ORACLE

KPMG

ORACLE AND KPMG CLOUD THREAT REPORT 2019

Defining Edge Intelligence: Closing Visibility Gaps with a Layered Defense Strategy

Contents

Foreword

Mary Ann Davidson, CSO, Oracle Corporation, and Tony Buffomante, US Cyber Security Services Leader, KPMG LLP

The Oracle and KMPG Cloud Threat Report 2019 examines emerging cyber security challenges and risks that businesses are facing as they embrace cloud services at an accelerating pace. The report provides leaders around the globe and across industries with important insights and recommendations for how they can ensure that cyber security is a critical business enabler. Cyber security leaders and practitioners can use this report to educate lines of business about the real security risks the cloud can present.

With cloud services now critical to all aspects of business operations, the demand for speed and agility is coupled with the expectation of greater security. In fact, 73% of survey respondents indicate the cloud offers a more secure environment than they can provide on-premises. This perception has resulted in continued and growing cloud adoption: a clear majority of organizations have increased the amount of business-critical information they host in the cloud.

With business and cyber goals so completely interdependent—and the risk of data loss or misuse so dire—enterprise leaders need to find new ways to align their business and cyber strategies. This effort starts with enabling full visibility across the hybrid cloud environment – identifying misconfigurations, managing patches and misuse – and it continues with strategic risk mitigation plans. Cyber security must be embedded within all aspects of the cloud—including development, integration, deployment, monitoring and maintenance.

In this environment, accountability is critical, both for providers and their customers. Providers must explain the security responsibility demarcation lines so that customers better understand their role in maintaining a secure posture. For their part, customers need to identify their critical assets, look at their top risks, and ask the questions that will let them know whether a particular provider is capable of helping manage those risks. Knowing what data is where is a top challenge, especially with so many new cross-border regulations that vary depending on where data is collected.

“With cloud services now critical to all aspects of business operations, the demand for speed and agility is coupled with the expectation of greater security.”

Developers need to give initial attention to securing applications and data, and business leaders need to consider the value of the data to the business and the impacts to the business if that data is compromised. Unless companies take security into account up front, there will always be an unrealistic and unsustainable reliance on people and manual processes, posing numerous risks to business value and operations.

The cyber security skills gap is indeed a significant problem. Strategies such as managed service providers, strategic partners, increased training, and accelerated recruiting should be considered as potential business enablers. Those who leverage advanced technologies such as machine learning will see an increase in output and allow bandwidth for a greater focus on strategic planning. The need to address the skills gap underscores the importance of all sides understanding risk tolerance in line with business strategy.

> “Machine learning, automation, the speed at which we can execute security processes – it’s all resulting in minimal downtime for some customers and the enhanced ability for all to use cyber security as a business enabler.”

For all the concerns about the accelerating pace of change, emerging technology developments continue to strengthen cyber security teams’ ability to support the business. The ability to help address vulnerabilities automatically is very exciting. Machine learning, automation, the speed at which we can execute security processes – it’s all resulting in minimal downtime for some customers and the enhanced ability for all to use cyber security as a business enabler. These services and technologies are maturing to the point that we can really start to make headway mitigating points of exposure, in keeping with business strategy.

At the end of the day, it will always cost less to prevent problems than to fix them. We hope the insights and recommendations in this report will help you in your own efforts to align cloud security with the goals of business strategy.

Executive Summary

Public cloud-hosted and -delivered services have become the centers of gravity for many organizations' information technology infrastructures. Cloud applications and platform services have enabled businesses to move faster than ever, intensifying organizational dependence on the availability, integrity, and security of those services. Last year's Oracle and KPMG Cloud Threat Report explored market research that revealed how organizations are struggling to keep pace with the speed and scale at which their businesses are using cloud services, creating a cloud security readiness gap. A year later, it is clear that the business-critical nature of cloud services has substantially raised the stakes for securing public cloud assets. IT organizations are operating with a strategic imperative to address a myriad of both old and new cybersecurity challenges, highlighting the need to retool the foundational elements of a cybersecurity program to bring the cloud into scope. We'll discuss both the challenges of and strategies for securing the business cloud by exploring the following key findings in the *Oracle and KPMG Cloud Threat Report 2019:*

- **The mission-critical nature of cloud services has made cloud security a strategic imperative.** Cloud services are no longer nice-to-have tertiary elements of IT—they serve core functions essential to all aspects of business operations.
- **Confusion around the shared responsibility security model has resulted in cybersecurity incidents.** A lack of clarity on this foundational cloud security construct has had real consequences for many enterprises, including the introduction of malware and loss of data.
- **Visibility remains the top cloud security challenge.** The fact that the infrastructure that hosts and delivers cloud services is managed by a third party can create a visibility gap that existing network-based security controls are ill-fitted to address.
- **Cloud adoption has expanded the core-to-edge threat model.** An increasingly mobile workforce accessing both on-premises and cloud-delivered applications and data dramatically complicates how cybersecurity professionals must think about their risk and exposure.
- **CISOs are too often on the cloud security sidelines.** The decentralized adoption of cloud services by line of business leaders who do not follow approval methodologies creates a visibility gap for the organization's cybersecurity leaders.
- **Shadow IT continues unabated.** SaaS consumption, empowered by the line of business, driven by the need for fast time-to-value, and enabled by the consumerization of IT, is here to stay, independent of attempts to control usage with policies.

- **Intelligent automation is gaining steam to address long-standing patching issues.** The operational obstacles to better patching practices are starting to be addressed by automating the never-ending patch cycle to help protect vulnerable systems against exploits.

- **Passwords are past due.** The headache of password management, poor password hygiene, and the friction of introducing a second factor of authentication are being replaced with new primary factors of authentication and adaptation for the secondary factors.

- **Machine learning is being employed to improve the fidelity and frequency of triaging security events.** Of the many use cases for machine learning, organizations are leveraging this important technology to bring some relief to security event fatigue, improving the accuracy and scale of security analytics.

KEY RESEARCH FINDINGS

7 of 10
Use more business-critical cloud services YoY

3.5x
Increase in organizations with 50% of their data in the cloud 2018-2020

93%
Are dealing with rogue cloud app usage

1 in 10
Organizations can analyze 75%+ of their security events

45%
Plan to deploy automated patch management in the next 24 months

85%
Are interested in replacing passwords with new forms of authentication

82%
Of cloud users have experienced security events due to confusion over Shared Responsibility Security Models

53%
Are using machine learning for cybersecurity purposes

Save for younger, cloud-native companies, the use of public cloud services now represents a critical dimension of a hybrid and multi-cloud data center. As such, an appreciation and understanding of both the old and new is essential to evolve an organization's cybersecurity program that contemplates protecting traditional infrastructure as well as the increasingly critical set of cloud services.

1

Cloud Services Have Become More Business-critical

Organizations are increasingly relying upon cloud services for business operations and trust them to store sensitive data

The Use of Cloud Services Continues to Grow

There is no denying the wealth of benefits businesses realize in leveraging cloud applications, often collectively summed up as agility. It is now well understood that SaaS applications help eliminate the cost and complexity associated with on-premises infrastructure and that its self-serve nature empowers lines of business to accelerate time to value. With 84% of organizations who participated in this year's research sharing that SaaS services are in use at their company, use is near-ubiquitous. The lack of comprehensive visibility into the use of shadow IT cloud applications, as discussed later, is such that the actual usage of SaaS applications is likely even higher.

The digital transformation of the enterprise is about more than simply consuming SaaS apps. Many non-technology companies are now developing their own custom software internally and by doing so are becoming software companies in their own right. It is through this lens that the ongoing adoption of both infrastructure- and platform-as-a-service should be viewed. This year's report saw a notable year-over-year increase in both types of cloud services, especially PaaS, environments designed specifically to expedite the development of new applications.

> Nearly half (49%) of all respondents expect to store the majority of their data in a public cloud by 2020."

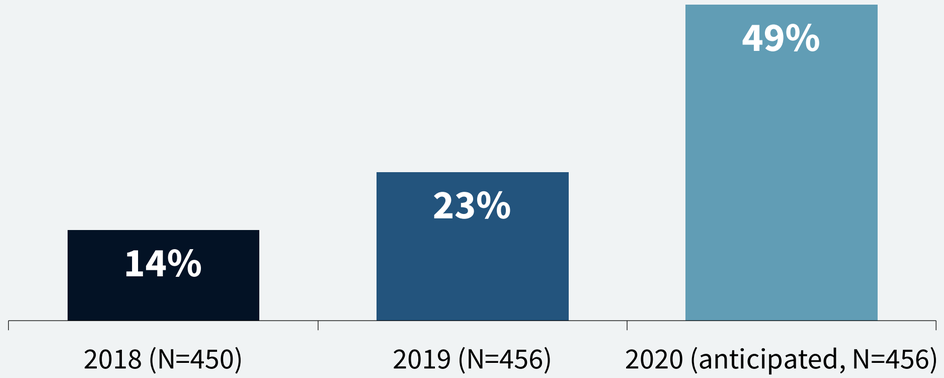
One result of the continued expansion of cloud services is that cloud services are becoming the primary data store for many organizations. In fact, over 50% of participating North American organizations already have 26% or more of their data in the cloud, and nearly half (49%) of all respondents expect to store the majority of their data in a public cloud by 2020 .

However, not all stakeholders share the same assessment of how much of their company's data is and will be stored in a public cloud service. For example, 53% of the surveyed CISOs stated that 25% or less of the company's data is currently in a public cloud compared with only 34% of CIOs. This disparity between CISOs and CIOs is troublesome as it indicates a lack of awareness and involvement in the use of cloud services by one of the organizational leaders responsible for securing that usage. To be clear, CIOs and CISOs, along with other leaders, including the Chief Privacy Officer, Data Protection Officer, line of business leaders, and others share the responsibility to secure their organization's data, irrespective of location.

RESEARCH HIGHLIGHT

Percentage of organizations with more than 50% of their data in any public cloud.

(Percent of respondents)



North America orgs have more cloud-resident data (> 50% = 26%)

CISOs more often believe 25% or less of company data is cloud-resident (53%) versus CIOs (34%)

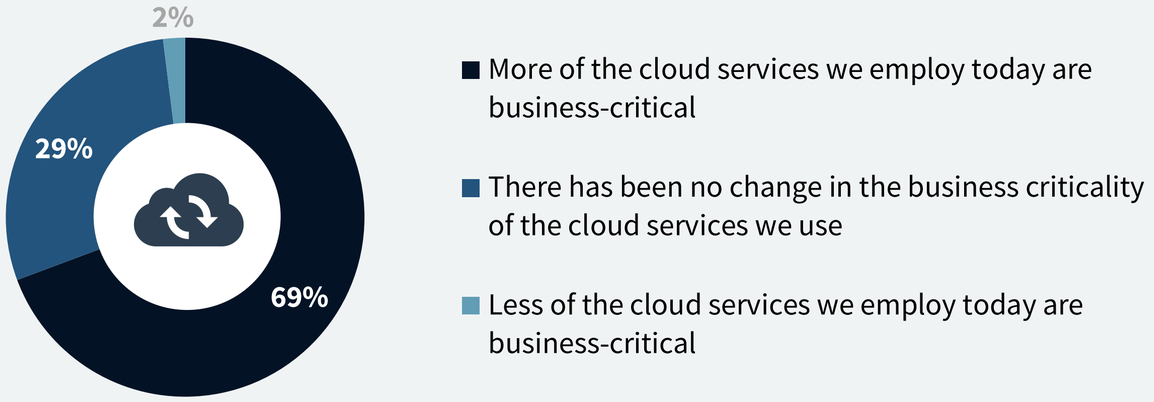
Confidence Has Increased the Strategic Nature of Cloud Services

The adoption of cloud services has grown, and so has the confidence in public clouds. A notable 72% of participating organizations shared that they view public clouds as much more or somewhat more secure than what they can deliver on-premises, a 10 percentage point increase from last year's study. Increased confidence coupled with cloud-first initiatives has increased not only the consumption of cloud services, but also their strategic role for the business.

RESEARCH HIGHLIGHT

How has the nature of the cloud services used by your organization changed, if at all, in the last 12 months?

(Percent of respondents, N=456)



> "A notable 69% of respondents stated that more of the cloud services they use are business-critical compared with 12 months prior."

To that point, when asked how the importance of cloud services used by their organization has changed, a notable 69% of respondents stated that more of the cloud services they use are business-critical compared with 12 months prior.

Such a perspective on the criticality of the cloud is in contrast to just a few years ago when cloud applications and services were viewed as complementary but less important to on-premises IT infrastructure. This evolved view of the importance of cloud services is an acknowledgement by respondents of the cloud's central role in meeting the business needs of their organization.

> The amount of any organization's sensitive data that is cloud-resident serves as a reasonable proxy for just how business-critical cloud services have become."

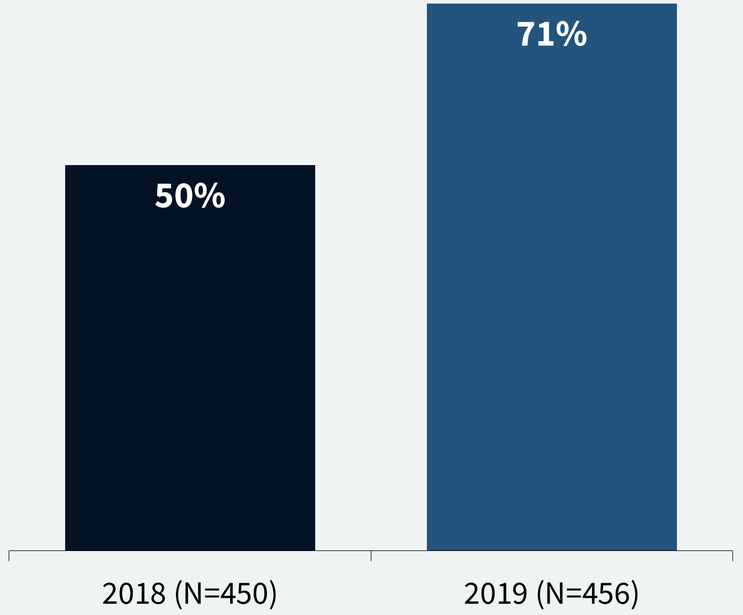
Spotlight: The Sensitive Data Proxy

As has always been the case in any IT environment, the principal resource is the data created by users, applications, and sensors, whether that data resides on-premises or in a cloud service. Today's data-driven business models make securing data assets even more critical. But not all data content is of equal value to a business; it's the data an organization deems to be sensitive that warrants the strongest levels of protection. As such, the amount of any organization's sensitive data that is cloud-resident serves as a reasonable proxy for just how business-critical cloud services have become. The sensitive data measuring stick has grown appreciably over the last year, with 71% of organizations reporting that the majority of their cloud-resident data is sensitive, a sizable increase from the 50% of organizations who said the same in last year's report. Contributing to this year-over-year increase are regulatory requirements, especially those that are data-privacy-related, that expand the types of data businesses must now treat as sensitive.

RESEARCH HIGHLIGHT

Percentage of respondents reporting the majority of public-cloud resident data is sensitive.

(Percent of respondents)



2

The Dependency on Cloud Services Is Compounding Cybersecurity Challenges

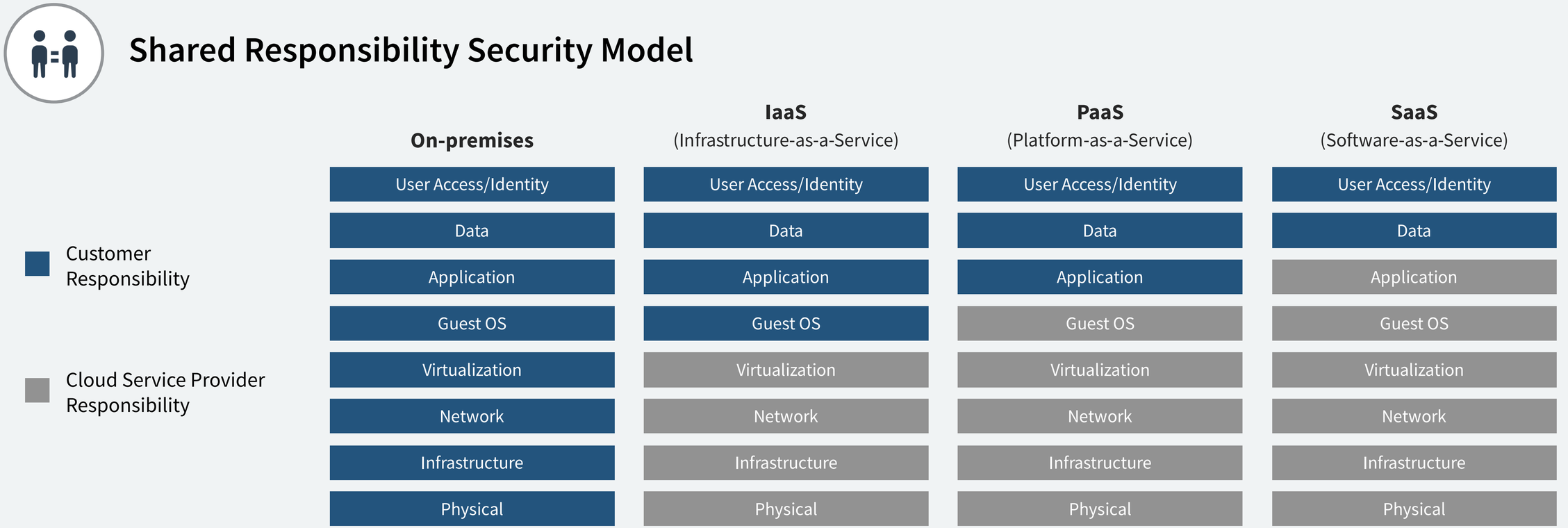
An expanded attack surface contributes to alert storms and the skills shortage, but focus and funding has improved.

Cloud Security Is a Confusing Shared Responsibility

Of all the challenges associated with securing cloud services, perhaps the most noteworthy is the level of confusion around the shared responsibility security model (SRSM), the primary foundational construct of a cloud security strategy. The shared responsibility security model, in essence, depicts the division of labor between the cloud service provider (CSP) and the subscriber of a given cloud service for how that service, including the associated data, is secured. Gaining clarity on the demarcation line between CSP and customer and removing all ambiguity is critical for businesses using cloud services.

> “Of all the challenges associated with securing cloud services, perhaps the most noteworthy is the level of confusion around the shared responsibility security model.”

Shared Responsibility Security Model



While many CSPs will provide some native cloud security controls such as data encryption, it is still the responsibility of the customer to apply and manage those controls or those provided by a third party. It is ironic that the less the customers are responsible for, the more they're confused about their obligations. To that point, more than half of the research participants (54%) reported confusion with the shared responsibility security model for software-as-a-service (SaaS) versus 47% who said the same for infrastructure-as-a-service (IaaS).

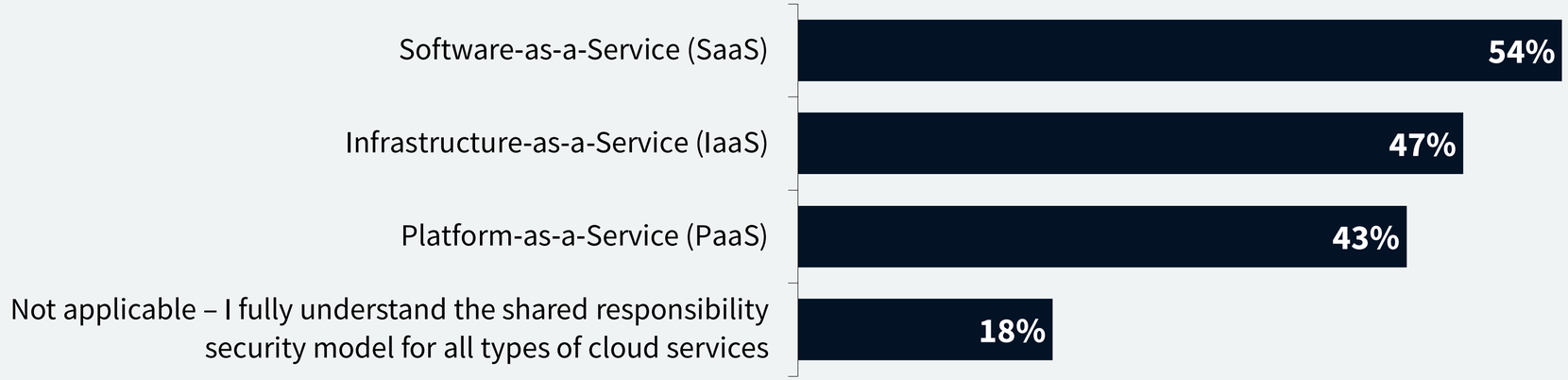
Perhaps most concerning is that those who should be most knowledgeable about the shared responsibility security model are not. Only 10% of the CISOs in this year's research fully understand the shared responsibility security model, compared with 25% of CIOs who report no confusion. Cybersecurity leaders' lack of complete clarity on the model is indicative of their lack of involvement in the use of cloud services, which is often driven autonomously by lines of business. As discussed below, cloud security architects can help bridge that gap as the resident expert in the shared responsibility security model.

"Perhaps most concerning is that those who should be most knowledgeable about the shared responsibility security model are not."

RESEARCH HIGHLIGHT

For which of the following types of cloud services do you find the shared responsibility security model the most confusing?

(Percent of respondents, N=456, multiple responses accepted)



Only 10% of CISOs state they fully understand the SRSM model (versus 25% CIOs)

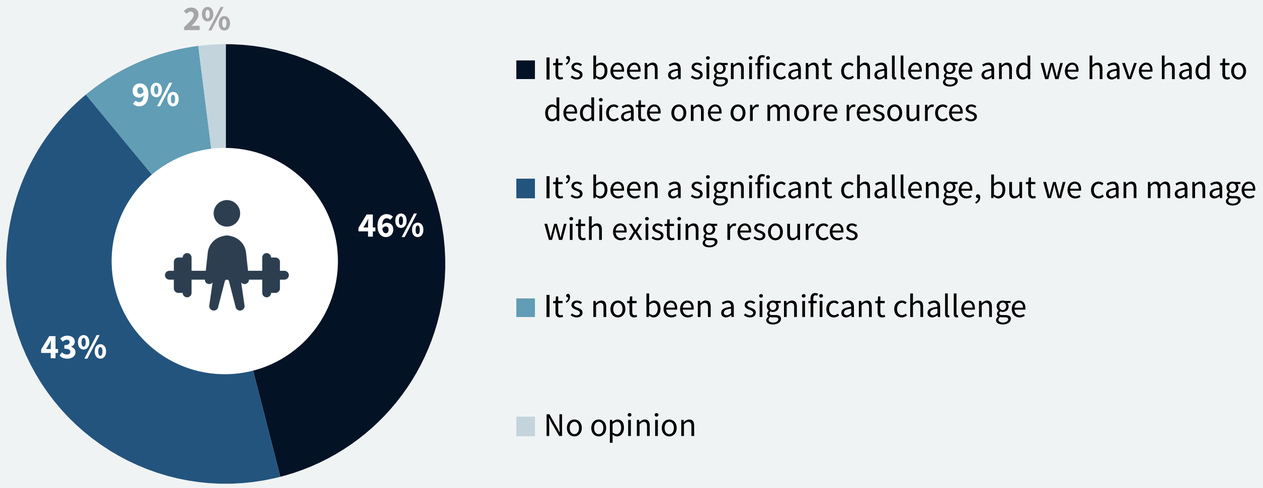
Confusion about SRSM has come at a cost, with over a third of organizations participating in this year's research sharing that such confusion has led to the introduction of malware (34%) and a similar number of respondents (32%) noting it has exposed them to increased audit risk. This lack of a clear understanding of the shared responsibility security model has also put data at risk, with 30% of organizations reporting that, as a result, data was accessed by unauthorized individuals. Additionally, 29% of respondents reported an unpatched or misconfigured system was compromised as a result of confusion, highlighting the fact that public-facing cloud infrastructure is constantly subject to botnet attacks exploiting improperly configured public services.

Contributing to the confusion is a lack of consistency in the model between cloud service providers, which has also had ramifications. Keeping current with the differences between CSPs, sometimes nuanced ones, is a significant challenge, one that 46% of respondents indicated required one or more dedicated resources to manage. Confusion, and the resulting consequences, around the differences in the shared responsibility security model between CSPs is, in part, the cost of using multiple CSPs.

RESEARCH HIGHLIGHT

Which of the following best represents the effort required to maintain a clear understanding of the differences in the shared responsibility security model between different cloud service providers (CSPs)?

(Percent of respondents, N=456)



Security Visibility Has Become More Cloudy, Increasing Event Storms

Reports such as these tend to enumerate cybersecurity challenge upon challenge. While there are certainly plenty of challenges to go around again this year, there is also some good news indicating progress.

The notion of a visibility gap created by the use of cloud services once again takes the top spot as the biggest cybersecurity challenge faced by participants in this year's study. Specifically, a third of the respondents cited detecting and reacting to events in the cloud as their top cybersecurity challenge. CISOs are particularly aware of the cloud security visibility gap, with 38% citing the inability of network security controls to provide visibility into public cloud workloads as their top cloud security challenge. This view on the lack of applicability of network security controls is rooted in the shared responsibility security model in which cloud services providers are responsible for securing the lower levels of the Open Systems Interconnection (OSI) model. Customers simply do not have access to network tap and span ports. As such, IT and cybersecurity teams need to use purposeful controls designed to provide visibility into the layers of cloud services customers are responsible for securing.

RESEARCH HIGHLIGHT

What are the biggest cybersecurity challenges currently experienced by your organization today?

(Percent of respondents, N=456, three responses accepted, five most frequently reported challenges shown)

> "CISOs are particularly aware of the cloud security visibility gap, with 38% citing the inability of network security controls to provide visibility into public cloud workloads as their top cloud security challenge."

A lack of visibility is not exclusive to the cloud, however, with visibility across the attack surface inclusive of the network and endpoints also of concern. The visibility issue spans the full spectrum of how cybersecurity and IT leaders should think of core-to-edge monitoring and response.

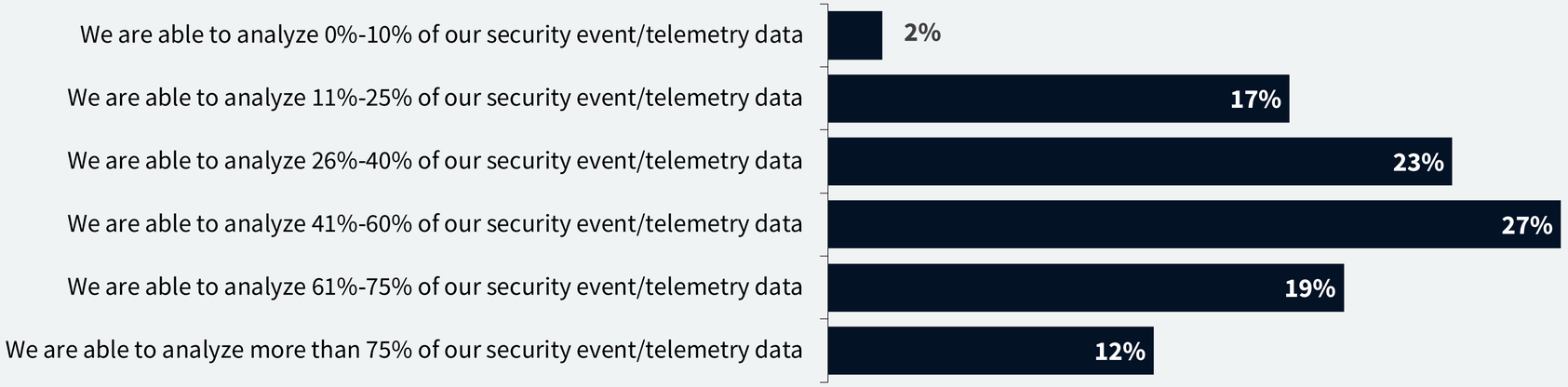
> It is startling that only one in ten participating organizations are able to process over 75% of their security event data."

The challenge of keeping pace at scale discussed in depth in last year's Oracle and KPMG Cloud Threat Report surfaced again this year in different areas of the study, but most prominently when it comes to an organization's ability to collect and analyze security telemetry/event data. The inability to analyze and respond to security events is a long-standing issue and one that has been at the center of numerous prominent data breaches. It is startling that only one in ten participating organizations are able to process over 75% of their security event data. As such, the vast majority of companies lack visibility currently by being unable to process the growing stream of security event telemetry. This is akin to driving without side and rearview mirrors or other sets of such guardrails. Moreover, the fact that detecting and reacting to security incidents in the cloud was the most-cited cybersecurity challenge indicates respondents are concerned this challenge of scale will only get worse. In the context of the shared responsibility security model, this concern is specific to incidents the subscriber is responsible for investigating, not those targeted at lower levels of the infrastructure for which the CSP is responsible.

RESEARCH HIGHLIGHT

How would you describe your organization's ability to collect and analyze security event/telemetry data at scale (i.e., across the entire enterprise)?

(Percent of respondents, N=456)



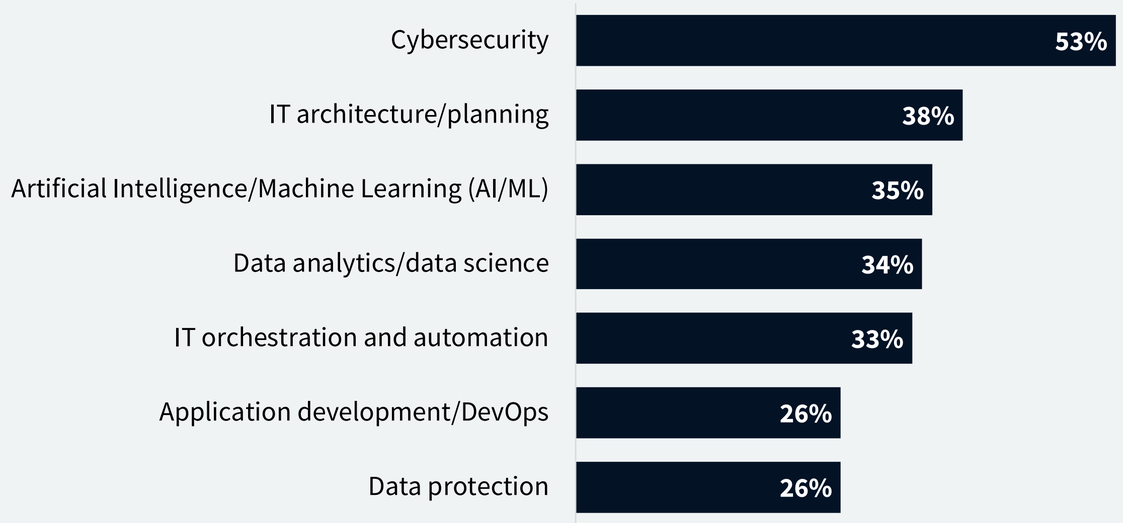
CIOs 2x more likely to report ability to analyze more than 75% of data versus practitioners (16% v 8%).

But respondents present varying perspectives on the processing of security events based on their respective roles and responsibilities. CIOs, for example, are more likely than hands-on cybersecurity practitioners to state that their organization is able to process more than 75% of their event data. Why this disparity? Security leaders and practitioners are more aware of the breadth of event data, including application and network performance events, that provide the telemetry necessary to gain a full picture of activity. CIOs, on the other hand, likely have a more myopic view of what constitutes a security event as only those generated from security controls.

RESEARCH HIGHLIGHT

In which of the following areas do you believe your IT organization currently has a problematic shortage of existing skills?

(Percent of respondents, N=586, multiple responses accepted)



> “Contributing to an inability to process security events is an acute shortage of cybersecurity skills.”

Contributing to an inability to process security events is an acute shortage of cybersecurity skills, second most-frequently cited cybersecurity challenge cited by our participants. A related ESG research study highlights this issue, with 53% of organizations stating cybersecurity is an area in which they have a problematic shortage of skills.[1] Another study predicts there will be 3.5 million cybersecurity unfilled jobs by 2021, contributing to zero unemployment for cybersecurity professionals.[2]

So, what about the good news promised at the outset of this section? Participants did, in fact, share some reasons for optimism. Concerns about lack of leadership engagement, funding, and consistent policies across disparate environments were all cited less often year-over-year, representing an overall improvement in organizational focus on cybersecurity.

[1] Source: ESG Research, *2019 Technology Spending Intentions Survey*.
[2] Source: Cybersecurity Ventures, *Cybersecurity Unemployment Rate Drops to Zero Percent*, September 2016.

Spotlight: Cloud Adoption Is Creating New Challenges and Exacerbating Old Ones

In addition to cloud adoption further complicating security event management, cloud-specific security challenges span technology, organizational dynamics, and compliance concerns.

The most-frequently cited cloud security challenge in this year's study reminds us that configuration management is a critical security discipline, especially when considering the immutable nature of production cloud-resident server workloads, which are typically not updated or patched. It is in this context that the largest percentage of research respondents cited maintaining secure configurations for server workloads as one of their top cloud security issues (39%).

That is, what is pushed to production better be hardened, and if it's proven otherwise, intelligent automation must be employed to orchestrate the deployment of a new build to close the attack window.

RESEARCH HIGHLIGHT

Which of the following represents the biggest cloud security challenges for your organization?

(Percent of respondents, N=456, five responses accepted, seven most frequently reported challenges shown)

While satisfying one's security team that public cloud infrastructure is secure is still a top cloud security challenge (38%), this proverbial horse of cloud adoption has long since left the barn, leading to the next top challenge: maintaining strong and consistent security across data centers and public clouds (38%). Participants in this year's study recognize the need for a change in modality from silos to a unified approach. The use of separate controls by siloed teams securing different environments creates operational overhead. A unified approach is likely to yield greater efficiencies and fosters consistency of security policies across disparate infrastructures of a hybrid cloud.

> "30% of respondents to the Oracle/KPMG research survey cited the inability of their network security controls to provide visibility into cloud-resident server workloads as a top cloud security challenge."

Other cloud security challenges from this year's study reveal the ineffectiveness of existing controls to secure public cloud applications, infrastructure, and data. While network security continues to be the top area of cybersecurity investment reported by respondents in ESG's 2019 Technology Spending Intentions research,[3] 30% of respondents to the Oracle/KPMG research survey cited the inability of their network security controls to provide visibility into cloud-resident server workloads as a top cloud security challenge. Similarly, 30% of respondents noted the lack of support for DevOps tools as a top cloud security challenge. It is encouraging that respondents are aware of the need to employ purposeful controls that are designed for public cloud environments, including those that integrate natively with the DevOps tools used by their application development teams.

[3] Source: ESG Research, *2019 Technology Spending Intentions Survey.*

3

Today's Diverse Threat Landscape Spans Core-to-edge

Organizations must secure core-to-edge applications and data and improve awareness.

Phishing Attacks are Targeting Cloud Services

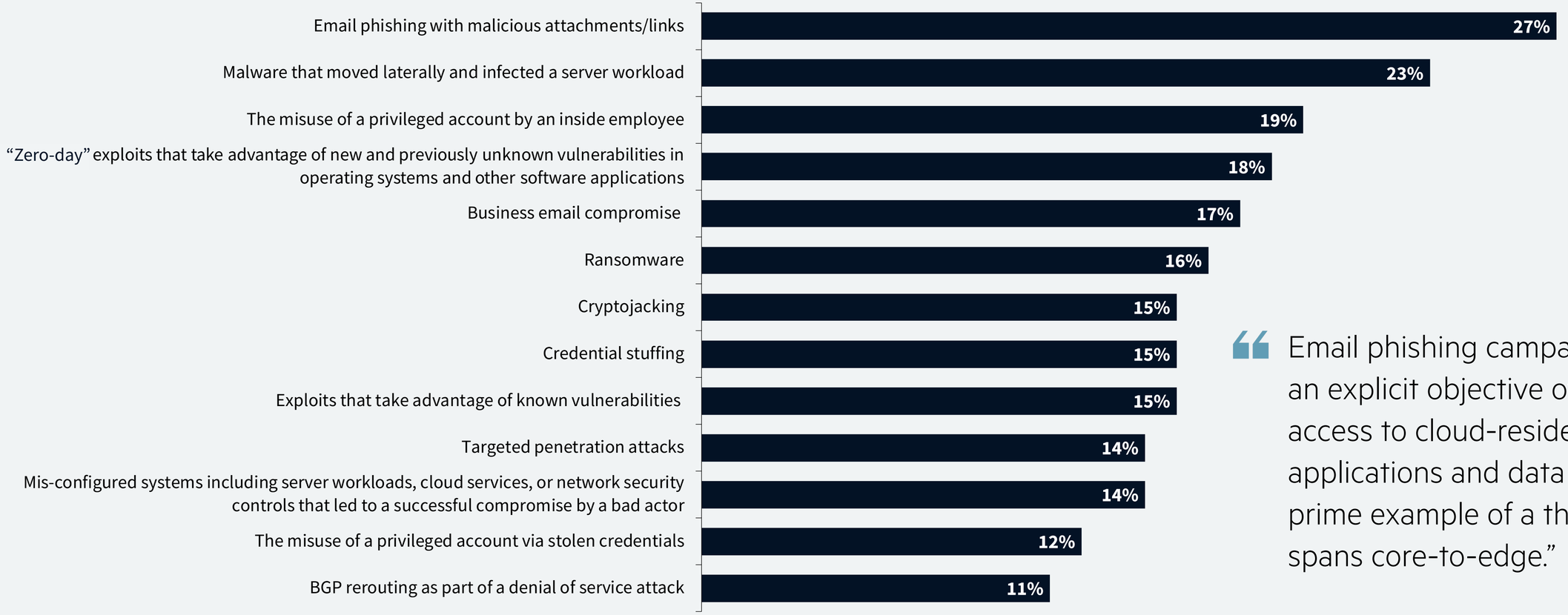
While participating organizations report experiencing a wide range of cyber-attacks over the last 24 months, email phishing took the top spot as the attack vector that was experienced most often during that period, a dubious distinction to be sure. The ongoing high incident rate of email phishing is a reminder that cyber adversaries will default to those methods that have proven effective and leverage them in new ways.

The broad use of cloud services has created an opportunity for hackers to exploit the ways in which cloud applications are used via socially engineered phishing attacks that put those very services and the data they store at risk. Indeed, email phishing campaigns with an explicit objective of gaining access to cloud-resident applications and data are a prime example of a threat that spans core-to-edge with the recipient of phishing emails the edge and the cloud assets being targeted the core.

RESEARCH HIGHLIGHT

Which of the following cybersecurity attacks, if any, has your organization experienced most often within the last 24 months?

(Percent of respondents, N=456, three responses accepted)



> "Email phishing campaigns with an explicit objective of gaining access to cloud-resident applications and data are a prime example of a threat that spans core-to-edge."

Some phishing email campaigns designed to steal login credentials exploit the social networking aspect for how we use cloud services. Sharing files via enterprise file sync and share services (EFSS) such as Box, Dropbox, and Google Drive is commonplace, with recipients receiving emails from others to access files and from the service providers themselves to learn more about advanced features and more. Hackers are now taking advantage of this established workflow by phishing users with seemingly legitimate emails from well-known file sharing service providers with a call to action to download a file, review an updated privacy agreement, or to update their account information, including their username and password. Clicking on the embedded link directs the user to a well-crafted web site to enter their credentials. After capturing their username and password, the user may be redirected to the legitimate login page, further masking the fact that they have just been compromised.

“Some phishing email campaigns designed to steal login credentials exploit the social networking aspect for how we use cloud services.”

This method of stealing login credentials has also been used to gain access to cloud infrastructure services. In this case, the targeted individual is a user with privileged credentials, such as a developer or release engineer. Armed with such credentials, hackers can access cloud infrastructure management consoles, provision new services such as compute instances, and begin to move laterally across the affected company’s cloud infrastructure.

Spoofed emails that fool the recipient to take action other than clicking on an erroneous link or downloading a malicious payload have proven effective as a means for cybercriminals to perpetrate payment fraud. In fact, business email compromise (BEC) attacks that fool the victim into making a payment based on the direction to do so from a fake executive or vendor email have resulted in appreciable financial loss. A report issued by the United States Securities and Exchange Commission states that the FBI estimates over $5B in losses since 2013 due to successful business email compromise campaigns.[4] These attacks are further examples of fraud at scale.

[4] Source: SEC Release No. 84429, Oct 16, 2018

All told, the spate of email phishing highlights that the incessant targeting of end-users makes them the ever-so-vulnerable edge. An increased focus on people, processes, and technology to mitigate the risk of phishing attacks, including business email compromises, is clearly required. As such, sharing a set of known best practices is warranted, **including:**

Conduct ongoing end-user awareness training to better enable knowledge workers to detect phishing emails, including those viewed on a smartphone, which makes identifying bogus email addresses more difficult. This training should include educating users on new forms of phishing including those discussed above, exploiting the use of cloud services and business email compromises.

Use email security solutions that inspect email content, inclusive of addresses, text, links, and attachments, with a variety of techniques to detect malware, links to malicious web sites, and business email compromises.

Conduct simulated email phishing attacks to test the effectiveness of end-user awareness training, identify weaknesses, and benchmark progress over time.

Update endpoint security software to the latest release to detect and prevent file and file-less malware attempting to gain a foothold via a phishing attack.

Consider advanced identity and access management controls including multi-factor authentication (MFA) and user behavior analytics to detect anomalous end-user activity.

> “All told, the spate of email phishing highlights that the incessant targeting of end-users makes them the ever-so-vulnerable edge.”

A secure messaging strategy is a microcosm of a holistic people, process, and technology approach to cybersecurity that has become more critical due to the way in which the use of cloud services has made phishing even more attractive to cyber adversaries.

Multiple Attack Types, Vectors, and Methods Are of Concern

Shifting from the rearview mirror to the windshield, research participants are, understandably, concerned with a multitude of cyber-threats moving forward. Starting with the vulnerable edge, email as an attack vector is a well-understood weak link, with phishing and business email compromises coming in as two of the threat types respondents are most often concerned about (91% and 90% were at least somewhat concerned, respectively).

Ransomware has settled into its place alongside other forms of attacks that organizations are clearly concerned about over the coming 12 months (89% reported being at least somewhat concerned). While ransomware incidents have plateaued, cybercriminals have diversified the methods employed to introduce new ransomware variants including via botnets. The Viro botnet detected by Trend Micro in September of 2018 is such an example, with this malware both serving as ransomware and having the ability to enlist infected machines into a botnet to further propagate itself.[5] Cybercriminals are also diversifying their business models by monetizing ransomware attacks not only by extortion but by selling stolen data, especially personal health information (PHI), on the dark web.

RESEARCH HIGHLIGHT

Percentage of respondents at least somewhat concerned about threat type

91%
Email phishing

90%
Business email compromises

89%
Ransomware

> “The focus on server configurations is well placed, as cloud-deployed workloads represent one of the perimeters of a hybrid cloud that must be secured by assuring only hardened systems are deployed into production.”

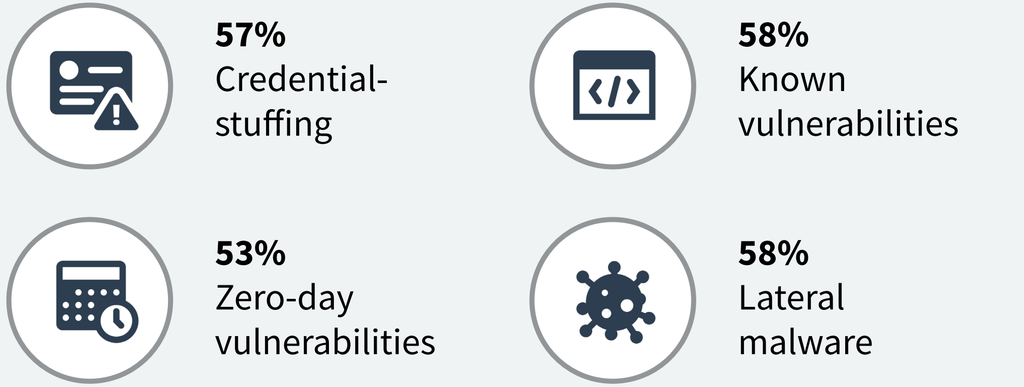
[5] Source: Trend Micro Security Intelligence Blog, *Viro Botnet Ransomware Breaks Through*, September 2018.

Credential-stuffing, attacks that automate the entering of stolen or leaked usernames and passwords to gain access to and take over systems is another area of high concern for 57% of our respondents. Because users often use the same password for multiple systems, lists of usernames easily purchased on the dark web are used in credential-stuffing attacks on multiple web applications. Such attacks may result in holding data for ransom and data loss. When it comes to protecting core applications and data assets, concerns around exploits predictably include known vulnerabilities as well as new and unknown zero-day vulnerabilities (58% and 53%, respectively, cited these issues as a top concern). Research respondents are also mindful of exploits that take advantage of misconfigured server workloads. The focus on server configurations is well-placed, as cloud-deployed workloads represent one of the perimeters of a hybrid cloud that must be secured by assuring only hardened systems are deployed into production. Proactive penetration testing and requesting the results of penetration tests conducted by CSPs can help mitigate the risk associated with configuration vulnerabilities. For example, exploitation techniques, including "fuzzing," which exposes hardware and software vulnerabilities by inducing crashes and leaks via the introduction of random or invalid data, are forms of dynamic analysis pen testers leverage to identify such vulnerabilities. This need to secure the core of server workloads is also reflected in the 58% of research participants who cited malware that moves laterally to infect them as a high concern moving forward.

New to the cyber-attack scene over the last few years is cryptojacking, the unauthorized use of compute cycles by malware to mine cryptocurrency. Just as botnets are now being used as a vector to introduce and self-propagate ransomware, so too are they being leveraged to distribute cryptojacking malware. In fact, Kaspersky Lab reports a decrease in the use of botnets for DDoS attacks and an increase in their use for cryptojacking.[6] A notable cryptojacking incident of 2018 occurred when multiple container images in Docker Hub were infected with cryptojacking malware and downloaded millions of times. While the reported profits were modest, the real cost of these attacks are the CPU cycles paid for by legitimate businesses and stolen by cybercriminals. While cryptojacking is considered by some as a victimless crime, making it an attack type of relatively less concern than others for the coming 12 months, the vectors and methods being used to disseminate cryptojacking malware indicate a need to fortify defenses.

RESEARCH HIGHLIGHT

Percentage of respondents highly concerned about threat type



[6] Source: Kaspersky Lab Bulletin 2018, *Story of the year: miners*, November 2018.

The expected internal implications of such attacks for an organization's cloud infrastructure are somewhat ironic: those on watch could lose their jobs while the new team gets incremental funding. In addition to holding individuals personally accountable and increasing costs, participants naturally expect additional scrutiny by auditors, the need to fund response and remediation activities, and an increase in their cybersecurity insurance premiums. The post-breach incident response measures will initially focus on determining the scope of the breach and extend into understanding root cause, which may be used for prosecutorial purposes as well as to improve security policies and processes.

Research participants whose organization experienced one or more cybersecurity attacks over the last 24 months reported a range of problematic outcomes. The resulting effects of cyber incidents include delayed IT projects, reduced knowledge worker productivity, capital expenditures to upgrade systems, and a general negative impact on business operations. These ramifications also include the need to further evaluate third-party risk, per the 26% who shared that a cybersecurity incident prompted them to re-evaluate the security posture of third parties.

Spotlight: Third-party Risk

When it comes to who has access to cloud-resident sensitive data, there are many users, including business partners, contractors, supply chain partners, auditors, part-time employees, customers, and others. These individuals will use different devices and operate under different policies and norms than an organization's full-time employees, putting cloud-resident data at risk.

“These individuals will use different devices and operate under different policies and norms than an organization's own employees, putting cloud-resident data at risk.”

At the center of how the use of cloud services has increased the risk associated with third-party access are enterprise file sync and share services (EFSS). EFSS services are often used by employees to share corporate data not only with each other but as a means to easily collaborate with external partners. Because EFSS tools are one of the most common types of shadow IT applications, their use, including with whom data is being shared, is often not governed, creating additional risk for the business.

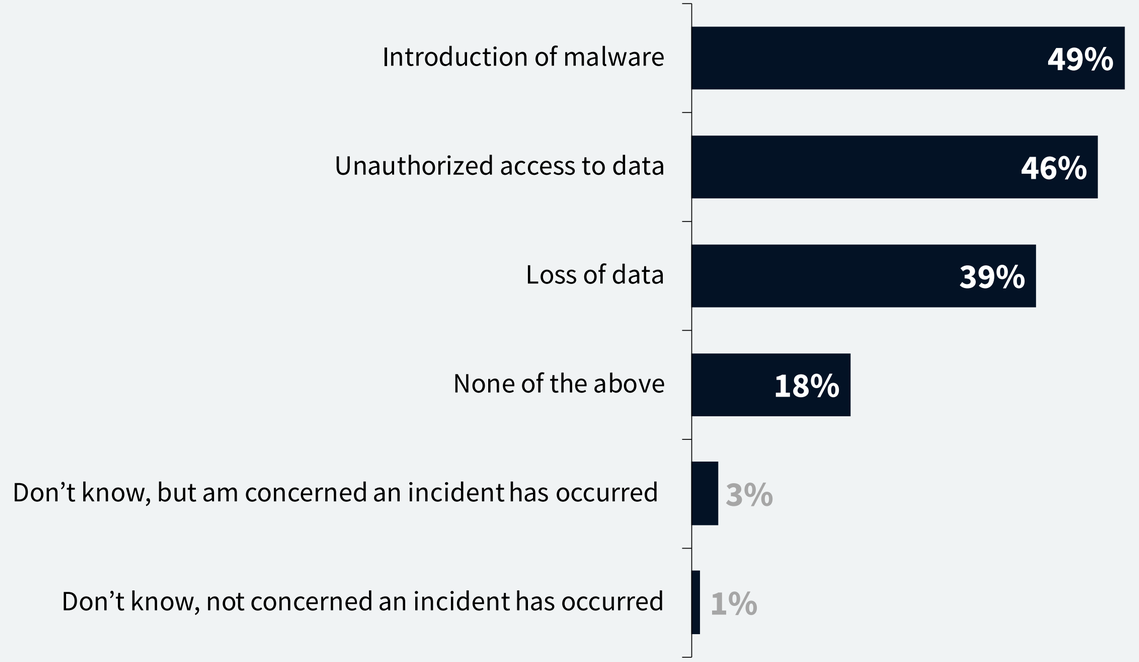
> “The loss of data due to third-party access is more acute for small and medium businesses.”

Nearly half (49%) of the organizations in this year’s study report a compromised third party was the cause for introducing malware, with another 46% reporting that a third party was the cause of unauthorized access to data and 39% sharing that they lost data as a result of a third party. The loss of data due to third-party access is more acute for small and medium businesses, with 44% of those organizations reporting this outcome, indicative of the fewer processes and controls employed by smaller organizations. These research findings highlight that more attention to third-party risk management is required.

RESEARCH HIGHLIGHT

Which of the following cybersecurity incidents, if any, has your organization experienced due to a third-party compromise?

(Percent of respondents, N=456, multiple responses accepted)



4

The Shadow IT Norm Creates a Policy Conundrum

Methodologies alone are ineffective as a strategy for securing cloud applications.

Cloud Application Approval Policies Are Widely Disregarded

Shadow IT's rather long history dates back to the PC and the subsequent ongoing consumerization of IT. As such, shadow IT has a broader scope than just the unauthorized use of cloud applications, including shadow infrastructure, the use of unapproved websites, and other IT-related activities that fall outside of established IT usage policies and guidelines.

The extensive use of shadow IT applications punctuates this dynamic, as line of business leaders simply no longer accept a process-bound multi-month schedule to stand up new business applications. In sharp contrast, today's self-service world of SaaS applications makes being your own IT team as easy as creating a personal Dropbox account. This is an example of how IT has become consumerized. In fact, that same personal Dropbox account may be the application of choice for sharing corporate data files with business partners.

The challenge of stemming the tide of shadow IT is evidenced by the lack of adherence to policies. Even though most organizations in our research study stated they have a formal policy to review and approve cloud applications, there has been a substantial year-over-year increase in the concern that such policies are being violated. Indeed, the 92% of research participants reporting concern that their company has individuals, departments, or lines of business in violation of their security policies for the use of cloud applications is a notable 10 percentage point increase from last year's research.

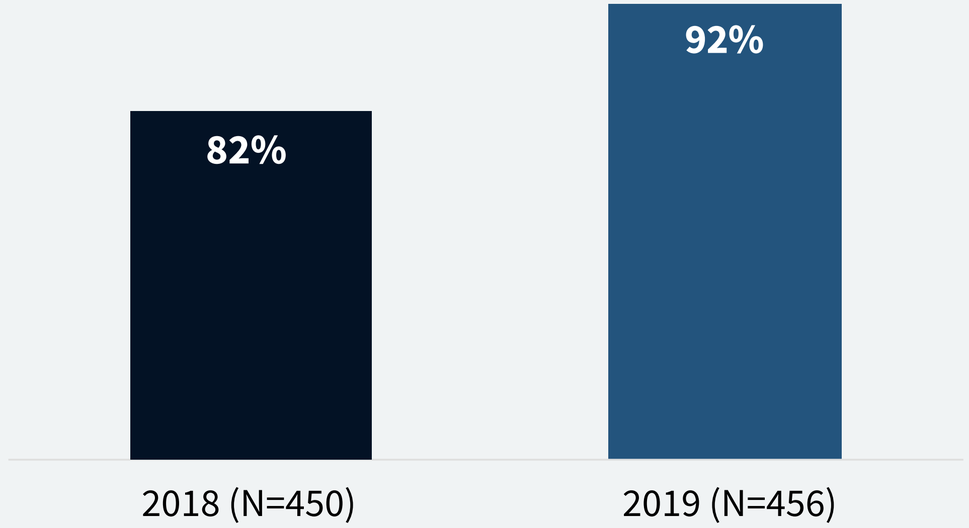
> "Even though most organizations in our research study stated they have a formal policy to review and approve cloud applications, there has been a substantial year-over-year increase in the concern that such policies are being violated."

But is the concern that individuals, departments, or lines of business are not following policies, resulting in actual shadow IT application usage? A whopping 69% of organizations stated that they are aware of a moderate or significant amount of shadow IT apps, with another 15% stating they are aware of a few such apps in use. Shadow IT seems to be especially problematic with North American organizations, 40% of which report a significant amount of shadow IT applications in use, compared with 26% in the complete sample set.

RESEARCH HIGHLIGHT

How concerned are you that individuals, departments, and/or lines of business within your organization are in violation of your security policies for the use of cloud applications?

(Percent of respondents)



Percentage of respondents very concerned/ concerned/somewhat concerned

The Use of Shadow IT Applications Has Had Consequences

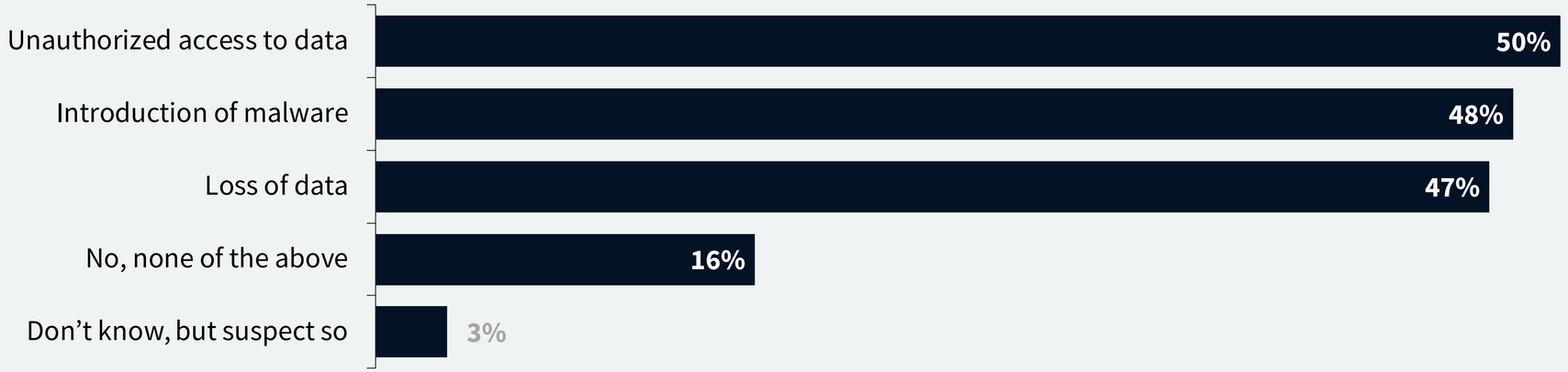
The findings in this year's research study are clear: Shadow IT has led to the very outcomes cybersecurity teams try to guard against. Exactly half of the participating organizations report the use of shadow IT apps has led to unauthorized access to data, which is easy to understand when tools like enterprise file sync and share (EFSS) services are widely used to share corporate data internally and externally. Nearly as many companies (47%) report actual loss of data due to the use of shadow IT apps. Such incidents include storing sensitive corporate data in an unauthorized personal cloud application that is lost should the employee leave the company.

"The findings in this year's research study are clear: Shadow IT has led to the very outcomes cybersecurity teams try to guard against."

RESEARCH HIGHLIGHT

Has the use of unsanctioned/shadow IT cloud applications resulted in any of the following cybersecurity incidents?

(Percent of respondents, N=456, multiple responses accepted)



CISOs 2x more likely versus CIOs to report an incident due to shadow IT apps (23% versus 10%)

> Shadow IT has also often resulted in the introduction of malware (48%), as cyber adversaries employ cloud apps as an attack vector."

Shadow IT has also often resulted in the introduction of malware (48%), as cyber adversaries employ cloud apps as an attack vector. Hackers have successfully expanded socially engineered attack campaigns by enlisting cloud applications for store and forward purposes. Such attacks compromise a cloud storage service, often by stealing credentials, place malware to be distributed in that cloud service, and then execute a phishing campaign to fool users into downloading said malware from the compromised cloud service. The social networking aspect of such an attack chain is exploiting the fact that so many of us are now accustomed to downloading legitimate files shared by colleagues and partners, as well as friends and family, from cloud-hosted file sharing services. Subsequently, those who have their devices configured to synchronize with trusted EFSS services are unceremoniously automatically infected.

Another notable finding regarding the implications of shadow IT is the difference in perceptions between CISOs and CIOs, with CISOs feeling shadow IT is more problematic than CIOs. CISOs report incidents caused by shadow IT apps at more than twice the frequency of CIOs (23% versus 10%). CIOs may, in fact, see a budgetary benefit from the use of shadow IT apps with the cost of subscriptions being submitted as a business expense versus hitting a funded IT line item. CISOs are unlikely to make such a distinction since they feel responsible for securing all applications and services in use, whether they are approved or unauthorized.

> CISOs report incidents caused by shadow IT apps at more than twice the frequency of CIOs (23% versus 10%)."

Spotlight: The Improper Use of Approved Cloud Applications

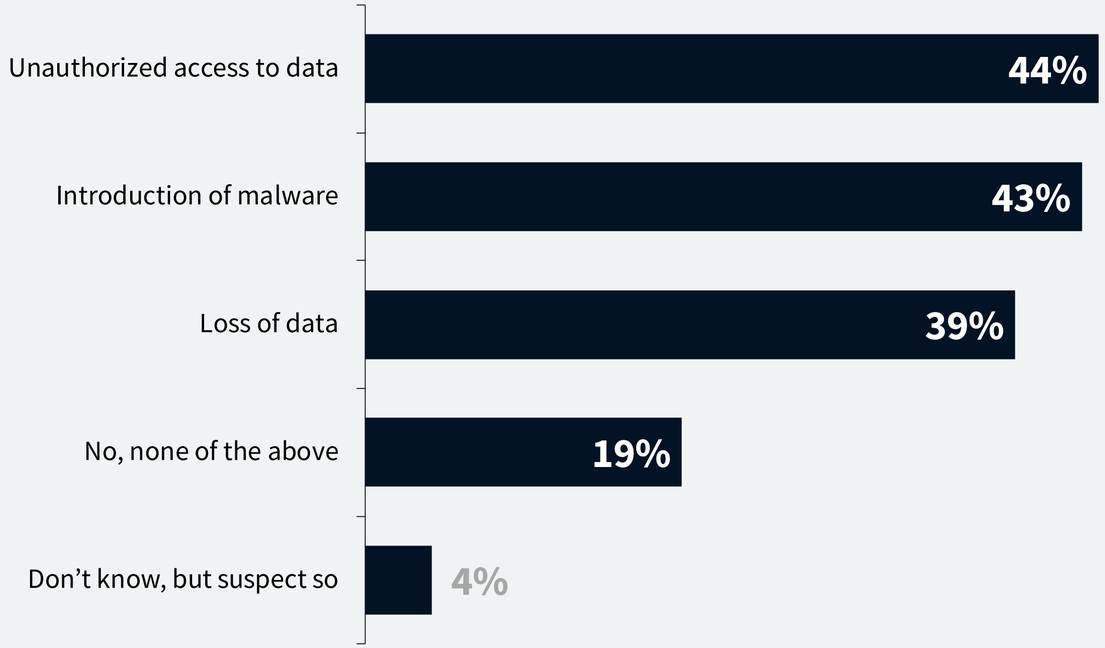
One may think it is only the rogue use of cloud applications that results in such cybersecurity incidents. This is a false assumption, as the improper use of sanctioned cloud applications—those approved and rolled out by the IT team—is also too often the cause for the very same set of issues. In fact, although on a slightly smaller scale, the very same outcomes of unauthorized access to data (44%), the introduction of malware (43%), and loss of data (39%) have been experienced by businesses due to the improper use of sanctioned cloud apps.

> “One may think it is only the rogue use of cloud applications that results in such cybersecurity incidents. This is a false assumption…”

RESEARCH HIGHLIGHT

Has the improper use of an authorized/sanctioned cloud application resulted in any of the following cybersecurity incidents?

(Percent of respondents, N=456, multiple responses accepted)



This leads to the question of what constitutes the improper use of approved cloud applications. The scenarios include not only how the end-user community is using sanctioned applications, but also how the IT and cybersecurity teams are securing their use. The absence or partial implementation of a cloud access security broker (CASB), a set of security controls designed specifically to protect the data stored with cloud apps and to prevent them from being hijacked as a means to introduce malware, could result in the incidents experienced by research respondents. Another common factor is the use of multiple instances of the same cloud application within an organization, including personal editions of file sharing services. Here, again, a CASB can help by distinguishing between personal and business editions of cloud applications and applying the appropriate usage policies to protect sensitive data.

“A CASB can help by distinguishing between personal and business editions of cloud applications and applying the appropriate usage policies to protect sensitive data.”

End-users may also be inappropriately storing and even sharing corporate data via approved cloud applications, representing another CASB requirement and use case, the discovery and classification of sensitive data as the basis for applying data loss prevention (DLP) policies. This type of improper use of cloud applications has obvious implications for complying with the General Data Protection Regulation (GDPR), for which the discovery and classification of personal data for citizens of European Union counties is required to then be able to apply access policies and maintain audit trails.

“The security and compliance implications of improper usage extends beyond cloud applications to cloud infrastructure services.”

The security and compliance implications of improper usage extends beyond cloud applications to cloud infrastructure services. Developers running approved server workloads and application containers for development and test purposes may, for example, inadvertently deploy them externally facing instead of connected to a jump host. These systems will then be immediately subjected to port scanning. Moreover, at the center of some of the most prominent data breaches over the last few years have been misconfigured Amazon S3 storage buckets. “Public” access control settings that some felt made the S3 buckets available to others with access to the same AWS account actually made the data available to anyone who could simply hack the URL of the bucket(s).

5

Users Are Turning to Automation to Remedy Chronic Patching Problems

Deferred patching puts business applications at risk and highlights the need for intelligent automation.

SLAs and Compatibility Overshadow the Proven Effectiveness of Patching

When it comes to closing the holes attackers exploit, the value of penetration testing to find them and expedited patching to close them is well understood. In fact, penetration testing and patching more frequently are the two actions cited most often as having had the most positive impact on an organization's cybersecurity posture. However, even with an appreciation for the efficacy of patching, legitimate operational considerations may delay patching a production system.

> "However, even with an appreciation for the efficacy of patching, legitimate operational considerations may delay patching a production system."

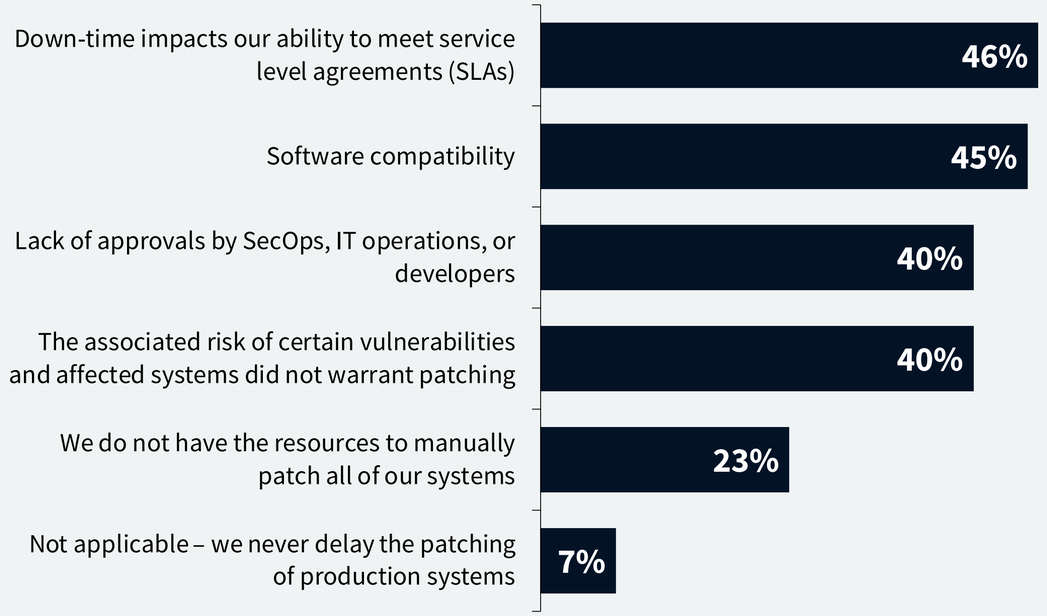
Some patches require a reboot, which would impact availability and the agreed upon service level agreement (SLA) IT has with the business for certain applications, the most-cited reason for delaying patching, as cited by 46% of the participating businesses. As a result, some clearly conflate the operational importance of critical applications with the need to secure those systems from compromise via more proactive patching, especially when multiple patches are in the queue. Compatibility with software was nearly as common a reason to delay patching, a bi-directional obstacle when either the current version of a software package does not yet support the version of the operating system to be patched or vice versa. There are also process obstacles with respect to approval cycles for change control and the fact that the risk associated with some vulnerabilities is such that IT does not view the patching as warranted.

The patching and server configuration management challenges experienced by our research respondents shed additional light on why some take a measured approach to patching. The top issue has been one of opportunity cost, with 51% of the participants noting patching delayed other IT projects. The fear of downtime impacting the ability to meet SLAs was real for the 39% of organizations who reported that patching required system downtime, with a similar set of respondents noting that a patch forced an application upgrade.

RESEARCH HIGHLIGHT

For which of the following reasons/concerns has or would your organization delay applying a patch to a production system?

(Percent of respondents, N=456, multiple responses accepted)



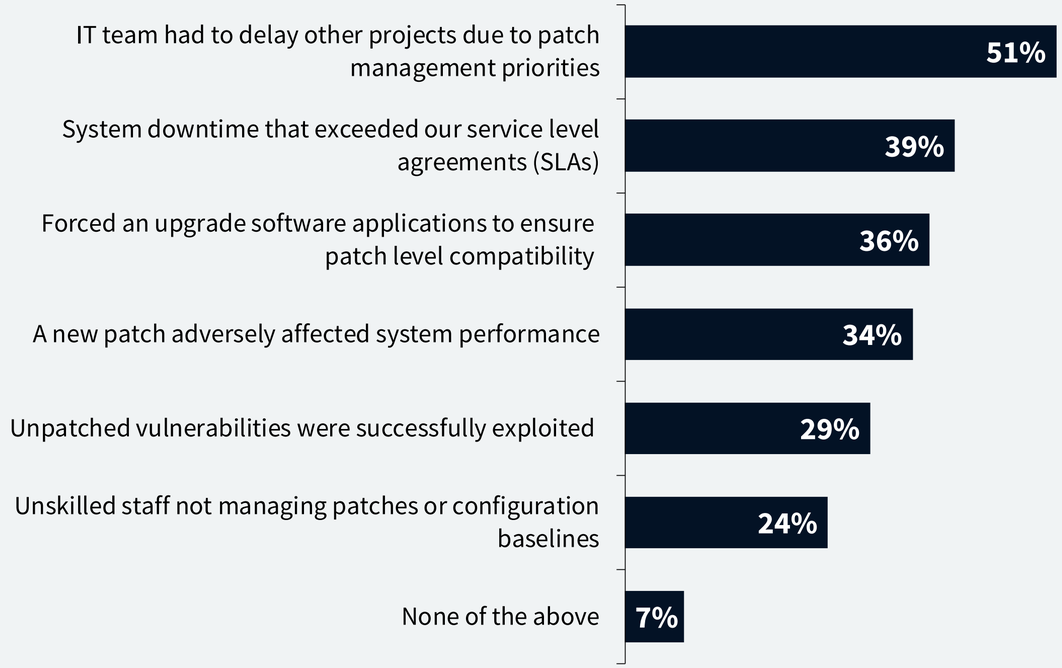
> “This reality creates a race condition between bad actors disseminating an exploit and businesses patching their systems.”

In another related ESG research study, 52% of organizations shared they prioritize patching based on known exploits associated with the vulnerabilities.[7] The absence of an exploit in the wild in the hours and days after a patch is made available may backburner that patch and leave the business exposed when exploits do arrive on the scene. IT and cybersecurity professionals should be mindful that once a patch is released, hackers are also evaluating the patch, but through a very different lens, by decompiling and otherwise reverse engineering the patch to create an exploit. This reality creates a race condition between bad actors disseminating an exploit and businesses patching their systems. Some may feel they have mitigated the risks associated with a vulnerability by employing controls that detect and prevent exploit behavior, serving as a virtual patch. Those who have opted to defer patching requirements may find their systems appear in the results of a Shodan search. Public shaming concerns aside, we clearly have a need to further operationalize policy-based patch and configuration management. Enter automation.

RESEARCH HIGHLIGHT

Have you experienced any of the following patching and server configuration challenges in the last 24 months?

(Percent of respondents, N=456, multiple responses accepted)



[7] Source: ESG’s 2018 Risk Management Study

Organizations Have Strong Interest in Automated Patching to Eliminate Operational Obstacle

The next most impactful cybersecurity improvement step, after penetration testing and more frequent patching, is automated patching. The use of automated patching is already in play for 43% of our researched organizations, with 50% of larger organizations (i.e., enterprises with 2,500 or more employees) already doing so. Additionally, a notable 46% more plan to implement automated patching over the next 12-24 months.

> “IT and security teams are clearly leveraging automation both to address chronic operational issues and to improve their company’s cybersecurity posture.”

RESEARCH HIGHLIGHT

Have or does your organization plan to deploy a solution that automates patch management for production environments?

(Percent of respondents, N=456)

RESEARCH HIGHLIGHT

You indicated you have or plan to deploy an automated patch management solution. Which of the following was the primary reason for doing so?

(Percent of respondents, N=404)

The drivers? We know that the efficacy of cybersecurity controls and the operational efficiency of managing them have too often been mutually exclusive outcomes. IT and security teams are clearly leveraging automation both to address chronic operational issues and to improve their company's cybersecurity posture. Nearly half of those who have automated or plan to automate patching cite operational efficiency as their primary reason for doing so, with another 29% citing reducing the window in which a vulnerability can be exploited as their primary reason.

In a cloud-specific context, automation is even more applicable. While the providers of SaaS applications and platform-as-a-service (PaaS) platforms are responsible for patching, consumers of infrastructure-as-a-service (IaaS) services are responsible for patching cloud-hosted server workloads. Automating the application of patching via the continuous integration and continuous delivery (CI/CD) tools of DevOps is one of many "DevSecOps" uses cases. CI/CD integration can automate both testing for known vulnerabilities as a gate check before deployment to production and the build and deployment of patched configurations.

Spotlight: Applying Autonomous Driving to Patch Management

Letting go and allowing automation to take over is one of the most notable recent innovations in the automotive industry, with more manufacturers now building cars with autonomous driving capabilities. As is the case with automating the management of information technology, there are levels of autonomous driving,[8] with each representing an increased confidence in allowing the car to do the driving or, in our IT context, confidence in allowing the system to do the patching.

As is the case with automating the management of information technology, there are levels of autonomous driving, with each representing an increased confidence in allowing the car to do the driving or, in our IT context, confidence in allowing the system to do the patching.

Going from no automation to a modest level of assistance allows cars to apply braking when getting too close to another vehicle, just as when vulnerability scans will not only alert on the presence of a vulnerability but also its relative severity. At this level, customers still need to do manual work such as investigating whether there are yet any exploits. Partial autonomous driving requires the driver to still be actively engaged, just as automated patching may require an administrator to manually approve the deployment of a patch. Conditional autonomous driving is often based on speed, just as the automated application of a patch can be driven off the severity of the associated vulnerability.

> “Complete automation truly hands over the keys by allowing an autonomous patch management system to factor in severity, the release of an exploit, compatibility, and SLAs as inputs to automating patching.”

Higher levels of autonomous driving occur when conditions are safe. Such is the case when automatically applying a patch that is known not to impact availability, performance, or application compatibility. Finally, complete automation truly hands over the keys by allowing an autonomous patch management system to factor in severity, the release of an exploit, compatibility, and SLAs as inputs to automating patching.

[8] Source: Tech Republic, *Updated: Autonomous driving levels 0 to 5; Understanding the differences*, January 2016.

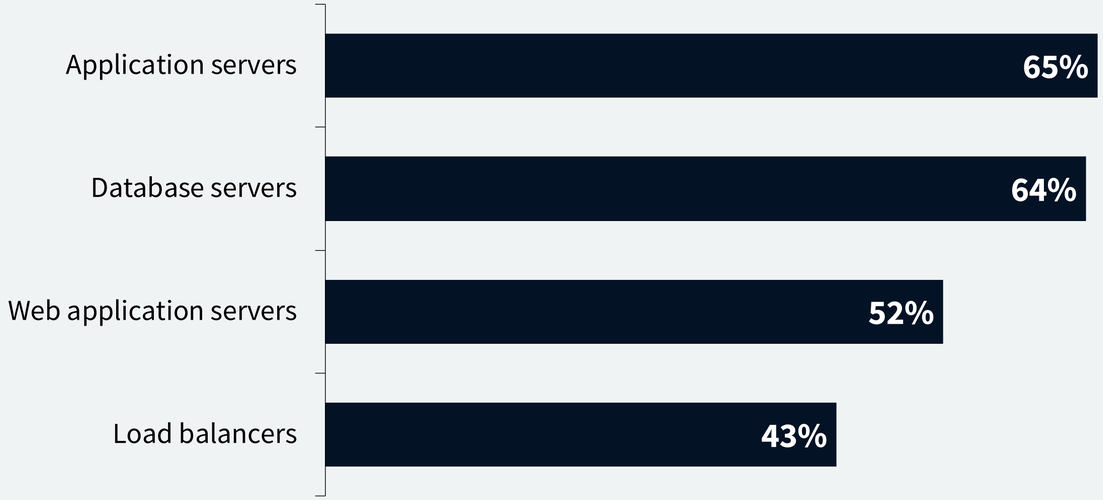
So, in this context, how are our research participants automating patching? Well, for starters, IT and cybersecurity teams that automate patching are prioritizing doing so for their most critical production servers. Nearly two-thirds of participants (65%) are automating the patching of application servers, including a little over half (52%) who are automating their web tier.

Our research also shows a clear strategic intent to leverage automation so databases can autonomously patch themselves, without material impact to availability, while assuring compatibility with higher-level business applications. Among organizations automating database patching, 58% have already fully or mostly automated patching their database servers, with another 42% having somewhat automated database patching. The difference in the degree to which organizations have already automated database patching is well aligned with the levels of automation discussed above with some manual intervention or conditions required. As the underpinnings of most business applications and the keepers of sensitive data, databases truly are business-critical assets that require advanced, proactive security measures, starting with automation to protect them against compromise.

RESEARCH HIGHLIGHT

For which of the following production server types has your organization deployed an automated/autonomous patch management solution?

(Percent of respondents, N=181, multiple responses accepted)



6

IT is Seeking Alternatives to Passwords

Streamlining authentication is gaining favor as a means to address identity and access management challenges.

Cloud and Mobility Are Complicating Identity and Access Management Strategies

The multitude of ways that increasingly mobile knowledge workers access core applications and data has complicated the management and policy facets of identity governance and administration (IGA). The importance of a strong identity and access management program cannot be overstated and must be viewed as the binding fabric in an organization's layered defenses. To effectively authenticate end-user access and manage entitlements, an identity and access management strategy must consider the use of company-owned and personal devices, an increasingly remote and mobile workforce, the use of approved and shadow IT cloud applications, and varying access patterns. This reality is highlighted in this year's report, which reveals that the most significant identity and access management challenges reported by respondents are the use of mobile devices and cloud applications, which our respondents note make identity and access management controls and monitoring more difficult.

> "The importance of a strong identity and access management program cannot be overstated and must be viewed as the binding fabric in an organization's layered defenses."

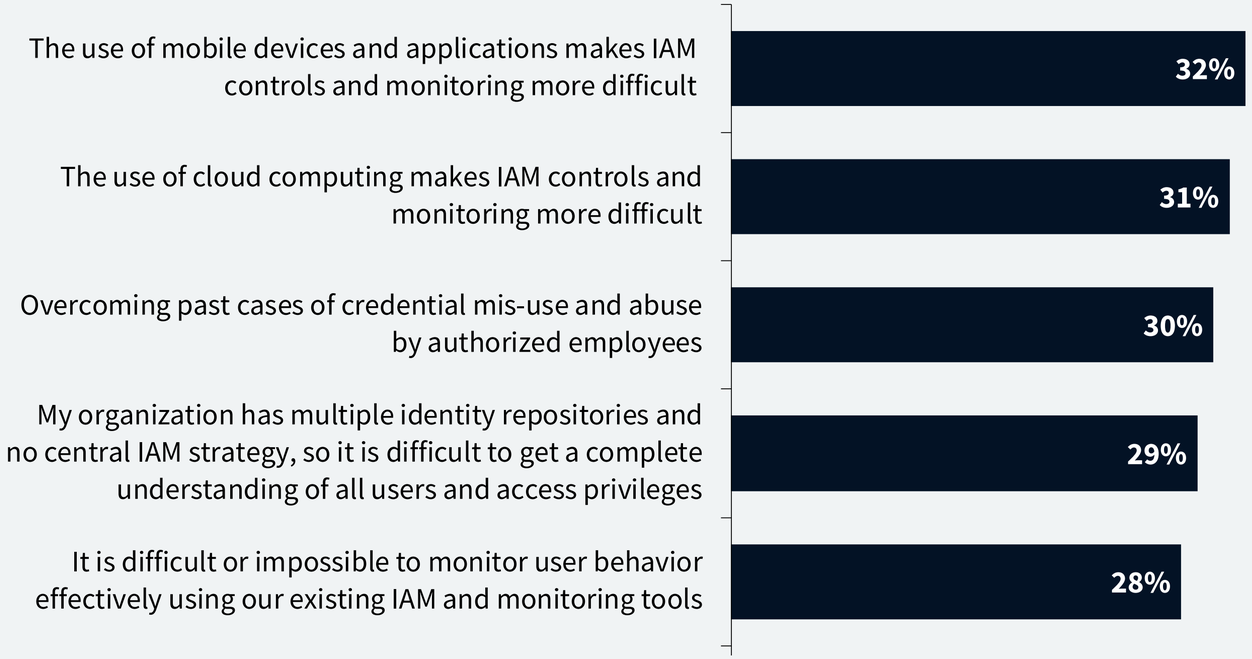
An operational example of how cloud usage and mobility, combined, create challenges is the use of VPN authentication by remote employees to attain credentials to access cloud services, the “hairpin” flow of which introduces latency. Such an approach is an artifact of traditional identity and access management architectures with identity-as-a-service (IDaaS) providing a cloud-delivered implementation that eliminates the need for a reverse proxy implementation. Most IDaaS offerings provide a set of management services to federate authenticated access to a broad set of cloud services, including a universal directory, single sign-on (SSO), and adaptive authentication.

Respondents also shared that credential misuse and managing multiple identity repositories are notable challenges. End-user resistance to the use of multi-factor authentication (MFA) was also found to be a significant identity and access management challenge. Given the need for stronger authentication schemes that don’t introduce any additional friction into the user experience, how are organizations rethinking the role of passwords?

RESEARCH HIGHLIGHT

Which of the following are your organization’s most significant identity and access management (IAM) challenges?

(Percent of respondents, N=456, five responses accepted, five most frequently reported challenges shown)



> “Change is afoot, with 57% of businesses actively evaluating replacing passwords or planning to in the next 12-24 months.”

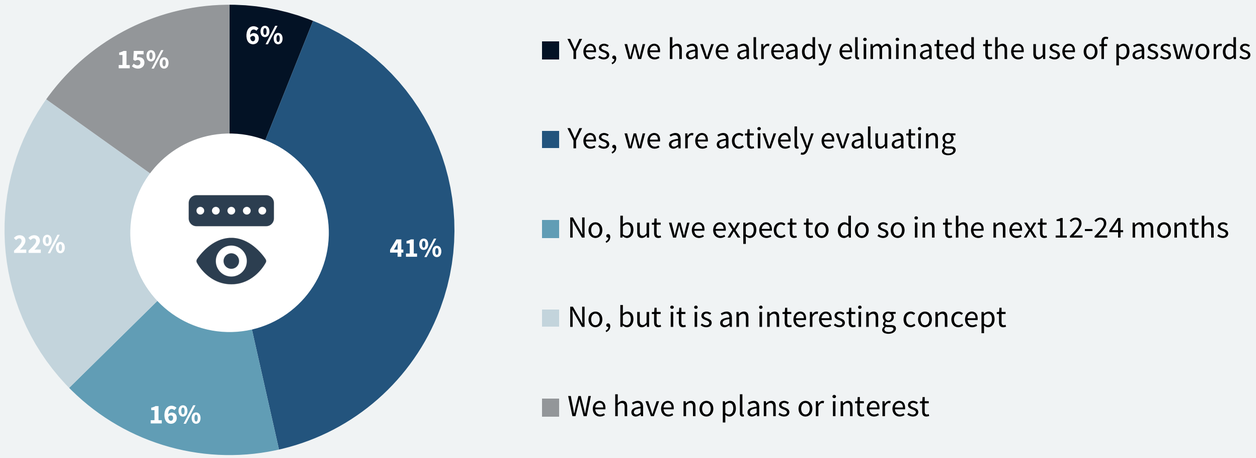
Other Forms of Authentication Are Emerging

Password management is another long-standing issue that impacts not only IT operations teams with constant requests to reset forgotten passwords, but also end-users. Beyond such inconveniences, bad actors have become adept at stealing credentials through a variety of tactics and methods. This includes installing key stroke logging malware and fooling users into entering their usernames and passwords as the result of a successful phishing attack. Given these recurring issues, we asked the organizations who participated in our study whether passwords were past due as the only form of authentication and what other forms of authentication would be used. While only 6% of participants have already replaced passwords, change is afoot, with 57% of businesses actively evaluating replacing passwords or planning to in the next 12-24 months. Nearly another quarter of respondents find replacing passwords an interesting concept while only 15% are dismissive of the idea, noting their organization has no plans to replace passwords.

RESEARCH HIGHLIGHT

Is your organization evaluating the replacement of passwords with another form of authentication (e.g., SMS text message, YubiKey smart card, facial recognition, finger print, token, etc.)?

(Percent of respondents, N=441)



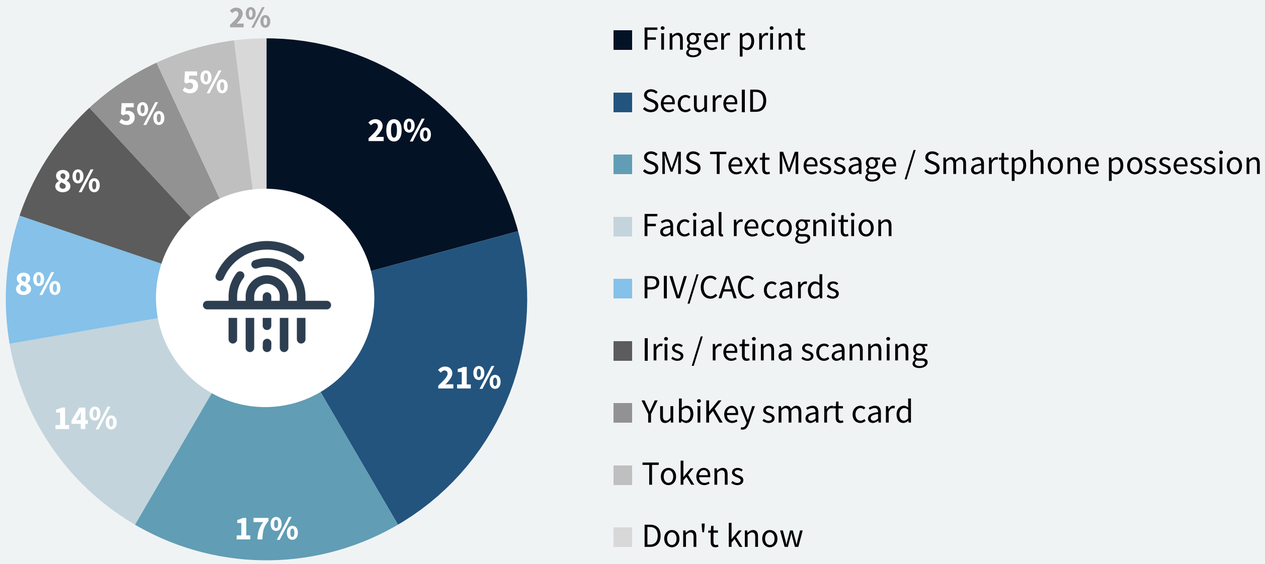
Additional forms of authentication need to be easy for IT to implement and easy for users to enter. Enter biometrics. Of the various forms of primary authentication under consideration by those looking to move away from passwords, different forms of biometrics (e.g., fingerprints, iris/retina scanning, and facial recognition) were cited by nearly half of the respondents (47%) as the forms of authentication their organizations will use. Physical tokens, including SecureID, will serve this purpose for another 26% of organizations, and SMS text messaging and/or smartphone possession are likely for another 17%.

While replacing passwords with biometrics is an understandable reaction to the seemingly never-ending cycle of password resets and credential theft, a strong dose of caution is warranted. There are fundamental pitfalls with biometrics as the primary form of authentication—biometric identifiers can all too easily be captured or stolen, and once they are in the wrong hands, they cannot be changed. Fingerprints, for example, are easy to replicate from high resolution pictures, are sometimes transmitted in the clear, and have been stolen in bulk credential theft data breaches as was the case in the 2014 hack of the United States Office of Personnel Management. Unlike passwords, compromised fingerprints cannot be changed. As such, in the context of a defense-in-depth approach to managing identities, the use of biometrics should be evaluated as an additional factor of authentication used in conjunction with passwords.

RESEARCH HIGHLIGHT

You indicated that you have, plan to, or are evaluating replacing passwords. Which of the following forms of authentication will be used as the first factor of authentication?

(Percent of respondents, N=277)



As is the case with the adoption of most new technologies, there will be a transition that will slow mass adoption of biometrics as the primary form of authentication. One obstacle will be the lack of hardware to support biometric authentication, especially in cases where IT opts for less expensive endpoint devices that do not come with hardware support for biometrics-based authentication. Ironically, biometrics is already more broadly used by consumers with smartphones and tablets that have fingerprint and facial recognition built into both the operating system and hardware. YubiKeys, however, can fill the void by providing a means of fingerprint authentication for devices equipped with a USB port but no other means of biometric authentication.

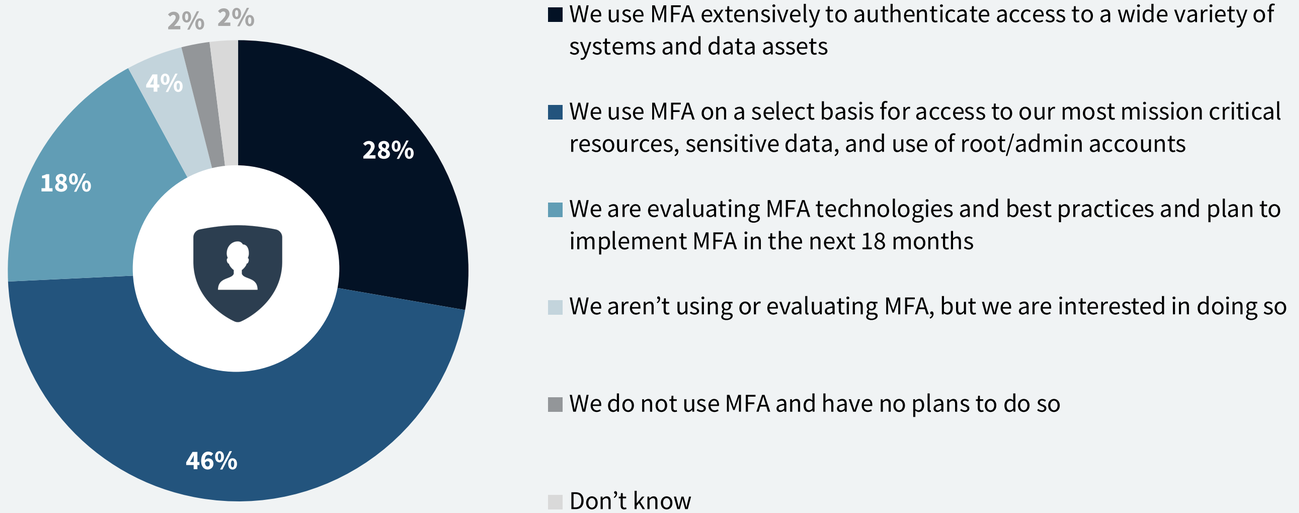
Spotlight: Expanding the Use of MFA with an Adaptive Approach

Beyond reevaluating the role of the password as the first factor of authentication, there is pending change in the approach to how second factors will be employed, with the goal of expanding the use of MFA to additional applications. Currently, only 28% of companies in this year's study use multi-factor authentication extensively to secure access to a wide variety of systems and data assets, while nearly half of our participating companies (46%) are doing so selectively. More specifically, systems that store secrets and sensitive data are the most likely use cases for which MFA is being used.
The top system for which an additional factor of authentication is required makes perfect sense: the identity and access management servers themselves that truly hold the keys to the kingdom. Customer relationship management (CRM) and enterprise resource planning (ERP) systems are next in line for MFA usage, with 39% and 37% of organizations, respectively, employing this extra layer of security for those business-critical applications.

RESEARCH HIGHLIGHT

How does your organization employ multi-factor authentication (MFA)?

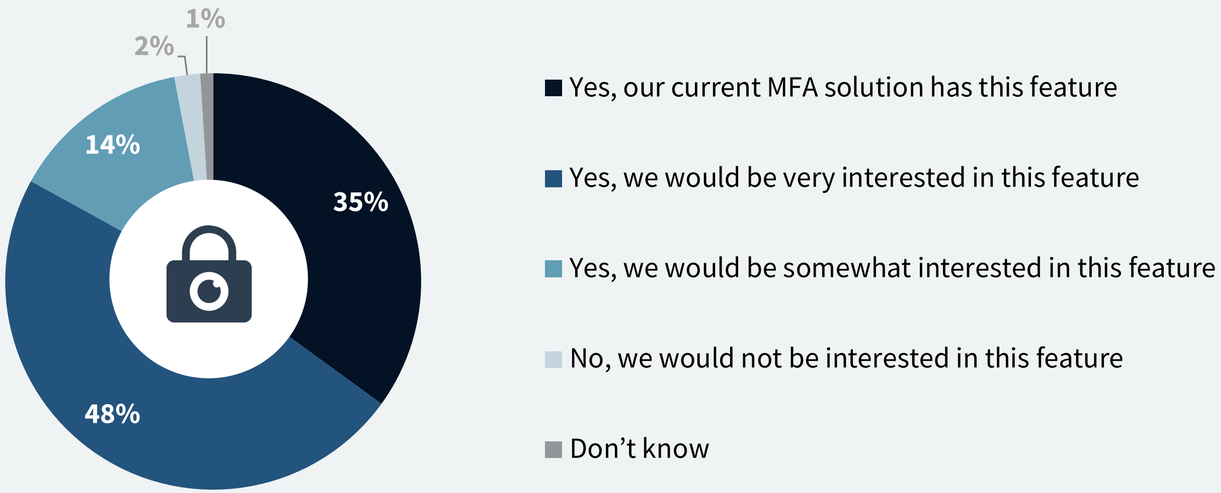
(Percent of respondents, N=456)



RESEARCH HIGHLIGHT

A feature of some MFA solutions is the ability to automatically trigger a second factor of authentication upon detecting anomalous user behavior.
Do you believe your organization would be interested in this type of feature?

(Percent of respondents, N=441)



> “Business agility and mitigating the risk of unauthorized access and data loss are at odds.”

Multi-factor authentication and automated patching are both recognized best practices that need to be extended to all business-critical systems. But requiring MFA for access to more applications and data stores introduces additional friction to the user experience in a world where businesses leverage cloud services to move quickly. In this context, business agility and mitigating the risk of unauthorized access and data loss are at odds, but other areas of life provide examples of security realities necessitating compromise. Air travel is such an example, where multiple security measures are employed, from expediting security checks for known travelers to requiring additional scrutiny for those exhibiting suspicious behavior. Fortunately, such a contextual and adaptive approach to multi-factor authentication is now being used more extensively in IT shops using or interested in MFA, with 35% of these respondents sharing they are already using adaptive authentication to trigger a second factor of authentication when anomalous end-user activity is detected and nearly half of the participants (48%) noting that they would be very interested in this feature.

7

The People, Processes, and Technologies of a Cloud Security Program

Bringing cloud into the scope of a security program requires a retooling of the fundamentals.

Core-to-edge Security Requires a Defense-in-depth Strategy

The discussion of the research in this report has thus far explored how mobility has expanded the edge and how cloud services have expanded the core. A core-to-edge orientation provides the basis for a defense-in-depth approach to cybersecurity that encompasses the basics of people, process, and technology. The actions our research participants took that had the most positive impact on improving their organization's cybersecurity posture fall into each of these three areas.

The top three actions that respondents reported as having moved the cybersecurity needle the most are all about the processes associated with reducing the attack surface by more proactively finding and closing vulnerabilities. This is why the most impactful actions of conducting more frequent penetration testing, patching systems more frequently, and employing automation to do so represent an excellent set of best practices all organizations should adopt.

> "A core-to-edge orientation provides the basis for a defense-in-depth approach to cybersecurity that encompasses the basics of people, process, and technology."

RESEARCH HIGHLIGHT

You indicated your organization experienced one or more cybersecurity attacks in the last 24 months. Which of the following actions did your organization take that had the most positive impact on improving your organization's cybersecurity posture?

(Percent of respondents, N=409, three responses accepted)

The next set of actions are about people, both the company's cybersecurity team charged with detecting and preventing threats as well as the end-user community targeted by socially engineered attacks. To stay current on adversary tools, tactics, and procedures, 25% of respondents cited training their staff on new threats and best practices as having the greatest impact, similarly 25% report engaging with a managed security service provider (MSSP) for staff and skill augmentation as having the most impact.

> "A unified approach should lead to more consistent security policies and provide some operational efficiencies in the process."

There are also plans to change the default approach of separate teams and controls for disparate environments by moving to a unified approach. In a related ESG research study, a notable 61% of research respondents shared they currently have different teams responsible for securing the on-premises and public cloud portions of the hybrid cloud, but plan to merge these responsibilities in the future.[9] A unified approach should lead to more consistent security policies and provide some operational efficiencies in the process.

Edge-based Controls Are Essential Security Technologies

The demise of the physical perimeter and the importance of securing the new perimeter has arguably been overstated. After all, most organizations, with the exception of those that were born in the cloud, operate in a hybrid cloud reality with both on-premises and public cloud footprints with physical and virtual perimeters to be secured. The ongoing relevance and strategic importance of edge-based security controls is a case in point.

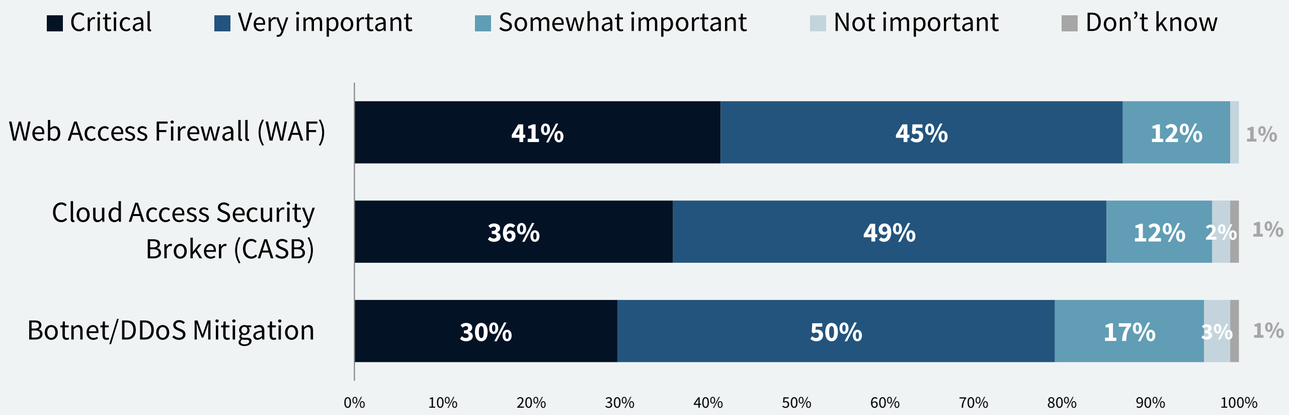
Respondents rated the relative importance of edge-based controls with web application firewalls (WAF), cloud access security brokers (CASBs), and botnet/DDoS mitigation controls all rated as very important, if not critical. The prevalence of web applications and their susceptibility to SQL injections and cross-site scripting attacks make WAFs the most important edge control, with 86% of respondents citing them as very important or critical.

[9] Source: Source: ESG Master Survey Results, *Trends in Cloud Data Security.*

RESEARCH HIGHLIGHT

How important are the following edge security technologies in helping to identify risk and threats impacting your cloud footprint?

(Percent of respondents, N=456)



CASBs in particular have taken center stage as a set of critical controls for securing an organization's use of cloud services. CASB implementations allow IT and cybersecurity teams to gain greater visibility into their organization's use of cloud services by discovering shadow IT applications and reporting on their associated risk, classifying sensitive data as the basis for applying data loss prevention (DLP) policies, and detecting both in-flight threats and malware stored with cloud services.

> "CASBs in particular have taken center stage as a set of critical controls for securing an organization's use of cloud services."

Concerns over distributed denial of service (DDoS) attacks is reflected in the respondents' rating of these mitigating controls as critical. The importance of botnet and DDoS mitigation control is well founded, given the number of such attacks over the course of the last year, including, as discussed in a blog from Kaspersky Labs, one against the GitHub code-hosting service that peaked at 1.3 terabits per second, one of the largest on record. Nation-state-perpetrated DDoS attacks included those on public transportation, with the attack on the Danish railway company DSB a possible continuation of a similar attack in 2017 on neighboring Sweden's rail system.[10] In April of 2018, the website of the largest political party in Russia, United Russia, was taken off-line for two days after British and US law enforcement officials warned that Russian hackers had seized a significant number of devices for a botnet.[11] In other cases, such as that which was thought to be an attack on an opposition party's website during the 2018 presidential election cycle in Mexico, outages were actually caused by a wave of legitimate traffic.

[10] Source: Kaspersky Lab Report, *DDoS Attacks in Q2 2018*
[11] Ibid.

Spotlight: The Role and Responsibility of the Cloud Security Architect

While many of the approaches for securing cloud environments are similar to those employed for protecting on-premises infrastructure, their implementation varies in notable ways. For example, a cloud security program needs to contemplate the API-centric nature of IaaS and PaaS provisioning, and the facts that cloud-delivered server workloads in auto-scaling groups are temporary. The lack of access to a physical network tap requires different ways to inspect network traffic, and the CI/CD methodology of a DevOps approach is akin to stepping onto a conveyor belt. Cloud security architect (CSA) is a role that has emerged over the last few years to bring cloud skills to cybersecurity and DevOps teams. Last year's report shared the emergence of this new role, so this year we explore the responsibilities of cloud security architects.

To start, 41% of participating organizations in the study have a CSA. Related ESG research shows that this individual most often reports to a C-level leader, with a third of the respondents saying their CSA reports to their CIO. Reporting to the CIO, CISO, or CTO versus the company's security architect or network security team indicates CSAs have a strategic charter, a mission well-aligned with the imperative to secure the business cloud. This reporting structure provides the C-suite with a direct chain of command and visibility into the cloud security architect's initiatives. Reporting structure alone does not, however, mean CSAs have the authority to implement their initiatives unhindered by other agendas. As such, CSAs must embrace the collaboration and transparency norms of a DevOps culture to gain favor for cloud security priorities.

RESEARCH HIGHLIGHT

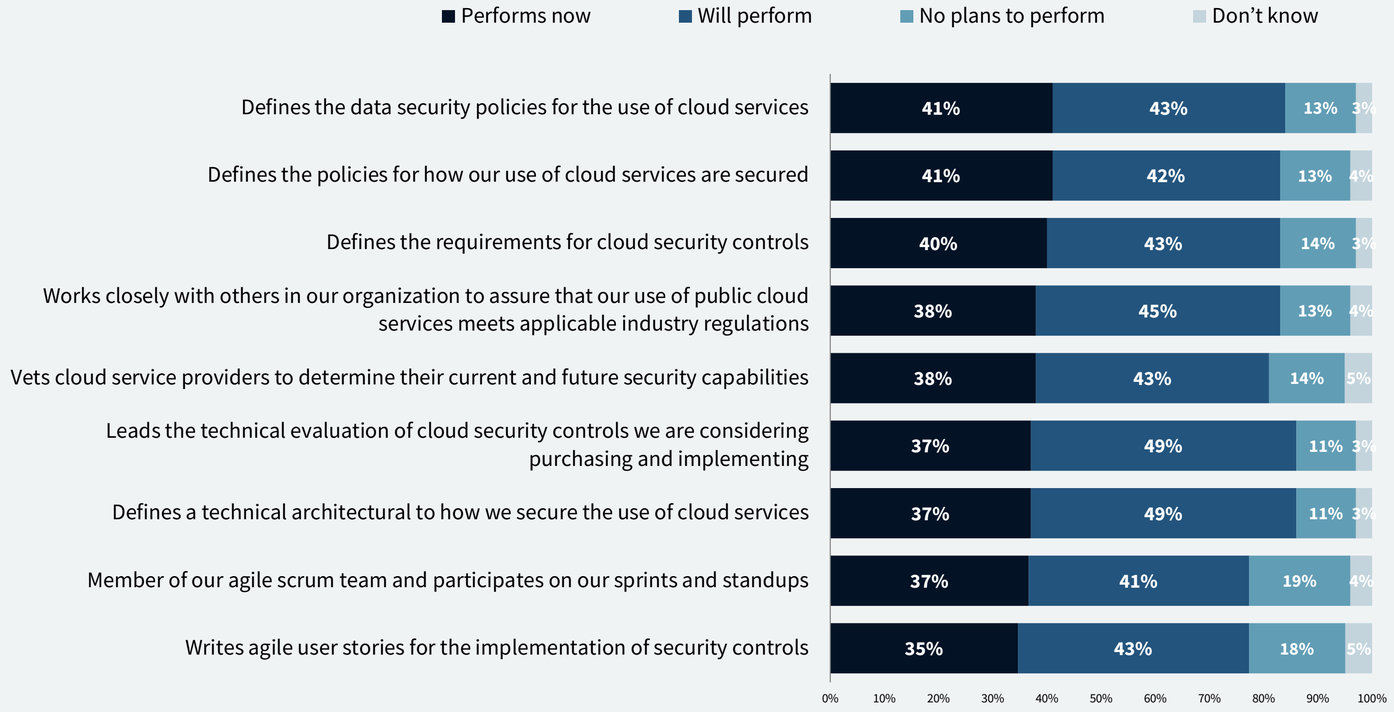
To which individual or group does – or will – your organization's cloud security architect(s) directly report?

(Percent of respondents, N=364)

RESEARCH HIGHLIGHT

What are – or likely will be – the primary areas of responsibility assigned to your organization's cloud security architect(s)?

(Percent of respondents, N=364)



But what, exactly, does a CSA do? It starts with defining policies around how cloud services are used and, perhaps most importantly, defining a technical architecture for how their organization secures their use of cloud services, assuring they meet their obligations of the cloud shared responsibility security model. When it comes to compliance and governance considerations an intimate knowledge of the cloud shared responsibility security model makes cloud security architects a go-to resource for data privacy and data protection leads to consult on data privacy regulatory considerations. CSAs are also responsible for defining the requirements for cloud security controls and leading the technical evaluation of these products and services.

One of the aspects of cloud security often overlooked is how agile software development practices are the cadence with which security practitioners need to align with application development cycles by becoming a member of scrum teams and attending daily standups. Additional ESG research highlights the importance of agile, with 78% of participants noting their cloud security architect is also currently or will be responsible for writing agile user stories for the implementation of security controls. Embracing agile is, in fact, how cloud security architects get their initiatives implemented. The user stories authored, and often implemented, by CSAs need to span the continuous integration and continuous development (CI/CD) stages of DevOps from development to production. For example, code committed to source code repositories should be required to pass a static analysis test, automated builds should check for software and configuration vulnerabilities so that only hardened images are deployed to production, and orchestration platforms should be instrumented to deploy runtime controls.

8

The Future in Focus: Scaling Security Operations with Machine Learning-powered Analytics

Businesses are leveraging machine learning to accurately speed detection in a sea of security events.

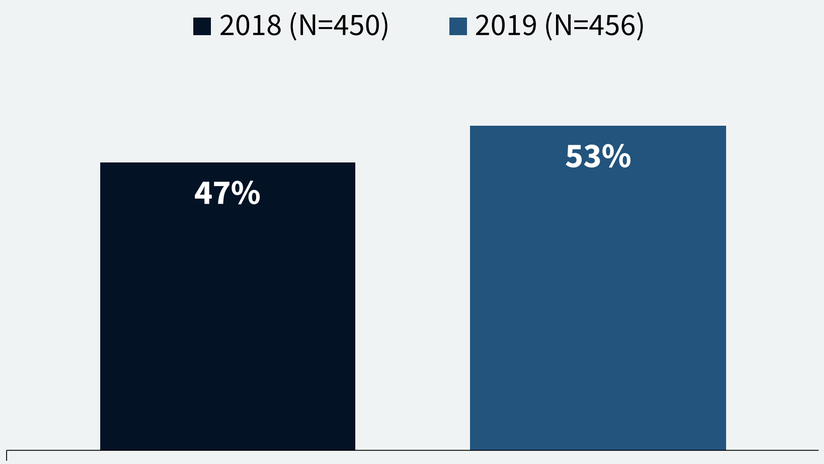
Machine Learning Is Becoming a Foundational Technology

Advances in artificial intelligence, specifically machine learning, have had highly promising results in improving the efficacy of cybersecurity technologies such as endpoint security to detect and prevent new and previously unseen-in-the-wild malware. Machine learning is now incorporated into seemingly every new cybersecurity control intended to protect core-to-edge applications and data assets from compromise. In addition, some companies that have a requirement to train machine learning algorithms on industry-specific data sets, such as sensor data from smart automobiles, employ their own data scientist. These organic and integrated use cases have appreciably increased the use of machine learning for cybersecurity purposes over the last year. In fact, more than half of the respondents report they are using machine learning technology for cybersecurity purposes to some degree, up from 47% in 2018. North American companies are ahead of the curve with more intense usage of machine learning-based controls, per the 29% of those companies leveraging machine learning extensively. This level of adoption has made machine learning a foundational cybersecurity technology and especially applicable for certain use cases.

RESEARCH HIGHLIGHT

Has your organization deployed–or does it plan to deploy–machine learning technologies for cybersecurity purposes?

(Percent of respondents)



Percentage of respondents reporting ML technologies for cybersecurity currently in use

> “There is good news with respect to the use of machine learning to address the top cybersecurity challenges discussed in this report: It is improving the triage of large volumes of security events generated from edge to core.”

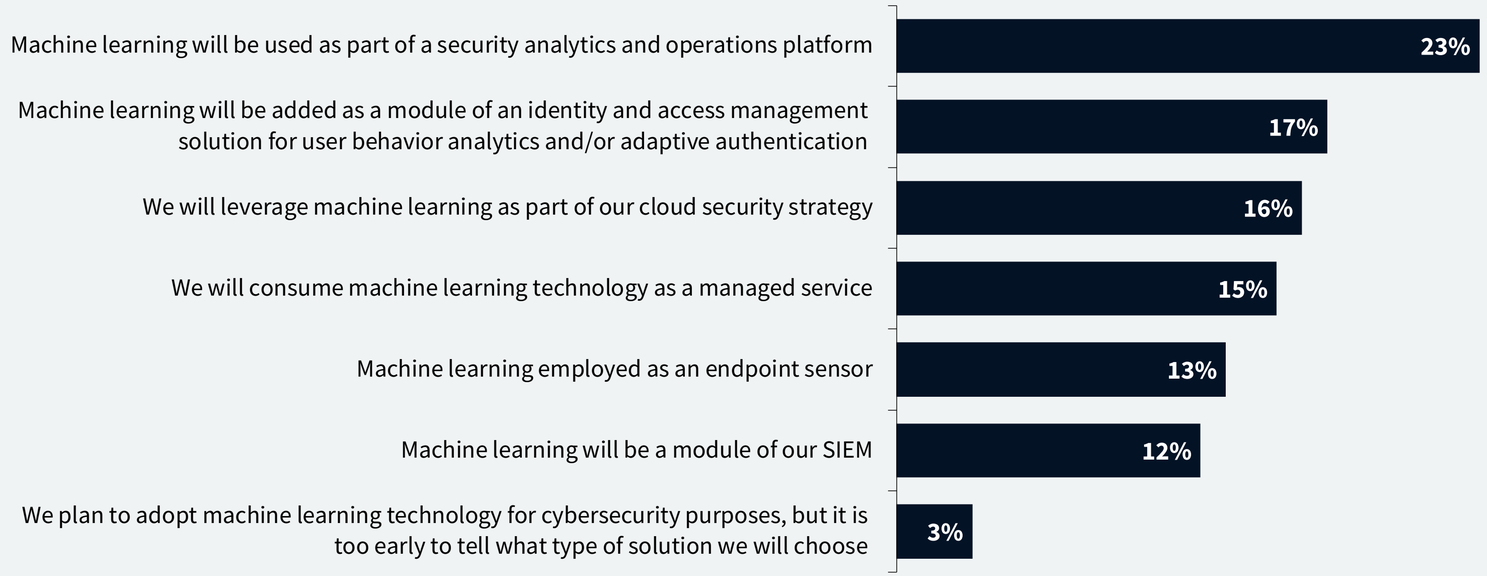
IT Is Applying Machine Learning to Address Perennial Security Challenges

There is good news with respect to the use of machine learning to address the top cybersecurity challenges discussed in this report: It is improving the triage of large volumes of security events generated from edge to core. In fact, the top two primary benefits that respondents reported related to the use of machine learning in cybersecurity controls were helping practitioners investigate more security alerts and improving accuracy by reducing false positives.

RESEARCH HIGHLIGHT

How has or does your organization plan to deploy machine learning for cybersecurity purposes?

(Percent of respondents, N=406, multiple responses accepted)



This perceived benefit of machine learning is directly correlated with the top use cases reported by respondents for the technology, which are as part of a security operations and analytics platform architecture (SOAPA) and for detecting anomalous end-user activity. While some security analysts may grumble that machine learning minimizes the importance of their role, citing the need for human intervention to evaluate alerts, cybersecurity leaders faced with the reality of an acute shortage of cybersecurity skills embrace machine learning as a means of making junior analysts more productive.

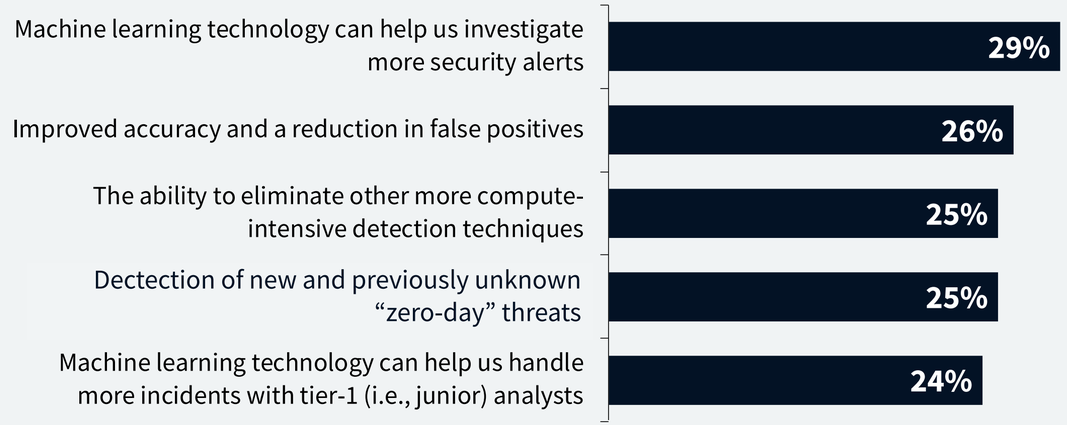
Spotlight: The Efficacy and Efficiency Benefits of Machine Learning

Cybersecurity teams too often face a tradeoff between improving the efficacy of threat detection and prevention and the operational efficiency of managing the controls required to do so. Larger, well-resourced organizations can opt to use more controls to improve their security posture, even if it means they have to manage more agents and management consoles to wade through more false positives. Smaller businesses simply do not have such options and lean toward those solutions that are more operationally efficient. This research reveals that machine learning can help cybersecurity teams improve both detection efficacy and operational efficiency.

RESEARCH HIGHLIGHT

Which of the following do you view as the primary benefits of machine learning being employed in cybersecurity controls?

(Percent of respondents, N=406, three responses accepted, five most frequently reported benefits shown)



> “In addition to alleviating some of the nagging operational challenges, 25% of research respondents cited the ability of machine learning to detect new and unknown zero-day threats as a primary benefit of machine learning.”

Case in point: In addition to alleviating some of the nagging operational challenges, 25% of research respondents cited the ability of machine learning to detect new and unknown zero-day threats as a primary benefit of machine learning. As cyber adversaries exploit new and unknown vulnerabilities and introduce new malware variants, the significance of the ability of machine learning to fortify defense against such zero-days cannot be overstated. Indeed, the adoption, use cases, and perceived benefits make machine learning an essential technology in any organization’s cybersecurity program.

In Summary: The Cloud Security Imperative

If there is a single, seminal take away from this year's Oracle and KPMG Cloud Threat Report, it is urgency, because what has fundamentally changed is the strategic nature of how cloud services and applications are being used by the businesses consuming them. Indeed, fully leveraging all the cloud has to offer in order to move quickly in competitive markets is nothing short of a critical success factor for enterprises in all industries.

The cloud security readiness gap and the challenges associated with keeping pace at scale discussed in last year's report persist as core-to-edge cybersecurity threats pose risks to how businesses operate. Threatening to further widen this gap is a problematic shortage of cybersecurity skills that will continue to impede traditional approaches to traditional challenges. This year's report is a call to action to treat cloud security as a strategic imperative, one that entails a multifaceted approach to secure the business cloud.

> "This year's report is a call to action to treat cloud security as a strategic imperative, one that entails a multifaceted approach to secure the business cloud."

The starting point for protecting mission-critical cloud services is understanding the changes that cloud adoption has brought to cybersecurity programs, including the reality of shadow IT, in which business units do not seek approval; the creation of new threat vectors; and the idea that cloud security is a responsibility shared with the service provider. The Oracle and KPMG Cloud Threat Report 2019 offers reasons for optimism that new and perennial security issues can be addressed with automation and machine learning, which promise to improve operational and threat detection efficacy. The imperative to secure the business cloud is also an opportunity to modernize cybersecurity programs for today's and tomorrow's core-to-edge compute model.

For More Information:

Additional information regarding The Oracle and KPMG Cloud Threat Report 2019 can be found here: ww.oracle.com/ctr

Details on how Oracle and KPMG can help your organization's cloud security journey can be found here:

Oracle www.oracle.com/security

KPMG www.kpmg.com/us/cyber

Appendix

Research Methodology

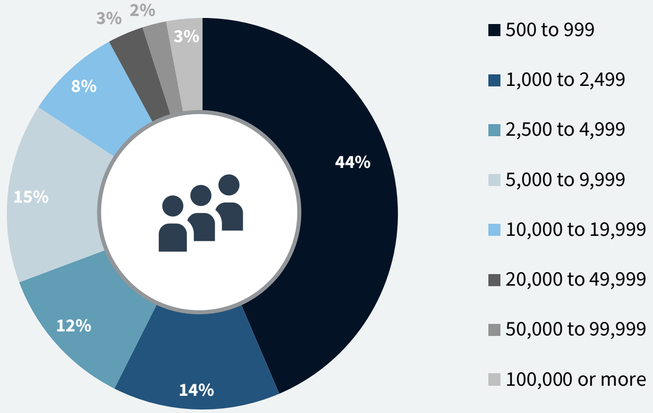
The data presented in this report was collected via a broad online survey conducted by Enterprise Strategy Group of 456 cybersecurity and IT professionals from private- and public-sector organizations in North America (United States and Canada), Western Europe (United Kingdom), and Asia (Australia and Singapore) between October 19, 2018 and November 5, 2018. To qualify for this survey, respondents were required to be responsible for evaluating, purchasing, and managing cybersecurity technology products and services and to have a high level of familiarity with their organization's public cloud utilization. All respondents were provided an incentive to complete the survey.

Note: Totals in figures and tables throughout this report may not add up to 100% due to rounding.

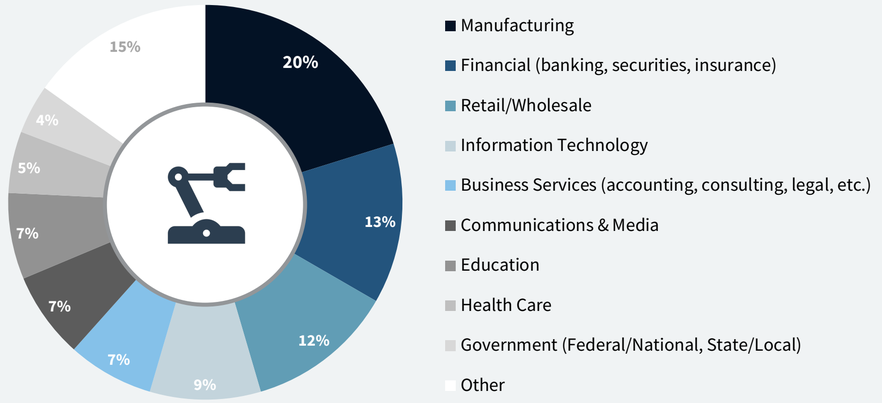
Participant Demographics

The following figures detail the demographics of the respondent organizations.

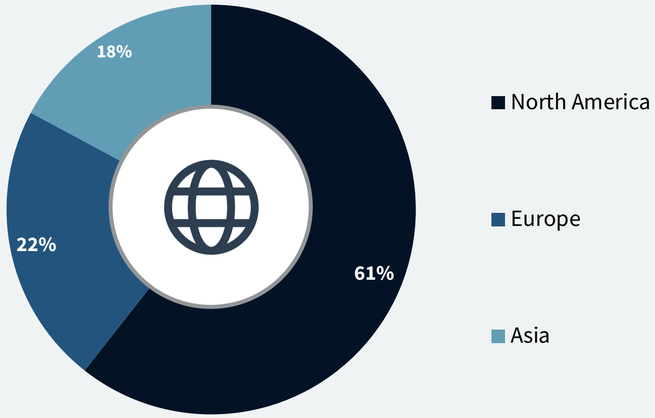
Respondents by number of employees (Percent of respondents, N=456)



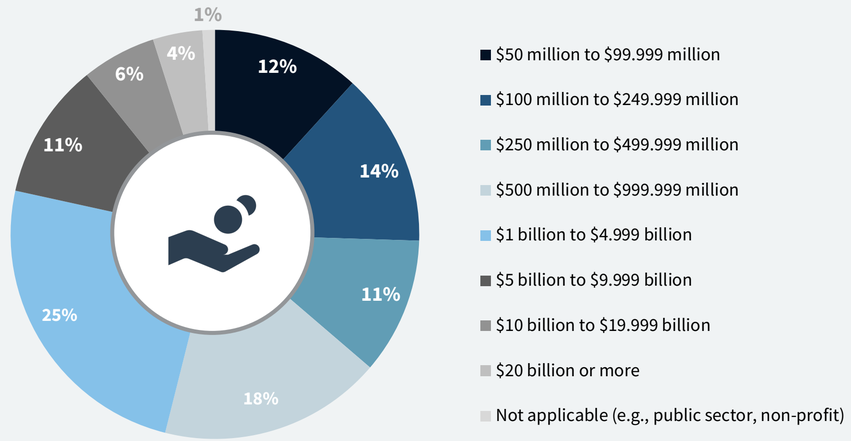
Respondents by industry (Percent of respondents, N=456)



Respondents by region (Percent of respondents, N=456)



Respondents by annual revenue (Percent of respondents, N=456)



Key Contributors

Mary Ann Davidson
Chief Security Officer – Oracle Corporation

Greg Jensen
Senior Principal Director of Cloud Security – Oracle Corporation

Tony Buffomante
Principal – KPMG LLP

Laeeq Ahmed
Managing Director – KPMG LLP

Brian Jensen
Managing Director – KPMG LLP

Doug Cahill
Group Director and Senior Analyst – Enterprise Strategy Group

Special Thanks:
Mike Beaudet, David Belson, Suzanne Blackstock, Darren Calmen, Steve Daheb, Adam DeMattia, Vidhi Desai, James Finlaw, Matt Flynn, Sailesh Gadia, Jennifer Gahm, Laurent Gil, Dain Hansen, John Hodson, Mike Kane, Brendan Keane, Troy Kitch, Dan Koloski, Fred Kost, Russ Lowenthal, Nicole Maloney, Eric Maurice, Mary Beth McCombs, Josh McKibben, Lori Schneider Pierskalla, Peter Sinanian, Tim Stahl, Kyle York