JumpCloud

2016 IT Department Guide to

Onboarding AND Offboarding

It's lunchtime and you're headed out with your colleagues. You sit down to order lunch and your phone lights up with numerous calls and texts flying in. An engineer was let go and it didn't go so well. Unfortunately, the engineer has access to all of the source code, some production machines, and knows critical passwords to services such as Github. The VP of Engineering is texting to see if you can quickly cut off access to everything. The HR Director is on the phone telling you what is happening. There's panic in her voice.

This scene may sound far-fetched, but it happens all of the time.

People are hired and fired without IT being in the loop. It shouldn't ever happen, but it does.

This is just one of many onboarding/offboarding scenarios that can leave you behind the curve and needing to react quickly. Do you have the right systems in place to execute on these types of emergencies?

> "Everything must be made as simple as possible. But not simpler."
>
> Albert Einstein

While improper offboarding is a security risk, improper onboarding is an efficiency issue.

You want to be able to onboard a new employee so that it doesn't take up too much of your time. You should have centralized control so that you can delegate the appropriate levels of access to resources that new employees will need. Everything needs to be ready for them on their first day.

Organizations with a standard onboarding process report 54% greater new hire productivity.

source: Urbanbound

When your organization has everything ready for a new employee from the moment they arrive, it sends a message that you care about your employees and their productivity. It also says that your organization is execution-oriented and that employees are expected to follow suit.

Onboarding and offboarding employees is a critical task for IT.

Onboarding sets a foundation.

You are setting up your employees for success by connecting them to the IT resources they need. This includes systems, applications, networks, and more.

The onboarding process is also an opportunity to ensure that the new employee understands your policies and standards around IT and security. **This is huge in a world where 52% of security breaches are caused by human error.**

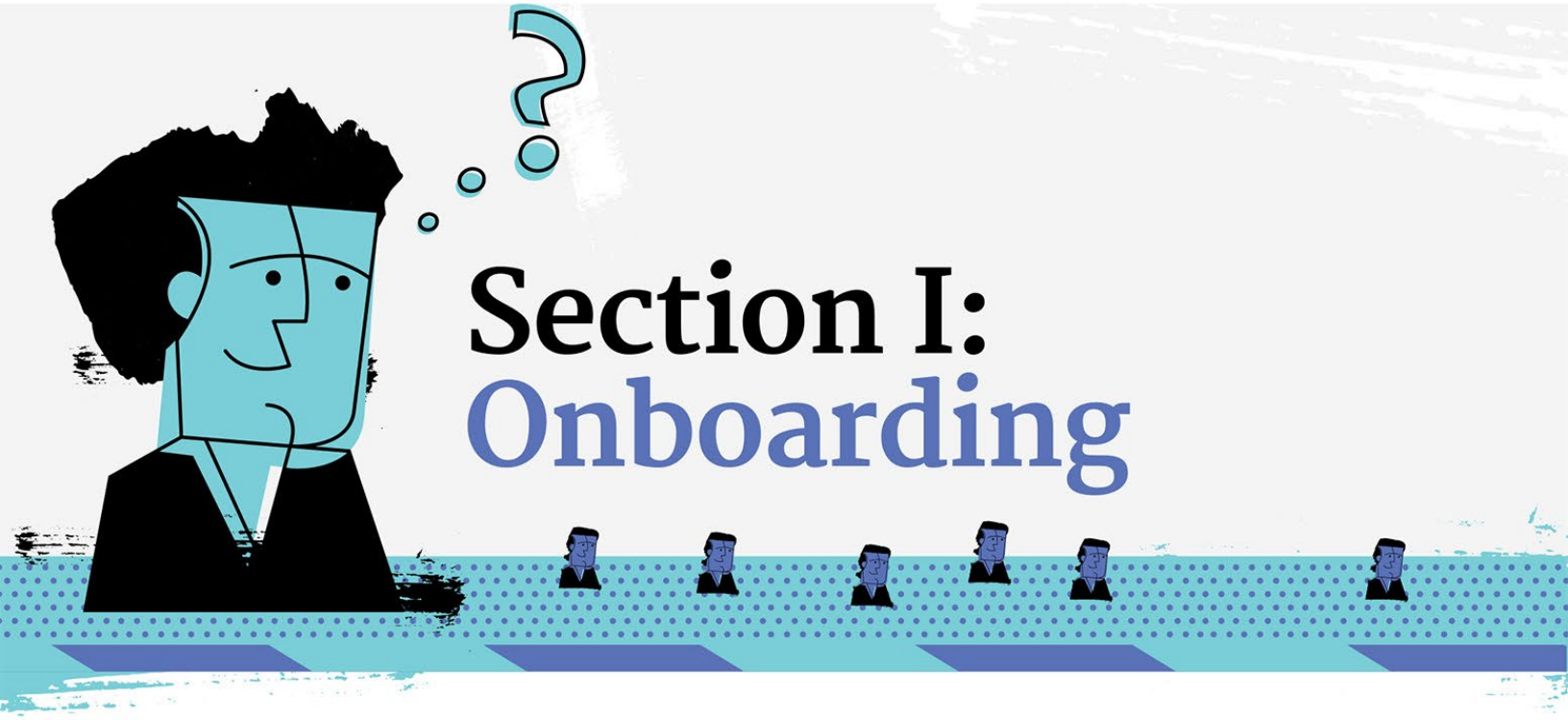
Offboarding keeps it secure.

Once you've decided to move on from an individual, you need to ensure that your organization is safe. That means deprovisioning access quickly and completely. Unlike the onboarding process, offboarding is something that needs to happen all at once, in a moment in time.

Your security is only as good as your reflexes.

This is where strong systems make a difference. The better the system, the faster the response. The faster the response, the safer the organization.

In this eBook, we delve into the topic of building strong processes and systems to help with onboarding and offboarding.



Section I: Onboarding

Do I need a process for onboarding my employees?

For certain small companies (10 employees or under) an onboarding system isn't 100% necessary. But onboarding process is much more than just ensuring that a new hire is connected with all the IT resources they need.

As an organization grows, security risks increase. The biggest threat comes from your own employees, who often have insecure passwords and file transfer methods, or who implement shadow IT and shared accounts. Onboarding is your chance to instill proper proper security practices from the get-go.

It's also their first impression of the organization. It's the first real view into the company culture. Effective onboarding sets the expectation of effective work.

Organizations with a standard onboarding process benefit from 54% greater new hire productivity and 50% greater new hire retention.

Source: Urbanbound

The Onboarding Process must be:

Accurate

Users need to have access to the appropriate resources at the appropriate levels. This starts with building in proper user management controls.

Efficient

You can save valuable hours for IT and HR with efficient onboarding Automation will save time and limit mistakes.

Secure

Ensure that your new employees have access to the IT resources they need (networks, devices, and servers) and nothing they don't need. This will create a much more secure working environment from the start. Security must be built into the system as well.

Automation is key. Automating onboarding tasks results in 16% higher retention of new hires.

source Aberdeen Group

Before You Get Started...

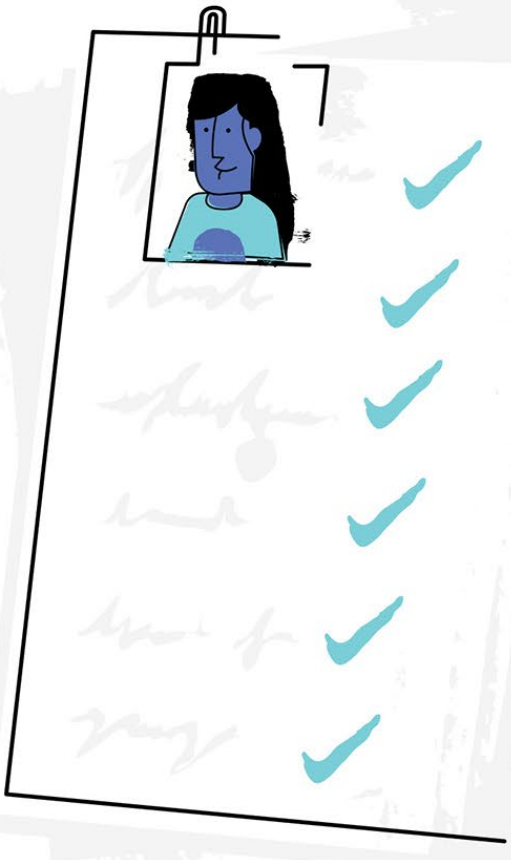
While this guide is primarily for IT, to streamline the onboarding process make sure the new hire and HR have all the information they need to get started, specifically:

- The signed offer letter
- Legal paperwork
- Basic information about the individual
  - Who they are working for
  - Position
  - Group within the company

Begin Onboarding

Here's what IT will need to address in onboarding:

- Directory Service
- Implementing Email system
- Device Provisioning
- Server and Infrastructure
- Applications
- WiFi Access
- Printers



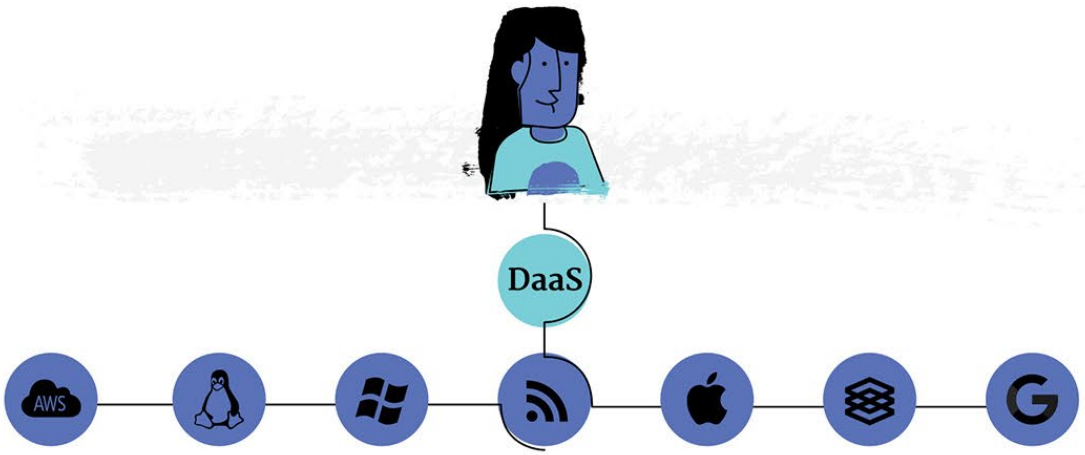
Directory Service

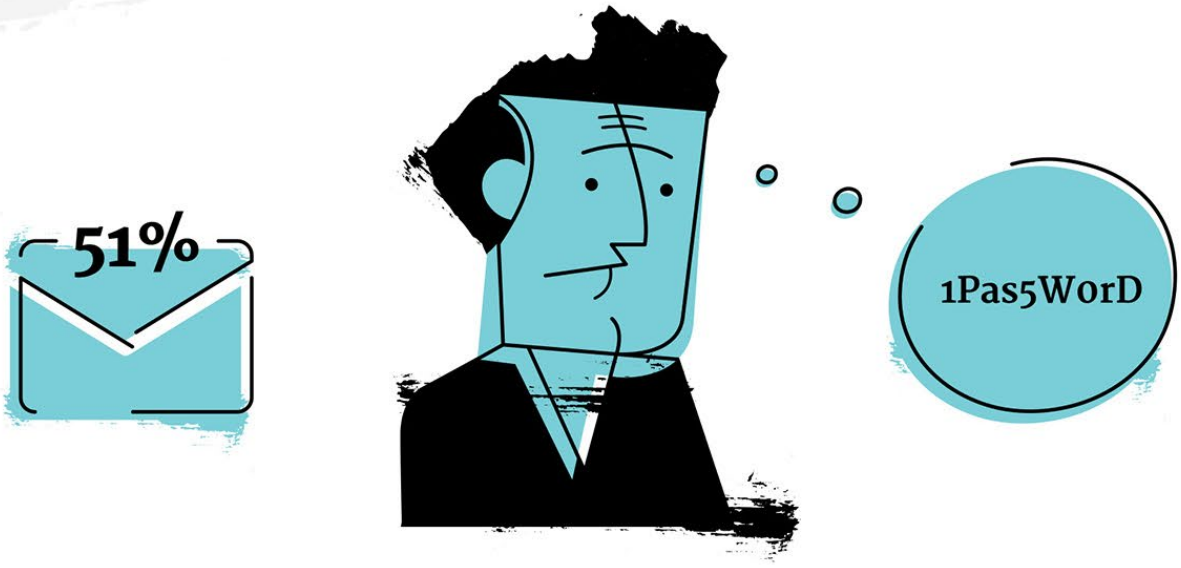
The first step on the IT side is to add the user to the core user database, also known as the directory service. The legacy option here is an on-premises directory such as Microsoft Active Directory (AD) or in some cases, OpenLDAP. These are generally best suited to managing a contained office environment, with all devices using one operating system (e.g. Windows in the case of AD).

Conventional directories also require infrastructure on-premises, which won't work for a company that is utilizing cloud infrastructure (SaaS applications or cloud-based servers). Increasingly, companies are turning to cloud-based directory services such as Directory-as-a-Service (DaaS).

This is because today's IT environment is heterogeneous and driven by SaaS-based models. Remote workers are flourishing. Device platforms and operating systems are multiplying.

Microsoft Windows isn't the only choice and, in fact, it's often not even the first choice for many companies any more. Macs and Linux devices are increasingly becoming the norm, and a legacy directory is ill-equipped to manage them. A DaaS connects to a variety of operating systems and can centrally manage resources and applications across the cloud.





Implementing the Email System

There are a number of approaches to creating email addresses. It can be implemented when the employee is entered into the HR system through APIs with Google Apps, Microsoft Office 365, or even Exchange. Email creation can also be automated through some directory services.

What's important is that the IT admin is not the conduit of the password.

Instead, implement a system that sends the password to the user directly. This can be done via text message or by sending a message to an existing email account. That way the admin keeps their hands clean and security is preserved.

A recent Dimensional Research survey of almost **2,250** workers showed that **51%** of their devices were password protected with a single word. Ouch. All these systems are at risk. Dictionary attacks are still a very common attack vector. Another common breach originates from when an employee uses the same password for their work device to access other applications and even servers. Once one instance of the password is obtained, all accounts are compromised.

Device Provisioning

Some organizations issue a standard device configuration and others allow more customization by the new employee. Most organizations are leveraging a Bring Your Own Device (BYOD) policy.

> "Employees using BYOD in The United States save an average of 81 minutes per week" (Cisco).

When considering the pros and cons of a BYOD policy, remember this: employees will bring their own device no matter what. 67% of people use their own personal devices at work, regardless of the office's official BYOD policy (CBS News). If you want to be safe, you'll need to be ready to manage people's devices, be they Macs, Linux, or Windows devices.

When it's time for onboarding, you'll start by creating the user's account on the machine. This can be done by connecting the device through the directory service. A good directory service will be vendor neutral, which is a plus for companies with a BYOD policy, as they can easily manage Macs, Linux, and Windows devices. Further, personal devices which may also be accessing corporate emails need to be remotely decommissioned from accessing corporate resources.

Servers and Infrastructure

If your new employee needs access to your server or network infrastructure, you must provision their access. Today, much of this infrastructure is located in the cloud at providers such as AWS or Google Compute Engine.

This is where a Directory-as-a-Service comes in handy. Users who have a DaaS will be able to easily provision and manage the new accounts. For legacy directories such as Active Directory, you'll need to ensure that your directory and servers or infrastructure are securely connected, at which point you'll be able to provision access.

Applications

Apps have become an essential part of the work environment – and therefore an essential part of onboarding.

Many companies respond to this challenge by implementing single sign-on (SSO) technology. Yet most current SSO providers only provide web application single sign-on.

It helps to think about it this way: when single sign-on was born over a decade ago, it was able to empower your workstation to sign-on to everything that you needed. One set of credentials was used to login to everything: your devices, applications, network, and more. Back then, the network was primarily all Microsoft Windows. IT used Active Directory and a domain controller to authenticate and authorize access to everything on-premises, which was almost all Microsoft Windows-based devices and apps. For cloud applications, SSO providers integrated with Active Directory to provide access to the organization's web applications. So when it began, SSO was able to control everything an employee had access to in one neat little package.

This is not to imply that SSO isn't a necessary and secure part of your IT toolbox. But it's important to remember that implementing SSO without an accompanying directory to lock down employee servers, devices, and networks is missing a huge security piece in your onboarding toolkit.

WiFi Access

One of the first things that your new worker will want to do is to jump on to the Internet. Some organizations just have an SSID and passphrase as their process to log on to the WiFi network. As IT admins know, this is weak security. Why? Well, as wireless networks overtook wired LANs in offices, the wireless network started to expand beyond the walls of a business. If a hacker had the credentials to the network, they could even hack into your company's confidential information from the parking lot! An SSID and passphrase can be easily compromised, and with employees joining and leaving the company often, it's hard to keep track of who has access to your network.

In response to this security concern, IT admins often require that users authenticate with their own corporate credentials when they access the company WiFi. Those credentials could be passed by LDAP or RADIUS, which are two common protocols for this assignment. However, this is a huge headache on an IT admin's part and there's some additional work on the client side as well.

IT organizations can take their network security up a notch by leveraging the WiFi infrastructure that is connected to the core directory service via RADIUS-as-a-Service. This ensures that every user must have credentials in your user store in order to access the network, but without the IT hassle.

Once your user arrives and picks their password, they'll need to enter it into the offboarding supplicant on their machine and they will be connected to the WiFi infrastructure via RADIUS.

Printers

Business still gets done on paper. And there are few things more frustrating than trying to print a simple document and being confronted by error messages.

Save your employees (and IT) that pain by ensuring that every new user's machine is configured to print to their nearest printer. Different WiFi networks can also have different permissions, ensuring increased security.

Security Training

So you've provisioned their accounts and you've still got the new employee in front of you. This is a great time to do some security training.

Every organization does things a little differently, so getting your users up-to-speed will help avoid problems and support calls later. Ideally, you'll have a help document with FAQs or an internal website that can help your users solve their own issues.

We can not stress enough the importance of early and regular security trainings. Employees are the leading cause of data breaches, but they often don't know that their behaviors could have catastrophic consequences. Nip those problems in the bud by making security training a serious component of your onboarding process.

Onboard, On Point

Setting up your onboarding process to be accurate, efficient, and secure is setting up your new employees for success.

Every organization's onboarding process will be different, but the components, steps, and security needs are the same.

Now onto offboarding employees, below.

Section 2: Offboarding

Onboarding employees is about enabling a user to be productive. Offboarding is about mitigating risk.

Nobody wants to think about parting ways with their employees, but it happens more often than we'd like. Nearly half of new hires are gone within 18 months [CNN]. Once a person's employment has been terminated, the organization should be focused on ending the relationship in a way that is:

- Efficient
- Respectful
- Eliminates Risk

The Risks of Improper Offboarding can be Fatal to your Business

When an employee is first terminated, he or she still likely has access to sensitive data (e.g. code, sales data, plans, pricing, or other materials).

Step 1: Remove the Employee from the Directory

Removing the employee from your directory should disable any services that need to authenticate the user. So, the user will not be able to login to their devices, will be deactivated from email, and application access will be terminated. If you have leveraged RADIUS for their WiFi access, that too will be disabled. Once their main user account has been halted, their core access has been terminated. Although you still have some work to do, major portions of your risk have been reduced.

Step 2: Terminate Access Across Infrastructure

The next area to focus on when offboarding is to eliminate the user's access across all additional pieces of infrastructure, outside of your core directory service. If you have a good directory service, this piece will be done when you disable the employee on your directory.

For example, if you are leveraging Infrastructure-as-a-Service solutions such as AWS or Google Compute Engine, you'll need to manage the former employee's access to these services. They likely have manually created accounts.

You'll want to disable access to all servers. If you don't have a central system to do this such as a cloud-based directory or a configuration management solution, then you'll need to do it manually.

Tip: The key here is to not forget any servers. Depending upon your architecture, there may be a "jump box" to focus on first and then the individual servers themselves.

If the former employee had a technical skillset and a high level of access, then they may have access to additional network infrastructure. Make sure you've tracked all employee access and that you're able to terminate it. A well functioning directory makes this seamless for you.

Step 3: Terminate Access to Apps / Resources

> "93 percent of organizations surveyed are running applications or experimenting with infrastructure-as-a-service."
>
> Forbes

From SalesForce to Google Apps, companies are using cloud-based apps in droves.

If your central systems or your single sign-on solution can deprovision users, then you'll have a head start on this function. A directory that's integrated with your SSO solution makes this instant. But even the best identity and access control solutions won't give you 100% coverage over every application. It's your responsibility to make sure all of your bases are covered.

Critical applications that should be thought of immediately include financials, CRM, and code repositories.

Start with the most important applications and work your way backwards to the less important ones. Deprovision the user on each application. When possible, you may want to assign data or access to certain components to the person that is taking over (or who is the backup).

Step 4: Deprovision Devices

Devices go one of two ways.

If the individual was using a company-owned device for work, it's straightforward. The device must be returned to the organization and their account disabled.

If the machine is a machine owned by the individual, then it gets more tricky. The device is theirs, but the access and data belongs to the company. You must respect the former employee's ownership while also ensuring that the data is cleared off the device.

> "Having an existing BYOD policy is absolutely essential."

There's always the honor system. You can just simply request that the former employee wipe the data and revoke their account access. You'll have to take their word for it.

If your company instituted a policy wherein you maintain the right to wipe the data clean from the device, then you'll want to take that step. This can even be done remotely with a lightweight agent embedded on the machine that should be part of your directory services.

Offboarding Complete

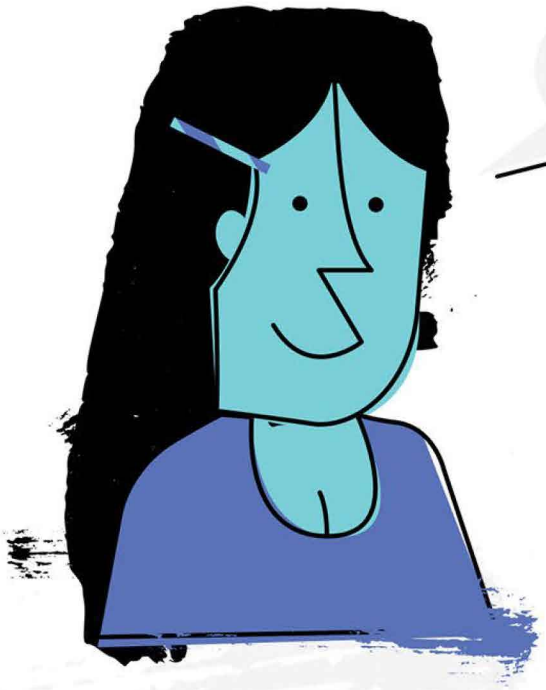
That was easy, right?

There will still be some remaining items such as exit interviews, physical access to the facility, parking passes, and other ancillary items. Those may overlap with IT, but they're more within the purview of HR.

"The most important thing for IT is to be prepared when the time comes for offboarding."

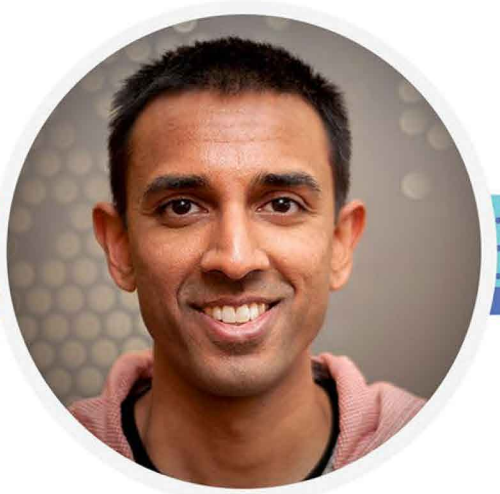
Offboarding employees is a critical, sometimes delicate, task – and one that shouldn't be left to the whims of the day. There should be a process with a specific checklist that is followed. Every company is different, so take the time to build your own thorough and systematic process that you can share with your IT employees before it comes time for a termination.

Ensuring that you have systematically disabled a past employee's access can be the difference between data being stolen and your company being kept safe.



Want to learn more?

- **Our IT guide to doing more faster covers:**
  - Hybrid infrastructure
  - SaaS-based applications
  - BYOD Policies
  - DevOps



About the Author

Rajat Bhargava is co-founder and CEO of JumpCloud, the first Directory-as-a-Service (DaaS). JumpCloud securely connects and manages employees, their devices and IT applications. An MIT graduate with two decades of experience in industries including cloud, security, networking and IT, Rajat is an eight-time entrepreneur with five exits including two IPOs, three trade sales and three companies still private.

Connect with JumpCloud

Reach out on Facebook, Twitter, or email. Read our engineer's blog **here**