Whitepaper

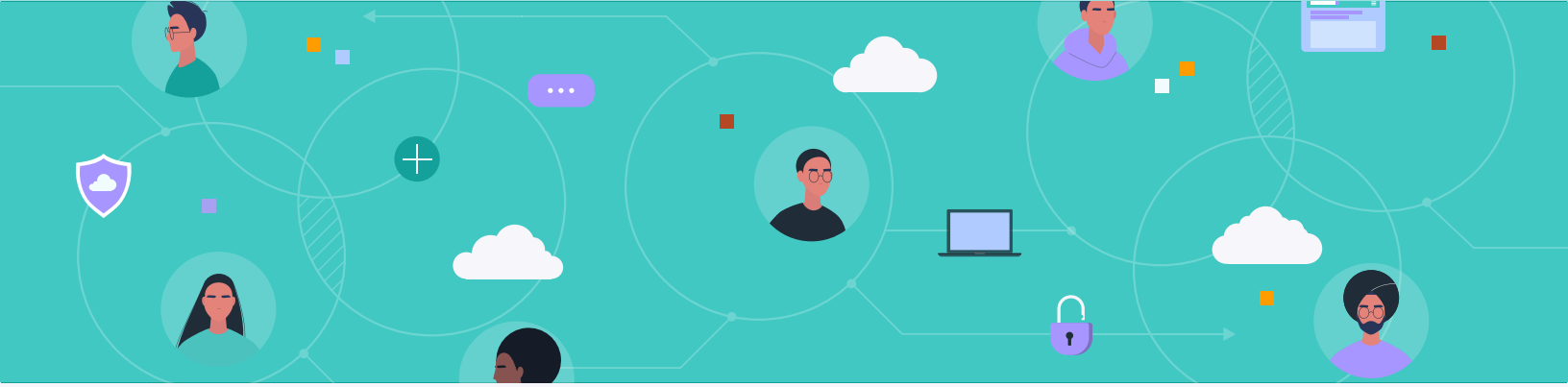
jumpcloud

Version 2

# The Five Key Components of Modern Device Management

## Contents





## Long gone are the days of domain-joined enterprises using majority (or exclusively) Windows-based devices.

Today's IT environments are far more intricate with Mac, Windows, and Linux devices, remote employees, cloud services, a mix of Internet facing web- and browser-based apps plus locally-installed apps, and increasingly sophisticated cybersecurity threats.

Traditionally, the management of a full cross-OS fleet environment has required multiple tools and processes to accomplish core management and maintenance functions. An organization's course of action depends on various factors, including the platforms in use, user locations, the existing directory structure, legacy tools, and more. Most organizations have been forced to use a mixture of manual management, clunky open source solutions, single OS / platform point tools, and other semi-effective approaches.

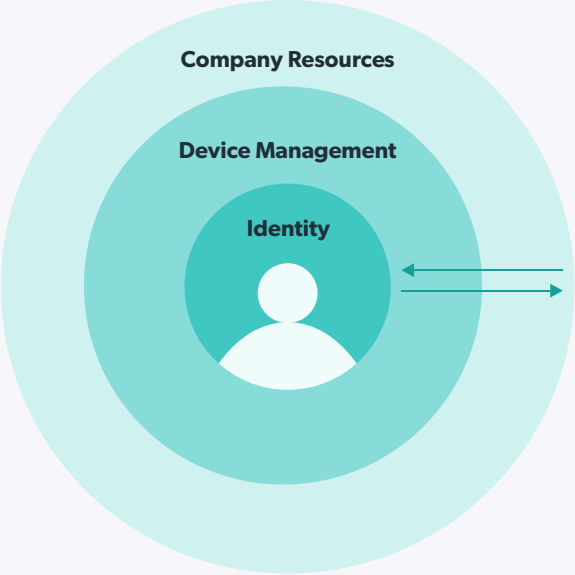
These approaches place additional strain on IT, a team (possibly only one or two people strong) that is likely already stressed and stretched thin. IT is forced to spend time and energy juggling multiple solutions instead of thinking creatively and tackling larger initiatives. As a result, end users are either overly controlled or literally "left to their own devices" without the proper support or guidance they need to get the right setup in place, or get the right access in a timely manner. This only heightens the tension that can exist between end users and IT, and it is ultimately the organization that suffers.

What if instead there was a consolidated, holistic, secure and compliant approach IT could take to meet their organization's device management needs without forcing them down a specific path? What if there was a single place to manage policies, settings, and everyday admin tasks for every single endpoint, regardless of the network they reside upon, applications they need to access, or operating system they use? As the environment in which IT operates becomes more diverse, the management tools used to deploy, secure, and manage devices must shift to meet today's needs. To pave a more effective way forward, we must also shift our understanding of device management.

© 2021 JumpCloud Inc. All rights reserved.

# Device Management Redefined for the Modern Era

There has been a substantial shift towards remote work due to the global pandemic. In the next five years, the number of remote workers is expected to be nearly double what it was before COVID-19. No longer tied to on-prem infrastructure, employees are now working on a wide range of device types, operating systems, and networks. IT needs to be able to securely manage remote users and devices everywhere they exist, from anywhere.




To accomplish this successfully, the focus of device management can no longer be on devices alone. Although user management has not traditionally been considered a part of device management, *identity* is now at the core of what IT manages, and as such, the device is an integral component of one's identity at an organization. It is the *identity* that ultimately accesses company resources: by a user, via a device. Comprehensive device management in modern IT environments must encompass both user management and device management.

There are four characteristics of the modern IT environment that are driving this shift in perspective:

**Location-independence:** The focus of IT has expanded beyond the management of on-prem technology. Firewalls and perimeter security are no longer enough to secure fleets. Every single endpoint in every single employee's home must be able to be remotely secured and managed.

**Vendor-agnostic:** There is diversity in device, app, and operating system usage. Highly productive employees can choose the tools they prefer to work with without being limited by an organization's management system. Employees who have the freedom to take ownership of their tools perform 22% higher in performance reviews and are 17% more likely to stay with an organization.

**User-focused:** Not only is user management vital for securing organizations with a distributed workforce, but the end user experience is also important for making sure work happens effectively both inside and outside of the office. It's important for IT to build a culture of user trust by giving users what they need while also allowing for free-flowing communication. This empowers users to work where they need to work, not just where the office needs them to work.

**Touchless:** The need for touchless workflows (read: automation) for safe onboarding and ongoing management is essential for IT in a post-pandemic world.

© 2021 JumpCloud Inc. All rights reserved.

Modern device management plays two critical roles in today's IT environments:

**Keeps an organization safe and secure.** A user's device is not only a gateway to their work, it is a potential conduit for hackers to breach an organization. If a device is compromised, that user's identity and the resources they access are likely compromised. IT is responsible for both preventing and mitigating those risks.

**Enables end-user productivity.** A user's device becomes a conduit to their IT resources, which subsequently helps those users get their work done. A core part of IT's role is to securely connect users to those IT resources with as little friction as possible. IT must also manage devices for optimum performance (i.e. uptime, speed, reliability, etc) and security (see below).

> **"When modern device management is thought about this way - as a conduit to IT resources that needs to be high performing and secure in a remote and on-prem work environment - IT admins can break down the management tasks into five key areas."**

© 2021 JumpCloud Inc. All rights reserved.

# 5 Key Components of Modern Device Management

The following components of modern device management create an overall approach that should be consistent across all devices, independent of their operating system or intended use case. As this can create complexity without a central platform from which to implement this approach, a cloud directory platform is best suited to be the true owner of all users, devices and IT resources.

## 1 Zero-Touch Enrollment & Deployment

Provisioning machines used to be a huge hassle, but modern mechanisms are making enrollment and deployment as easy as Zero-Touch for IT admins. Technology such as Microsoft's Autopilot and Apple's Automated Device Enrollment through Apple Business Manager are enabling IT organizations to drop ship machines directly from the manufacturer to the end user. When the end user opens the machine, it automatically configures settings, software, and accounts based on the company requirements and policies downloaded from the cloud.

All of the processes that used to require the maintenance of a master disk image now happen automatically, and the manual installation and configuration of individual machines is not required. The best part is IT can orchestrate this entire process remotely and securely, without the need to create a temporary account and password for the end user.

## 2 Full User Management Control

As discussed previously, ensuring a user's account is properly managed and secured is one of the most important tasks for IT and a core part of modern device management. An organization is only as secure as its weakest user. Over time, validating a user's identity on a machine will be leveraged to assert their identity with other applications, file servers, networks, servers, and more.

Identity management can be combined with other aspects of multi-factor authentication (biometrics, one-time passcodes, etc.) or conditional access policies (known IP ranges, known devices, etc). Updating that identity is one of the riskiest parts of the identity management process since phishing is responsible for one-third of cyberattacks on businesses. Secure password updates on the machine can completely side-step this and reduce the risk of being phished.

© 2021 JumpCloud Inc. All rights reserved.

## 3 Remote Device Configuration

Device management doesn't just stop with the initial deployment, though. Company policies change, new OS updates add new configuration points, and apps are frequently updated. A vital aspect of a modern device management solution is being able to update configurations remotely. If IT needs to achieve PCI or HIPAA compliance, then full disk encryption, a firewall, and a screensaver lock is a must. If there is a zero-day exploit, IT might need to adjust a setting or configuration to prevent a breach. As a result, IT requires the flexibility to address these changes quickly and remotely. As technology changes, the level of management can evolve as well. Don't assume the level of control required to keep devices in compliance today will last for the machine's lifecycle.

Some important questions to ask of a device management system:

— Can it make custom registry changes or deploy custom mobile configuration profiles?
— Can it set GPO-like configs across a cross-platform fleet?
— Can it turn on full-disk encryption? Enforce MFA?
— Can it disable a machine if it goes missing?

## 4 Software & OS Update Management

Despite the rise of web applications, IT admins still have a number of on-device applications that need to be managed. From the Microsoft Office suite to Adobe to Zoom to security solutions such as anti-malware or EDR, there is a wide range of software that needs to be controlled, managed, and updated. Not to mention all of the software that IT admins want to ensure is not on a machine. A device management solution needs to have the ability to install, manage, update, and remove applications regardless of the device's location.

From a compliance and audit perspective, an IT administrator should have the ability to see what apps are on their managed devices at all times and have the ability to block certain ones in the future. When combined with zero-touch deployment, a company's managed apps can be installed before the user is finished logging into their computer for the first time. Add in browser software and this is a major category of managing a device. Keeping the OS and all applications up-to-date is a massive chore for IT admins, especially when considering all of the different OS patch cycles and application updates. IT admins need a solid system that informs, updates, and reports on patch status.

## 5 Device Health & Telemetry

Even after a machine is deployed, configured, and secured, constant vigilance is necessary, especially with remote employees. A corporate laptop is used for eight or more hours per day, and that means configurations, settings, and security settings can inadvertently change, be maliciously compromised, and more. Having deep and continuous telemetry and understanding about the OS and the software, and knowing quickly what problems and issues can arise, means IT admins can help their users stay productive and avoid a security incident. It's not about creating a "big brother" environment but rather ensuring that essential corporate IT resources remain secure. And, it's possible to generate this telemetry without interfering with user privacy or preventing the user from doing their job.

© 2021 JumpCloud Inc. All rights reserved.

# How to Achieve Modern Device Management

> There is an alternative to cobbling together various solutions to accomplish zero-touch deployment, device management, user control, app control, and device telemetry. This modern approach is called a cloud directory platform.

JumpCloud simplifies device-management workflows while providing user access control across virtually every resource in your IT infrastructure — all from a cloud-based console that can be accessed from anywhere by both admins and employees. JumpCloud MDM leverages Apple's MDM protocol to secure and manage devices with JumpCloud configurations and security commands. For those running Microsoft technologies, you can apply Windows Security Commands to restart, shut down, lock, or erase a device in moments to keep end user machines safe as well as GPO-like policies. Windows devices with the JumpCloud Agent installed that are online will receive commands right away, and commands will execute on offline devices the next time they come online. JumpCloud can also be used to manage and secure Linux-based devices. From the latest Mint desktop distros on workstations and laptops to Ubuntu servers and AWS infrastructure running on ARM64 processors in the cloud, JumpCloud enables efficiency, performance and the most cost effective device management, all from a single platform.


jumpcloud

Get started today with the full JumpCloud platform for 10 users and 10 devices with 24/7 support included for your first 10 days in action.

Try JumpCloud Free →