

Securing the cloud

An industry trend report on cloud security challenges and how to solve them



Sections of the report

Methodology..... 3

Executive summary 4

Key findings..... 5

Supply-chain security..... 6

Incidents and concerns 7

Team skills..... 8

Security practices and budget..... 9

Methodology

This trend report is based on a survey of 501 IT engineers, architects, developers, security managers, and directors. It takes a global perspective by polling quantitatively and qualitatively across the US, Germany, and the UK.

It additionally compares how professionals in each of these markets may differ in their approach to cloud native technologies, while revealing the state of cloud native adoption. The seniority of those polled ranges from c-suite to IT decision makers.

It explores the regulatory push for supply-chain security, identifies potential areas that may become higher priorities in the next 12 months, and delves into organizations' intentions to review their own software supply-chain for increased security. Additionally, it investigates the prevalence of cloud workloads, cloud-related security incidents, and major cloud security concerns.

It touches upon the importance of skills, tools, data integrity, and open source platforms in addressing security gaps and decision-making regarding cloud migration. It concludes with an inquiry into the percentage of IT spending allocated to cloud native security and current cloud security practices employed by organizations.

Executive summary

At SUSE, we recognize that every business is on a journey of digital transformation, and that transformation can be enhanced and accelerated by open source software. ‘Securing the cloud’ trend report tells the story of how cloud security has become a top priority for IT teams in the wake of growing cloud adoption. It explores how widespread use of increasingly complex cloud environments pose significant challenges and concerns as well as examines how professionals are facing these challenges.

The results reveal that 88% of teams have experienced a cloud security incident over the last 12 months. Of this number, 76% experienced multiple incidents, and 11% having had more than 10 issues over the last year.

This contributes to concerns about security holding back cloud technologies, as a further 88% of professionals agree that their teams would migrate more workloads to the cloud and to the edge if they knew their data couldn’t be tampered with.

Respondents in the US identified source-code audibility as a priority (45%), as well as investing more in security technologies. It’s likely this is in response to the [NIS2 directive](#), US NIST SP [800-218](#), and [government memorandum M-22-18](#). In comparison, Germany and the UK are falling behind in terms of source-code auditing priorities (just 23% and 26%, respectively), and spend less on cloud native security.

The results of this report indicate that the growing adoption of cloud native technologies faces security challenges. SUSE is exceptionally prepared to support businesses which are choosing open and looking to transform with the cloud. Cutting-edge companies are already entrusting SUSE with their mission critical needs.



Key findings

88%	of teams have confirmed a cloud security incident over the last 12 months
88%	of professionals agree that their teams would migrate more workloads in the cloud and to the edge if they knew their data couldn't be tampered with
33%	of IT decision makers have increased goals on source-code auditability
35%	of the work of those surveyed is in the cloud
86%	of IT decision makers believe their team has the right skills and/or tools to detect and fix security gaps
36%	of those surveyed say they spend just over a third of their overall IT budget on cloud native security

Supply-chain security

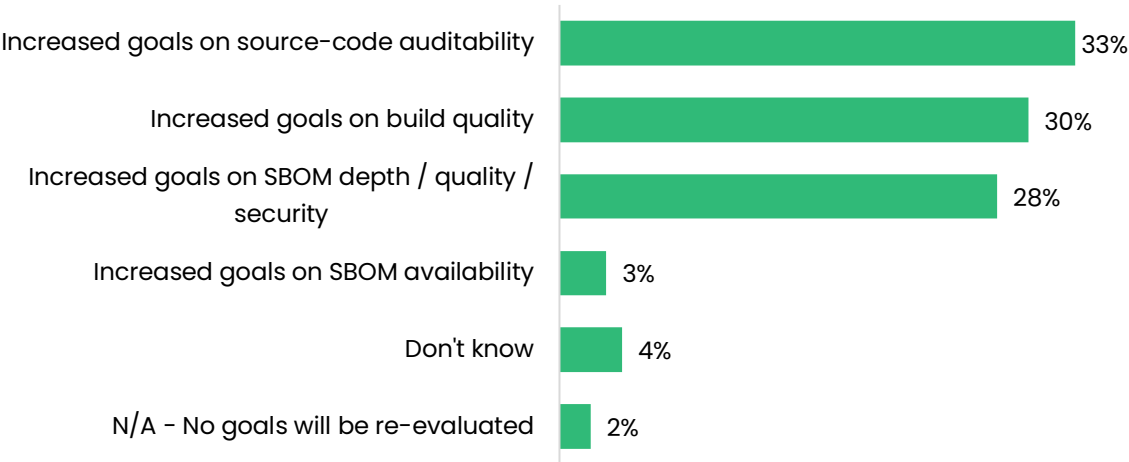
Increased goals on source-code auditability are the top category to be re-evaluated in the upcoming months

Three in ten IT decision makers believe that increased goals on source-code auditability (33%), build quality (30%), or SBOM depth / quality / security (28%) will be re-evaluated upward in the next years to become more of a priority.

Those living in the US believe that goals on source-code auditability (45%) and SBOM depth / quality / security (36%) will be re-evaluated to a significantly greater extent than those based in Europe (24% and 23%, respectively). On the other hand, European respondents (40%) are significantly more likely to believe that goals on build quality will be re-evaluated than US respondents (15%).

The data further varies with respondents' present role in the business. For example, those working as software / network engineers, technical architects, or developers are more likely to believe that goals on source-code auditability will be re-evaluated (46% v 33% average), but less likely to think that goals on SBOM depth / quality / security will be re-evaluated (17% v 28% average).

Thinking about the recent regulatory push for supply-chain security, which of these goals do you think will be re-evaluated upward in the next 12 months to become more of a priority?



Considering recent regulatory changes, the majority (95%) of respondents intend to review their own software supply-chain to increase security. This includes half (51%) who have already reviewed it, rising to nearly seven in ten of those US-based (68%) and three fifths (59%) of software / network engineers, technical architects, or developers, but going down to only two fifths (40%) of those Europe-based.

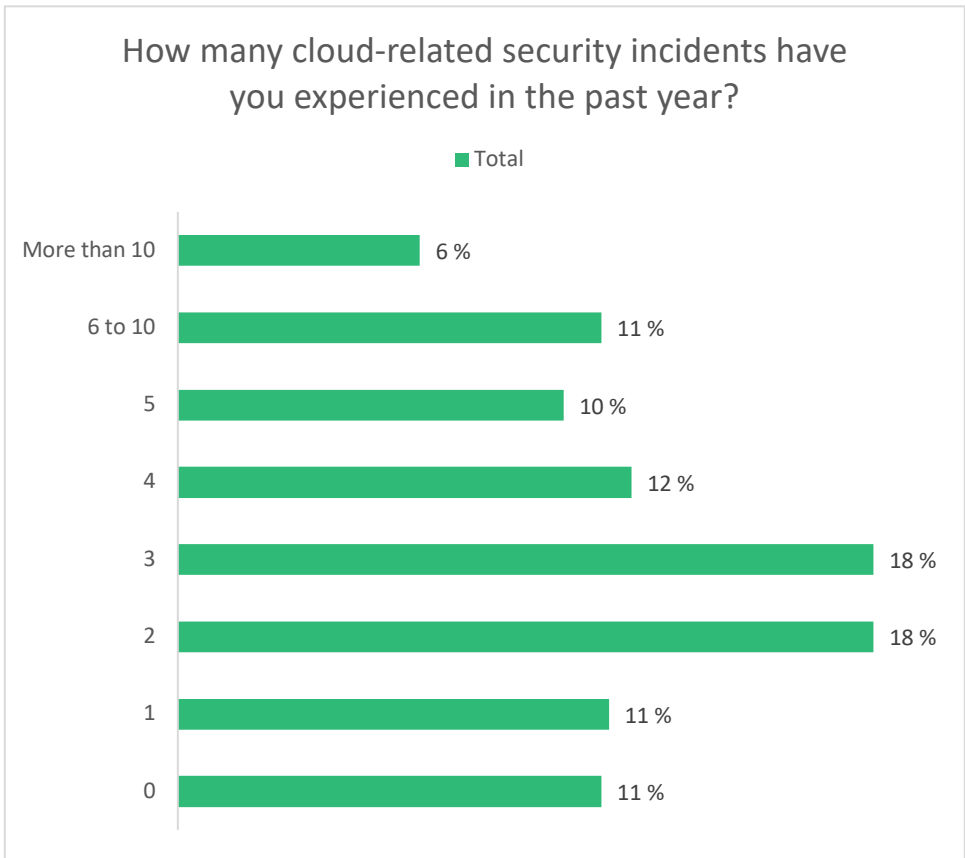
Incidents and concerns

On average, IT decision makers experience 4 cloud-related security incidents yearly

On average, those surveyed say a third (35%) of their work is in the cloud. Interestingly, US-based IT decision makers (37%) have a significantly greater proportion of their work in the cloud than those based in Europe (29%).

IT decision makers have experienced, on average, 4 cloud-related security incidents in the past year, going up to 5 for those in the US and down to 3 for those in Europe.

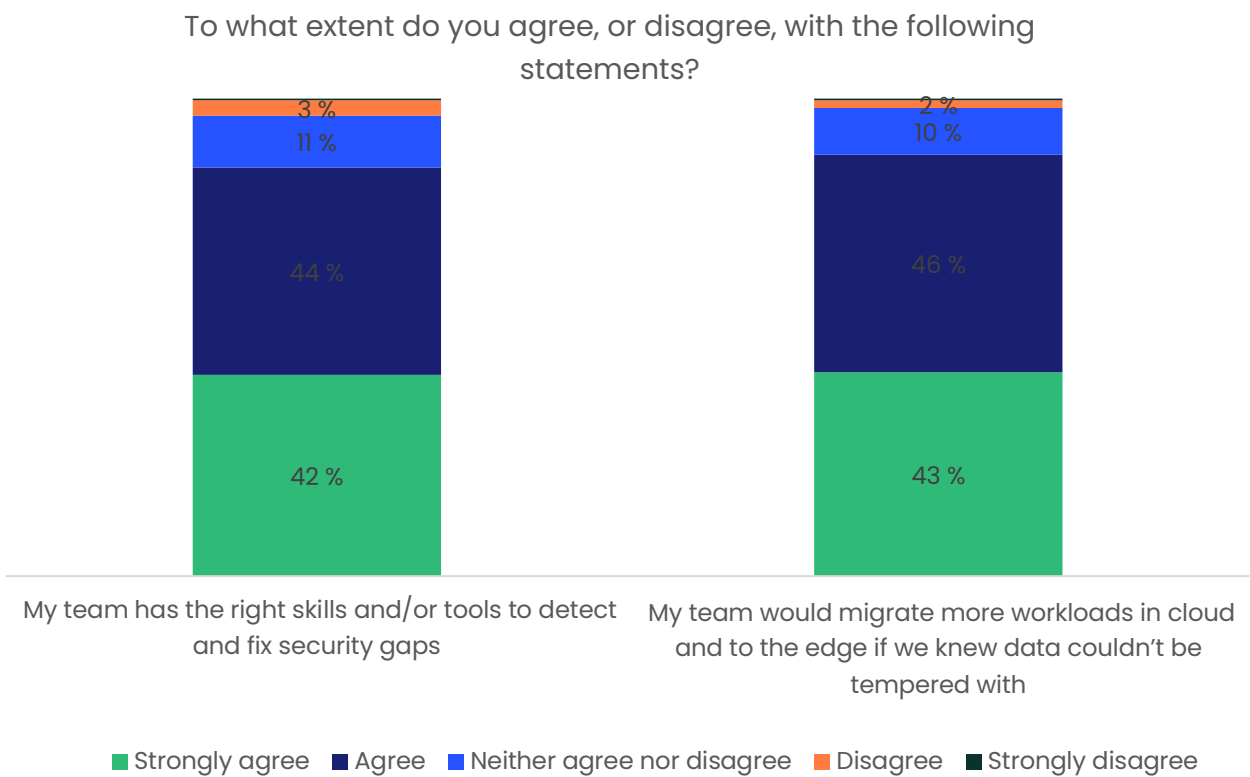
At a total level, the top cloud security concern is data stores hosted by Cloud or 3rd party (31%), followed by runtime attack from hackers, on par with security policy management, federation and automation (29% each). US IT decision makers (35%) are significantly more likely to believe that security policy management, federation and automation are one of their biggest cloud security concerns than those in Europe (25%), while this represents the biggest worry for software / network engineers, technical architects, and developers (35%).



Team skills

The majority trust their team when it comes to fixing security issues

Nearly nine in ten (86%) believe their team has the right skills and / or tools to detect and fix security gaps. This is significantly higher for US (90%) than European (83%) respondents. In addition, a similar proportion (88%) would migrate more workloads into the cloud and to the edge if they knew data couldn't be tempered with.



Security practices and budget

Over a third of IT budget is spent on cloud native security

On average, those surveyed say they spend just over a third (36%) of their overall IT budget on cloud native security. This is significantly higher for US (42%) than European (33%) respondents.

When it comes to the cloud security practices currently used, security automation and container firewall are the most popular overall (38% each), followed by security policies and management tools provided by Cloud vendor (36%), and security policy automation (34%). Interestingly, there are numerous cloud security practices that are significantly more popular amongst US-based IT decision makers compared to those in Europe, including CSPM, CWPP, CNAPP solutions (42% v 26%), free / paid observability or security tool (33% v 24%), PSP / PSA policies (31% v 22%), Kubernetes network policies (32% v 15%), and free CVE / paid scanner (26% v 18%).

