Cloud Security Survey

Credit: SANS Cloud Security Survey 2018

Andrea Lanzi
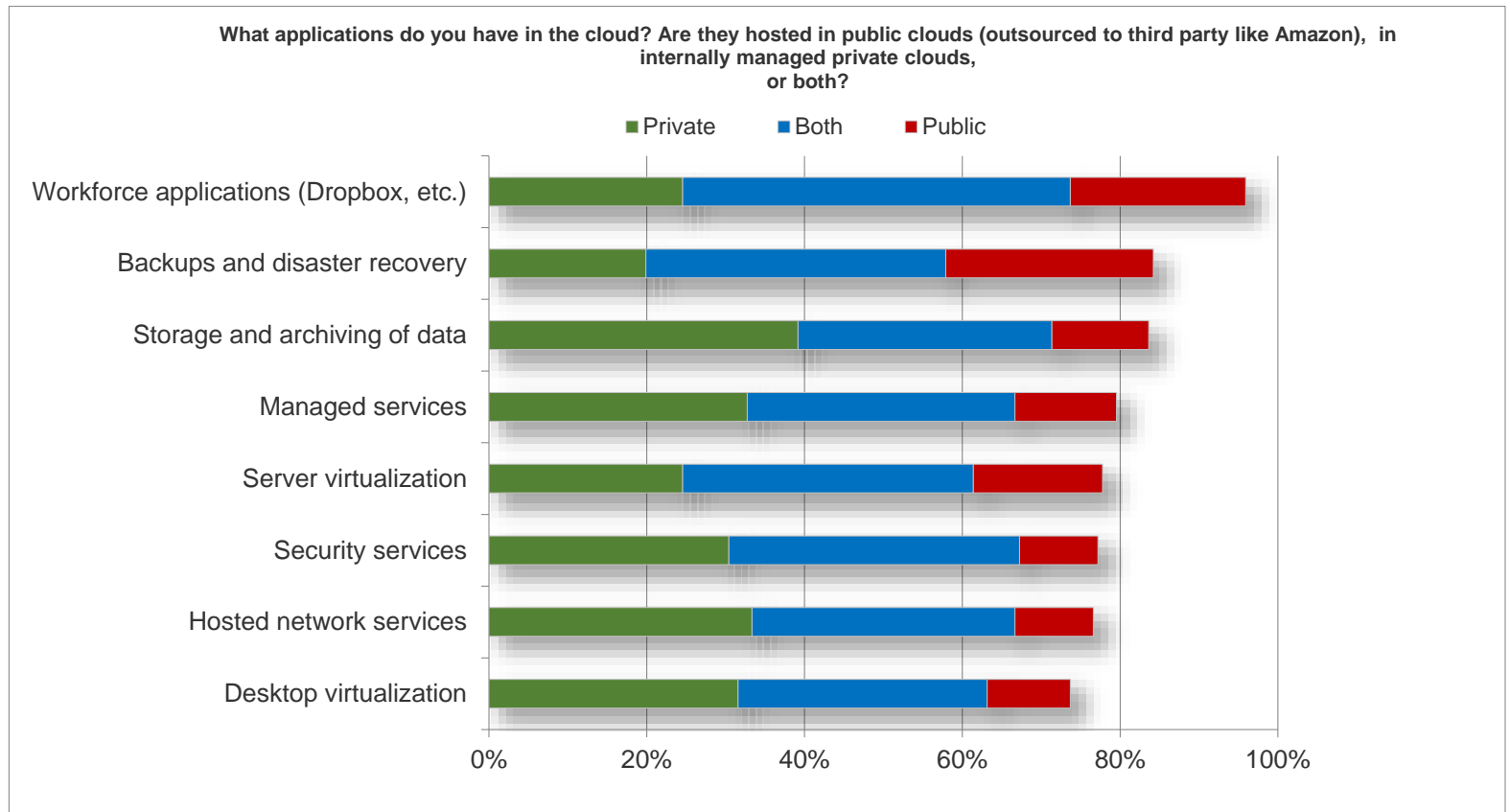
Introduction

- Key takeaways from this year:
  - More and more PII in the cloud…40% this year
  - More security controls are in use, including MFA, antimalware, and scanning tools
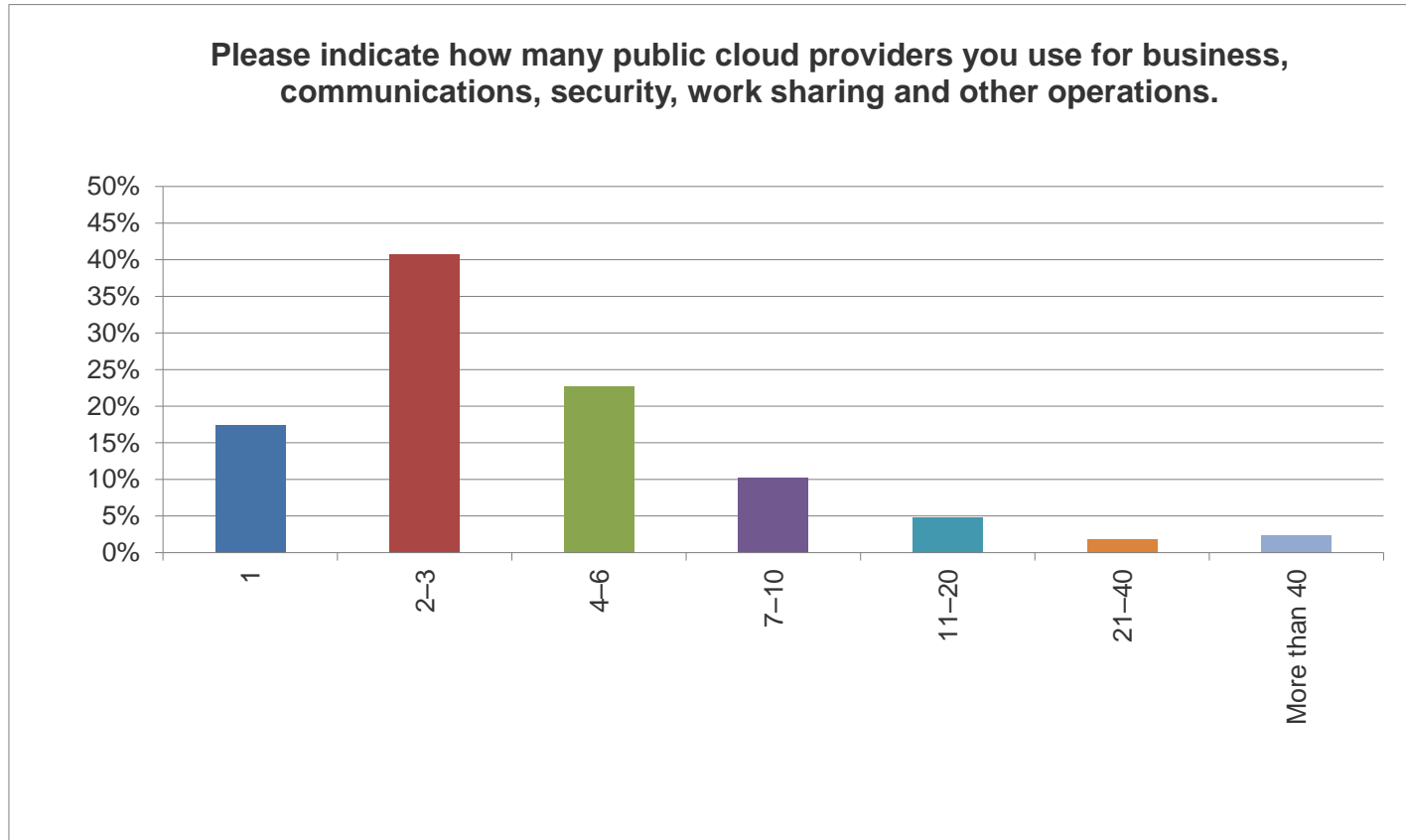 - 55% are still feeling hindered from gathering evidence and performing IR in the cloud

Use of Cloud is Increasing

Type of Application	Increase by 100%	Increase by 70% to 90%	Increase by 40% to 60%	Increase by up to 30%	No Change	Decrease
Mission-Critical Apps	6.33%	1.89%	15.20%	26.59%	32.28%	1.26%
Applications Overall	7.4%	4.32%	24.69%	44.46%	17.27%	1.86%

Workforce Apps Lead the Way

What applications do you have in the cloud? Are they hosted in public clouds (outsourced to third party like Amazon), in internally managed private clouds, or both?

Legend: ■ Private ■ Both ■ Public

- Workforce applications (Dropbox, etc.)
- Backups and disaster recovery
- Storage and archiving of data
- Managed services
- Server virtualization
- Security services
- Hosted network services
- Desktop virtualization

0% 20% 40% 60% 80% 100%

More Public Cloud Providers

Please indicate how many public cloud providers you use for business, communications, security, work sharing and other operations.

Sensitive Data in the Cloud!

Type of Data	2016	2018
Employee Records	48.2%	47.5%
Business Intelligence	**40.9%**	**42.6%**
Business Records (Finance and Accounting)	**37.8%**	**38.3%**
Customer Personal Information	**35.4%**	**40.4%**
Intellectual Property	35.4%	34.0%
Customer Financial Information	24.4%	22.0%
Health Records	**18.9%**	**21.3%**
Customer Payment Card Information	**18.3%**	**19.2%**
National Security or Law Enforcement Data	11.6%	6.4%
Student Records	11.0%	10.6%

Top Cloud Threats/Concerns: 1

What are your organization's major concerns related to the use of the public cloud for business apps? Which reflect actual incidents during the past 12 months? Leave blank those that don't apply.

■ Actual Incident   ■ Major Concern
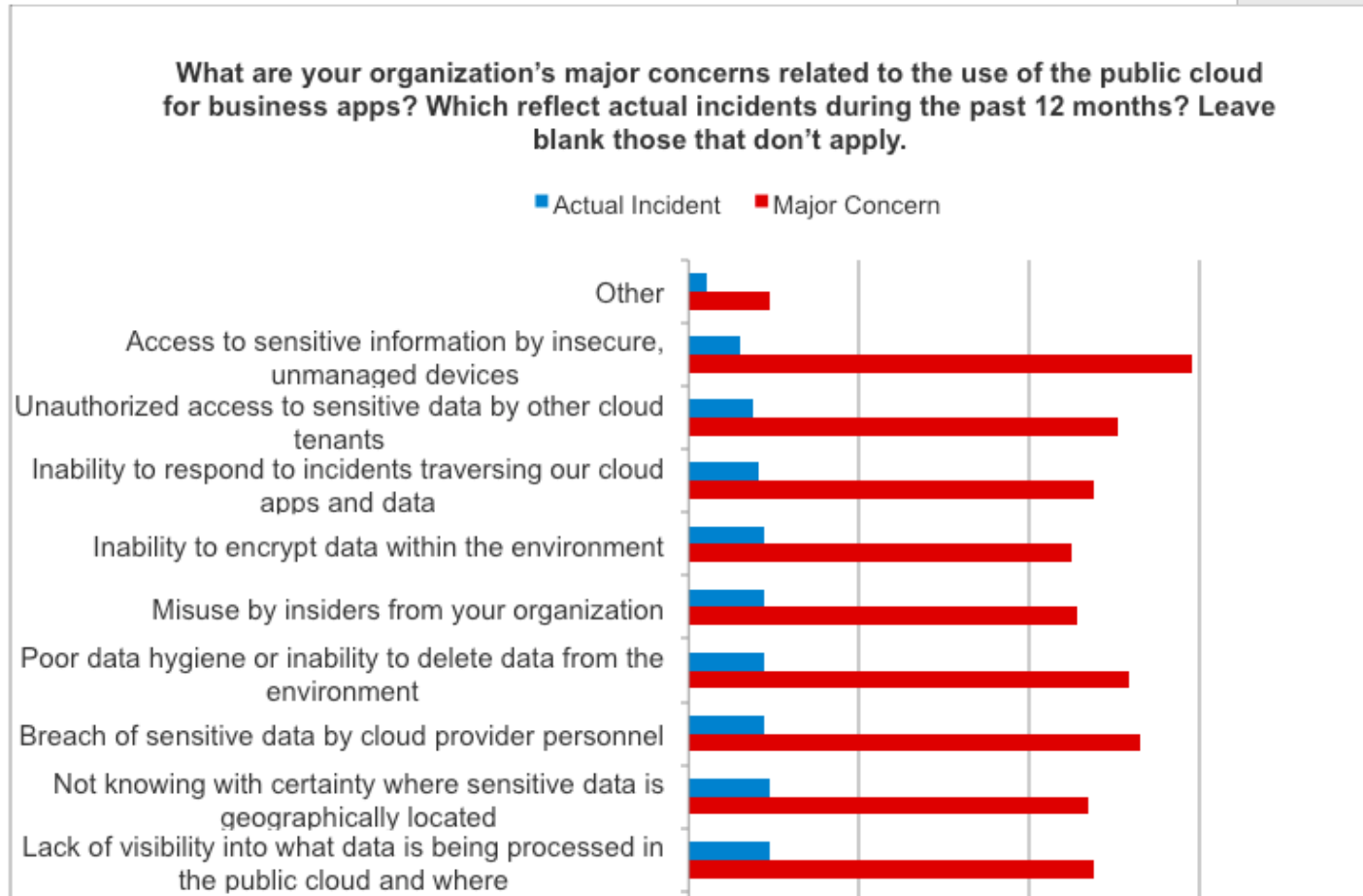
Top Cloud Threats/Concerns: 2
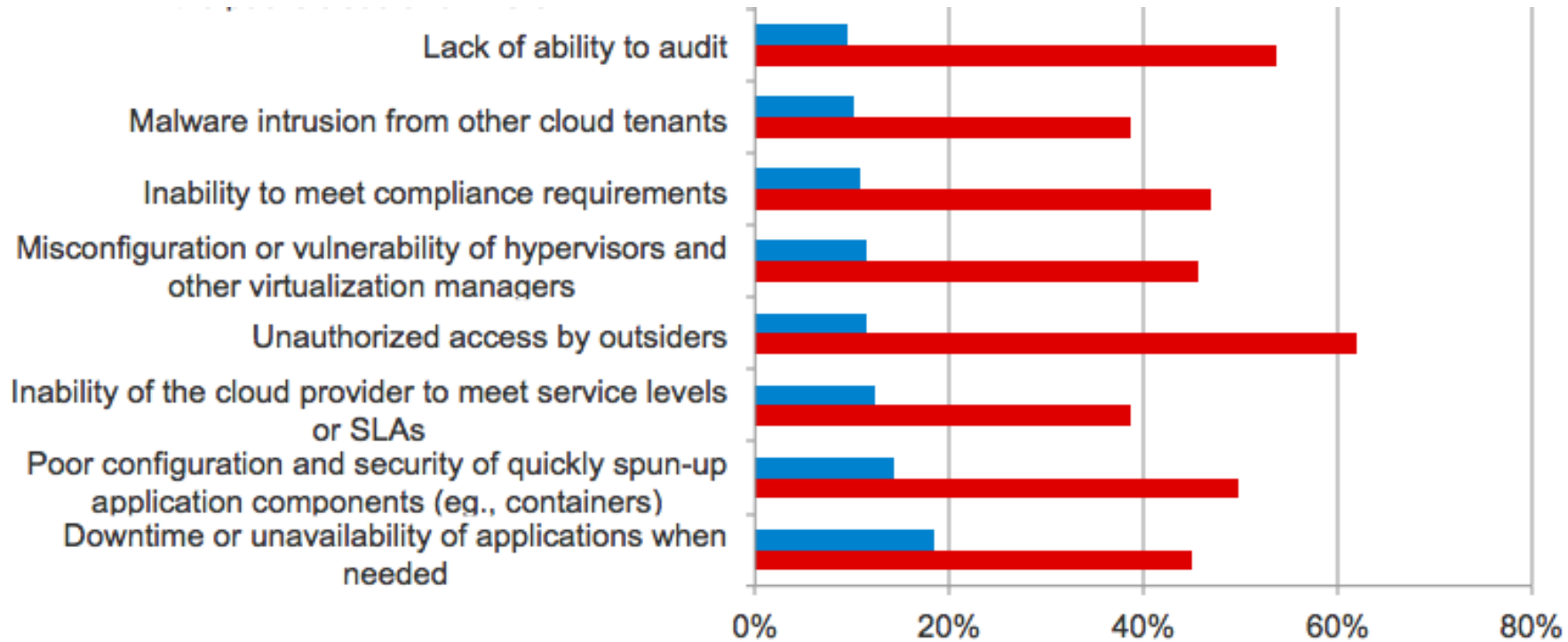
Any real breaches? Do we know?

- Last year, just over 10% of organizations claimed they had a breach involving cloud applications and data, which was a slight increase over 2015 (9%).
- The bad news is that this number went up significantly in 2017—in fact, it almost doubled (20%).
- This is likely due to more attackers focusing on the cloud, particularly on poorly configured cloud applications and management interfaces.
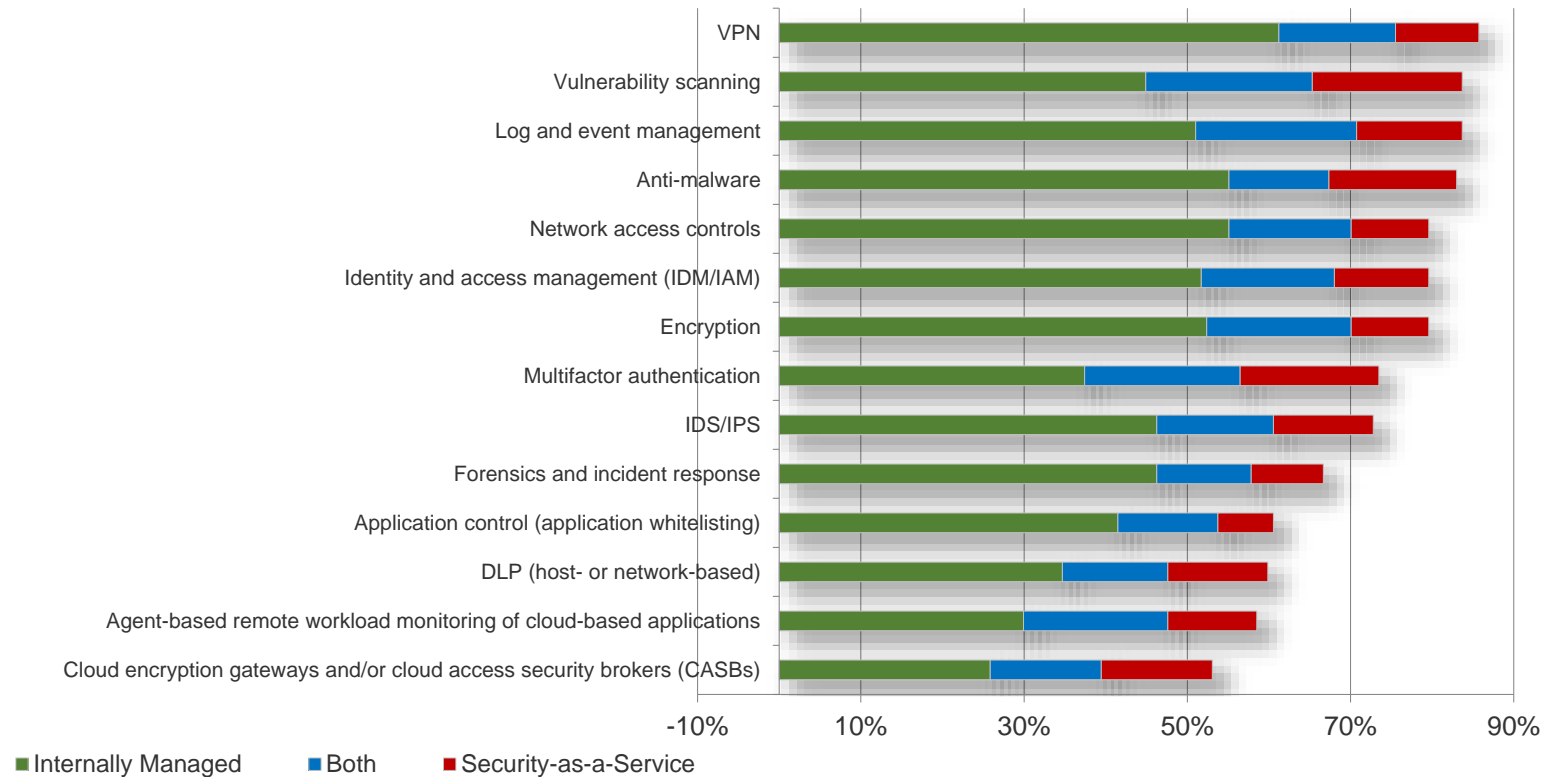- In 2016 22% didn't know whether they had been breached, and 21% were unsure in 2017.

What's involved in cloud attacks?

What was involved in the attack(s)? Select all that apply.
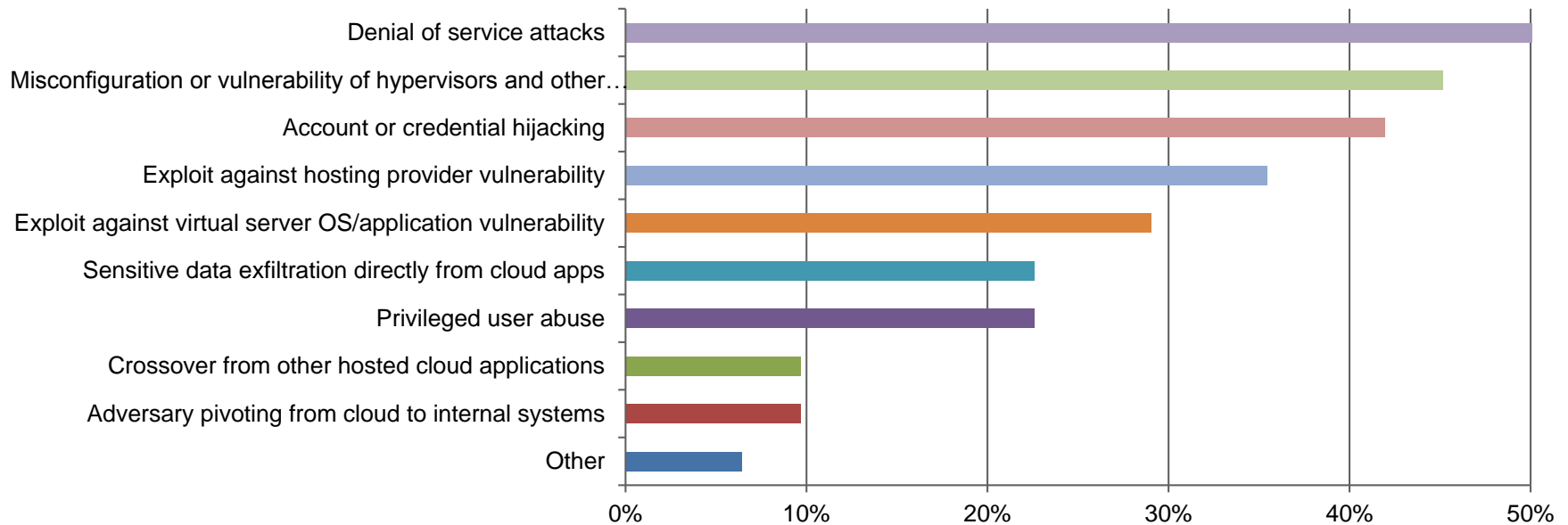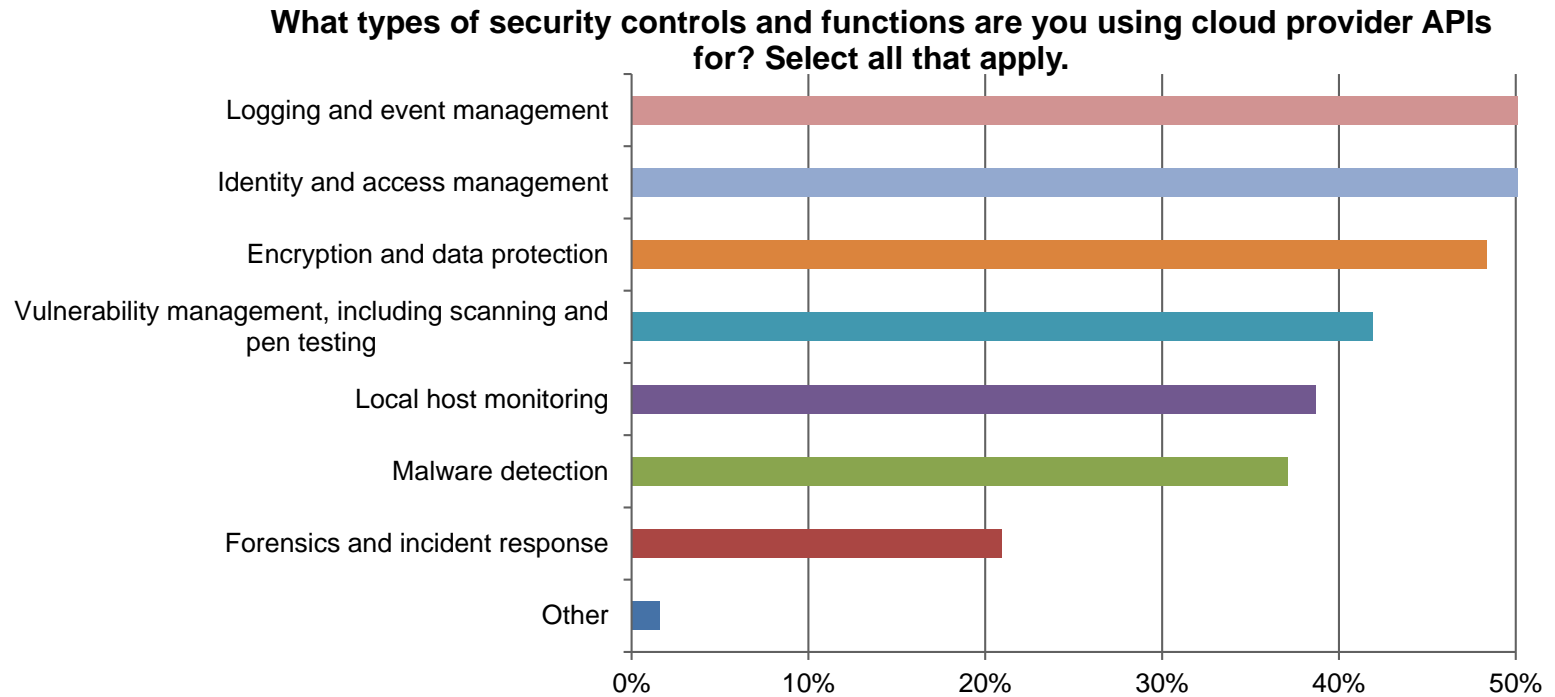
Growth in SecaaS

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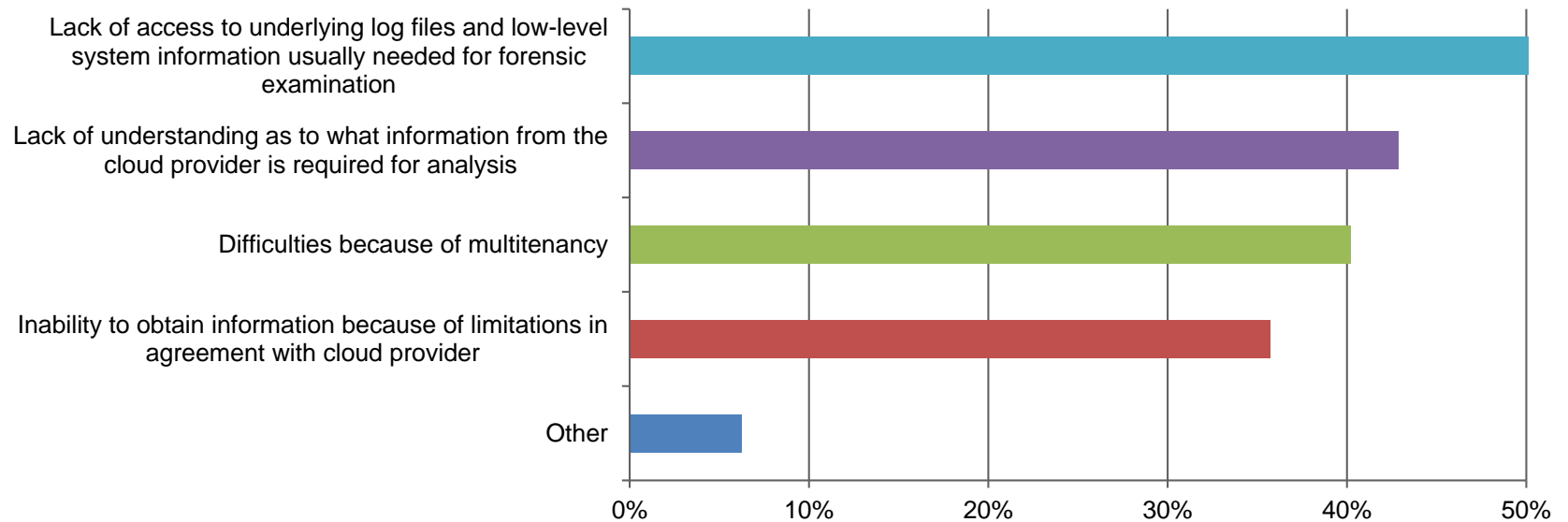
■ Internally Managed ■ Both ■ Security-as-a-Service

Cloud-Native Security Tools: API Integration

What types of security controls and functions are you using cloud provider APIs for? Select all that apply.

IR & Forensics Challenges

What challenges have you faced in adapting your incident response and forensic analysis to the cloud? Select all that apply.

So what IS working?

Which of the following security technologies have you been able to integrate between the private and public cloud? Check only those that apply.