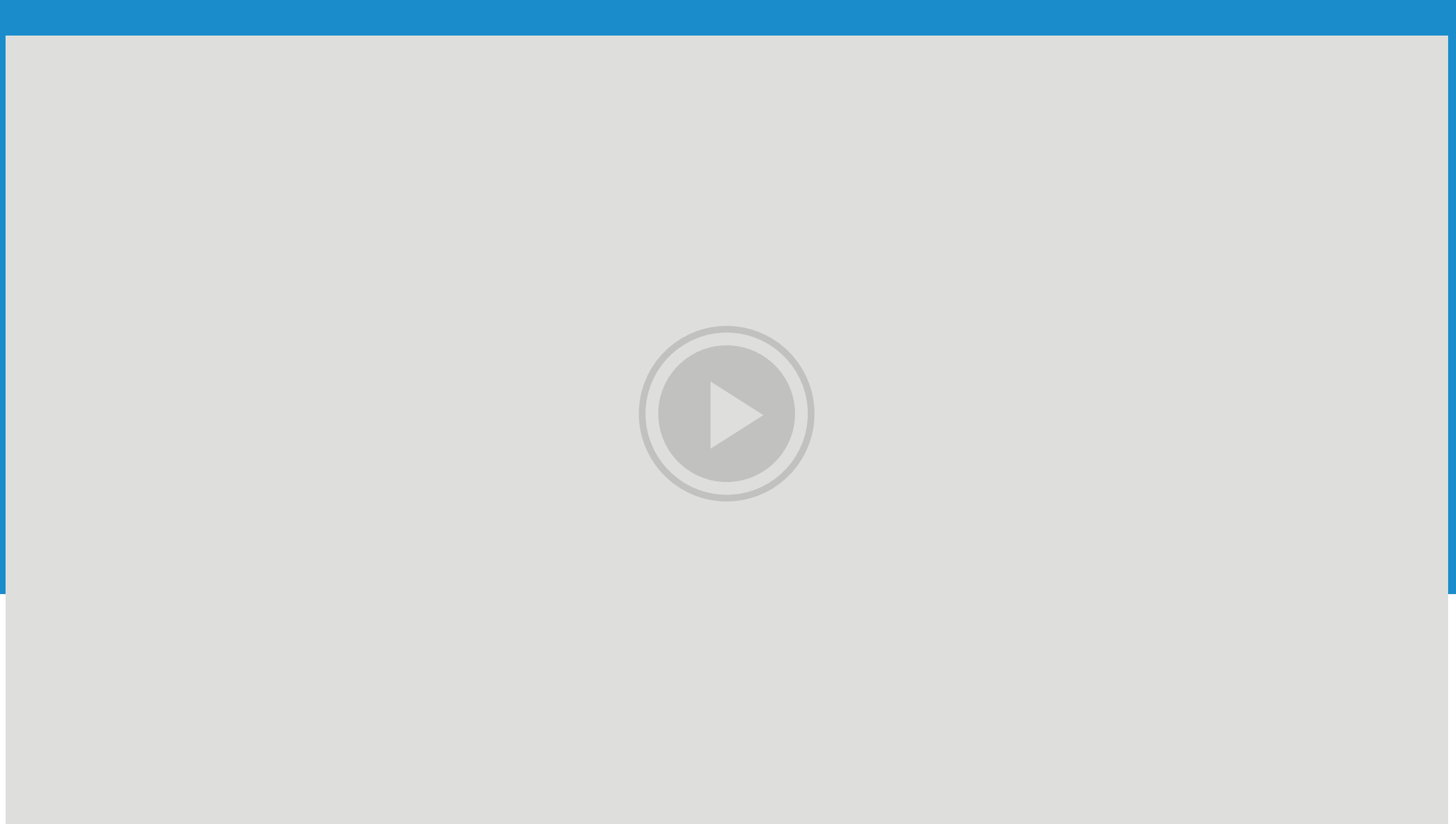
The Ex-Employee Menace

Intermediaʼs 2014 SMB Rogue Access Study explains why your former coworkers could be your next great security threat.



Share our Rogue access video!

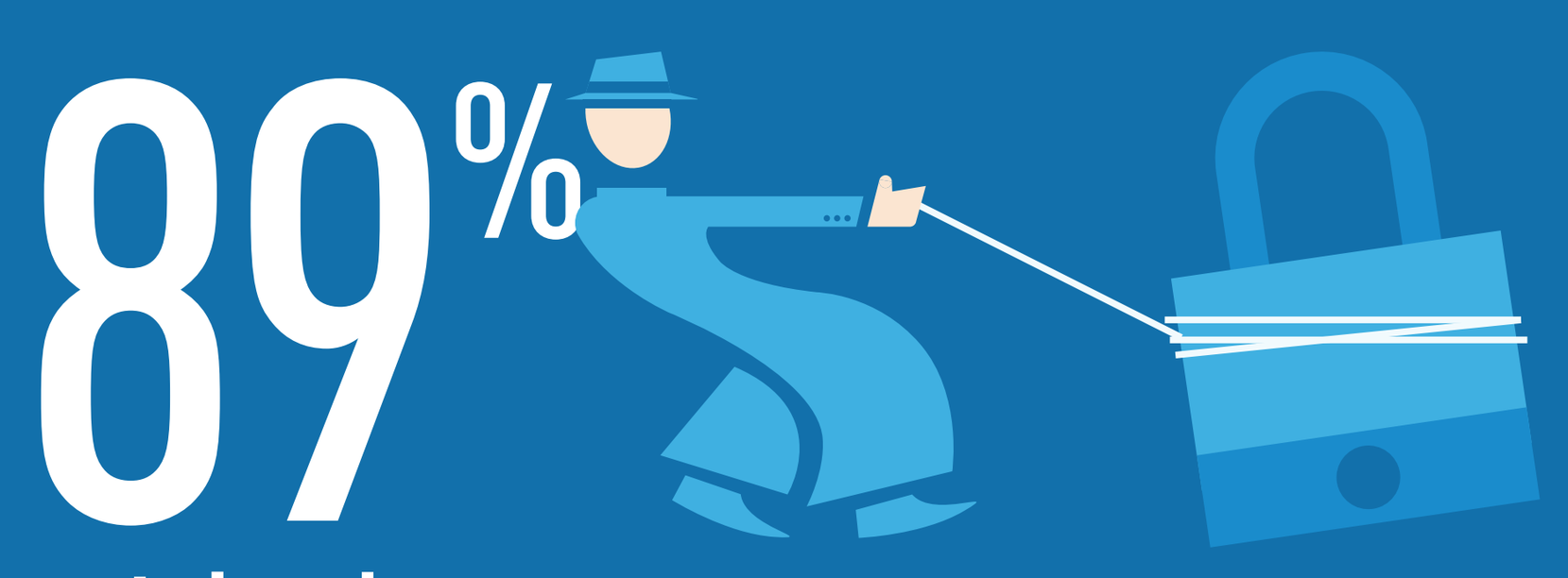
194

On August 12, 2014, the Bureau of Labor Statistics released its latest Job Openings and Labor Turnover Survey. It found that XXX,000 people in Professional and Business Services industry left their jobs in June, 2014.

The question is: what kind of IT access did those XXX,000 peo le take with them? Confidential files in their personal Dropbox, for example? Access to leads in Salesforce? Logins for corporate Twitter accounts? Passwords for Quickbooks or Paypal?

Intermedia and Osterman Research teamed to up to quantify the scope of the problem. **What we learned should be a wake-up call for every business in the country.**

Ex-employees are walking away with their passwords.

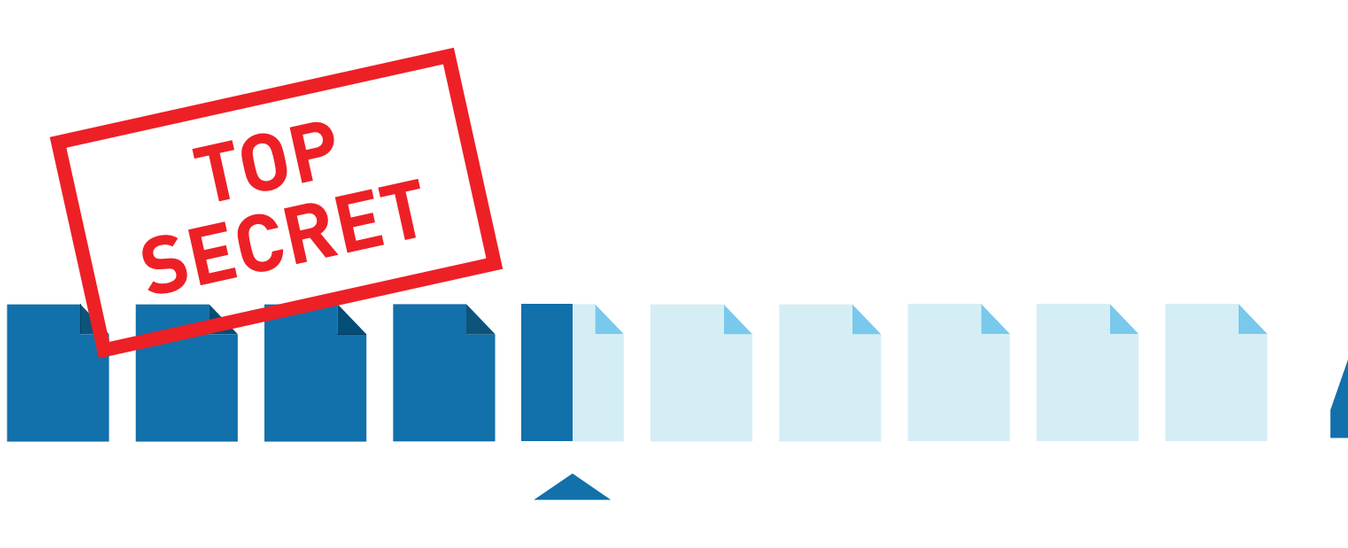


89%

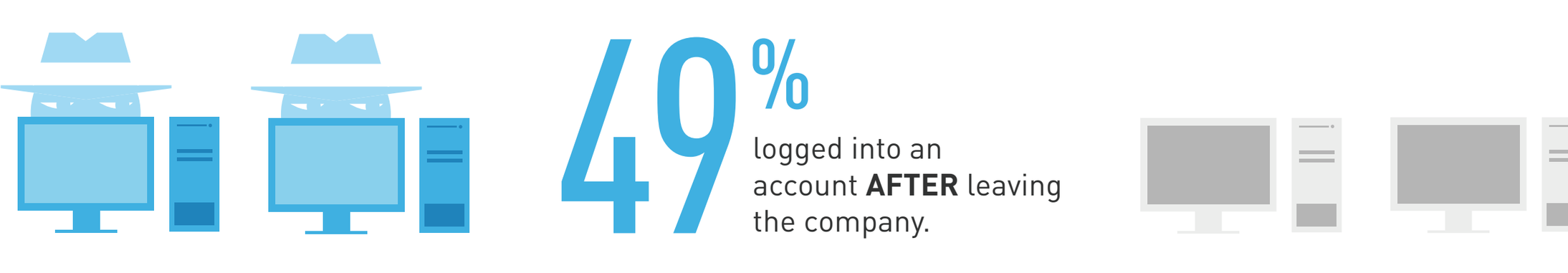
retained access

to Salesforce, PayPal, email, SharePoint, Facebook and other sensitive corporate applications.

89% of the survey respondents retained access—that is, their login and password—to at least one application from a former employer. They named nearly every major app you can think of: Basecamp, Shopify, Desk.com, Office 365, Google Apps, MailChimp, Wordpress, and many more.



45% retained access to “confidential” or “highly confidential” data



49% logged into an account **AFTER** leaving the company.

> “Users continue to have access to a wide range of accounts, IT services and platforms that they used when working for a previous employer. For example, 24% of users still have access to a PayPal account they used when working for a previous company, 21% have access to Facebook and 18% have access to LinkedIn.”
>
> — Osterman Research, “Do Ex-Employees Still Have Access to Your Corporate Data?”, August 2014

Maybe your exit interview is missing something?

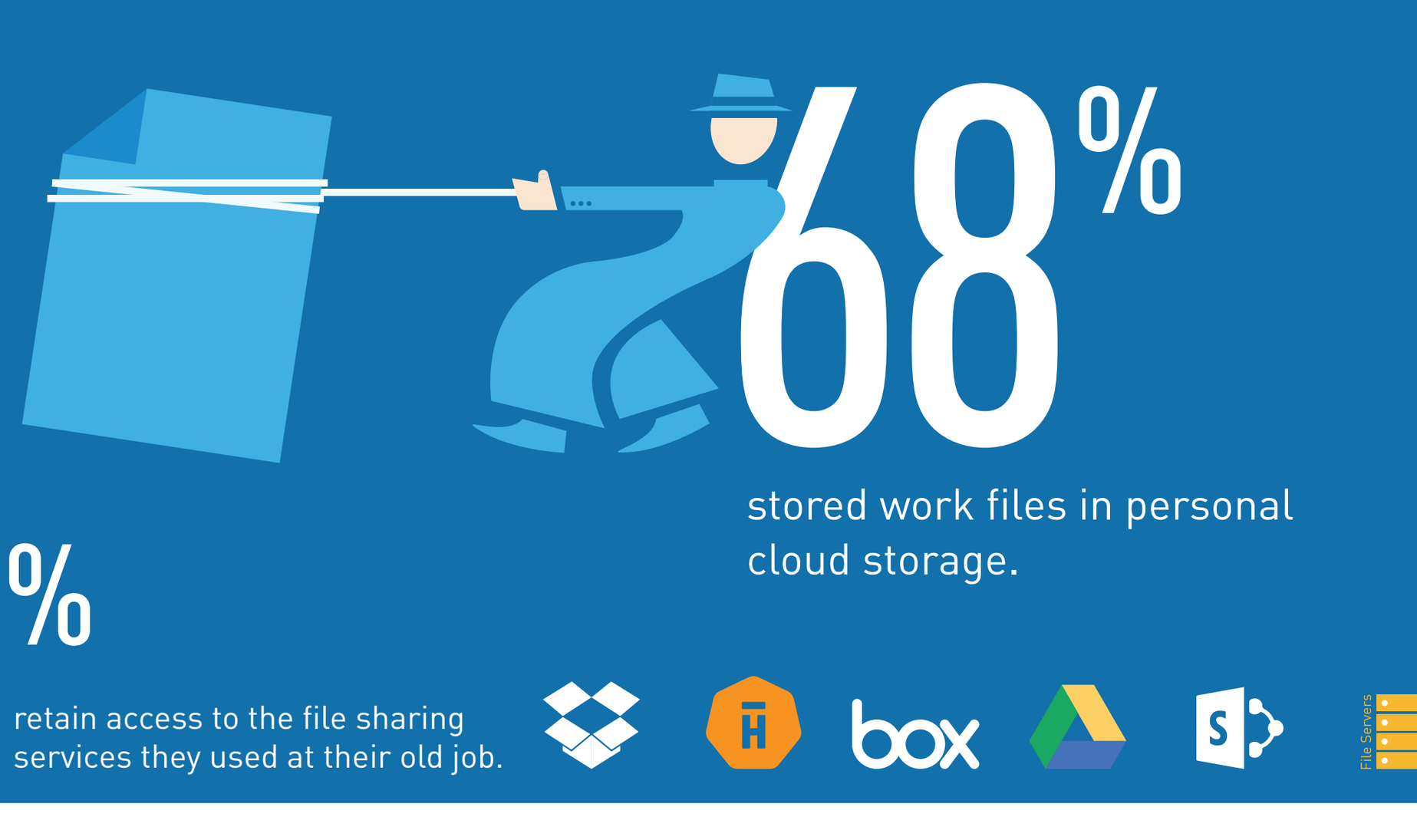
60% of respondents were **NOT** asked for their cloud logins when they left their companies

Itʼs not surprising that cloud apps are falling through the cracks during the employee offboarding process. In many companies, the responsibility for provisioning apps falls to different departments: email is provisioned by IT, payroll apps are provisioned by HR, and line-of-business apps are provisioned by department managers.

With this approach, there is no clear responsibility for decommissioning and deprovisioning. The result: rampant rogue access.

> “Employers should do something that most of them are not doing: ask departing employees, as well as those who are staying with the organization, for the login credentials to all of the repositories that might contain corporate data. This might seem like an obvious thing for employers to do, but they are not doing it and should be.”
>
> — Osterman Research, “Do Ex-Employees Still Have Access to Your Corporate Data?”, August 2014

Ex-employees are also walking away with your files.



68% stored work files in personal cloud storage.

88% retain access to the file sharing services they used at their old job.

Youʼve probably heard of BYOS/BYOA: Bring Your Own Service/App. Itʼs the sequel to the Bring Your Own Device trend. Except with BYOS/BYOA, employees arenʼt just using their own phones or laptops—theyʼre creating project plans in Google Docs. Or using SurveyMonkey instead of the corporate Qualtrics account. Or spinning up AWS servers because thereʼs too much red tape inside the corporate datacenter.

This may make users more productive, but it introduces huge security holes. Because if IT doesnʼt know the where the companyʼs data is, how can it control what ex-employees can access?

Personal file sync and share services are probably the worst offenders. Whatʼs the likelihood that IT will wipe corporate files stored in a personal Dropbox or Google Docs account?

> “File sync and share tools are widely used in organizations of all sizes, and most of these tools are deployed by individuals independently of any sort of ʻblessingʼ from their IT department.”
>
> — Osterman Research, “Do Ex-Employees Still Have Access to Your Corporate Data?”, August 2014

What kind of risks does this “rogue access” create?

- **Stolen secrets.** An ex-employee could bring account and billing data to your competitors. Or they could use your product plans to beat you to market.
- **Lost data.** One day, an ex-employees casually purges her personal cloud storage accounts—and suddenly youʼve lost the only copy of all their work.
- **Regulatory compliance failures.** Many regulations obligate you to protect sensitive or confidential data. How can you be in compliance if ex-employees can still enter your systems?
- **Data breaches.** Forty-six of the states require you to notify parties whose data has been breached. Does “rogue access” constitute a breach?
- **eDiscovery risks.** Can you satisfy an eDiscovery order if you donʼt have full and ready access to all of your discoverable data—such as those stored on ex-employeesʼ personal accounts?
- **Out-and-out sabotage.** Imagine what a disgruntled ex-employee could do with access to your social media reputation. Or the price settings on your ecommerce site. Or the leads in your CRM.
- **Hacker field days.** What if the bad guys nab an ex-employeeʼs device—with all the passwords to your systems stored in plain text?

BEFORE you read about the three methods to prevent rouge access, thereʼs an even more important step you should take: educating your coworkers. Awareness of the Rogue Access issue translates directly into prevention.

Share this report with your IT and HR managers

194

There are three methods for preventing rogue access.

1. Implement rigorous access management and IT offboarding processes.

To successfully manage user access during employment—and revoke it when they leave—your business needs to build processes around best practices for managing employee access to IT services. It also needs a rigorous IT offboarding checklist for departing employees.

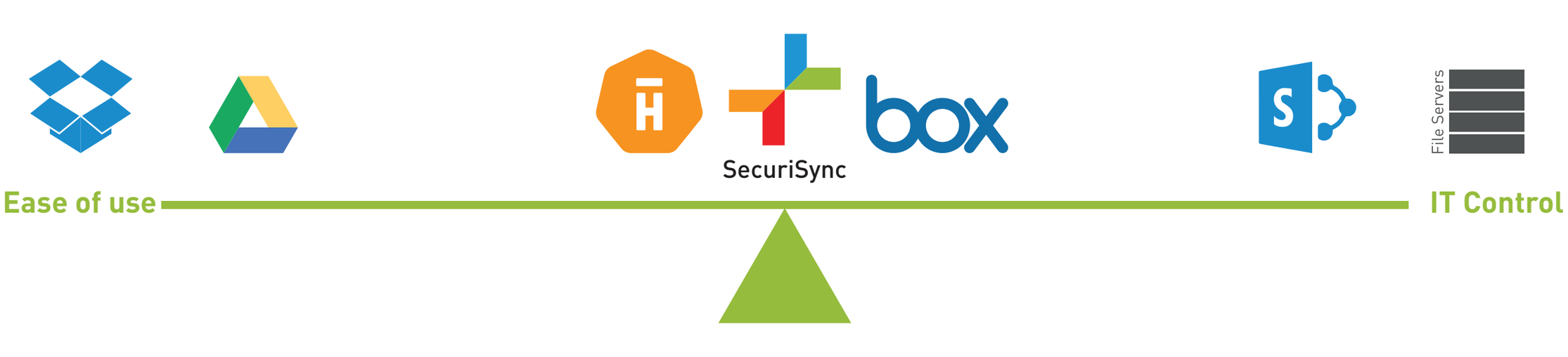
Good news: weʼve drafted these documents for you. (You can download them at the end of our report.) Our templates include guidelines for setting up internal processes as well as specific actions to take when onboarding and offboarding employees. In addition, they include recommendations specific to regulated industries such as financial services, legal services and healthcare.

2. Deploy a business-grade cloud storage service thatʼs better than personal services.

Users want to access and share their files across multiple devices and collaborators. Personal services like Dropbox or Google Docs make that absolutely simple. If your corporate tools require even marginally more effort—even if itʼs just logging in to the VPN—then people will naturally gravitate to the simpler solution.

Thatʼs why you have to provide an alternative thatʼs just as easy to use but still gives IT full control over access privileges. (We, of course, recommend Intermediaʼs SecuriSync.)

Find the balance to mitigate access leaks



3. Deploy a business-grade cloud storage service thatʼs better than personal services.

A single sign-on (SSO) portal is a service that gives employees access to all their apps with just one password. For users, itʼs as simple to use as the good-old “Start” menu: once youʼre logged in, you click on the app youʼre looking for and it launches immediately. No need to hunt for login pages or password hints.

SSO portals are increasingly popular for helping users be more productive in the face of a sprawling cloud footprint. (In Intermediaʼs previous report, Death by 1,000 Cloud Apps, we talked a lot more about the challenges posed when there are too many apps.)

An SSO portal alone canʼt stop Rogue Access. But it CAN make leaks less likely.

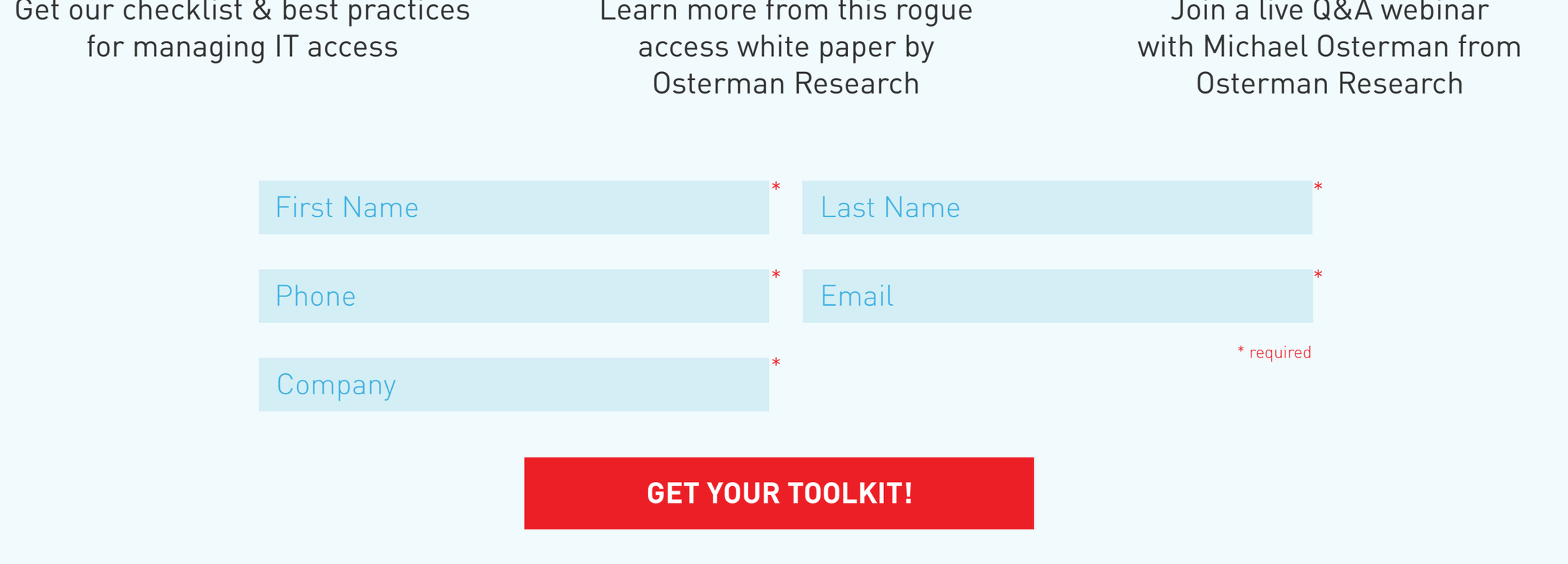
Users can be deprovisioned in a single click.
This on its own does not eliminate Rogue Access. But it makes it harder for a departing employee to retain access or cause mischief.

Users are less likely to remember their passwords.
An SSO user only types in a password when setting up an app or when the app requires a password reset. This less likely that the SSO user will remember his or her password.

IT admins can see what apps an employee is using. Many security holes are introduced when employees use apps without ITʼs knowledge. With an SSO portal, IT can review the logins saved by a departing employee to spot any unknown services and flag them for deprovisioning.

The safest password? No password at all.
Some SSO services let admins provision apps without users ever knowing their password. This is one of the most effective tool an SSO portal provides to prevent Rogue Access. (Itʼs currently available with Intermedia AppID Enterprise, and coming soon to Intermedia AppID.)

Download this toolkit to eliminate Rogue Access in your business.



Get our checklist & best practices for managing IT access + Learn more from this rogue access white paper by Osterman Research + Join a live Q&A webinar with Michael Osterman from Osterman Research

First Name * Last Name *

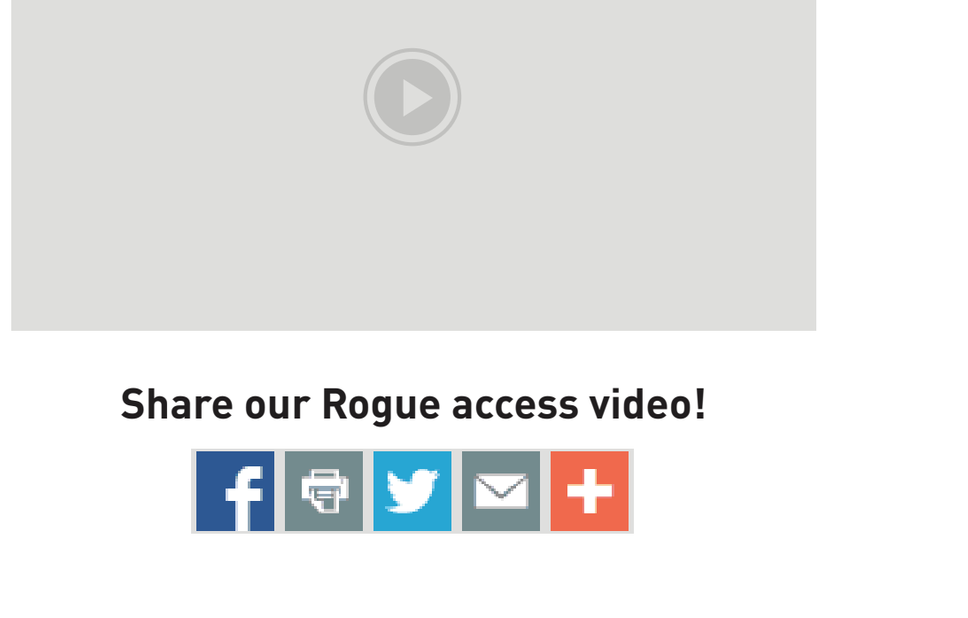
Phone * Email *

Company * * required

GET YOUR TOOLKIT!

Need more ideas for stopping Rogue Access?

Follow @intermedia_net or join the conversation at #StopRogueAccess.



Share our Rogue access video!

Share our Rogue Access infographic!

About Intermedia
Intermediaʼs Office in the Cloud suite of cloud IT services are fully integrated, secure and mobile. Theyʼre all managed through our central HostPilot control panel. Services include email, phones, file sync and share, single sign-on, security, mobility, archiving and more. Our services thwart the ex-employee menace by making it simple to revoke access to the entire cloud footprint with just one click. Learn more about Intermedia >>

Deploy Intermediaʼs business-grade file sync and share. SecuriSync by Intermedia offeres simple, easy-to-use cloud file sharing thatʼs secured by industry-leading access control and protection. Learn more about SecuriSync >>

Deploy Intermediaʼs Single Sign-On Portal. Intermedia AppID is the only single sign-on solution designed specifically for SMBs—including deployment that doesnʼt require consultants to execute. Learn more about AppID >>

Sources: Osterman Research. (August 2014). Do Ex-Employees Still Have Access to Your Corporate Data?
Bureau of Labor Statistics. (August 2014). Job Openings and Labor Turnover Survey.