About Me

THOMAS MACLELLAN
Director, Policy & Government Affairs,
Symantec

Focused on the national cybersecurity policy challenges facing state and local governments and higher education institutions, I engage with state and local elected officials and other senior officials within the education, homeland security, and information technology industries, to improve the nation's overall cybersecurity.

With nearly 20 years' experience in cybersecurity, forensics, privacy, energy assurance, and more, my goal is to educate officials on the threats facing their constituents and the solutions available to them. Previously, I've held director of national homeland security roles for FireEye and the National Governors Association. In addition to training governors and other senior leaders on cybersecurity and disaster response, I have directed the Governors Homeland Security Advisors Council, created the first national effort aimed at improving states' cybersecurity, as well as established the first national network of governors' criminal justice policy advisors; co-created the NGA Prescription Drug Abuse Policy Academy; and helped staff the Council of Governors that resulted in the ratification of the Joint Action Plan for State-Federal Unity of Effort for Cybersecurity.

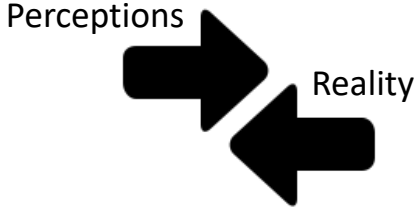
I hold a Bachelor of Arts degree in English and Psychology from the College of the Holy Cross, as well as a homeland security degree from the Naval Postgraduate School Executive Leaders Program.

2019 Symantec Cloud Security Threat Report (CSTR)

What It Is:

The 2019 Cloud Security Threat Report Compares and contrasts the perceptions versus realities of cloud security using a combination of an external market study of 1250 IT decision-makers in 11 countries worldwide against various security telemetry that Symantec tracks across Cloud, email, Web security services, threat intelligence and other internally managed data sources.

Surveyed 1250 IT Decision Makers / Across 11 Countries



Download your copy today!

2019 CSTR Key Findings

Enterprises have reached a tipping point

53% OF WORKLOADS ARE IN THE CLOUD

54% SAY THEIR CLOUD SECURITY CAN'T KEEP UP

The main reasons?

Confidence is low

69% BELIEVE THEIR DATA IS ALREADY FOR SALE ON THE DARK WEB.

Overtaxed IT Staff

25% OF CLOUD SECURITY ALERTS GO UNADDRESSED.

Immature Security Practices

3/4 EXPERIENCED A SECURITY INCIDENT DUE TO POOR CONFIGURATION, NOT USING 2FA, DLP OR ENCRYPTION

Lack of Visibility

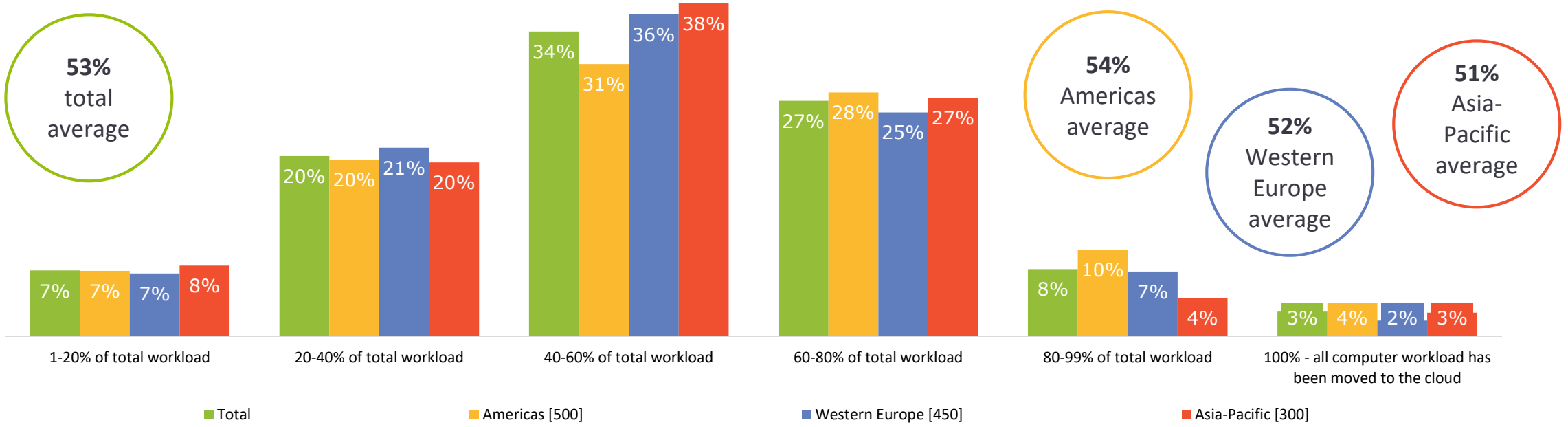
4x COMPANIES ESTIMATE THEY USE 452 CLOUD APPS; THE ACTUAL NUMBER IS NEARLY FOUR TIMES HIGHER (1,807)

Risky End-User Behavior

1/3 OF DATA IN THE CLOUD SHOULDN'T BE THERE.

2019 CSTR Key Findings

The movement of workloads onto the cloud



Analysis showing what percentage of workload at respondents' organizations have already been moved to the cloud. Asked to all respondents (1,250), split by geographic region (base in chart [x])

Struggle to keep up with cloud

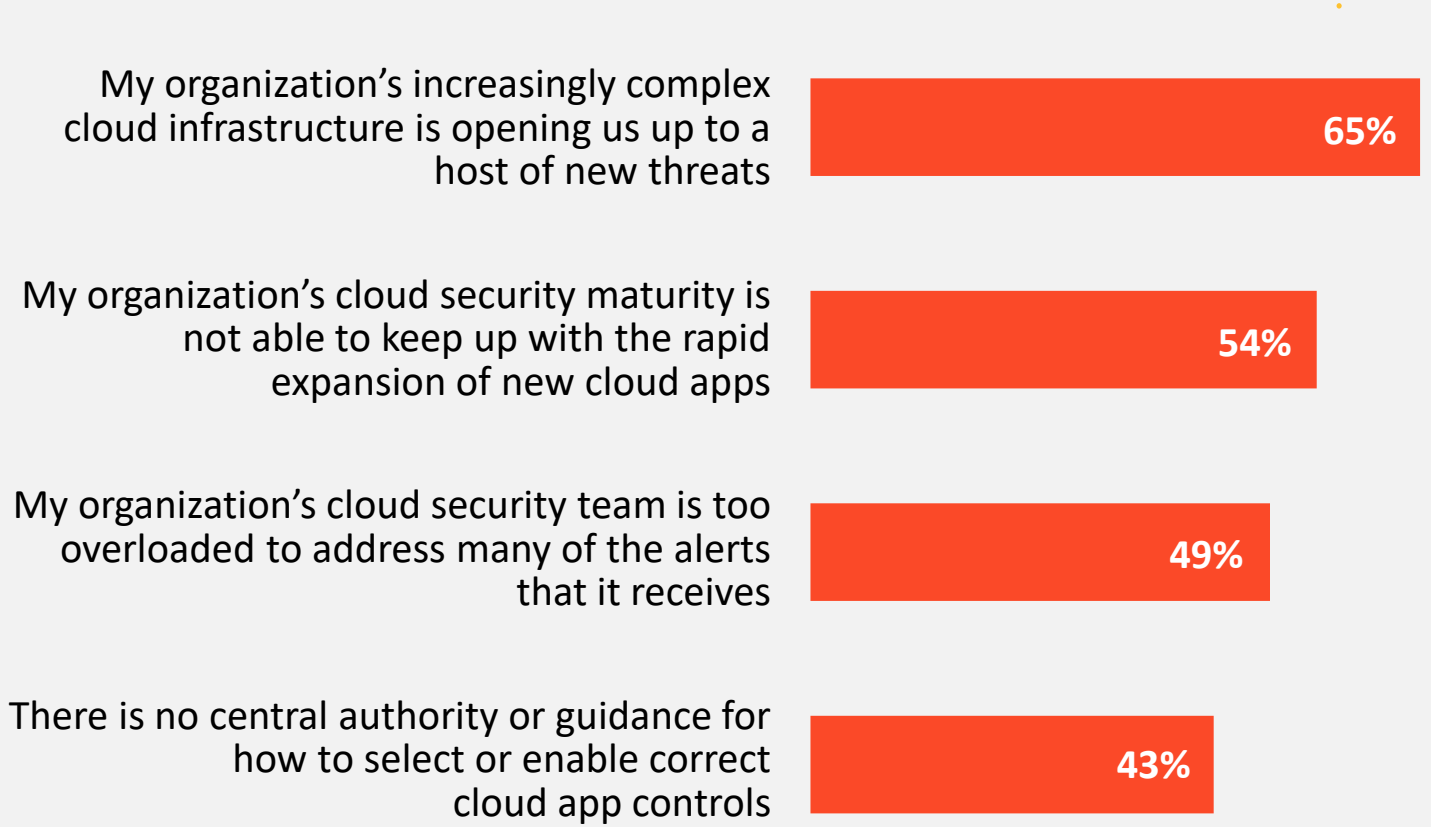


FIGURE 26:
Analysis showing the percentage of respondents who agree with the statements above. Asked to all respondents (1,250)

2019 CSTR Key Findings

Losing visibility when expanding cloud infrastructure

36%

Download and Run Cloud Apps without informing IT

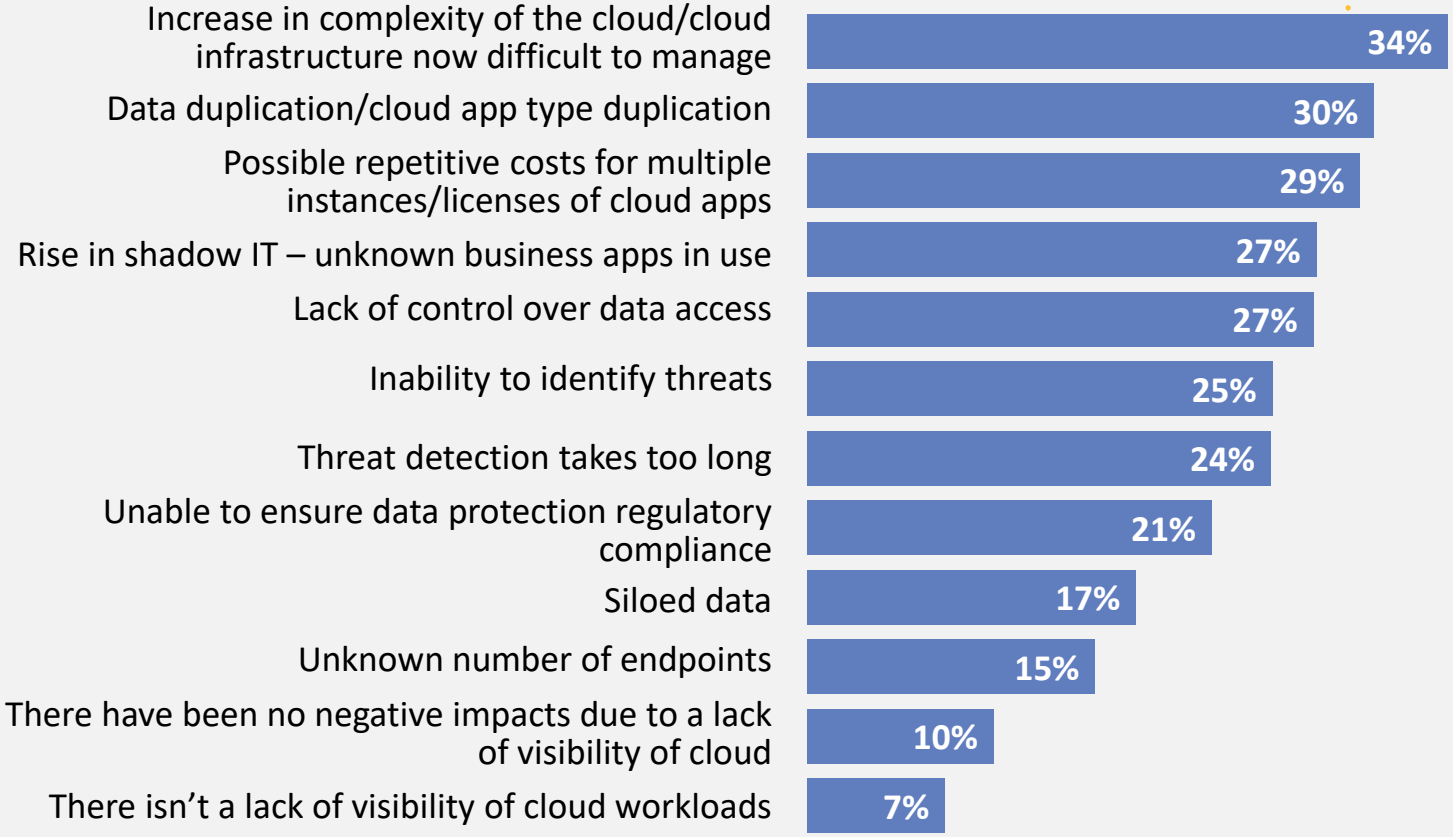
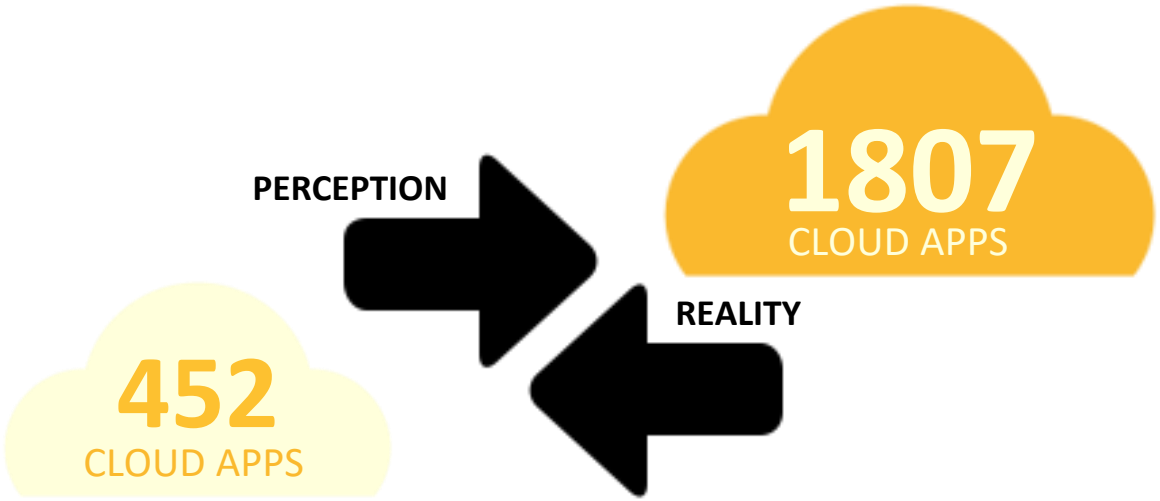


FIGURE 5:
"Has your organization encountered problems due to a lack of visibility of cloud workloads when expanding cloud infrastructure?" asked to all respondents (1,250)

2019 CSTR Key Findings

Losing visibility when expanding cloud infrastructure



ACCORDING TO SURVEY RESPONDENTS, THE AVERAGE ORGANIZATION BELIEVES ITS EMPLOYEES ARE USING **452 CLOUD APPS**. HOWEVER, ACCORDING TO SYMANTEC'S OWN DATA, THE ACTUAL NUMBER OF SHADOW IT **APPS IN USE PER ORGANIZATION IS NEARLY FOUR TIMES HIGHER**, AT 1,807.

2019 CSTR Key Findings

Oversharing sensitive files

93% OF RESPONDENTS BELIEVE OVERSHARING CLOUD STORED FILES CONTAINING COMPLIANCE DATA IS A PROBLEM

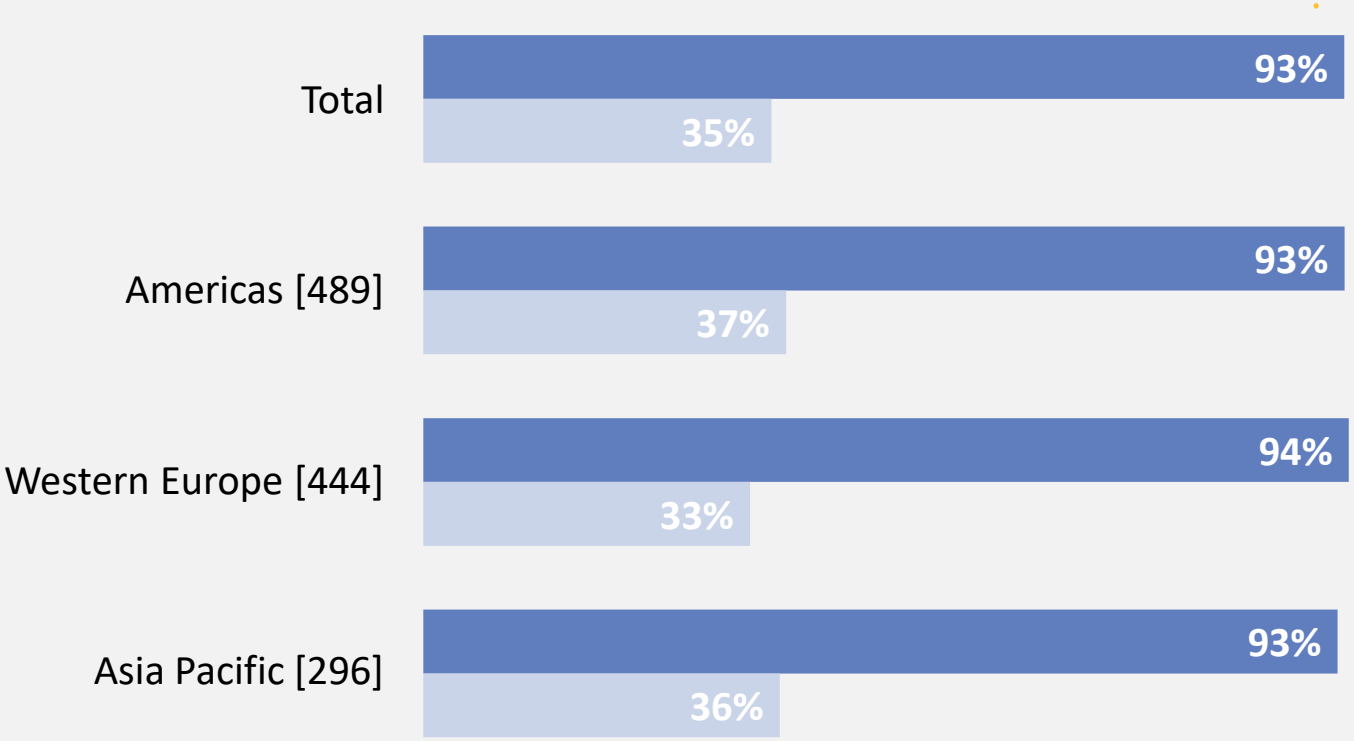
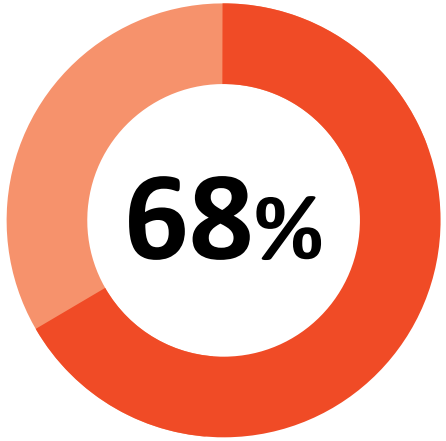


FIGURE 10:
Analysis showing the percentage of respondents who think that cloud stored files containing compliance data are overshared within their organization, vs. the average percentage of cloud stored files that are overshared in respondents' opinions. Asked to respondents whose organization stores data on cloud (1,229), split by geographic region (base in chart [x])

Data on the dark web



HAVE SEEN DIRECT OR LIKELY EVIDENCE THAT THEIR DATA HAD BEEN FOR SALE ON THE DARK WEB

FIGURE 25:
"Has your organization seen any evidence of its data being sold/offered on the dark web to third parties?" asked to all respondents (1,250)

2019 CSTR Key Findings

Security incidents

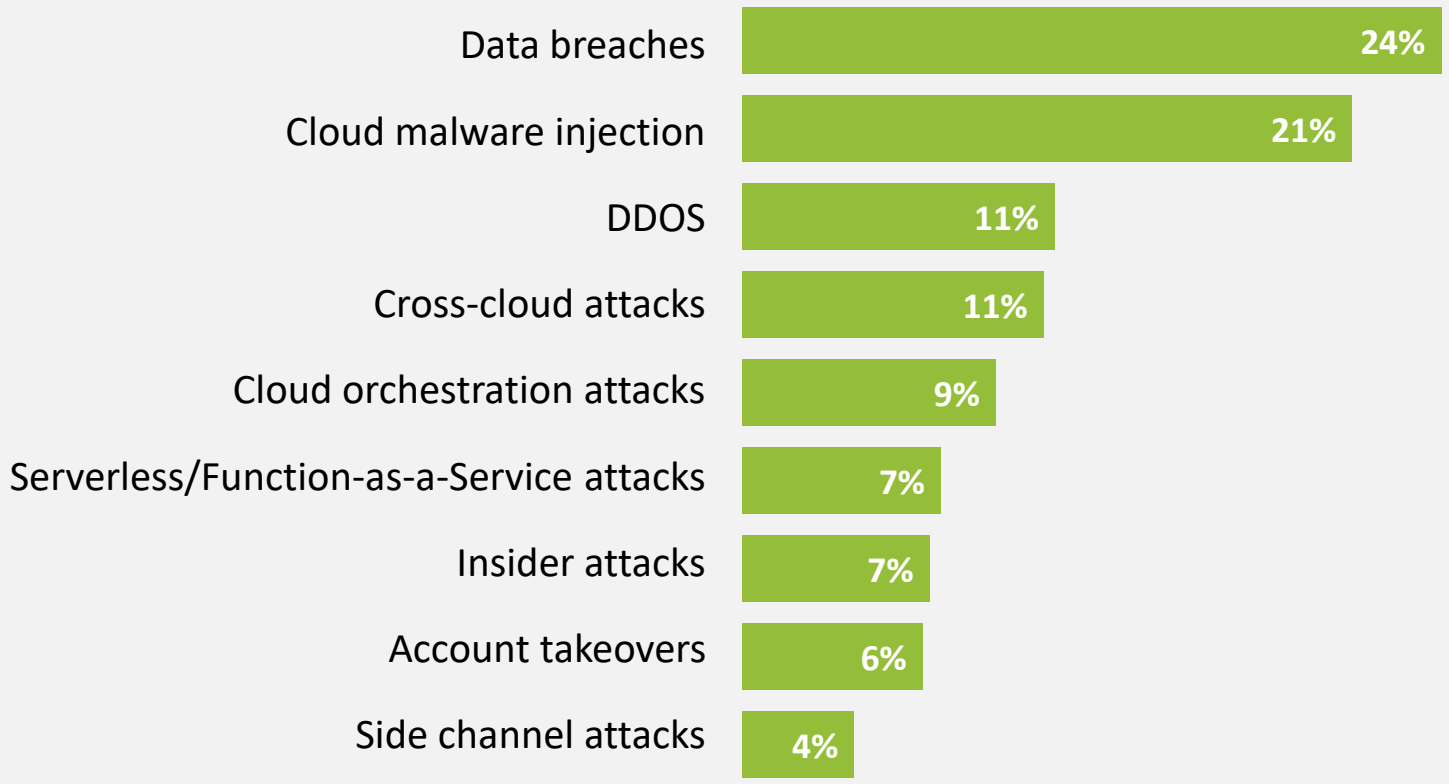


FIGURE 8:
"When thinking about your infrastructure or apps in the cloud, what types of security incidents are you investigating the most?" asked to all respondents (1,250)

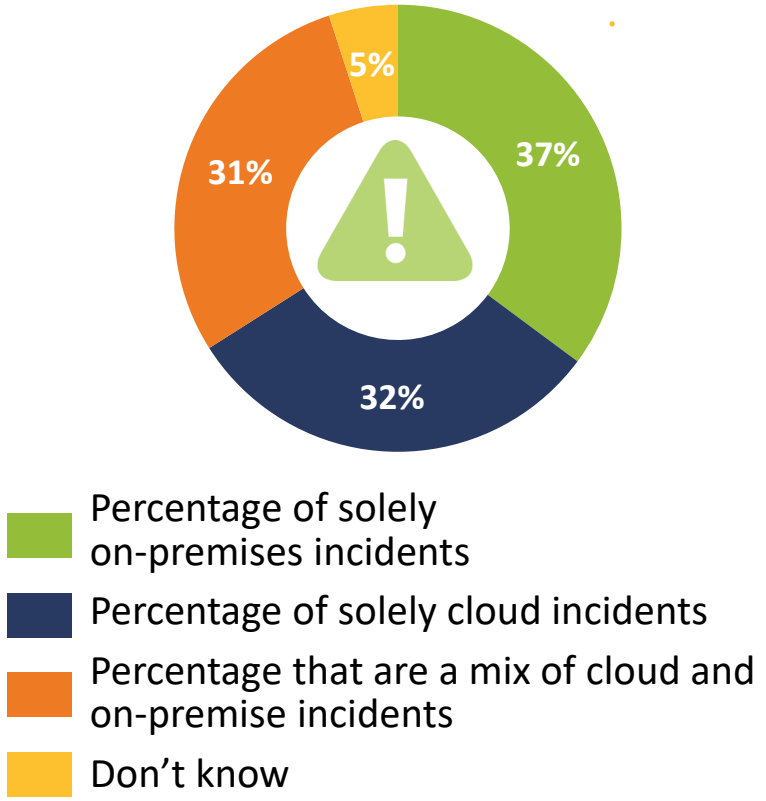
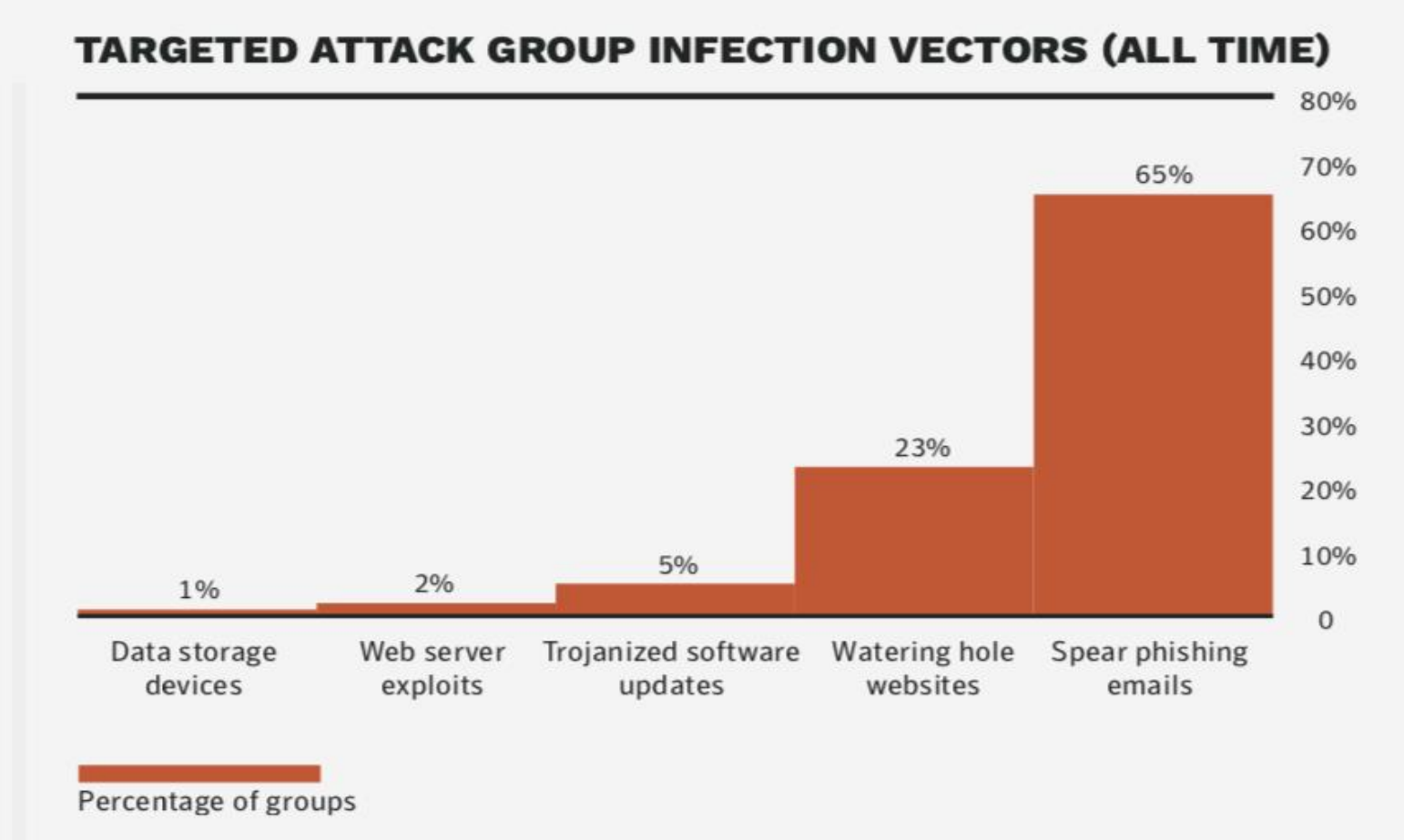


FIGURE 9:
"What percentage of security incidents investigated by your organization have occurred in the cloud or on-premise over the past 12 months?" showing the average percentage specified for each answer option, asked to respondents whose organizations stores data both in the cloud and on-premise (838)

Targeted Attack Groups



Threats to cloud infrastructure

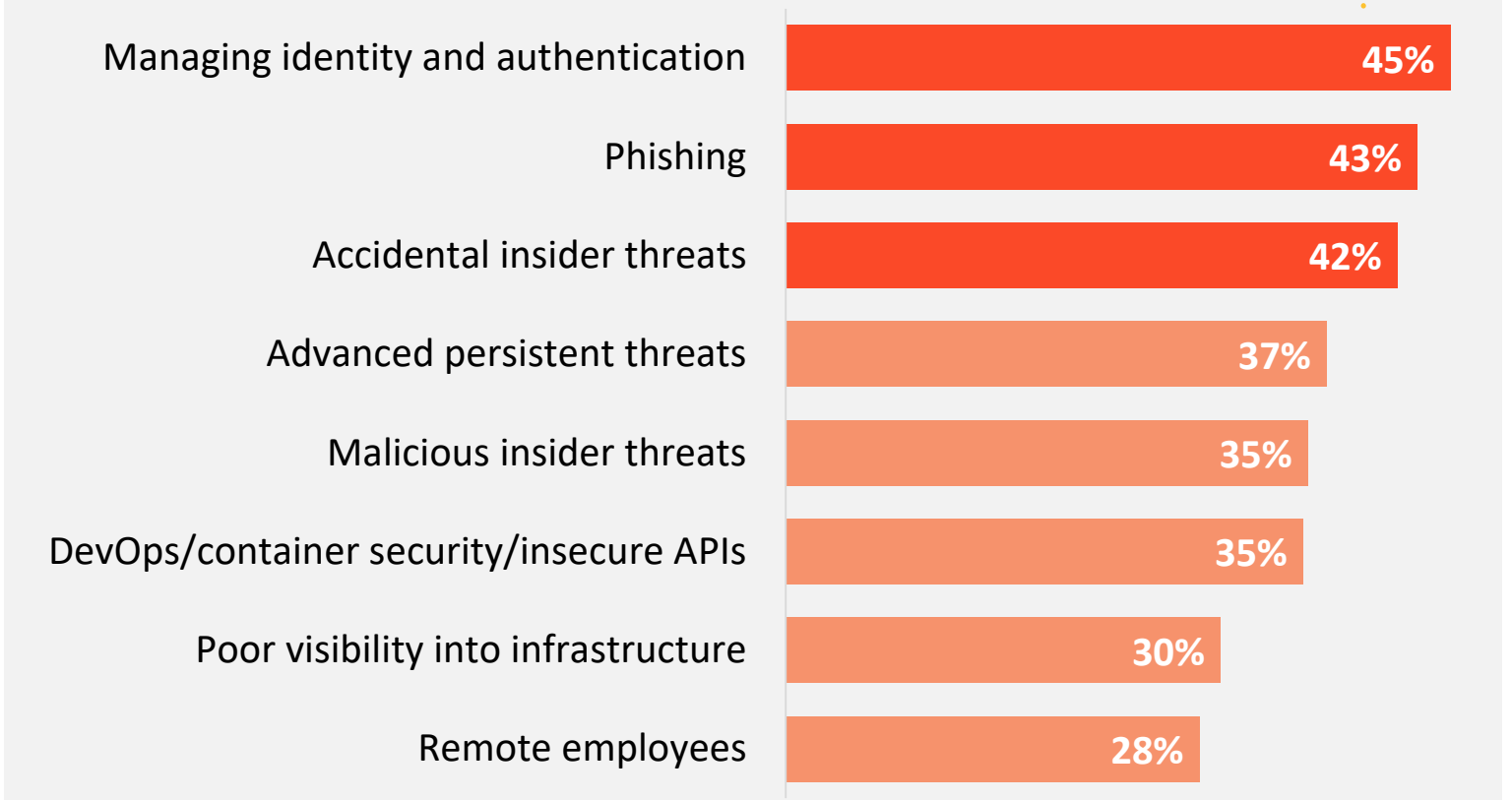


FIGURE 14:
"What have been the biggest threats to your organization's cloud infrastructure over the last 12 months?" displaying a combination of responses ranked first, second, and third, asked to all respondents (1,250)

2019 CSTR Key Findings

Risky behavior by employees

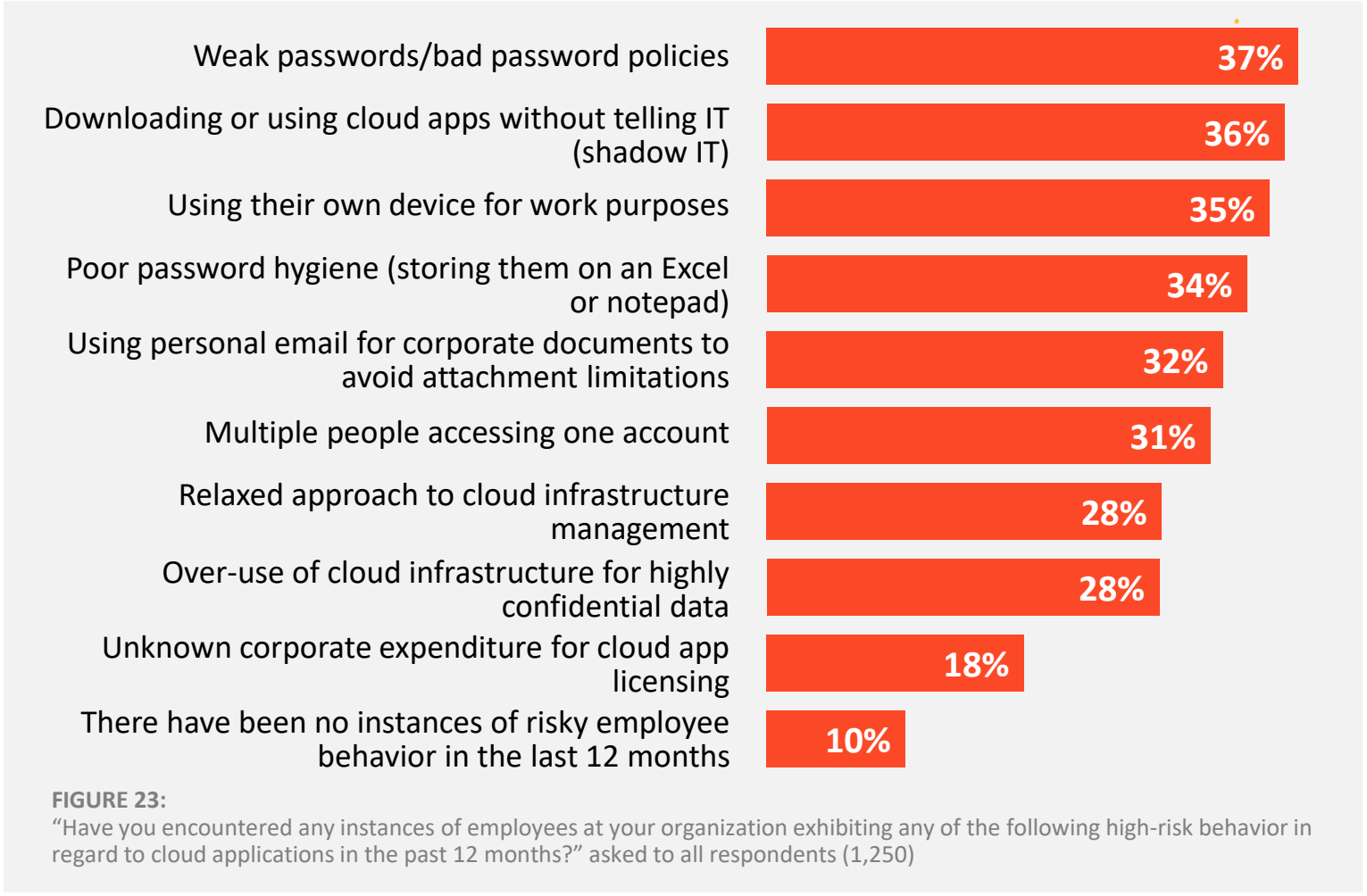


FIGURE 23:
"Have you encountered any instances of employees at your organization exhibiting any of the following high-risk behavior in regard to cloud applications in the past 12 months?" asked to all respondents (1,250)

Best Practices: Building an Effective Cloud Security Strategy

DEVELOP A GOVERNANCE STRATEGY SUPPORTED BY A CLOUD CENTER OF EXCELLENCE (CCoE)

EMBRACE A ZERO-TRUST MODEL

PROMOTE SHARED RESPONSIBILITY

USE AUTOMATION AND ARTIFICIAL INTELLIGENCE WHEREVER POSSIBLE

AUGMENT IN-HOUSE CLOUD SECURITY EXPERTISE WITH MANAGED SERVICES

The Future of Cloud Security

Concerns for the future

Cloud attacks & breaches may explode as a function of greater usage

CSTR Fact: Organizations have reached a tipping point with 54% of their workloads residing in the cloud.

Ubiquity of compute (cloud & IoT), storage (cloud & IoT) and bandwidth (5G) challenges notion of Security at Scale

CSTR Fact: 25% of cloud security alerts go unaddressed.

Is the ubiquity of compute leading to a loss of privacy?

- GDPR is not the last privacy regulation – more are coming
- Greater accountability and liability for PII breaches and stewardship

CSTR Fact: 1/3 of the data in the cloud shouldn't be there.

The Future of Cloud Security

Concerns for the future

As cloud matures, will enterprises maintain agility, portability & choice?

CSTR Fact: 54% of organizations agree that their cloud security maturity isn't able to keep up with the rapid expansion of new cloud apps

Do we need to reimagine the role security plays in the enterprise?

CSTR Fact: Organizations underestimate their use of cloud apps by nearly 4x.