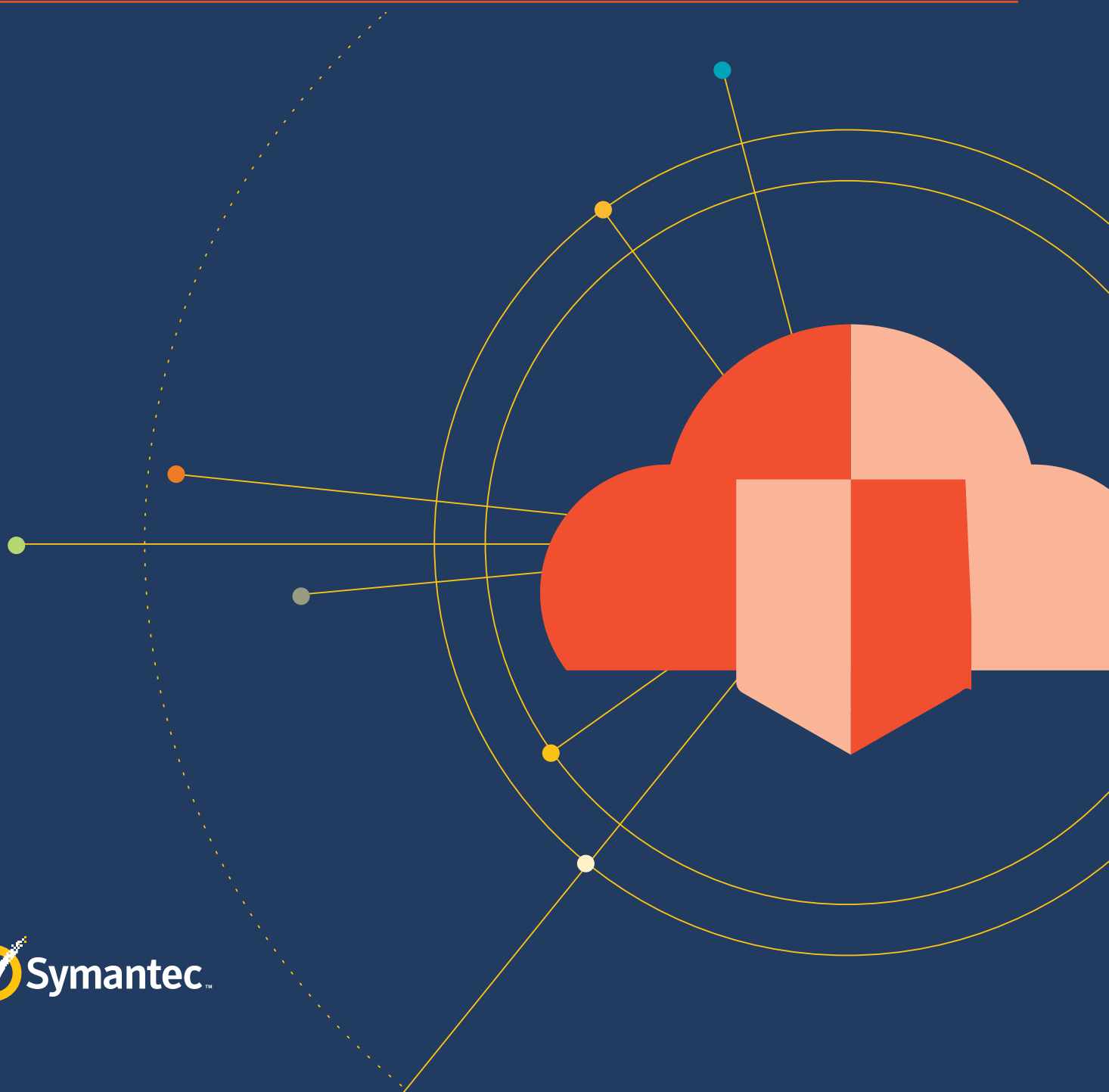
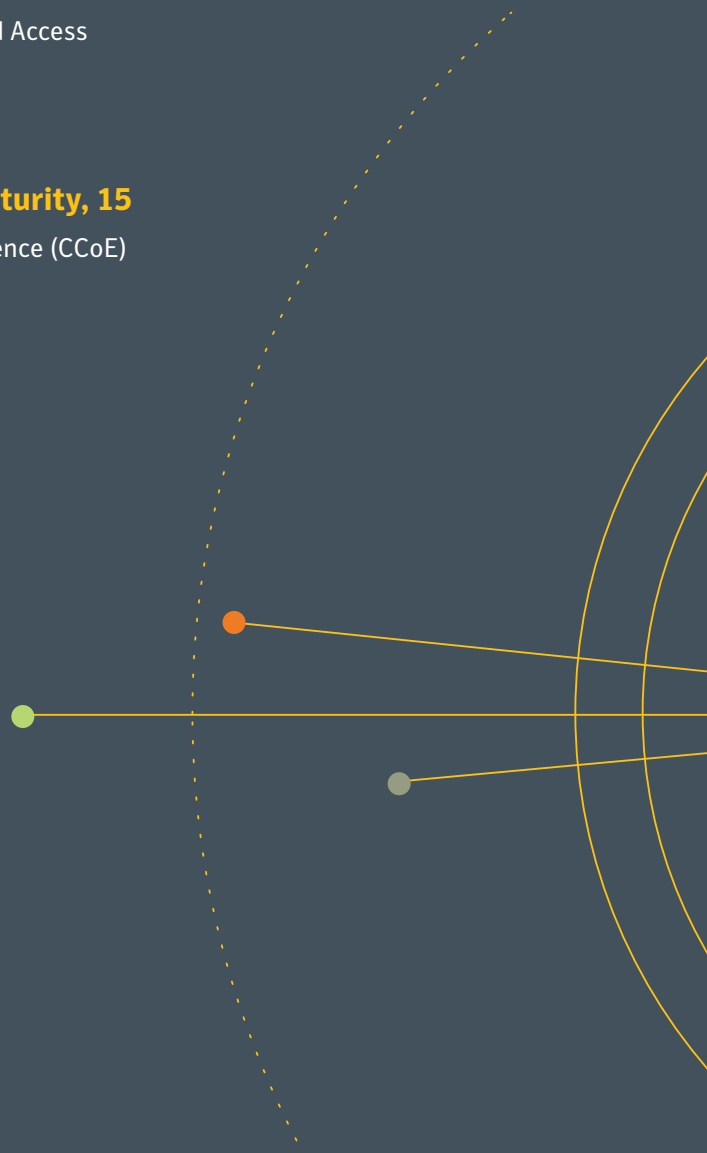
Cloud Security Threat Report (CSTR)
Volume 1 | June 2019

Adapting to the New Reality of Evolving Cloud Threats



Symantec™

Table of Contents



Preface

The Cloud Security Alliance (CSA) has always viewed cloud computing as having inherent security advantages when properly deployed, but the reality is that any fast-growing platform is bound to see a proportionate increase in incidents.

Organizations must realign and in some cases, reinvent their security programs for this new reality. Symantec's inaugural Cloud Security Threat Report (CSTR) helps shine a light on current challenges and provides a useful roadmap for your cloud security future.

Identity-related attacks are a critical threat vector in cloud, making proper identity and access management the fundamental backbone of security across domains in a highly virtualized technology stack. The speed with which cloud can be "spun up" and the often decentralized manner in which it is deployed magnifies human errors and creates vulnerabilities that attackers can exploit. A lack of visibility into detailed cloud usage hampers optimal policies and controls.

A Zero Trust strategy, building out a software-defined perimeter, and adopting serverless and containerization technologies are critical building blocks. Organizations must design security architectures with an eye towards scalability while embracing automation and cloud-native approaches like DevSecOps to help facilitate the new controls.

The good news is there is a plethora of solutions that address cloud security threats with the right mix of technology, process, and an educated workforce. The bad news is that many organizations are not aware of the full magnitude of their cloud adoption, the demarcation of the shared responsibility model, and are inclined to rely on outdated security best practices.

Cloud is the center of IT and increasingly, the foundation for cyber security. Understanding how threat vectors are shifting in cloud is fundamental to making the necessary updates to your security program and strategy. Symantec's CSTR shines a light on how to secure the digitally transformed, virtual organization of today and tomorrow.

Jim Reavis, co-founder and CEO, Cloud Security Alliance

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.

These challenges are forcing a rapid evolution in information security (InfoSec) roles, technologies, and practices. Employees and business units are adopting SaaS apps that bypass IT security reviews and management protocols for convenience and speed. The sheer volume of cloud apps and content makes it nearly impossible to maintain visibility and control without new and automated cloud-based security solutions as well as the skill sets and processes needed to effectively manage them.

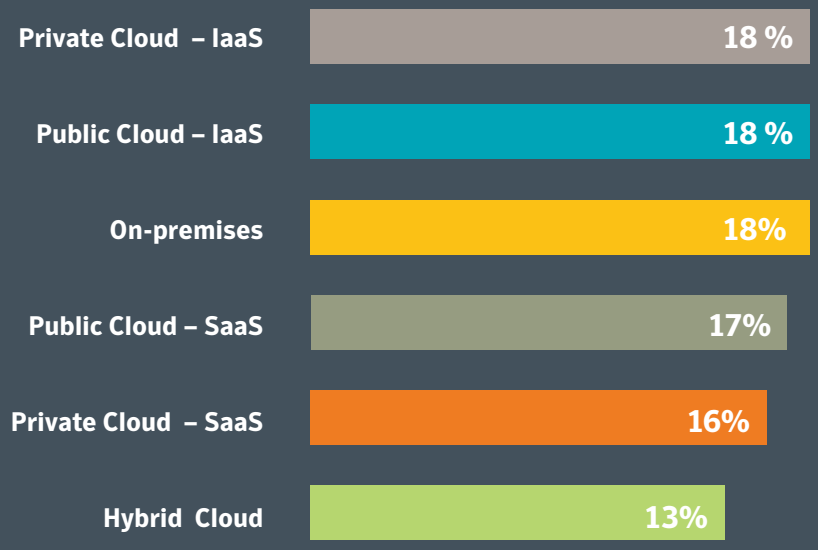
Symantec surveyed 1,250 security decision makers worldwide in Spring 2019 to understand the shifting cloud security landscape, the scope of Shadow IT and Shadow Data usage, and to gauge the maturity of security practices as enterprises transition to the cloud. Compared to aggregated and anonymized telemetry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

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.



93%

ARE STORING DATA IN MORE THAN ONE ENVIRONMENT

While most organizations (53 percent) are forging ahead with cloud deployment and using at least some form of cloud for their workloads, 69 percent of survey respondents are still storing some data on premises. This heterogeneity makes it difficult to achieve visibility across applications and workloads, ushering in a host of challenges that tax the expertise and bandwidth of IT staff and make some legacy cyber defense tools and processes obsolete.

Visibility is Cloudy

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

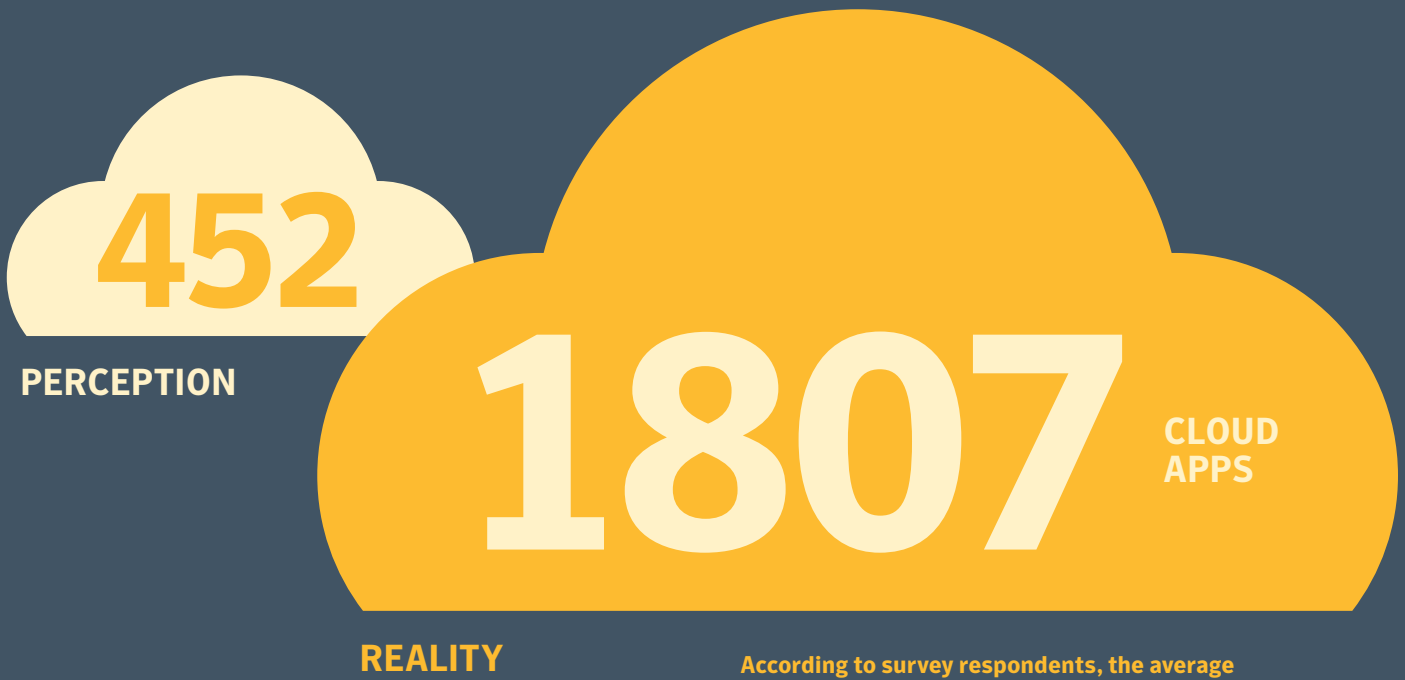
According to survey respondents, the average organization believes its employees are using 452 cloud apps. However, according to Symantec's own data, the actual number of Shadow IT apps in use per organization is nearly four times higher, at 1,807. Past Symantec Internet Security Threat Reports[1] (ISTR) confirm the scope of the disconnect: While CIOs reported their organizations use up to 40 cloud apps, the reality was vastly higher, in the 1,000 range. The spread reveals how difficult it is to gain visibility into cloud deployments when any department can budget and use a public cloud app service.

The visibility and control problem will only get worse. According to the survey, cloud app deployment increased 16 percent over the past 12 months and is expected to surge 21 percent over the next year. Unless CIOs get a firmer grip on the cloud apps used by their own organizations, they should expect that lack of visibility will lead to unwelcome surprises in both the scale of the problem, as well as how threats enter the environment.

The majority of workloads have also shifted to the cloud. On average, organizations report that over half (53 percent) of their workload has been migrated to the cloud. However, only a small minority (3 percent), 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. Interestingly, poor visibility into IaaS was called the top threat by just three in ten, and the most critical vulnerability by only one in ten, spotlighting again that perceptions and understanding are scrambling to keep up with the reality of poor visibility.

[1] Source: Symantec Internet Security Threat Report, Volume 22.

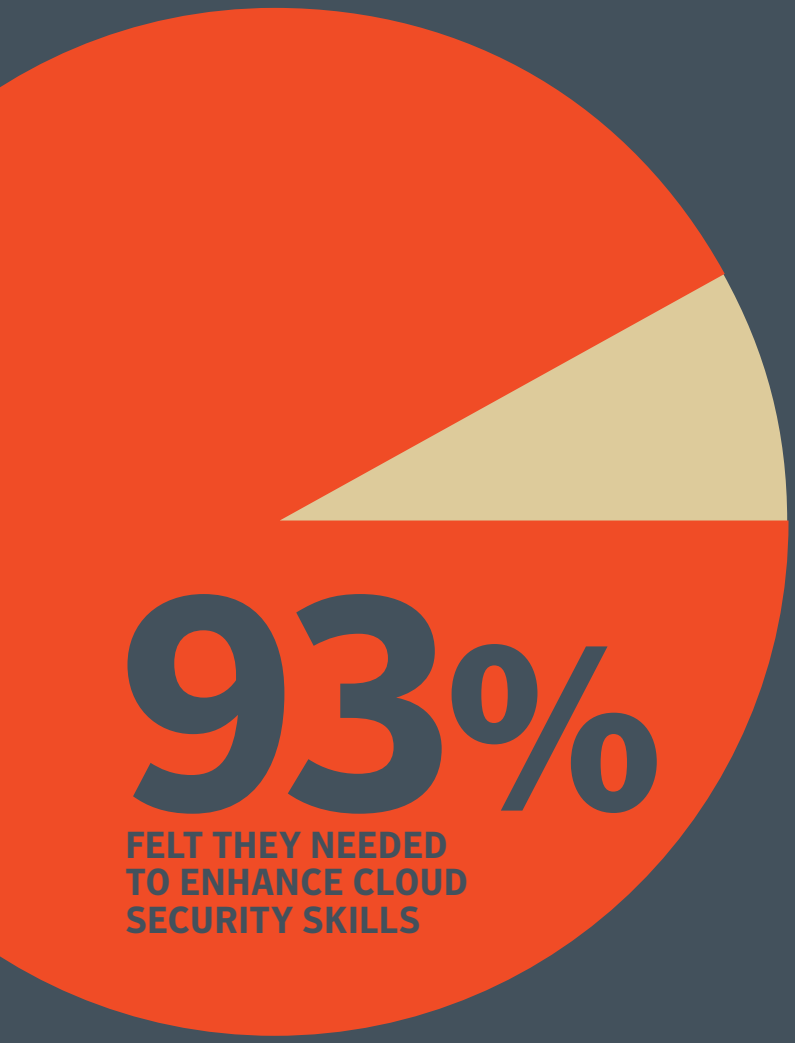


According to survey respondents, the average organization believes its employees are using 452 cloud apps. However, according to Symantec's own data, the actual number of Shadow IT apps in use per organization is nearly four times higher, at 1,807.

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 (92 percent) while 84 percent confirmed they needed to add staff to close the gap.

Only 27 percent of responding organizations were confident in their ability to address all cloud security alerts.



Employee Behavior is Risky Business

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

Section

02

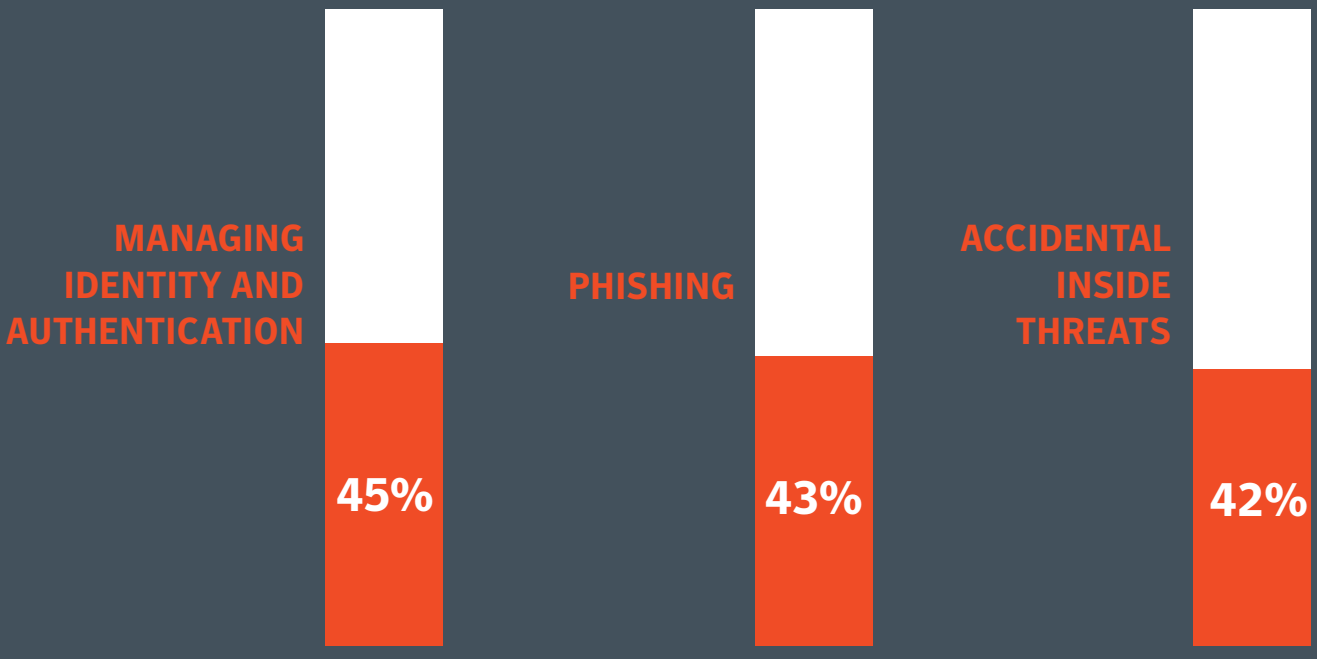
The Top Threats and What to Do About Them

New forms of cross-cloud attacks are on the rise even as InfoSec doubles down on more familiar terrain like tamping down malware and DDOS attacks. The Symantec external study found cloud malware injection is ranked second among cloud threats after data breaches, with one in five respondents confirming it consumes investigation resources.

Symantec's own data, however, indicates that unauthorized access accounts for the bulk of Cloud security incidents (64 percent), which encompasses a variety of both sophisticated and simple exploits. Digging deeper, companies are underestimating the scale and complexity of cloud attacks: File camouflage, account takeovers, and lateral-spreading threats constitute the bulk of risky behavior (70 percent) and provide gateways to cross-cloud attacks, cloud orchestration attacks, and side-channel attacks.

Account takeover in particular is a pervasive but under-rated problem due to the impact of shadow IT on visibility into cloud infrastructure. The external survey found only 7 percent of respondents calling out account takeover as one of their biggest risks, while Symantec data shows that 42 percent of risky behavior detected indicated potential cloud-account compromise. Without a lens into such activity, organizations are at a disadvantage for identifying and remediating them.

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



Get Risky Apps, Data, and Users Under Control

SaaS apps are available with a few clicks and a credit card. Employees can adopt them without telling IT and without enterprise security oversight. Unfortunately, many of these newly-adopted apps have inadequate built-in security—i.e. limited or no support for encryption or multi-factor authentication. 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.

93%

GRAPPLE WITH USERS OVERSHARING CLOUD FILES CONTAINING SENSITIVE AND COMPLIANCE-RELATED DATA

68%

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

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. Less than a third (31 percent) did not believe their data was at any risk.

Digging deeper, Symantec's data paints a more nuanced picture of the problem: 30 percent of all PHI (Protected Health Information) stored and shared in the cloud is over exposed, while 13 percent of PII (Personally Identifiable Information), and 8 percent of PCI (Payment Card Industry Data Security), is over exposed. Even in the healthcare industry, where controls are greater, 14 percent of PHI in the cloud is still overexposed, opening up companies in that sector to substantial financial risk due to the higher value of stolen PHI data on the black market.

How to Fix It

Instead of applying more manual effort into finding Shadow Data and IT, organizations should enlist advanced automation and analytics services to help identify and prioritize risky behaviors, identify malicious users, and escalate crucial security alerts. Tools such as a Data Loss Prevention (DLP) platform and a Cloud Access Security Broker (CASB) can help here. In addition, AI and machine-learning technology can accelerate analysis of targeted attacks, enabling organizations to direct limited resources to the most pressing problems.

Contain Risks from Misconfigured Servers, Malware, and Unauthorized Access

With more workloads shifting to IaaS and PaaS platforms such as AWS, Microsoft Azure, and others, it becomes critical to take a consistent approach to discovering, monitoring, and remediating service misconfigurations, malware, and inappropriate access and privileges.

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.

Additionally, organizations make things harder on themselves through complexity, duplication, and inefficient configurations. One in three survey respondents report that they are experiencing problems that create further risks, including lack of visibility and control, due to complexity of cloud configurations, duplication, and multiple server instances.

As organizations move to multi-cloud infrastructure environments, they face the challenge of managing a highly fragmented set of security and compliance controls. It becomes especially difficult when those controls are configured uniquely for each platform without consistent oversight. Security and DevOps teams should focus on centralizing their cloud security posture management and implementing security controls - such as identity, monitoring, and network policies - uniformly across environments.

How to Fix It

Security tools designed to discover, monitor, and remediate cloud workloads can deliver visibility and security across myriad cloud services. Cloud Access Security Brokers (CASB) can create a view across multi-cloud and on-premises workloads. In addition, Cloud Workload Protection (CWP) platforms help defend cloud workloads on IaaS and PaaS platforms against evolving malware attacks while addressing faulty configurations that can invite security breaches. A third pillar of protection is Cloud Security Posture Management (CSPM) that can assess the cloud infrastructure to ensure compliance with regulations while identifying security vulnerabilities.

Keep the Bad Guys Out

There's no question that bad guys are finding a way into organizations, many through risky websites. 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, though more likely to impact companies in Asia-Pacific (73 percent) and growing faster in Asia-Pacific region (22 percent) than compared to the Americas (19 percent) or Western Europe (21 percent). Given that security is all about metrics, the more IoT devices that connect to IaaS, the higher the chance one of these devices will be linked to a security incident.

How to Fix It

With employees accessing websites from anywhere and BYOD bringing massive amounts of devices into the enterprise ecosystem, it's critical to implement total endpoint security to protect devices, apps and networks against malware, ransomware and other emerging threats.

Recent industry attacks like the Petya ransomware have targeted decades-old cyber-physical systems to use the very protocols defined by the manufacturers against them.

It's important to implement control points protecting against USB-borne malware, network intrusion, and zero-day exploits. Deploying application whitelisting and sandboxing capabilities also can prevent malware from installing and executing.

Don't Ignore the Threat from Inside

External bad actors are not the only cause of security incidents and data breaches. 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. Employees are also participating in other high-risk behavior like relying on weak passwords, using personal devices for work, and shared single credentials. On average, the external survey found that 28 percent of employees are indulging in high-risk behavior that jeopardizes a firm's security posture.

65%

DON'T DEPLOY MULTI-FACTOR AUTHENTICATION AS PART OF THE CONFIGURATION OF IAAS

80%

DON'T USE ENCRYPTION

How to Fix It

Investment in training programs and other initiatives is crucial to getting users up to speed on new protocols to change risky behavior. Simultaneously, organizations need to find or cultivate new security talent to fill the gaps brought on with new technology or security tools.

Changing the company culture to support a shared security model can be the most important part of the process. Rather than writing off cloud security as someone else's job, users need to take ownership of avoiding bad practice in data hygiene and adhere to corporate standards like robust password policies, use of MFA and encryption, and avoiding personal devices for work-related tasks wherever possible.

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. Many bad habits go undetected until there is an incident, compounded by lack of visibility across the cloud landscape, and fewer than half of respondents do post-analysis of incidents to improve their cloud security practice. 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)

With a cloud governance strategy, organizations can establish and enforce consistent security policies and compliance across on-premises and cloud environments while deterring unsanctioned cloud usage. To support the effort, organizations should establish a CCoE made up of a diverse group of business stakeholders, including app development, sales and marketing, and security. All stakeholders are tasked to provide input into platform security, data controls, what's required for regulatory and internal compliance, and all the other elements comprising a mature cloud security posture.

Along with representation from core business groups, the CCoE must have executive sponsorship from a high-level leader with authority to enforce policy changes (for example, the CIO or CMO) in order to be effective. The CCoE, in concert with security teams, should take an iterative approach to improvement, building up the security posture over time based on the governance plan and with regular checkpoints to gauge success based on agreed-upon success criteria.

At the same time, companies can elevate their cloud security posture by embracing a cyber security framework, adapted specifically for cloud, that aids in effectively prioritizing and addressing risk consistent with their business goals and mission needs.

Embrace a Zero-Trust Model

The future of enterprise security lies with Zero Trust, a conceptual and architectural model that promotes a more holistic approach to information security with special focus on processes and technologies. Old-school security approaches authenticate and determine trust for users at the network's edge, allowing entrance to those who meet the criteria. With Zero Trust, no one gets a free pass anywhere on the network.

Zero Trust models a micro-segmented approach with granular protections applied to the data, and controls implemented at all points of access, including mobile devices, cloud workloads, and corporate networks. Data within the micro perimeters is classified based on sensitivity, and the architecture accounts for continuous change, allowing access rights to be modified based on behavioral risk scores and device type, among other factors.

Beyond segmentation and access controls, all network traffic is scanned and monitored for threats using tools such as email gateways and web gateways. The network segmentation and data isolation will minimize the impact of any potential breach. Any cyber-security solution enforcing Zero Trust should feature automated orchestration capabilities to lower the operational burdens on security teams.

Promote shared responsibility

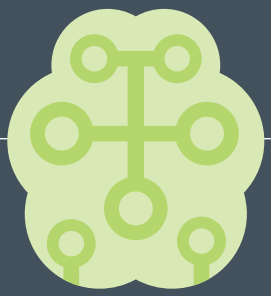
By its very definition, the public cloud is a shared security model with a cloud provider, which means organizations need to rethink their role and become much more active in managing security than they may have been in the past. With IaaS, for example, cloud service providers are responsible for protecting their clouds while customers must step it up and counter any vulnerabilities or exploits of their workloads.

To ensure the proper safeguards, the old way of designating a centralized IT or security organization needs to be replaced with a decentralized model where application owners take responsibility for security policies and practices as part of their development efforts and according to agreed-upon guidelines. That means everyone in the organization, executives and rank-and-file employees, need to become part of the company's security workflows and best practices. Organizations should be prepared to up their investment in security training and awareness efforts to ensure employees are cloud security savvy and committed to embracing the new, more secure way of working.

Use automation and artificial intelligence wherever possible

A growing number of security platforms have incorporated AI and machine learning to automate tasks and bring a higher level of intelligence to incident handling. This includes User Behavior Analytics, used to identify potential security risks by establishing a usage baseline over time to identify abnormal cloud activity. Underlying machine learning capabilities work in tandem with human-aided behavior analysis to find the proverbial needle in the haystack of existing security incident data.

Automating the compilation and modeling of existing network data using behavioral analytics not only helps organizations more readily identify and classify potential threats, it also makes them more efficient. Incident data should be parsed and automatically categorized, giving organizations insight into whether an event is problematic, a result of a broken business processes, or simply standard business behavior that requires a policy adjustment. In the end, accuracy and prioritization of incident handling is dramatically improved and the process becomes far more efficient, reducing the manual investigation and freeing up security staffers to redirect efforts toward actual incidents.



Make way for DevSecOps

Traditionally, security has been an afterthought for most applications, bolted on at the end and not integrated throughout the development process. Given agile development speeds, this model has broken. Enter DevSecOps, aligned with the DevOps movement, which is about inserting security practices into every step of the agile development process.

With DevSecOps, there is no longer one team solely responsible for code security—rather the development teams share responsibility by taking ownership of assessing security risks and fixing code as part of their core development process. Moreover, application security has evolved to fit within the release management pipeline, today recognized as the continuous integration/continuous delivery (CI/CD) practice fueled by automation.

Given the cloud's short release cycles, security testing and validation needs to move at the same speed and be part of the same release pipeline. A DevSecOps approach accomplishes just that, making security just another error class to manage much like a bug.

The AI Security Alliance (www.AIsecurityAlliance.org) predicts two major trends that will affect SaaS application security in the near term:

1. AI vs AI. **AI used by adversaries to subvert AI-based threat detection. These attacks would probe AI detection for cloud apps and determine appropriate attack responses. AI techniques, such as reinforcement learning (which uses human input to learn), can mitigate AI-enabled attacks.**

2. AI detection/remediation automation. **AI-enabled threat detection reduces time to attack detection by eliminating the human analyst. AI-enabled remediation would then execute appropriate security policy responses and test the remediation for resiliency through simulated attacks.**

Section

04

Conclusion
Organizations Underestimate Cloud Risks at Their Peril

The heterogeneity of the modern enterprise environment, spanning both on-premises and diverse cloud platforms, 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.

Without a clear picture into the cloud infrastructure, security organizations are grappling with issues from data duplication to the inability to identify threats in a timely manner, with a loss of control over data access and the protection to meet regulatory compliance.

A proper cyber security defense requires acknowledgement that Shadow IT and Shadow Data exist, assessing its scope, measuring the risk it poses, and then writing policies to secure it.

As development continues at lightning speed and data centers move cloudward, companies need to reevaluate their actual versus perceived risks, especially as business processes are digitalized and emerging technologies in the Internet of Things (IoT) open the door to new types of -as-a-Service product offerings and business models.

Too many companies are not acknowledging the perception gap in cloud security and are vastly underestimating today's threats, leaving themselves vulnerable to cloud account compromises and data exposures that pose substantial reputational and financial risk. 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—which is no easy feat considering all the change management challenges. 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.

Glossary

Business Readiness Rating (BRR) is a rating system developed by Symantec that indicates how secure a cloud app is for business use. It is calculated individually for tens of thousands of cloud apps based on numerous risk attributes, such as whether an app supports MFA or is SOC 2 compliant.

Cloud/SaaS Application: SaaS applications are cloud apps where the software and infrastructure are owned and managed by the application service provider but where you retain full control of the data, including who can create, access, share, and transfer information stored in the hosted application.

Data Exfiltration: Data exfiltration is the unauthorized copying, transfer or retrieval of data from a computer or server. Data exfiltration is a malicious activity performed through various different techniques, typically by cyber criminals over the internet or other network.

Data Oversharing: Data oversharing is the practice of employees uploading documents that contain sensitive information to cloud-based file sharing services.

File Camouflage: File Camouflage is the practice of hiding information to exfiltrate it by making it look like something else. For instance, an attacker could put data inside a file and call it an image, or utilize steganography – the practice of concealing messages or information within other non-secret text or data.

Infrastructure-as-a-Service (IaaS): Infrastructure-as-a-service refers to online services that provide high-level APIs used to dereference various low-level details of underlying network infrastructure like physical computing resources, location, data partitioning, scaling, security, backup etc.

Lateral Spreading Threats: Lateral Spreading Threats refer to when an attacker has made it inside of an entity (e.g., network or machine) and wants to spread to other nodes. Attackers use this technique in order to compromise someone in the organization with escalated privileges or until they find the information they want.

Shadow IT: In the context of the cloud, Shadow IT refers to the adoption and use of SaaS apps without the IT department's oversight or sanction. Proliferation of Shadow IT can result in users storing and sharing confidential data in apps with inherent security risks or that are unmanaged by the IT department, increasing the likelihood of data loss or destruction.

Shadow Data: Shadow Data comprises all of the unmanaged content that users are uploading, storing, and sharing not only using unsanctioned cloud apps, but sanctioned ones as well.

User Behavior Analytics (UBA): User Behavior Analytics is a cyber security process used for the detection of insider threats, targeted attacks, and financial fraud. UBA solutions look at patterns of human behavior, and then apply algorithms and statistical analysis to detect meaningful anomalies from those patterns—anomalies that indicate potential threats. Instead of tracking devices or security events, UBA tracks a system's users.

Methodology

The Symantec Cloud Security Threat Report (CSTR) is the product of analysis and correlation of data between an external market study and data sourced from Symantec products and services, as described below.

In the spring of 2019 Symantec commissioned Vanson Bourne, a market research company, to conduct 1,250 interviews with cloud and IT security decision makers in the US, Canada, Brazil, Mexico, France, Germany, Italy, the UK, Australia, Japan, and Singapore. Respondents all worked at organizations with at least 250 employees, across a range of public and commercial sectors. To find out more about Vanson Bourne and their research, you can visit their website www.vansonbourne.com

Symantec CloudSOC™ CASB Audit tracks customer cloud app usage of tens of thousands of cloud and mobile apps along with their individual Business Readiness Rating (BRR). Symantec CloudSOC CASB Securlets includes an intrinsic DLP function, ContentIQ™, that tracks, classifies, and determines exposure of billions of cloud stored files, emails, and email attachments stored and shared by Symantec CloudSOC customers. The Symantec Detect function used by CloudSOC CASB includes User Behavior Analytics (UBA) functionality to detect activities by CloudSOC users which are indicators of compromise. Detect assigns a risk score to each CloudSOC user. All data derived from CloudSOC for this report is aggregated and anonymized to protect customer confidentiality.

The Symantec Global Intelligence Network (GIN) comprises more than 123 million attack sensors, recording thousands of threat events per second, and contains over 9 petabytes of security threat data. This network also monitors threat activities for over 300,000 businesses and organizations worldwide that depend on Symantec for protection. Telemetry from across Symantec's threat protection portfolio helps our 3,800 cyber security researchers and engineers identify the top trends shaping the threat landscape.

Analyses of spam, phishing, and email malware trends are gathered from a variety of Symantec email security technologies processing more than 2.4 billion emails each day, including: Symantec Messaging Gateway for Service Providers, Symantec Email Security.cloud, Symantec Advanced Threat Protection for Email, Symantec's CloudSOC™ Service, and the Symantec Probe Network. Symantec also gathers phishing information through an extensive anti-fraud community of enterprises, security vendors, and partners.

Filtering more than 322 million emails, and over 1.5 billion web requests each day, Symantec's proprietary Skeptic™ technology underlies the Symantec Email and Web Security. cloud™ services, utilizing advanced machine learning, network traffic analysis, and behavior analysis to detect even the most stealthy and persistent threats. Additionally, Symantec's Advanced Threat Protection for Email uncovers advanced email attacks by adding cloud-based sandboxing, additional spear-phishing protection, and unique targeted attack identification capabilities.

Billions of URLs are processed and analyzed each month by Symantec's Secure Web Gateway solutions, including ProxySG™, Advanced Secure Gateway (ASG), and Web Security Solution (WSS), all powered by our real-time WebPulse Collaborative Defense technology and Content Analysis System, identifying and protecting against malicious payloads and controlling sensitive web-based content.

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