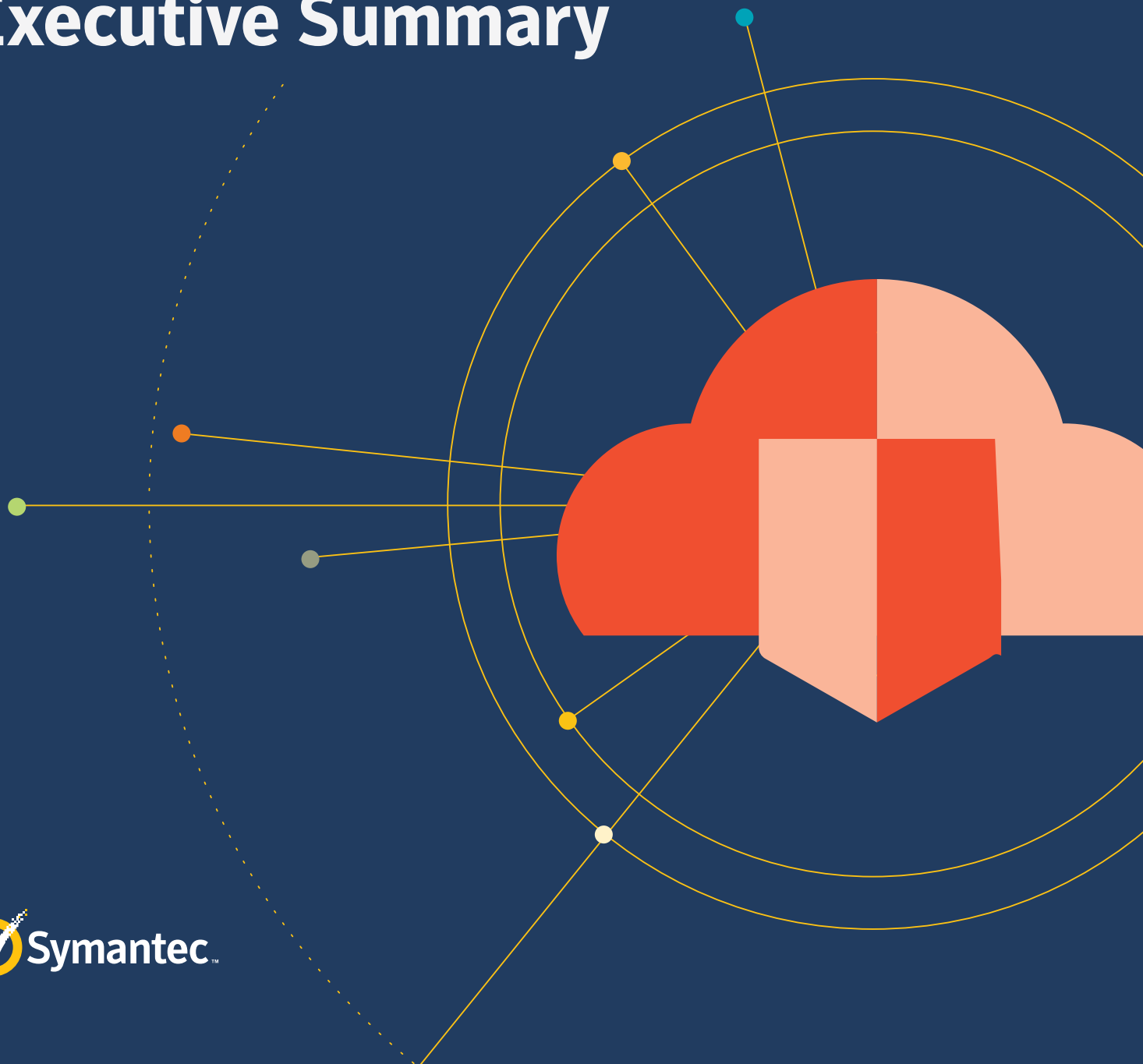
Cloud Security Threat Report (CSTR)
Volume 1 | June 2019

Adapting to the New Reality of Evolving Cloud Threats

Executive Summary



Symantec

Introduction

While Software-as-a-Service (SaaS) application usage is proliferating, and workloads are increasingly migrating to IaaS platforms like AWS and Azure, on-premises applications, storage, and private clouds persist. The resulting hybrid IT environment is challenging existing security paradigms, creating complexity, and leaving organizations scrambling to keep up.

Symantec surveyed 1,250 security decision makers worldwide in Spring 2019 to understand the shifting cloud security landscape, the scope of Shadow IT and Shadow Data usage, and to gauge the maturity of security practices as enterprises transition to the cloud. Compared to aggregated and anonymized telemetry data from Symantec data sources, what we found was eye opening and often quite alarming.

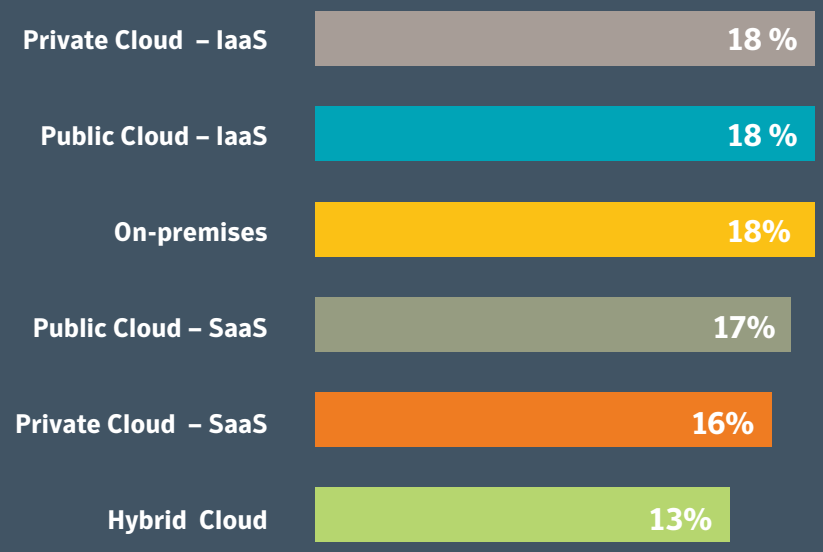
Symantec

Section

01

The Tipping Point Is Here. Few Are Ready.

One of the biggest takeaways from our external survey is that firms are storing data in more than one environment.



53%

ARE FORGING AHEAD WITH CLOUD DEPLOYMENT

69%

ARE STILL STORING SOME DATA ON PREMISES

Visibility is Cloudy

Most IT and SecOps organizations don't know how fast their cloud portfolio is growing or what's being used.

The majority of workloads have also shifted to the cloud. On average, organizations report that over half (53%) of their workload has been migrated to the cloud. However, only a small minority (3%), have transferred all of their workloads to a cloud platform.

Visibility into these cloud workloads is a problem. An overwhelming majority of survey respondents (93 percent) report issues keeping tabs on all cloud workloads.

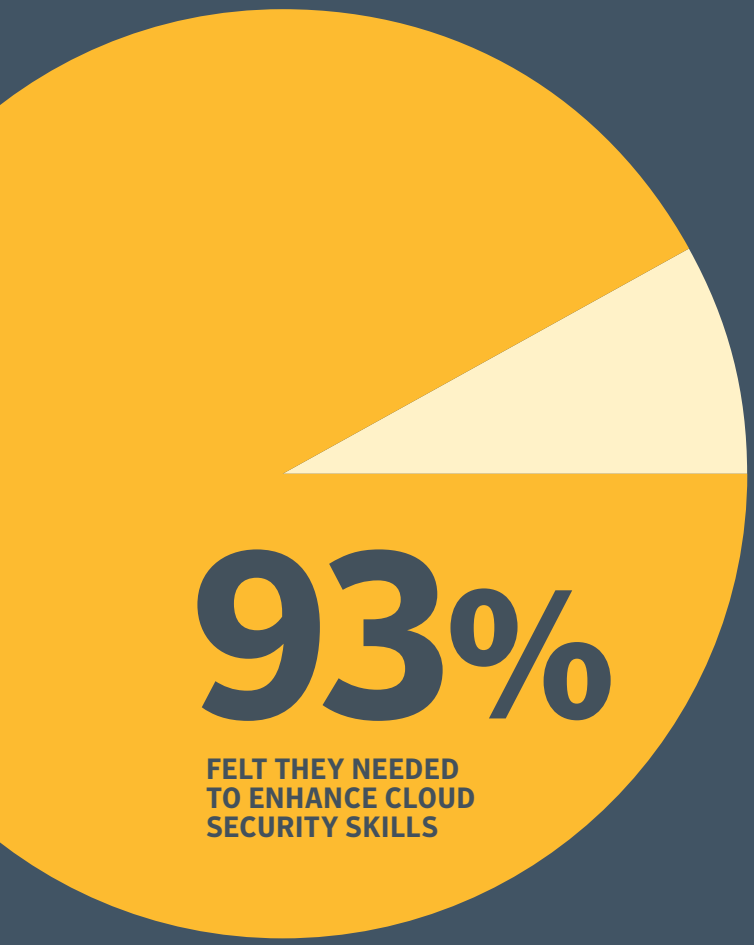
452

PERCEPTION

1807 **CLOUD APPS**

REALITY

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.



Capacity is Maxed

Forty-nine (49) percent of respondents confirmed their cloud-security manpower is inadequate to deal with all incoming alerts.

A skills and security personnel shortage is the primary culprit: most respondents said they need to enhance Cloud security skills (93%) while 84 percent confirmed they needed to add staff to close the gap.

Immature Practices Prevail

Most organizations' cloud maturity is not advancing as rapidly as the expansion of new cloud apps being deployed—a hurdle confirmed by over half (54 percent) of respondents in the external survey. Seventy-three (73) percent blame immature security practices, including use of personal accounts, and lack of multi-factor authentication (MFA) or data loss prevention (DLP) services, for at least one cloud incident. Only 1 in 10 survey respondents say they are able to adequately analyze cloud traffic.

73%

BLAME IMMATURE SECURITY PRACTICES FOR AT LEAST ONE CLOUD INCIDENT

28%

OF EMPLOYEES ENGAGE IN SOME KIND OF HIGH-RISK BEHAVIOR

Employee Behavior is Risky Business

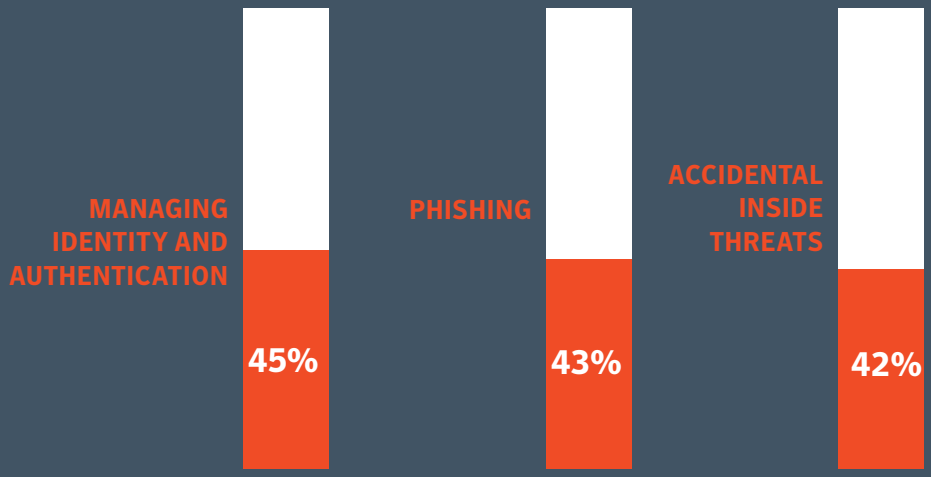
Companies underestimate the security impact of employee misuse of cloud apps. The external survey estimates that 28 percent of employees engage in some kind of high-risk behavior. Symantec's own research again illustrates how reality outpaces survey perceptions: 85 percent of the larger organizations (more than 1,000 employees) reported some high-risk users, and 30 percent of those had 100 or more high-risk users.

Section

02

The Top Threats

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



According to Symantec internal data, of nearly 33,000 apps evaluated for their Business Readiness Rating (BRR), which is based on 80+ security attributes, less than 1 percent have the requisite built-in security for regular business use while 39 percent are not suitable at all for business use. The majority exhibit only some necessary security controls.

Shadow Data is proliferating within both sanctioned and unsanctioned SaaS services. More than half of external survey respondents (52 percent) said that increased use of cloud apps to store and share sensitive corporate data was a problem. The vast majority (93 percent) said that they grapple with users oversharing cloud files containing sensitive and compliance-related data, while on average 35 percent of cloud files are overshared.

More worrying are the fall-out effects that can happen from this lax approach to security controls. The external survey reports that 68 percent of respondents have either seen direct or likely evidence that their data had been for sale on the Dark Web.

Risks from Misconfigured Servers, Malware, and Unauthorized Access

Survey respondents say that nearly two-thirds of security incidents under investigation in the last twelve months have occurred at the cloud level, and nearly one-third of all incidents has been classified as cloud-only.

The Threat from Inside

Cloud incidents that result from insider threats—either purposeful, inadvertent, or through compromised credentials, are a major concern for 48 percent of respondents. In addition, 21 percent of respondents said the problem was increasing in intensity.

Immature security practices are creating serious gaps and driving higher incidents of insider threats. Symantec research found that 65 percent of organizations neglect to implement multi-factor authentication (MFA) as part of the configuration of IaaS and 80 percent don't use encryption.

65%

NEGLECT TO IMPLEMENT MULTI-FACTOR AUNTHENTICATION (MFA)

Bad Guys

Symantec research shows that 16 percent of outbound web traffic may come from compromised servers, directed to known command-and-control domains that control bots or other malware attacks. The external survey findings bear this out, with responding organizations rating an average of 11 website visits per week as risky, and 11 as malicious. While the numbers don't jump out on paper, if you do the math, the results add up to approximately 572 risky or malicious website visits a year, which significantly increases corporate exposure.

Internet of Things (IoT) devices are fast becoming another important attack vector. According to external survey respondents, the number of IoT devices causing IaaS incidents rose for seven in ten organizations over the last year.

572

RISKY OR MALICIOUS WEBSITE VISITS PER YEAR

Section

03

Best Practices for Building an Effective Cloud Security Strategy

More than half of respondents in the external survey confirmed their cloud security practices were not mature enough to meet the demands of the growing use of cloud apps, and nearly three-quarters said they experienced a security incident in cloud-based infrastructure due to this immaturity. Symantec's own data confirms that 85 percent of customers are not using Center for Internet Security (CIS) best practices.

Companies that continue to engage or accelerate cloud services without a plan to mature their security practices do so at their own peril. Organizations should consider these key steps to shore up their cloud security posture:

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

Section

04

Conclusion
Organizations Underestimate Cloud Risks at Their Peril

The heterogeneity of the modern enterprise environment has added a broader set of vulnerabilities and strike vectors. Huge visibility gaps leave organizations in the dark about how much and where data and workloads reside, making it harder to identify and mitigate mounting security risks.

Too many companies are not acknowledging the perception gap in cloud security and are vastly underestimating today's threats. Investment in cloud cyber security platforms that leverage automation and AI to supplement limited human resources is a clear way to automate defenses and enforce data governance principles. Beyond technology, it's time to recalibrate culture and adopt security best practices at a human level. It's a combination of both that will ensure the enterprise is sufficiently safeguarded today and more importantly, for tomorrow when it's anyone's guess what the future may bring.

About Symantec

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps organizations, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure.

Likewise, a global community of more than 50 million people and families rely on Symantec's Norton and LifeLock products to help protect their digital lives at home and across their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit www.symantec.com, subscribe to

Symantec Corporation World Headquarters
350 Ellis Street
Mountain View, CA 94043
United Stated of America
+1 650 527–8000
+1 800 721–3934

For specific country offices and contact numbers, please visit our website.
For product information in the U.S., call toll-free 1 (800) 745 6054.

Symantec.com

Symantec