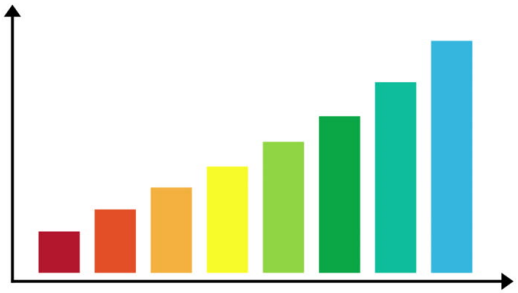
The State of Cloud Security: How Does Your Organization Compare?

Introduction

- We've seen an increasing number of data breaches and incidents related to cloud
  - S3 buckets galore
  - Open Kubernetes APIs: Cryptomining!
  - Microsoft's outage in 2019
- Has the state of cloud security changed?
  - More controls? Better processes?
- Believe it or not, there's some good news this year

About the Survey

- Several hundred respondents
  - In tech, finance/banking, cybersecurity, and more
- A wide range of small, mid-size and large/large++ organizations
- A broad array of roles responded:
  - Architects, ops, and executives
- Most responses from the US, Europe, and Asia



Key Findings from 2019

Analyst Program

- A significant increase in unauthorized access by outsiders into cloud environments or to cloud assets;
  - 31% of organizations in 2019, in 2017 this was only experienced by 19% of organizations

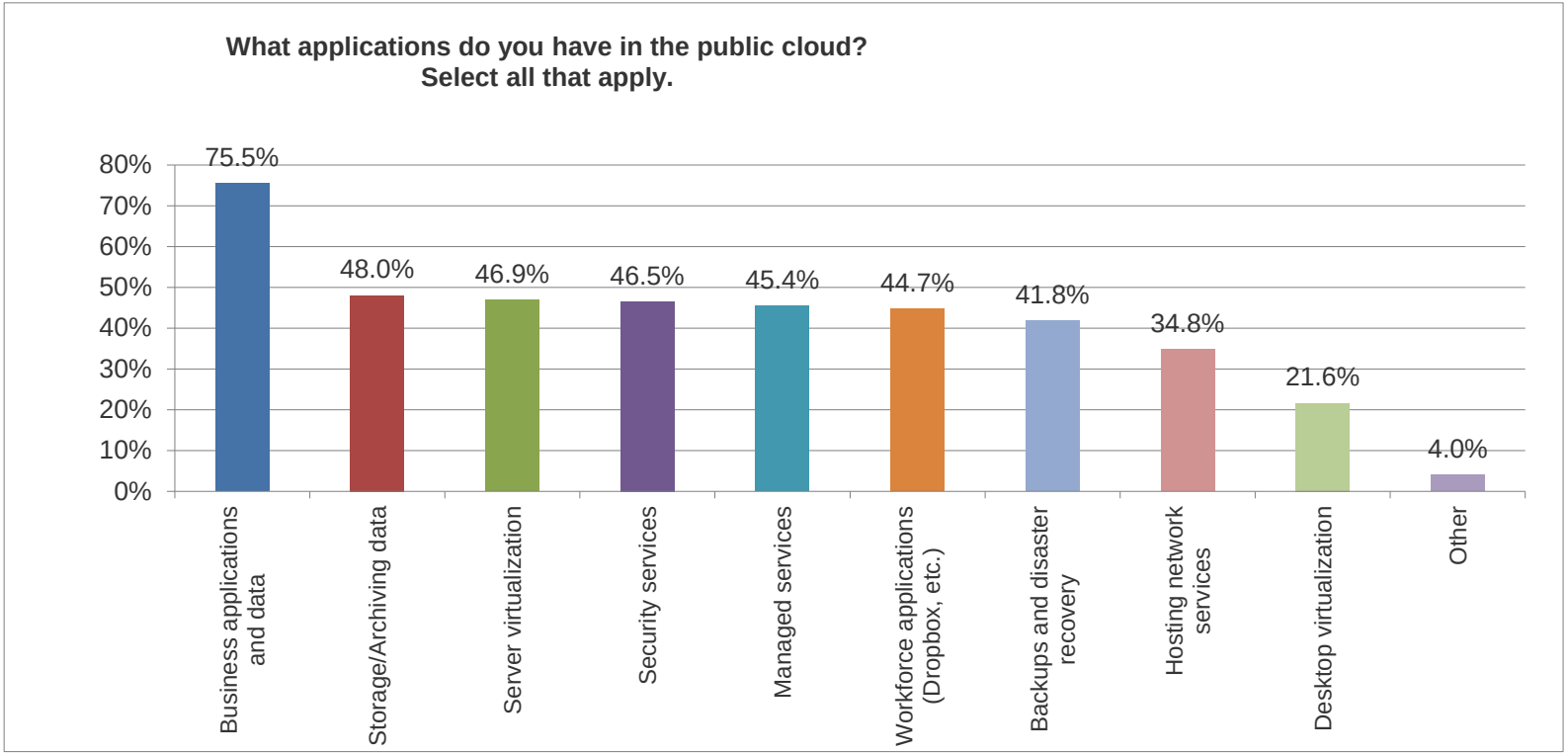
- More than 55% of respondents stated that they were frustrated trying to get low-level logs and system information for forensics in 2017, and only 30% said as much in 2019

- ISO 27001 reports continue to be the most valuable audit reports made available by cloud providers, and more organizations are able to perform pen tests of their cloud provided environments than in the past.

What We're Using in the Cloud

- Business apps and data top the list (76%)
  - Big drop in the use of workforce apps such as Dropbox.
  - Only 45% said they were using such apps today versus 84% in 2017
- Overall storage/archival of data: 48%
- Server workloads: 46.9%
- Security services: 46.5%

What We're Using in the Cloud

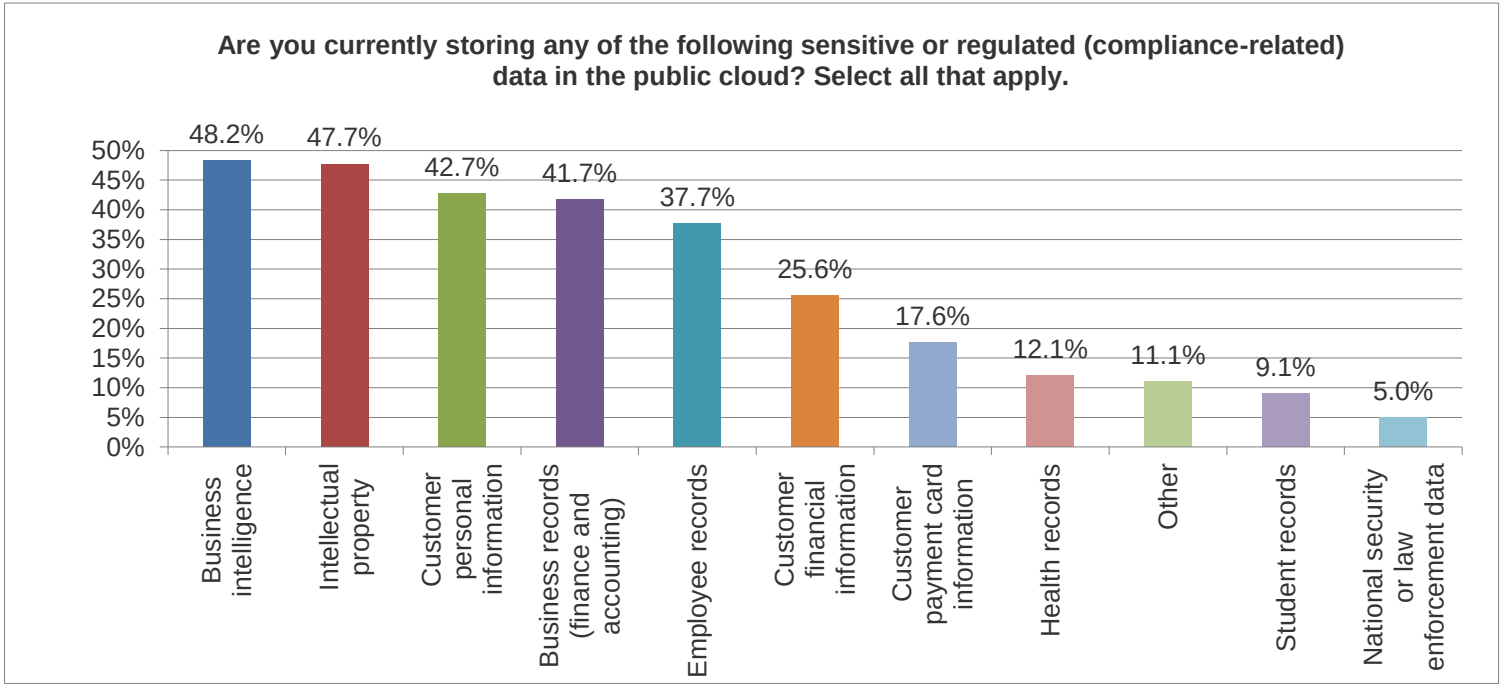


More Stats on Cloud Use

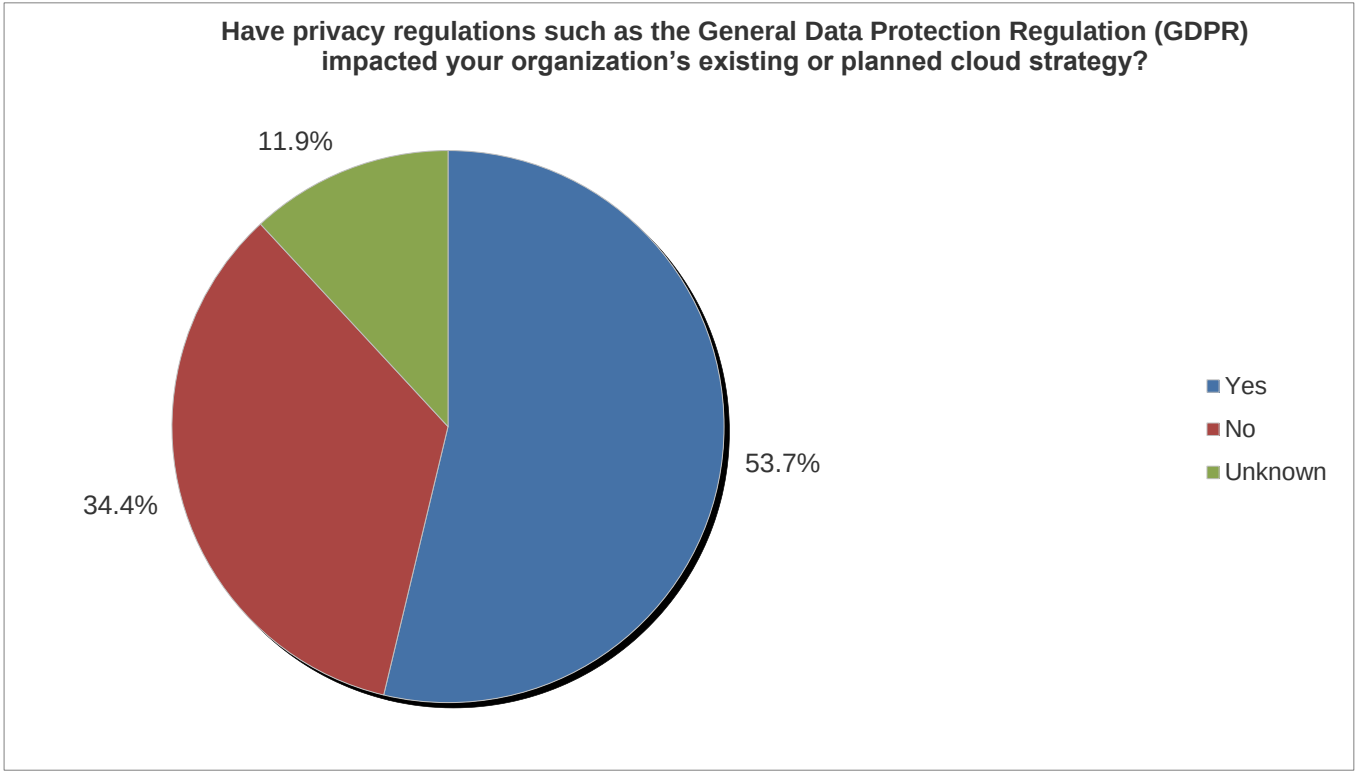
- Top number of cloud providers: 2-3
  - Consistent from 2017-2019
  - Roughly 1/3 of respondents
- A higher percentage of respondents were using only one provider in 2017 (17%) versus today (16%)
- 7.4% use more than 20 cloud providers
  - 4% in 2017

Sensitive Data in the Cloud

- Short answer: Yes

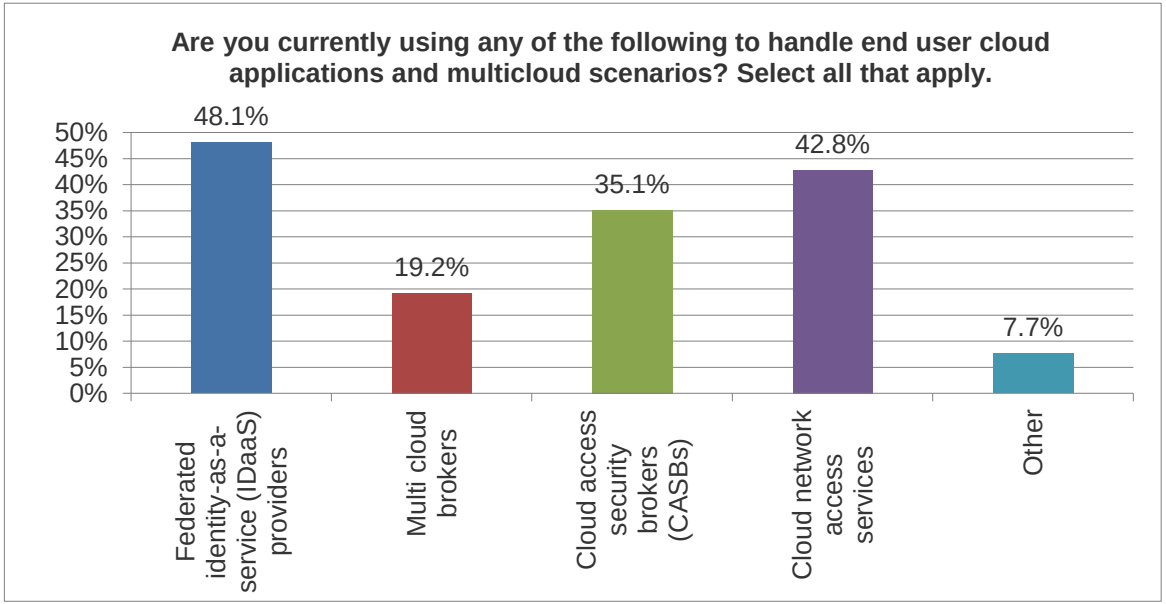


Privacy: A Growing Concern



New Security Tools in the Cloud?

- Are organizations using more cloud-centric security technologies?



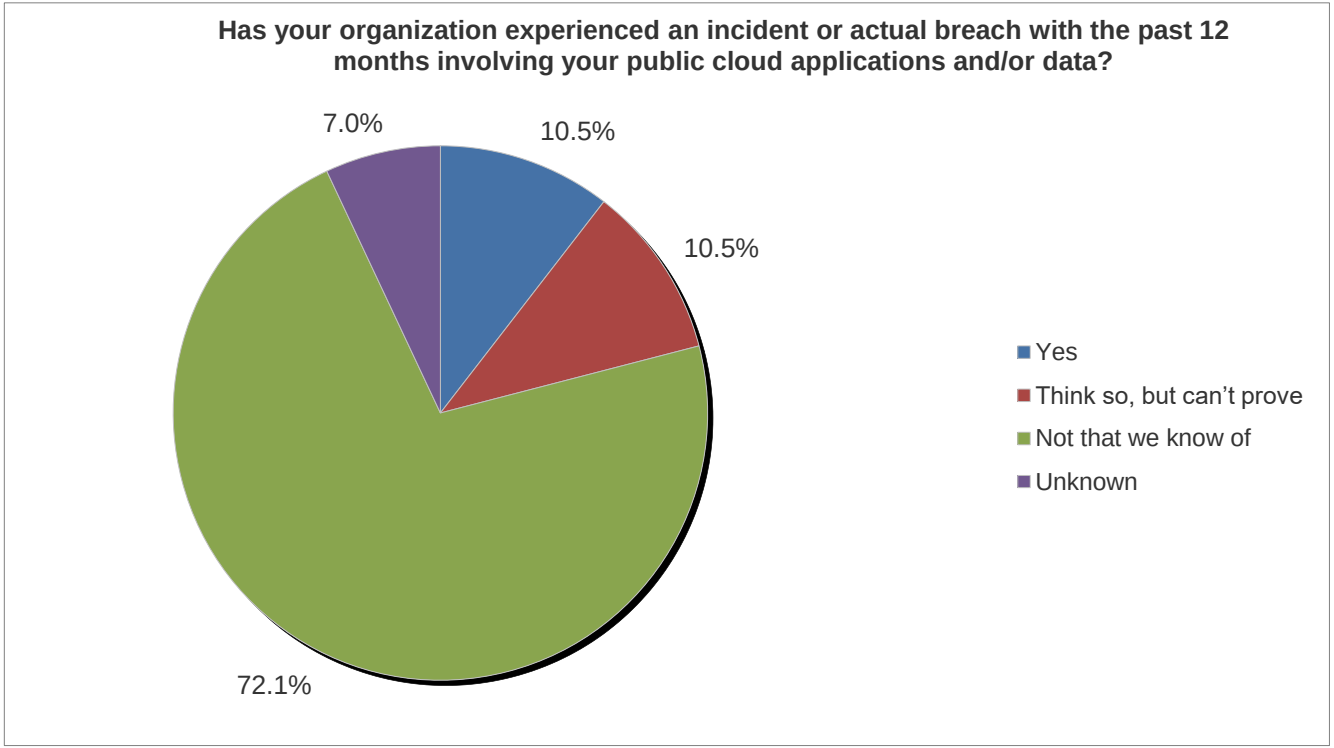
Concerns and Threats in the Cloud

- As in 2017, unauthorized access to data by outsiders topped the list of concerns at 56% (slightly lower than in 2017 but still the highest category).
- In second position, inability to respond to incidents (52%) moved up from seventh position in 2017, where 48% chose this concern.
- Other major concerns was were lack of visibility into what data is being processed and where (51%, up from 48% in 2017) and unauthorized access to data from other cloud tenants at 50%, also (very similar to our responses in 2017

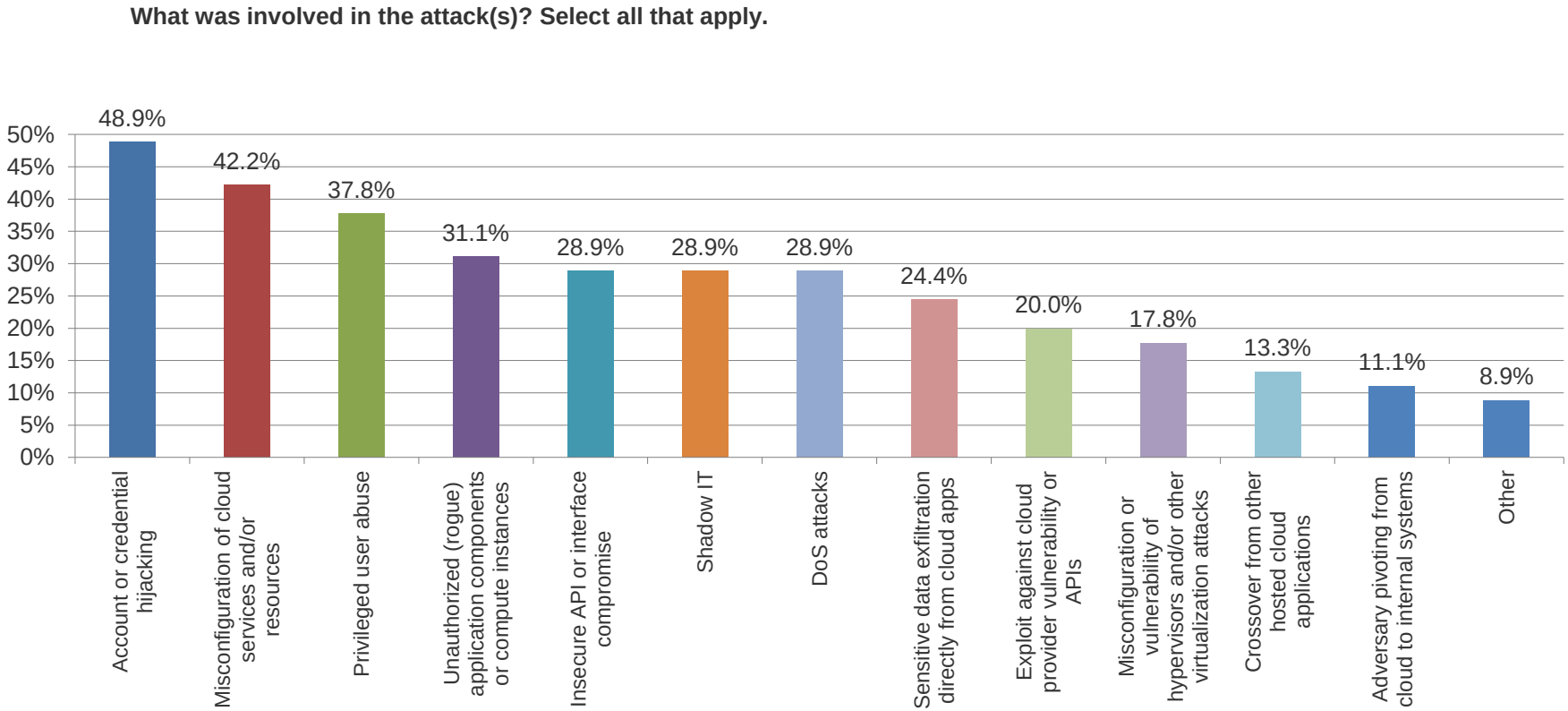
Concerns and Threats in the Cloud

- For the issues that were actually realized, downtime was fairly consistent from the last survey (up slightly from 18% to 21%).
- The biggest change overall this year was a significant increase in unauthorized access by outsiders at 28%—in 2017 only 12% of respondents' organizations reported this problem.
- We also saw an increase in misconfiguration issues with application components and APIs.

Actual Breaches in the Cloud



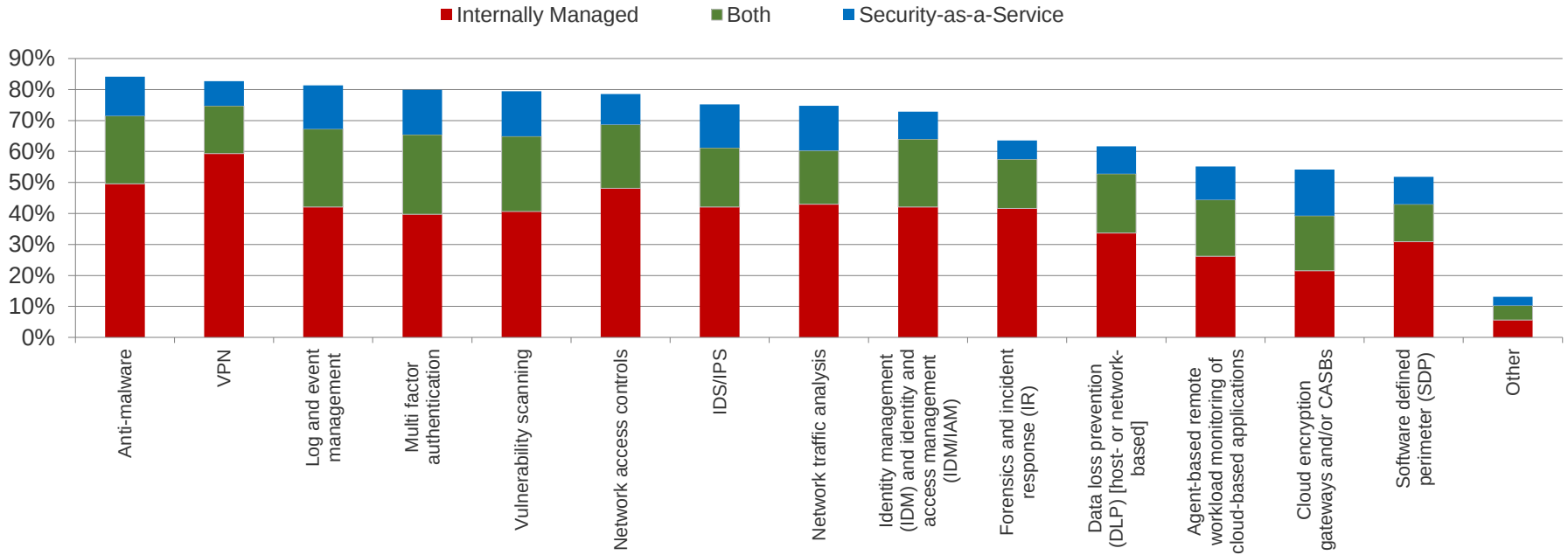
What was Involved?



Cloud Security Controls in Use

Analyst Program

Which of the following technologies have you successfully implemented to protect sensitive data and access in your public cloud environment(s), whether internally managed and/or in the form of Security-as-a-Service?



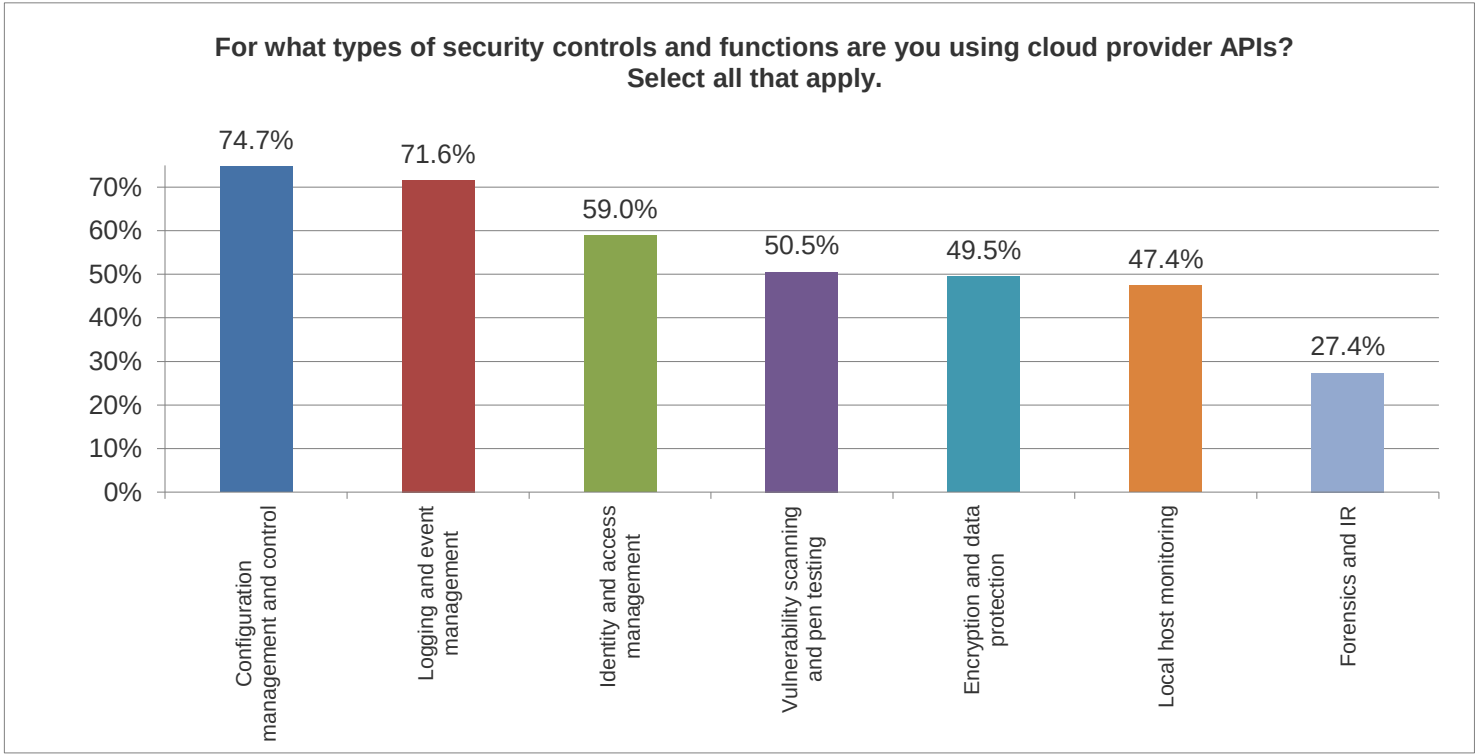
Key Takeaways: Controls

- the majority of controls across the board are still being managed internally
- Growth: CASBs and encryption gateways (as much as 18% for hybrid management) and identity management solutions (as much as 22% in hybrid management)
- Altogether, the numbers are low!

More Cloud Maturity?

- **Positive**: Today, 68% of organizations have cloud security and governance policies in place,
  - Up from 62% in 2017
  - 24% stated that they didn't, and 8% weren't sure
- **Negative**: Only 44% of respondents stated they were leveraging cloud provider APIs in the cloud to implement security controls (a critical element of automation and cloud security maturity)
  - Almost unchanged from 2017 (43 %)

Use of CSP APIs…

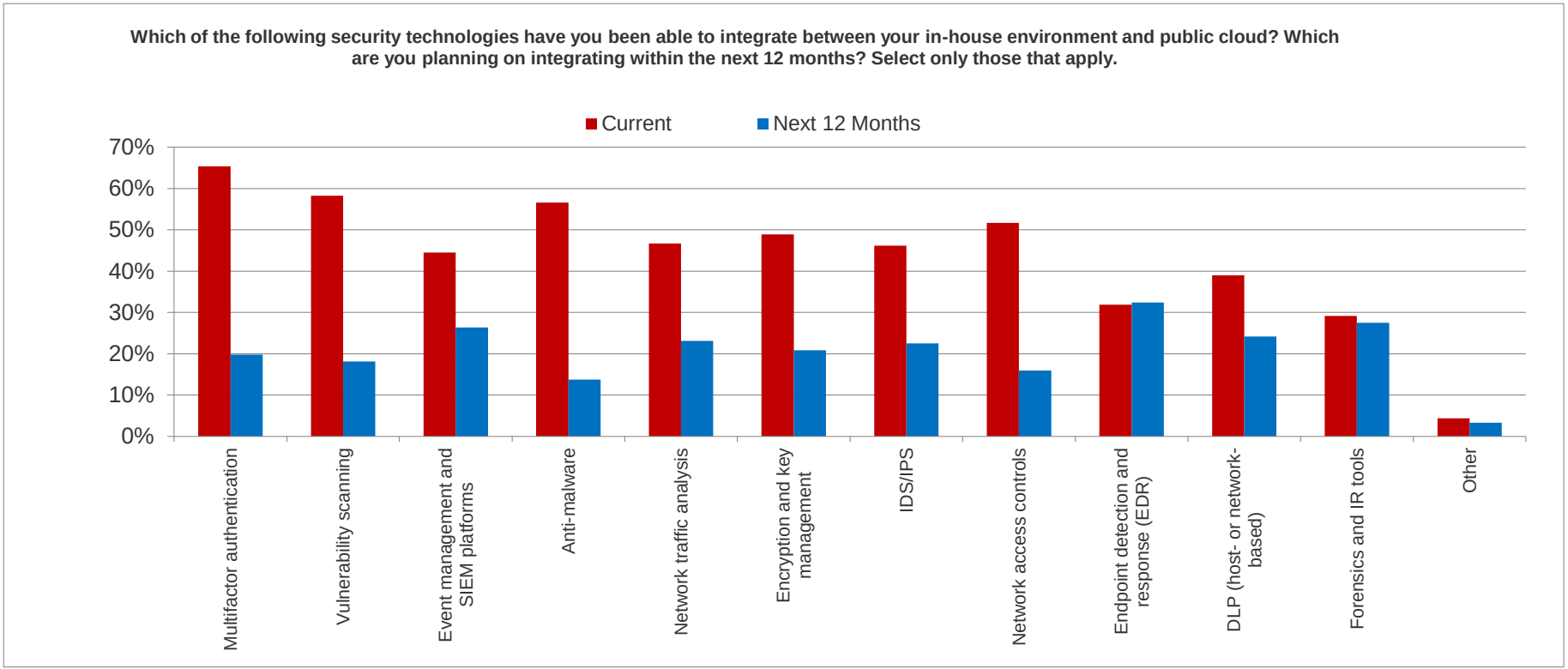


Controls Integration

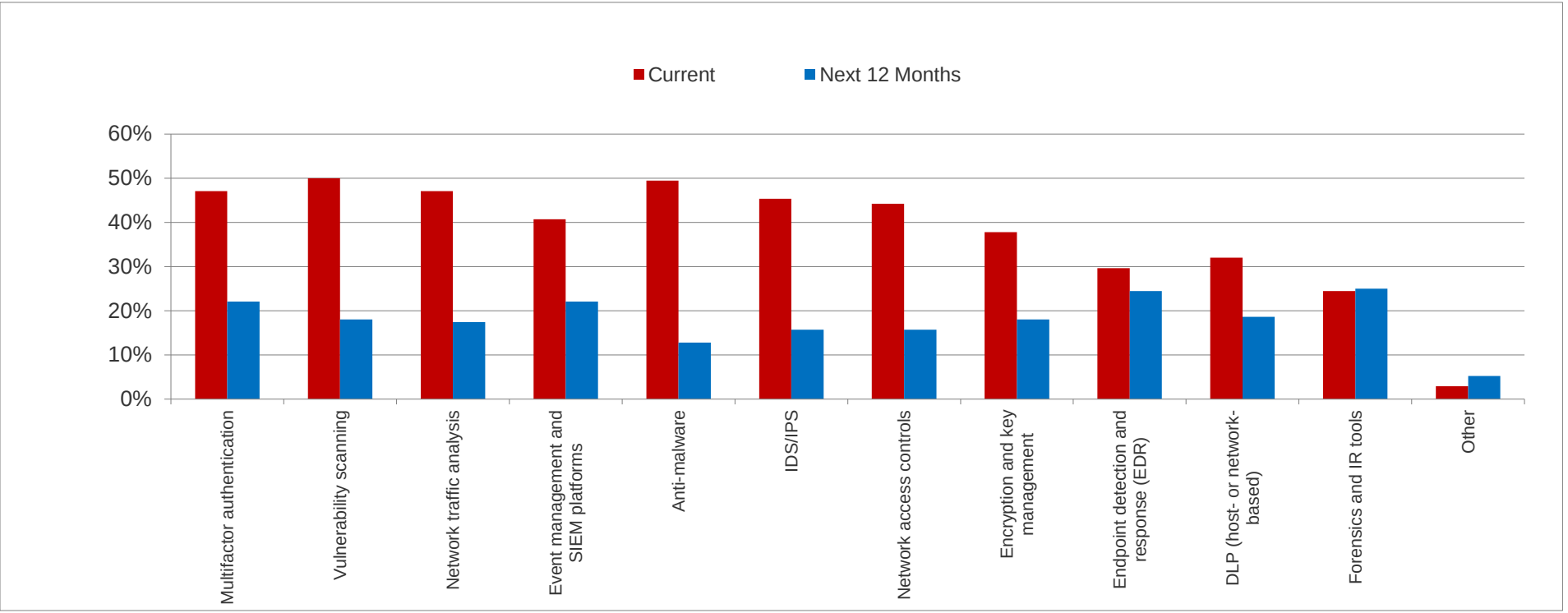
- More than 50% have integrated network access controls (52%) and47% have integrated network traffic analysis
- Another 45% have integrated SIEM and event management tools, too
- Future Controls:
  - Endpoint detection and response (EDR) tools (32%)
  - Forensics and IR tools (28%)
  - Event management once again with 26%

Controls Integration

Analyst Program



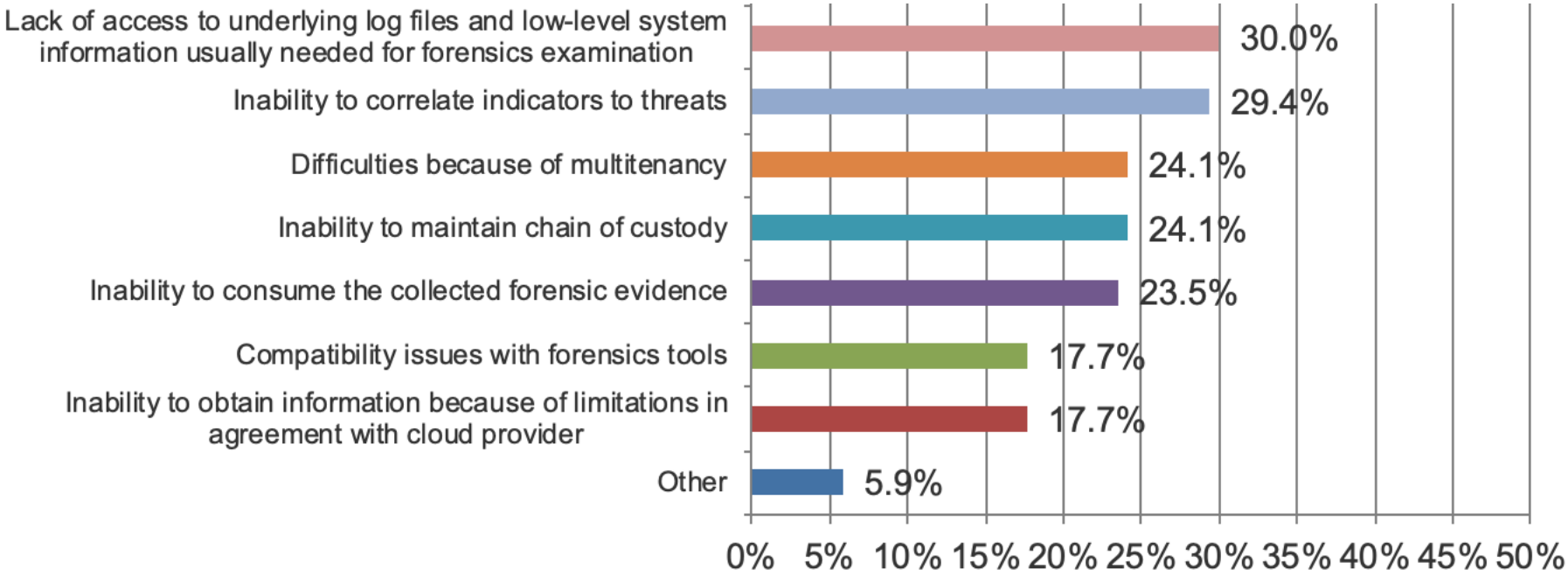
Single Vendor Options?



IR and Forensics Challenges

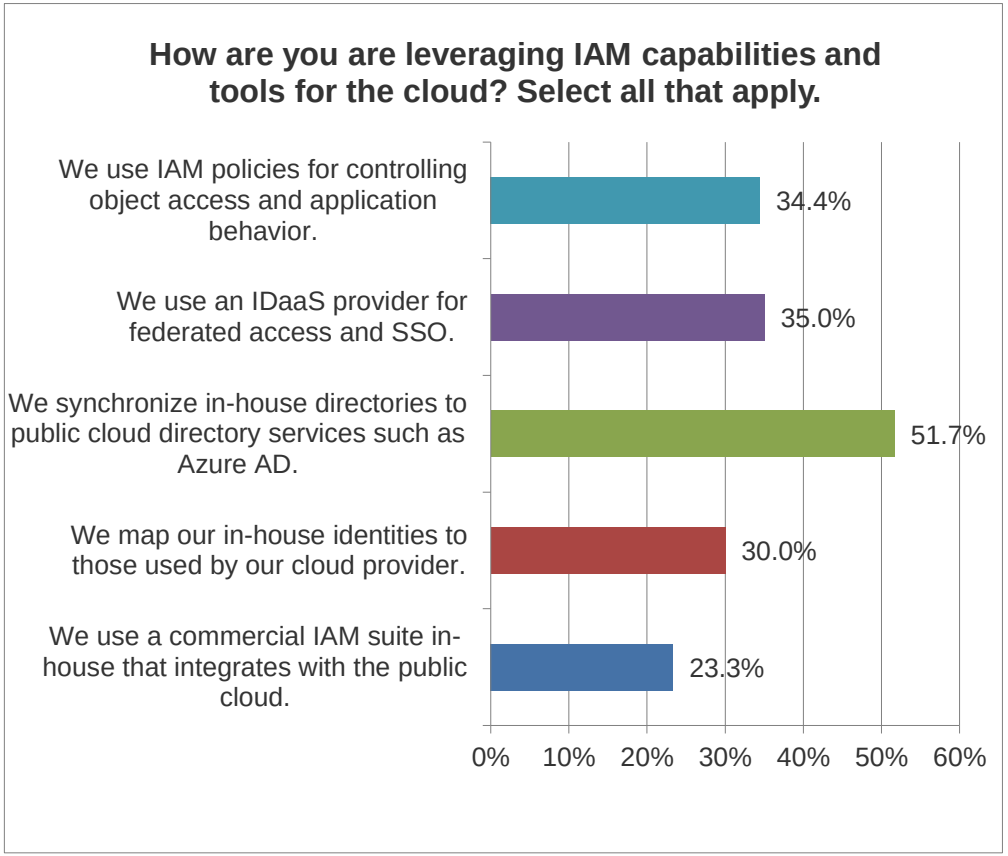
- Biggest challenge: A lack of real-time visibility into events and communications involved in incidents
  - EDR tools and network “taps” may help
- Other major challenges cited include:
  - Difficulty correlating events between on-premises and cloud environments
  - Immature forensics and IR processes
  - Inability to acquire forensic evidence
  - Also: Getting logs and low-level system data (55% in 2017 vs 30% today)

Additional IR & Forensics Challenges

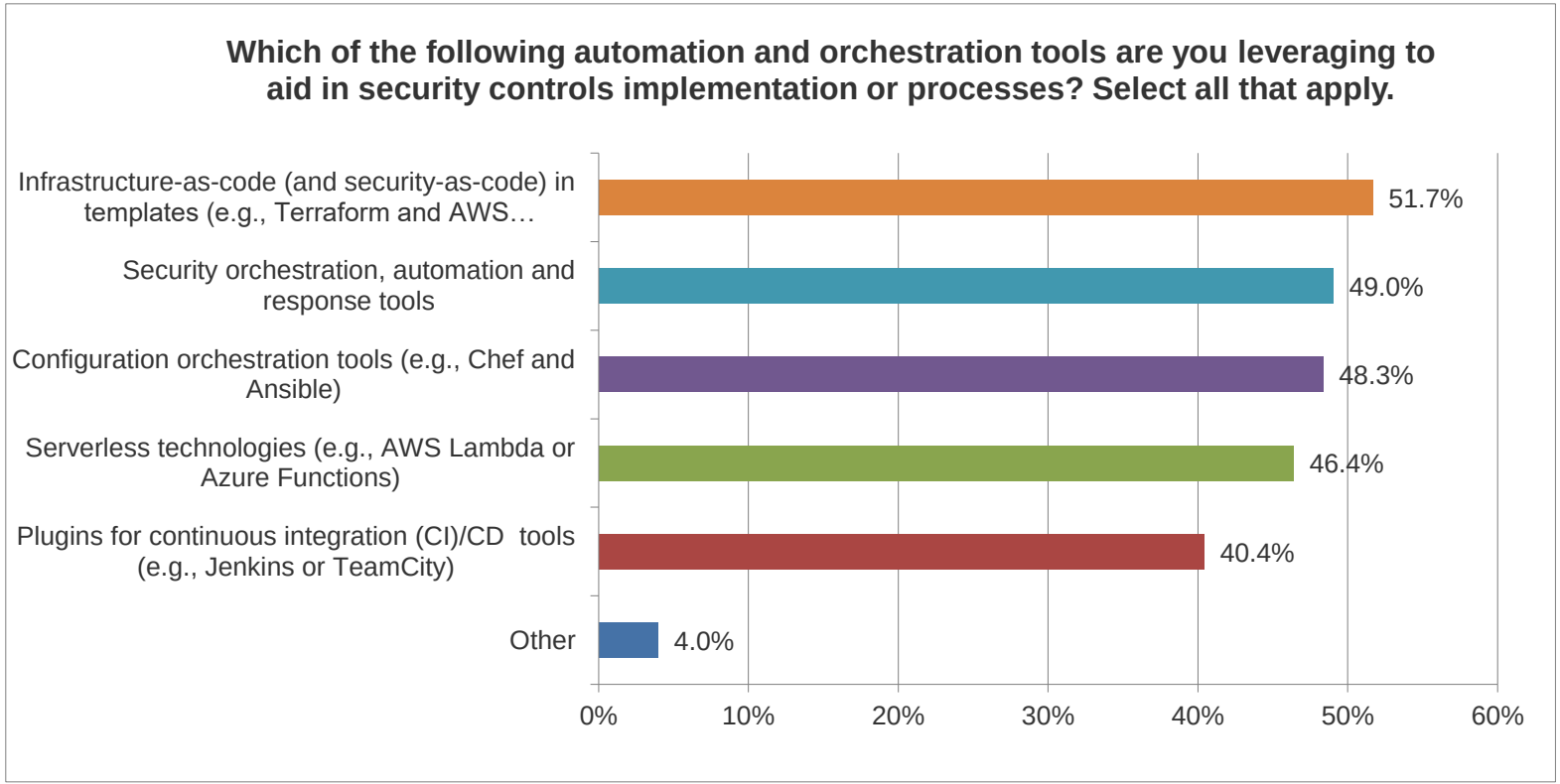


Another Big Challenge: IAM

- IAM is a major element of all cloud deployments
- Directory sync is becoming a “must have” control
- IDaaS and SSO align with this, too

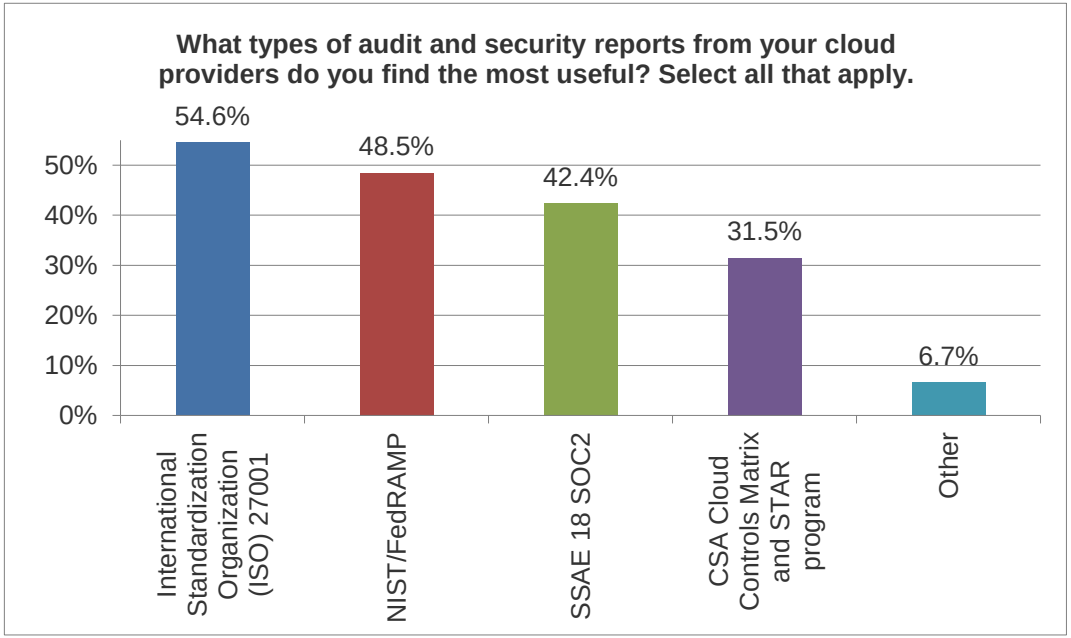


Automation & Orchestration



Audits and Pen Tests

- Top audit reports are ISO 27001, NIST/FedRAMP, and SOC 2
- Pen testing:
  - 54.7% Yes
  - 24.2% No, but we get reports
  - 10% No
  - 11% Unknown/etc.



Wrapping Up

- There are lots of takeaways from the survey this year:
  - Cloud use is growing, more sensitive data is in the cloud, and number of providers is basically stable at the low end and higher with 20+
  - IR and forensics is still frustrating
  - Use of hybrid solutions is growing
  - We need more automation & API integration