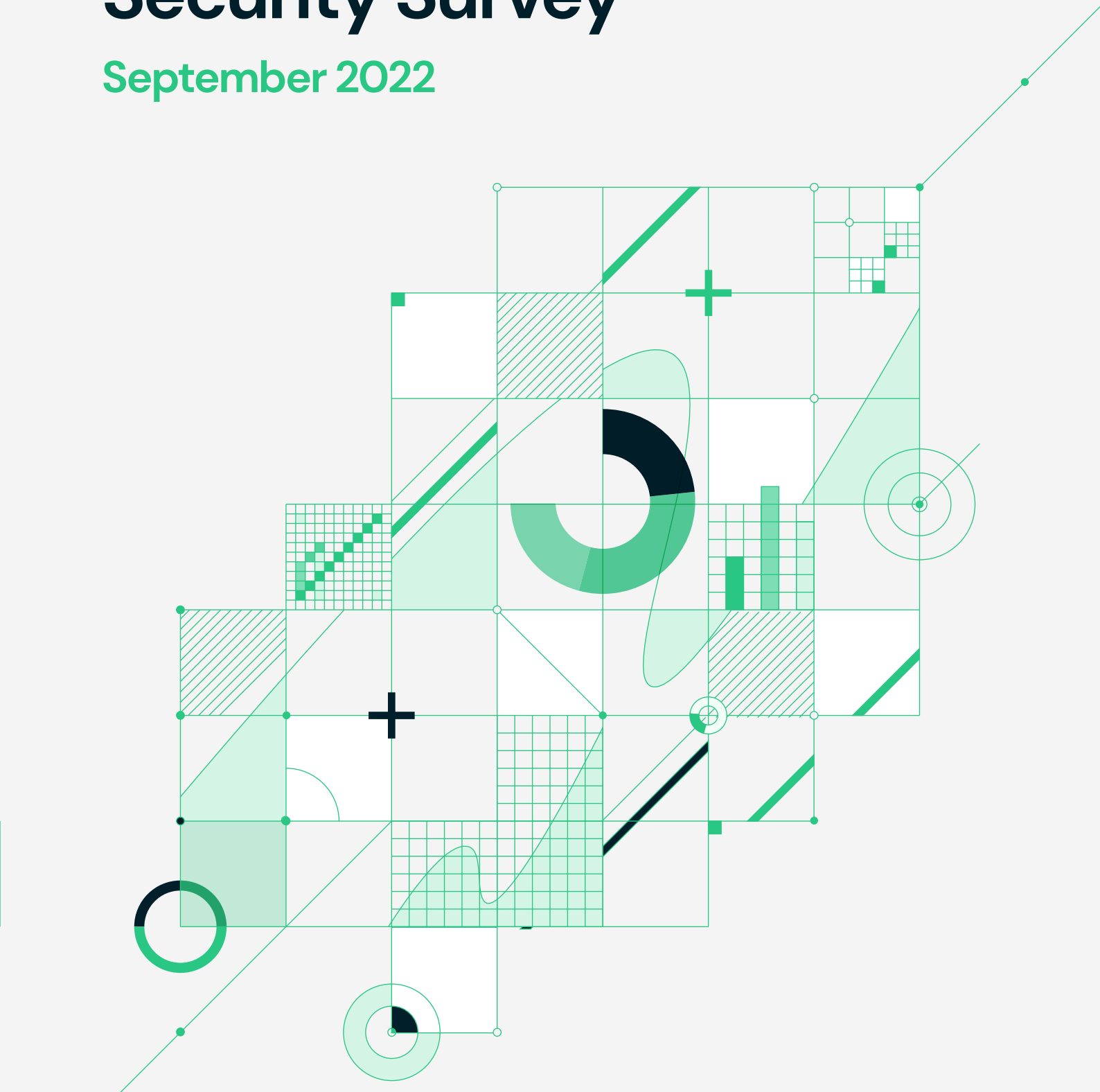
FLOW.

The Annual Cloud Data Security Survey

September 2022



Contents

Introduction and Key Findings

Introduction & Methodology

Remember the days when data security felt simple? Companies held data in one or two places, and this data was mostly static. Today, companies have overwhelmingly made the shift to modern architecture, and workloads are fragmented and dynamic. Not only do businesses have thousands of applications, but the data itself can be held and managed anywhere from databases and data stores to external services like SaaS and other third parties. The data itself is no longer static, and there's no such thing as a finite business environment with a clear perimeter or controls. Suddenly, businesses need to think about what's on the outside as well as their internal data governance and access.

The next big change is the way that organizations navigate and utilize their data. Companies used to send data to production every few weeks, but now it's not uncommon to update or release every day or even every few hours. Each unit of the business now touches sensitive data, and there are more moving parts than ever before to consider.

As market leaders in protecting data in an ever-changing environment, we undertook this survey to analyze these widespread shifts, and to get an insight into how today's security decision-makers are managing and visualizing their data. What are CISO's and security experts priorities when dealing with today's cloud data threats, and how much effort does it take to contain the growing risk? Which security initiatives are top of the agenda, and how is budget being channeled to support data governance and control?

Methodology

To shine a spotlight on these essential security drivers, we commissioned a survey of 200 security decision-makers from the United States and the United Kingdom. The survey was completed by Global Surveyz, an independent survey company, and took place during Q1 and Q2 2022.

The survey is based on Data, IT Security, and Information Security roles from Director level to Senior Management such as VP, Heads of and C-level employees in companies with more than 500 employees. The respondents were recruited through a global B2B research panel, invited via email to complete the survey. The average amount of time spent on the survey was 9 minutes and 47 seconds. The answers to the majority of the non-numerical questions were randomized, in order to prevent order bias in the answers.

Key Findings

1. Almost a third of companies' data is being stored and handled externally

Respondents report that 31% of their environment is based on external services such as SaaS that handle or store their sensitive data. This creates a large gap between what companies can visualize, and what they should be able to visualize — and is a dangerous cloud data security blind spot.

2. CISOs and security experts lack visibility and satisfaction over their sensitive data processes

88% of CISOs say they are investing a high level of effort in discovering network data flows, and 52% are not satisfied with this process. This is unsurprising, as the same percentage of CISOs admit they need to proactively reach out to developers to identify changes to the sensitive data they hold responsibility over, a heavily manual task which is prone to gaps and errors.

3. Cloud security budget is growing, and clear investment priorities have been mapped out

98% of companies increased their cloud security budgets in 2022, and on average these budgets are increasing by 44%. The top area that this extra budget is being channelled towards is insecure interfaces and APIs. In fact, this stood out as the most prominent cloud security threat on the radar this year, with a 70% increase in priority compared to 2021.

4. Monitoring sensitive data sent to external services is the biggest threat on a CISOs and security experts radar

As education spreads about the growing risks of externally held data, CISOs and security experts are placing their attention firmly in this direction. While in 2021, the top threat was seen to be shadow databases, today, just 28% call this out as a top challenge. Instead, the highest priority is monitoring sensitive data sent to external services, as well as insecure interfaces and APIs, sharing the top spot at 52%.

State of Cloud Data Security

Percentage of Production Workloads Moved to the Cloud

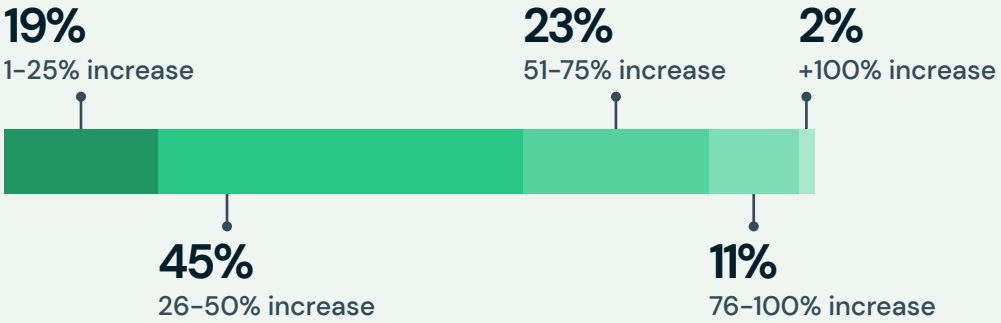
More than half of companies report that more than 80% of their production environment is cloud-native.Modern architecture is becoming ubiquitous in today's businesses, and just 22% have less than half of their workloads in the cloud. Recognizing that we have shared full demographic information on our respondents at the end of this report, we wanted to call out this data as an initial baseline for the survey, to show the status quo for today's production workloads front and center.

78%

of companies have most of their workloads in the cloud

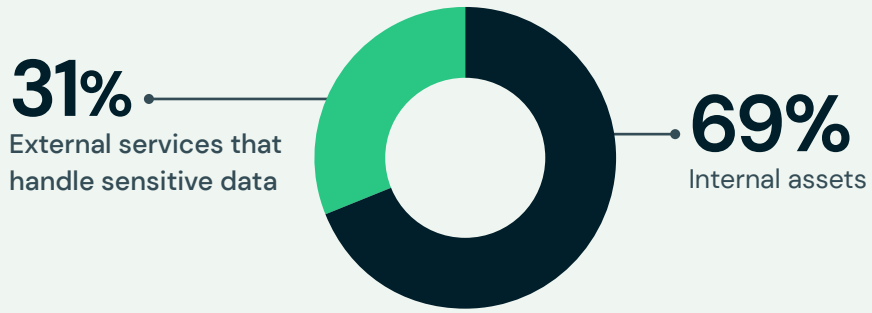
2022 Growth in Cloud Data Security Budgets

98% of companies increased their budget this year for cloud data security. On average, the cloud data security budget will increase by 44% in 2022.



Assets Handling or Storing Sensitive Data

Almost a third of the respondents' (31%) environments are external services handling sensitive data. While companies tend to focus on the data being handled by internal assets, there is a huge blind spot here which is opening them up to risk.

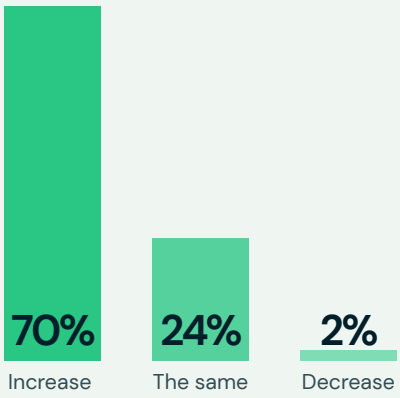


CISOs' and Security Experts Identification of Sensitive Data Related Changes Made in App Environment

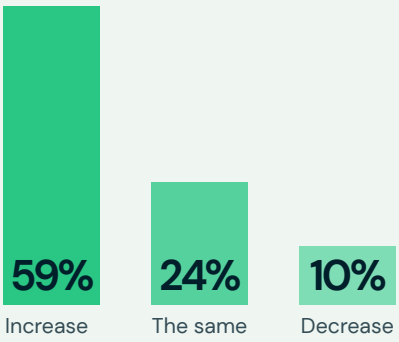
52% of CISOs and security experts need to proactively reach out to developers to identify changes to sensitive data, leaving just 48% of security experts able to identify sensitive data as part of the approval process. CISOs and security experts are heavily dependent on developers to get the information about the data for which they are responsible. This process is prone to errors, heavily manual, and could leave CISOs and security experts with dangerous gaps.

Top Cloud Data Security Threats to Channel Investment, 2022 Vs. 2021

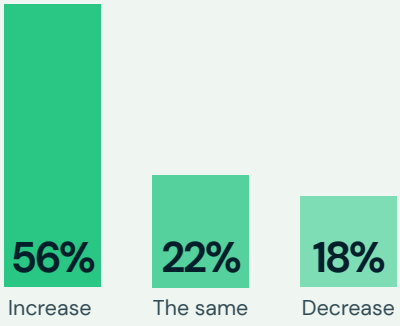
We asked respondents how their investment priorities to combat specific cloud security threats would change in the next 12 months. All investment priorities will increase by at least 50%, showing the growing threat across the board in data security. The biggest increase in priority for cloud data security threats is insecure interfaces and APIs, with a 70% increase. About a fifth (18%) reported a decrease in data access governance threats.



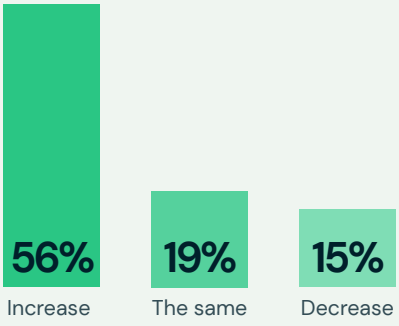
Insecure data flows and APIs



Data stores scanning for sensitive data



Data access governance



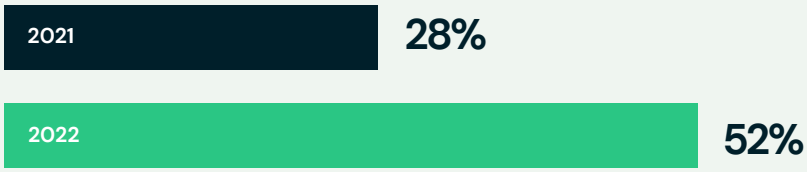
Discovering shadow databases

*Results exclude those answering I don't know. As result, percentages per row will not add up to 100%

CISOs and Security Experts' High Priority Cloud Data Security Threats, 2022 Vs. 2021

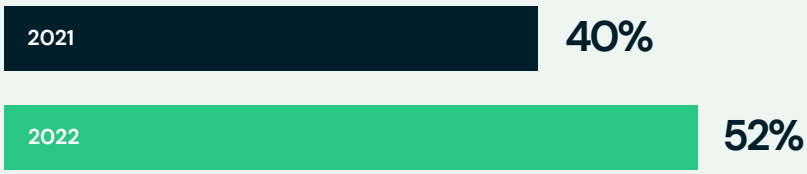
Overall priorities have changed dramatically for CISOs and security experts in the past 12 months. The highest priority in cloud data security in 2022 is monitors sensitive data sent to external services, and insecure interfaces and APIs (52%). This has replaced the biggest threat in 2021 – discovering shadow databases. 52% defined shadow databases as their companies' biggest threat in 2021, but the percentage is just 28% in 2022). Data access governance was only seen as high priority for 28% of respondents in 2021, and today it is called out as a high priority for 48% of CISOs and security experts.

Monitoring sensitive data sent to external services



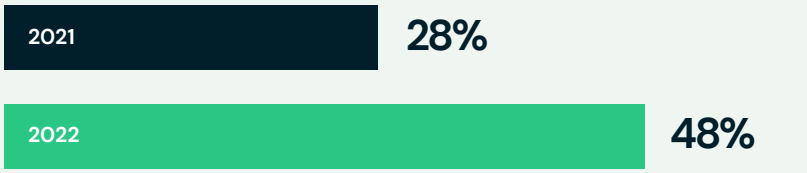
1st Place 2022

Insecure data flows and APIs



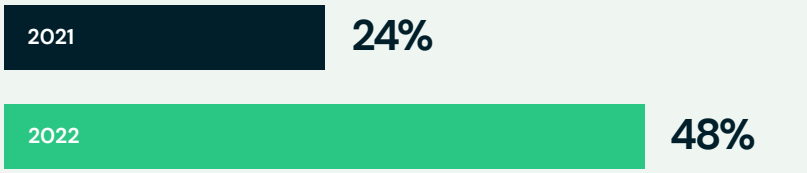
2nd Place 2022

Data access governance



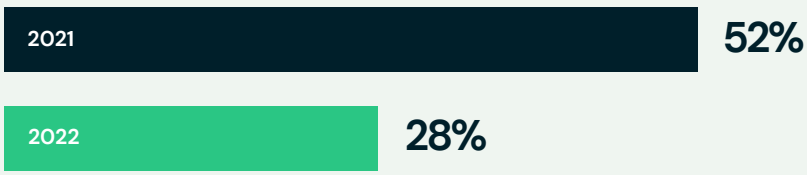
3rd Place 2022

Data stores scanning for sensitive data



4th Place 2022

Discovering shadow databases

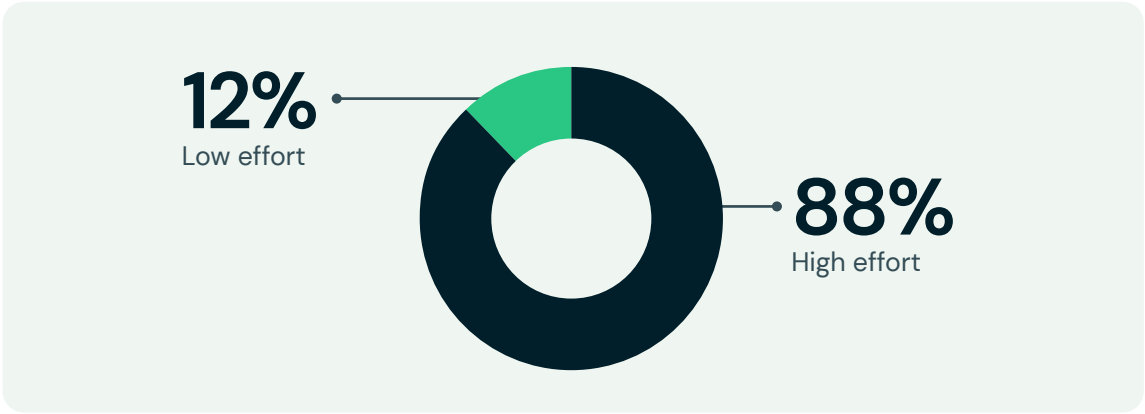


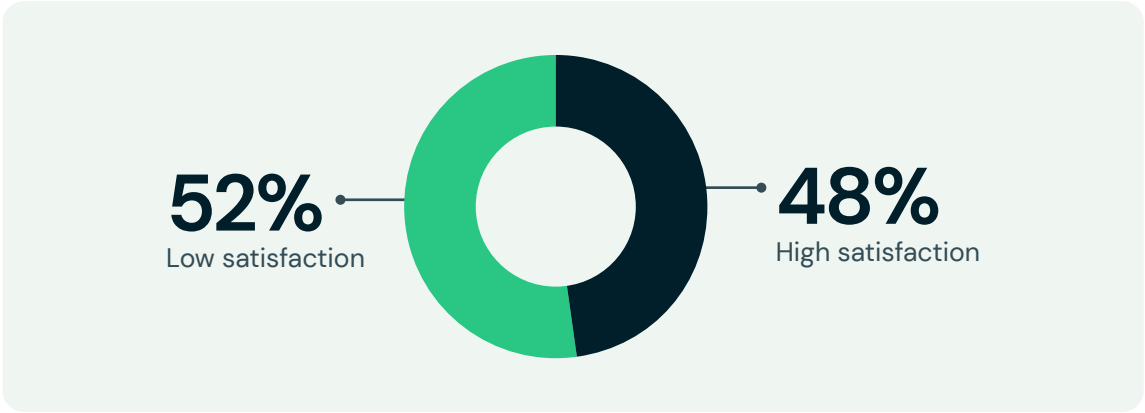
5th Place 2022

*This question allowed more than one answer and as result, percentages will add up to more than 100%

Discovering Network Data Flows — Effort and Satisfation Level According to CISOs and Security Experts

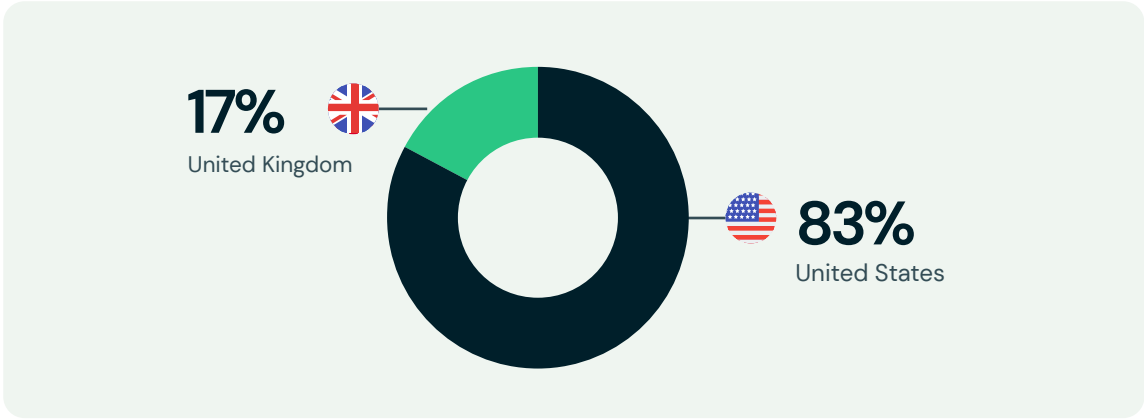
CISOs and security experts were asked how much effort they expended to uncover sensitive data flows within their network. 88% of CISOs and security experts are investing a high level of effort and only 48% say that are satisfied with this model. Security leaders need to look for a less manual approach to discovering sensitive data flows and changes, to avoid blind spots, security gaps and added risk. This would have a direct impact on their overall satisfaction.



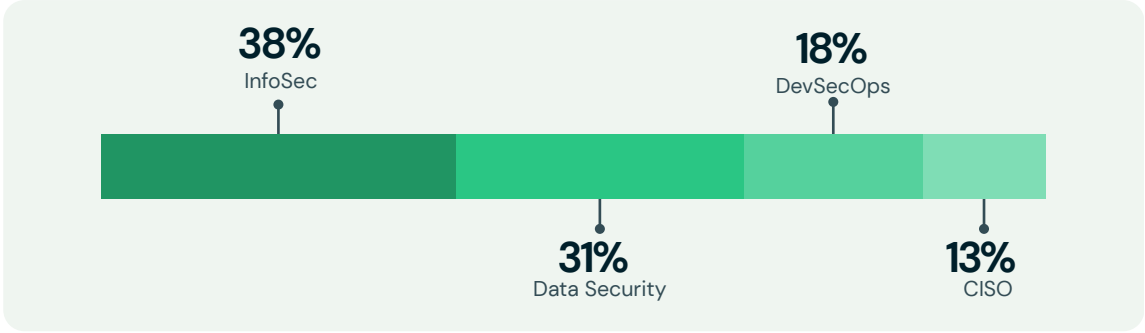


Demographics — Country, Job Role, Seniority and Company Size

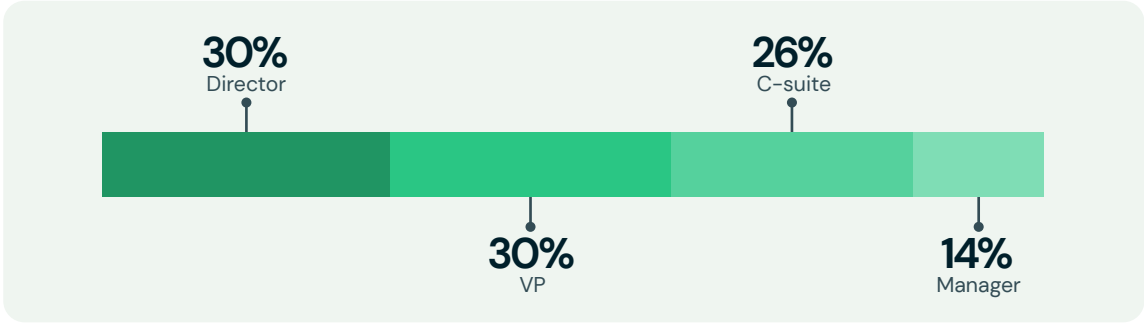
Country



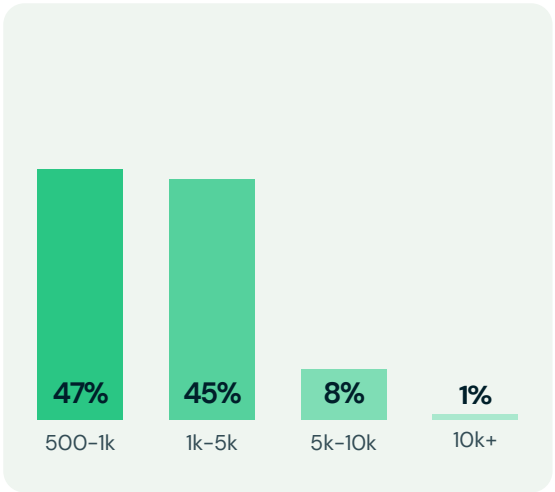
Role



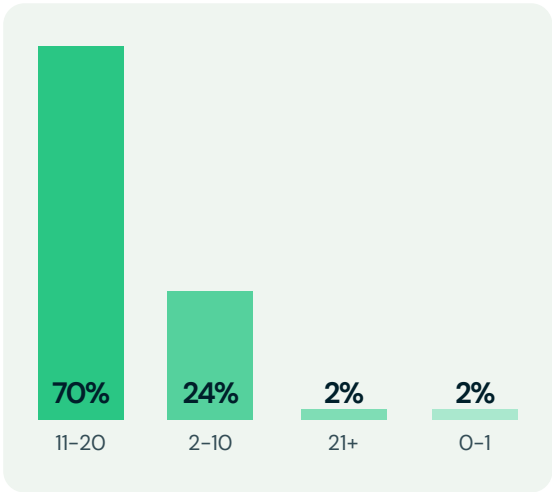
Seniority



Company size (employees)



Number of monthly deployments



Recommendations

Include SaaS providers and unmanaged databases in the scope of your data security posture management

Many companies currently focus their efforts on data discovery, classification, and protection of their managed databases in the cloud. Our data has uncovered that this approach leads to partial results only. To achieve true data security, companies need to extend the scope of their data security efforts to anywhere data can be held. This means adding visibility to unmanaged databases, and also covering external services, who hold a third of today's sensitive data.

Eliminate the human factor in data security posture processes

Manual processes are known to require a large amount of resource investment, and be prone to human error. Despite this, today's most sensitive data discovery and protection processes rely on heavily manual approaches, such as the use of engineering teams. To improve the outcomes of data security, sensitive data discovery and protection needs to be automated, reducing the human factor as much as possible.

Redouble your efforts on protecting against insecure data flows and APIs

The biggest increase in investment priorities among security teams is channelled to protecting against insecure data flows and APIs. This is due to today's chaotic modern application environments which have led to a proliferation of sensitive data, most of which is shared between multiple players. In order to maintain a secure environment without slowing down the development process, we suggest focusing efforts on this growing threat.

Secure Your Data Wherever It Flows

Book a Demo Now

FLOW.

Flow Security's solution

Flow's data security posture management solution discovers and manages all data drifts in your application environment. By mapping **all data owing** through your **internal and external services**, Flow understands where, when, and why **sensitive data is in motion**. Flow's platform allows development and security teams to communicate contextually and in a common language for **faster risk analysis and remediation**.

info@flowsecurity.com

+1 (415) 671-6111

www.flowsecurity.com

Visit Our Website