Symantec™

Cloud Security Threat Report (CSTR)

Adapting to the New Reality of Evolving Cloud Threats

June 2019

Key Insights

Cloud becoming the business backbone:

53% of all compute workload are in the cloud

Visibility is a challenge:

93% struggle to keep tabs on cloud workloads

Loss of control:

93% report oversharing sensitive data

Data for sale on dark web:

68% have evidence their data has been for sale

Security can’t keep up:

54% say cloud security maturity can’t keep up

Key Insights

Open door for Lateral Movement:

64% of cloud security incidents are due to unauthorized access

Immature security practices add to risk:

65% don‘t implement MFA with IaaS

80% don’t use encryption

Insiders can be a threat:

accidental insider ranked **#3** threat to cloud infrastructure

Behind the times:

85% are not using CIS best security practices

Users behaving badly:

weak passwords **(37%)** and poor password hygiene **(34%)** top list of bad behaviors

CSTR

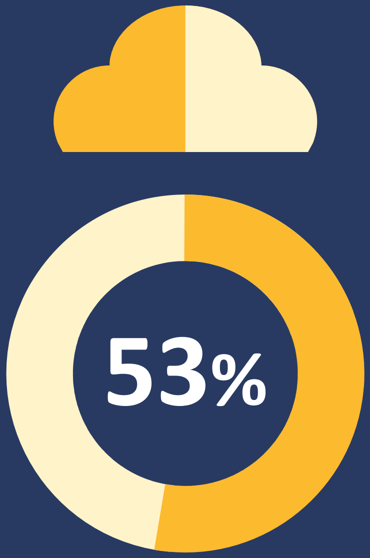
Cloud Security Threat Report

Volume 1 | June 2019

CLOUD IS AT THE TIPPING POINT:

Few are Ready

Cloud is Becoming the Business



of all compute workload has now been migrated to the cloud

cloud grew at **16%** in past 12 months

expected to grow at **22%** next 12 months

Cloud Use Underestimated
1/3 Say Lack of Visibility Causing Issues

Cloud Applications in Use

452

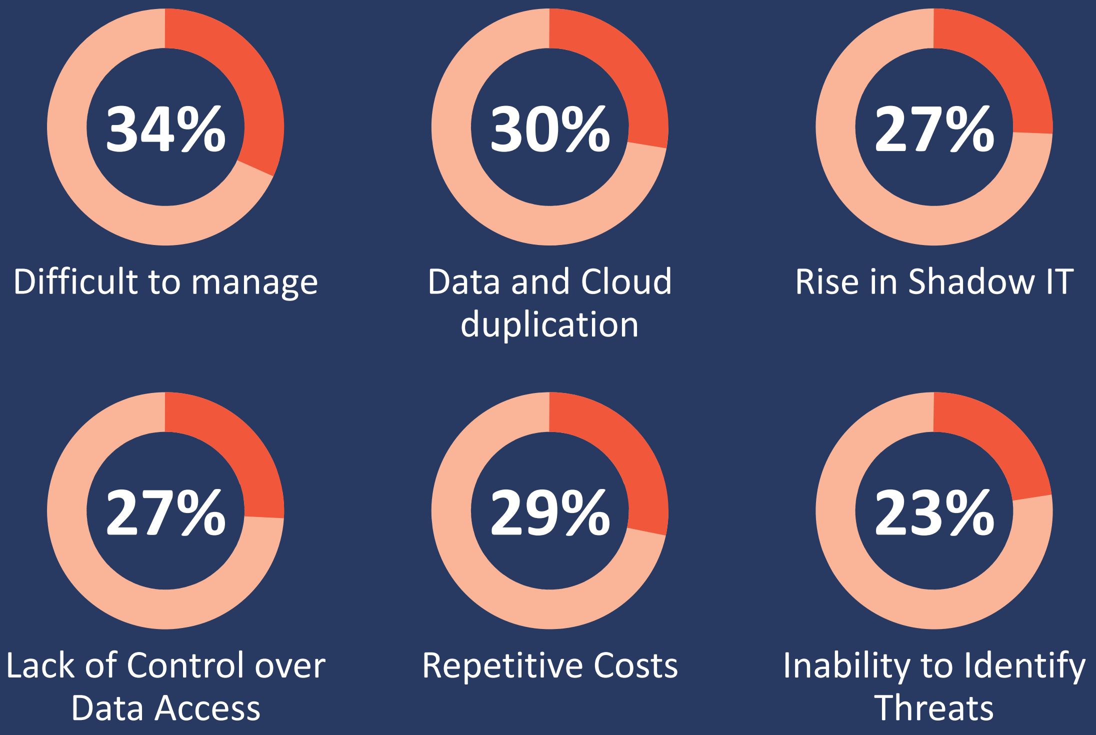
PERCEPTION

1807 CLOUD APPS

REALITY

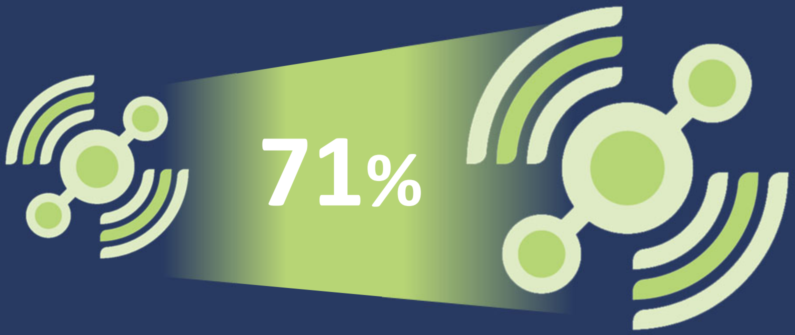
1/3 participants say poor visibility made identifying threats more difficult

Top Issues Caused by Lack of Visibility



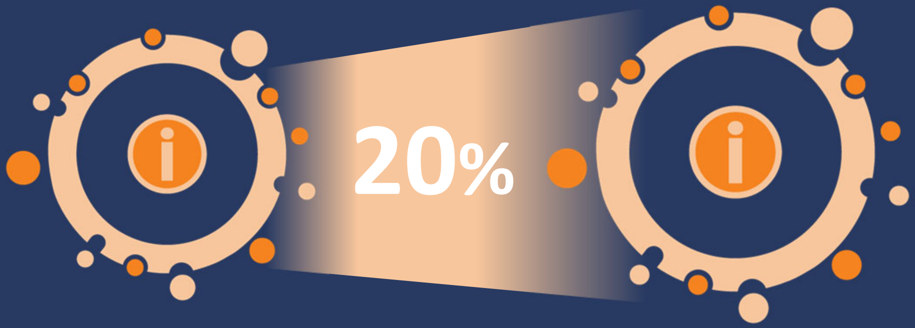
IoT Use Skyrocketing—Creating Risk

Past 12 Months



71%

increase in IaaS incidents
related to IoT devices



20%

increase number of IoT devices
connected to IaaS

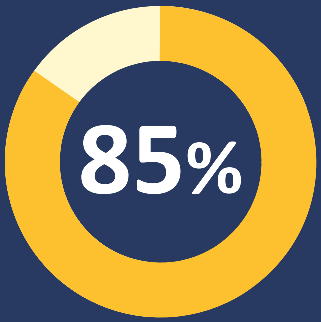
CSTR

Cloud Security Threat Report

Volume 1 | June 2019

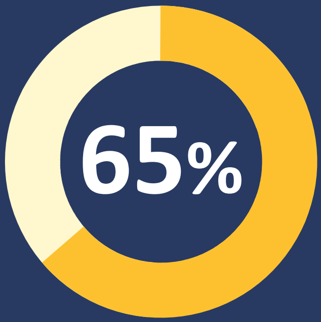
THREE QUARTERS OF COMPANIES EXPERIENCED INCIDENTS DUE TO CLOUD SECURITY IMMATURITY

Skills and Best Practices are Lacking

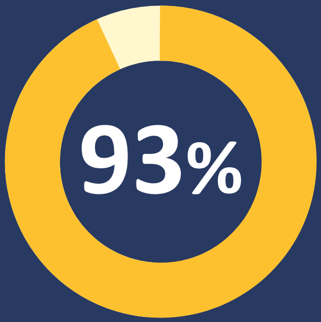


not using Center for Internet Security best practices*

*Symantec Internal Data



neglect to implement multi-factor authentication

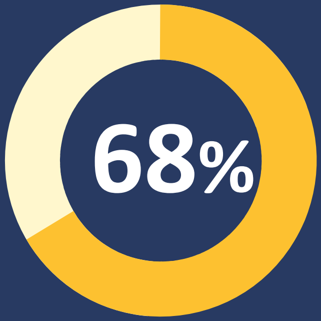


need to enhance cloud security skills

Data Compliance Compromised by Immature Cloud Culture

93%

believe oversharing cloud stored files containing compliance data is a problem



68%

have evidence that their data had been for sale on the dark web

CSTR

Cloud Security Threat Report

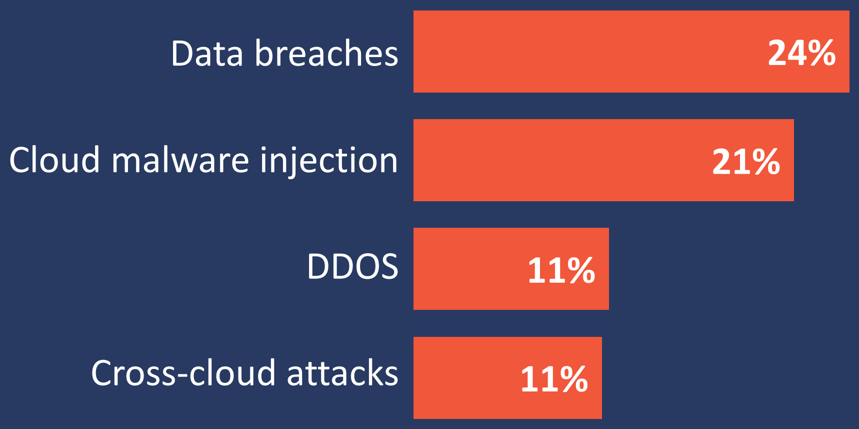
Volume 1 | June 2019

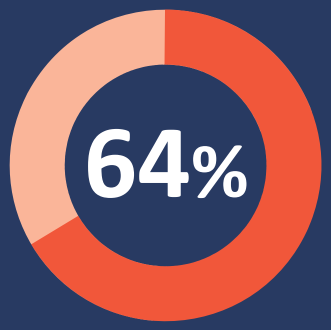
TOP THREATS:

Is your Focus Where it Should be?

Are you Guarding the Door while Attacks Come in the Window?

Most Investigated Cloud Infrastructure Attacks





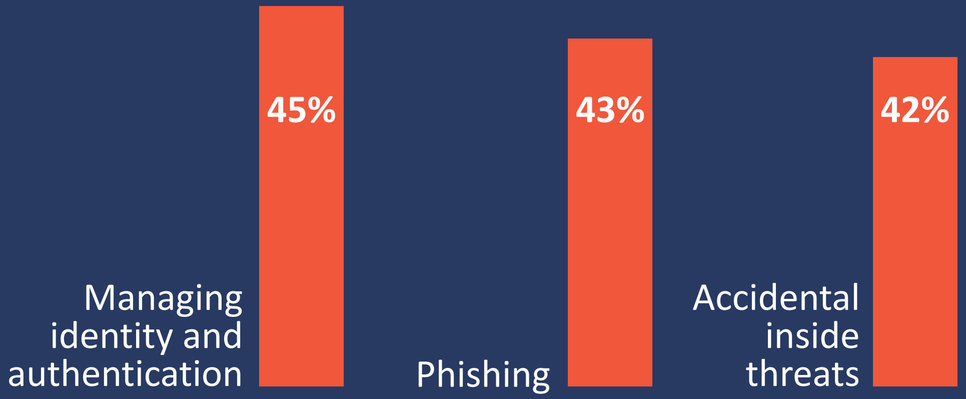
cloud security incidents caused by unauthorized access*

*Symantec internal data

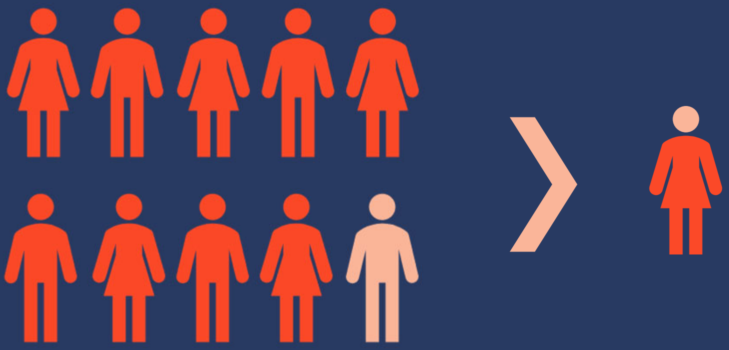
Emerging Threats to Cloud Infrastructure

THE TOP THREE THREATS

The three highest threat categories, according to the external survey respondents, are:

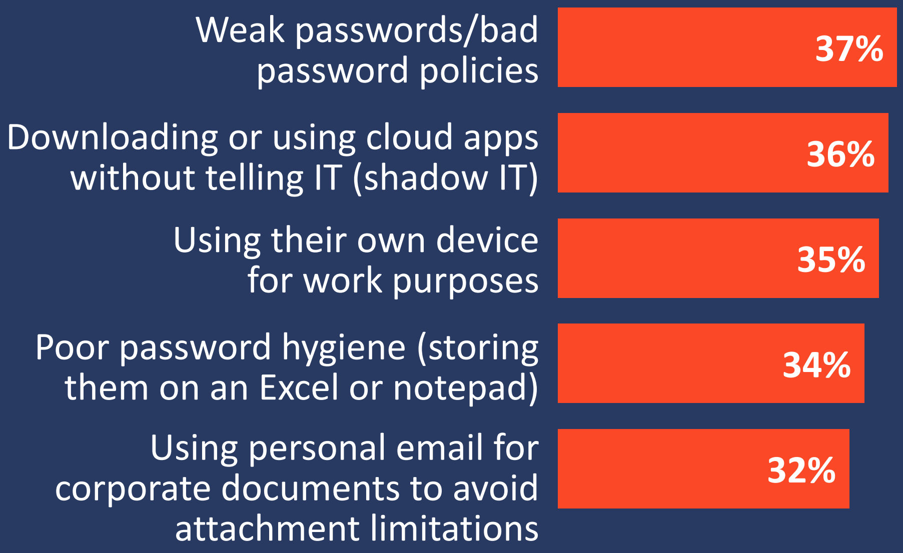


Risky Employees not Being Investigated



9 out of 10 have encountered high-risk employee behavior

at the same time, only **7%** of participants are investigating insider threats



CSTR

Cloud Security Threat Report

Volume 1 | June 2019

YOU CAN'T STOP THE CLOUD:

Now What?

Best Practices:
Building an Effective Cloud Security Strategy

develop a governance strategy supported by a cloud center of excellence

embrace a zero-trust model

promote shared responsibility

use automation and artificial intelligence wherever possible

augment in-house cloud security expertise with managed services

CSTR

Cloud Security Threat Report

Volume 1 | June 2019

QUESTIONS

Learn More at https://go.symantec.com/CSTR

Symantec™