ORACLE KPMG

Oracle and KPMG Cloud Threat Report 2020

Addressing Security Configurations Amidst a State of Constant Change

Research conducted in partnership with ESG

Contents

03 Executive Summary

06 Cloud Adoption Expands and Diversifies

07 Strategic Initiatives are Driving Cloud Adoption

07 Public Clouds Are Viewed as More Secure than On-premises Environments

09 Business-critical Applications Are Moving to Public Clouds

10 IaaS and PaaS Usage Shifts to Production

11 **Spotlight:** True Hybrid Cloud Deployments Are Emerging

13 The Cloud Security Readiness Gap

14 Cloud Adoption Outpaces Security Readiness

15 Specialty Tools Are Increasing Complexity

17 **Spotlight:** New Cybersecurity Leadership Roles Are Emerging

18 A Network-centric Orientation Persists

18 **Preview:** Demystifying the Cloud Security Shared Responsibility Model

20 Cloud Configuration Management Challenges and Ramifications

21 Cloud Consumption Is Creating Visibility Blind Spots

22 Organizations Are Not Following the Rule of Least Privilege

23 **Spotlight:** Unprotected Cloud Secrets Are Being Exposed

24 **Preview:** The Business Impact of the Modern Data Breach

26 Securing Cloud Configurations Requires a Focus on Identity

28 Cloud Configuration Management via DevSecOps

29 Integrating Security with DevOps Requires a Cultural Shift

31 The Need for Automation Is Driving DevSecOps Adoption

32 **Spotlight:** The Pets versus Cattle of Immutable Infrastructure

33 DevSecOps Automates Securing the Application Lifecycle

Build-time Use Cases

Runtime Use Cases

Dev-time Use Cases

35 **Preview:** The Mission of the Cloud-centric CISO

36 Cyber-attacks and Business Fraud

37 Phishing Targets and Techniques Are Expanding

38 **Spotlight:** The Phishing of Privileged Cloud Credentials

39 A Focus on the Human Perimeter Is Required to Combat Phishing

40 **Preview:** Addressing Cyber-risk and Fraud in the Cloud

42 The High Expectations of Machine Learning

43 AI/ML Are Core Product Requirements

45 AI/ML Are Viewed as Applicable for a Range of Cybersecurity Use Cases

46 There Is Overly Exuberant Confidence in the Efficacy of AI/ML

48 In Summary: Culture Is the Catalyst to Close the Readiness Gap

50 Appendix

51 Research Methodology

51 Participant Demographics

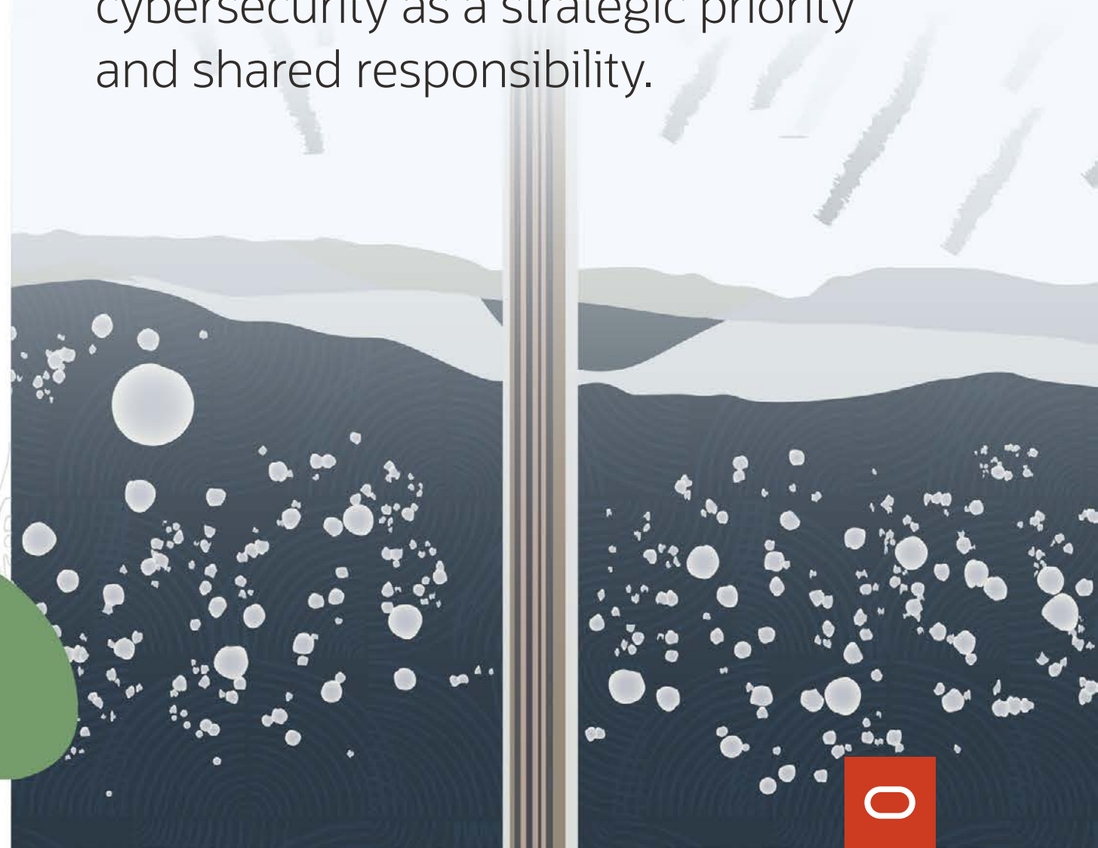
Executive Summary

Today's businesses are embarking on sweeping digital transformation (DX) initiatives to fundamentally retool business operations and rethink entire business models through the strategic use of digital technologies such as cloud services, mobile applications, and data analytics. The broad adoption of cloud applications is helping support a surge in remote workers while also creating new opportunities for cyber-criminals to conduct cyber fraud.

The flexibility and scalability of cloud services and applications make these technologies a prerequisite for all modern DX strategies. This is forcing businesses around the world to embrace an essential cultural shift in the relationship between business and technology, one that empowers business units to leverage the self-service and on-demand nature of cloud services to transform the business with new levels of agility. However, as progressive business leaders move quickly to digitally transform their operations, effective security controls are all too often an afterthought as companies eschew proven best practices and make it difficult—if not impossible—for the business to accurately assess and manage enterprise risk.

This situation is untenable. Disparate perspectives and agendas need to be unified into a cohesive strategy, with all constituents—lines of business, application development, IT operations, cybersecurity, risk, and compliance teams—internalizing cybersecurity as a strategic priority and shared responsibility. Secure DevOps programs (or DevSecOps) offer a means to both automate the integration of security into DevOps processes and, most importantly, serve as a cultural catalyst to move security closer to the business. Those who treat their journey to the cloud as an opportunity to proactively cultivate a culture of "security first" will strike the right balance between enabling the use of cloud services and protecting sensitive transactions and data.

Disparate perspectives and agendas need to be unified into a cohesive strategy, with all constituents—lines of business, application development, IT operations, cybersecurity, risk, and compliance teams—internalizing cybersecurity as a strategic priority and shared responsibility.



The Oracle and KPMG Cloud Threat Report 2020 not only analyzes cloud adoption trends and the current threat landscape, but also focuses on how businesses can automate configuration management best practices to help close this near-ubiquitous cloud security readiness gap. This year's report is the first in a 5-part series, with follow-on reports offering insights into research findings on central cloud security topics including:

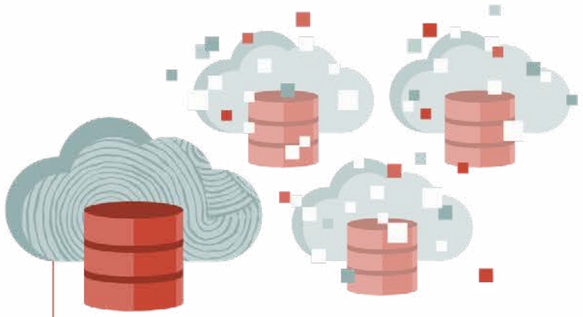
- Demystifying the cloud security shared responsibility model.
- The business impact of the modern data breach.
- Addressing cyber-risk and fraud in the cloud.
- The mission of the cloud-centric CISO.

But first things first. Key findings explored in the Oracle and KPMG Cloud Threat Report 2020 include:

- **Cloud adoption continues to expand.** Digital transformation, cloud-first initiatives, and a bullish level of confidence in the security of public clouds is driving an expanded use of cloud services.
- **Cybersecurity teams are playing catch-up.** Organizations are simply not ready to secure the rate at which the business has already adopted cloud services, creating a palpable cloud security readiness gap.
- **The basics of cloud security are still not understood.** Worsening confusion over the shared responsibility security model is a key contributor to the readiness gap.
- **Cyber fraud takes center stage.** The threat landscape is evolving, with tried and true phishing attacks leading to an increase in cyber business fraud and compromised privileged cloud credentials.
- **Misconfigured cloud services are prevalent, problematic, and the top cloud security priority.** A cloud security visibility gap has made hardening the configuration of cloud services a systemic challenge.
- **Retooling for the cloud starts with people and process.** DevSecOps, integrating cybersecurity into DevOps processes, offers the means to automate cloud configuration management best practices and narrow the cloud security readiness gap.
- **Business information security officers (BISOs) have a clear charter.** To better align cybersecurity and business objectives, cybersecurity leaders are being embedded in the business.
- **Many are betting on machine learning (ML).** Machine learning, as an implementation of artificial intelligence, has become a foundational cybersecurity technology, which many organizations now view as a must-have technology for a range of use cases, including an expanded role in the security operations center (SOC).

88%

All workloads will be autonomously updated within 3 years.



3/4

Have experienced data loss from a cloud service more than once.

50%

Will have all their data in public cloud stores in 2 years.

Have or plan to hire a CISO with more cloud security skills.

92%

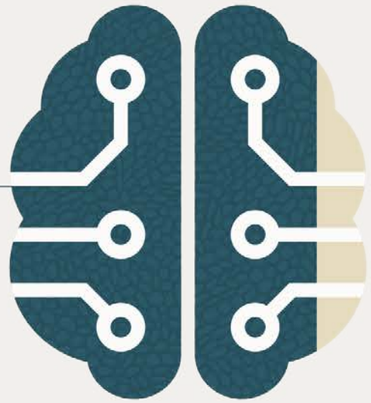
Have a cloud security readiness gap.

****

59% Have had privileged cloud credentials phished.

87%

View artificial intelligence as a must-have for security controls.



3/4

Feel the cloud is more secure than their data center.

3x

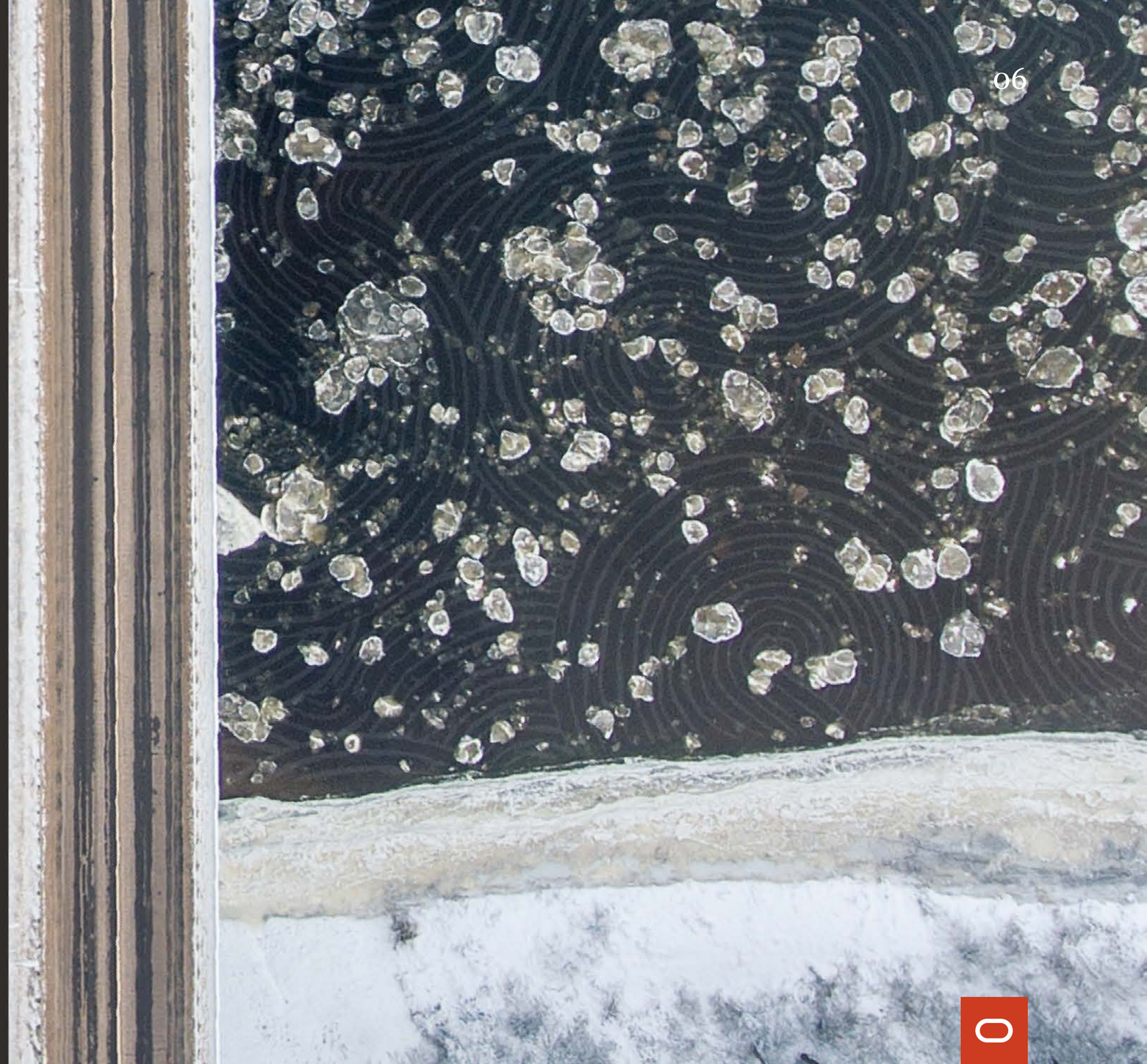
More worried about corporate security than safety at home

>10

Data loss events experienced by orgs with multiple misconfigured cloud services.

Cloud Adoption Expands and Diversifies

The Varied Uses of Cloud Services and Platforms Define Today's Hybrid, Multi-cloud Environments



Strategic Initiatives are Driving Cloud Adoption

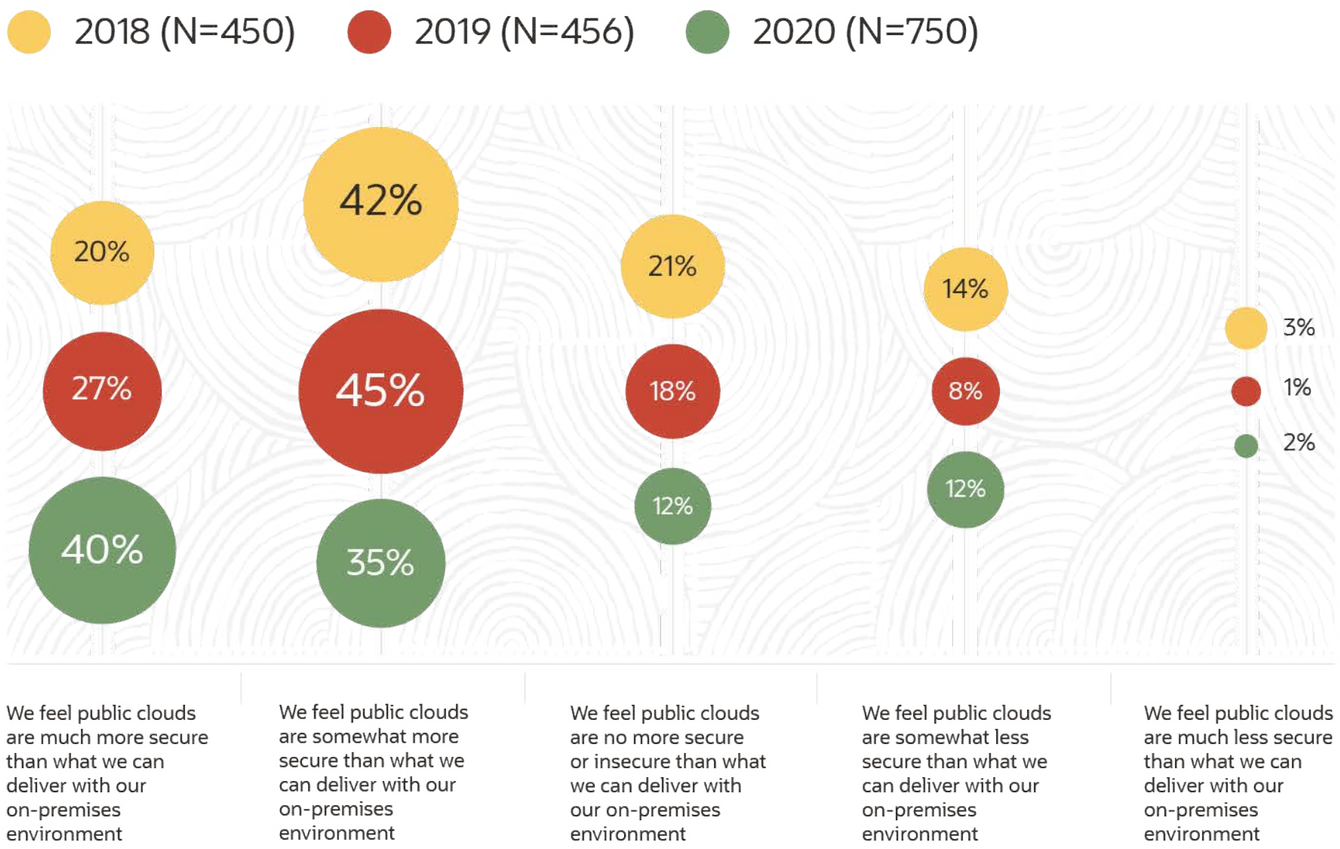
The migration to cloud services is often part of broader strategic initiatives, principally digital transformation (DX) and cloud-first.[1] The profound impact that DX has on business strategy, business models, and business processes by leveraging new technologies is often enabled by an aggressive cloud-first strategy that calls for delivering new business applications from the cloud. The symbiotic relationship between these strategies is directly correlated with cloud adoption, per the 88% of organizations who have attained a more mature level of digital transformation by utilizing cloud services—specifically, infrastructure services, which are seen as critical enablers of the 2020 economy. Furthermore, 3x as many IT professionals are more worried about the security of company financials and intellectual property (IP) than the security and safety of their own house and family.

[1]Source: ESG Research Report, 2020 Technology Spending Intentions Survey, February 2020.

Public Clouds Are Viewed as More Secure than On-premises Environments

Most are well past concerns about whether public clouds are secure and other such concerns inhibiting adoption. In fact, the conversation is now about relativity: how secure public cloud environments are perceived to be relative to customer-managed data centers. The verdict is in and the sentiment is clear—public cloud environments are viewed as more secure than what organizations can deliver in their on-premises environments.

The verdict is in and the sentiment is clear—public cloud environments are viewed as more secure than what organizations can deliver in their on-premises environments.



Even in the face of well publicized public cloud data loss incidents, many consider public clouds as more secure and resilient environments. In fact, 40% of our respondents shared a sentiment that they view public clouds as much more secure than what they can deliver with their on-premises environment, a notable 13% year-over-year increase. Such bullishness punctuates the positive view of the security posture of public clouds.

But for some, there is at least some concern when it comes to trusting cloud service providers (CSPs). Specifically, the concentration of market share by a handful of cloud services providers has 81% of our respondents concerned about the potential for complacency. Another 80 percent of IT professionals are also concerned that the cloud service providers they do business with will become competitors in their core markets. There is no ambiguity—now that customers have gotten comfortable with the security of public clouds, they want to make sure CSPs stay vigilant and committed to strong cybersecurity measures.

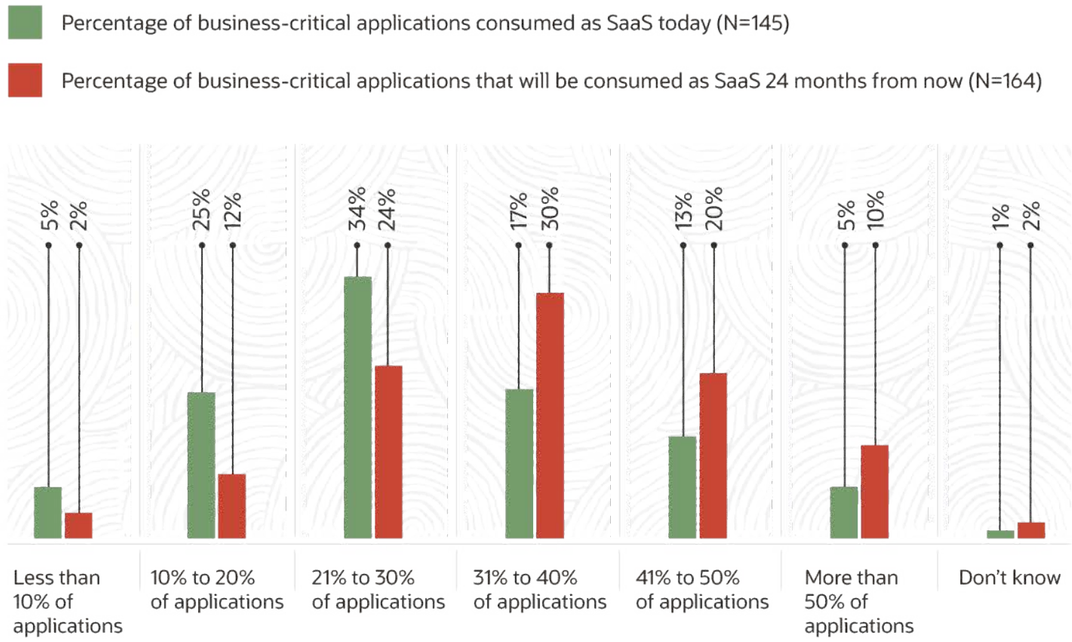
Business-critical Applications Are Moving to Public Clouds

The fact that nearly 9 out of 10 companies who participated in this year's study are now using software-as-a-service (SaaS) does not tell the full story of SaaS adoption. Behind this statistic is the widespread use of SaaS for office productivity and collaboration and, notably, a planned increase in SaaS for business-critical applications. The expansion of SaaS as a consumption model and delivery mechanism includes the full stack of business-critical applications, from customer-facing front-office interfaces through middle-office transaction processing to back-office operations.

When it comes to consuming business-critical applications as a service (i.e., via SaaS), organizations cite, on average, a 9% increase over the next 24 months. This shift to SaaS for those applications that are truly mission-critical is another indicator that businesses are increasingly comfortable with the security posture of cloud service providers. Indeed, the applications that are the backbone of business operations—enterprise resource planning (ERP), customer relationship management (CRM), human capital management (HCM), IT service management (ITSM), and more—are now in the process of moving to the cloud.

The expansion of SaaS as a consumption model and delivery mechanism includes the full stack of business-critical applications, from customer-facing front-office interfaces through middle-office transaction processing to back-office operations.

What percentage of your business-critical applications are SaaS? How do you expect this to change over the next 24 months? (Percent of respondents)



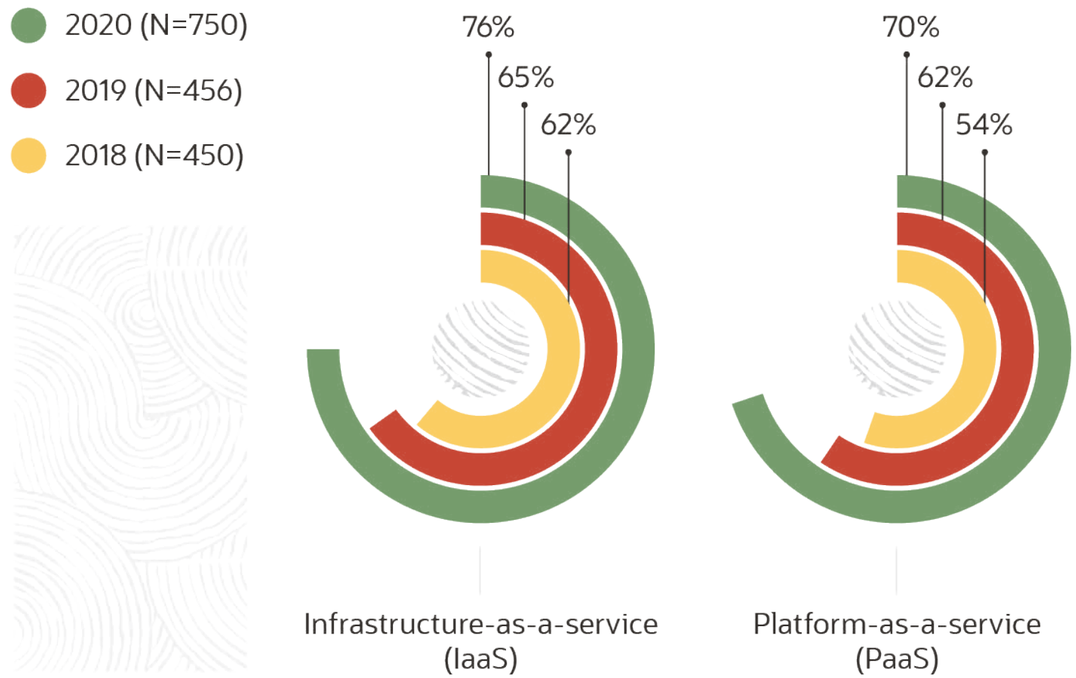
IaaS and PaaS Usage Shifts to Production

This year's research reveals that an organization's journey to the cloud can take different forms, with some businesses opting to migrate their existing on-premises business-critical applications to the cloud via a "lift-and-shift" approach. Just over a third of the business-critical applications operated by the companies who participated in our study will be migrated to the cloud "as-is" over the next 24 months. Lift-and-shift projects, which utilize a CSP's infrastructure-as-a-service (IaaS) platform ostensibly as a hosting environment for production applications, are one of the drivers behind a notable year-over-year increase in the use of IaaS.

In addition to an uptick in the adoption of IaaS, platform-as-a-service (PaaS) usage has grown, indicating many organizations are developing new, cloud-native applications. The lifting and shifting of applications to a public cloud is often an interim step to either re-platforming those applications or consuming them as a SaaS offering from a third party. The net result is the diverse portfolio of cloud services of today's hybrid, multi-cloud enterprise.

This year's research reveals that an organization's journey to the cloud can take different forms, with some businesses opting to migrate their existing on-premises business-critical applications to the cloud via a "lift-and-shift" approach.

Which of the following types of cloud services – sanctioned and unsanctioned - are in use at your organization? (Percent of respondents, multiple responses accepted)

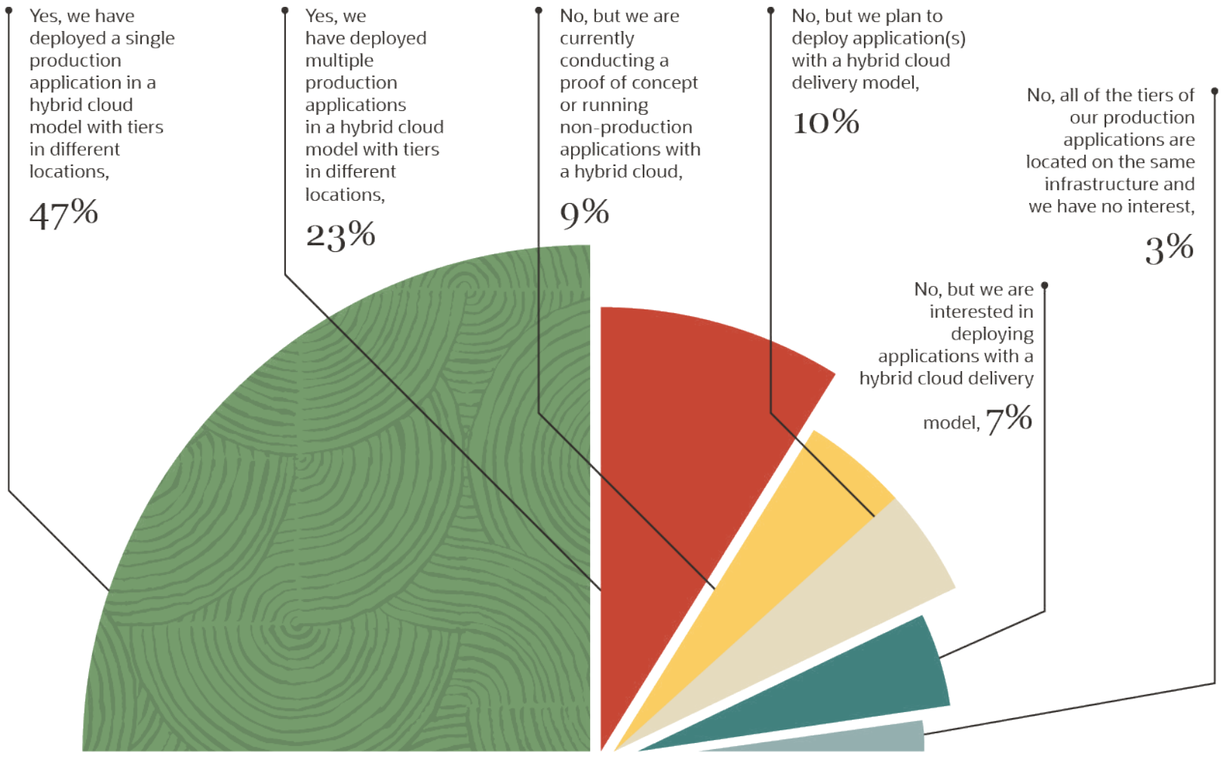


Spotlight: True Hybrid Cloud Deployments Are Emerging

The terms “hybrid cloud” and “multi-cloud” continue to foster confusion, yet, for most organizations, hybrid, multi-cloud environments are, in fact, the complexion of the modern data center. Since definitions are in order, for the purposes of this year’s report, multi-cloud environments are simply those that use services from more than one cloud service provider. Although a hybrid cloud could simply mean having both a customer-managed data center and a footprint in a public IaaS platform, we will view hybrid clouds at the application level in which tiers of an application are deployed across both an on-premises environment and a public cloud.

So, in that context, what did research participants share about true hybrid cloud deployments? While 55% of organizations noted that 41% of their server workloads will be in a public cloud within 24 months,[2] plenty of servers will remain on-premises or in customer-managed colocation facilities. Nearly half (47%) of respondents from this year’s Oracle/KPMG survey have deployed a single application in a hybrid manner, in which the tiers of an application are deployed in different environments, and nearly another quarter (23%) have done so with multiple applications. What’s behind these true hybrid deployments?

Do any of your company’s workloads currently run in this hybrid manner? (Percent of respondents, N=750)



[2]Source: ESG Master Survey Results, Leveraging DevSecOps to Secure Cloud-native Applications, December 2019.

Complexity is an enemy of cybersecurity programs as hybrid clouds exacerbate existing cybersecurity challenges while introducing new obstacles.

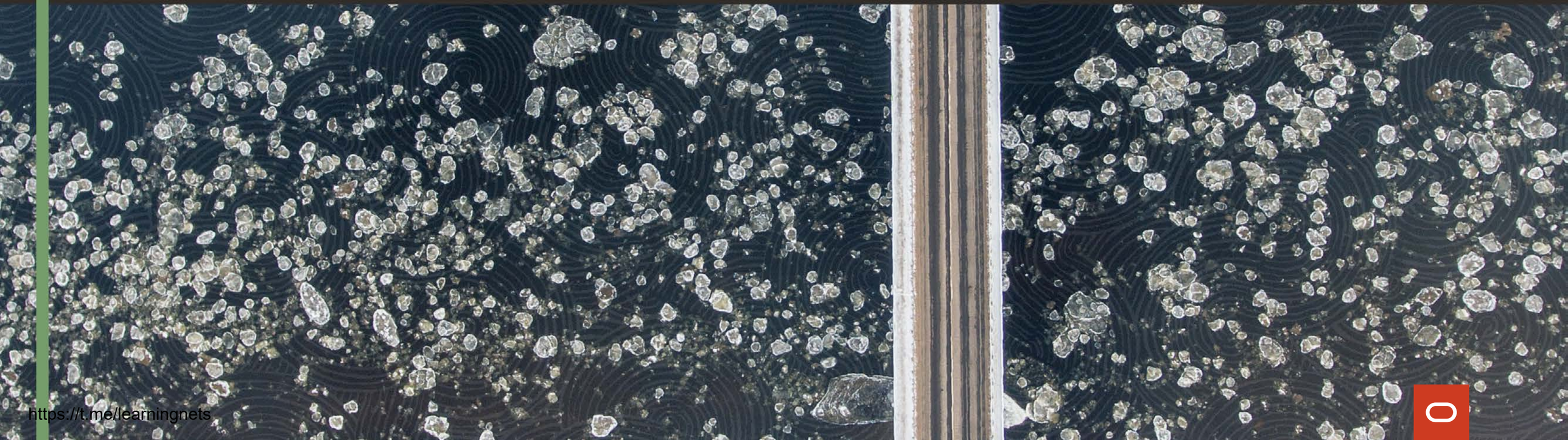
For some businesses, security and compliance considerations are such that database tiers need to stay directly under their control. At the same time, there are clear benefits to leveraging public cloud platforms for performance-related considerations, including auto-scaling groups to accommodate peak demand periods, obviating the need to over-provision server farms, and overcoming the staffing challenges impacting businesses today. Other performance drivers include the use of content delivery networks (CDNs) to optimize local access to web-based front-ends via caching.

Another dynamic driving hybrid cloud application deployments is the increased use of application containers, which provide a level of portability, and thus flexibility, for deploying across the different environments that comprise hybrid, multi-cloud organizations. To that point, 46% of participants in another recent survey found that their container-based applications will be deployed across a combination of public cloud platforms and private data centers in the future.[3] Unfortunately, complexity is an enemy of cybersecurity programs, and as this report discusses, hybrid clouds exacerbate existing cybersecurity challenges while introducing new obstacles.

[3]Source: ESG Master Survey Results, Leveraging DevSecOps to Secure Cloud-native Applications, December 2019.

The Cloud Security Readiness Gap

Unprepared for the Velocity of Cloud Usage,
Organizations Struggle with Retooling



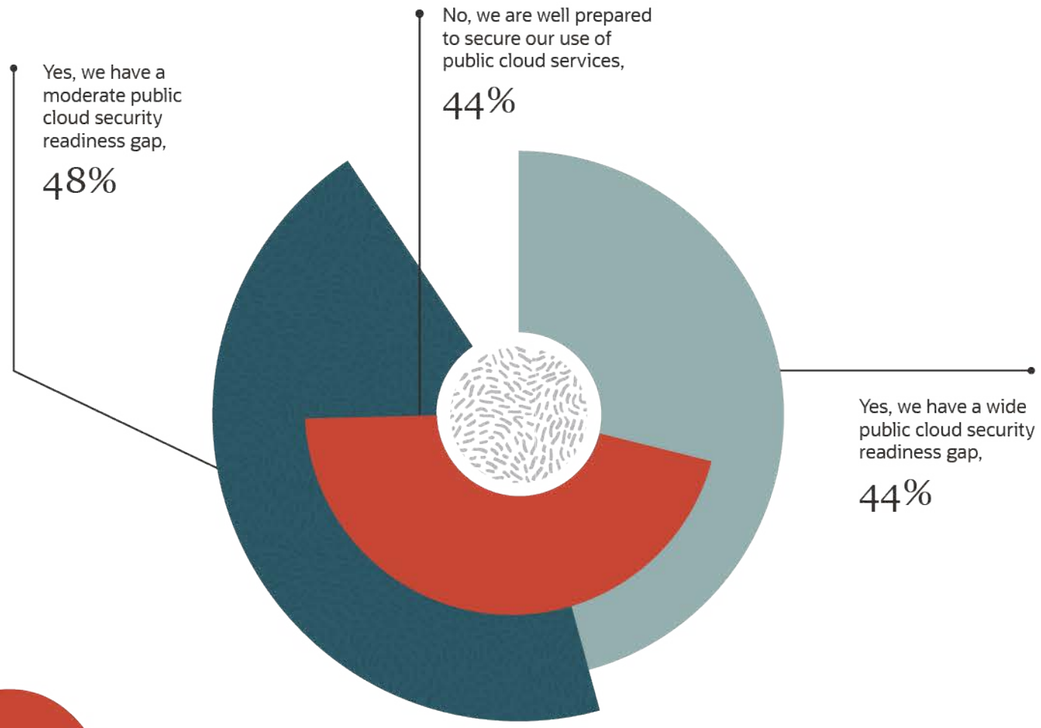
Cloud Migration Outpaces Security Readiness

The sheer rate at which the use of cloud services is expanding is creating an appreciable cloud security readiness gap. In fact, 92% of this year's research respondents admitted that their organization has a gap between current and planned cloud usage and the maturity of their cloud security program. This issue is punctuated by a disconcerting 44% of our participating organizations who said they have a wide gap.

But how did we get to a state of such a divide between use and readiness? For starters, cloud services and applications are often consumed by a business unit outside of the purview of the centralized IT and cybersecurity teams. Then, as lines of business realize rapid time to value, use expands. Collaboration with the cybersecurity team is perceived as threatening to throttle speed. Herein lies the issues of velocity outpacing security readiness and the need for a cultural shift in how organizations approach cybersecurity.

92% of this year's research respondents admitted that their organization has a gap between current and planned cloud usage and the maturity of their cloud security program.

Do you feel your organization has a readiness gap created by its current cloud use, rate of expansion, and the maturity of its cloud security program? (Percent of respondents, N=750)



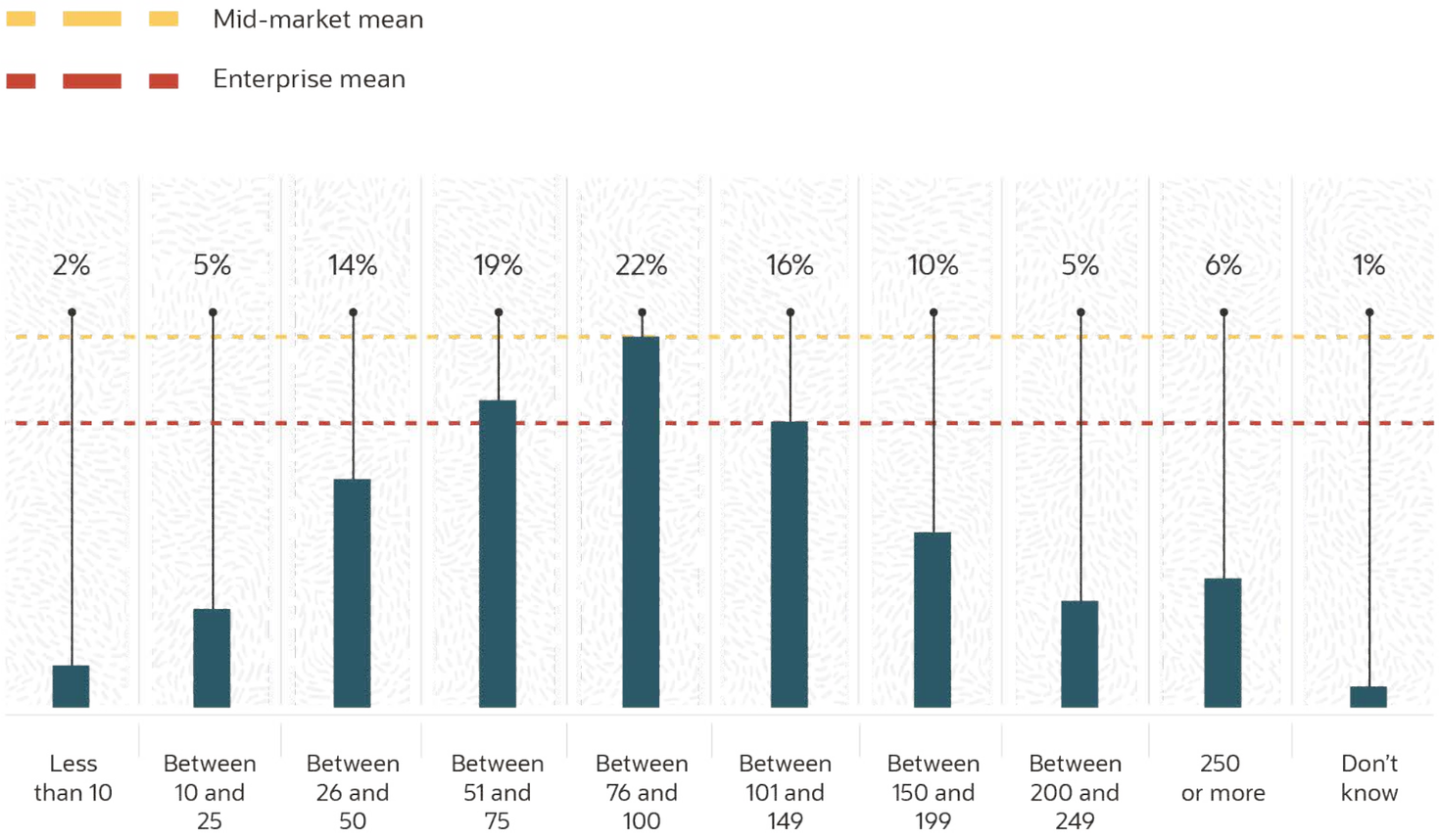
Specialty Tools are Increasing the Need for Security

The cloud security readiness gap manifests in a variety of challenges for respondents, including environmental differences, per the 78% who noted that the differences between cloud-resident and on-premises applications and infrastructure require a different set of security policies and processes. Such environmental differences have led directly to the acquisition of additional discrete controls, introducing additional complexity. To this point, 70% of our research participants shared that too many specialized tools are required to secure their public cloud footprint.

Just how many cybersecurity products are used by organizations charged with securing increasingly complex hybrid, multi-cloud environments? On average, our research respondents report their organization uses over 100 discrete cybersecurity controls!

On average, our research respondents report their organization uses over 100 discrete cybersecurity controls.

Approximately how many discrete cybersecurity products do you believe/estimate are in use across your entire company/ organization today? (Percent of respondents, N=750)



There is, however, scrutiny on the economics of such incremental investments. Some businesses are treating the need to refresh their stack of cybersecurity controls as an opportunity to consolidate a disparate set of tools into an integrated platform. In fact, 80% of organizations are now considering buying a significant amount of their cybersecurity technologies from a single vendor.[4] Businesses are also starting to align their organizational model for a more unified approach to securing hybrid, multi-cloud environments. While only 18% have already done so, another 50% of respondents note that although they currently have different teams responsible for securing cloud-native applications, they plan to merge those responsibilities in the future.[5] Who is leading this effort that requires a strategic perspective?

[4]Source: ESG Master Survey Results, Enterprise-class Cybersecurity Vendor Sentiment, March 2020.

[5]Source: ESG Master Survey Results, Leveraging DevSecOps to Secure Cloud-native Applications, December 2019.

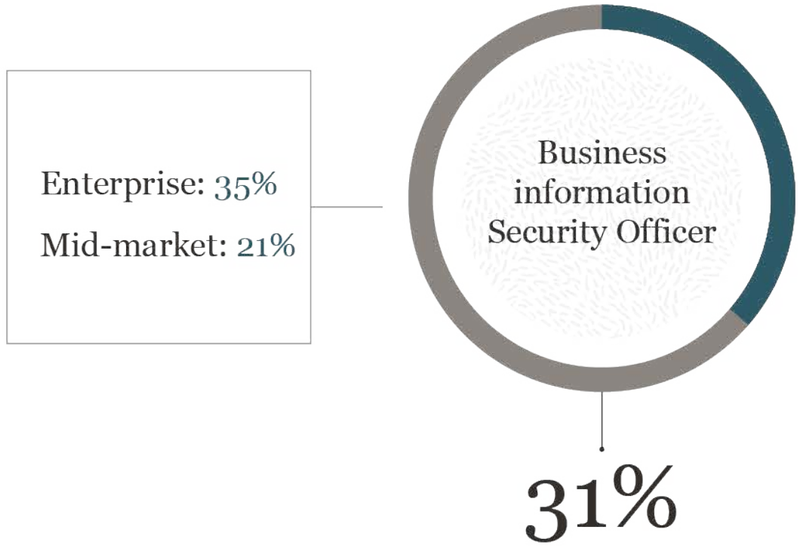
Spotlight: New Cybersecurity Leadership Careers Are Emerging

This year's study reveals that more organizations have a cloud security architect than a security architect, reflecting a retooling of cybersecurity programs to address the readiness gap.

Prior Oracle and KPMG Cloud Threat Reports have noted the rise of cloud security architects to drive the implementation of cloud security strategies inclusive of policies and tool selection. This year's study reveals that more organizations have a cloud security architect than a security architect, reflecting a retooling of cybersecurity programs to address the readiness gap. Cloud security architects are working with the CISO and others on evaluating how the shift to the cloud, and the need to retool their stack of cybersecurity controls, represents an opportunity to reduce the number of controls they operate.

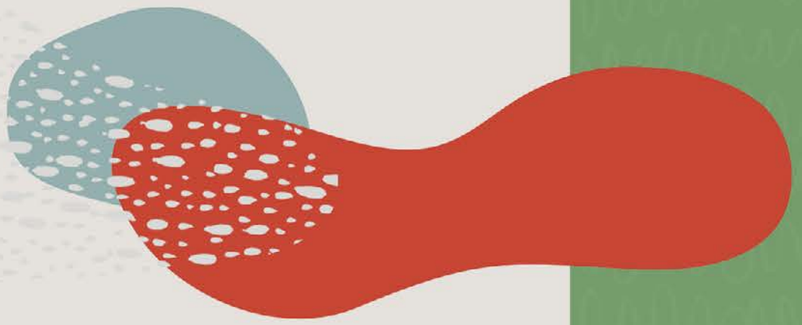
The broad adoption of cloud services has resulted in the emergence of another cybersecurity leadership role, the business information security officer (BISO). Larger organizations are, not surprisingly, ahead of mid-market businesses in expanding and diversifying their cybersecurity leaders, with over a third already employing at least one BISO. This report series will include a more in-depth discussion on the role of the BISO in our upcoming CISO report.

Which of the following security leadership roles does your organization have? (Percent of respondents, N=750, multiple responses accepted)



A Network-centric Orientation Persists

On-premises cybersecurity programs have often been designed, in large part, based on a castle and moat threat model and thus a focus on network security processes, technologies, and skills. As enterprises with a network-centric orientation transition more of their applications and infrastructure to public clouds, it is natural to expect, as cited by 73% of respondents, that a lack of access to the physical network, along with the elastic nature of cloud computing, creates blind spots. Improving cloud security visibility starts with revisiting how we think about the amorphous perimeter of today's hybrid, multi-cloud environments.

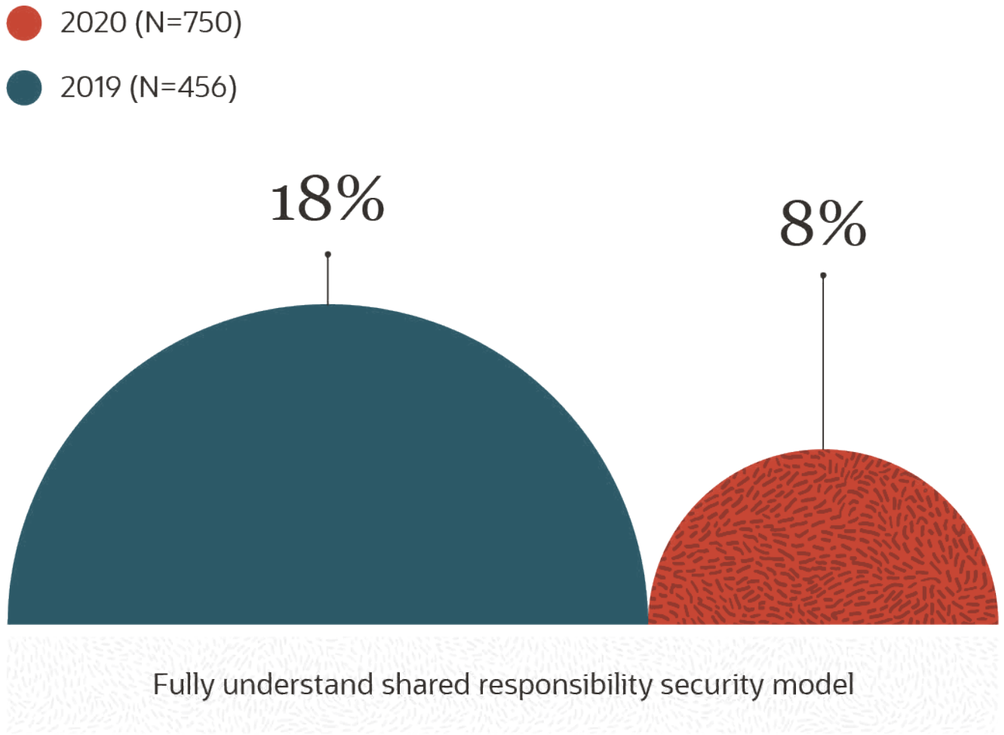


Preview: Demystifying the Cloud Security Shared Responsibility Model

The notion of cloud security as a shared responsibility is a foundational cloud security and risk management construct for conveying the division of labor between the cloud service provider and service subscriber. A clear understanding of the shared responsibility model for all types of cloud services is nothing short of a cornerstone for cloud security programs. Confusion has worsened around all types of cloud services, including roughly two-thirds (67%) of respondents who indicated they find the shared responsibility model for securing SaaS applications the most confusing, a 13% year-over-year increase. And only 8% of this year's respondents state that they fully understand the cloud security shared responsibility model for all types of cloud services, compared with 18% in 2019.

A clear understanding of the shared responsibility model for all types of cloud services is nothing short of a cornerstone for cloud security programs.

I fully understand my team's role with regards to the shared responsibility security model. (Percent of respondents, N=750, multiple responses accepted)

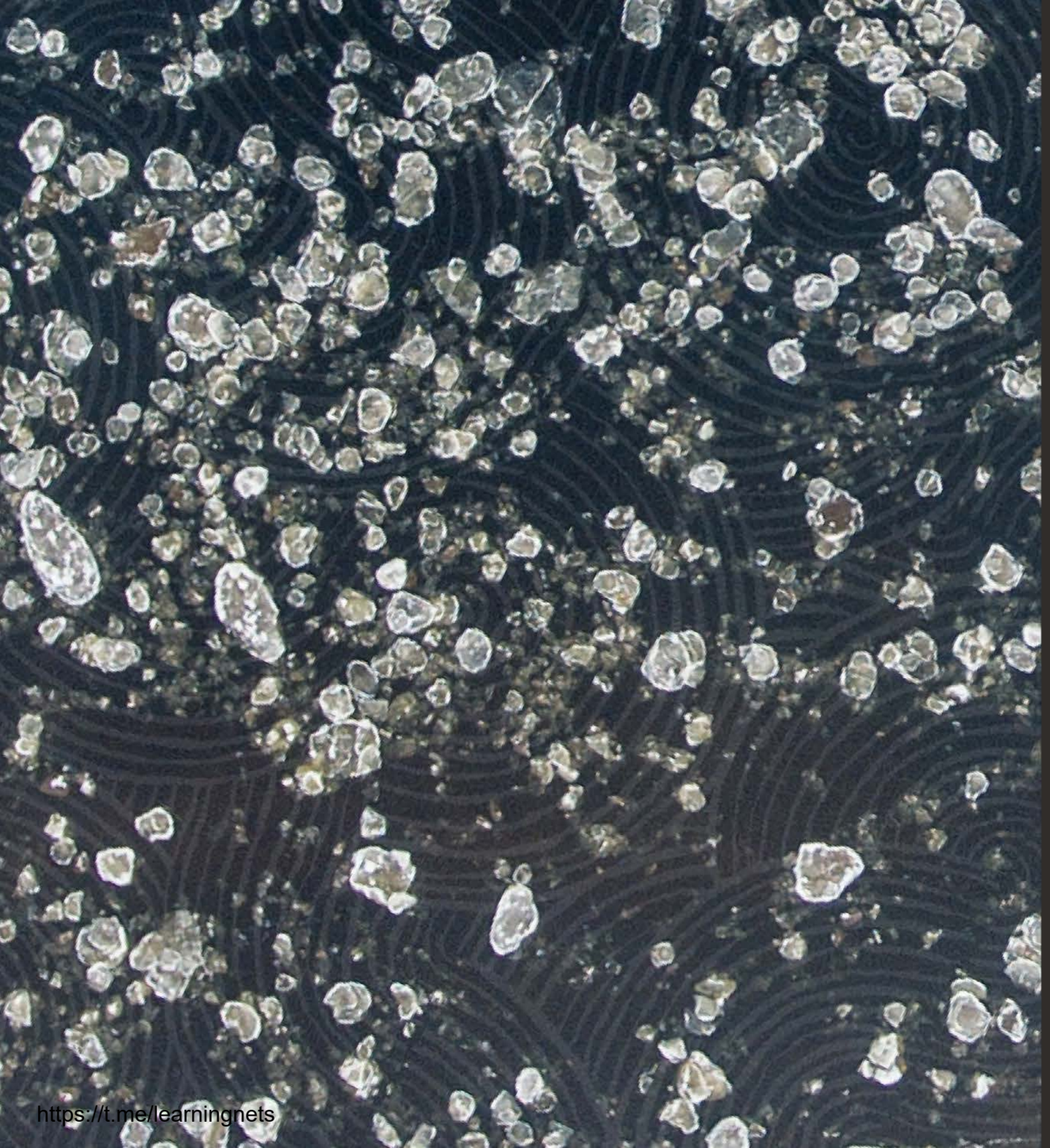


When it comes to SaaS applications, subscribers need to be clear that they are responsible for data security, identity and access management, and compliance with applicable industry regulations. Considering the broad adoption of SaaS applications, we, as an industry and community, have work to do.

This lack of clarity on this foundational cloud security concept is a key contributor to the cloud security readiness gap. The issue is compounded by the broad portfolio of cloud services nearly all organizations use in which there are discrepancies between not just the type of services but between service providers.

As a pillar of cloud security, this topic warrants further exploration. As such, stay tuned for our upcoming report, Demystifying the Cloud Security Shared Responsibility Model, which will be part of the ongoing Cloud Threat Report series.

When it comes to SaaS applications, subscribers need to be clear that they are responsible for data security, identity and access management, and compliance with applicable industry regulations.



Cloud Configuration Management Challenges and Ramifications

Many are not following best practices, leading to data loss and a need to retool.

Cloud Consumption Is Creating Visibility Blind Spots

The abstract nature of operating in someone else's data center and sharing responsibility has led to a common refrain: a lack of visibility. We wanted to put some definition to this issue in this year's report and found a clear theme: Cloud adoption has created a series of configuration management challenges. In fact, the biggest cloud security challenge shared by our respondents is also one of the areas in which they need to improve visibility into their organization's use of public cloud services: the configuration of server workloads.

Two other configuration management issues that are closely related—identifying misconfigured security groups (i.e., host-based firewalls) and externally facing servers—are also top of mind. Such configuration issues expose servers to unauthorized inter-workload traffic that would allow for the lateral movement of malware as well as near-instant port scanning by armies of malicious bots.

Which areas do you feel are the most important to improve security visibility for your organization's use of public cloud services? (Percent of respondents, N=674, three responses accepted)

Organizations Are Not Following the Rule of Least Privilege

The fundamental concept of restricting access rights for users and accounts to the minimum needed to conduct a task and do one's job is paramount in today's hybrid, multi-cloud reality.

Beyond the need for greater visibility into the configuration of cloud infrastructure, we wanted to gauge whether research participants detected any misconfigured cloud services over the last 12 months. What did we find out? There is no shortage of improperly configured cloud services reported by our respondents, which, given the visibility gap, is not in itself surprising. But the thread that connects the types of configuration issues reported by our respondents reminds us that on-premises principles apply in the cloud.

At the forefront of such best practices is the need to implement least privilege access policies. To be clear, this is not the responsibility of the service provider, irrespective of the type of cloud services. The fundamental concept of restricting access rights for users and accounts to the minimum needed to conduct a task and do one's job is paramount in today's hybrid, multi-cloud reality. An abstracted environment in which there is a matrix of many-to-many relationships between users, accounts, and clouds arguably complicates implementing least privilege, as evidenced by our research findings. Front and center, and leading off as the top misconfigured cloud service, is over-privileged accounts.

- **Over-privileged accounts (37%).** Not all accounts need root or admin privileges. The more accounts that have escalated rights, the greater the risk for business and the greater the reward for attackers.
- **Exposed web servers and other types of server workloads (35%).** Server workloads that are externally facing are subject to port scanning if they are not routed through a bastion host or if their security groups are not properly configured to prevent unauthorized protocols and traffic over open ports. A bastion host is a minimally configured, hardened, single purpose proxy that provides access to an internal network from the internet.
- **Object store-resident data not appropriately secured via access control lists (ACLs) (34%).** Confusion related to the ACLs that control who can access what types of data stored in object stores has led to unauthorized access and data loss.
- **The lack of multi-factor authentication (MFA) (33%).** Cloud consoles are the point of control for cloud accounts, and, as such, access should be protected with an additional authentication challenge. We will revisit this important topic.
- **Disabled logging for capturing an audit trail of cloud activity (31%).** The dynamic and temporal nature of IaaS platforms requires retaining an audit trail of activity for regulatory compliance and investigative purposes.

Spotlight: Unprotected Cloud Secrets Increase Business Vulnerability

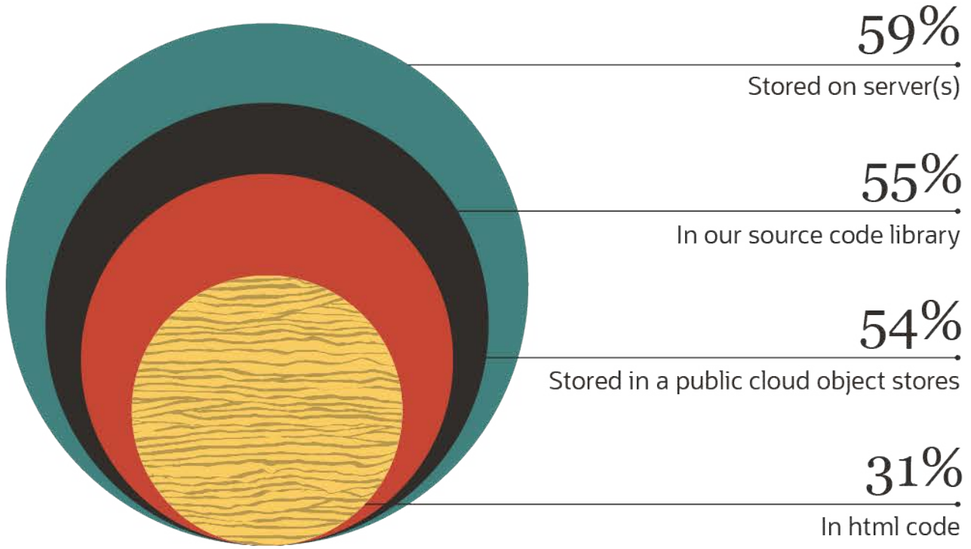
Of the types of misconfigured cloud services reported by our respondents, one is of particular concern: unprotected cloud secrets (i.e., passwords, API keys, encryption keys, and admin and service account credentials). Let's connect a few research dots.

The most commonly cited misconfigured cloud service, over-privileged accounts, is directly related to unprotected cloud secrets. It's clear these credentials are in demand by attackers, per the high percentage of organizations that reported spear phishing attacks designed to steal privileged cloud credentials. Stolen privileged cloud credentials can be used to gain access to additional cloud secrets and, from there, a wide variety of cloud services including data stores such as databases and object stores.

The location of said secrets is clearly part of the problem, with respondents noting that secrets have been discovered in unprotected locations such as:

Of the types of misconfigured cloud services reported by our respondents, one is of particular concern: unprotected cloud secrets (i.e., passwords, API keys, encryption keys, and admin and service account credentials.)

You indicated that your organization discovered unprotected cloud secrets (e.g., passwords, API keys, encryption keys, admin credentials). Where were these secrets located? (Percent of respondents, N=226, multiple responses accepted)



The placement of cloud secrets, sometimes in clear text, in unprotected locations is another byproduct of competing objectives. Dev teams are simply moving fast and not thinking about where they are placing secrets. Best practices to secure cloud secrets include, again, the implementation of least privilege policies and storing secrets in a secure store such as a hardware storage module (HSM) or key vault.

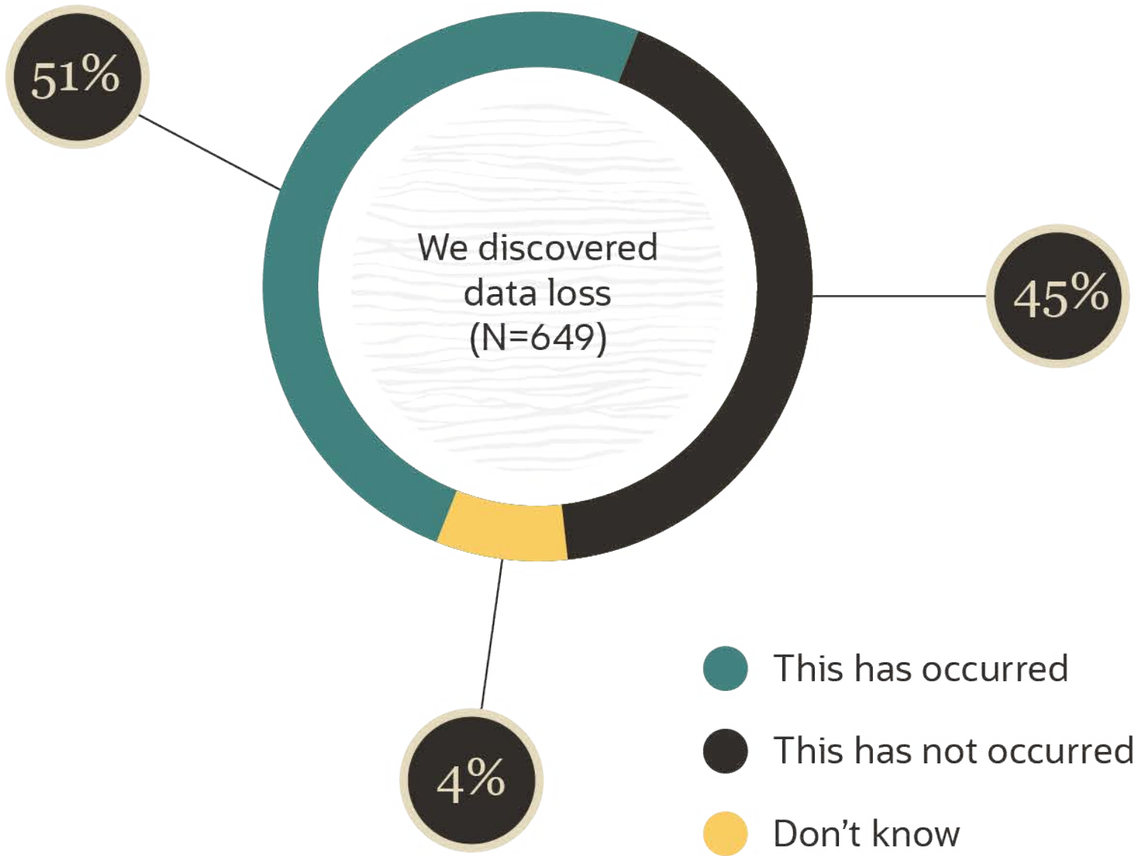
Preview: The Business Impact of the Modern Data Breach

The causes of data loss are many, with an amorphous perimeter created by the use of cloud services representing another egress point for data exfiltration. Our research found that the failure of subscribers to properly secure the configuration of cloud services is an additional contributor to data loss. Tied as a top direct result of misconfigured cloud services, over half of our respondents shared this has caused data loss. In fact, organizations who shared they discovered misconfigured cloud services experienced 10 or more data loss incidents.

Download

Our research found that the failure of subscribers to properly secure the configuration of cloud services is an additional contributor to data loss

Which of the following was a direct result of issues your organization experienced with the misconfiguration of cloud services? (Percent of respondents)



As more data migrates to public cloud stores, such configuration issues will become even more weighty. This year's research shows the trend will continue: Over the next two years, half of the data of our participating organizations will be cloud-resident. The fact that our respondents point to configuration issues as the cause of data loss is encouraging as a measure of self-awareness. It is also abundantly clear that data breaches experienced by other organizations prompt action, per the 79% of businesses that noted that such incidents caused them to increase focus on securing their data.

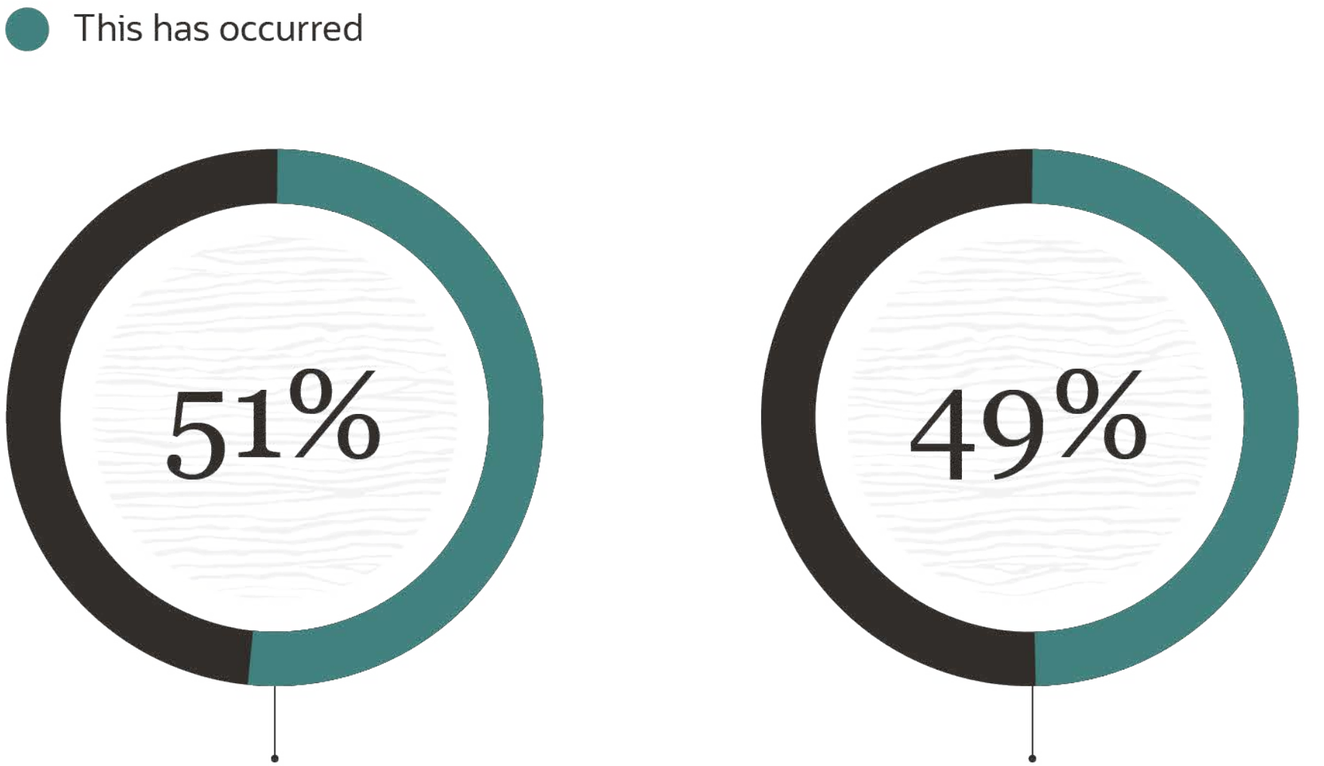
The astoundingly high number of times organizations noted that they have lost public cloud-resident data is highly concerning, and brings up a series of questions: What were the top causes of cloud data loss? What industries have been impacted the most? How have businesses responded, and who, if anyone, was held responsible?

We will explore these questions and more in another upcoming report in the ongoing Cloud Threat Report series, The Business Impact of the Modern Data Breach.

Securing Cloud Configurations Requires a Focus on Identity

Misconfigured cloud services served as a catalyst for many to start retooling their cloud security controls and processes with a focus on securing the human perimeter via stronger identity and access management measures. To that point, the top direct result of misconfigured cloud services, as cited by over half (51%) of our respondents, was the adoption of multi-factor authentication (MFA) for their most critical cloud accounts.

Which of the following was a direct result of issues your organization experienced with the misconfiguration of cloud services? (Percent of respondents)



We need to think of these accounts and credentials as the cloud equivalent of those that provide privileged access to on-premises domain controllers. Given the damage that can be done with unfettered access to privileged cloud credentials as a means to compromise essential cloud services, this year's report has a clear call to action: All cloud accounts that require the use of privileged credentials must be secured via the use of MFA.

How are we doing on the MFA front when it comes to securing critical cloud accounts? Less than half of our participating organizations are using MFA for access to cloud management consoles, DevOps orchestrations tools, and the admin accounts for their SaaS business applications. Also concerning is a modest use of MFA to secure access to source code management (SCM) repositories.

But MFA should really be viewed as table stakes. Fortunately, our survey respondents agree and are doing more to secure the human element than just implementing MFA to lock down access to cloud services. Nearly half of these organizations are also deploying a user entity behavior analytics (UEBA) solution. And these dots connect via adaptive authentication that will issue a secondary challenge in the event that a UEBA solution detects anomalous activity, an approach that should be applied to more than just privileged accounts.

For which of the following types of cloud services and systems does your organization use, or plan to use, multi-factor authentication (MFA)? (Percent of respondents, N=695, multiple responses accepted)

This year's report has a clear call to action: All cloud accounts that require the use of privileged credentials must be secured via the use of MFA.

Cloud Configuration Management via DevSecOps

Dev and Ops Have Come Together, But What About Security?

Integrating Security with DevOps Requires a Cultural Shift

Just as DevOps required a cultural shift that led to a different mindset, culture will be the starting point for integrating security into DevOps processes

Agile software development and DevOps are both based on an iterative approach to continuous improvement predicated on organizational transparency and a collaborative culture. Just as DevOps required a cultural shift that led to a different mindset, culture will be the starting point for integrating security into DevOps processes. As a harbinger for this change that ultimately treats security as a business requirement and a shared responsibility by all members of a project team, let's first look at the state of DevOps adoption.

DevOps is no longer a methodology employed exclusively by cloud-native companies, those less than 10 years old that have never operated their own data center. In fact, our research base of largely enterprise organizations shared that DevOps is being broadly adopted across the board, with only 6% saying their company has no plans to employ DevOps. With nearly one-third of respondents already employing DevOps, almost another quarter planning to do so in the next 12-24 months, and another one-third interested in doing so, it is evident that DevOps is quickly becoming mainstream as the standard approach for how software is built and applications are deployed.

But where does this leave security?

With a similar percentage of businesses now incorporating security into their DevOps processes, it is clear security is emerging as a top DevOps use case, an approach often referred to as "DevSecOps." As a term, DevSecOps has been a controversial topic in the cybersecurity industry. Some view the term as nebulous and in need of a clear definition. Others assume that DevOps already includes security, obviating the need for the term. It is the view of this year's report that until security becomes the cultural norm, DevSecOps serves as a call to action.

Until security becomes the cultural norm, DevSecOps serves as a call to action.

For this year's report, DevSecOps is defined as automating cybersecurity processes and controls via integration with the continuous integration and continuous delivery (CI/CD) toolchain that orchestrates the application lifecycle. As such, a secure DevOps initiative, enabled by a culture to do so, will shift security left into the dev-time and build-time fold via integration with the following:

- Software development lifecycle (SDLC) tools, including interactive development environments (IDEs).
- Source code management (SCM) repositories.
- Automated build tools.
- Agile project management systems.
- Collaborative messaging platforms.

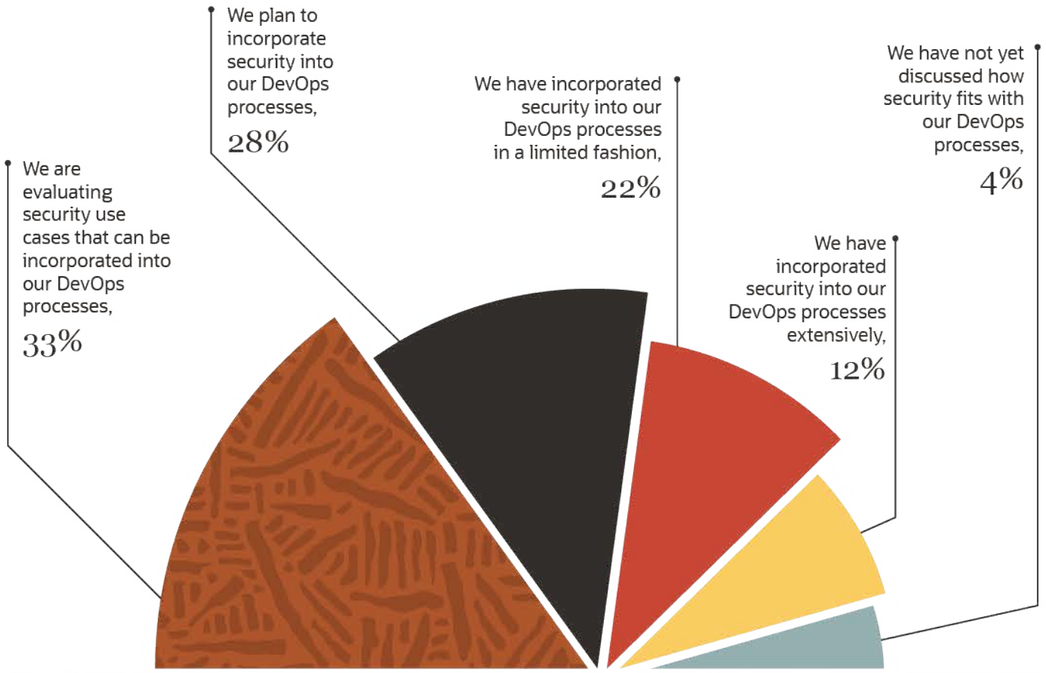
This “shift-left” approach must be augmented with a continued focus on runtime by integrating security controls with the CI/CD tools that orchestrate the delivery of new builds into production. Once again, organizational culture will prove to be a critical success factor, with DevOps teams needing to understand security operations. How? Security operations teams need an audit trail of security events for investigation and response purposes, which will require the use of controls that can capture system activity events on ephemeral cloud instances such as application containers.

This “shift-left” approach must be augmented with a continued focus on runtime by integrating security controls with the CI/CD tools that orchestrate the delivery of new builds into production.

As expected, the DevSecOps journey is a work in progress for our research participants. Just over one-third of respondents whose organization employs, plans to employ, or is interested in employing DevOps noted that their organization has already integrated security into their DevOps processes. What about the other two-thirds? As we saw with DevOps adoption, 28% are already planning to implement DevSecOps measures and another one-third are evaluating security use cases that can be incorporated into their DevOps processes. This is a prime example of where opportunities for establishing a culture of security are being missed from the design phase up.

To support advancing the maturity of secure DevOps programs, current and planned adoption of DevSecOps requires specificity of use cases and repeatability across project teams supported by organizational alignment that treats cybersecurity as a first-class citizen.

To what extent does your organization plan to incorporate security processes and controls via its DevOps processes (i.e., DevSecOps)? (Percent of respondents, N=667)

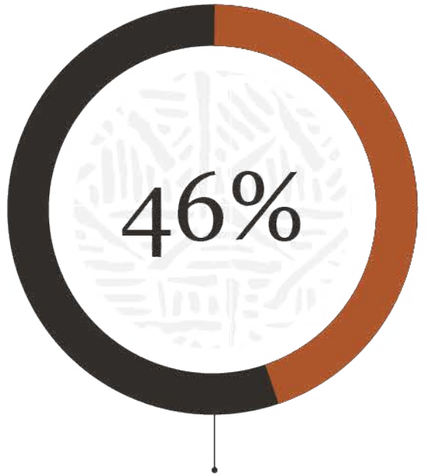


The Need for Automation Is Driving DevSecOps Adoption

In order for security to not get left off the continuous conveyor belt for how software is developed, integrated, and delivered into production, security must be integrated into CI/CD automation. Respondents agree wholeheartedly, as the top reason that organizations are employing or planning to employ DevSecOps is improving security posture by baking security into every stage of their continuous delivery tool chain

As the top reason that organizations are employing or planning to employ DevSecOps is improving security posture by baking security into every stage of their continuous delivery tool chain

What are the primary reasons why your organization employs or plans to employ DevSecOps? (Percent of respondents, N=415, three responses accepted)



46% indicate one of their top drivers for employing DevSecOps in the business is to integrate security controls for continuous integration and delivery tool chain

Other DevSecOps drivers are highly consistent with fundamental DevOps tenets, including:

- **Collaboration:** 40% shared that DevSecOps fosters a high level of collaboration between their development, infrastructure management, application owners, and cybersecurity stakeholders, a pillar of DevOps culture.
- **Efficiency:** 40% noted that DevSecOps allows them to gain greater operational efficiency vis-à-vis automation, always a welcome benefit given resource-challenged cybersecurity teams.

DevSecOps also serves compliance considerations, with over one-third (36%) sharing that DevSecOps allows them to assure that their business meets and maintains compliance with applicable industry regulations.

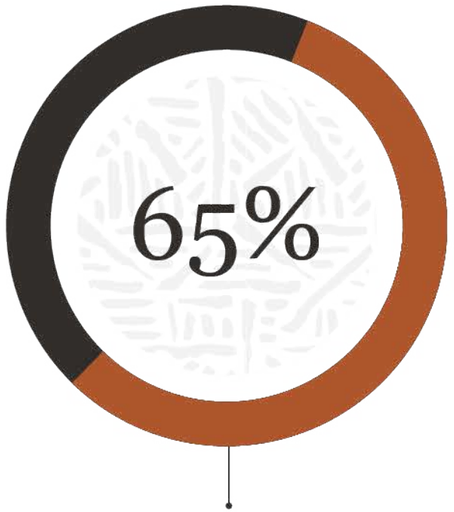
While these represent proactive reasons for integrating security into DevOps processes, some respondents revealed that they do so reactively due to a cybersecurity incident, one which may well have been due to misconfigured cloud services. In fact, respondents are also mindful of how DevSecOps can help address the configuration management challenges discussed previously, with 39% citing they have adopted or plan to adopt DevSecOps to automate updating the configuration of their cloud-resident server workloads.

Spotlight: The Pets versus Cattle of Immutable Infrastructure

The transient nature of cloud-resident workloads is such that they are often treated as immutable. That is, production cloud-resident server workloads are often not updated; they are replaced with new instances based on an updated gold image that may include an operating system update, a patch to an application, new code, configuration update but also hardware root-of-trust to wipe hardware of malicious code. Treating cloud-resident workloads as immutable infrastructure is now commonplace, with nearly two-thirds of this year's research respondents sharing that all or most of their cloud workloads are immutable, with a little more than another one-quarter saying some of their cloud-resident workloads are treated as immutable.

Automating configuration management is nothing short of the requisite approach to updating those server workloads that are immutable.

Does your organization treat its cloud-resident server workloads as immutable infrastructure? (Percent of respondents, N=750)



65% of organizations treat majority of their cloud resident workloads as immutable

The pets versus cattle metaphor has been used to effectively convey the distinction between how on-premises data center servers and cloud-resident workloads are managed. On-premises servers have been treated almost as family pets by being given cute names and nurtured with care and feeding to minimize any impact to their production runtime state. In contrast, immutable production servers are not patched, they are treated as cattle bred for slaughter. That is, the change management approach for immutable infrastructure is tearing down and replacing fleets of server instances via automated orchestration. It is in this context that automating configuration management is nothing short of the requisite approach to updating those server workloads that are immutable.

DevSecOps Automates Securing the Application Lifecycle

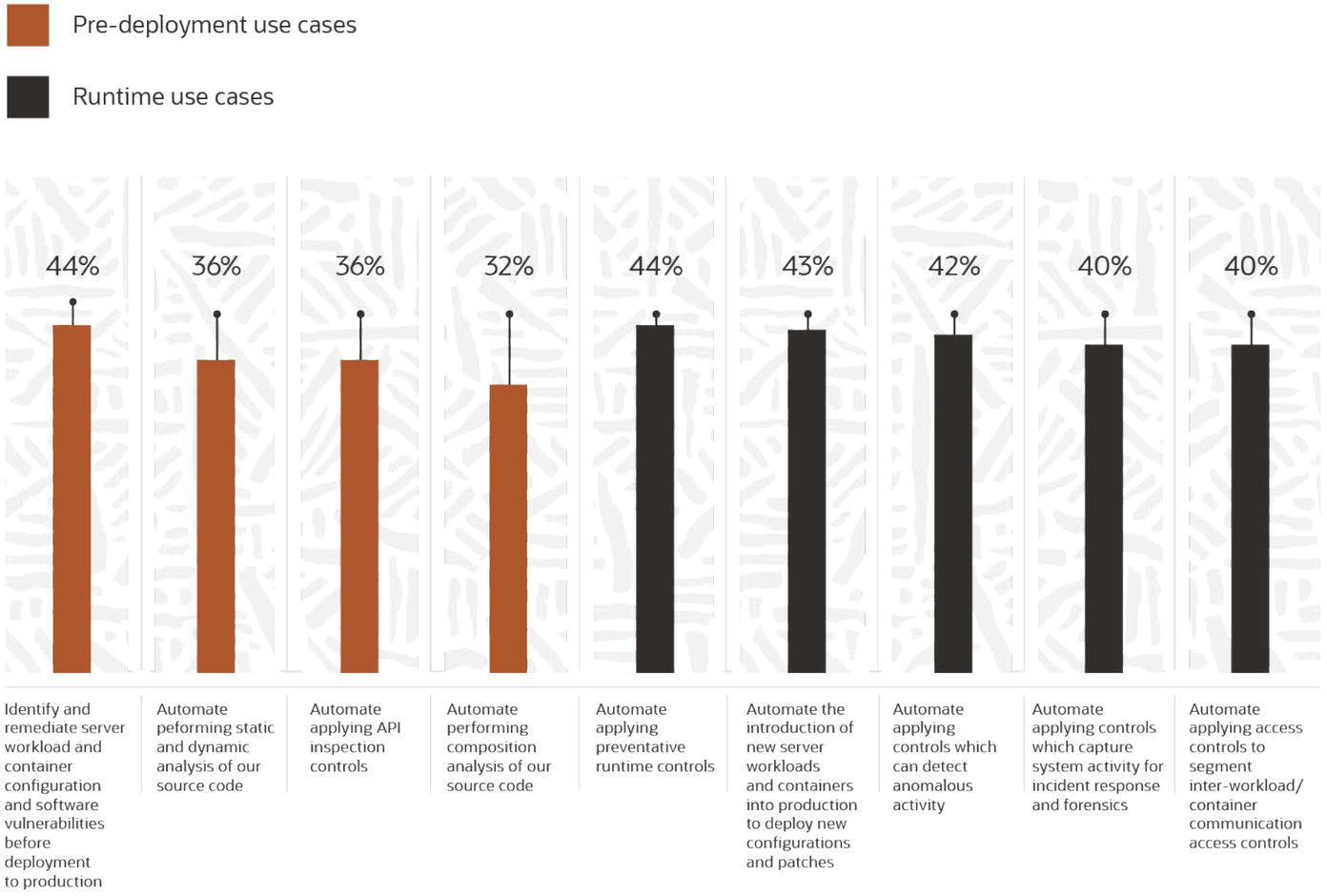
Given that more cloud-resident servers are being treated as immutable, and organizations are taking steps toward full automation, what does the future hold? An impressive 88% of research participants agree that, within the next three years, the majority of their cloud-resident servers will take advantage of intelligent and autonomous patching and updating. In addition to those systems that are truly autonomous, DevSecOps will play a central role in automating and updating cloud-resident servers.

Build-time Use Cases

The most-cited DevSecOps use cases represent threads that connect the central themes discussed in this year's report: a lack of visibility into cloud configurations, the range of misconfigured services, and the pressing need for automation. Toward that end, respondents are tackling configuration management at build-time by automating the identification and remediation of server and container configuration and software vulnerabilities before deployment to production. With hardened images in hand, DevSecOps is then being employed to automate the introduction of new server workloads and containers into production as a means to deploy these new configurations inclusive of patches. Another popular use case is automating the introduction of preventative runtime controls.

The most-cited DevSecOps use cases represent threads that connect the central themes discussed in this year's report: a lack of visibility into cloud configurations, the range of misconfigured services, and the pressing need for automation.

Which of the following best represents how your organization currently employs DevSecOps? (Percent of respondents, N=225, multiple responses accepted)



Runtime Use Cases

For many organizations, a central benefit of infrastructure-as-a-service platforms is seamless auto-scaling in which new server instances are instantiated and decommissioned as the application dynamically requires. In auto-scaling groups in which all members are based on the same gold image, there should be no deviations in runtime behaviors. As such, another compelling DevSecOps use case is automating the deployment of runtime controls that can detect any such deviations from known good system behavior baselines. Other runtime controls include the automated application of controls that segment inter-workload communication for the implementation of a least privileged security model between application tiers.

Dev-time Use Cases

With those build-time and runtime use cases in mind, our respondents are also utilizing DevSecOps at dev-time with various approaches to code analysis. These uses cases include composition analysis that could identify third-party and/or open source software components with known vulnerabilities as well as static and dynamic analysis to identify inadvertently introduced organic vulnerabilities. As is the case with all vulnerabilities, project teams will need to set and adhere to policies on what severity levels warrant remediation and would fail a build if not addressed in the development phase.

Preview: The Mission of the Cloud-centric CISO

Download

The cultural shift that is the prerequisite for leveraging DevSecOps automation to close the cloud security readiness gap will require a fundamentally new approach from cybersecurity leaders. Our research is unequivocal on a few central related organizational dynamics.

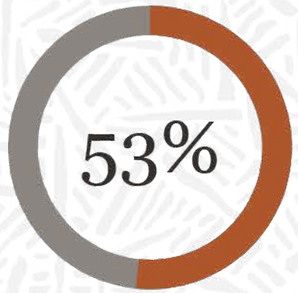
For starters, CISOs too often get involved in public cloud projects reactively, per the 69% who report their CISO got involved in the public cloud initiative after a cybersecurity incident. And two-thirds noted their CISO got in the loop due to a funding request. These research findings are a stark reminder of the disconnect between the lines of business and the cybersecurity team. But there is good news: the advent of the business information security officer (BISO) can help implement a cybersecurity mandate within the lines of business.

A review of BISO job descriptions on job boards reveals a central theme for this role: integrating a security culture into the business. Our respondents concur, with over half noting that the addition of a BISO tasked with collaborating with the CISO was a catalyst for getting the CISO more involved in their cloud projects.

A review of BISO job descriptions on job boards reveals a central theme for this role: integrating a security culture into the business.

Which of the following contributed to your organization's CISO/CSO becoming more involved in public cloud projects over the past 12-24 months? (Percent of respondents, N=370, multiple responses accepted)

Addition of a line-of-business leader/BISO tasked with collaborating with the CISO/CSO

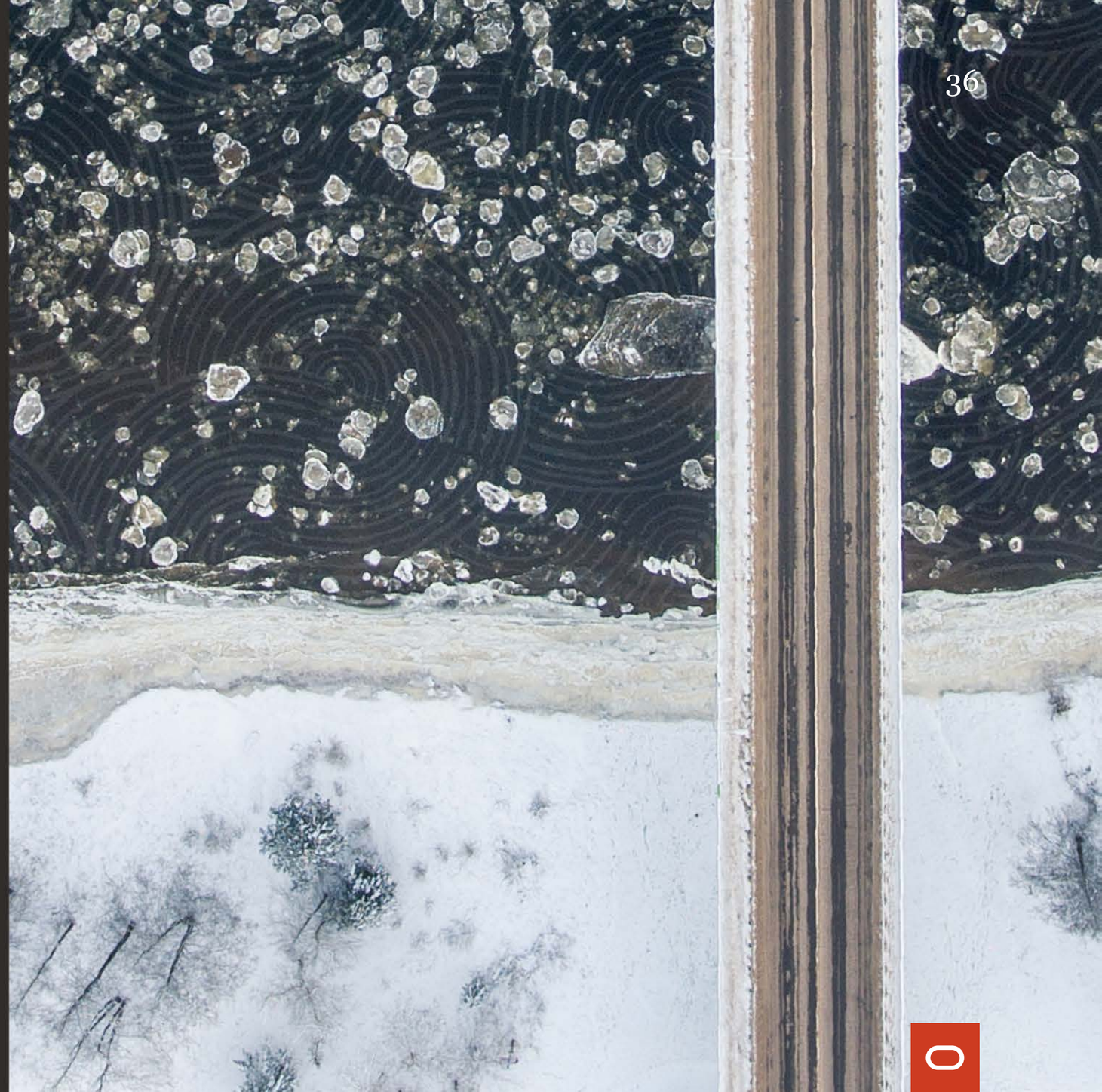


How involved has the CISO truly been in cloud projects? Do organizations feel their CISO adds strategic value such that they would like to see them leaning in more? And what about the impact of the cloud security readiness gap on job security? Are CISOs held accountable for failures in protecting data and privacy? Are organizations hiring cloud-forward CISOs who are more knowledgeable about cloud security?

The evolving role of the CISO is a seminal cloud security topic we will explore in another report in this series, The Mission of the Cloud-centric CISO.

Cyber-attacks and Business Fraud

While Proven Attack Types Persist, Cyber Business Fraud Presents New Challenges

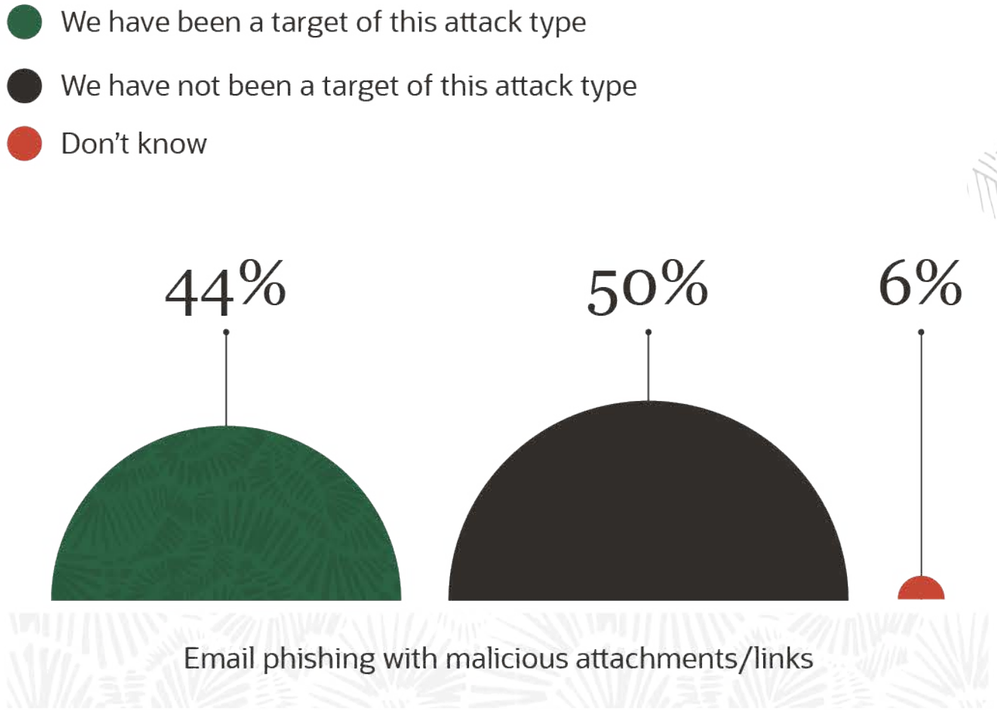


Phishing Targets and Techniques Are Expanding

This year's research reveals new ways in which phishing attacks are being perpetrated to steal a newer set of valuables: privileged cloud credentials

This year's study reveals that tried and true cyber-attacks endure, highlighted by the seemingly never-ending battle with phishing, which, once again, is the cyber-attack type most commonly experienced by research respondents. While the prevalence of phishing as an attack method and vector is well known, new phishing techniques are being employed to achieve new objectives.

Which of the following cybersecurity attacks has your organization been a target of within the last 24 months? (Percent of respondents, N=372)



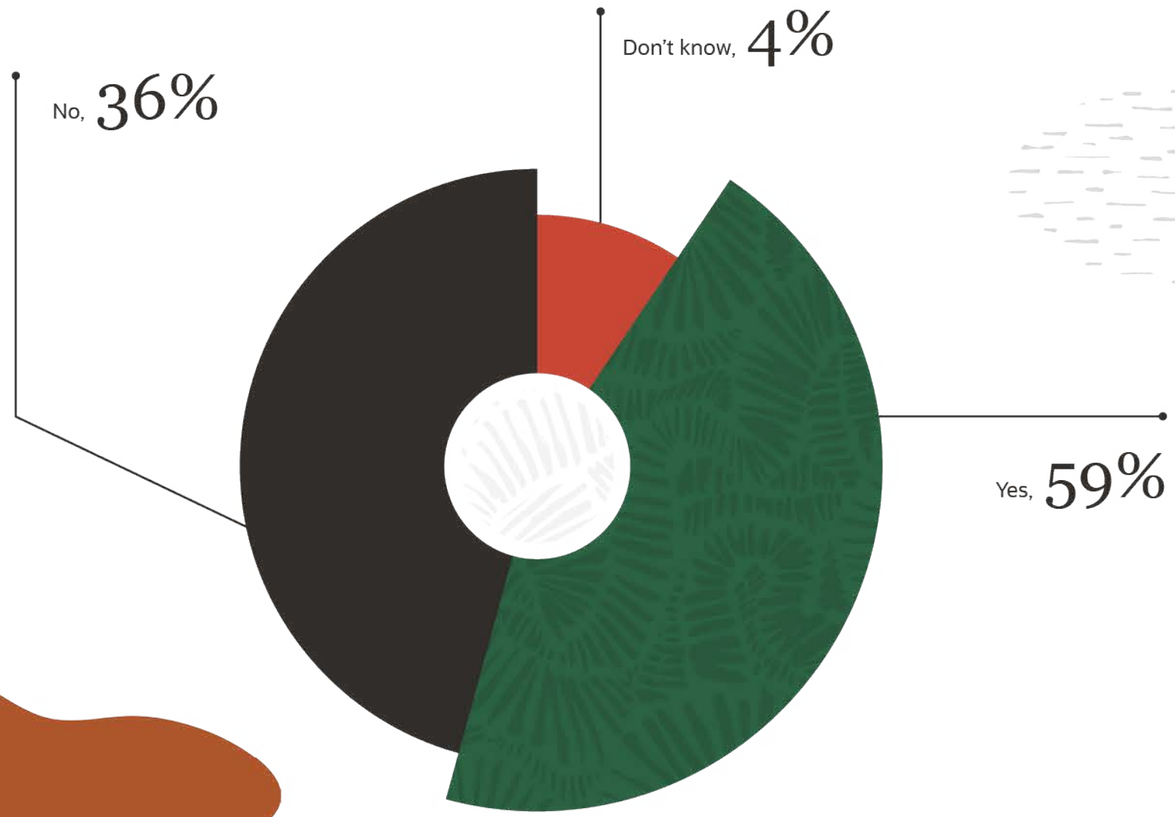
Spotlight: The Phishing of Privileged Cloud Credentials

Criminals are now stealing privileged credentials via targeted phishing to gain access to an organization's critical cloud services as well as the data associated with those services. A key takeaway of this year's cloud threat report is privileged cloud credentials are the new keys to the kingdom. Unfortunately, an astounding 59% of research respondents shared that members of their organization with privileged cloud accounts have had those credentials compromised by a spear phishing attack.

To what end? Those who have been the victim of such spear phishing attacks report data loss as well as fraud and financial loss. Readers should think of privileged cloud credentials as not just those that have admin and critical configuration access to cloud consoles, but also service accounts.

Privileged cloud credentials are the new keys to the kingdom

Have any members of your organization with privileged cloud accounts been compromised by a spear phishing attack designed to steal their cloud credentials? (Percent of respondents, N=236)



A Focus on the Human Perimeter Is Required to Combat Phishing

The ongoing high incident rate of phishing, and the fact that hackers have raised the stakes by going after privileged cloud credentials, warrants revisiting a set of best practices to mitigate the prevalent threat of phishing attacks. This year, in light of the exponential increase of remote workers, we suggest a thematic approach, one focused on securing the human perimeter with a set of must-have modern technologies and hardened processes.

Essential controls include:

- Identity and access management including multi-factor authentication (MFA) for access to critical systems, and adaptive authentication to issue a secondary challenge upon detecting anomalous end-user activity.
- Email security that vets the validity of all aspects of the email from sender to content, attachments, and URLs, including the ability to detect bogus pages designed to steal credentials and take over accounts.
- Next-generation endpoint security controls that detect and prevent both file-based and file-less malware introduced via phishing as well as application control that only allows trusted and approved binaries to execute.
- IT and cybersecurity teams should also consider the following set of proactive measures:
- Adopt identity and access management governance as a framework to review the policies and processes that manage identities and their privileges.
- Continuous red teaming to establish a baseline of successful phishing attacks and to measure progress over time.
- Ongoing end-user awareness training, especially as remote users need to operate securely and independently.

Finally, given the spate of cyber business fraud, IT, cybersecurity, and finance teams should collaborate on reviewing and tightening internal processes for payment processing with an eye toward implementing a new set of checks and balances.

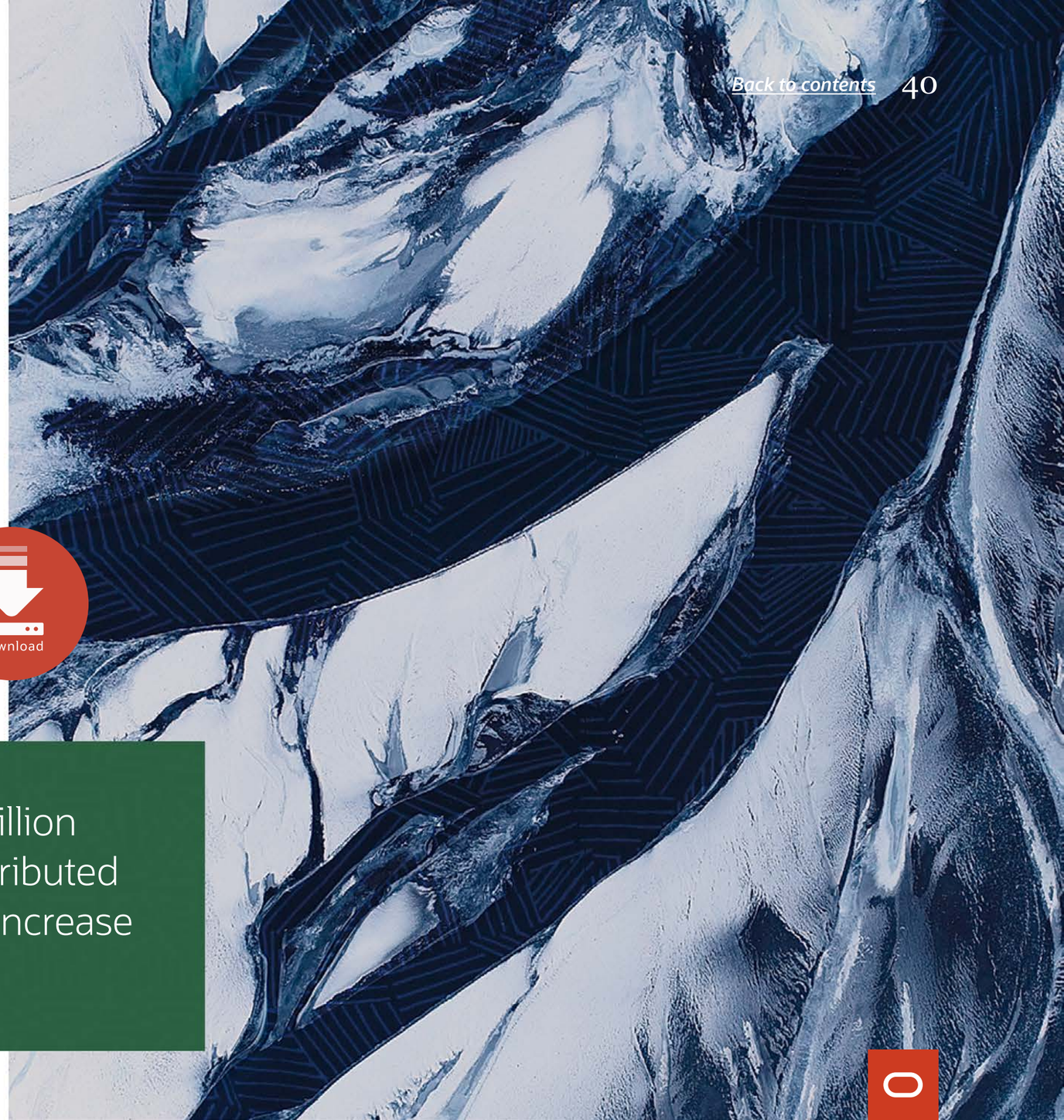
In light of the exponential increase of remote workers, we suggest a thematic approach, one focused on securing the human perimeter with a set of must-have modern technologies and hardened processes

Preview: Addressing Cyber-risk and Fraud in the Cloud

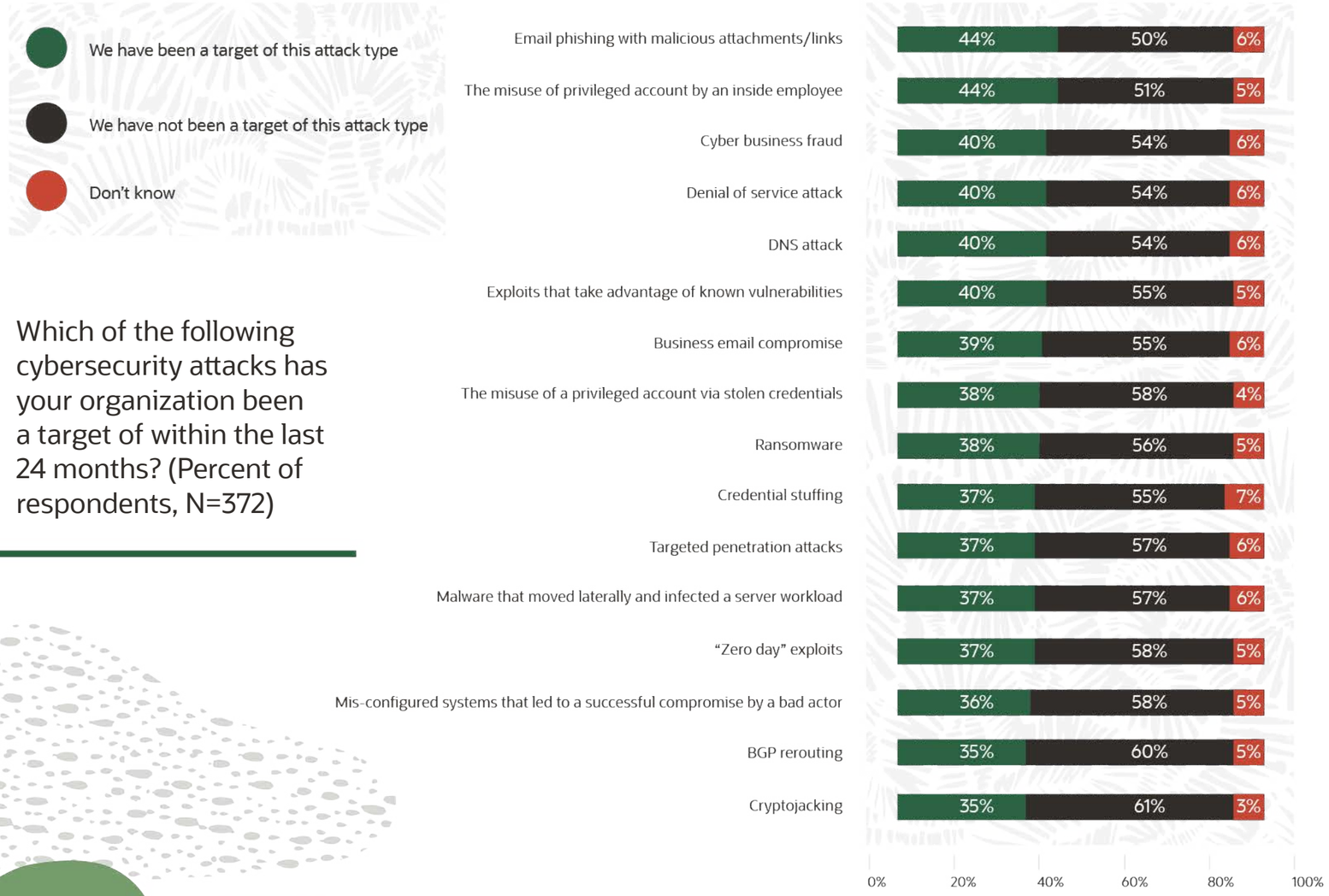
Tracking to the rise of ransomware a few years ago, the incidence rate of business email compromise (BEC) attacks is disconcerting, with 39% of respondents sharing that their business had experienced a BEC attack over the last 24 months. This method of exploiting email to impersonate a sender who instructs a subordinate to process a fraudulent payment is leading to massive financial loss.

Based on statistics shared by the FBI Internet Crime Center (IC3) in its 2019 Internet Crime Report of nearly 500,000 complaints, BEC is clearly good business for cyber-criminals. The report notes that BEC scams conducted in 2019 yielded $1.8 billion to the perpetrators, half of the $3.5 billion attributed to cybercrime and a notable year-over-year increase of a half billion dollars in BEC fraud. And with many BEC cases going unreported, these statistics likely understate the actual financial impact of BEC and other types of cyber fraud.

Download



BEC scams conducted in 2019 yielded $1.8 billion to the perpetrators, half of the $3.5 billion attributed to cybercrime and a notable year-over-year increase of a half billion dollars in BEC fraud.

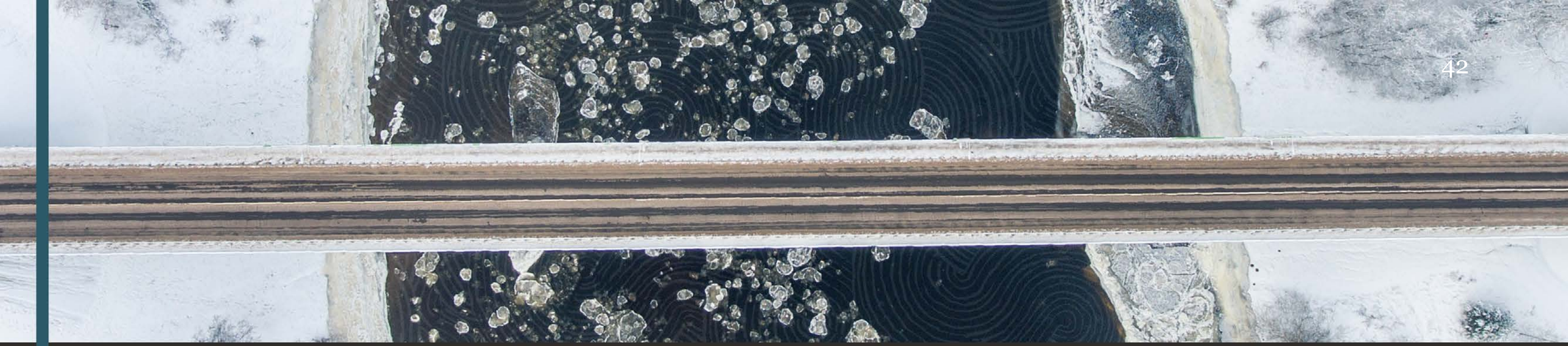


Which of the following cybersecurity attacks has your organization been a target of within the last 24 months? (Percent of respondents, N=372)

While BEC is the type of cyber fraud that gets the most attention, 40% of respondents shared that their organization was the victim of other types of cyber business fraud over the last 24 months. Such attacks include those perpetrated by insiders for personal financial gain.

But what level of risk has the broad adoption of cloud services, specifically SaaS applications, introduced by creating new means by which cyber-criminals and malicious insiders conduct fraud? How is identity fraud conducted via account takeover (ATO) attacks and bogus SaaS login pages? And how are improperly secured SaaS applications, such as those with overprovisioned access and a lack of segregation of duties, exposing businesses to various forms of cyber fraud?

These are some of the issues that will be discussed in greater depth in the upcoming report, Addressing Cyber-risk and Fraud in the Cloud, part of the ongoing Cloud Threat Report series.



The High Expectations of Machine Learning

Artificial Intelligence (AI) and Machine Learning (ML) Have Emerged as Foundational Cybersecurity Technologies

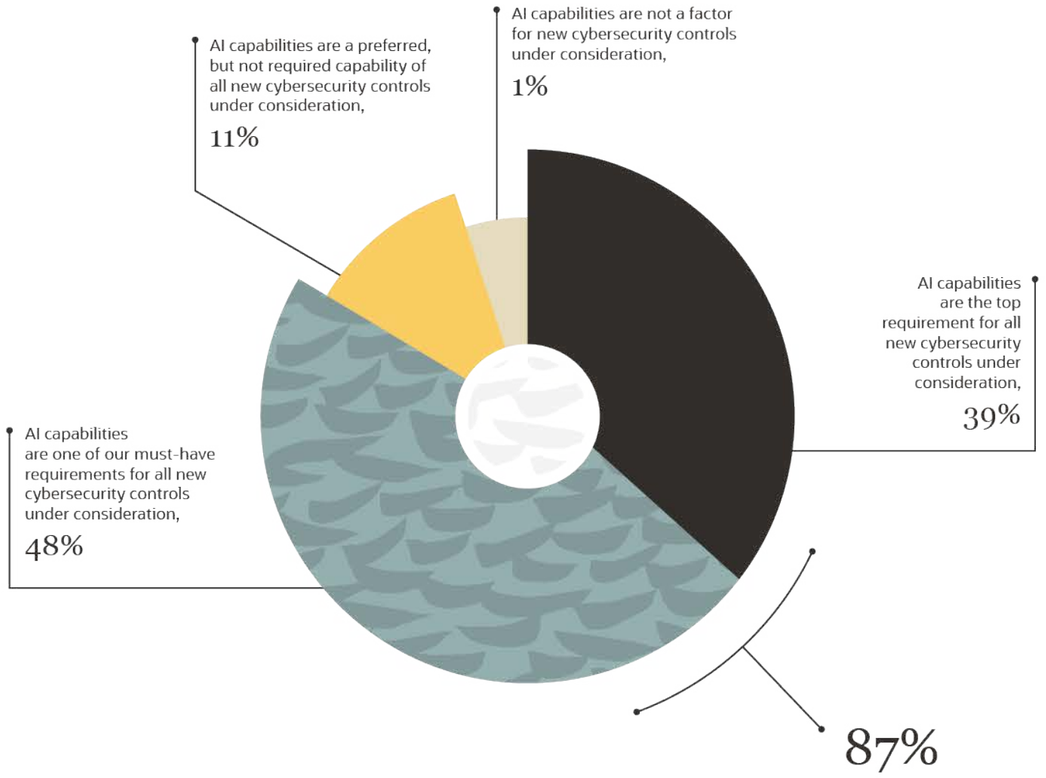
AI/ML Are Core Product Requirements

Prior Oracle and KPMG Cloud Threat Reports positioned machine learning (ML), an application of artificial intelligence (AI), as a technology on the fast approaching horizon. Fast indeed: AI/ML are now dramatically impacting purchasing decisions and being relied upon for a variety of use cases.

Nearly all cybersecurity vendors now cite the use of some form of machine learning in their products as a means to protect against zero-day threats and malicious behaviors that evade more traditional forms of detection. But just how do buyers view the relative importance of cybersecurity controls that utilize AI/ML? When it comes to AI as a driver for selecting cybersecurity controls, there is no ambiguity: AI/ML use is a priority, with nearly 9 out of 10 of our participants citing the technology as a fundamental requirement.

AI/ML are now dramatically impacting purchasing decisions and being relied upon for a variety of use cases

How much priority does your organization place on the use of artificial intelligence (AI) capabilities in cybersecurity controls your company is considering purchasing? (Percent of respondents, N=206)



The extensive use of cloud services, as explored in this report, only adds to the level of noise in which security analysts are looking for a high fidelity signal

Spending intentions reflect this sentiment. When asked what areas of their cybersecurity budget will increase the most over the next 12-18 months, AI took the top spot, with 32% citing cybersecurity technology that employs AI as the top area of incremental investment.[6]

The reasons AI/ML have emerged as foundational cybersecurity technologies are grounded in the challenges cybersecurity teams face on a daily basis. In addition to leveraging AI/ML to detect, and thus prevent, new and unknown threats (e.g., new malware variants, exploits, or phishing tactics), growing streams of event telemetry are flooding security operations centers (SOCs). The extensive use of cloud services, as explored in this report, only adds to the level of noise in which security analysts are looking for a high fidelity signal. It is no wonder, then, that the expectations for applicability of AI/ML are high and the potential use cases are many.

[6]Source: ESG Research Report, 2020 Technology Spending Intentions Survey, February 2020.

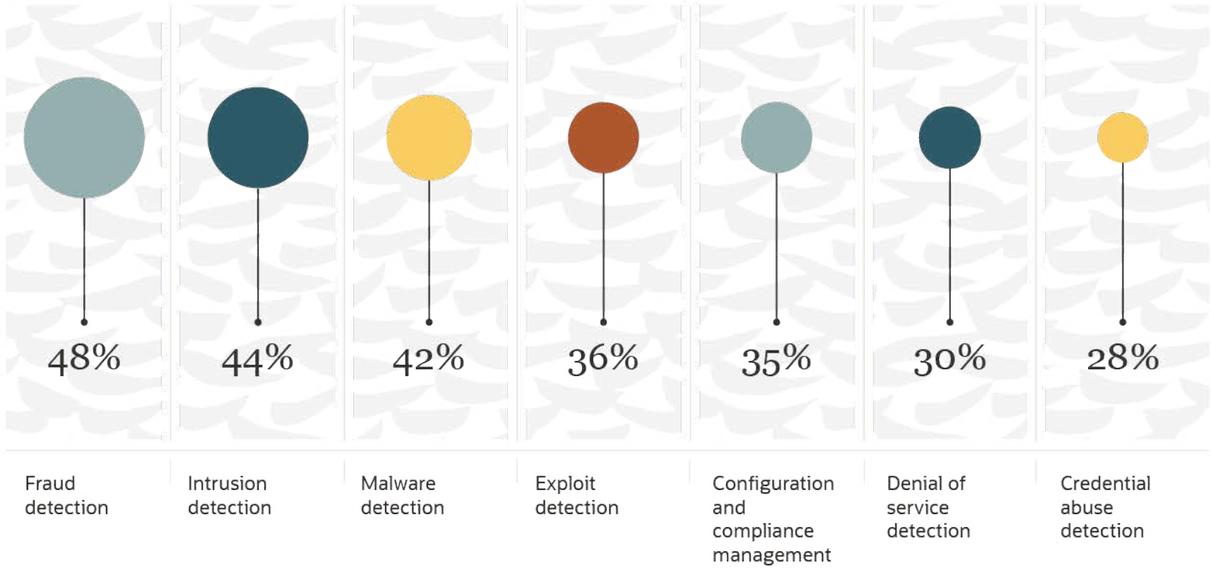
AI/ML Are Viewed as Applicable for a Range of Cybersecurity Use Cases

The range of use cases that is driving demand for cybersecurity solutions that utilize AI/ML has clearly expanded from the beachhead application of the technology to applying machine learning algorithms trained on large collections of binaries to detect new and unknown malware. An expanded set of use cases cited by our research respondents reveals an expectation that AI will prove effective for detecting a range of threats beyond malware. Those detection use cases run the gamut of attack types, with fraud clearly top of mind followed by intrusions, malware, exploits, denial of service, and credential abuse.

Planned AI/ML use cases are not limited to detection, with over a third of the respondents noting they view the technology as having a role in addressing the configuration management challenges cited in this year's Oracle and KPMG Cloud Threat Report. And furthering the expanded set of use cases, nearly half (48%) of respondents view AI/ML as playing a much broader role in the SOC.

An expanded set of use cases cited by our research respondents reveals an expectation that AI will prove effective for detecting a range of threats beyond malware

For which of the following cybersecurity use cases will your organization employ artificial intelligence within the next 24 months? (Percent of respondents, N=202, three responses accepted)



There Is Overly Exuberant Confidence in the Efficacy of AI/ML Cybersecurity Use Cases

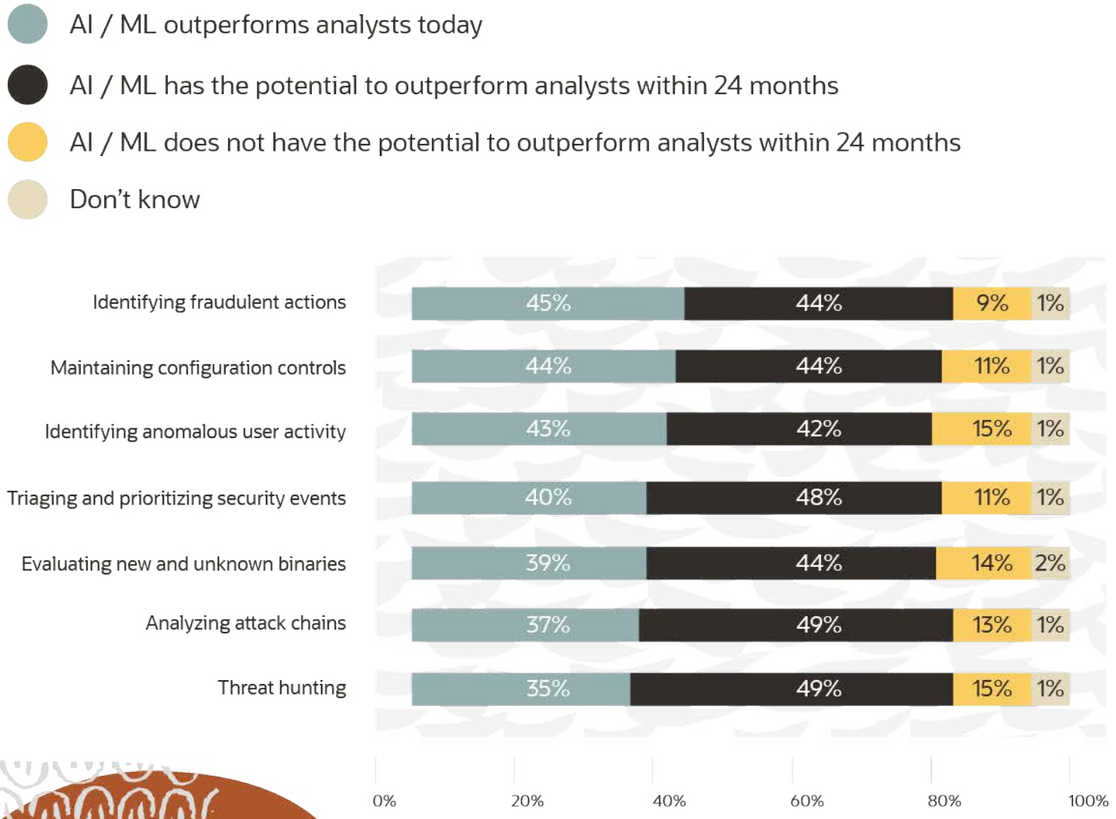
The view of artificial intelligence and machine learning as highly applicable for such a broad range of use cases makes one wonder whether AI can help alleviate the ongoing shortage of cybersecurity skills. The shortage of cybersecurity skills continues to be an acute issue, with 44% of organizations sharing that cybersecurity is, once again, one of the areas in which their company has the most problematic shortage of IT skills.[7] In this context, the question is: Does AI have the potential to outperform cybersecurity analysts staffing the SOC?

When asked whether AI has such potential, respondents were bullish, and arguably overly exuberant about the current ability and future potential of AI-powered technologies to outdo cybersecurity analysts. In fact, 40-45% feel confident that AI can do a better job than their security analysts in:

- Identifying fraudulent actions.
- Maintaining configuration controls.
- Identifying anomalous user activity.
- Triaging and prioritizing security events.

[7]Source: ESG Research Report, 2020 Technology Spending Intentions Survey, February 2020.

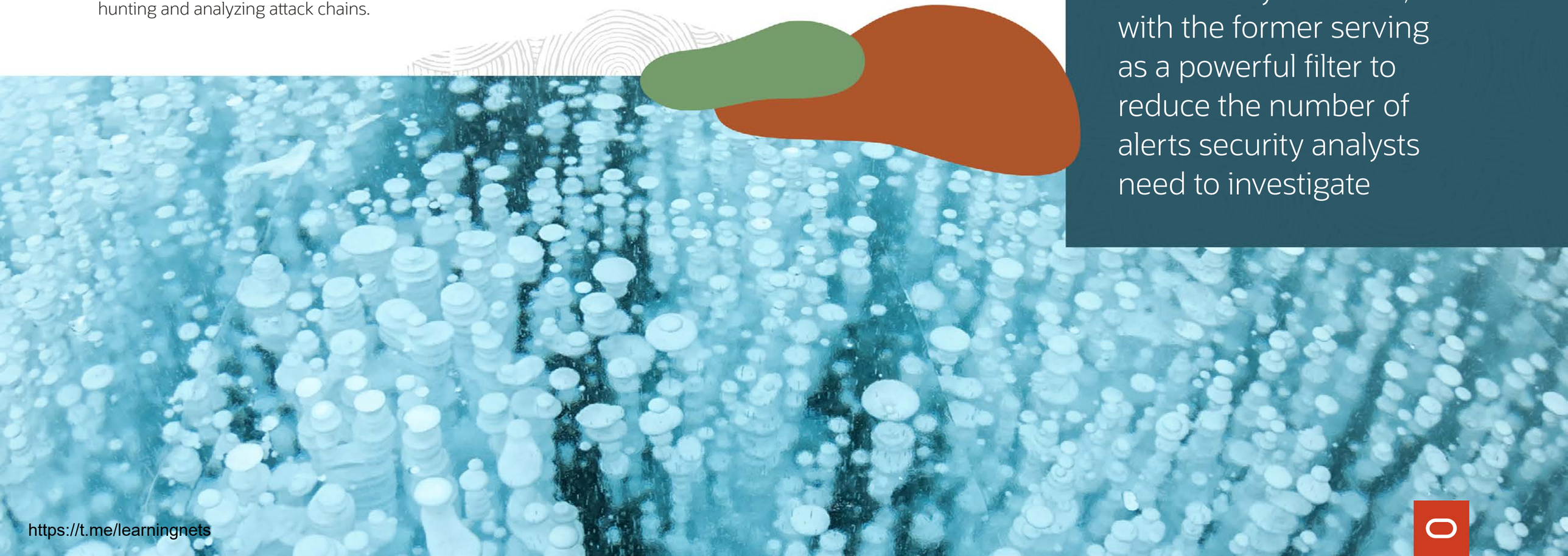
Which of the following tasks do you feel artificial intelligence can perform more effectively than your organization's cybersecurity analysts? (Percent of respondents, N=350)

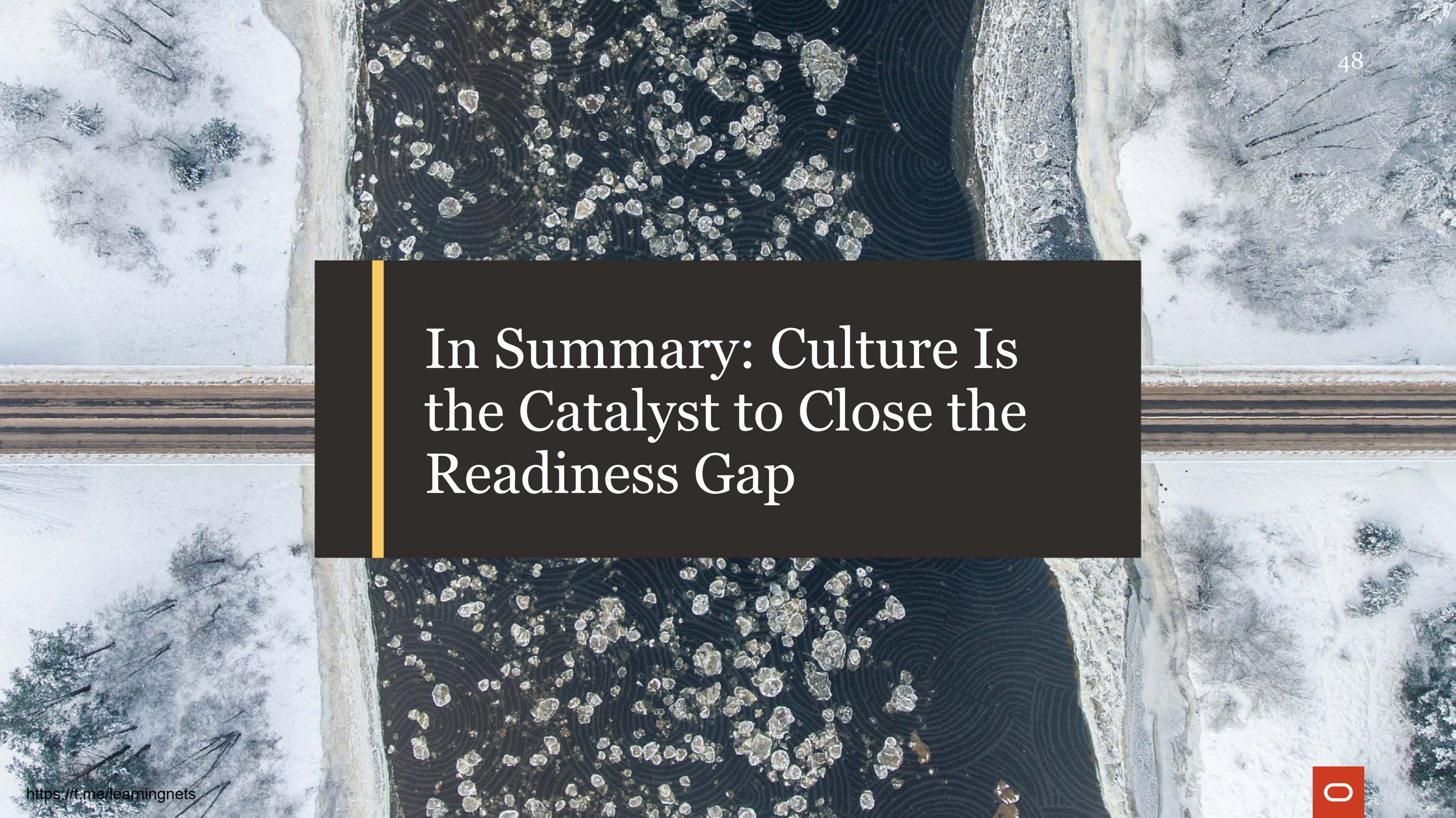


Of these applications of AI, the confidence in AI to triage and prioritize security events better than an analyst seems ambitious at best. Triaging and prioritizing security events requires context with respect to the risk profile of the asset potentially being compromised and how the attributes of an in-flight attack could compromise those assets. That is, automating the detection of adversarial activity relative to an organizational specific threat model is aspirational, if not an unrealistically high bar for the current state of AI/ML. Nonetheless, moving forward, respondents are confident in AI outperforming analysts for threat hunting and analyzing attack chains.

But it is reasonable to look to AI/ML to help with the issue of scale. There are simply not enough analysts to triage alerts. AI and humans will not be mutually exclusive, with the former serving as a powerful filter to reduce the number of alerts security analysts need to investigate. The result of more pragmatic applications of AI/ML will be improved, efficient investigations that deliver the business outcomes that all cybersecurity teams strive for: preventing incidents from becoming breaches, maintaining availability of services, and more.

AI and humans will not be mutually exclusive, with the former serving as a powerful filter to reduce the number of alerts security analysts need to investigate





In Summary: Culture Is the Catalyst to Close the Readiness Gap

Security has all too often been viewed as a tax on the business and awkwardly but quite literally bolted on to projects already in production. The alarming cloud security readiness gap exposed in this year's report reveals that today's line-of-business-driven consumption of cloud services threatens to leave security considerations even further behind. The incessant cycle of phishing, malware, increasing cyber fraud, and a range of misconfigured cloud services further stretch already challenged cybersecurity programs.

The cloud security imperative of merging the parallel agendas of leveraging the cloud services for business agility and managing the associated risk can be accomplished by focusing on a few critical initiatives.

This year's report explored many important topics while saving other equally critical issues for exploration in future reports that will be published over the course of 2020. We conclude this year's first in a series of Oracle and KPMG Cloud Threat Reports by offering a theme for all of the reports: culture. It is essential that we share best practices, learnings, and tips with one another to help all organizations secure their journey to the cloud by addressing tactical issues, such as cloud configuration management, with a security-first culture.

Be a catalyst to bring about cultural change within your organization so that the use of cloud services and applications is not at odds with cybersecurity objectives.

Become an expert on the cloud security shared responsibility model to eliminate any ambiguity on how you and your cloud services providers divide securing your company's portfolio of cloud services.

Leverage DevSecOps automation as a means to implement repeatable cloud configuration management best practices to secure the entire lifecycle of cloud applications.

Get savvy on cyber business fraud to better secure what will be an expanded use of SaaS applications in all areas of your business.

Appendix

Research Methodology

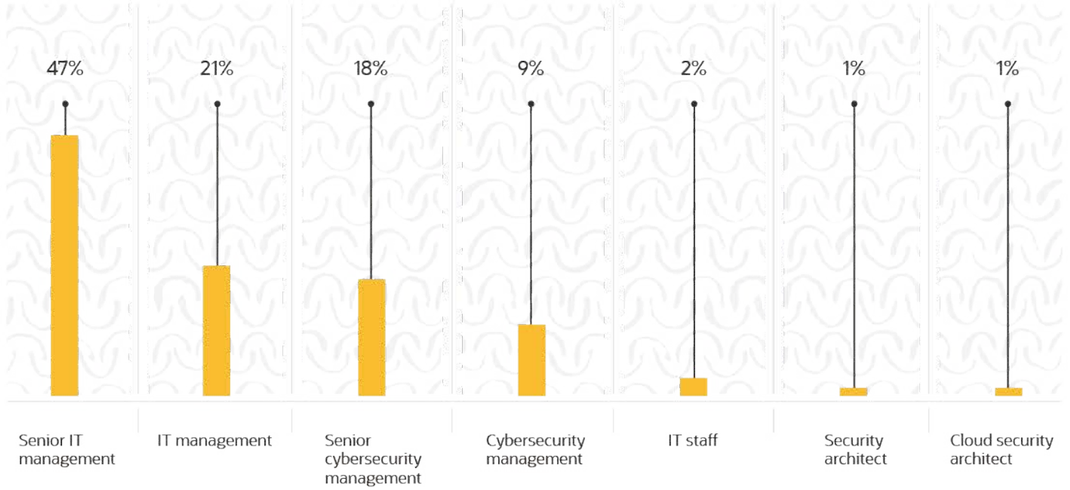
The data presented in this report was collected via a broad online survey conducted by Enterprise Strategy Group of 750 cybersecurity and IT professionals from private- and public-sector organizations in North America (US and Canada), Western Europe (UK and France), and Asia-Pacific (Australia, Japan, and Singapore) between December 16, 2019 and January 16, 2020. 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.

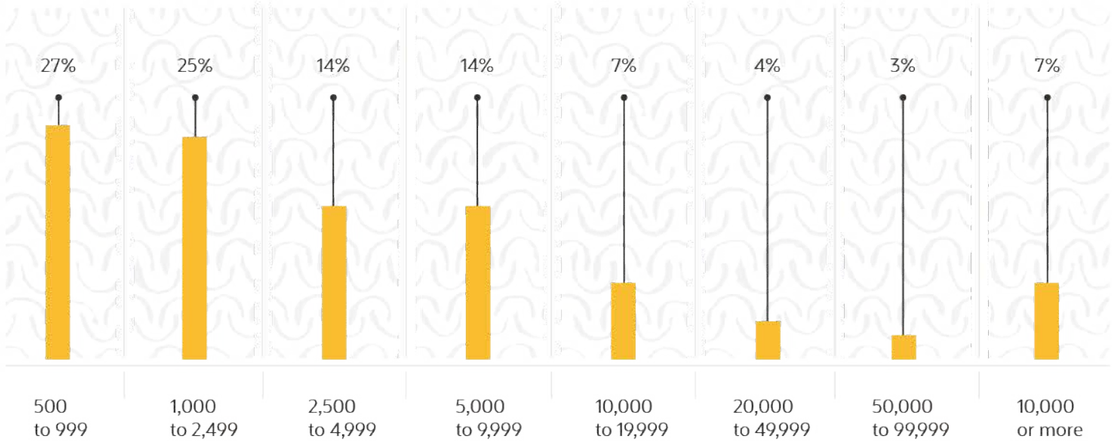
Participant Demographics

The following figures detail the demographics of the respondent organizations.

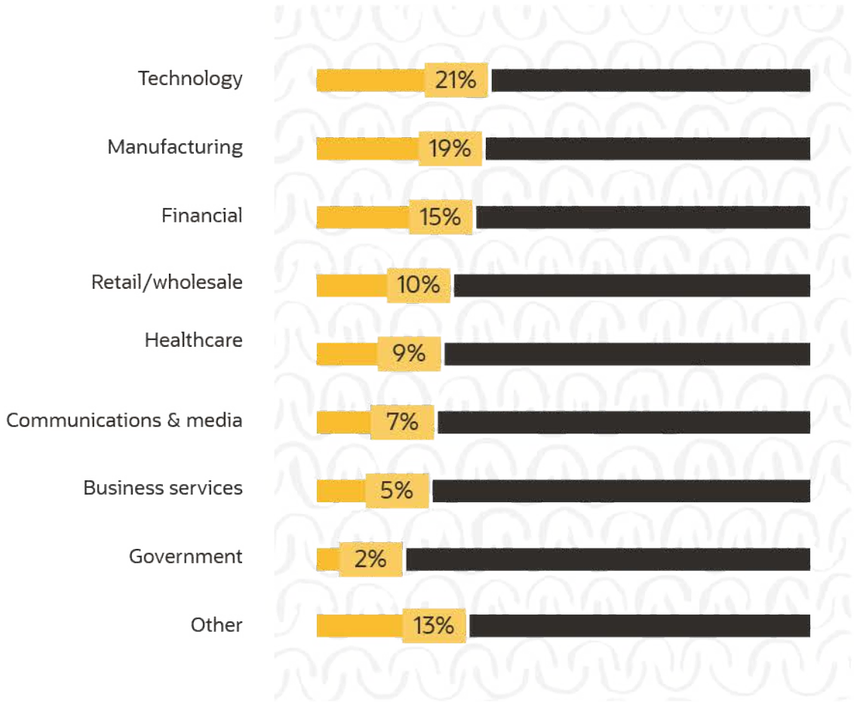
Which of the following best describes your current responsibility within your organization? (Percent of respondents, N=750)



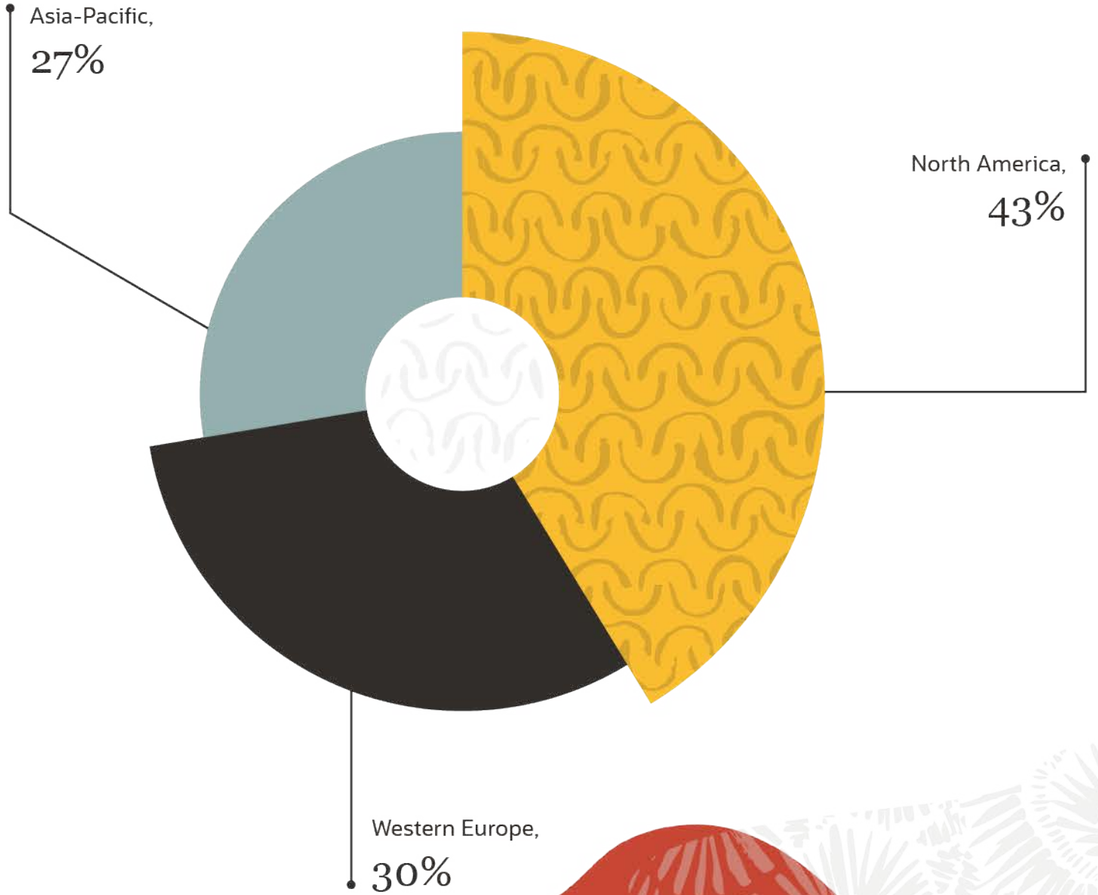
How many total employees does your organization have worldwide? (Percent of respondents, N=750)



What is your organization's primary industry?
(Percent of respondents, N=750)



Respondents by region. (Percent of respondents, N=750)



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

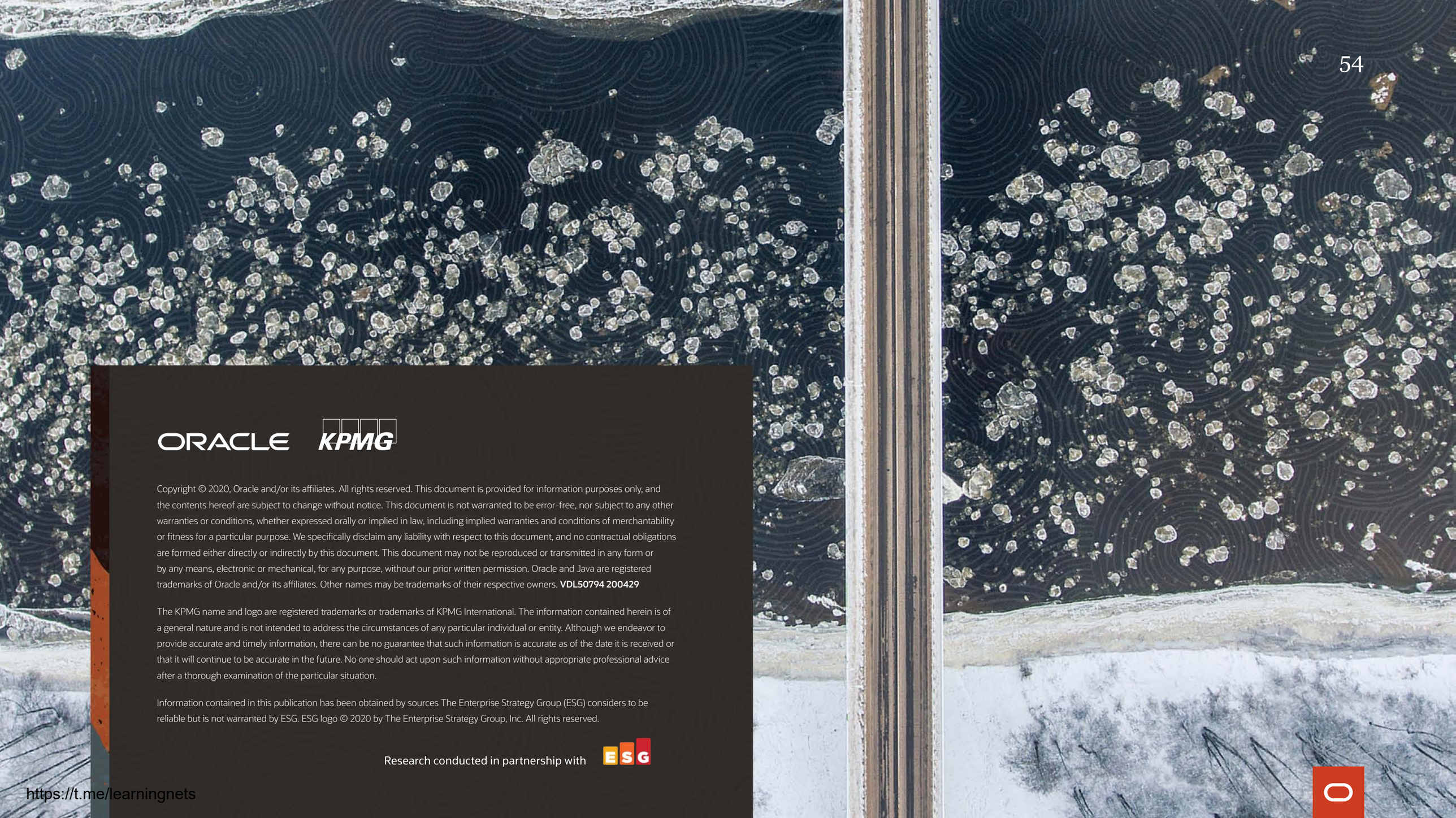
Brian Jensen
Managing Director – KPMG LLP

Doug Cahill
Vice President & Group Director – Enterprise Strategy Group

Jon Oltsik
Senior Principal Analyst – Enterprise Strategy Group

Special Thanks:

Mike Beaudet, Fred Kost, Steve Daheb, Ariel Kelman, Adam Demattia, Mary Beth McCombs, Jennifer Gahm, John Hodson, Tristana Flores, Darren Calmen, Johnnie Konstantas, Taylor Lewis, David B Cross, Graham Hardt, Dan Koloski, Richard Evans, Simon Jones, Nicole Maloney, Travis Anderson, Eric Maurice, Steve Enevold, Maywun Wong, Sean T Cahill, Miles McAlister, Genissa Ross, John Grady, Alan Zeichick, WaiSau Sit and Sami Munassar.



ORACLE KPMG

Research conducted in partnership with ESG