AKEYLESS

The State of Secrets Management 2024 Survey Report

Table of Contents

Introduction and Key Findings

Introduction & Methodology

With companies increasingly moving their business operations to the cloud, there have been significant changes in how they develop applications as well. Containerization, automated DevOps methodologies, and zero-trust policies have led to a rise in machines and machine identities, including scripts, applications, containers, databases, and more.

These machines require continuous authentication and authorization via credentials, certificates and keys, also known as secrets. These secrets are in constant use in the CI/CD pipeline – "sprawled" throughout the typical organization's tech ecosystem. And since these secrets can frequently be found in vulnerable and unprotected locations, they have become an attractive target for hackers, particularly since secrets such as encryption keys and the keys to a company's cloud services can unlock access to significant volumes of sensitive data.

The proliferation of secrets, as well as recent high-profile breaches – like those experienced by LastPass, Uber and SolarWinds due to compromised credentials – have raised awareness around the risks of secret leaks. As a result, it is becoming a more important focus for security teams, who are increasingly recognizing that a fragmented approach to secrets management does not scale with today's modern computing environments, and that the most effective solution is a scalable and unified platform that can automate processes for creating, storing, rotating, and revoking secrets.

To gain more insight into the current state of secrets management, we commissioned a survey of 200 security leaders to shed light on their main challenges and concerns around secret security, how effective they have been at stopping breaches and solving hacks with their current tools, and how they plan to improve their capabilities in dealing with secrets management moving forward.

Methodology

This report was administered online by Global Surveyz Research, an independent global research firm. The survey is based on responses from 200 CISOs, Directors and Managers in the fields of Application Security, Cloud Security and Information Security, security engineers and other senior security professionals in companies with 1,000+ employees, across the US, UK, Germany and France. The respondents were recruited through a global B2B research panel and invited via email to complete the survey, with all responses collected during June 2023. The average amount of time spent on the survey was 7 minutes and 33 seconds. The answers to most of the non-numerical questions were randomized, to prevent order bias in the answers.

Key Findings

1 Secrets sprawl is a continuing problem

Secrets are still found throughout DevOps code, files and systems, with 96% of respondents reporting that organizational secrets are kept outside of secrets managers in vulnerable code, config files, and CI/CD and infrastructure tools (Figures 1 and 2). These secrets are low-hanging fruit for malicious actors.

2 ...And a major concern for security professionals

It's no surprise, therefore, that 88% of the respondents are concerned about secrets sprawl (Figure 3). In companies that are larger than 5,000 employees, the concern is even more acute, with 49% of security professionals "very concerned" about this challenge.

3 1 in 3 security professionals say that secrets management is one of their top 5 priorities

Given the level of concern around secrets sprawl, it makes sense that not only is secrets management one of the top five priorities for the coming year among respondents (Figure 5), but that 96% of respondents are planning a centralized enterprise solution for secrets management by 2024 or already have one implemented (Figure 10).

4 Only 44% of respondents are currently using a secrets management system to manage their secrets

Many security professionals are attempting to solve the challenge of secrets management with solutions that can't fully provide the comprehensive features and capabilities needed to manage the full range of secrets. Despite their awareness of secrets sprawl and its dangers, most security teams still aren't leveraging a unified secrets management platform that manages multiple types of machine secrets. A full 44% of the respondents expect to use PAM solutions to manage machine secrets, while 42% expect to use Password Management solutions for this purpose (Figure 6).

5 Although secret leaks are common, time-consuming and expensive, top management may not fully understand the cost of secret leaks

70% of respondents have experienced secret leaks in the past two years (Figure 11), with an average of 36 hours required to mitigate a secret leak (Figure 13). But while managers and directors – who frequently deal with secret leaks themselves – estimate the average cost of a leak as 40-42 hours, C-Suite professionals think such leaks can be handled in significantly less time (Figure 15).

Survey Report Findings

Secrets Sprawl in the Organization

Secrets sprawl remains widespread across organizations.

When respondents were asked, "Where are secrets kept in your organization?", their responses revealed they are more aware than ever of the truth of secrets sprawl, with nearly all respondents (96%) acknowledging storage of secrets outside of secrets managers in vulnerable locations (Figure 1). Almost half (48%) indicate they keep secrets in configuration files, with a similar number (48%) storing secrets in infrastructure tools. Security professionals also acknowledge keeping secrets in CI/CD tools (35%) and code (33%), indicating their understanding of how wide-ranging secrets sprawl can be (Figure 2).

The larger the magnitude of the sprawl, the bigger the risk of secret leaks, hacks and breaches due to compromised credentials, so it's no wonder that security professionals are concerned about the secrets sprawl phenomenon (see Figure 3 below).

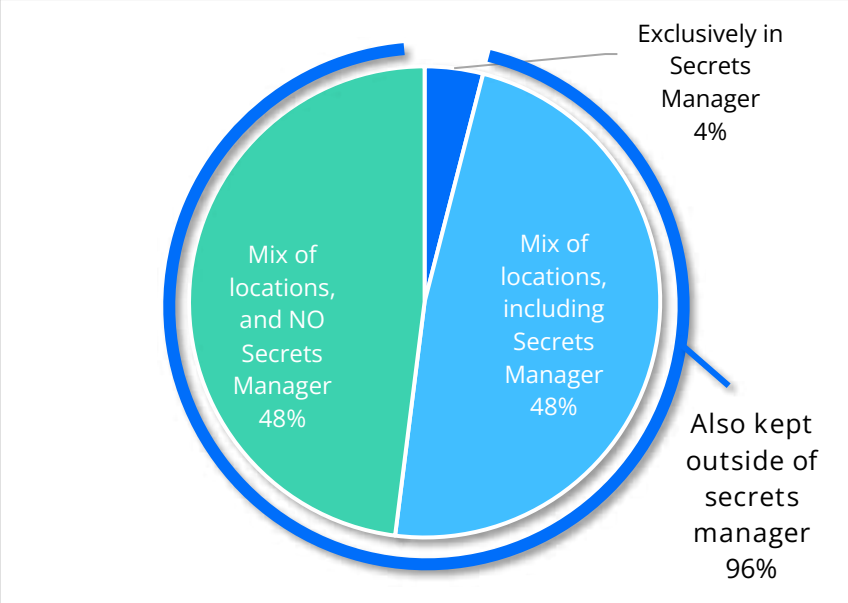


Figure 1: Where Secrets are Kept in the Organization, by Location

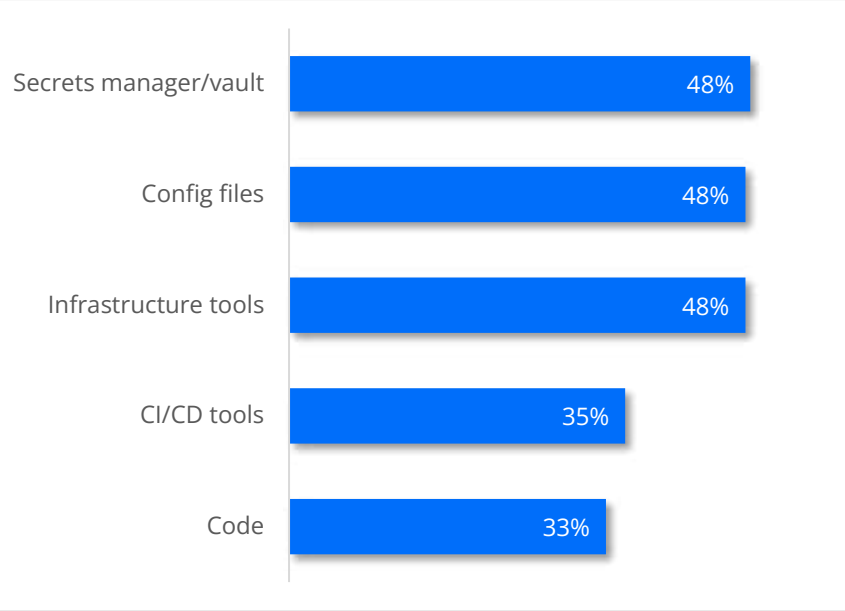


Figure 2: Where Secrets are Kept in the Organization, Overall

Question in Figure 2 allowed more than one answer and as a result, percentages will add up to more than 100%

88% of Security Professionals are Concerned About Secrets Sprawl

When asked how concerned they are about the secrets sprawl phenomenon, 88% of the respondents indicated some level of concern, with 40.5% being very concerned and 47.5% being slightly concerned.

This concern is understandable given that secrets are typically found in multiple (and often vulnerable) locations if they are not stored in a centralized secrets management solution (as shown in Figure 3), making them easy to hack.

When further investigating the results by company size, 90% of the respondents in companies with <5K employees are concerned about the secrets sprawl phenomenon compared with 86% of respondents in companies with 5K+ employees. The fact these results are so similar suggests the concern is widespread in companies of all sizes.

When looking specifically at whose who said they are "very concerned", however, respondents from larger companies (over 5K employees) are understandably more concerned (49%) than those from smaller companies (34%), given that the scale of secrets sprawl is far larger in bigger companies, making them even more vulnerable to hacks.

Question allowed more than one answer and as a result, percentages will add up to more than 100%

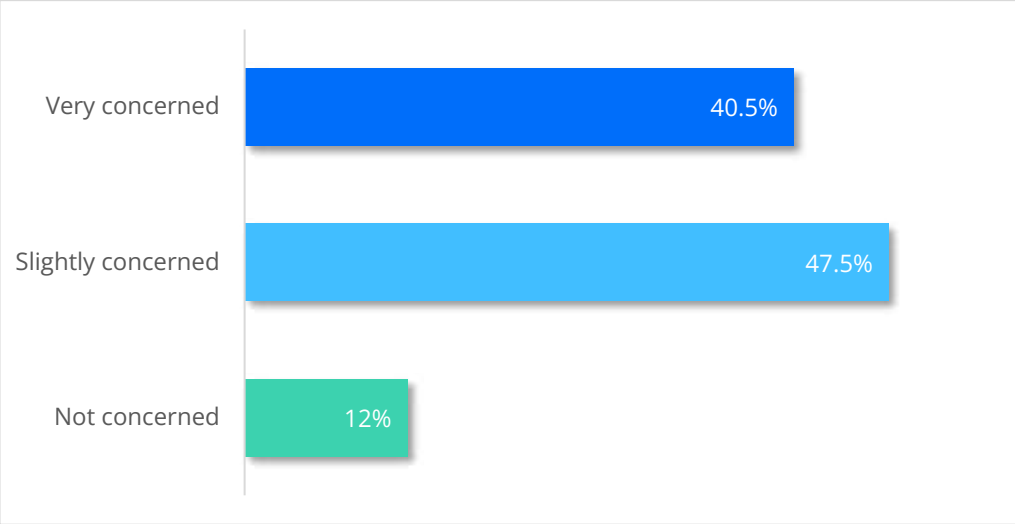


Figure 3: Level of Concern About the Secrets Sprawl Phenomenon

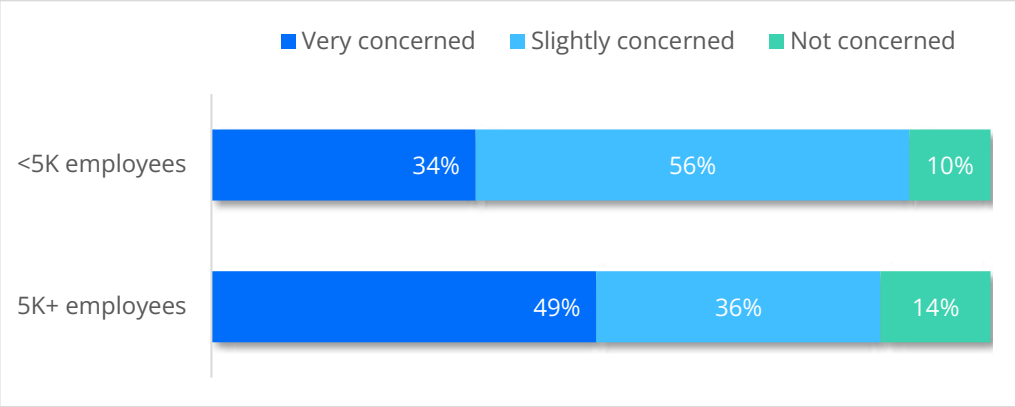


Figure 4: Level of Concern About the Secrets Sprawl Phenomenon, by Company Size

Secrets Management is a Top Five Cybersecurity Priority for Security Teams

We asked survey respondents what their top priorities are for their cybersecurity strategy in 2024. Secrets management was named among the top five priorities (33%), in conjunction with major security initiatives such as cloud security (45%), API security (42%), endpoint security (36%), and threat intelligence (34%).

This finding reinforces the importance of secrets management for developing robust cybersecurity strategies for 2024 and beyond.

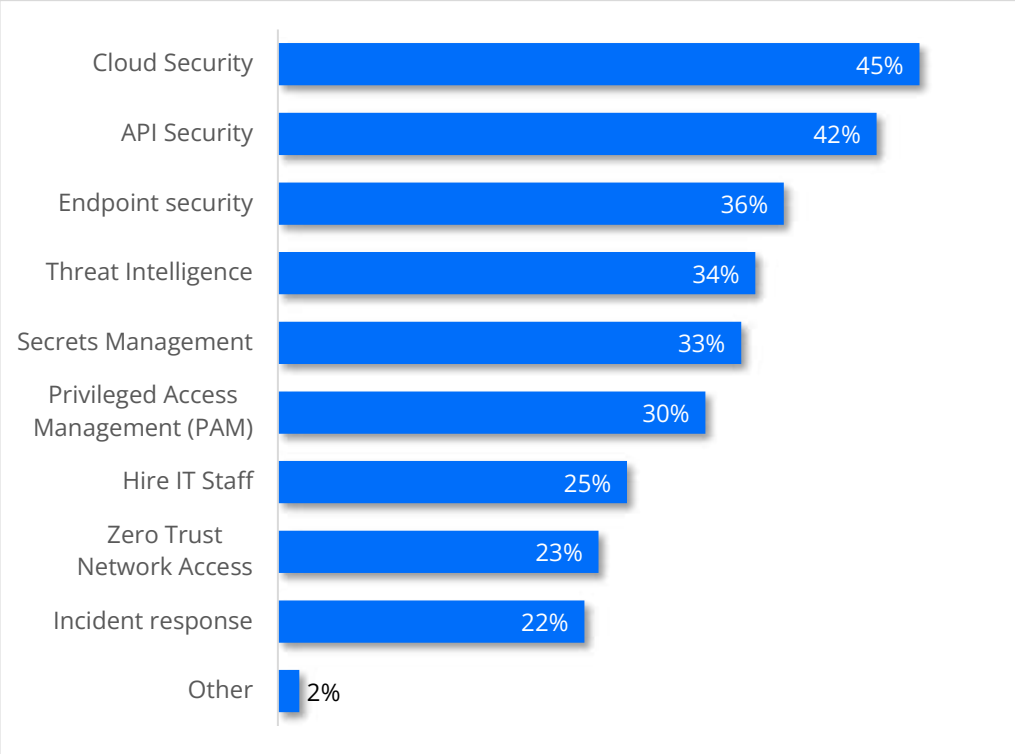


Figure 5: Top Priorities for Cybersecurity Strategy in 2024

Question allowed more than one answer and as a result, percentages will add up to more than 100%

Less Than Half of Security Teams (44%) Are Using a Secrets Management System

We asked survey respondents, “Which of the following security tools do you currently use to manage and secure keys, certificates, credentials and other organizational secrets?”

Although 99% of respondents indicated they are using some kind of tool (or combination of tools) to manage and secure organizational secrets, more than half are still focusing on point solutions, with their primary tools including Key Management Systems (48%), Certificate Management Systems or PKI (45%), and Privileged Access Systems (44%). These point solutions, however, can only solve the secrets management challenge for encryption keys (KMS), certificates, or human privileged access (PAM) respectively, leaving much of the CI/CD pipeline and its secrets unsecured.

Only 44% of respondents are currently using a secrets management system, which is the only solution designed to handle a broader range of secrets, particularly those included in DevOps and hybrid cloud environments.

Tip: Download this E-book to learn more about securing secrets at scale, including how to protect and manage credentials, certificates, and keys to support your DevOps and Cloud initiatives.

Question allowed more than one answer and as a result, percentages will add up to more than 100%

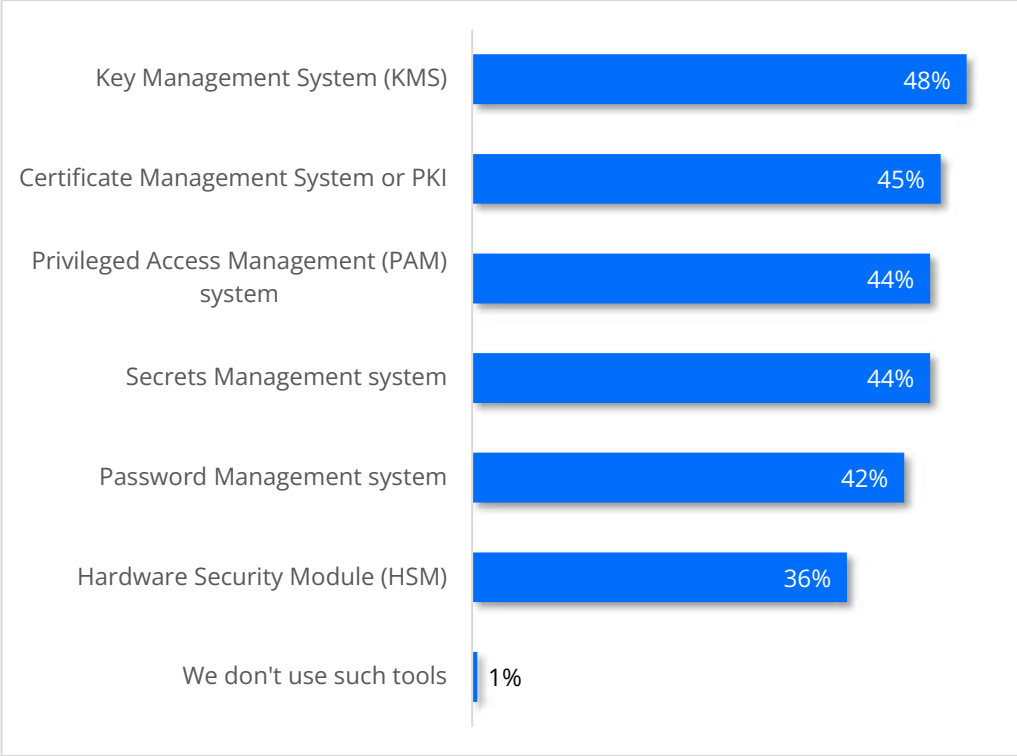


Figure 6: Tools for Managing and Securing Organizational Secrets

Prevalent Tools for Protection from Credential Breaches

We asked survey respondents, “What tool would be best to protect your organization from breaches resulting from compromised credentials (whether you currently have it or not)?”

While over half of the respondents (55%) see Privileged Access Management solutions as the top tool for protecting against breaches due to compromised credentials, it was closely followed by Secrets Managers (49%), showing an understanding of just how important it is to safeguard machine secrets to prevent breaches.

Password Managers are also perceived as a preferred solution (48%), perhaps showing a misunderstanding of the full scope of the problem, which goes far beyond passwords.

Only 41% of respondents included an HSM, reflecting the widespread move to cloud-native systems and solutions.

Tip: Breaches currently occurring as a result of hacks involve the full range of secrets: credentials, certificates, and keys, including encryption keys. To prevent these hacks, it is imperative to use tools that can manage all types of machine secrets.

Question allowed more than one answer and as a result, percentages will add up to more than 100%

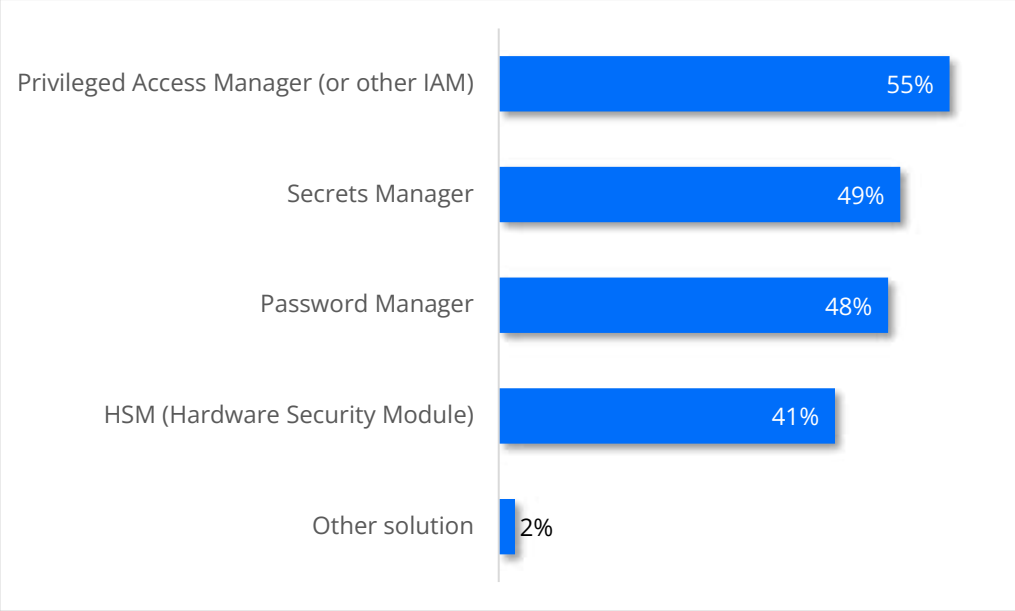


Figure 7: Prevalent Tools for Protection from Credential Breaches

Top Solutions for Managing Workload Secrets

When asked how their workload secrets are currently being managed, respondents mentioned enterprise self-deployed solutions (36%), SaaS solutions (26%), and open-source self-employed solutions (17%) as their preferred tools. Only 1% of respondents said their workload secrets are not being managed at all, reinforcing the overwhelming consensus among security professionals that workload secrets must be managed.

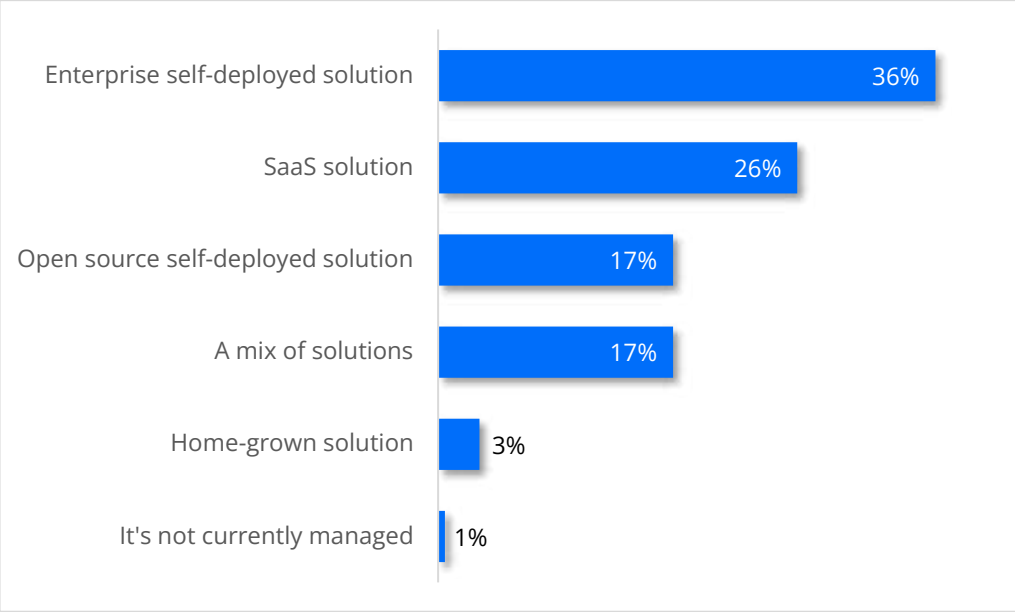


Figure 8: Solutions for Managing Workload Secrets

Top Drivers of Dissatisfaction with Current Secrets Management Solution

We asked respondents, "In what way are you not fully satisfied with your current solution or approach to secrets management?"

Among those dissatisfied, the top reason for their dissatisfaction is that not all secrets are secured (54%). This aligns with the previous finding (Figure 6) that more than half of security teams are still using point solutions to manage and secure organizational secrets. Since these solutions are only designed to address certain types of secrets, this approach leaves other aspects of the CI/CD pipeline and its secrets unsecured.

Other drivers for dissatisfaction are that there is no central management (43%) – which is again a consequence of siloed solutions rather than a unified secrets management platform – and that there are problems with adoption (43%), indicating that certain secrets management platforms are not as easy to deploy and use as they should be.

Figure 9: Dissatisfaction Drivers

Question allowed more than one answer and as a result, percentages will add up to more than 100%

Plans to Implement a Centralized Enterprise Solution

With 96% of respondents indicating they have either already implemented a centralized enterprise solution (62%) or are planning to implement one by 2024 (34%) – it is clear there is widespread recognition of the importance of a centralized enterprise approach to secrets management.

That said, the fact that 62% of the respondents claim to have already implemented some kind of centralized enterprise solution (Figure 10) while only 44% indicated they are currently using a secrets management system (Figure 6), shows there may be a gap in the understanding of what a centralized secrets management solution actually is. For example, some security teams may be using several point solutions that address certain secret types, but this does not mean that all secrets are being properly managed and secured.

Another explanation for the discrepancy could be that a solution has been purchased but is not being fully utilized due to adoption issues. Or in other words, the chosen secrets solution is not easy enough to use, deploy and manage.

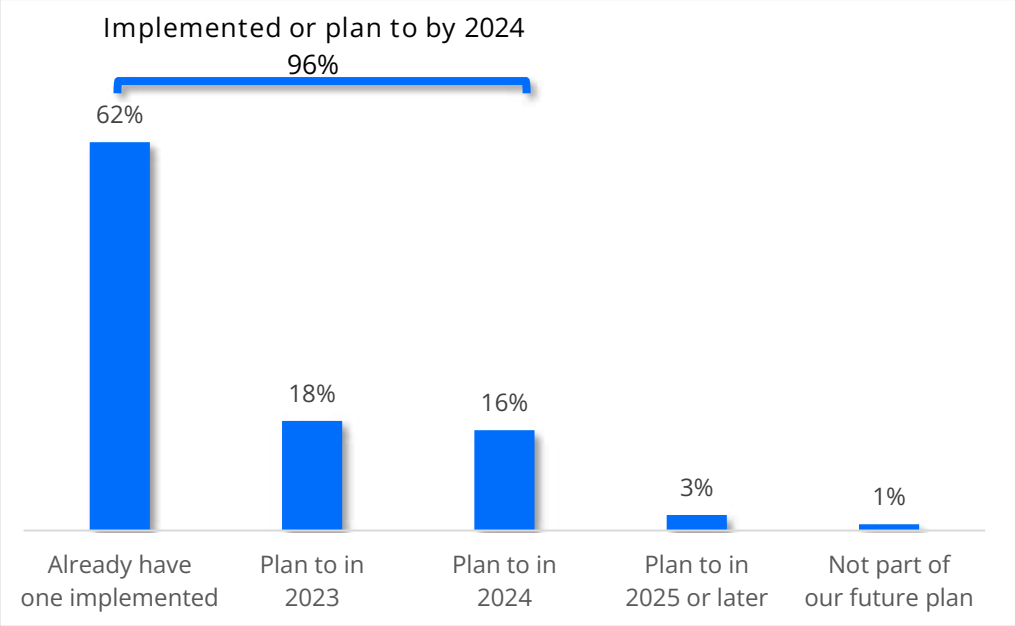


Figure 10: Plans Concerning Implementation of a Centralized Enterprise Solution

Secret Leaks are Increasingly Common

70% of respondents indicated they have experienced secret leaks in the past two years. This has inevitably raised awareness around machine secrets and their increasing appeal to hackers.

The measure most widely used by respondents to mitigate secret leaks is recreating identities (71%), reflecting a "start from scratch" approach, which suggests that an efficient secrets management system was likely not in use when the leaks occurred.

30% of respondents used the industry best-practice of temporary permissions (that expire automatically), and 38% were also able to rotate secrets to mitigate harm.

Only 18% of the respondents said they had no secret leaks at all. This demonstrates that secret leaks are becoming increasingly common and reinforcing the importance of implementing a secrets management system.

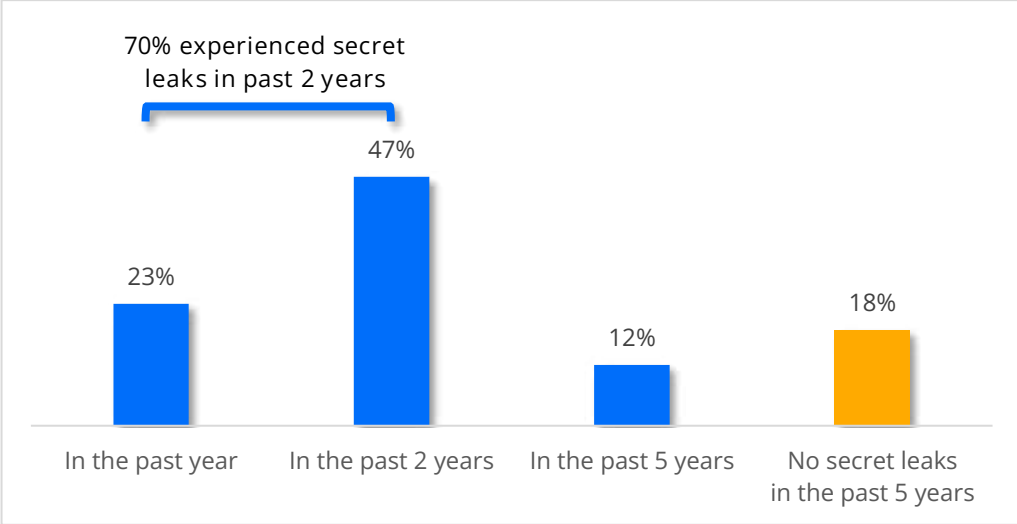


Figure 11: Experience of Secret Leaks

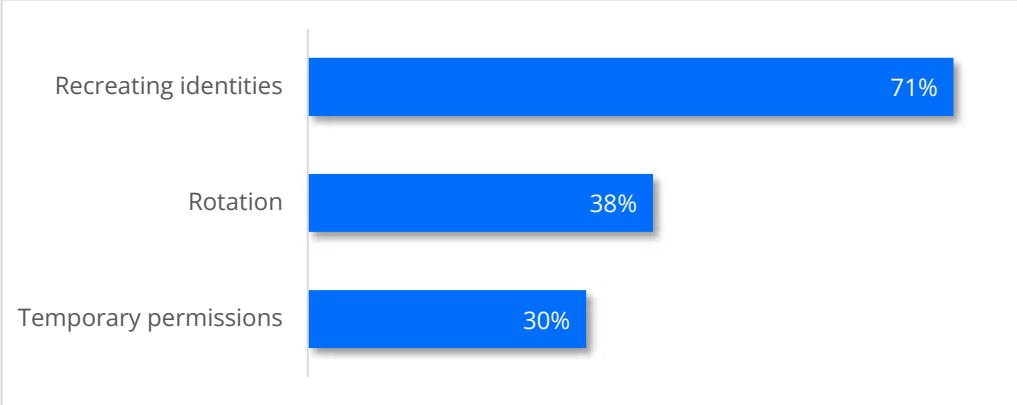


Figure 12: Mitigation Measures to Deal with Secret Leaks

Question allowed more than one answer and as a result, percentages will add up to more than 100%

Average Time to Deal with a Secret Leak

Virtually all respondents acknowledged that dealing with secret leaks can be tremendously time-consuming, requiring an average of 36.1 hours for each mitigation process.

50% of respondents spent 21-50 hours to mitigate a secret leak.

Only 2% of respondents were able to mitigate a secret leak in under 5 hours.

Given that "time is money", these results demonstrate just how burdensome mitigating secret leaks is, both in terms of cost and as a strain on resources.

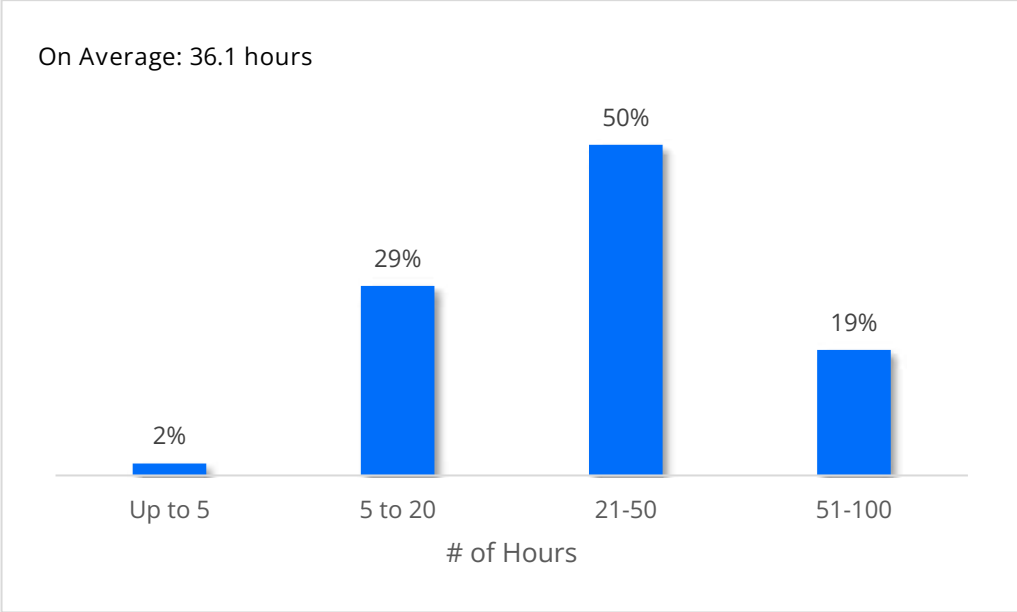


Figure 13: Average Time to Deal with Secret Leaks

Differing Perceptions of Time Needed to Deal with Secret Leaks

Although the overall average time to deal with secret leaks is 36 hours (Figure 13), further investigation of the mitigation of these risks by department and role revealed some interesting insights.

Professionals in security teams – who are arguably the most 'hands-on' line of defense when dealing with secret leaks – estimated a much higher time for mitigation (43 hours on average) – compared to members of R&D (36 hours on average) and IT teams (32 hours on average).

The average time to deal with secret leaks also differs by role: the average time for managers is 40 hours, for directors 42 hours, for VP/Heads 30 hours and for C-suite 33 hours.

Interestingly, the fact that managers and directors – who frequently need to deal with such leaks themselves – estimated the average cost of a leak as 40/42 hours, while VPs and C-Suite professionals thought such leaks could be handled in only 30/33 hours on average, suggests that top management may not fully understand the cost of secret leaks.

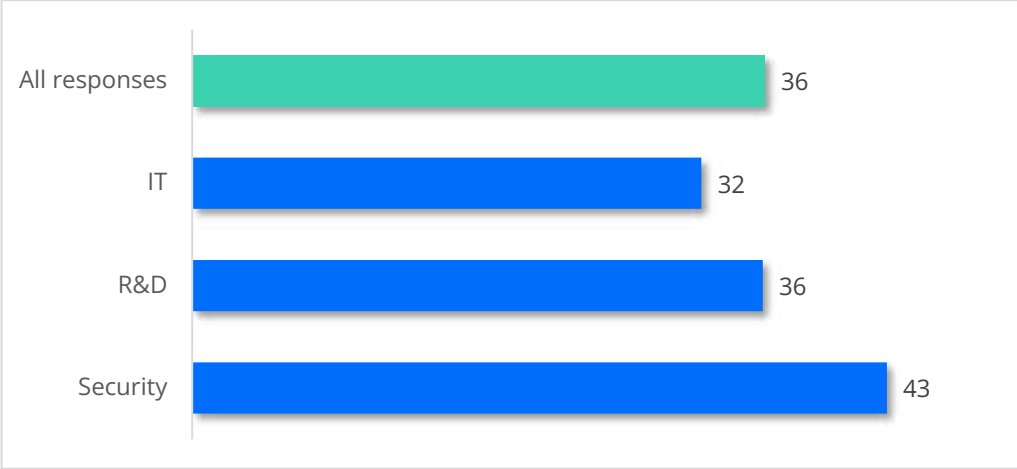


Figure 14: Average Hours to Deal with Secret Leaks, by Department

Figure 15: Average Hours to Deal with Secret Leaks, by Role

Question allowed more than one answer and as a result, percentages will add up to more than 100%

Demographics

Country, Industry, Company Size, Department, Seniority, and Role

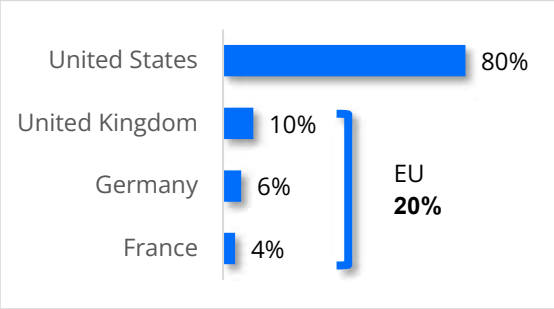


Figure 16: Country

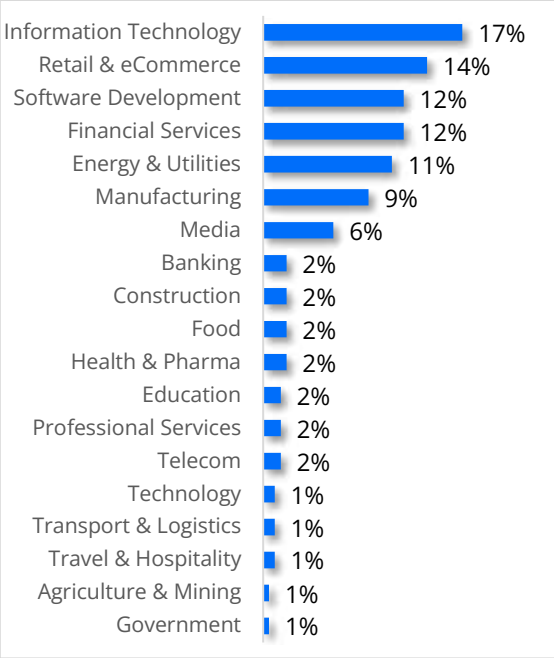


Figure 19: Industry

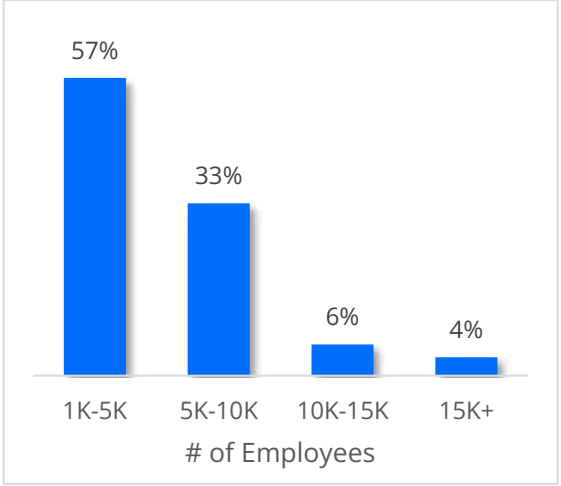


Figure 17: Company Size

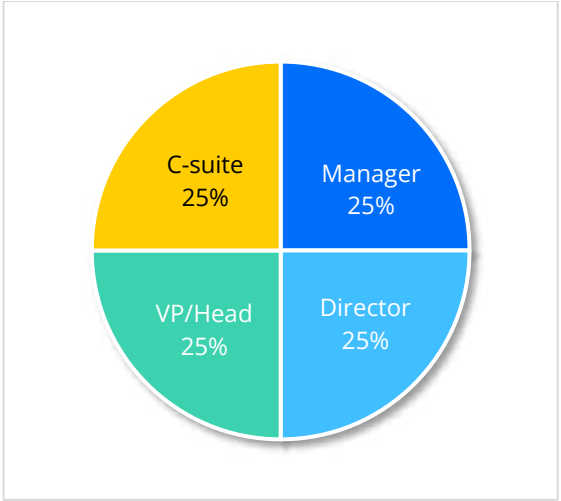


Figure 20: Seniority

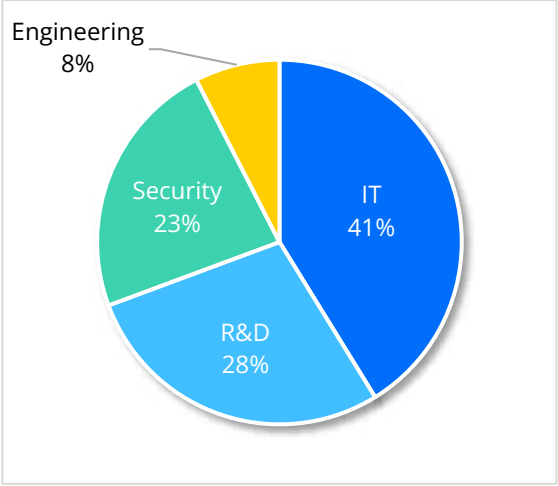


Figure 18: Department

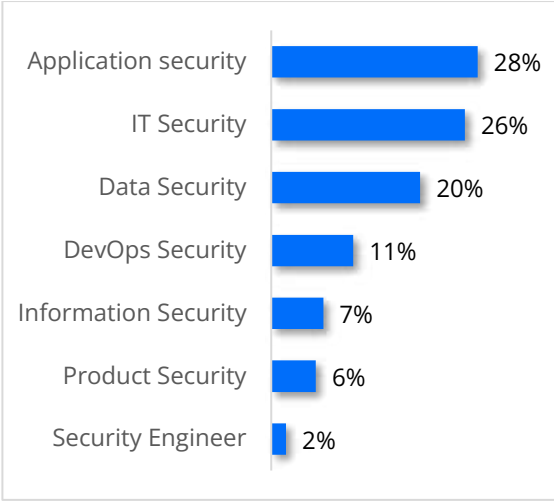


Figure 21: Role

About Akeyless

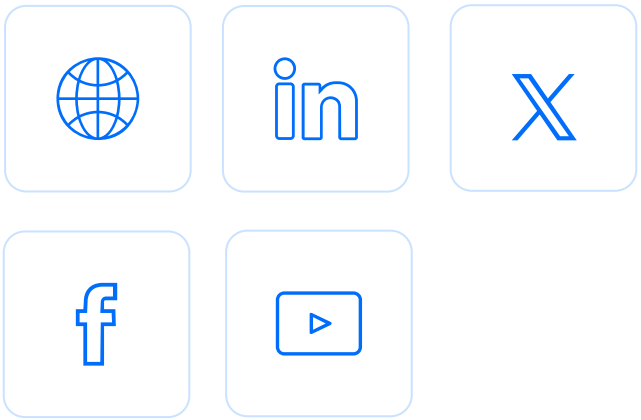
The Akeyless Vaultless Platform enables enterprise DevOps and Infosec teams to effectively and efficiently manage their secrets (credentials, certificates and keys). Vaultless secrets management is designed for the modern “everywhere” enterprise – cloud-native and delivered as-a-service.

The Akeyless platform uses Distributed Fragments Cryptology (DFC™) to ensure zero knowledge – meaning that secrets are created as distributed fragments in the cloud and never found in one place. This patented technology securely eliminates the need for vaults along with the complex and burdensome necessity of vault management, resulting in up to a 70% reduction in costs.

Request a Demo

For more information,

please visit us:



contact-us@akeyless.io