



# The IT Checklist for Employee Offboarding

The 10 critical steps

To smooth and simple employee offboarding



## Fast employee offboarding the era of SaaS

New Software-as-a-Service (SaaS) tools are simple to adopt and quick to put to work, so it's easy to see why we like them so much. As IT managers, we know the benefits that SaaS can deliver, but we are also aware of the complex problems SaaS can cause when it comes to managing the offboarding of employees. It's vital to have visibility over the SaaS accounts that departing employees have open, so you don't end up paying for licenses you are not using and to keep company data secure. Often, when an employee leaves the company, it falls to the IT team to close down their SaaS accounts and revoke permission of the departing employee. The IT team also needs to understand what data lies within those apps so they can establish what should be deleted.

That's why we at Torii have put together this Employee Offboarding Checklist for IT. Your simple guide of the necessary steps to take when your employees move on.



## Offboarding example checklist:

- 1 Revoke system access from IdP and SSO
- 2 Close employee SaaS accounts
- 3 Terminate VPN and review any remote access methods
- 4 Change/revoke shared account's passwords
- 5 Change system's ownership
- 6 Forward employee's email address
- 7 Recover company equipment and assets
- 8 Reclaim employee licenses
- 9 Update credit card payments
- 10 Schedule account deletion for suspended accounts.

# 1. Revoke system access from your IdP and SSO



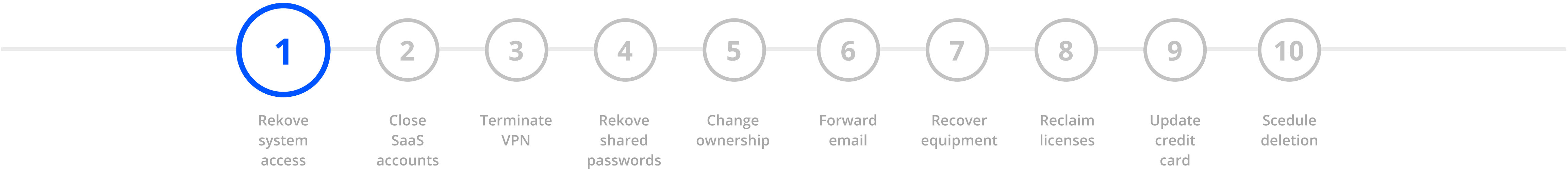
Your Identity Provider (IdP) is usually the first port of call. This is your single source of truth and in many cases, the access point to many other internal and external systems.

Log into your G Suite or Azure Active Directory admin console and suspend or disable the user.

**Tip:** *At first, you probably don't want to delete the user as you may need the data in that account at a later stage*

If you have a Single Sign-On (SSO) solution such as Okta, OneLogin or others, then disabling the user account on your SSO is one of your most important steps since the mission-critical systems are protected behind it.



**Pro tip:** *Do not reuse an old email address for new employees. For example, if john@example.com has left the company and then another John joins, do not give him the john@example.com address. This may allow him access to unrestricted resources.*

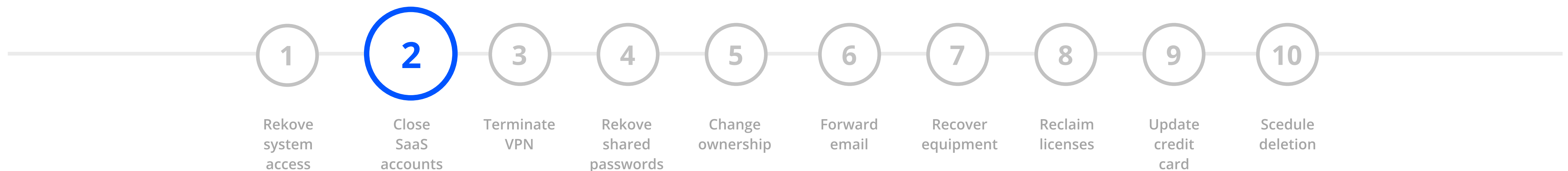
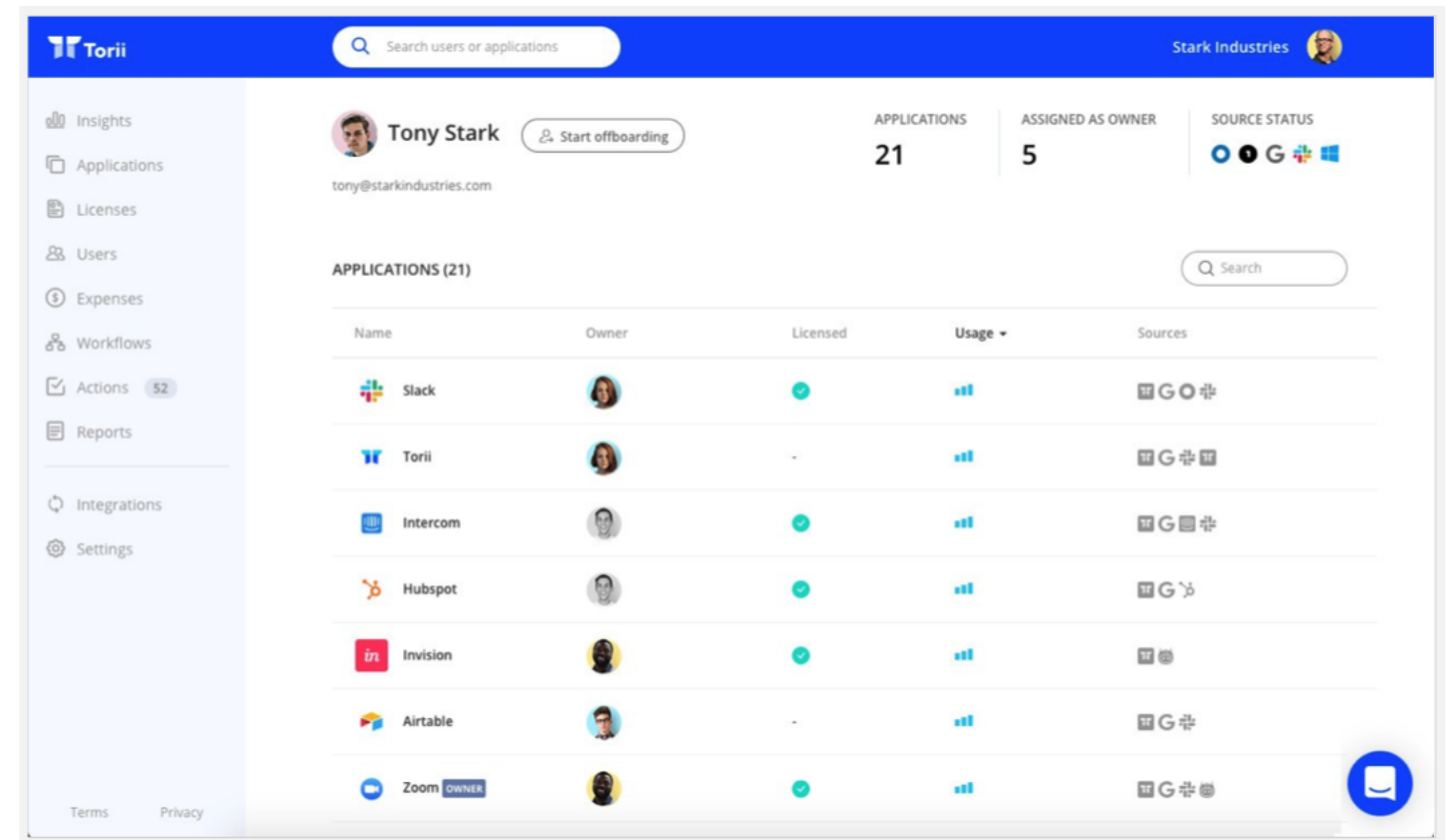


## 2. Close employee SaaS accounts

According to Torii's data, the average employee has access to around 30 different SaaS accounts that should all be closed for security, compliance, and cost-saving reasons.

These include:

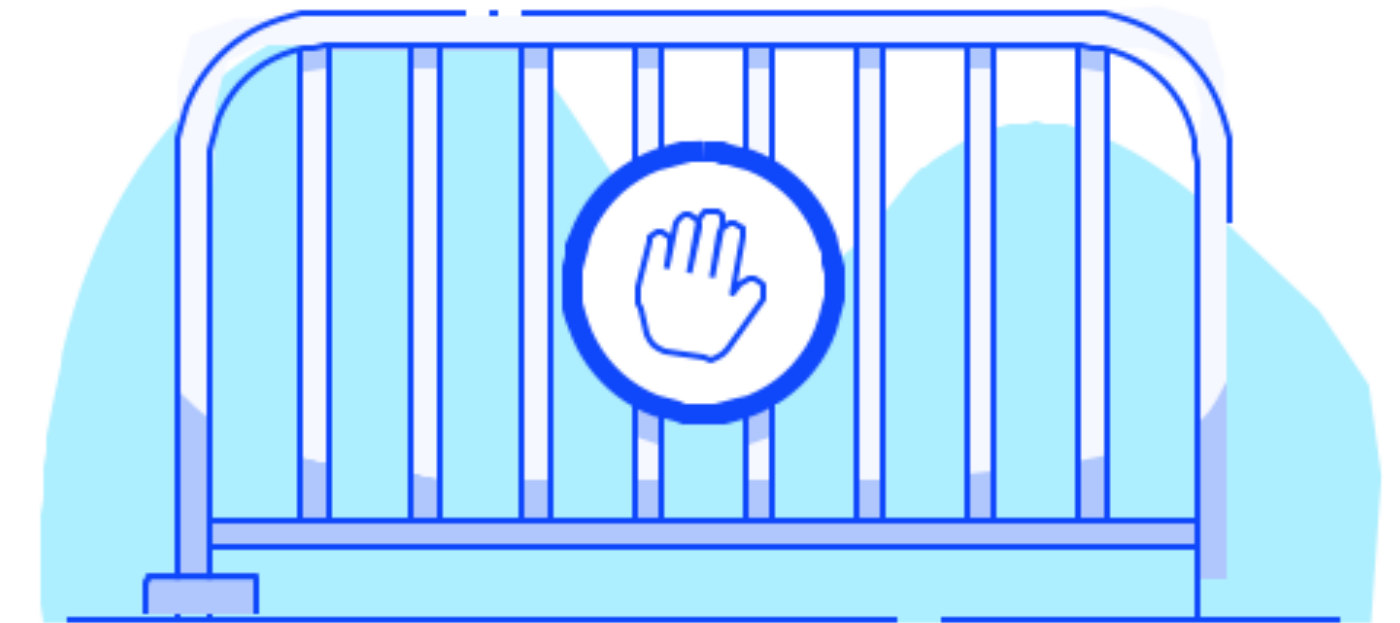
-  SaaS tools for which the employee has an active account
-  SaaS tools the employee has used in the past



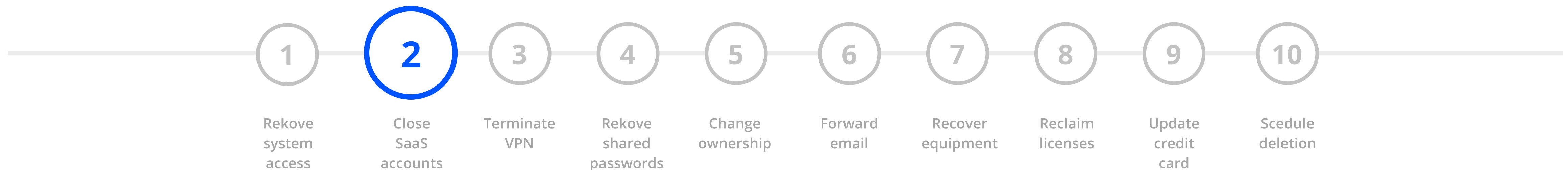
Make sure you also close the accounts of SaaS tools that are behind the SSO login. SaaS vendors are unaware of the fact that you've disabled the account access from the SSO or G Suite.

These means:

- 🖥️ Employee account data still lies with the third-party provider. What happens if the vendor gets hacked? Will they notify you of the data breach of an employee who is no longer with your company?
- 🖥️ Employee sessions might still be valid. While the employee may not be able to perform a new login, a long-running session may leave the account exposed
- 🖥️ A vendor license is probably allocated to the employee and you may still be paying for it
- 🖥️ API (application programmer interface) access tokens might still be valid, leaving the backdoor open without you knowing about it



**Tip:** Remember that revoking G Suite/SSO access is not enough. While it may block the user from accessing the system, it doesn't delete their data on that tool and their account may still occupy a paid license seat.





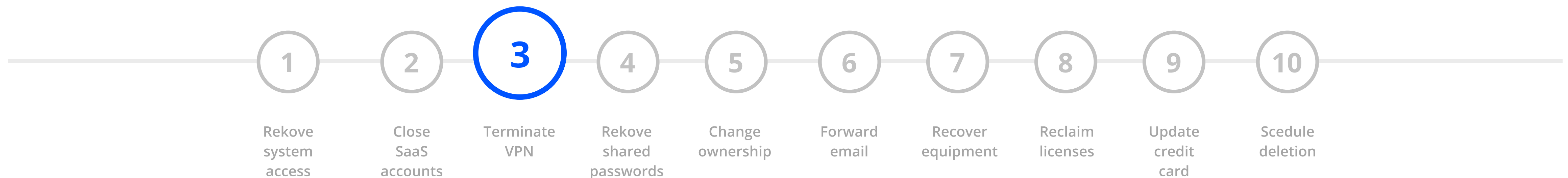
### 3. Terminate VPN and review any remote access methods

It is usual for employees to have remote access to internal or cloud services, whether they work from home or from a satellite office.

Make sure you revoke the former employee's access from all methods of logging into the virtual private network (VPN), remote desktop or any other remote access forms.



**Tip:** It is good practice to review your VPN and remote access logs once in a while, making sure nothing has fallen between the cracks



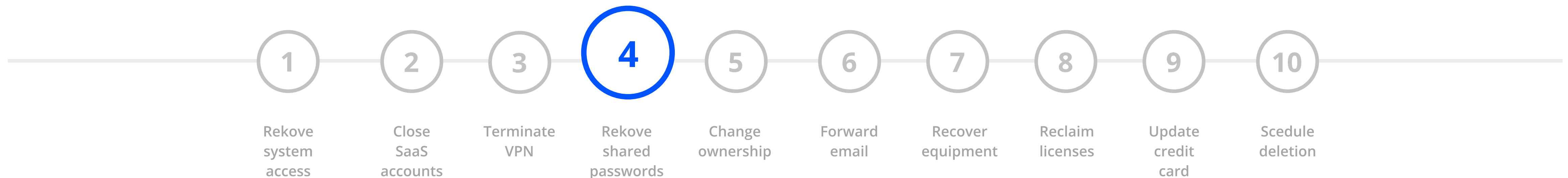
## 4. Change/revoke shared account passwords

Having shared accounts is bad security practice, however, you may have some services where you've created a shared user for several employees. Whether that's a database password, router access or a SaaS shared account, this is a backdoor left open.

In case the departing employee had access to a shared account, you should revoke all existing tokens and sessions and create a new password. This might also be a good time to revisit this shared account and create separate accounts where possible.



**Tip:** Shared accounts are bad security practice and should be avoided. They impose both security and compliance risks..

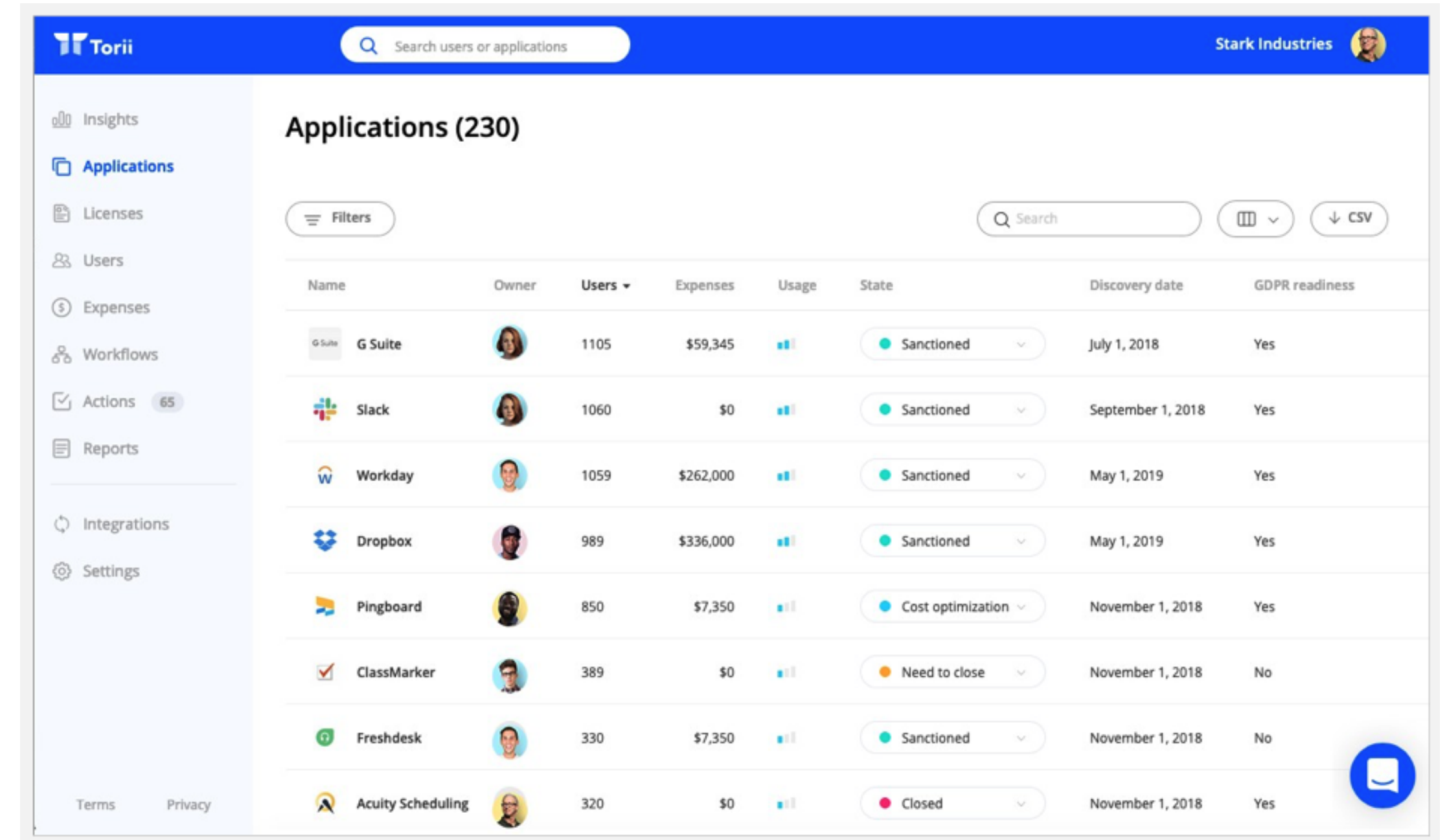


## 5. Change systems ownership

The departing employee might have acted as the system owner of one or more tools. Make sure you have someone else assigned to the role and have the proper system permission to do so.



**Tip:** Keeping a list of system owners is good practice. You should have one go-to person who owns the system. Look at creating additional roles, such as a business owner and budget owners.



Name	Owner	Users	Expenses	Usage	State	Discovery date	GDPR readiness
G Suite		1105	\$59,345		Sanctioned	July 1, 2018	Yes
Slack		1060	\$0		Sanctioned	September 1, 2018	Yes
Workday		1059	\$262,000		Sanctioned	May 1, 2019	Yes
Dropbox		989	\$336,000		Sanctioned	May 1, 2019	Yes
Pingboard		850	\$7,350		Cost optimization	November 1, 2018	Yes
ClassMarker		389	\$0		Need to close	November 1, 2018	No
Freshdesk		330	\$7,350		Sanctioned	November 1, 2018	No
Acuity Scheduling		320	\$0		Closed	November 1, 2018	Yes

1

Revoke  
system  
access

2

Close  
SaaS  
accounts

3

Terminate  
VPN

4

Revoke  
shared  
passwords

5

Change  
ownership

6

Forward  
email

7

Recover  
equipment

8

Reclaim  
licenses

9

Update  
credit  
card

10

Schedule  
deletion



## 6. Forward former employee's emails

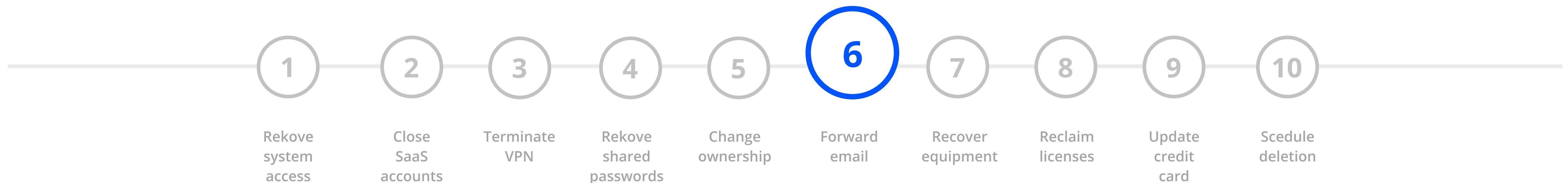
To ensure business continuity, it is important to forward the emails of the departing employee to a colleague or a manager, at least temporarily. You should probably do this when you disable the employee's G Suite or Office 365 email account.

It is good practice to create an automatic reply on behalf of the departing employee, letting the sender know that their email will be addressed by a new employee.

This is especially important for employees who were the single point of contact with a customer or a supplier.



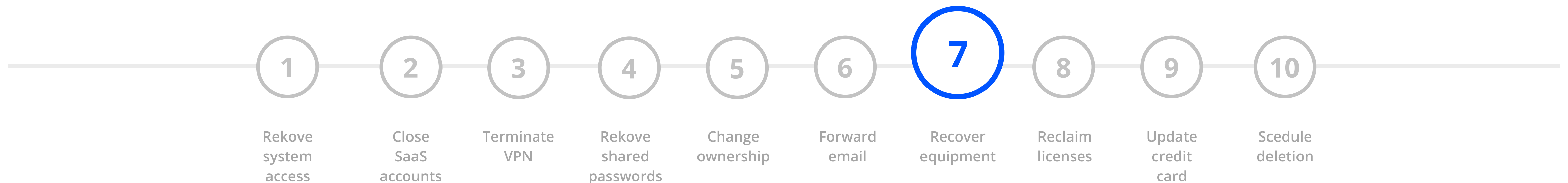
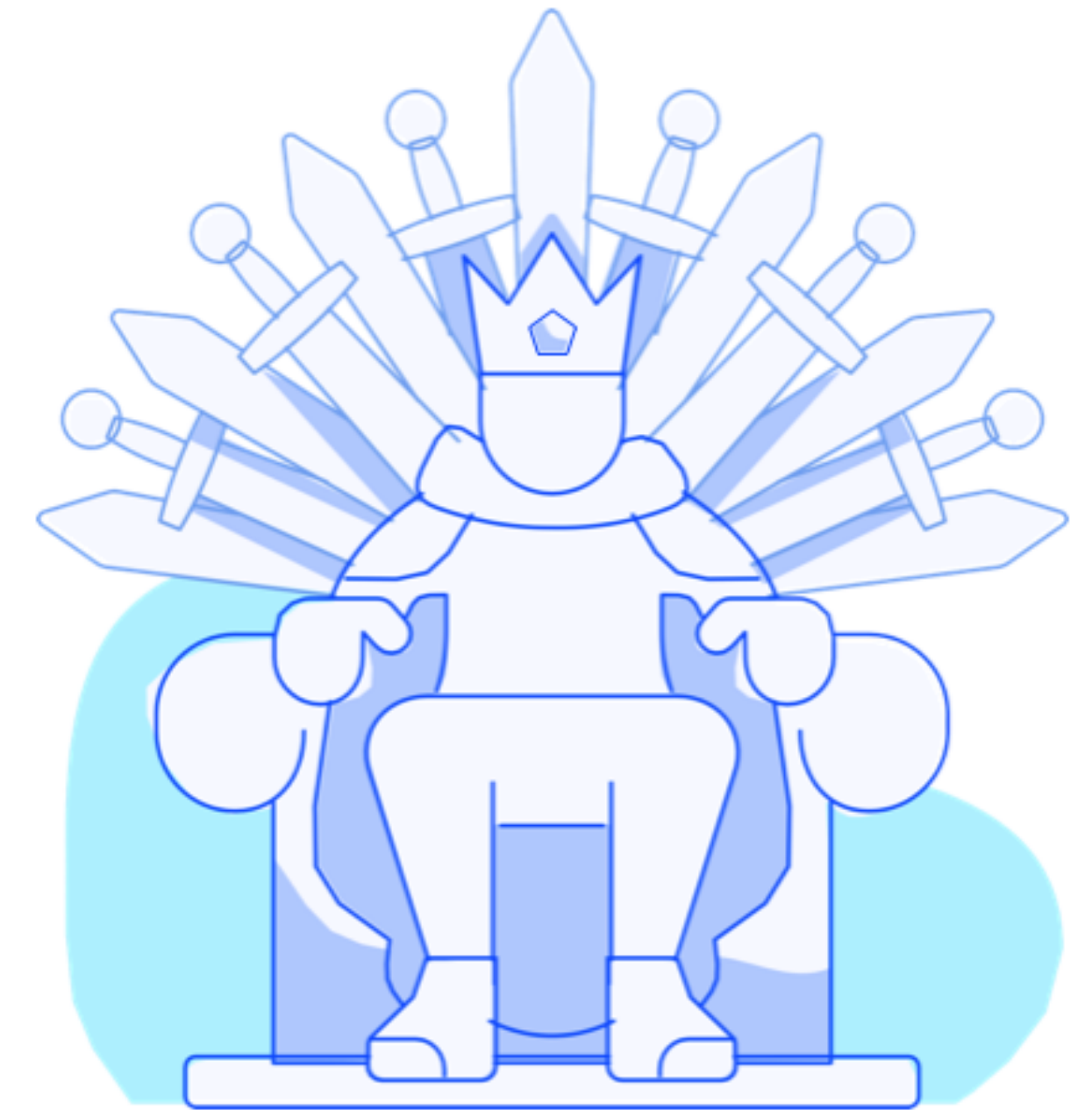
**Tip:** When thinking about single-point-of-contact employees, look beyond forwarding solely managers or sales executives' emails. Remember that in today's SaaS era, many individual contributors in various departments might have signed up for a SaaS tool. An important email from a vendor might be lost unless you create a forward rule for all employees once they leave.



## 7. Recover company equipment and assets

It may appear obvious, but without an updated and comprehensive company asset register, company property might get lost. Keeping updated inventory of company assets used by each employee is good practice and checking these assets when the employee leaves is a must.

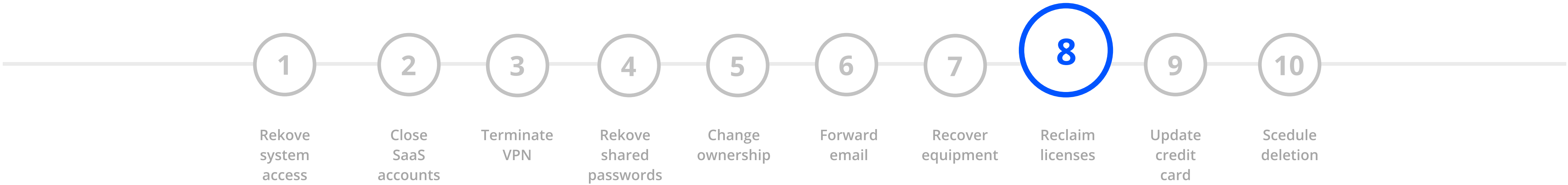
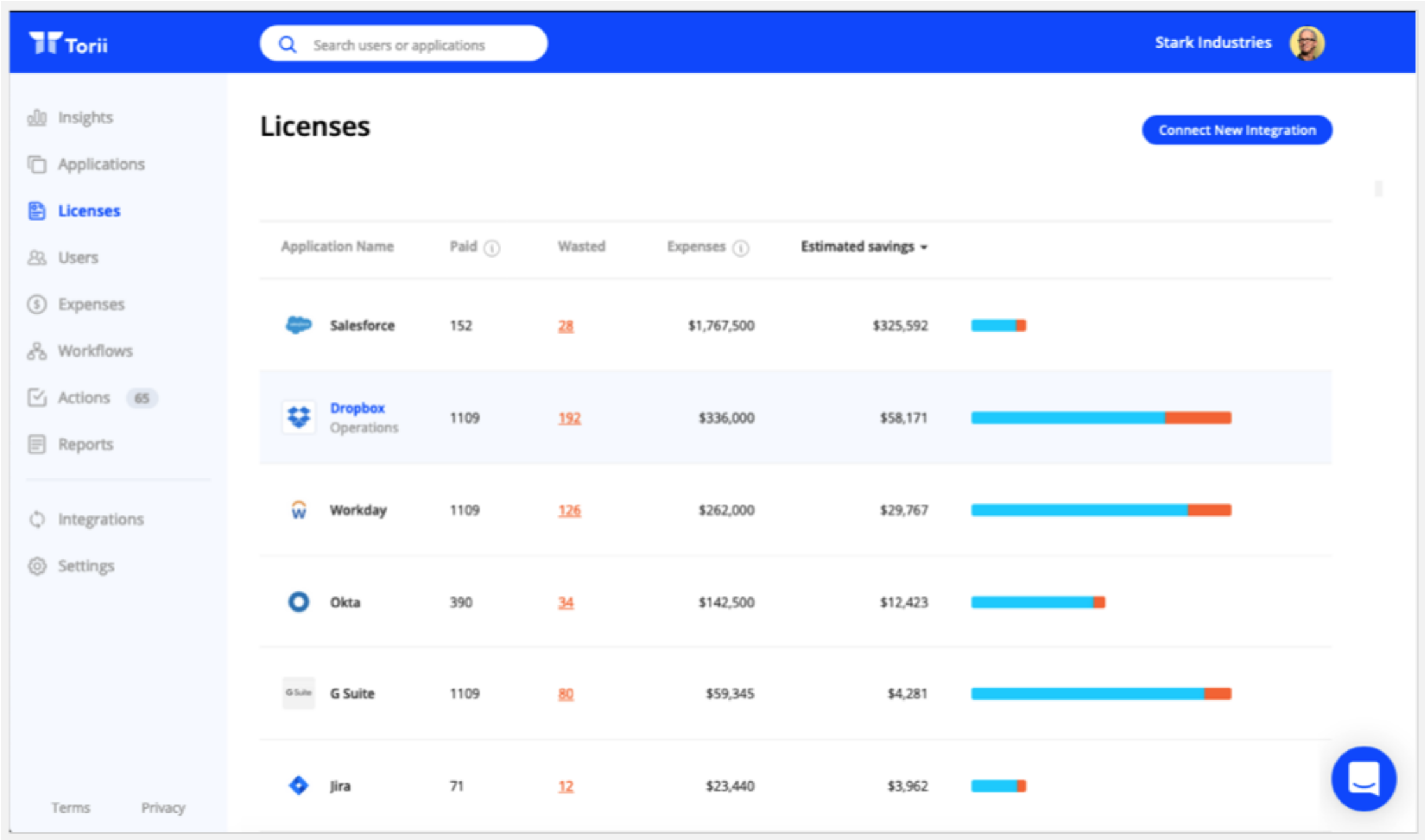
Recover all company property from the departing employee, including laptop, cell phone, peripheral devices, office keys, access cards, etc.



## 8. Reclaim employee licenses

Some SaaS applications offer a fair billing policy, while others may continue to charge for accounts that are left open, including employees that are no longer with the company. Our research finds that the total cost of wasted licenses can be around 30% of your total SaaS license cost.

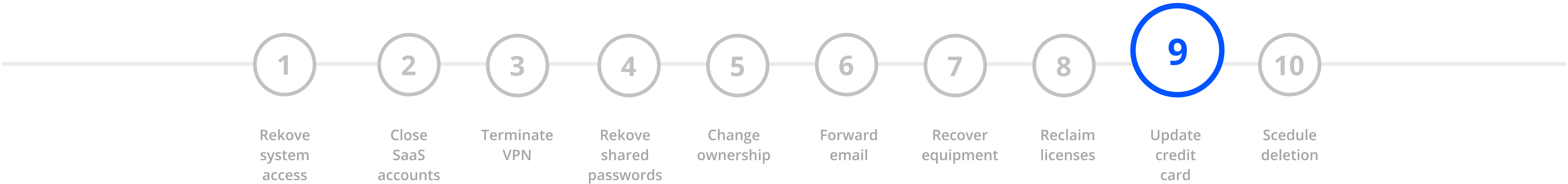
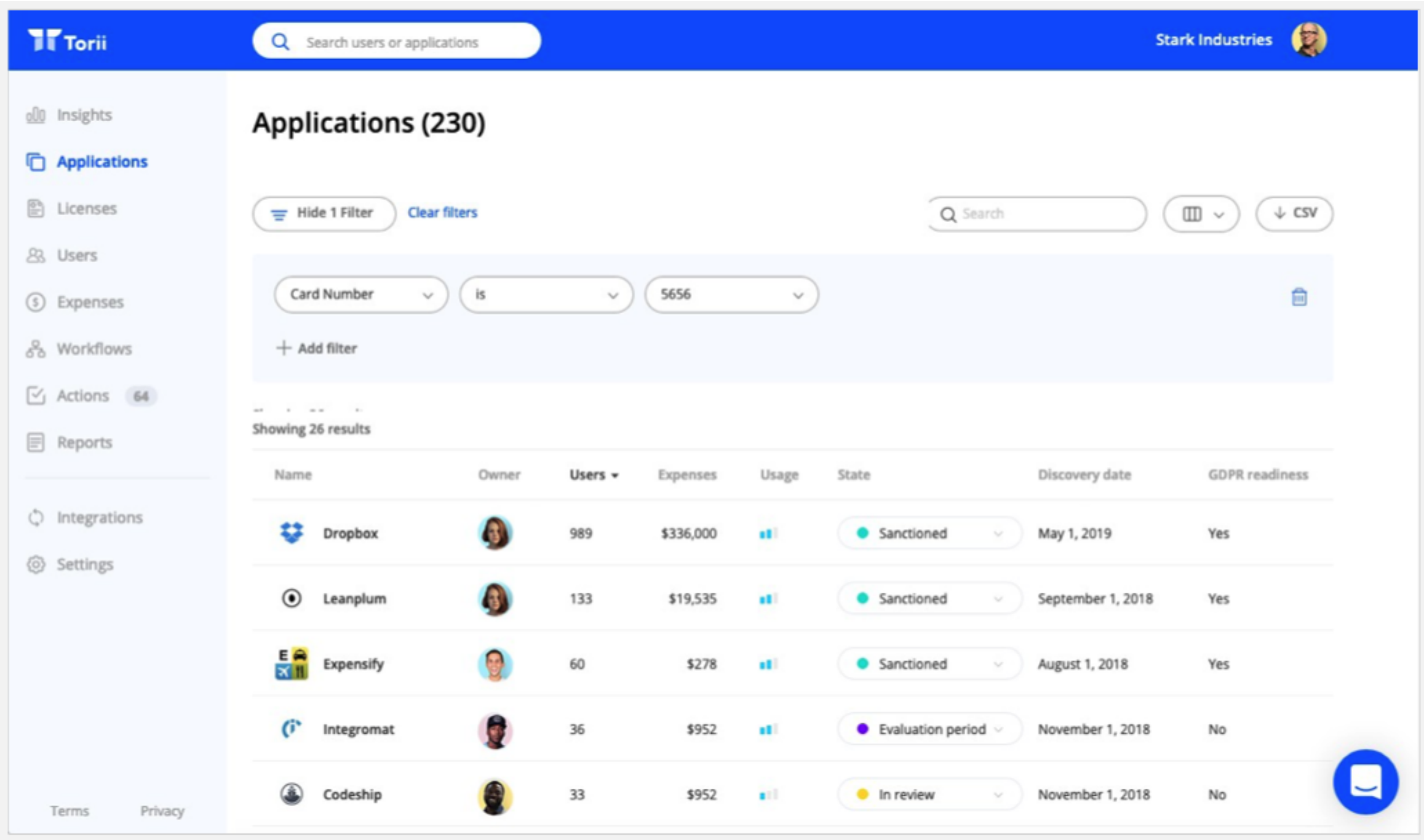
To save costs, make sure you reclaim the SaaS licenses of departing employees. Pay attention to the different license models of the various providers. With many tools, you keep paying for disabled/suspended accounts as if they were active accounts. Usually only removing the account will actually stop the license cost charges.



# 9. Update credit card payments

Charging your credit card is very common with SaaS applications. Your finance department will revoke the corporate card held by a departing employee, but how would you know for which SaaS applications this card has been paying?

Keeping an up-to-date list that matches the credit cards and their SaaS apps billing records is critical if you would like to ensure business continuity. Once you have this list in place, you need to make sure you regularly update new cards and apps on the list. Failing to do so might result in the vendor blocking access to the service or limiting its functionality.



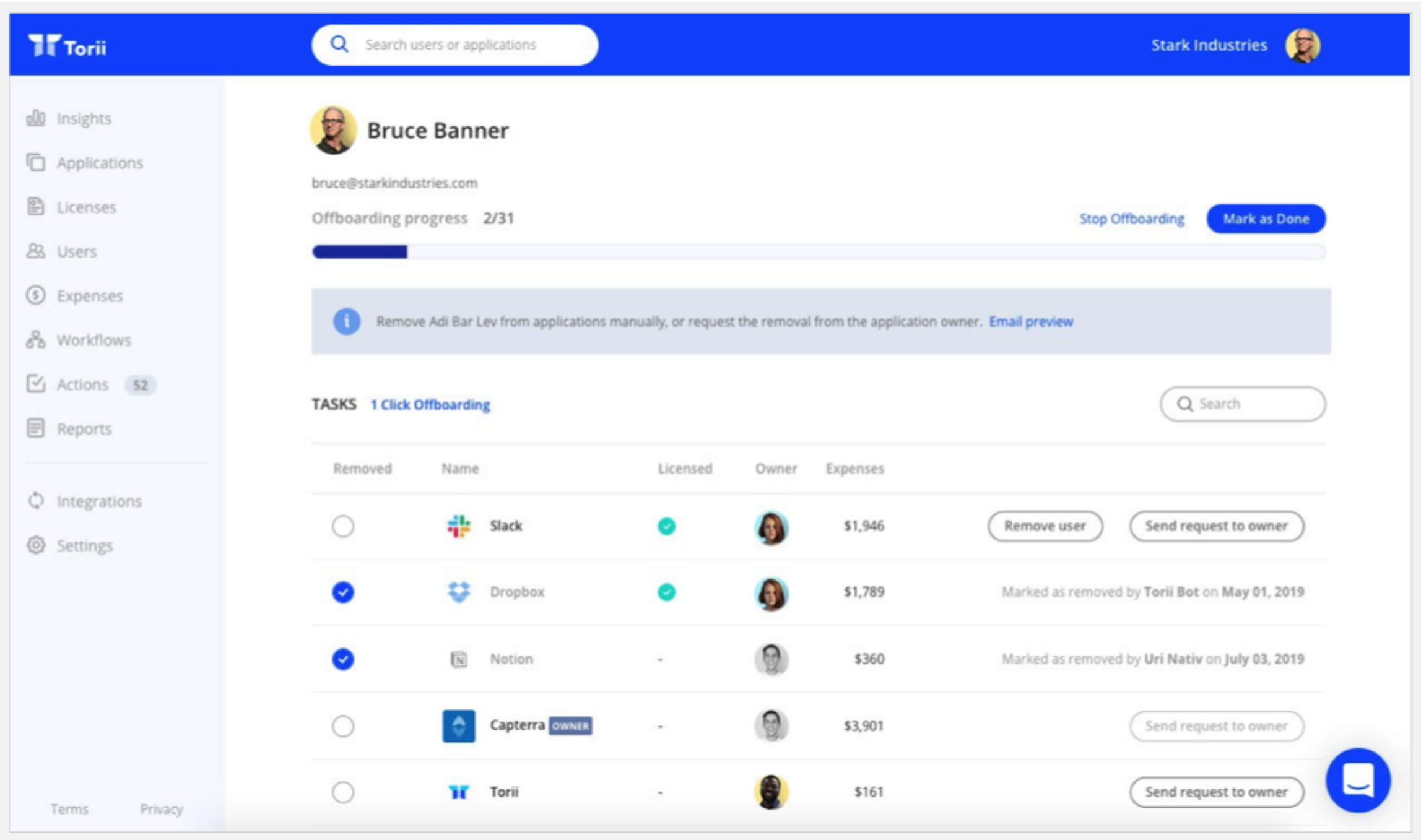


# 10. Schedule account deletion for suspended accounts

With many services such as Salesforce, G Suite, Dropbox, and others, you have the ability to suspend or disable the user before deleting it. This allows you to disable the departing employee’s access to a certain account without losing important corporate data.

While this is good practice, it is easy to forget to review those accounts and delete them once the data has been transferred.

Make sure you install a good process to revisit suspended accounts after a fixed period of time to delete them.



## Bottom line

A smooth employee exit is just as important as a great start for both the departing employee and for the company. Formalizing the offboarding process not only mitigates legal and security threats, but also ensures that employee's departure causes minimal disruption. The proliferation of SaaS tools has made the employee's offboarding task considerably more difficult.

Follow checklist to keep your operation smooth and the organization secure and compliant; Keeping all employees' SaaS licenses under control makes sure money is not wasted.

Need help with employee offboarding?

Give Torii a try!



- 1 Revoke system access from IdP and SSO
- 2 Close employee SaaS accounts
- 3 Terminate VPN and review any remote access methods
- 4 Change/revoke shared account's passwords
- 5 Change system's ownership
- 6 Forward employee's email address
- 7 Recover company equipment and assets
- 8 Reclaim employee licenses
- 9 Update credit card payments
- 10 Schedule account deletion for suspended accounts.