eines neuen Endgeräts im ERP-System dieses auch automatisch in der Managementlösung angelegt wird – inklusive Inventarnummer, Kostenstelle und weiterer Daten. Parallel erhält es sofort die passende Software und nötigen Konfigurationen.

Ebenso ist eine Integration in das Ticketsystem möglich. Support-Teams erhalten Echtzeitdaten zu genutzter Hard- und Software und lösen bei Bedarf Neuinstallationen per Knopfdruck aus – effizient und NIS2-konform.

3 Schnittstellen und Co-Management

In diesem Kapitel erfahren Sie, wie offene Schnittstellen, Co-Management und DEX-Integrationen IT-Systeme vernetzen, Prozesse automatisieren und so Effizienz, Stabilität und NIS2-konforme Sicherheit gewährleisten.

Aktuelle Endpoint-Management-Lösungen setzen auf standardisierte, offene Schnittstellen wie REST-APIs, um Daten nahtlos zwischen Systemen auszutauschen. Inventardaten, Gerätestatus, Schwachstelleninformationen oder Compliance-Details fließen bidirektional in ITSM-Ticketsysteme wie ServiceNow oder Jira – und umgekehrt. So entfällt die manuelle Dateneingabe: Tickets werden automatisch mit Kontext zu Hardware, installierten Anwendungen und laufenden Prozessen angereichert. IT-Teams können somit schneller und präziser arbeiten, was die Erstlösungsrate erhöht und Eskalationen reduziert.

Co-Management für hybride Umgebungen

Co Management ermöglicht einen durchgängig hybriden Verwaltungsansatz, indem es lokale Management-Systeme nahtlos mit Cloud Diensten wie Microsoft Intune verbindet. Endpoint Daten werden dabei in regelmäßigen Intervallen synchronisiert, sodass Unternehmen von einer stabilen, skalierbaren Datenbasis profitieren. So lassen sich automatisierte OS-Deployments, Patch Verteilungen und Konfigurationsänderungen zuverlässig orchestrieren, ohne dass Admins manuell eingreifen müssen. Neue Geräte werden parallel in beiden Systemen eingebunden, während zentrale Daten wie Lizenzen oder Inventarnummern konsistent bleiben und Medienbrüche vermieden werden. Das schafft Einheitlichkeit über hybride Arbeitsumgebungen hinweg, reduziert Administrationsaufwand und verhindert doppelte Arbeit.

DEX-Integration für proaktives IT-Management

Digital Employee Experience (DEX)-Plattformen ergänzen UEM und ITSM um Echtzeitmetriken zur Nutzererfahrung – etwa Boot-Zeiten, App-Abstürze oder Netzwerk-Latenz. Über APIs, verknüpft mit Endpoint-Daten, lassen sich Anomalien frühzeitig erkennen. Eine erhöhte Crash-Rate kann direkt einen Patch oder Neustart anstoßen, noch bevor ein Support-Ticket entsteht. Solche proaktiven Workflows verringern das Ticket-Volumen und verbessern die Mitarbeiterzufriedenheit – was insbesondere unter den Anforderungen von NIS2 an reaktionsfähige IT-Strukturen an Bedeutung gewinnt.

Nahtlose Automatisierung über Systeme hinweg

Auch ERP-Systeme liefern Gerätedaten wie Inventarnummern oder Kostenstellen, die automatisch in UEM- und ITSM-Systeme übernommen werden – neue Assets sind somit sofort managebar. Schwachstellen-Scans aus dem UEM können Priorisierungsprozesse im ITSM anstoßen, während DEX-Analysen Entscheidungsgrundlagen liefern. Diese vernetzte Automatisierung reduziert manuelle Aufwände, unterstützt Compliance und schafft Freiräume für strategische IT-Aufgaben. Die baramundi Management Suite nutzt diese Prinzipien optimal durch bConnect, eine leistungsstarke REST-API für bidirektionale Integrationen mit ERP-, ITSM- und DEX-Lösungen wie perform2work. Ergänzt um robustes Co-Management mit Microsoft Intune sorgt sie für NIS2-konforme Prozesse, minimale Störungen und maximale Stabilität.

4 Mobilgeräte managen

In diesem Kapitel erfahren Sie, wie modernes Mobile Device Management (MDM) flexible BYOD-Konzepte sicher ermöglicht und warum nur eine integrierte UEM-Lösung effiziente Verwaltung, Automatisierung und Schutz aller Gerätetypen gewährleistet.

Bring-Your-Own-Device (BYOD) ist in Unternehmen zum Standard geworden: Mitarbeiter möchten private Notebooks, Tablets oder Smartphones für den Zugriff auf Firmendaten nutzen. Das bringt Vorteile wie Flexibilität und Produktivität, doch IT-Verantwortliche müssen sich der Risiken bewusst sein. Effektiver Schutz, Inventarisierung und Automatisierung sind Voraussetzung – idealerweise integriert in eine moderne UEM-Lösung.

Umfassendes Management aller Gerätetypen

Gute Lösungen managen alle Gerätearten – von mobilen Geräten (iOS, iPadOS, Android) bis zu Desktops (Windows, MacOS, Linux). Ohne einheitliche Verwaltung erfordern z. B. Exchange-Konfigurationen (Name, E-Mail, Server, Verschlüsselung) bei iOS und Android unterschiedliche Eingaben. Plattformübergreifende Profile und zentrale Konsolen automatisieren diesen Prozess – effizient für jeden Gerätetyp.

The screenshot shows an iOS 'Account' setup screen. At the top, there are three buttons: 'Cancel', 'Account', and 'Done'. Below these are several input fields: 'Email' with the value 'apple.fan@bartoso.de', 'Server' with 'mail.bartoso.de', 'Domain' with 'bartoso.de', 'Username' with 'Apple.Fan', and 'Password' with 'Required'. There is also a 'Description' field with 'Apple.Fan' and an 'Advanced Settings' link with a right arrow. At the bottom, a note reads: 'These settings are installed by the profile "apple exchange baustein"'.

Exchange-Konfiguration auf verschiedenen Mobilplattformen

Die Einbindung eines Smartphones oder Tablets in die Unternehmensverwaltung erfolgt heute schnell und automatisiert – etwa über Apple Automated Device Enrollment (ADE) oder per QR-Code. Nach dem Enrollment können IT-Teams sämtliche Konfigurationen, wie z. B. E-Mail-Einrichtung oder Sicherheitsrichtlinien, zentral auf einer einheitlichen, plattformübergreifenden Oberfläche vornehmen und „Over-the-Air“ auf die Geräte ausrollen.



Plattformübergreifende Profilbausteine zur Konfiguration mobiler Endgeräte

Fehlerarme Verwaltung

Der große Vorteil liegt in der einfachen, fehlerarmen Verwaltung ohne manuelles Eingreifen. Workflows lassen sich vorbereiten, automatisieren und für viele Geräte gleichzeitig nutzen – egal ob iOS oder Android. Das spart wertvolle Zeit und erhöht zugleich die Sicherheit.

Mobile Devices gehen schneller verloren oder werden häufiger manipuliert als klassische PCs, umso wichtiger sind automatisierte Sicherheitsmaßnahmen. Dazu zählen sichere Passwörter, automatisches Sperren, Remote-Löschung und kontinuierliches Monitoring.

Moderne Managementlösungen prüfen automatisch die Geräte-Compliance, erkennen Jailbreaks oder Verstöße und leiten bei Bedarf automatisch Gegenmaßnahmen ein – von einer Nutzerbenachrichtigung bis hin zur Sperrung oder Löschung aus der Ferne. Ebenso entscheidend ist die automatisierte Firmware-Aktualisierung, um eventuelle Sicherheitslücken zeitnah zu schließen.

Neu hinzugekommene Co Management Funktionen erweitern diesen Schutz um eine enge Integration mit Microsoft Umgebungen. Dabei wird der von der baramundi Management Suite ermittelte Compliance Status mobiler Endgeräte an Microsoft Intune und Microsoft Entra ID übermittelt. Auf dieser Basis können Unternehmen Conditional Access Richtlinien definieren und dadurch den Zugriff auf Microsoft 365 oder andere Unternehmensressourcen abhängig vom Sicherheitszustand des jeweiligen Geräts steuern. Geräte, die nicht compliant sind, werden automatisch vom Zugriff ausgeschlossen – ohne manuelles Eingreifen.

Dieser automatisierte Abgleich schafft ein durchgängiges Sicherheitsmodell: baramundi übernimmt das Gerätemanagement, während Intune und Entra ID den Zugriff auf sensible Daten absichern. Für IT Administratoren entsteht so eine einheitliche Sicht auf Compliance, Zugriff und Gerätestatus – nahtlos eingebettet in ihre bestehende Infrastruktur.

Kontrolle über Apps

Zur Kontrolle installierter Apps unterstützen aktuelle Lösungen für Unified Endpoint Management sogenannte Block- und Allow-Listen. Somit lässt sich unerwünschte Software entweder blockieren oder der Zugriff ausschließlich auf freigegebene Unternehmens-Apps beschränken.

Als aktives Mitglied der AppConfig Community nutzt baramundi etablierte Standards und native Plattformfunktionen, um die Verteilung, Konfiguration und Absicherung von mobilen Anwendungen zu automatisieren. Die baramundi Management Suite vereint Mobile Device-, Application- und Content Management (MDM, MAM, MCM) in einer zentralen Plattform. Dadurch können IT-Admins Smartphones, Tablets und PCs über ein einziges Interface effizient verwalten, Richtlinien durchsetzen und Sicherheitsupdates automatisiert ausrollen. Diese ganzheitliche Integration reduziert Verwaltungsaufwand, schließt Sicherheitslücken schneller und sorgt dafür, dass Unternehmen auch zukünftige Gerätetypen nahtlos in ihr Endpoint Management einbinden können.

5 Datensicherheit und Datenschutz

In diesem Kapitel erfahren Sie, wie automatisierte Backups, NIS2-konforme Datensicherheit und Security by Design den Datenschutz in UEM-Lösungen gewährleisten und Compliance-Risiken minimieren.

Automatisierte Backups in UEM

IT-Administration trägt die Verantwortung für Datensicherheit, wobei UEM-Lösungen automatisierte Backups mit regelmäßigen Integritätsprüfungen, Redundanz und Wiederherstellung unterstützen – gefordert durch NIS2 für Geschäftskontinuität inklusive Backup-Management. Diese umfassen regelmäßige Sicherungen kritischer Laufwerke und Systeme sowie die sichere Ablage an Offsite-Standorten. So wird im Ernstfall eine schnelle Wiederherstellung und die Aufrechterhaltung des Geschäftsbetriebs gewährleistet.

Datenschutz und Compliance

NIS2 und DSGVO schreiben Risikoanalysen, Incident Management, Verschlüsselung bei Speicherung bzw. Übertragung und Multi-Faktor-Authentifizierung vor. UEM-Lösungen erfassen potenziell Userdaten, daher sind differenziertes Rechtemanagement (IAM, Zugriffsbeschränkungen), Pseudonymisierung und aggregierte Speicherung essenziell, um Profiling zu vermeiden. Hersteller müssen diese Anforderungen („Security by Design“) von Grund auf berücksichtigen und implementieren: zentrale Sicherheitsrichtlinien, Patch-Management, Asset-Inventarisierung und Lieferkettensicherheit.

baramundi UEM-Vorteile für NIS2

Die baramundi Management Suite vereinheitlicht Endpoint-Sicherheit für alle Gerätetypen, inklusive OT und Mobile. Sie unterstützt Schwachstellen-Scans, automatisierte Resets nach Angriffen sowie Audit-Reporting. So gewährleisten Unternehmen ihre Geschäftskontinuität NIS2-Konformität.

Über die baramundi software GmbH

Die baramundi software GmbH sorgt als Spezialist für Unified Endpoint Management (baramundi Management Suite) und Proactive Endpoint Operations (baramundi Proactive Hub) dafür, dass Unternehmen und Organisationen effizient, sicher und plattformübergreifend Arbeitsumgebungen und digitale Arbeitsplätze managen – On-Prem und in der Cloud. Der Hauptsitz der baramundi software GmbH befindet sich in Augsburg. Die Produkte und Services des im Jahr 2000 gegründeten Unternehmens sind komplett Made in EU. Beim Vertrieb, der Beratung und Betreuung von Kunden arbeitet baramundi weltweit erfolgreich mit Partnerunternehmen zusammen.

www.baramundi.com



Sie möchten mehr über die baramundi Management Suite erfahren?

Melden Sie sich zum Live-Webinar an! Erleben Sie im kostenfreien Webinar, wie Sie die baramundi Management Suite Ihre Endpoints, Server und Mobilgeräte automatisiert verwaltet und absichert.

<https://www.baramundi.com/de-de/it-training/webinare/>

Kontaktieren Sie uns.

Wir freuen uns auf Sie!



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

