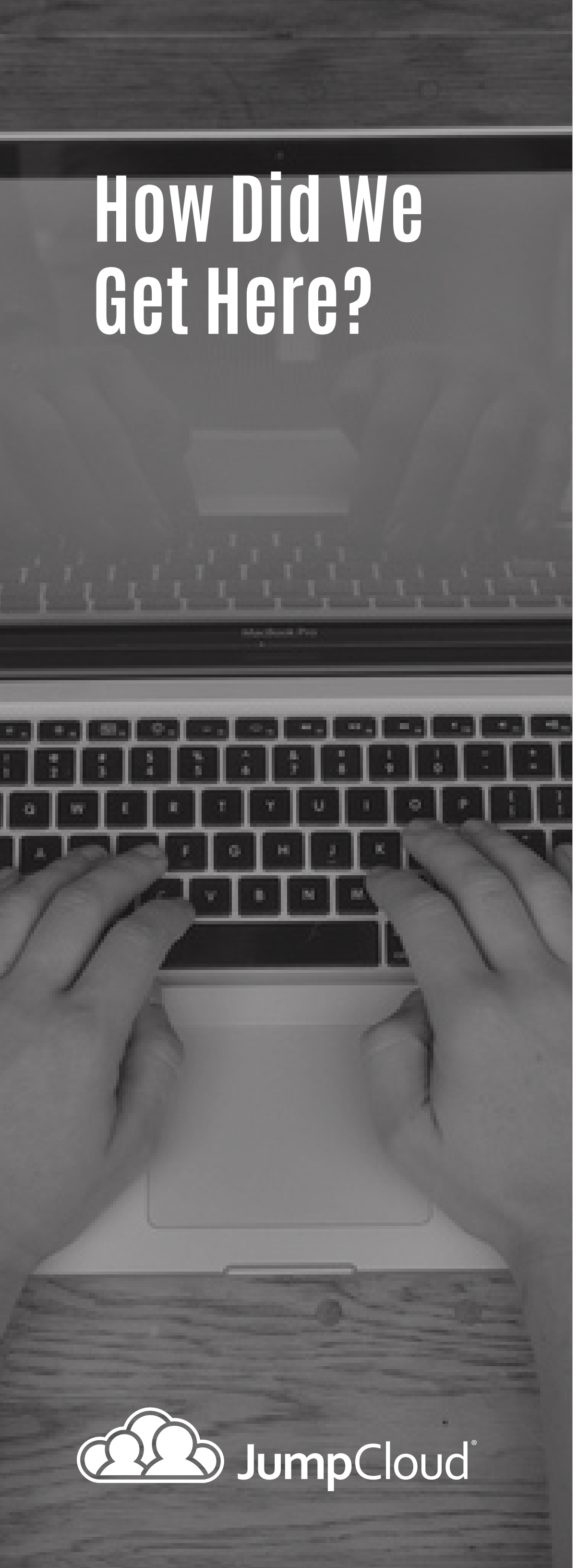
Integrate Mac Users And Devices Into Your IT Infrastructure

A guide for how modern IT teams easily manage Mac users and devices

JumpCloud®



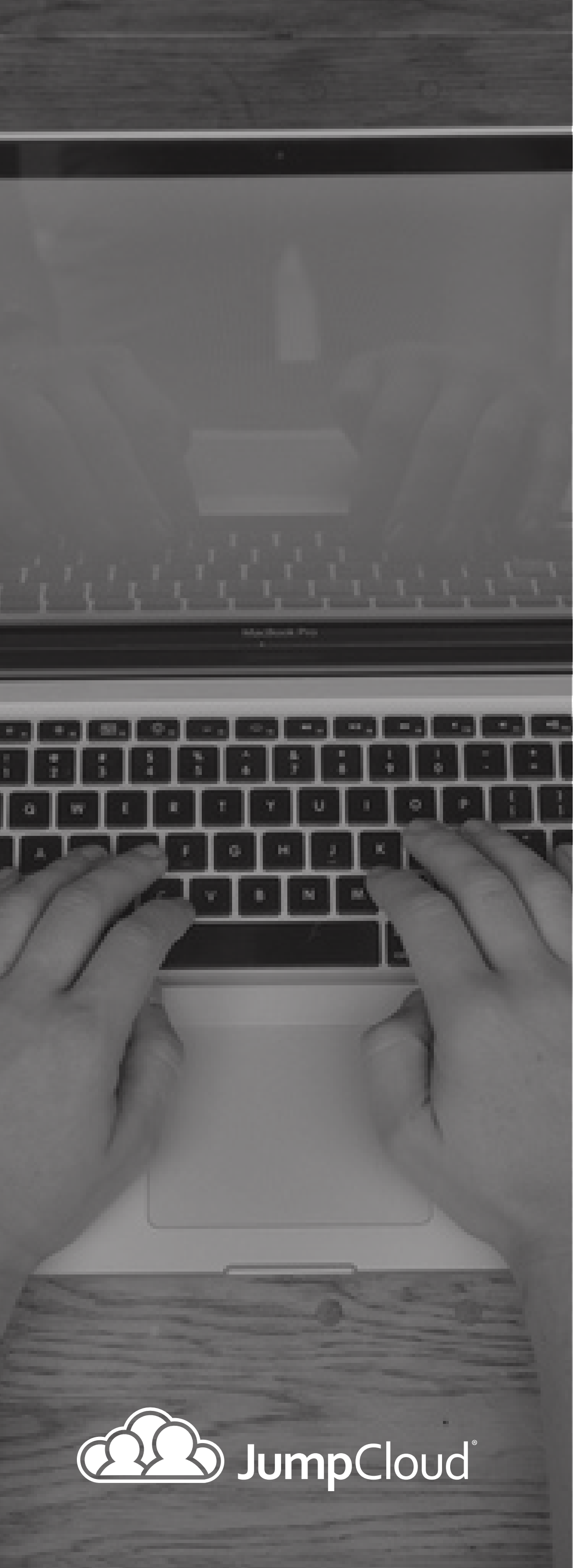
How Did We Get Here?

The move to the cloud, coupled with the acceptance of Macs in corporate environments, has created headaches for IT teams

Fundamental shifts in the technology industry over the last decade are challenging IT teams when it comes to managing their infrastructure. First, corporate environments have adopted sleek looking Mac desktops and laptops en masse as the preferred corporate device. Simultaneously, there is an increased transition into cloud-based systems and away from the traditional network “domain.” For example, many businesses have moved to Google Apps and Gmail versus Microsoft’s Exchange, while maintaining Active Directory (AD) as a central control point for users and Windows device management AD is the authentication solution of choice for on-premise services, but as applications move to the cloud, IT admins struggle with control over authentication, authorization, and management.

With these two major shifts in corporate structure, IT admins are now forced to reassess their internal IT infrastructure.

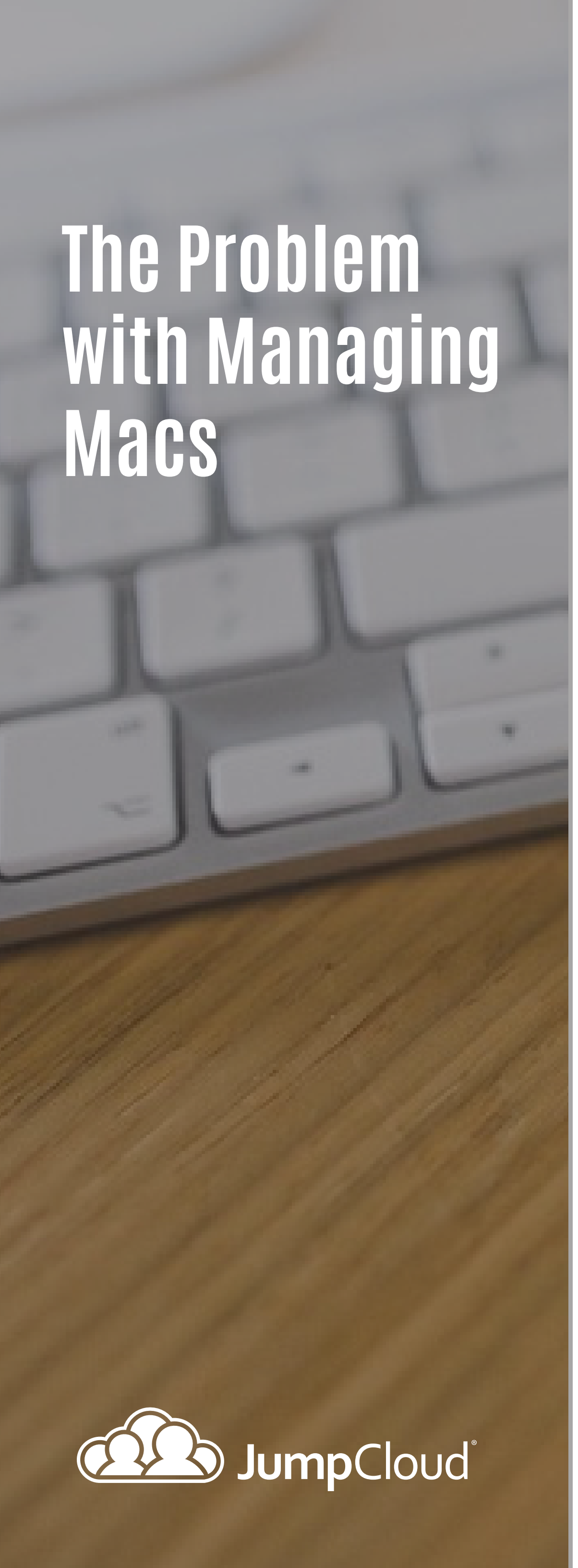
The technological shifts in corporate solutions result in a similar shift in on-premise network infrastructure. Server rooms and data centers are falling by the wayside as IT teams shift services to cloud-based services



such as file storage, CRM, and many other applications. As the demand for on-premise networks decreases, and businesses shift to using Macs as the preferred end-user device, where does that leave IT admins who are still required to manage their user's access to the network and their devices? The solutions to date are limited, and, many cases, cost prohibitive.

Extracting value from Active Directory becomes far more challenging as business solutions become increasingly cloud-based. Further, as Macs infiltrate organizations, it quickly becomes obvious that the level of management AD can provide is not sufficient. And, with less infrastructure on-premises, where is AD installed?

For some organizations, the question is: Do they even require any Microsoft infrastructure anymore? The move to Gmail—while solving the specific problem of reliable, cost-effective email—doesn't solve the problem of access control and device management in either a Windows or Mac context.



The Problem with Managing Macs

IT administrators are looking to solve these common problems with their Mac devices

CONTROL ACCESS

Controlling access with Macs is not easy. While the systems can be connected to AD or the open protocol, LDAP, there are serious limitations including how to provide for more secure access with multi-factor authentication. In scenarios where AD or LDAP do not exist, there's no control over access unless it's manually managed.

DEVICE MANAGEMENT/ SUPPORT

As with any other type of desktop or laptop, Macs can have issues, can require patching, and can fail. IT admins have many easy-to-use tools to help manage Windows devices, but Macs require expensive, enterprise-class software.

SECURITY

Unmanaged Macs represent serious security risks to an organization. While they're touted to be more secure with fewer viruses and trojans, unmanaged Macs cause risk with data leaving the organization. With many of today's developers having full development environments on their Macs with source code, and often with full "Administrator" level access on the device, a terminated employee could still have full source code access to an organization's applications.

Exploring Traditional Solutions to the Mac Problem

Organizations have been opting for one of three solutions to the difficult problem of managing Macs in their environment

NO MANAGEMENT

“In many “bring your own device” contexts, or in start-ups ramping up their employee base, organizations allow Macs on network but don’t manage them at all. User access is not controlled, security is not managed, and the users are largely on their own from a desktop support perspective. Or, in some cases, IT admins will help where they can, but they don’t have tools to remotely execute tasks or manage the device. This is the most common scenario in smaller organizations, or organizations where there isn’t Active Directory or LDAP.

MANUAL MANAGEMENT

Where organizations have concerns about security or are connecting to AD/LDAP, admins may setup and manage the Mac devices manually. There may be a standard Mac “build” with admin accounts created on the device. This enables IT admins to control users and support with issues, but is not scaleable.

Exploring Traditional Solutions to the Mac Problem

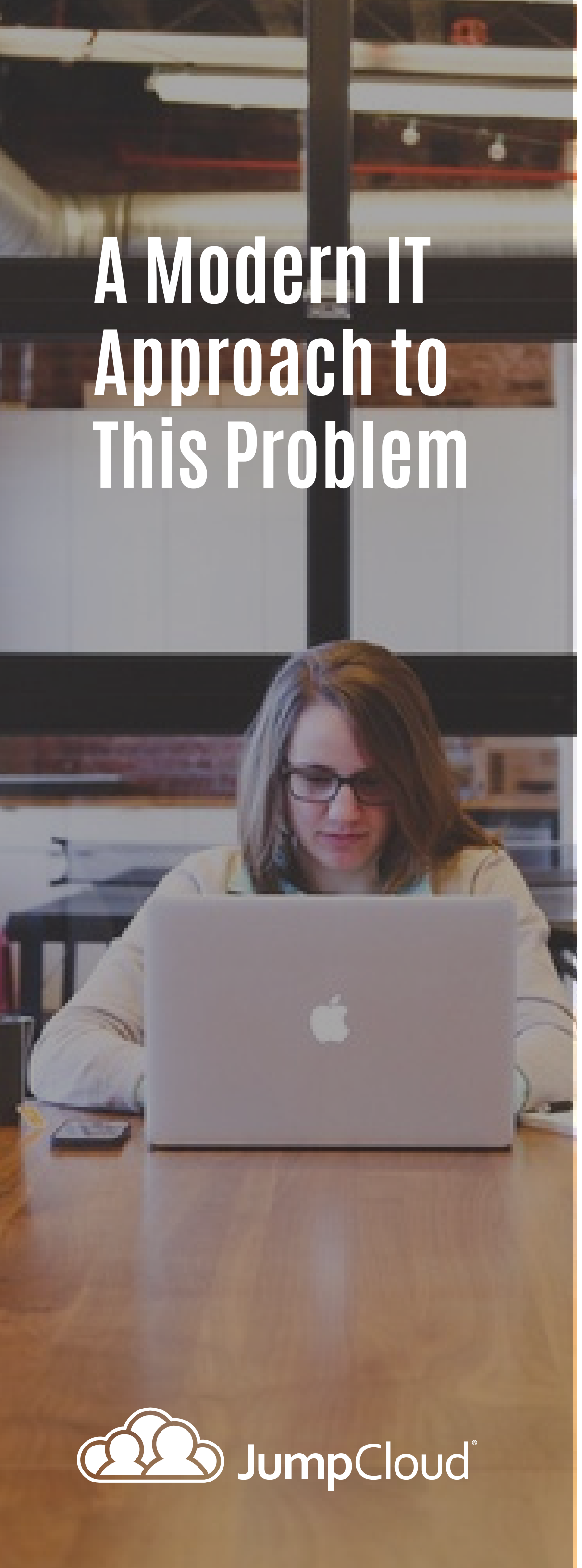
JumpCloud®

ENTERPRISE-CLASS ON-PREMISES SOLUTION

Larger enterprises may have enterprise-class administration tools including those with identity access control. These solutions often have an agent on the Mac device that helps with access control and management. The server software is housed on-premises and is used to manage the entire desktop infrastructure. However, this scenario becomes a challenge as the organization decides to move to Google Apps/Gmail or starts to shift their infrastructure to the cloud.

For modern, innovative organizations, none of these solutions will suffice. Their IT admins need an infrastructure that is agile, scalable, and resilient. And, therefore are turning to cloud-based solutions, where they have both the availability to let their users bring whatever devices they want, and take security controls seriously in an era where theft of identities can lead to access to a company's crown jewels.

A Modern IT Approach to This Problem



Easily manage Mac users and devices through SaaS-based user management platforms

Innovative organizations are leveraging SaaS-based services to manage their Mac desktops and laptops. Whether the organization has AD or LDAP already on-premises, or they are leveraging Google Apps, these SaaS-based services make managing Mac devices simple, cost-effective, and secure.

The service approach is simple to introduce. A small, lightweight agent is installed on each Mac in the business, and the agent communicates securely to the SaaS-based console. From the console, IT admins can control such tasks as: (1) creating, deleting or modifying users; (2) remotely patching machines or checking on configurations; and (3) troubleshooting or fixing problems remotely regardless of where the device is and what network it is connected to.

If companies have already invested in AD or LDAP as a part of the organization's infrastructure, it can be connected to the SaaS-based service allowing for easy syncing of user access, and can assist the organization with bridging users to "hard to reach" infrastructures such as servers managed in the cloud. This capability extends AD or LDAP to the Mac and provides for fine-grained control over user accounts. If the organization is leveraging Google Apps, users can be imported and synced with that directory while authentication services can be provided by the SaaS-based service.

The Benefits of a SaaS-based service to manage Macs

ONE SYSTEM TO CONTROL USERS AND MANAGED DEVICES

IT admins have a way to address the risks that their Macs pose to their organization. A simple SaaS-based offering to manage Macs gives admins the control and security that they need. A terminated or disgruntled employee no longer needs to be seen as a security risk. Access to their device and any other infrastructure can be terminated immediately, or IT admins can wipe the drive remotely. With these capabilities, admins can rest easy knowing that they have the control they need.

INCREASED SECURITY

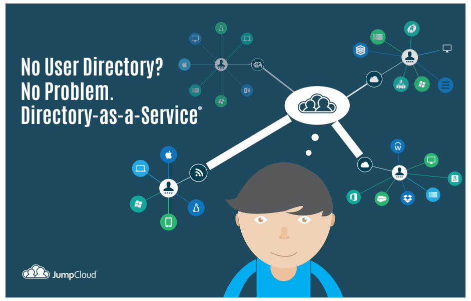
A SaaS-based service is efficient and effective. It gives admins the ability to control access while also giving them the ability to manage the device with only one agent to deploy. IT admins solve their core needs of user control and device management with one SaaS-based service.

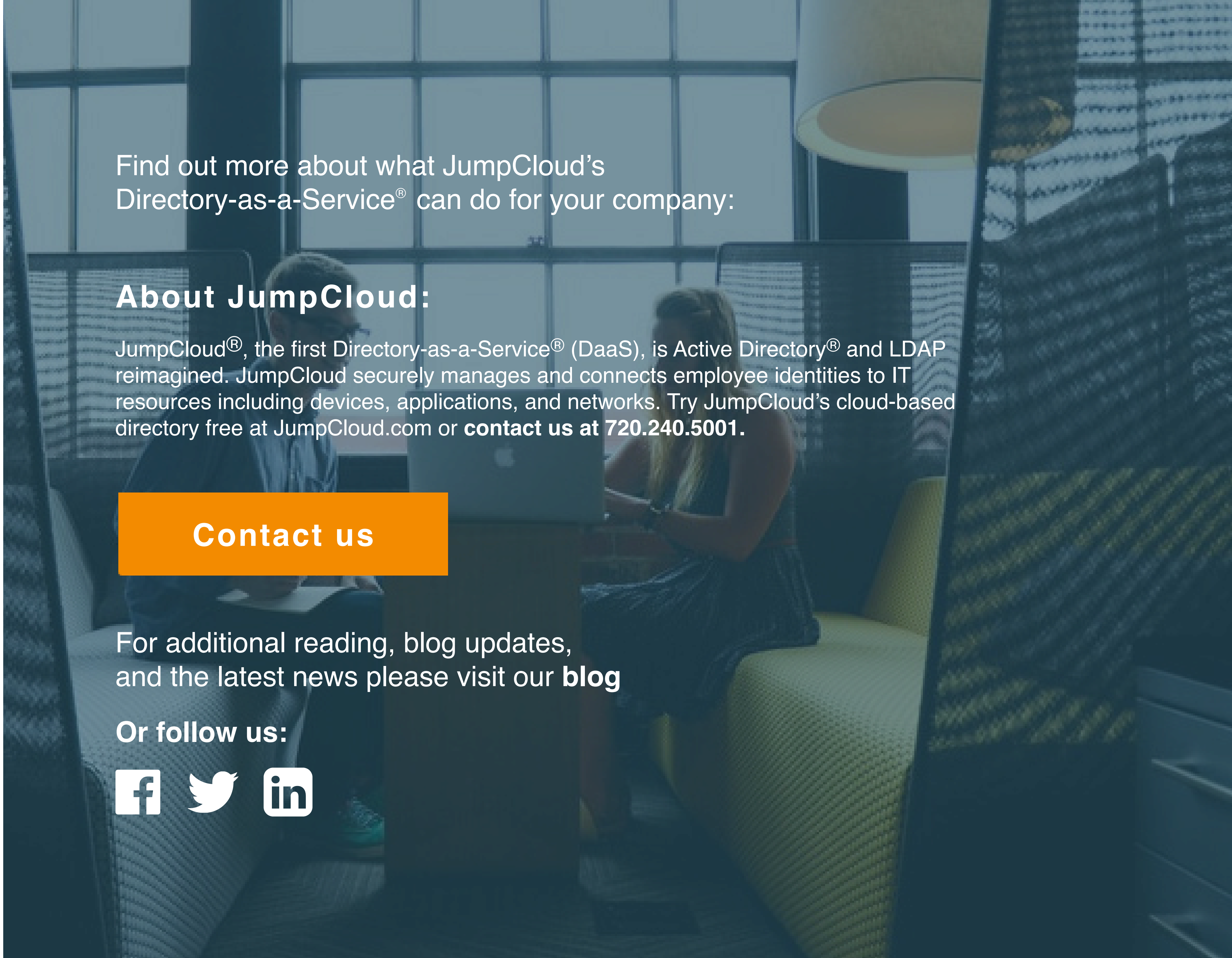
COST-EFFECTIVE

The most innovative organizations are turning to SaaS-based Mac user- and device-management services. This is because SaaS solutions offer inexpensive, pay-as-you-go features that allow companies of any size to assess and manage their directory.

Looking for more information?

Click these guides to learn more about DaaS:





Find out more about what JumpCloud's Directory-as-a-Service® can do for your company:

About JumpCloud:

JumpCloud®, the first Directory-as-a-Service® (DaaS), is Active Directory® and LDAP reimagined. JumpCloud securely manages and connects employee identities to IT resources including devices, applications, and networks. Try JumpCloud's cloud-based directory free at JumpCloud.com or **contact us at 720.240.5001.**

Contact us

For additional reading, blog updates, and the latest news please visit our **blog**

Or follow us: