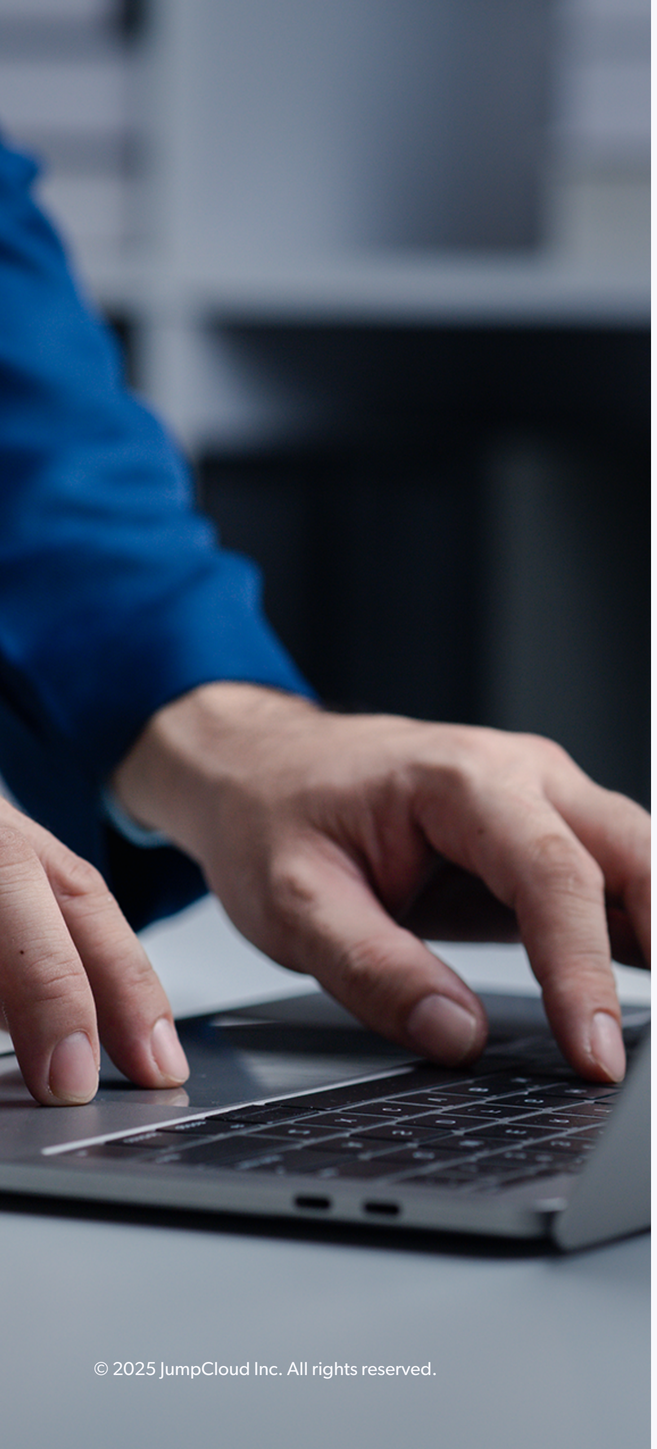
jumpcloud™

eBook

How to Choose a Device Management Solution

The 4 Critical Elements of Modern Device Management



Welcome to Permanently Mobile Work

Whether you're working in the office, hybrid, or remote, there's no question that your device fleet is mobile. Employees are accustomed to using a diverse set of devices to get their work done (whether they're sanctioned by IT or not). This has made bring your own device (BYOD) a business norm. Even choose-your-own-device (CYOD) approaches are becoming popular to help companies stand out to potential new hires.

This permanently mobile workplace presents a challenge: you need to be able to manage all of those devices. This may have been straightforward in a traditional office setting. But in modern workplaces, this proves much more difficult. That's because many of the device management solutions on the market were developed for traditional, non-mobile offices. They can't handle today's mobile and dynamic device fleets.

This puts you in a difficult position: you're tasked with managing a wide variety of different device types, operating systems, and ownership models, but your outdated device management solution is holding you back.

You need a device management solution built for today's mobile world — not yesterday's cubicle-clad offices.

So, what should that solution look like?

This eBook will cover the key elements of a modern device management solution to help you choose the right solution for your environment.

4 Necessities in a Modern Device Management Solution

These are critical considerations when evaluating device management solutions. Ask these questions to make sure the solution is modern and flexible to keep up with your needs.

1. **IAM**: Does it include an identity and access management (IAM) solution, or can it integrate with yours?
2. **Device Types**: Can it manage multiple OSes, including Windows, Mac, and Linux? Can it handle desktop and mobile devices?
3. **Device-Ownership Permutations**: Is it flexible enough to manage all the device-ownership permutations you may come across?
4. **Unified Platform**: Can it do everything in one platform, or does it offer a fragmented experience?

1. It must integrate with your IAM program

To effectively manage devices, you need to treat devices as a function of identity. To do this, your device management program must be integrated with your IAM program. This allows you to take an identity-centric device management approach, which is more robust, flexible, and secure than the traditional (and outdated) device-centric approach.

With identity-centric device management, devices are treated as as an extension of user identities, rather than separate things that users use. This creates a holistic view of devices that accounts for not just the machine, but also the person using it. That includes their role, their permission levels, and the variety of resources they need to accomplish their work.

This information provides critical context that device-centric solutions lack. This context enhances **security**, **compliance**, and the **user experience**.

2. It must manage *all* devices

When we say all, we mean all. You should be able to manage all devices that access your organization's network, data, or resources. That includes:

- All operating systems, including mobile devices and open-source alternatives.
- Devices in any location.
- Employee-owned (BYOD) and company-issued devices (this must come with the ability to address user privacy).

While this sounds simple, it's actually one of the stickiest challenges with traditional device management solutions. Solutions were typically built with traditional devices and one OS in mind. If they do accommodate others, it's with complex integrations and add-ons. In all likelihood, you pay for and manage multiple, disparate solutions and still have gaps in coverage; and Linux devices still tend to miss the boat, even with these after-the-fact updates.

Capabilities to look for

Device lifecycle management

Automate device onboarding, management, and offboarding from anywhere. Solutions like zero-touch enrollment, for example, allows you to automatically provision and configure new devices without ever touching them.

Broad policy application

Apply policies across operating systems and device types. This helps ensure compliance avoid policy sprawl. Policies should broadly apply to avoid policy sprawl.

Security-first

Make sure your device management solution offers the security capabilities you need. For example, you should be able to remotely lock and wipe devices, support different authentication methods, and automate patch management.

Custom configuration

Administer laptops and workstations to your organization's specifications.

A Note on BYOD

The level of control you have over employee-owned devices will vary by factors like device use case, device type, and company policies. But as a rule of thumb, you should be able to view, verify, and (to some extent) control access to every device on your network or accessing company resources, including all BYOD devices.

BYOD Deep-Dive

To go deeper into optimizing your BYOD programs, check out the whitepaper, JumpCloud BYOD Management.

In addition, BYOD scenarios naturally call user privacy into question. Your device management solution should account for this with a means for addressing user privacy. This could include:

- Limiting IT's visibility and control to pertinent applications and use cases.
- Allowing users a choice to opt into the BYOD program.
- Ensuring users understand the scope of the organization's presence on BYOD devices, as well as their shared responsibility in keeping the device — and organization — secure.

Why Support BYOD?

Employees will use personal devices whether you sanction them or not. Supporting BYOD allows you to:

- ✓ Reduce shadow IT
- ✓ Improve employee satisfaction
- ✓ Raise productivity
- ✓ Improve visibility and control over all devices on the network

3. It needs to handle all user-device permutations

A wide variety of user-device permutations are becoming common in the workplace (BYOD is one example). The examples on this page only scratch the surface of possible scenarios — and new ones are likely to crop up as technology and its relationship with users continues to evolve.

The following are critical in an identity-centric device management solution:

- It assumes multiple devices per individual.
- It assumes multiple levels of ownership per individual.
- It can handle devices with multiple users.
- It can handle special use cases, like one device assigned to multiple users or “user-less” IoT.

These properties allow your device management program to revolve around identities first. This results in a flexible, powerful, and secure solution.

Diverse and complex relationships between users and devices are now the norm

A user logging into their laptop with an authenticator app on their personal phone.

Retail workers sharing a point-of-sale device.

Several nurses logging into the same workstation in a patient’s room.

4. It should do it all in one platform

Managing devices, identity, access, and security is great — but if you can't do it all with one tool, it tends to fall apart. By contrast, having everything work together with one platform allows you to see everything holistically, make changes easily, and manage your environment with ease.

Finding a single platform that provides all four elements of a modern device management solution is key to:

- Preventing blind spots
- Contextualizing data
- Ensuring security
- Maintaining compliance
- Empowering your IT team

Choosing the Right Platform

What should you look for in a vendor?

Finding a solution that can satisfy the requirements of a modern device management program may feel a bit unachievable, especially if you're starting with a fairly outdated solution.

Fortunately, though, vendors have begun responding to modern device management challenges with newer solutions designed to address the problem. problem with more modern device solutions. When shopping for a device management tool, look for vendors that are modern and solutions that have been developed more recently and are frequently updated.

More specifically, look for vendors and platforms that prioritize:

- ✓ IAM (included or integrated)
- ✓ Compliance
- ✓ Unified endpoint management (UEM)
- ✓ User experience
- ✓ Third-party integrations (i.e., Google Workspace)
- ✓ Flexibility
- ✓ Security
- ✓ Agnosticism (for OS, vendors, device types, and tools)

Typically, these solutions will be cloud-based and agnostic to device type and OS, they're flexible. This makes them future-proof investments, which means you'll more than make up for the cost of acquisition over time. And because these tools consolidate several functions, they can be a smarter and more cost-effective investment in the long-term.

Device Management with JumpCloud

Ultimately, your new device management program should reframe your device management program to be a function of identity management.

Practically, this means you should be looking for identity-centric solutions that provide both identity and device management in the same platform.

That's how JumpCloud approaches devices — as a function of identity. JumpCloud is an open directory platform that was founded with unified identity and device management as a guiding principle. It offers modern device management that's OS-agnostic, mobile-friendly, and built to accommodate the modern workplace.

With JumpCloud, you can integrate device management with JumpCloud's proprietary IAM solution or your existing IAM (like Microsoft AD or Google Workspace). If you stick with your existing IAM solution, JumpCloud integrates with it, so you can still manage all identities and devices in one platform. Learn more about JumpCloud's federation services.

To see JumpCloud's unified identity and device management in action, start a free trial today. Got questions? Contact sales to dive deeper and see how JumpCloud may fit into your environment.

jumpcloud™

About JumpCloud®

JumpCloud® delivers a unified identity, device, and access management platform that makes it easy to securely manage identities, devices, and access across your organization. With JumpCloud, IT teams and MSPs enable users to work securely from anywhere and manage their Windows, Apple, Linux, and Android devices from a single platform.

Learn more: https://www.jumpcloud.com/

Follow us: Blog | Community | Podcast | X | LinkedIn | YouTube | Resources

Click here to get started with JumpCloud.