

# Hiding in plain sight

How secrets (mis)management is creating the next big cybersecurity threat



# Four out of five IT and DevOps companies are not managing their secrets well, and it's leaving them vulnerable to attack.

The pace of software delivery is constantly increasing, thanks to new technologies like cloud services, microservices, continuous integration/continuous deployment (CI/CD), and DevOps. Together, these technologies have the intended effect of speeding up delivery cycles.

In pursuit of these accelerated timelines, developers are often forced to choose between speed and security. They leave infrastructure secrets like API tokens, SSH keys, and private certificates in config files or next to source code for easy access. Of course, the easier it is for developers to access these secrets, the easier it is for attackers to access them, too.

New 1Password research\* sheds light on the severity and pervasiveness of the problem. We asked 500 IT and DevOps companies about how they handle the secrets that power their digital infrastructure. What we learned is that, while companies are mostly aware of the problem, few are close to solving it.

Around 80% of companies surveyed admit to not managing their secrets well, and 52% of IT and DevOps workers say that the explosion of cloud applications has made managing secrets more difficult. Lacking a dedicated secrets management solution or framework, they're left to deal with secrets in a haphazard, ad hoc manner – spending about 25 minutes per day on secrets management alone, at a collective cost of \$8.5 billion per year.

But the greater threat is the increasing danger of a breach. 60% of companies surveyed have experienced secrets leakage of some kind, and more than three in four IT and DevOps workers still have access to their former employer's infrastructure secrets. It's a secrets management wild west, and it's going to take a mindset shift to correct the course.

*\*1Password conducted this research using an online survey among 500 adults in the United States who work full-time in their company's IT department or in a DevOps role at a company with more than 500 employees. Data was collected from April 8 to April 21, 2021.*



80%

of IT/DevOps organizations admit to not managing their secrets well

77%

of IT/DevOps workers still have access to their former employer's infrastructure secrets.

60%

of IT/DevOps organizations have experienced secrets leakage.

52%

of IT/DevOps workers say that the explosion of cloud applications has made managing secrets more difficult.

## The state of secret sprawl

One in four companies surveyed have secrets located in **10 or more different locations**. Worse, 50% of individual contributors in IT or DevOps roles say they don't know how many different locations their secrets could be found in, as there's too many to count.

The numbers may be alarming, but the causes are to be expected. Machine secrets fall in a digital no man's land. IT has traditionally been tasked with maintaining human secrets (passwords). The API token that developers need to access a database usually falls outside of IT's responsibilities.

And as we've seen, DevOps often have to compromise security for speed, so they leave secrets in places that are easily accessible to them – and also to attackers. In short, neither IT nor DevOps are well-positioned or properly incentivized to safeguard infrastructure secrets.

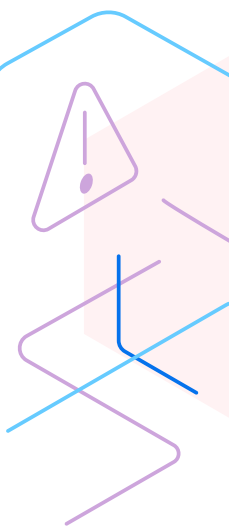
And lacking the tools to manage secrets properly, they're forced to deal with problems as they arise and the interruptions add up.

## The productivity drain

Around 66% of IT and DevOps leadership (VP and above) and 63% of team leads and managers say they're interrupted at least daily to find a secret or manage their company's secrets. 21% of IT/DevOps workers say that their workflow is disrupted to find a secret or manage company secrets at least 4 times a day, on average.

For many, it's the worst part of their workday.

## Managing secrets is the worst part of the workday



**30%**

of IT/DevOps team leads and managers say that managing secrets is the worst part of their workday.

**27%**

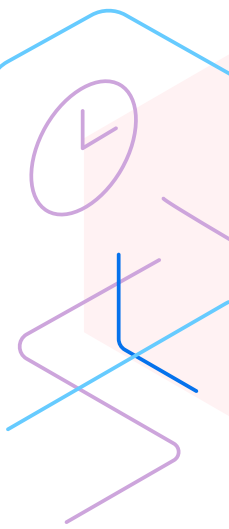
of VPs and above say that managing secrets is the worst part of their workday.

**26%**

1 in 4 IT/DevOps say that managing secrets is the worst part of their workday.

On average, IT and DevOps workers spend 25 minutes per day managing secrets, and the numbers are growing. Nearly two-thirds (66%) of IT and DevOps leadership say they spent more time than ever managing secrets last year.

## Lost time



**39%** of IT/DevOps workers spend 30 minutes or more a day on average managing enterprise secrets.

Half (**51%**) of IT/DevOps workers say their time spent managing secrets has increased in the last year, and for 10% it's more than doubled.

**60%** of IT/DevOps startup workers say that their time spent managing secrets has increased in the last year.

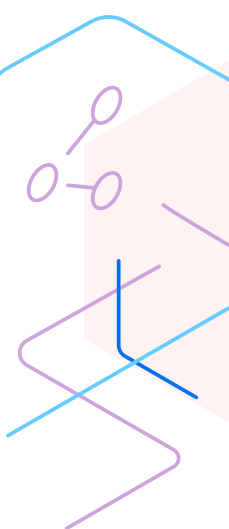
IT/DevOps VP and above are the most likely to admit to delays on projects due to poor secret management (**75%**), compared to team leads and managers (**60%**), and individual contributors (**52%**).

Delays are par for the course, too. Around 61% of projects are delayed due to poor secret management. And of the IT/DevOps organizations who report a product or feature delay due to secrets leakage, 55% say the delay cost them a month or more.

## The workaround problem

As we stated earlier, 80% of IT and DevOps organizations admit to not managing secrets well. In other words, they're well aware of the problem. But without a mechanism to handle secrets properly, they're forced to resort to unsanctioned, ad hoc, and risky workarounds.

## How (not) to share secrets



Nearly half (**48%**) of companies use a shared document or spreadsheet, whether having restricted access or not, to store and manage enterprise secrets.

**59%** of IT/DevOps workers have used email to share enterprise secrets with colleagues, followed by chat services (**40%**), shared documents/spreadsheets (**36%**) and text message (**26%**).

## Reusing secrets: everybody's doing it

Despite the well-known dangers of reusing secrets, workers are often left with little choice. And a bit counterintuitively, VPs and above are more than twice as likely to say they've reused secrets.

	VP and above	Team leads and managers	Individual contributors
Used the same secrets in production as I do in testing and staging environments.	64%	54%	23%
Reused secrets between projects	81%	65%	39%

## What's the cost?

With enterprise password managers becoming more common and secret sprawl growing, attackers were already beginning to turn their attention away from individuals to focus on businesses. For a long time, targeting the enterprise was too much effort for too little chance of a payoff.

But poor secrets management is making it easier for attackers to find their way in. And once they get in, the payoffs are larger than ever. Organizations who experienced secrets leakage resulting in financial damage, **lost, on average, \$1.2 million** in revenue.

## The secrets management money pit



Companies that experienced secrets leakage resulting in financial damage lost **\$1.2 million** on average.

Organizations lose **\$8.5 billion** annually to workers managing secrets.

The damage didn't stop with direct revenue impact, however. On top of the immediate cost, 40% of companies surveyed listed brand reputation damage as the second-largest cost of a breach. Many lose huge swaths of business, with 32% of those who lost clients due to secrets leakage losing more than 15% of their overall client base.

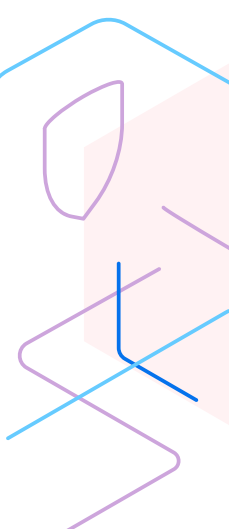
Perhaps more importantly, breaches can compromise your customers and employees. When an attacker gains access to your infrastructure, they often find passwords that customers and employees have reused – meaning when an attacker gains access to one account, they also gain access to any other account where that password has been used.

# Taming secret sprawl with a culture of security

Great security is about more than the technology used. It's also – even mostly – about people. That's because the most secure technology in the world has little impact unless people actually use it. Around 70% of U.S. workers believe it falls solely on the company to make sure work accounts aren't hacked or breached, which makes IT's job that much harder.

Creating a [culture of security](#) requires getting everyone, from C-level to individual employees – to understand that your company is only as secure as its weakest link:

## Building a culture of security

- 
- 1 Devote sufficient planning and resources, including educational materials and official password policies.
  - 2 Organize an official rollout, complete with a formal kick-off event, to show employees that the company takes security seriously.
  - 3 Train new and existing employees regularly.
  - 4 Reward employees for their involvement, and reinforce best practices.
  - 5 Revisit policies and technologies regularly. The threat landscape is constantly evolving, and a culture of security must evolve with it.



# The final piece of the puzzle: human and machine secrets management in one platform

1Password makes it easy for employees to generate and manage strong, secure passwords for any website or service. And because it's easy to use, they actually use it. That's why more than 80,000 businesses trust 1Password to keep their most important information secure.

But as we've seen, strong passwords are now only half of the puzzle. To protect all your company secrets, 1Password Teams and Business customers can add 1Password Secrets Automation to their plan. Secrets Automation protects infrastructure secrets with the same industry-leading security architecture as 1Password, then delivers those secrets when and where they're needed.

Together, 1Password and Secrets Automation give your company a single place to store all your company secrets, from passwords and credit cards to API tokens and SSH keys. Not only does Secrets Automation do for infrastructure secrets what 1Password does for passwords, it also eliminates the developer bottlenecks that come with tracking down secrets. When the secure thing to do is also the easy thing to do, [security and productivity go hand-in-hand](#).

1Password is the world's most-trusted enterprise password manager. Industry-leading security and usability help businesses securely manage passwords, secrets, and private documents to protect their most sensitive data from online threats. Find out more at [1Password.com](https://1password.com).

