

The image shows a person's hands typing on a laptop keyboard. Overlaid on the image are several digital security-themed graphics: a glowing blue shield with a keyhole in the center, surrounded by a network of nodes and lines; a glowing blue circular interface with concentric rings and a central light; and a network diagram with nodes and lines in the upper left. The background is dark blue with faint binary code (0s and 1s) visible.

WHITE PAPER

Automated Vulnerability Management

Identify, prioritize, and fix security vulnerabilities

Contents

1 Why Automate? Because Attackers Do	03
2 From Vulnerability to Cyberattack	04
2.1 Vulnerabilities, exploits, and more	04
2.2 The life cycle of a vulnerability	05
2.3 Attack vectors: How attacks bypass your firewall	05
3 Identifying and Closing Vulnerabilities	07
3.1 Manual vulnerability management doesn't scale	07
3.2 Automation accelerates detection and remediation	07
3.3 Automating update and patch management	08
4 Risk-Based Exception Management	10

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



1 Why Automate? Because Attackers Do.

When cyberattacks and data breaches make headlines, many people picture teams of skilled hackers using sophisticated cyberweapons against high-value targets. While that happens in some cases, many more attacks come from opportunistic criminals who use readily available hacking tools and AI-driven automation to scan for open vulnerabilities, deliver exploits, perform credential stuffing, and enable lateral movement. The result is a steadily rising number of damaging attacks on organizations ranging from small businesses to multinational corporations.

Traditional security mechanisms are reaching their limits

Firewalls and endpoint protection software are part of any cyberdefense strategy, but they no longer provide adequate protection against today's hacking tools and tactics. That's true not only when company systems are misconfigured or lack strong password policies and authentication methods, but also when busy IT administrators can't detect and close security gaps faster than cyberattackers can exploit them. That imposes a heavy burden on IT teams and company executives to protect data and infrastructure, especially when the consequences of a security incident include financial and reputational damage, as well as civil or criminal liability.

Automation is the key to security

As the number and types of vulnerabilities grow, IT teams need automated vulnerability management solutions integrated with a modern endpoint management system. This whitepaper explains how to implement automated vulnerability management, reduce exposure windows from weeks to hours, and manage security risks effectively as cyber threats evolve.



2 From Vulnerability to Cyberattack

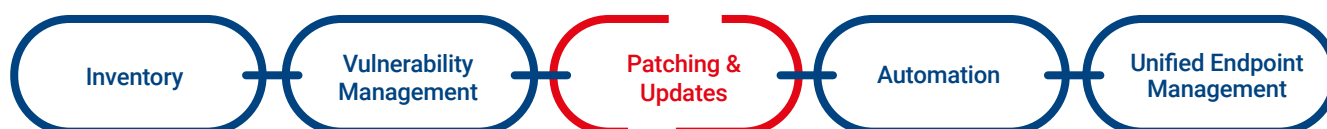
This section describes how vulnerabilities lead to cyberattacks and why rapid patching, modern security measures, and employee training can provide effective protection.

2.1 Vulnerabilities, exploits, and more

An unpatched vulnerability is an open attack surface. Attackers don't need to target your organization specifically because they typically use automated scanners to probe millions of internet-facing systems to find unpatched systems – sometimes within hours of public disclosure of a vulnerability.

The situation becomes critical when an exploit is available, i.e., code that takes advantage of a vulnerability to achieve unauthorized access, privilege escalation, or code execution. Exploits range from standalone proof-of-concept (PoC) code to weaponized modules in open-source penetration testing frameworks like Metasploit. Other examples include malware payloads that steal or encrypt data, integrate devices into botnets used for crypto-mining, credential stuffing, proxy services for further attacks, and a persistence infrastructure for ransomware groups.

The expression “a chain is only as strong as its weakest link” applies; just one incorrect OS setting or unpatched software vulnerability can jeopardize the entire infrastructure.



Endpoint security chain

2.2 The life cycle of a vulnerability

Modern software complexity makes vulnerabilities unavoidable, even after rigorous development and testing. Risk is determined by how quickly they're found and patched, and by how quickly IT teams can deploy patches.

A zero-day vulnerability is unknown to the vendor and therefore has no patch. Attackers may exploit zero-day vulnerabilities for weeks or months before they're discovered. Known vulnerabilities are identified by vendors, security researchers, and independent programmers and have patches available. They are assigned a Common Vulnerabilities and Exposures (CVE) number and reported through online forums and public sources such as the National Vulnerability Database (NVD). CVEs typically include a severity score based on exploitability and potential impact. Once a vulnerability is reported:

- Attackers compare code in patched and unpatched software to determine what was fixed, then develop an exploit to sell or share on underground forums. For high-severity CVEs in widely deployed software, exploits are often available within 24 to 72 hours of a patch release.
- Hackers then use automated scanning tools to probe the internet for unpatched systems to exploit.
- IT teams must identify affected systems, test and approve patches, and deploy them across the environment — all before attackers can find and exploit the exposure.

For vulnerabilities with public PoC code or Metasploit modules, mass exploitation can begin within hours of disclosure, sometimes before many organizations are even aware of the CVE. For example, exploitation of Log4Shell began within hours of public disclosure. The narrowing window between patch availability and patch deployment is when most breaches occur. Vulnerability management is designed to close that window quickly.

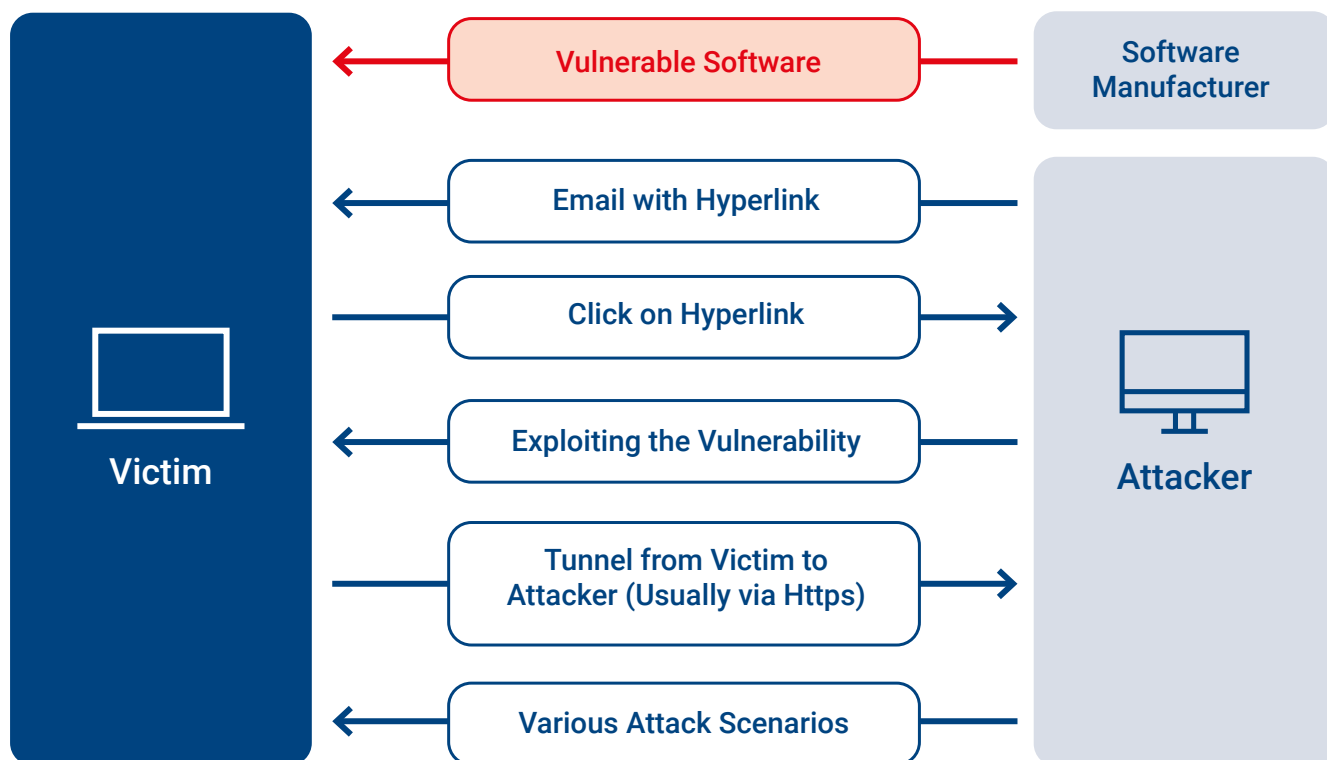


The window of vulnerability between patch availability and patch deployment

2.3 Attack vectors: How attacks bypass your firewall

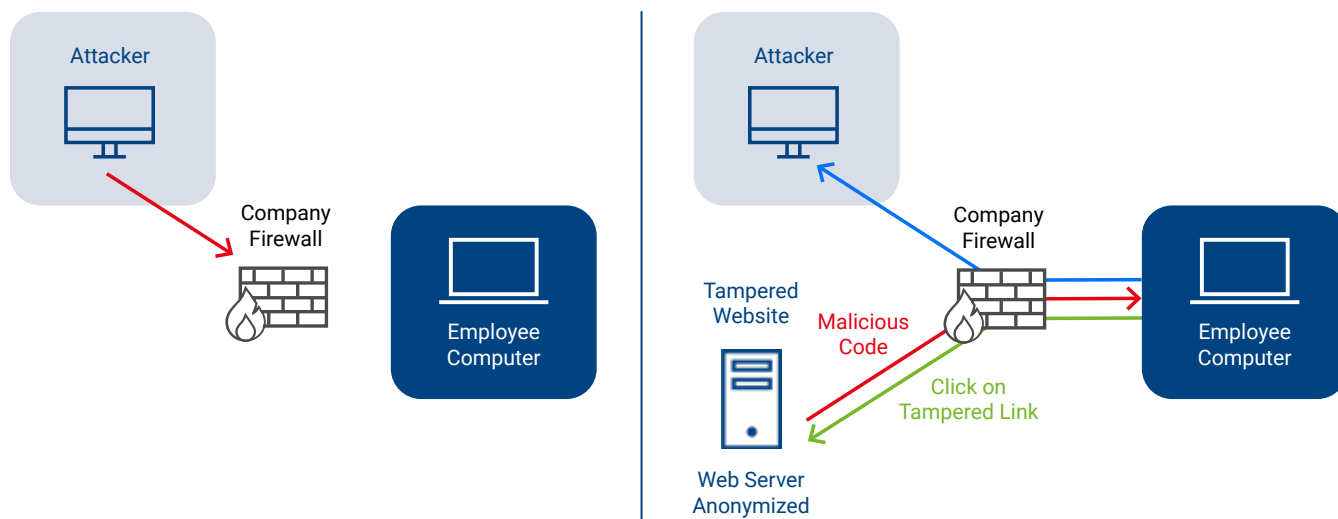
Cybercriminals no longer attack firewalls directly but instead use more subtle tactics, including compromised VPN gateways, stolen credentials, and unpatched software. Attackers are also using AI tools and automation to shorten the window between CVE publication and a weaponized exploit. LLM-assisted tools make it easy for hackers to write exploit code, while AI-driven scanners accelerate the discovery of attack vectors.

Other common entry vectors include compromised websites and malicious files — DOCX, PDF, ISO, LNK, and OneNote files have all been weaponized. Phishing emails and smishing SMS messages use publicly available social media data and personalized LLM-generated content to trick users into clicking malicious links. The exploit runs silently in the background; the user sees only a "corrupted file" error message, or nothing appears to happen. After an initial successful intrusion, attackers often use **living-off-the-land techniques** (e.g., PowerShell and WMI) to move laterally across the IT infrastructure while evading detection.



A successful phishing e-mail attack gives hackers multiple attack vectors

If the target system is unpatched, the malware communicates with the attacker via HTTPS or DNS tunneling, bypassing traditional firewalls. Attackers also use cloud services as covert channels, a technique known as Living Off Trusted Sites (LOTS). Traditional firewall rules and some next-generation firewalls cannot block these channels without additional controls.



Establishing a connection to the attacker

A capable firewall, endpoint security software, and identity and access management (IAM) that enforces least-privilege and role-based access controls (RBAC), together with prompt, consistent patch management and continuous user awareness training, remain essential security practices.

3 Identifying and Closing Vulnerabilities

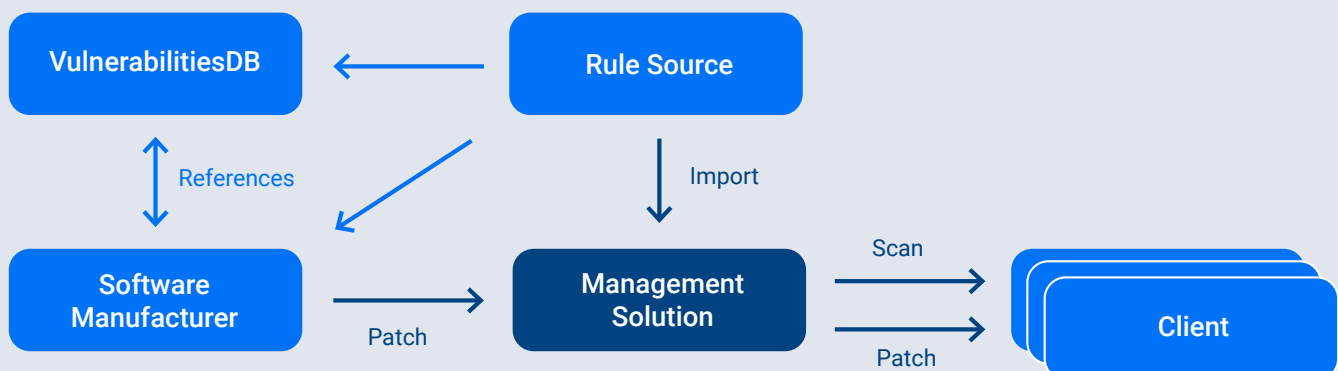
The section explains why manual vulnerability management is impractical in modern IT environments and how automated solutions can efficiently detect and close security gaps.

3.1 Manual vulnerability management doesn't scale

For IT administrators, manually checking all PCs, laptops, and servers for vulnerabilities is virtually impossible. They would need to constantly monitor the NVD, vendor security advisories, CISA KEV updates, and threat intelligence feeds for new vulnerabilities; assess risks and exposures; package and test patches; prioritize distribution; and verify installation on each affected system. This approach does not scale in medium and large networks and creates additional challenges for mobile, remote, and home office employees. At the same time, IT directors and CISOs must ensure compliance with frameworks that require or audit patch management, such as NIST SP 800-40, the CISA KEV catalog, PCI DSS Requirement 6, or the HIPAA Security Rule. IT teams must also be prepared to respond rapidly if an unpatched system is compromised.

3.2 Automation accelerates detection and remediation

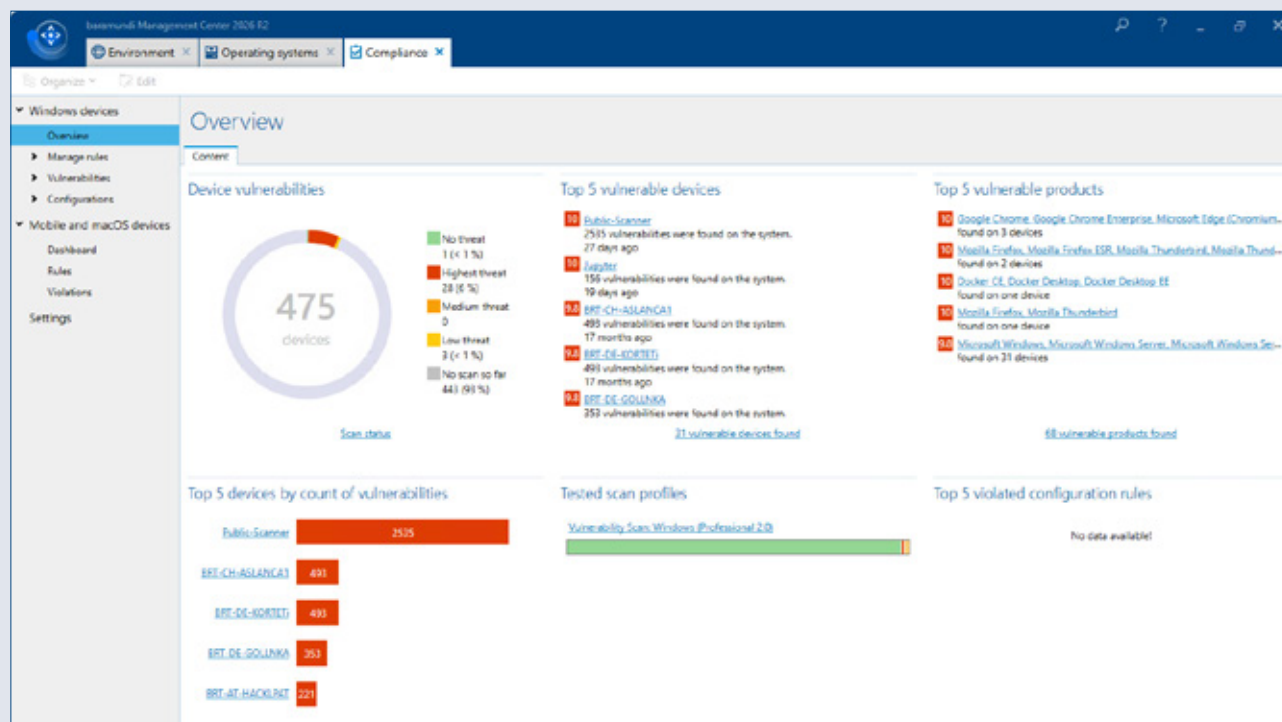
Solutions like the baramundi Management Suite automate end-to-end vulnerability management through continuous scanning and automated deployment of tested patches to affected systems.



Centralized, automated vulnerability management with a UEM solution

The Management Suite's automated Inventory solution detects and flags unauthorized software installations and other forms of shadow IT. The baramundi Vulnerability Scanner continuously checks all on-premises, branch office, mobile and home office clients and servers for missed or incorrect system settings and known OS and application vulnerabilities. Any detected vulnerabilities are flagged to IT administrators for appropriate remediation from a central location.

To detect vulnerabilities, the baramundi Vulnerability Scanner cross-references installed software and system configurations against continuously updated feeds from authoritative sources, including the National Vulnerability Database (NVD), CISA's Known Exploited Vulnerabilities (KEV) catalog, and vendor security advisories. Results are displayed in a centralized dashboard that gives IT administrators an at-a-glance view of the overall security posture, vulnerability severity, and recommended remediation steps. Administrators can view the data by device, by affected product, or by vulnerability count and severity — making it straightforward to prioritize remediation based on actual exposure.

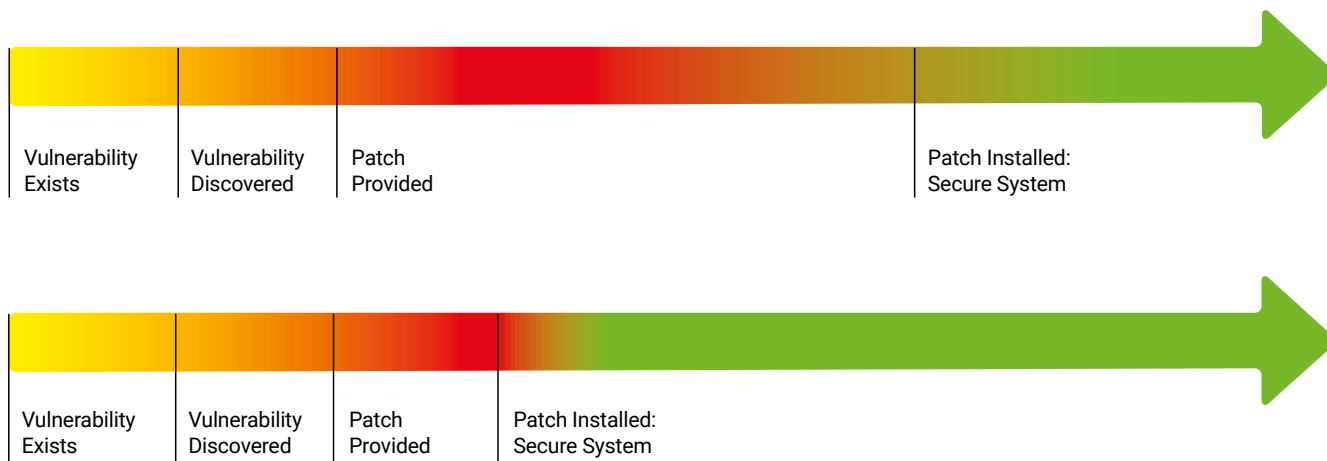


baramundi Management Suite: Vulnerability Scanner dashboard showing results

3.3 Automating update and patch management

Endpoint management systems can also automate the distribution of OS updates and application patches. The Update and Patch Management solution in the baramundi Management Suite provides updates for Microsoft products, which IT administrators can automatically distribute to target systems based on predefined rules. These rules give IT teams precise control over how, where, and when updates are distributed. Installations can run in the background; reboots can be grouped and scheduled during maintenance windows; installations can be delayed to a user-specified time; or installations can be suppressed and deferred for endpoints in production.

For third-party software, baramundi Managed Software delivers patches as deployment-ready packages. This significantly reduces the time and effort required to search for updates, create packages, configure parameters, and verify installation. The baramundi Management Suite automates distribution to all target endpoints, including remote and mobile PCs. It also supports offline patching by securely deploying updates and patches to devices even when they're disconnected from the internet or cloud services.



Automation accelerates patch deployment and reduces Mean Time to Remediation

By centralizing and automating update and patch distribution, the baramundi Management Suite gives IT teams real-time visibility into installation status, including identification of installation errors or unexpected delays. This provides clear, continuous visibility and enables IT administrators to take immediate action to ensure compliance.

4 Risk-Based Exception Management

This section describes risk-based management of update exceptions for legacy and specialized software while ensuring compliance.

While automated deployment of updates and patches for standardized operating systems and applications is relatively straightforward, vulnerability management in complex IT environments can be challenging. Installed software often includes a wide range of specialized, legacy, and in-house software, operating systems, and components. Managing the risk of vulnerabilities in these systems requires a different approach.

For example, a company may continue using legacy software with a known dependency vulnerability, such as an in-house application that bundles an older version of OpenSSL. However, the same vulnerability also exists in another installed application. That's when IT teams will define an exception for the legacy software during vulnerability scanning, while still scanning for and remediating the vulnerability in applications with available patches.

Vulnerability management tools in a modern endpoint management solution not only provide visibility into potential security gaps across the environment but also ensure a clear, transparent, risk-based process for documenting exceptions. This is important for compliance with regulatory frameworks such as PCI DSS, HIPAA, and SOC 2, which require documented justification for unpatched systems.

Add Exclusion

The results of the vulnerability rule still will be stored but due to this exclusion they will be ignored in the evaluation of the selected scope.

CVE ID: CVE-2010-5298

Selected device: --

Current group: --

Ignore scope: Global

Type: Conditional

Please enter a reason:
(User name and time will be recorded automatically)

Exclusion for VMware

Conditions for the exclusion:

- ☐ C:\Program Files (x86)\LibreOffice 4\program\ssleay32.c
- ☒ C:\Program Files (x86)\VMware\VMware Player\ssleay32.c
- ☒ C:\Program Files (x86)\VMware\VMware Player\x64\ssleay32.c
- ☐ C:\Program Files\WindowsApps\king.com.CandyCrushS...
- ☒ C:\Program Files (x86)\VMware\VMware Player\OVFTool.exe

Select all Deselect all

Save Cancel

Defining exceptions for vulnerability scanning

About baramundi software GmbH

baramundi software's Unified Endpoint Management (baramundi Management Suite) and Proactive Endpoint Operations (baramundi Proactive Hub) solutions enable organizations to manage IT environments and digital workplaces efficiently, securely, and across platforms – on-premises and in the cloud. baramundi software GmbH is headquartered in Augsburg, Germany. Founded in 2000, the company develops its products and services in the EU and supports them through offices in the U.S., Italy, and Poland. baramundi also collaborates with sales, consulting, and customer support partners worldwide.

More information about baramundi: www.baramundi.com



Register for our live webinar to learn more about the baramundi Management Suite!

Discover how the baramundi Management Suite automatically manages and secures your endpoints, servers, and mobile devices, then try it free for 30 days in your own network.

<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