

# Voice Of Practitioners

## The State of Secrets in AppSec

INSIGHTS FROM 507 IT DECISION-MAKERS  
ON SECRETS SPRAWL AND RISK MITIGATION



**Today** more than ever, secrets are omnipresent along the software development cycle. They tie together the building blocks of software applications, being the foundation of critical security mechanisms such as authentication, authorization, and encryption. In fact, digital identity and access management rely heavily on secrets.

Earlier this year, **GitGuardian's 2023 State of Secrets Sprawl** once again sounded the alarm about secrets in source code: no less than 10,000,000 secrets occurrences were detected on public GitHub in 2022 (+67% compared to 2021), over a total of 1.027B new commits scanned.

High-profile cybersecurity incidents involving secrets have affected some of **the largest tech companies** in recent years, underscoring the difficulty of properly

managing secrets at scale. Even as organizations become more concerned with the security of their code and the resiliency of their supply chains, adapting their security posture to the new landscape represents a significant challenge.

To better understand the awareness of the problem in the field and the obstacles encountered by security leadership, this year GitGuardian partnered with Sapio Research to conduct a field study about hard-coded secrets risk awareness and mitigation strategies.

Together, we analyzed the responses from **507 IT decision-makers** (IT director, VP of IT, CIO, CSO, CISO, VP of Cybersecurity, etc.) in the US and the UK. Here are the results.

## **Executive summary**

---

## **The Study**

---

The industry is aware of the risk of leaked secrets **07**

Secrets management maturity is still uneven **10**

Protecting AppSec bandwidth requires reprioritizing **15**

## **Deploying detection, remediation & prevention at scale**

---

Prevention **18**

Remediation: more complex than it appears **19**

Scaling remediation with developers' help **21**

Conclusion **23**

About GitGuardian **25**

Methodology **26**

# **Executive summary**

## Key insights from the study

**75%**

of respondents reported experiencing a secret leak.

**60%**

reported leaks impacting the company or its employees.

**47%**

identified “Hard-coded secrets” as key risk points in their software supply chain.

**27%**

admitted relying on manual reviews to detect hard-coded secrets.

**53%**

of the senior management (e.g., CSO, CISO, VP of cybersecurity) believe secrets are shared in plaintext through messaging apps.

**94%**

are planning to improve their secrets practices in the next 12-18 months.

**26%**

of respondents said they would invest in secrets detection and remediation in 2023.

# **The Study**

# The industry is aware of the risks of leaked secrets

The first objective was to assess awareness of the risks posed by exposed secrets in DevOps environments.

When asked: “Have you ever been impacted by, or heard of secrets (API keys, username and passwords, encryption keys, etc.) leaking within your organization?”

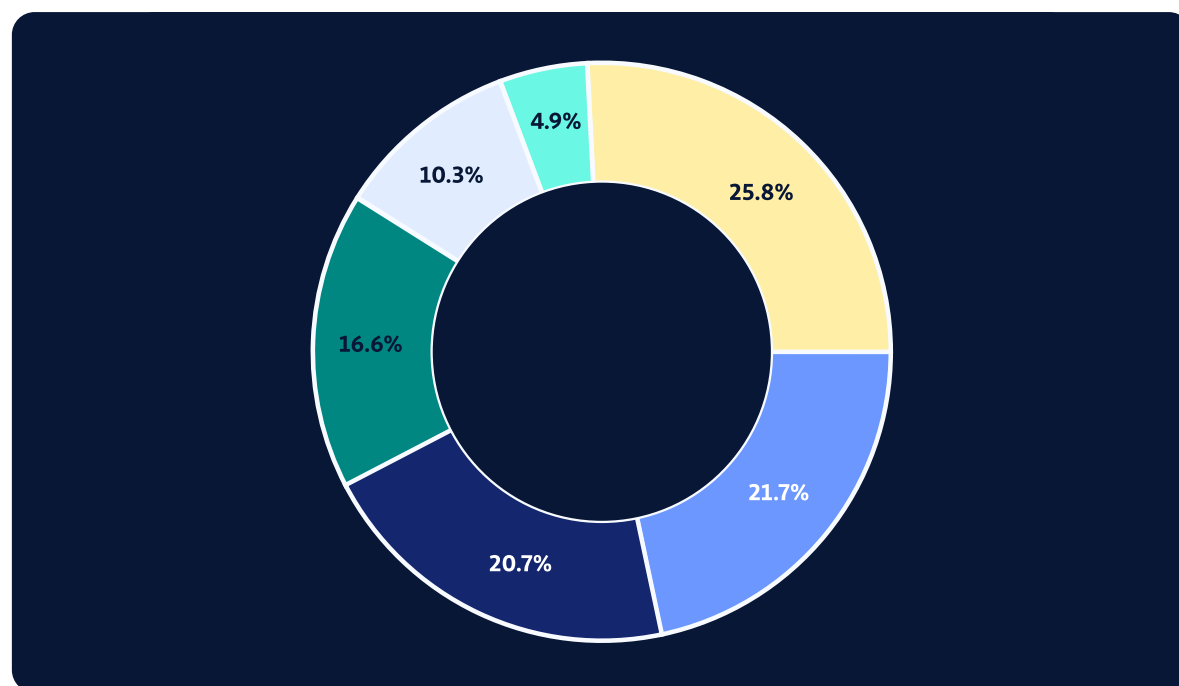
## 75%

of the respondents said a secret leak happened in the past.

## 60%

said it caused issues for the company, its employees, or both.

**Have you ever been impacted by, or heard of secrets (API keys, username and passwords, encryption keys, etc.) leaking within your organization?**



- ☒ Yes, I know a leak occurred, but I'm not sure what the impact was
- ☐ Yes, I know a leak occurred, but it had no impact
- ☒ Yes, I know a leak occurred, and it caused issues for both the company and employees
- ☒ Yes, I know a leak occurred and caused damage to the company (technical disruption, financial loss, brand image loss etc.)
- ☒ Yes, I know a leak occurred, and it caused issues for employees
- ☐ No

When asked about the key risk points within software supply chains:

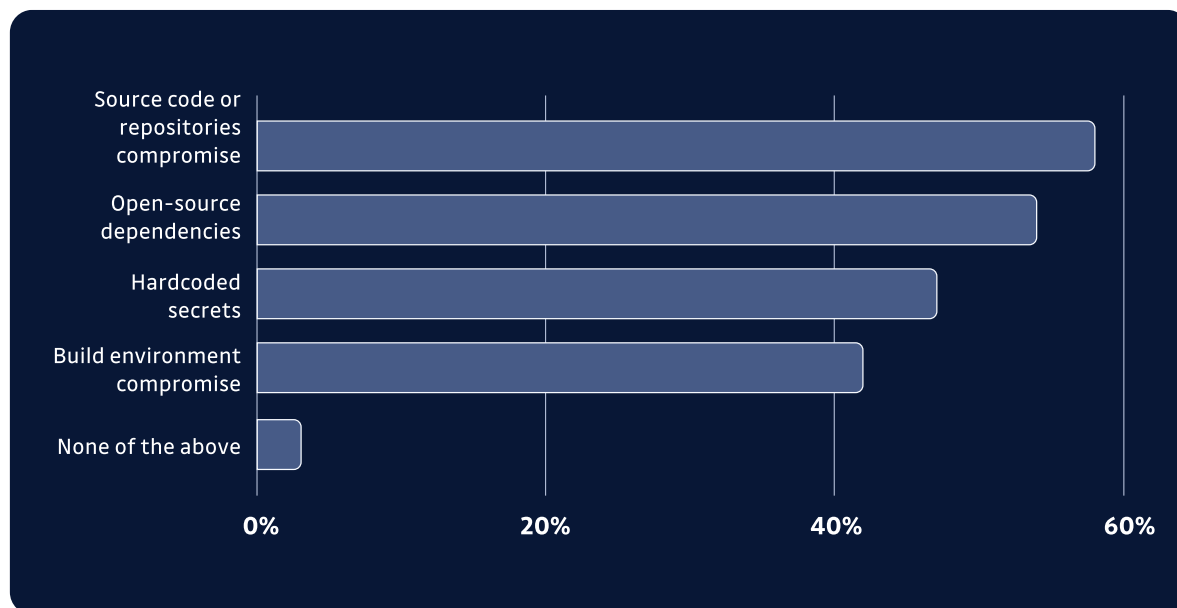
**58%**

of respondents identified “source code and repositories”.

**47%**

of respondents identified “Hard-coded secrets”.

In your opinion, what are the key risk points within your software supply chain?  
Select up to three



In other words, the majority of respondents consider **secrets protection** to be a **critical** component of application **risk management**.



## A Minimum Security Standard In the Making

“We recommend using heuristic tools<sup>1</sup> to examine the code for hard-coded passwords and private encryption keys. Such tools are feasible since functions or services taking these as parameters have specific interfaces. Dynamic testing is unlikely to uncover such unwanted code.”

Guidelines on Minimum Standards for Developer Verification of Software, NIST<sup>2</sup>

“Sensitive data, including credentials, are not stored in plaintext anywhere in the organization and can only be accessed by authenticated and authorized users. Credentials are stored in a secure manner, such as with a credential/password manager or vault, or other privileged account management solution.”

Cybersecurity Performance Goals (CPGs) Checklist, CISA<sup>3</sup>

Under the Biden administration, initiatives to strengthen the cyber resilience of infrastructures and SMEs are increasing, the most recent being the [National Cybersecurity Strategy](#). For the moment, these recommendations are not yet binding. However, this could quickly change: with cybersecurity a national priority, the White House pledged to focus on software vendors’ accountability and “shape market forces” to promote secure development practices.

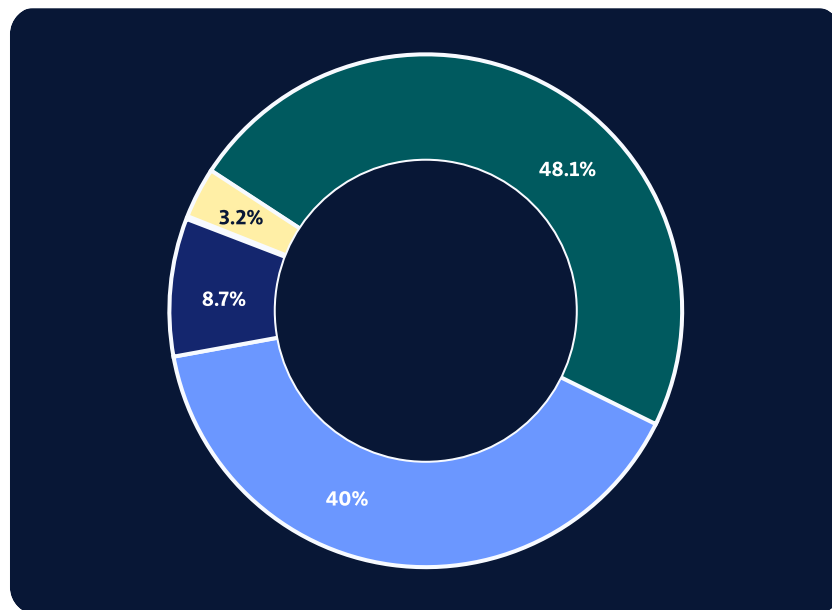
<sup>1</sup>Heuristic tools are tools designed to take into account uncertainty.

<sup>2</sup>[Guidelines on Minimum Standards for Developer Verification of Software](#)

<sup>3</sup>[https://www.cisa.gov/sites/default/files/2023-03/cisa\\_cpg\\_checklist\\_v1.0.1\\_final.pdf](https://www.cisa.gov/sites/default/files/2023-03/cisa_cpg_checklist_v1.0.1_final.pdf)

## Secrets management maturity is still uneven

When asked, “To what extent are you able to prevent secrets from being leaked today?” 48% of the respondents said they were able to prevent secrets from being leaked “to a great extent.”



To what extent are you able to prevent secrets from being leaked today?  
Select one

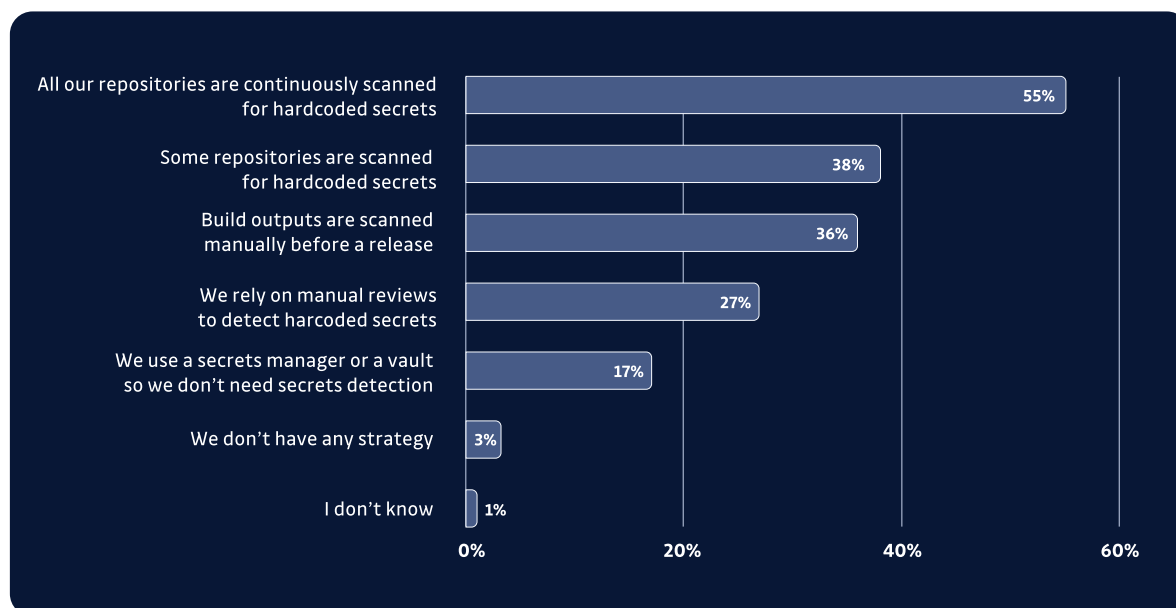
- ☒ To a great extent
- ☐ To some extent
- ☐ Very little
- ☐ Not at all

Yet, responses to other questions suggest a more mixed view. For example, when asked about their hard-coded secrets strategy:

- 27% of the respondents said, “We rely on manual reviews to detect hard-coded secrets”
- 17% said, “We use a secrets manager or a vault, so we don’t need secrets detection”
- 3% said, “We don’t have any strategy”

### Which of the following best describes your strategy about secrets hard-coded in source code?

Select all that apply



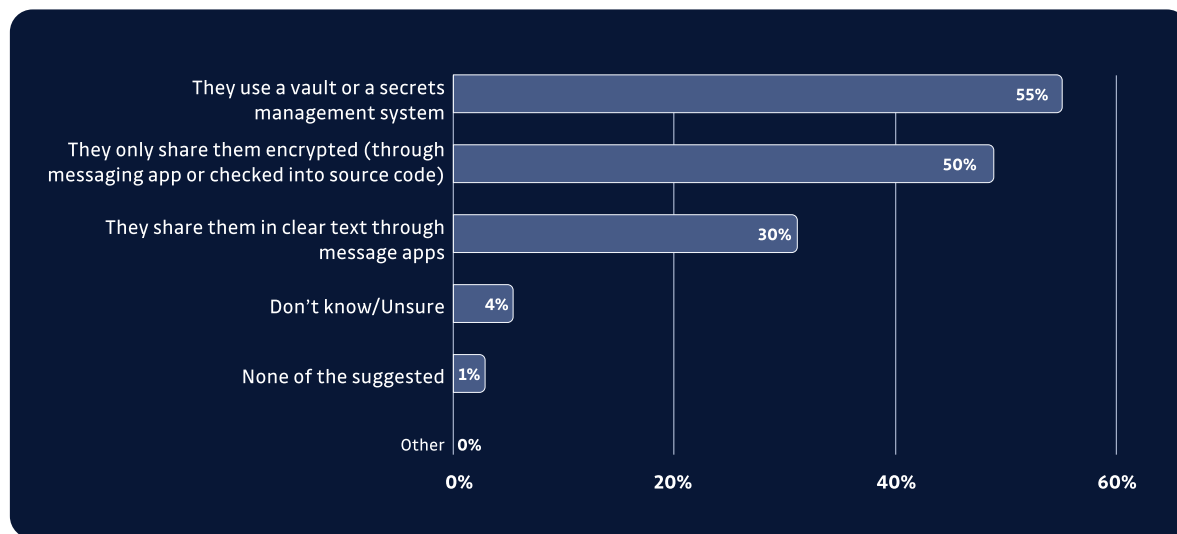
93% said either “all” or “some” of their repositories were continuously scanned for hard-coded secrets. However the previous results indicate secrets leak prevention capacities might be overestimated.

Manual code reviews are ineffective at detecting whether a secret has been hard-coded into the source code because the reviews only look at the most recent version of the code base, not at earlier revisions that may contain secrets ([more on this](#)). As for the use of a secrets manager, although it is essential, it does not offer protection against secret leakage either. Secrets management and detection are complementary functions.

Similarly, when asked, “How do your development teams share passwords and secrets when building applications today?”, 30% of the respondents said, “They share them in plaintext through messaging apps”— and 53% of the senior security management subgroup (e.g., CSO, CISO, VP of cybersecurity) too!

## How do your development teams share passwords and secrets when building applications today?

Select all that apply

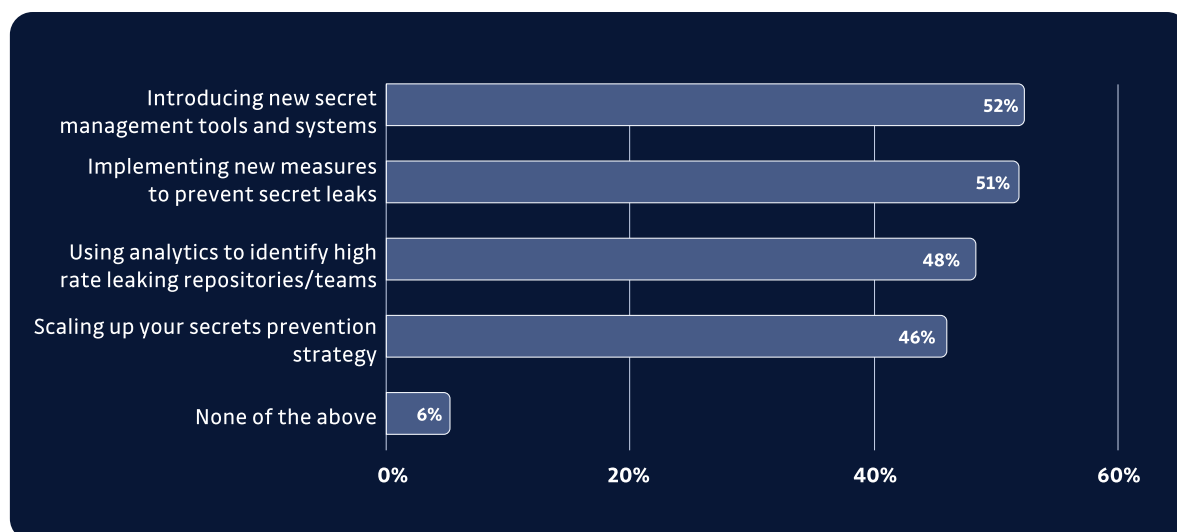


Based on our [secrets management maturity model](#), these responses suggest that for a significant portion of respondents, operational maturity is still low: it corresponds to the Uninitiated level, the lowest level on the maturity scale.

But there is a bright side. **94% of the respondents said they were, in one way or another, considering improving their secrets practices in the coming 12-18 months.**

## Are you considering implementing any of the following in the coming 12-18 months?

Select all that apply



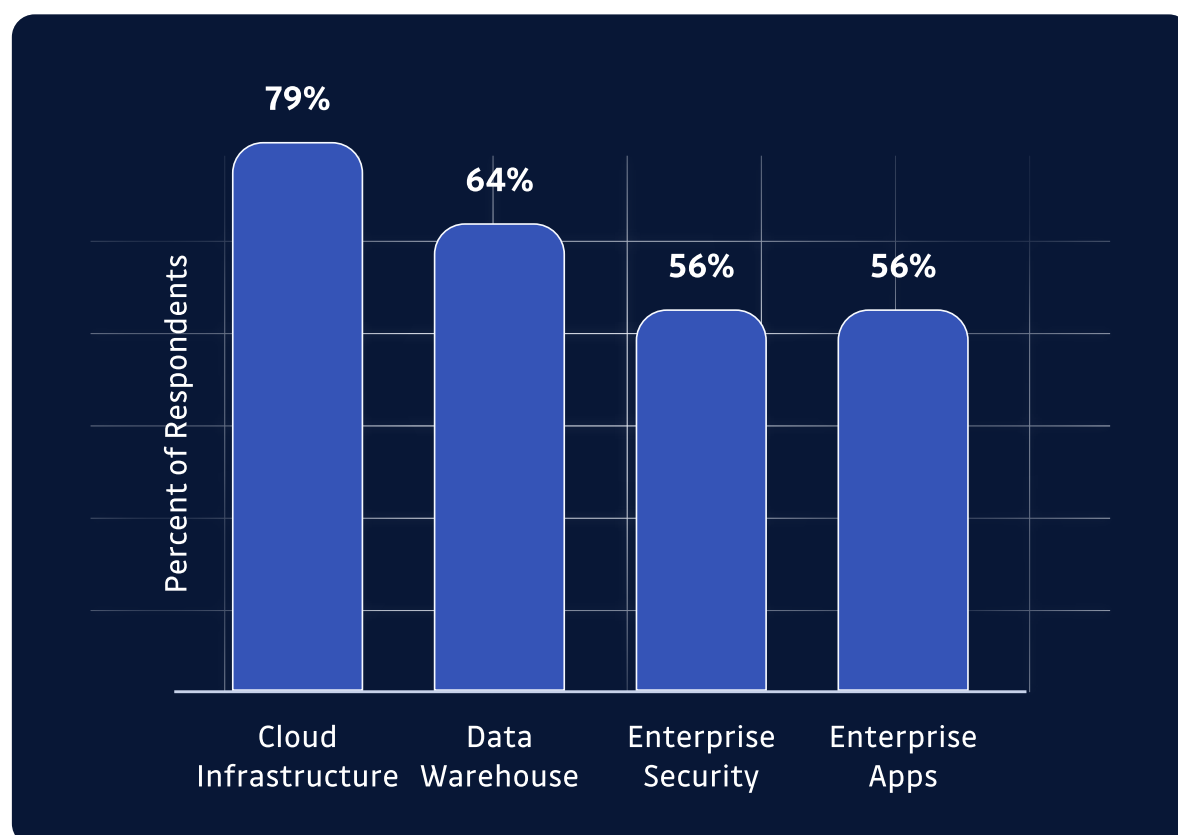
## Near term budget priorities for security investments.

Despite uncertain economic outlooks for some, security budgets for large enterprises remain stable, especially for spending priorities like enterprise security; these are some of the findings reported by [Battery Q1 2023 Cloud Software Spending Survey](#).

According to the report: *“Budgets remain relatively inelastic: 46% of CXO respondents expect to increase their total technology budget for 2023, despite continued macro headwinds.”*

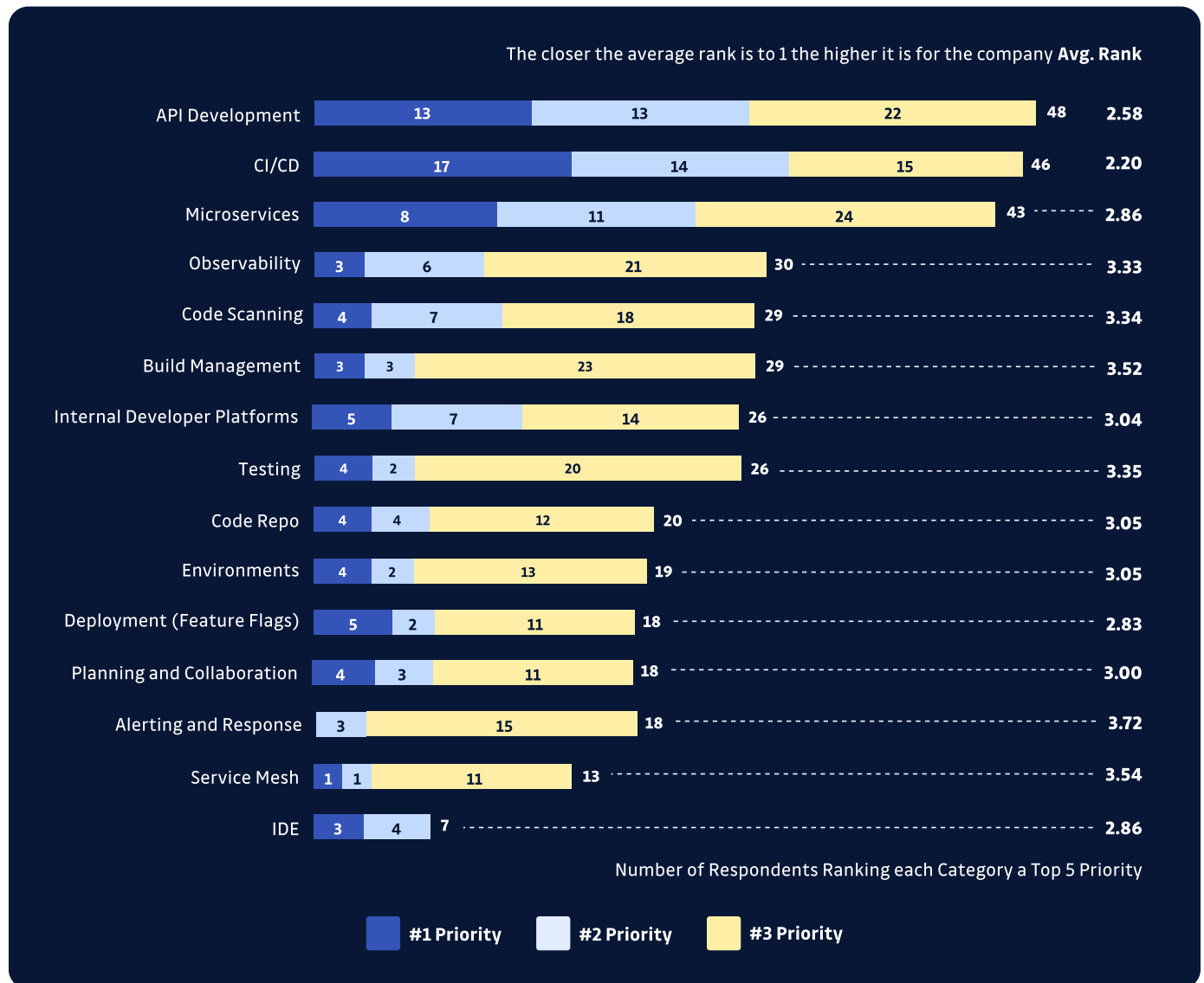
In particular, enterprise security is the third most prioritized category of investment for CXOs over the next 12 months: *“Most CXOs continue to focus on infrastructure software, enterprise security, and core enterprise applications as among the top 5 priorities.”*

### Top 5 Priority for CXOs Over Next 12 Months



*“Speed, safety, and resiliency are still the top developer tool priorities as enterprises focus on streamlining code into production reliably. AppSec and observability are shared by development and security teams.”*

### Companies Ranking Top 5 Priorities within Developer Tools

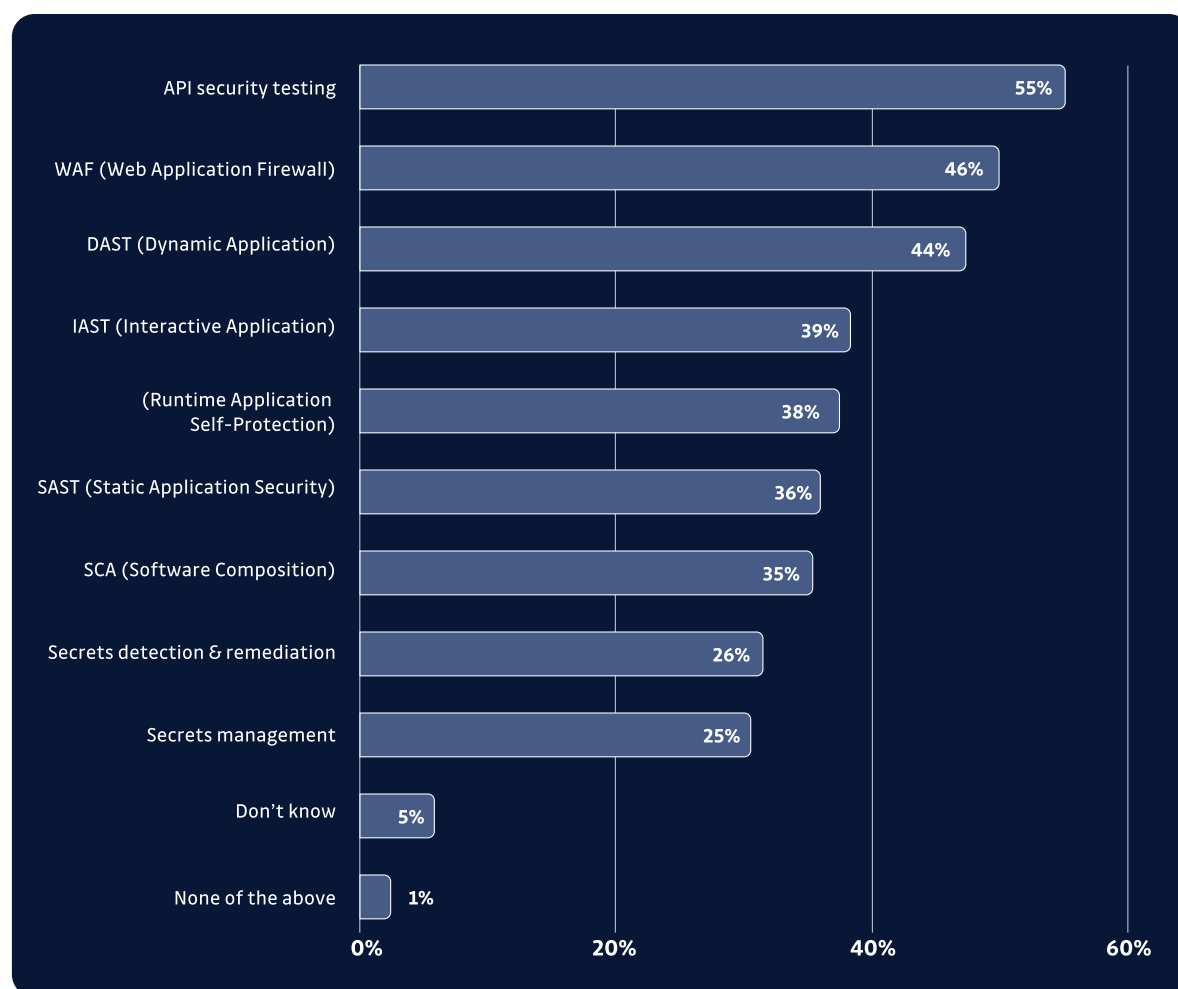


## Protecting AppSec bandwidth requires reprioritizing

In terms of priorities, the study revealed that secrets detection and remediation, as well as secrets management, are less prioritized (in terms of investment) compared to other tools, notably runtime protection tools.

**Roughly half as many decision-makers said they would invest in secrets protection compared to runtime protection overall:**

**Which Application Security tools will you invest in, in 2023?**  
Select all that apply



When asked the top 3 activities AppSec are spending most of their time on, 21% of respondents placed “Addressing hard-coded secrets issues” in their top 3, and half of the respondents picked “Running security tools or code reviews”.

Yet, only 26% of respondents said they would invest in secrets detection and remediation in 2023, and only 25% in secrets management, as opposed to the board-leading investments of API security testing (55%), WAF (45%), and DAST(44%).

There is a real need to protect AppSec bandwidth. Organizations need to increase the efficiency of their teams while also reducing alert fatigue. Last year, we highlighted that a single AppSec engineer faces, on average, 3,413 hard-coded secrets occurrences to investigate every year. Some strategies have proven more effective in alleviating this burden when deploying detection, prevention, and remediation at scale.



**Deploying  
detection,  
remediation  
& prevention  
at scale**

In 2022, GitGuardian partnered with a large-scale enterprise to help scale its leak prevention efforts using a multifaceted approach. With 7,500 developers and over 50,000 monitored sources, this enterprise needed a solution that was both robust and scalable.

In this section, we'll dive into the deployment of detection, prevention, and remediation at scale. We'll showcase the impact of GitGuardian's services and how they helped the enterprise better protect its sensitive information.

## Prevention

Prevention is a key factor in rolling out a security net at scale. A hard-coded secret becomes more expensive to address the further it penetrates the development lifecycle, as we'll see in the Remediation section. **Preventing secrets from being hard-coded in the first place is the best way to curb the accumulation of security debt over time.**

Secrets detection is most effective **at the pre-commit stage**, which is closest to the moment the code is being written. Remediation usually takes a matter of seconds since the sensitive information has not yet sprawled through other systems.

GitGuardian helped this company progressively deploy pre-commit hooks on its large developer base, with encouraging results: **in 10 months, developers adopting GitGuardian Personal Access Tokens tripled.**

**Personal Access Tokens** are tokens distributed to developers so they can install our secrets scanning solution on their local machine and “fasten their seat belt.”

Measuring shift-left progress and the positive impact of a shared responsibility model on prevention is a valuable approach for assessing the effectiveness of an AppSec program.

While detection is important, it's only part of the story when it comes to security. The other critical piece is remediation, which requires significant efforts to fully address any vulnerabilities or threats that are detected.

## Remediation: more complex than it appears

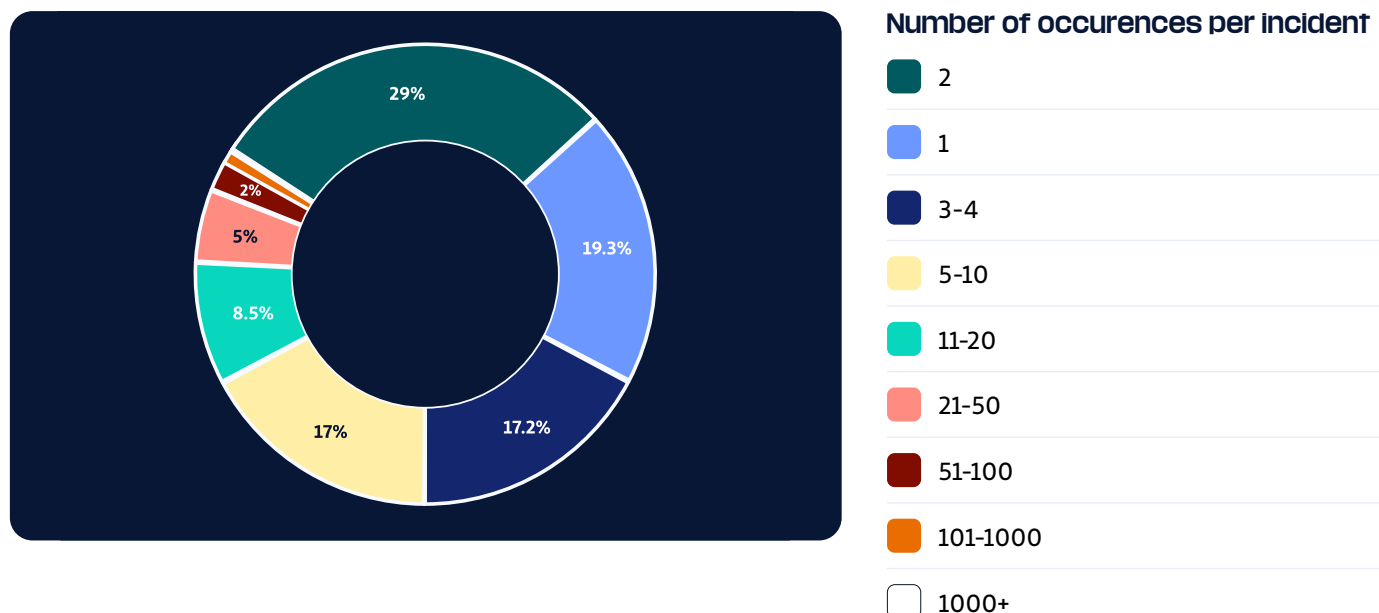
When a leaked secret is detected in central repositories, application security engineers must investigate the incident and prioritize remediation efforts based on the severity. Gathering context is also crucial to making informed decisions on how to proceed. Unfortunately, this process can often be hindered by friction.

To better understand the challenges of remediation, let's review some key metrics.

### Occurrences

---

When analyzing all the business repositories that GitGuardian monitors, we found that the **mean number of occurrences per incident was 41**. However, this figure must be taken with caution due to possible outliers. Nevertheless, this metric underscores the importance of being able to **group leaks into a single unit of work** in order to streamline the AppSec workflow. To better visualize this distribution, the graph below illustrates the number of occurrences per incident.



When examining the incidents detected by GitGuardian, almost half of them can be attributed to one of two causes:

- 2 occurrences due to a deletion commit or
- 1 occurrence due to a hard-coded secret that the author either did not realize or did not care about.

## Files

However, the number of occurrences is just one factor to consider. The dispersion of incidents across multiple files is another complexity factor. **On average, each incident is spread across 3.95 files**, and one-third of incidents occur in multiple files, which adds friction to the remediation process.

## Repositories

In addition, **17% of incidents have occurrences in more than one repository**. This highlights the importance of monitoring all repositories or version control systems to ensure that incidents are not marked as solved in one location while still being exposed elsewhere.

Taken together, these factors demonstrate the need for a comprehensive approach to remediation that addresses **all aspects** of a security incident.

## Scaling remediation with developers' help

The remediation phase is where the bulk of security work is done after a hard-coded secret has leaked. This phase is often more complex than it first appears, and the consequences of a mistake can be significant, such as interruptions to CI/CD pipelines or even production downtime.

To scale remediation efforts effectively, it's crucial to bring security engineers closer to the dev and ops teams. Developers outnumber security engineers and are closest to the code, making them ideally placed to lead remediation efforts. **Enabling developer-driven remediation is a crucial step in securing source code repositories.**

Automation also plays a vital role in streamlining remediation efforts. Automated validity checks and severity assignments support incident triage, and event-driven processes can accelerate security orchestration.

Finally, remediation workflows are highly organization-specific and require security managers to easily provide clear guidance to developers. With the right tools and processes in place, it's possible to streamline remediation efforts and reduce the risk of data leaks and other security incidents.

The risk companies face from the rapid sprawl of API keys, configuration variables, and secrets within engineering teams is immense. **Secrets are the gateway** to a company's most valuable asset, its data. We're at a **critical time** where it's necessary for engineering and security teams to have a holistic secrets strategy. While **sprawl is a problem** most companies experience, it's not a hard one to solve. There are tools available today that natively integrate into developer workflows for managing, orchestrating, and rotating secrets.

Brian Vallelunga  
CEO of Doppler

## Conclusion

This research provides support for what was already suspected: **most senior management in large companies are aware of the risks associated with hard-coded secrets.**

The findings showed that hard-coded secrets were identified as a key risk for 47% of the respondents.

However, addressing this issue is a complex task, **and a one-size-fits-all solution is unlikely to be sufficient** due to the complexity of the problem. Nevertheless, our research also showed that there is a clear willingness among respondents to enhance their development organizations' resilience to secrets leaks. In fact, 94% of respondents are planning to improve their secrets practices in the next 12-18 months.

To address the complex issue of secret leaks in development, a multifaceted approach is necessary, prioritized according to the most sensitive environments.

**The remediation phase is where the bulk of security work is done** after a hard-coded secret has leaked.

This phase is complex and expensive. Enabling developer-driven remediation is a crucial step in securing source code repositories.

At GitGuardian, we have seen firsthand the value of deploying solutions to help reduce the risk of data leaks and protect sensitive information. By deploying secrets detection & remediation capacities, [we are able to help large enterprises reduce the risk of a compromise](#), ultimately saving them valuable time and resources.

If you're interested in improving your organization's secrets management practices, we encourage you to take our [secrets management questionnaire](#) (anonymous) to assess your specific situation. It only takes five minutes to gain a quick overview of your organization's strengths and weaknesses and get started on the path to better security.

To gain a deeper understanding of our proposed maturity model, we recommend reading our accompanying [Secrets Management Maturity Model white paper](#). Additionally, you can learn more about the extent of secrets sprawl on GitHub with the [2023 State of Secrets Sprawl](#).

Finally, If you need guidance or help with DevSecOps, secrets management, or code security, don't hesitate to [contact us](#). Our team of experts is ready to assist you in any way we can.



# About GitGuardian

GitGuardian is a code security platform that provides solutions for the DevOps generation. A leader in the market of secrets detection and remediation, its solutions are already used by hundreds of thousands of developers.

GitGuardian helps developers, cloud operation, security, and compliance professionals secure software development and define and enforce policies consistently and globally across all systems.

GitGuardian solutions monitor public and private repositories in real-time, detect secrets, sensitive files, IaC misconfigurations, and alert to allow investigation and quick remediation. Additionally, GitGuardian's Honeypot module exposes decoy resources like AWS credentials, increasing the odds of catching intrusion in the software delivery pipeline.

GitGuardian is by far



**THE N°1 SECURITY APPLICATION  
ON THE GITHUB MARKETPLACE**

and is trusted by leading companies, including Instacart, Snowflake, Orange, Bouygues Telecom, Iress, Maven Wave, NOW: Pensions, DataDog, and PayFit.

**Learn more about GitGuardian:**

[Website](#)[Public Monitoring](#)[Secrets detection](#)[Honeypot](#)

# Methodology

## About Sapio Research

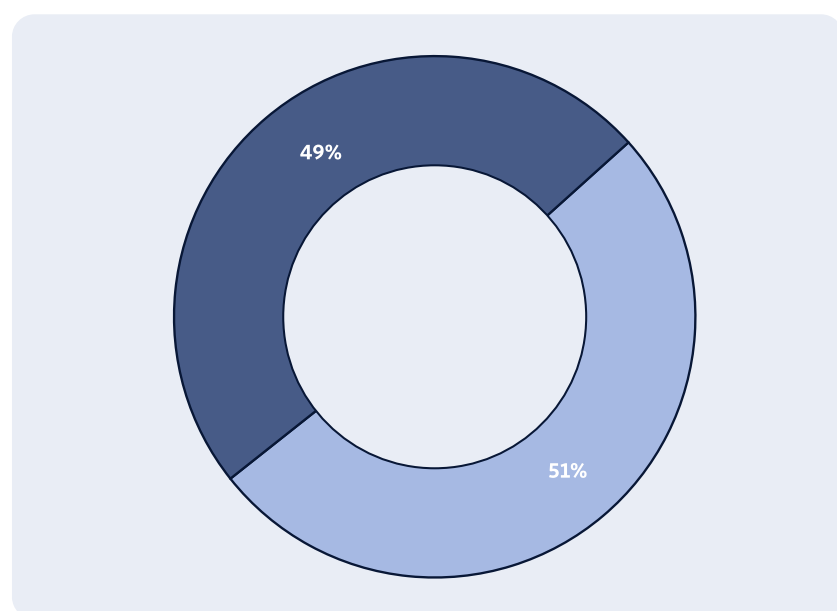
[Sapio Research](#) is an award-winning, international full-service market research consultancy.

Sapio can help in all areas of quantitative and qualitative research and welcome complex, challenging briefs.

They work in the specific fields of audience understanding, brand research, and content research.

## Questionnaire

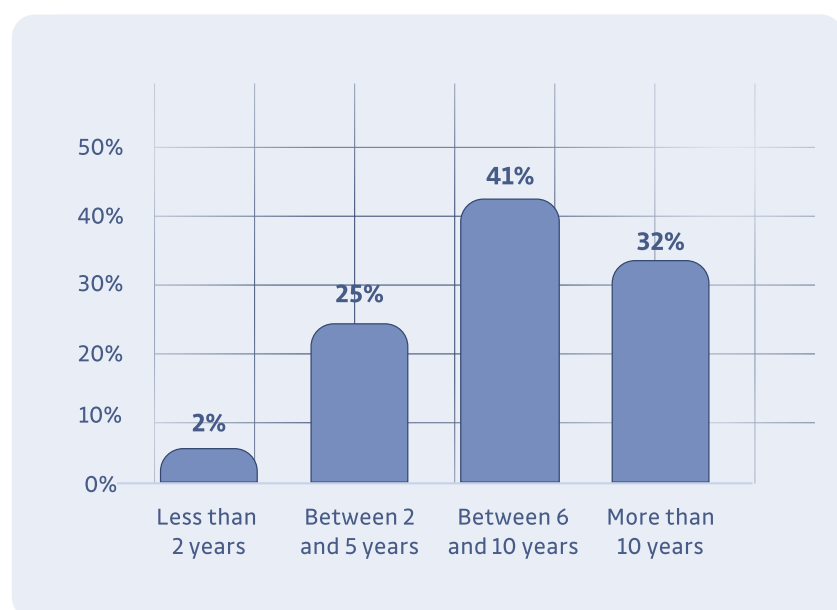
The questionnaire polled **507 IT decision-makers** in the US and the UK working in large enterprises:



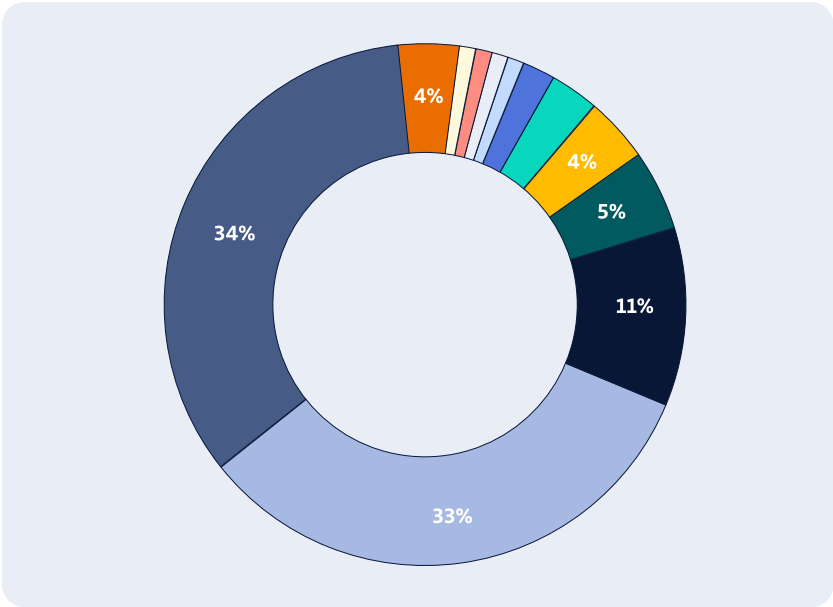
Which country do you live in?

UK

US

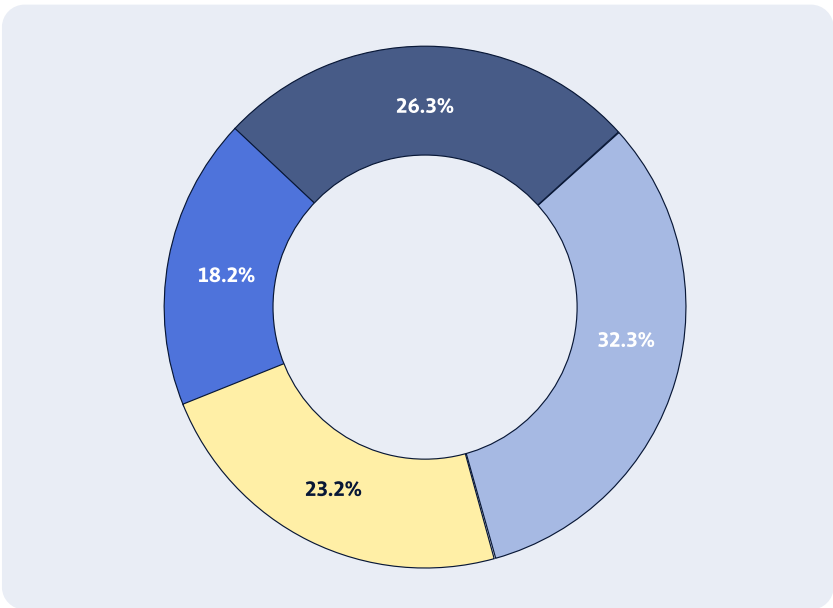


How many years of experience in your role do you have?



Which of the following best describes your current role?

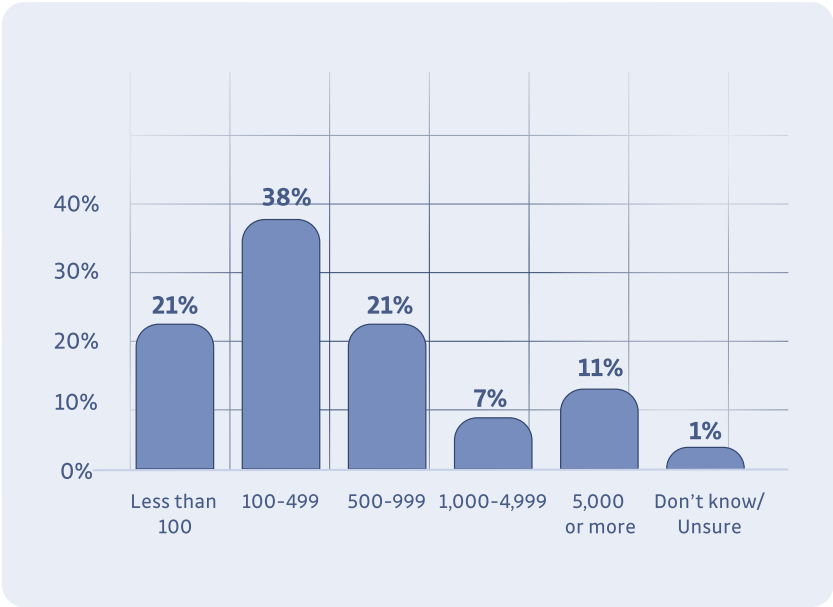
- IT management (e.g., Director of IT, etc.)
- Senior IT management (e.g., CIO, VP of)
- Senior software engineering management
- IT/network architect
- Development team leader
- Senior security management (e.g., CSO)
- Security/security operations management
- Infrastructure operations
- Cloud operations
- Application architect
- Cloud architect
- Other



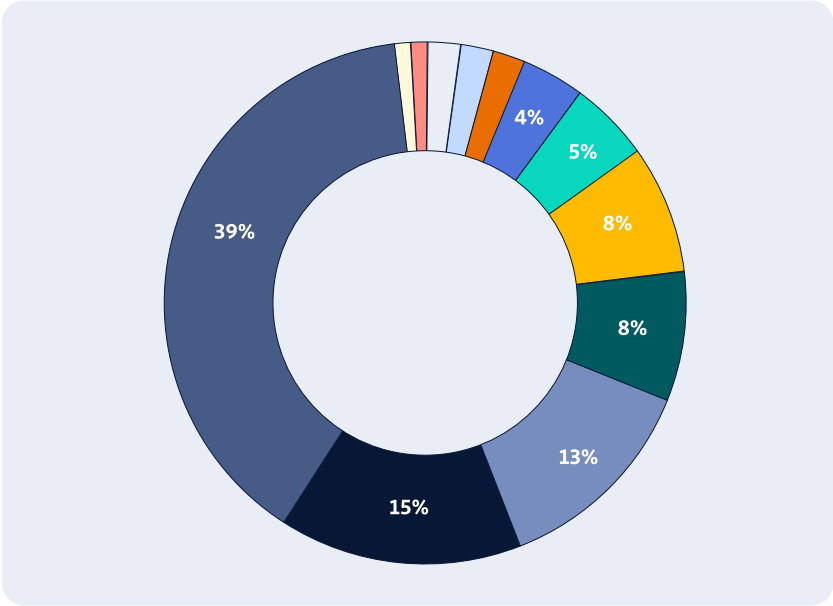
Counting all locations where your employer operates, what is the total number of persons who work there?

- 1,000-2,999
- 3,000-4,999
- 5,000-9,999
- 10,000+

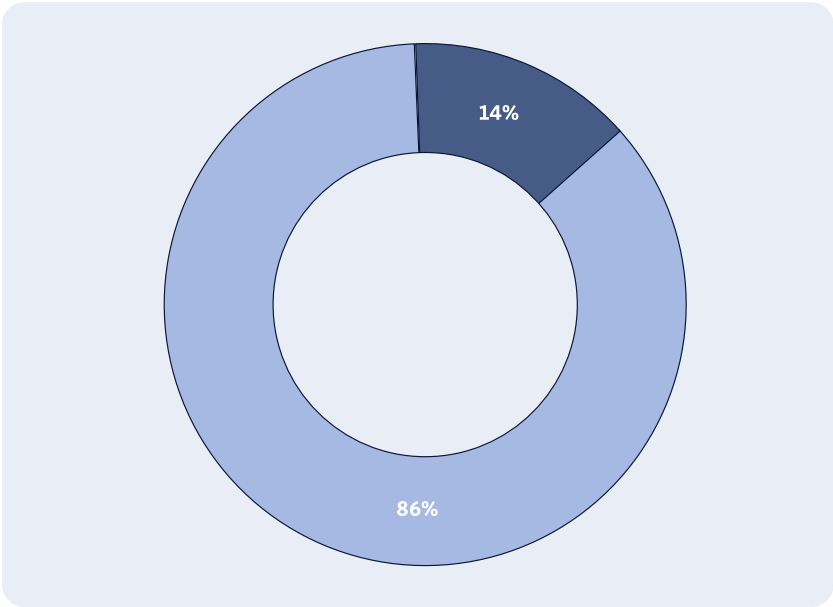
How many people work in software development teams within your business?



Which of the following most closely describes the industry your organization is in?

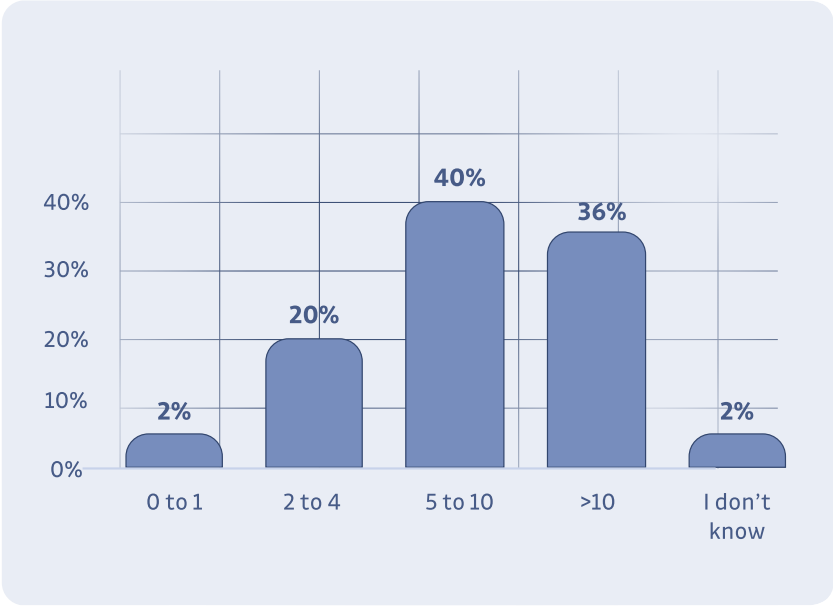


- Software/Technology/Telecommunications
- Manufacturing/Wholesale
- Finance/Insurance/Wholesale
- Hospitality/Retail
- Healthcare
- Transportation/Utilities
- Government/NGO
- Construction
- Other
- Education
- Communication/Marketing/Advertising
- Legal



**Does your organization have an Application Security (AppSec) program in place?**

- ☐ Yes, we currently do
- ☐ We don't at the moment but plan to in the future



**How many people work in Application Security within your business?**

