ORACLE

KPMG

ORACLE AND KPMG CLOUD THREAT REPORT, 2018

Keeping Pace at Scale: The Impact of the Cloud-enabled Workplace on Cybersecurity Strategies

A unique research-based view of the cybersecurity challenges and solutions born out of the broad adoption of cloud services.

CONTENTS

Foreword

Mary Ann Davidson, CSO, Oracle Corporation

There is an expression that "everything old is new again," and so it is with information technology (IT). My collegiate experience with IT included having the computer department at my university run programs (punch card decks) for students "as a service" (and one's "subscription" was severely limited each semester). Computers later became "personal" and not only accessible by the masses but a core backbone of almost every type of enterprise, even ones we don't think of as being IT-focused (e.g., agriculture).

Today, the challenge to organizations of managing their many critical IT assets—including finding enough IT talent—has led to the explosive growth of cloud services: everything from infrastructure-as-a-service (IaaS) to platform-as-a-service (PaaS), to fully-managed software-as-a-service (SaaS), the critical applications used by organizations. Most of us know instinctively the value of a service offering: we do not build our own houses, maintain our own cars, or participate in "do-it-yourself dental work." Instead, we find experts in those areas who can do more, with fewer resources, faster and at a better price point than we could provide ourselves. IT is merely a relative, if very large, latecomer to service delivery vehicles.

Organizations embracing cloud services benefit from the ability to uptake the latest and greatest technology instead of being bogged down by maintaining out-of-date, not-yet-capitalized equipment (some of which may be past its end of life). Furthermore, their IT-savvy resources can be used on innovation rather than up and down lifting. Innovation is in many cases directly enabled by cloud services with flexible, scalable workloads (you can "rent" the extra capacity you need), provisioning of highly proficient data analytics, and the ability of machines to draw inferences that mere mortals cannot. Cloud service adoption has moved from tentative, toe-in-the-digital-water trials to managing mission-critical data in the cloud, as many cloud adopters now believe putting such data in the cloud may make it both easier to secure and ultimately be a more secure organization. After all, is it easier for 5,000 customers to each test and apply a patch that addresses a critical security vulnerability—when they can get to it—or for a cloud provider to patch a service used by 5,000 customers? To delve into these topics, Oracle and KPMG partnered with the Enterprise Strategy Group to conduct the research study that serves as the foundation for this report.

The dazzling insights in the *Oracle and KPMG Cloud Threat Report, 2018* come not from professional pundits, but from troops in the trenches: security professionals and decision makers who have dealt with the security challenges of their own organizations and who are increasingly moving critical applications to the cloud. The respondents come from all over the map geographically and industry-wise, including manufacturing, health care, media, retail, and government (federal, state, and local). The majority of the respondents noted that they put sensitive data in the cloud and many respondents thought cloud security was as good as—or better than—on-premises security. Respondents also noted that cybersecurity leadership roles in their organizations continue to manage a significant number of best-of-breed solutions and tools to secure their area of the organization. Almost a third of respondents are already using machine learning, even if in a limited capacity. (Another benefit of cloud: not only "do it faster and better, but increasingly and systemically better.")

Organizations are experiencing exploits targeting known vulnerabilities in unpatched applications—a trend that is only likely to grow as hackers increase their ability to reverse engineer fixes and share exploit code with automated delivery mechanisms. Realistically, given the scope of patches released on a weekly basis, most organizations cannot patch everything they need to, much less do it fast enough. Cloud providers, with greater automation and the ability of DevOps to integrate new/improved components rapidly, can more quickly close the gap between vulnerability discovery, patch production, and patch application.

Increasing regulatory pressures add to the push to cloud. Most respondents indicated that one or more regulatory frameworks are applicable to their organizations, many if not all of which have ratcheted up security requirements. Among these are long-standing regulations such as the Payment Card Industry (PCI) Data Security Standard (DSS), Gramm-Leach-Bliley, Sarbanes-Oxley, and the Health Insurance Portability and Accountability Act (HIPAA). To these we can now add the impending European Union General Data Protection Regulation (GDPR), which many respondents noted affects their organizations.

In the age of social media, it is popular to speak of what's "trending." What we are seeing is not a trend, but a strategic shift: the cloud as an enabler of security.

Executive Summary

Cloud computing truly is a fundamental paradigm shift that is disrupting established markets and challenging established brands to move faster to realize competitive advantages, if not to simply maintain competitive parity. The broad adoption of cloud services, coupled with knowledge worker mobility, has created a new set of cybersecurity challenges. The agility of the cloud has created a strategic imperative to keep pace at scale. As organizations scale their infrastructure, applications, and users, the security requirements are lagging and further challenged to scale at the same rate. We'll discuss the implications of the cloud-enabled workplace on cybersecurity priorities by exploring the following key findings of the *Oracle and KPMG Cloud Threat Report, 2018:*

- **Cloud usage continues unabated.** Cloud-first initiatives and an increasing level of confidence in the security posture of public cloud environments have fueled the broad adoption of cloud services, resulting in an appreciable portion of an organization's sensitive data now being cloud-resident.
- **The threat landscape is increasingly complex and varied.** A range of threats, headlined by phishing, malware, and exploits, have been broadly experienced, with these and other threats such as business email compromises being top-of-mind concerns moving forward.
- **Detection and response is critical—but not always easy in the cloud.** Customers cite detecting and reacting to threats in the cloud as their top cybersecurity challenge. This creates a cloud "visibility gap" that customers must address.
- **Customers don't always understand their cloud security obligations.** Confusion about the interpretation of the shared responsibility security model poses a risk to securing cloud infrastructure and applications as customers are often not clear where their provider's role ends and theirs starts, creating gaps.
- **Security professionals worry about the impact of attacks on business operations.** While cybersecurity attacks result in financial loss, the top-cited impact is on business operations, including the ability to deliver core services.
- **Cloud and mobile-centric employees beget the need for new identity and access management strategies.** Knowledge worker mobility and the use of cloud-delivered applications have made identity management at scale a challenge, with aligning roles and permissions a strategic imperative.
- **Technology alone isn't enough.** Organizations are funding retooling initiatives to secure the use of cloud applications and infrastructure with a set of best practices that focuses on people, processes, and technologies.
- **Machine learning can help.** Emerging technologies such as machine learning and security automation promise to improve the efficacy of detecting and preventing threats, as well as the operational efficiency with which cloud-enabled workplaces are secured.

Key Research Findings

90%
of firms say at least half of their cloud data is sensitive information

41%
of companies say they have a dedicated cloud security architect

66%
of companies have suffered a significant business operations interruption in the past 24 months

38%
report issues detecting and responding to cloud security incidents, making this the most cited cybersecurity challenge in this survey

82%
of cyber leaders are concerned that employees do not follow cloud security policies

95%
of firms affected by GDPR report that it will impact their cloud strategies and service provider choices

47%
of organizations are using machine learning (ML) technologies for cybersecurity purposes

84%
of companies are committed to increased levels of security automation

> **many organizations are faced with the need to close the gap between their organization's use of the cloud and their readiness to secure a growing cloud footprint…"**

We are now moving past security concerns about the cloud being an impediment to the use of cloud services, but appreciable risk remains. Lines of business have not only demanded the agility the cloud provides, but very often consume cloud services without the involvement, never mind approval, of the corporate IT and cybersecurity teams. This manifestation of shadow IT, which bypasses cybersecurity policies and processes, clearly threatens corporate cybersecurity strategies. As a result, many organizations are faced with the need to close the gap between their organization's use of the cloud and their readiness to secure a growing cloud footprint, requiring a retooling of people, processes, and technologies. Participants in our study appreciate that closing the cloud security gap will require investments, with 89% of respondents expecting their organization will increase cybersecurity spending in the next fiscal year, and 44% of them anticipating a rise of 7% or more. And according to research conducted by ESG, cloud infrastructure security and cloud application security are two areas in which 43%[1] of organizations expect to make the most significant cybersecurity investments in 2018.

While this report focuses on these important considerations of securing an increasingly cloud-centric data center, it is important to note, and be mindful of the fact, that tried and true IT systems such as on-premises client-server architected applications are still serving business-critical functions. Because today's modern technology ecosystem is comprised of disparate infrastructures that span generations of computing technologies and practices, a holistic approach to security is required.

[1] Source: ESG Master Survey Results, *2018 IT Spending Intentions Survey*, December 2017.

Back to Contents

KPMG Perspective: A Cloud Security Call to Action

The cloud can be secured—but not by the vendor alone. Do you, the business leader, know your responsibilities and risks?

Tony Buffomante, Cyber Security Services U.S. Leader, KPMG LLP

Laeeq Ahmed, Oracle Security & Controls Leader, KPMG LLP

Companies are moving to leverage the cloud at an unprecedented pace, but few have considered the price they may ultimately pay for failing to appropriately manage the associated risks.

Cloud delivery platforms have introduced new risk and compliance requirements, impacting organizations across all industries and geographies. The momentum associated with the shift to the cloud has resulted in daily additions to an organization's cloud service portfolio, challenging even the best security group's ability to effectively protect critical information assets.

We appreciate that most organizations are struggling to establish cloud security standards and capabilities. These strategic and operational challenges compound the risks they face because every cloud platform and vendor has unique cybersecurity standards and requirements. In their push to migrate to cloud services, those business leaders—who may lack cybersecurity know-how—often neglect to implement critical controls due to the misperception that the cybersecurity measures provided by the cloud vendor are also sufficient to protect the business.

Underscoring the severity of this problem, KPMG and Oracle's joint research shows that the diversity of cyber threats and the regularity of attacks are now impeding business operations.

Call to Action

C-level, finance, HR, risk, IT, and security leaders are responsible for ensuring that the organization has a cybersecurity program to address risks inherent in the cloud.

Beyond making sure that risks are mitigated and compliance requirements are addressed, leaders should accept and assert their responsibility for protecting the business. A critical first step is to understand the "shared responsibility" principles for cloud security and controls. Knowing what security controls the vendor provides allows the business to take steps to secure its own cloud environment.

To further protect an organization, it is crucial that everyone in the organization—not just its leaders—is educated about the cloud's inherent risks and the policies designed to help guard against those risks. This requires clear communication and training to employees on cloud usage. KPMG and Oracle's research found that there may be considerable room for improvement in this area, as individuals, departments, and lines of business within organizations are often in violation of cloud service policies.

Understanding your responsibilities for cloud security

Cloud vendors have assumed some responsibility for security, but the business is primarily and fundamentally responsible for maintaining its own cybersecurity and managing its own risks and compliance.

As the use of cloud services introduces new threats, companies need to reassess how they've implemented traditional security protections—including firewalls, access controls, event logging, configurations, and other key controls—and make sure they remain secure.

Leaders must face this new reality and act quickly to dedicate a team, understand the shared accountability requirements, and leverage a framework to meet their responsibilities for securing the organization from cyber threats.

Many companies lack the budget, knowledge, and framework to succeed in these efforts. While they may have built on-premises security layers, companies should invest in enhanced security programs to support the realities of a new cloud-based world.

The challenges of cloud security cannot be solved with a single technology tool or collection of patches—but, rather, through a holistic advancement of cloud-focused security and risk functions. Successful migration to the cloud, and effective operation in it, require a strategic and flexible approach to protecting information, managing risk, and achieving compliance. Hybrid cloud environments, the threat landscape, and knowledge-worker mobility all create a multitude of cybersecurity challenges—regardless of cloud platform, use case, or phase of adoption.

Securing a cloud-enabled workplace requires a focus on people, processes, and business-critical assets. To succeed, organizations should develop specific capabilities to secure their cloud-based environments (just as they had done for on-premises systems). Organizations also need to be consistent in addressing risk and compliance.

KPMG can Help

KPMG has developed a broad cloud security architecture framework based on Oracle's technology solutions for enterprise adoption, with underlying security considerations of availability, integrity, and confidentiality, and a roadmap for implementation.

Our KPMG Cloud Security Framework helps companies define a target operating model for cloud security. Our framework helps organizations bring together people, process, technology, and policy so they can (1) secure the business, (2) advance processes related to cloud services, and (3) better position themselves to outperform competitors.

It's time to review your cloud environment for security risks. The results of our study and our experience can help.

Oracle Perspective: The Rise of the Cloud Security Architect

Greg Jensen, Senior Principal Director - Security, Oracle Corporation

Organizations often look for where they can make the single greatest impact to improve their organization's security posture. As organizations are adjusting their priorities around a cloud-centric strategy, one position has stood out as one of the most central and strategic in meeting security and compliance milestones—the Cloud Security Architect (CSA).

So, what are CSAs, and how do they compare to a security architect? Traditional security architects often focus on broad-reaching security topics that impact the on-premises, mobile, and even cloud world. Over the years, this role has become a bit of a "Jack of all trades" role. The CSA was created to be the "master of cloud security" who understands every possible security and compliance related challenge that a line of business (LoB) owner or infrastructure, platform, or app team could run into when deploying new cloud services. This has led us to a point where we are seeing the role of the CSA surpass the security architect in popularity, according to the *Oracle and KPMG Cloud Threat Report, 2018.*

In the most generalist terms, an *architect* plans, designs, and constructs structures. In Information Technology terms, it is very similar when applied to cloud security. The CSA is responsible for:

- Reviewing the security posture of all SaaS, PaaS, and IaaS projects for industry best practices.
- Identifying risks where security requirements cannot be fully addressed in the timeframe of a project.
- Looking for opportunities where security can be optimized and enhanced.
- Ensuring policies and mechanisms are in place to meet compliance requirements across the cloud.

CSAs are facing increased pressure to balance LoB requirements with corporate security guidelines, and those goals often clash due to time pressure, resources, or budget. Organizations are in a rush to roll out more applications and workloads to the cloud, often with multiple cloud service providers, each with their own SLAs. Every cloud service provider responds to vulnerabilities and incidents differently. The CSA can play an important role in identifying shortcomings from each vendor to understand points of risk, and then develop plans to address them with the provider or internal teams.

ORACLE

The Cloud Security Architect Toolkit

The CSA is under intense pressure to have constant visibility and metrics behind organizations' use of sanctioned cloud resources, as well as visibility into user behavior with unsanctioned applications.

Every day, more organizations are being infected with cryptocurrency malware, turning unsuspicious application servers or cloud applications into hosted platforms for cryptocurrency mining attacks. Few are aware of this unless they see the traffic impacts on Network Performance Monitoring (NPM) tools or Application Performance Monitoring (APM) tools feeding into the Security Operations Center. Forty-eight percent of respondents in the *Oracle and KPMG Cloud Threat Report, 2018* cited that they are now using APM/NPM event feeds to identify threats.

CSAs also are reaching for tools such as Cloud Access Security Brokers (CASB) to help identify all the cloud applications in use, apply a risk score on users, and recommend remediation plans when suspicious activities are identified.

For more information on ways Oracle can enable your CSA or IT security strategies, visit us at www.oracle.com/security

One of the key challenges is balancing the security and compliance needs between an organization's hybrid and multi-cloud environments. One approach that some organizations are focused on is the single vendor model that uses a tightly integrated framework across the full stack of cloud services (DaaS, SaaS, PaaS, and IaaS), which many argue reduces risk and points of exposure. The single vendor approach often lends itself to the challenges of securing an organization once, and enabling them to scale as they need. Key criteria CSAs should look for in a cloud service provider include:

- **Comprehensive** – Secure users, apps, data, and infrastructure across the full cloud stack (DaaS, SaaS, PaaS, and IaaS).
- **Automated** – Detect, prevent, predict, and respond to the latest security threats with AI and machine learning.
- **Data-centric** – Control access to sensitive, regulated data using encryption, masking, and user access controls.
- **Unified** – Collect security and operational data in a single data set to correlate and analyze cyber threats.
- **Integrated** – Developed, architected, deployed, and maintained to securely work together.

The role of the CSA is as strategic as the cloud vendors chosen to underpin and secure that cloud architecture. Oracle and KPMG have a longstanding history of supporting our customers with solutions that meet the very challenges facing today's CSA.

For more information on Oracle security solutions, please visit **www.oracle.com/security.**

1

Broad Cloud Adoption Puts the Spotlight on Cybersecurity

When attempting to thrive in the digital economy, organizations' need for agile technology solutions intensifies. The conventional mindset—that security is an obstacle to cloud adoption—is losing relevance. Public cloud services are now used at most organizations, regardless of the security team's position on the matter. CISOs must understand that cloud adoption, left ignored, is an impediment to security. This dynamic has shifted the realities of traditional cybersecurity approaches and challenged existing solutions.

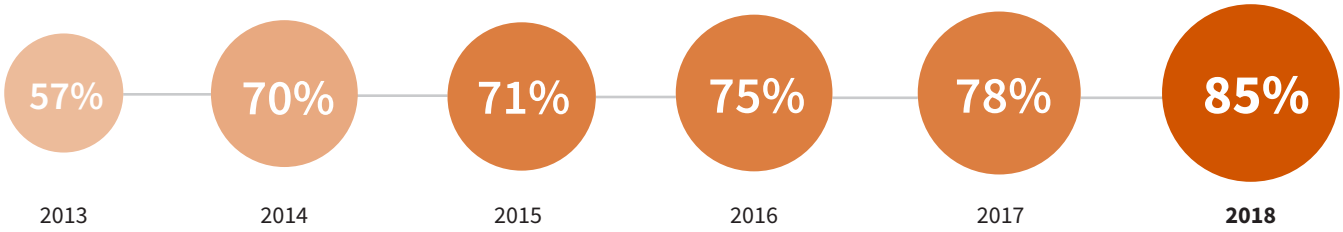
Cloud-first Initiatives Are Driving Adoption

Originally a United States Federal Government mandate, "cloud-first" now represents a strategic imperative for many private and public-sector organizations to deliver IT projects via the use of cloud services. Our research reveals just how broad cloud-first initiatives are with eighty-seven percent (87%) of respondents reporting that their organization has a cloud-first orientation.

Consistent with this finding, according to ESG research, the vast majority of businesses—85%—now use some form of public cloud service.[2] Looking back, the pace of adoption has been swift. Consider that in 2013, 21% of organizations said they used infrastructure-as-a-service (IaaS); this year, that number climbed to 51%, an increase of 143%, according to that same research study. Furthermore, the vast majority (81%) of companies consuming IaaS platform services say they use services from more than one cloud service provider.[3] SaaS adoption continues to outpace IaaS adoption rates, with 74% of organizations now stating they use SaaS applications compared with 51% who are currently using IaaS.

Figure 1. Public Cloud Adoption, 2013-2018

Overall usage of public cloud services, 5-year trend. (Percent of respondents)



[2] Source: ESG Master Survey Results, 2018 IT Spending Intentions Survey, December 2017.
[3] ibid.

Back to Contents

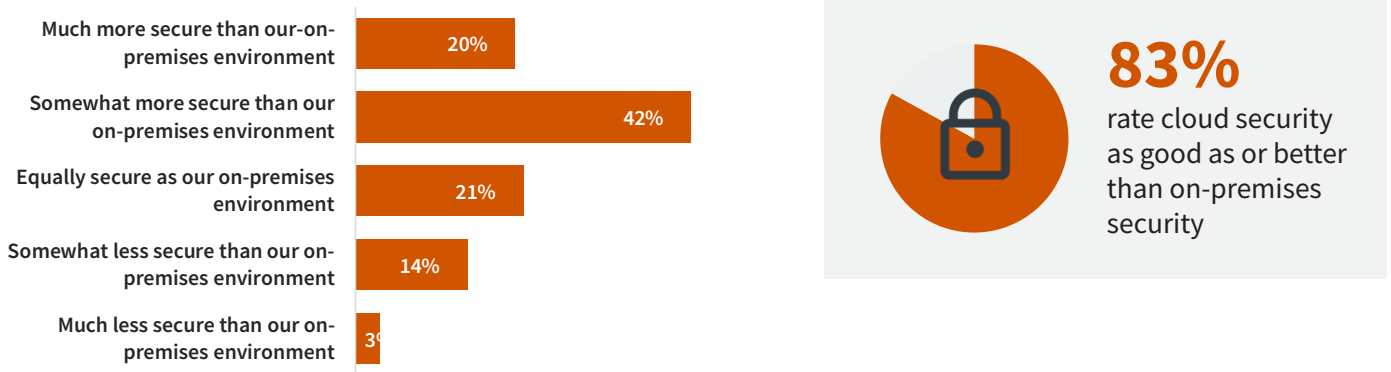
The result of the broad adoption of cloud services is a multidimensional data center comprised of an array of new technologies that run alongside traditional solutions being managed and secured with islands of disconnected tools and processes. Given the complex nature of this environment, it's no wonder that 26% of our research respondents cited a lack of unified policies across disparate infrastructure as a top challenge. After all, absent the ability to unify, IT and cybersecurity teams are left to define and apply policies in silos.

Customers Are Confident in Their Cloud Service Provider's Security, but Should Vet Rigorously

Perhaps most telling with respect to the growing confidence in the security posture of public cloud environments is how our research participants rated the security of cloud service providers (CSPs) relative to their own on-premises environments; 83% of survey respondents believe their CSPs' security is as good as or better than their own.

Figure 2. Customers Rate Their CSPs on Security

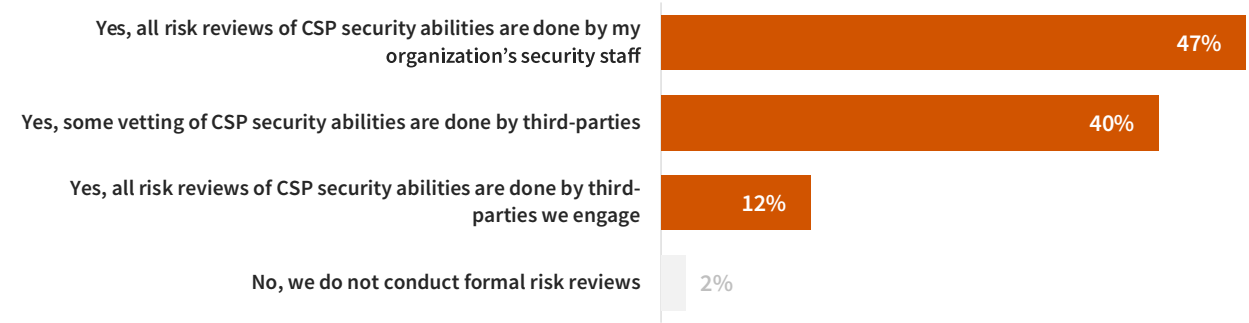
How does your organization view the security of public cloud environments to host and deliver its business applications and data assets? (Percent of respondents, N=450)



As strong a testament as this rating is, it comes as a by-product of good policy and diligence on the part of customers. Indeed, 98% of all organizations surveyed say they conduct formal cybersecurity reviews of their public cloud service providers prior to doing business with those firms (see Figure 3). It is worth noting that only 47% of these respondents say they can assess a CSP's security on their own, with 52% of organizations engaging a third-party to do some or all of the vetting. The challenge of assessing a CSP's security is compounded by the lack of a definitive industry standard that benchmarks a CSP's cybersecurity program, creating ambiguity for customers. This grey area requires that customers establish their own set of cybersecurity requirements against which they evaluate a CSP's cybersecurity program.

Figure 3. Customers Vigorously Vet Their CSPs

Does your organization conduct formal cybersecurity risk reviews of CSPs prior to utilizing their services? (Percent of respondents, N=447)



Working with third-party auditors to leverage the breadth and depth of their experience set is clearly a good practice given that, when customers evaluate the cybersecurity abilities of a prospective cloud service provider on their own, they do so at a rather cursory level. For example, the top action taken to vet a CSP by customers who do not engage a third-party, as shared by 51% of participating organizations, is a simple review of the CSP's cybersecurity policies. Other aspects are also evaluated, including reviewing the results of penetration tests, reviewing their privacy policy, and understanding levels of compliance with both industry regulations and data center certifications.

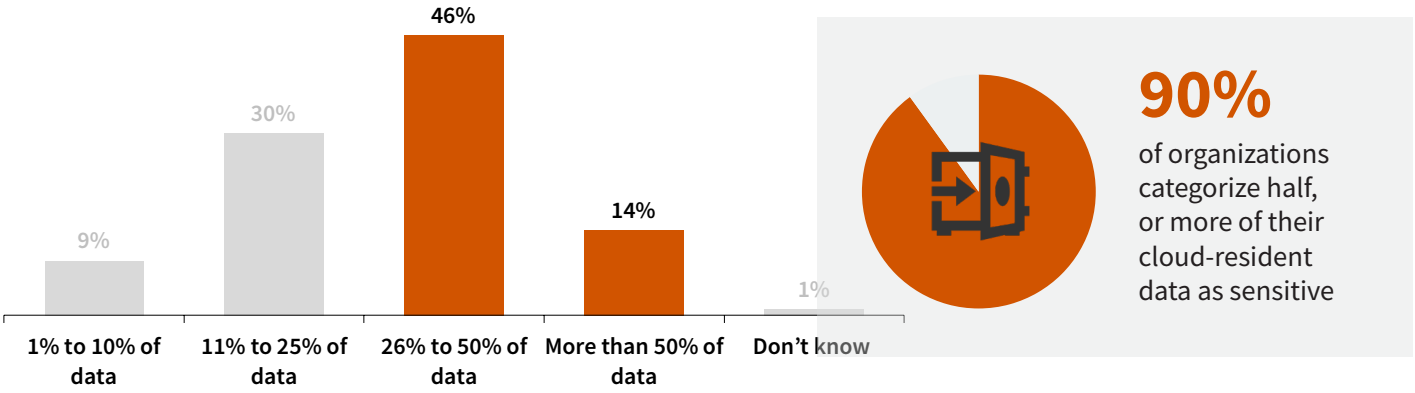
But these are arguably checklist items indicating more diligence is required, perhaps by working with a trusted third-party, to conduct a comprehensive assessment of a CSP's security posture. Doing so is especially warranted for an organization's most sensitive and business-critical cloud applications, namely Customer Relationship Management (CRM), Human Capital Management (HCM), Enterprise Resource Planning (ERP), and supply chain management (SCM) solutions. These applications are central to daily business operations and often contain a company's most critical data assets such that any compromise to their integrity represents significant risk to the business.

Sensitive Data Is Migrating Upwards to the Cloud

Many organizations are now so comfortable with the security of the cloud that an appreciable portion of their data assets are stored in the cloud. Sixty percent of organizations reported that more than a quarter of their data is now cloud-resident.

Figure 4. The Scope of Cloud-resident Data

To the best of your knowledge, approximately what percent of your company's data resides in any public cloud vs. on-premises? (Percent of respondents, N=450)



More striking, however, is the shear amount of data stored in the cloud that is considered sensitive. What individuals deem to be sensitive to their organizations is subjective and therefore could include a broad set of data types, including CRM data, personally identifiable information (PII), payment card data, legal documents, designs, source code, other types of intellectual property, and more. With that lens on, 90% of participants in our study shared that half or more of their cloud-resident data is sensitive, providing evidence of the level of comfort businesses now have in leveraging the cloud for even their most important assets.

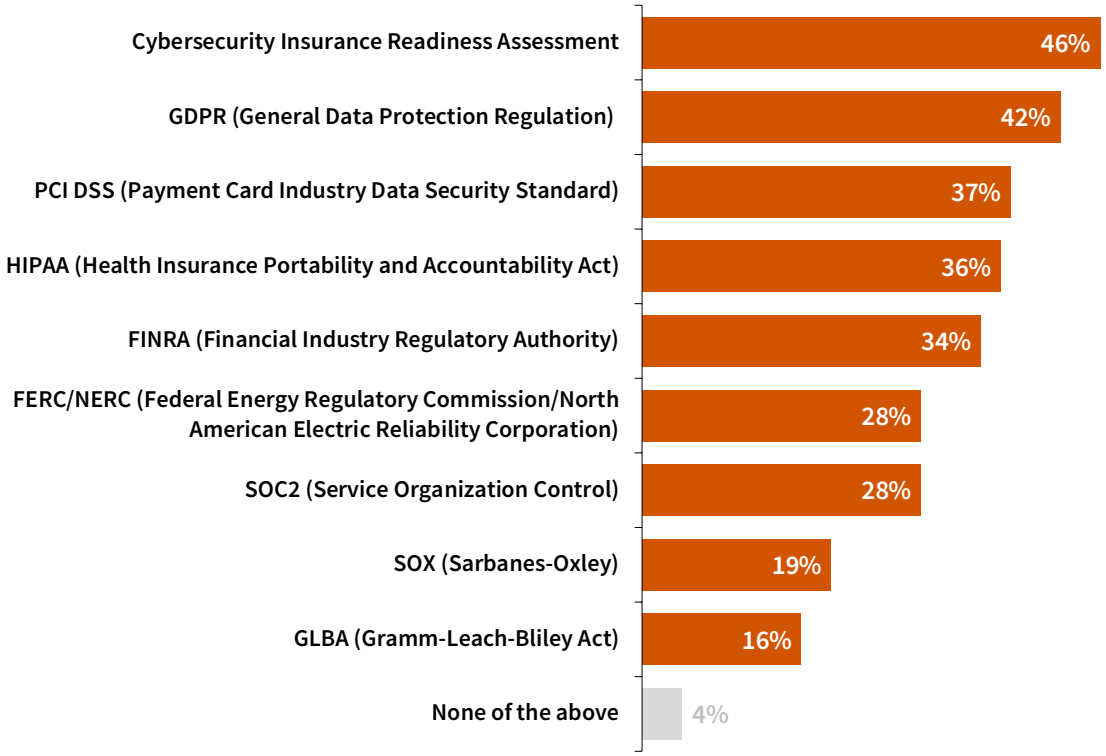
> **“GDPR introduces intricate new regulations and processes for handling the personal data of EU citizens.”**

Spotlight: GDPR Is Impacting Cloud Strategies

The European Union’s landmark General Data Protection Regulation (GDPR), which goes into effect May 25, 2018, will govern the protection of personal data of EU citizens across 28 member nations, requiring that businesses adhere to new obligations to protect the privacy of EU citizens. The scope, requirements, and penalties for breaches make GDPR a top-of-mind issue for most companies conducting business in one of the member nations. Forty-two percent of respondent organizations in our survey will be forced to comply with GDPR (see Figure 5).

Figure 5. Compliance Obligations for Survey Respondent Base

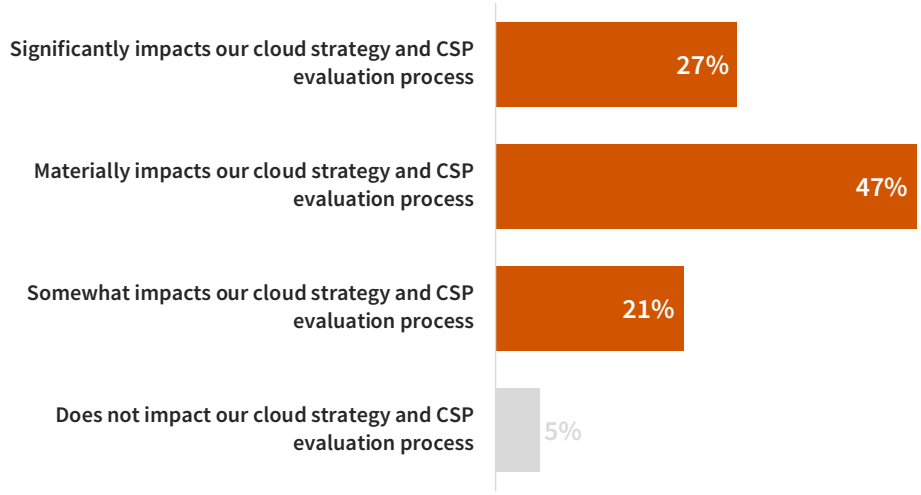
With which, if any, of the following industry regulations is your organization required to comply? (Percent of respondents, N=450, multiple responses accepted)



GDPR introduces intricate new regulations and processes for handling the personal data of EU citizens. It's a sprawling, complicated law that stipulates implementation of processes like complex data inventories, mandatory breach notifications, and data-portability rights, to name a few. Respondents to our survey are feeling the GDPR impact: 42% of responding organizations say that their company needs to comply with GDPR and a full 95% of those businesses that are subject to the legislation say it has affected their cloud strategy (see Figure 6).

Figure 6. GDPR Is Impacting Cloud Security Strategies

To what degree does your organization's requirement to maintain compliance with GDPR impact your cloud strategy and CSP evaluation process? (Percent of respondents, N=190)



95%

of respondent organizations that are subject to the legislation say it has affected their cloud strategy

One of the central considerations for how GDPR impacts the adoption of cloud services is the movement of that data between a CSP's data centers. Organizations will need to understand whether their cloud service provider (CSP) employs essential data security best practices including, but not limited to:

- **Separation of duties** by assuring that you, the customer and subscriber to the cloud service, are the custodian of the encryption keys. Many CSPs are now supporting Bring-Your-Own-Key (BYOK) and single-tenant Hardware Security Module (HSM) implementation options that provide customers more control to ensure separation of duties.

- **Data discovery and classification** against which policies can be applied enables an organization to meet its obligation, including the right to be forgotten, which, if invoked by an EU citizen, requires her personal data to be erased. Organizations must identify, tag, and track all personal information to be able to meet the right to be forgotten.

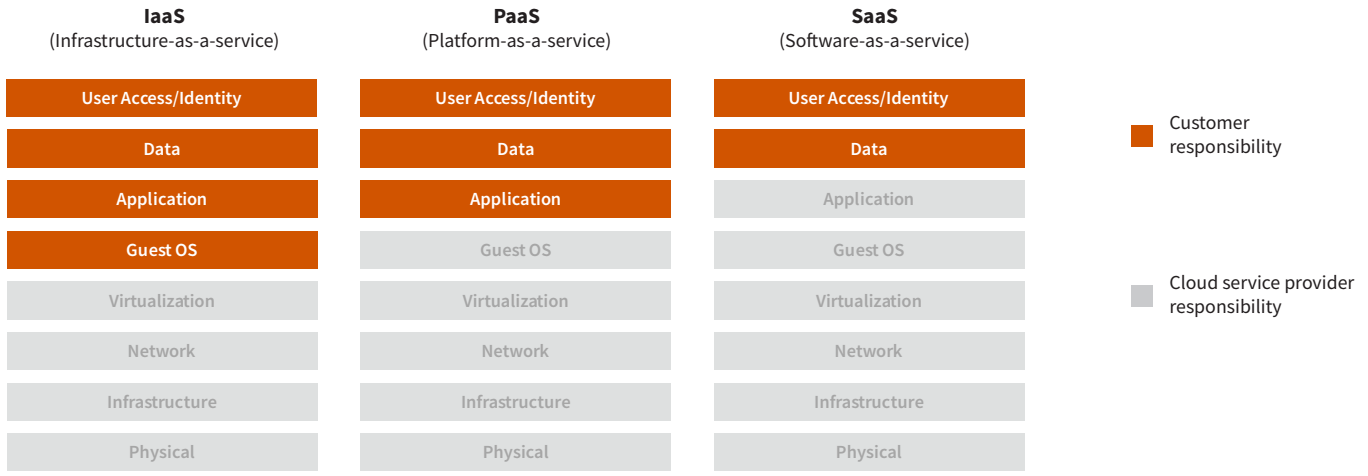
Furthermore, third-party services may be required to implement these and more steps to achieve compliance with not only GDPR, but also the other regulations that research participants cited as being applicable to their organizations. These include getting ready for a cybersecurity insurance underwriting audit, PCI DSS, HIPAA, and more.

Cloud Security Is a Misunderstood Shared Responsibility

In a shared responsibility security model, the cloud provider and the cloud consumer each have a role to play in securing cloud-resident infrastructure and cloud-delivered applications. The line of demarcation about what part of the stack each party is responsible for securing differs between SaaS, IaaS, and PaaS services. For example, IaaS CSPs are generally responsible for securing the physical infrastructure up to and including the virtualization layer with the customer then responsible for protecting the server workload. However, regardless of consumption model—IaaS, PaaS, and SaaS—the customer is generally responsible for data security and user access and identity management (see Figure 7).

> **"In our survey, fewer than half (43%) of respondents were able to correctly identify the most common IaaS shared responsibility security model."**

Figure 7. Cloud Security Shared Responsibility Model



While this graphic depicting the shared responsibility security model across the three types of cloud services is generally accepted, it's important for consumers to keep in mind that mileage will vary between providers. For example, some CSPs, as a compelling point of differentiation, are now providing autonomous patch management to protect critical systems, such as database servers, from exploits. Customers typically leverage a combination of CSP-provided native controls, such as host-based firewalls in concert with third-party cloud security tools, to meet obligations.

Shared responsibility sounds relatively straightforward, but customers often do not fully understand their responsibilities, a highly problematic reality. In our survey, fewer than half (43%) of respondents were able to correctly identify the most common IaaS shared responsibility security model. Confusion about how security is a shared responsibility extends into compliance. While a CSP's compliance with regulations such as SOC 2 is an indicator of certain security practices, customers who process credit card transactions do not, for example, inherit a CSP's compliance with PCI DSS. Similarly, health care organizations entering into HIPAA Business Associate Agreements (HIPAA BAAs) must do so with an understanding that HIPAA-compliant cloud services do not relieve them of their responsibility to protect patient health information (PHI). In all cases, customers should work with their CSP to understand that provider's specific shared responsibility security model to eliminate any confusion.

Another contributor to ambiguity around this notion of shared responsibility is the physical network security orientation of many practitioners. Organizations should augment the use of network security controls, such as physical and VM-based firewalls, intrusion detection and prevention systems, and gateways, with a set of purposeful workload and cloud application controls. For example, physical and VM-based firewalls that control access to cloud services from on-premises users and application tiers should be augmented with host-based firewalls on cloud-resident workloads for access control and segmentation. A notable example of a purposeful cloud security control is Cloud Access Security Brokers (CASBs) that provide essential capabilities to secure the use of cloud applications, including data loss prevention (DLP) policies to protect cloud-resident data assets.

2

Today's Threat Landscape Is Diverse and Recurring

Threat diversity and attack regularity disrupt business operations.

Cybercriminals Are Top-of-mind Cyber Adversaries

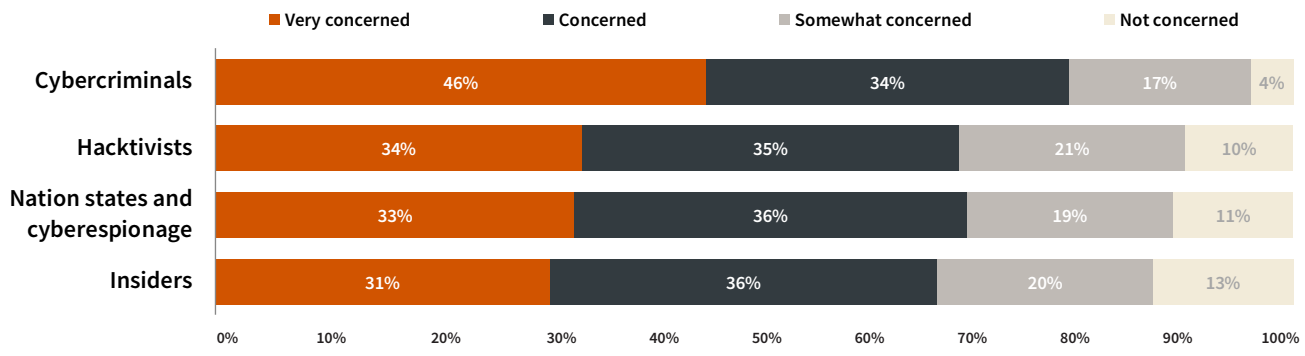
Today's cybersecurity threats are increasingly diverse, technically virulent, and often specifically engineered to target an organization's most valuable assets. They are designed and delivered by a global cast of bad actors, including cybercriminals, hacktivists, nation-states, and inside employees with differing motivations.

If there has been one breakaway threat over the last few years, however, it's ransomware. Almost two-thirds (62%) of respondents in an ESG research study say they were hit by a ransomware attack over the last 12 months.[4] Ransomware attacks such as NotPetya, which exploited unpatched operating systems infecting hundreds of thousands of computers in more than 100 countries, and WannaCry, which infiltrated more than 300,000 organizations worldwide, made headlines while other ransomware strains and variants wreaked havoc in a transactional attack campaign carried out by cybercriminals.

Given this epidemic level of ransomware over the last few years, it comes as no surprise that while all types of bad actors are of concern, four-fifths (80%) of respondents say they are very concerned or concerned about the threat cybercriminals pose to their data and networks (see Figure 8).

Figure 8. Concern Over Different Types of "Bad Actors"

What is your level of concern with respect to the threats posed by each of the following types of "bad actors" when it comes to protecting your organization from cybersecurity threats? (Percent of respondents, N=450)



[4] Source: ESG Master Survey Results, *2018 IT Spending Intentions Survey*, December 2017.

The ease with which ransomware can exploit system and human vulnerabilities makes these attacks all too common. And the financial motivation of cybercriminals is now being manifested beyond extortion tactics: Exploiting system vulnerabilities to steal processing power to mine cryptocurrencies— cryptocurrency hijacking —has become an increasingly popular means of realizing financial gain.

Spotlight: The Insider Threat

While cybercriminals are the top concern among our survey respondents, this research reveals that cybersecurity professionals are also concerned with the risk associated with insiders. While the insider threat includes stolen credential situations, in which case the insider is an unwitting proxy to an external adversary, the true malicious insider can be more difficult to detect. These individuals, depending on their objective, leverage their familiarity with a corporate IT environment and escalated privileges to stealthily steal data and potentially disrupt business operations.

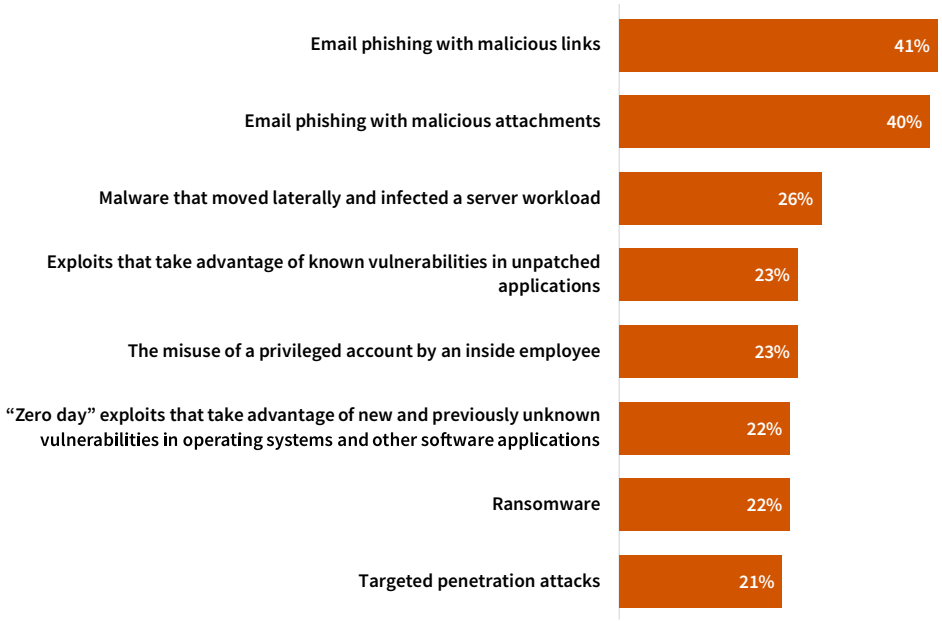
Essential best practices to mitigate the insider threat include the use of adaptive authentication to trigger a second factor of authentication based on context and monitoring for anomalous end-user activity to alert cybersecurity professionals to activity that could be indicative of nefarious intent.

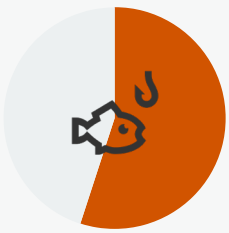
Phishing Is the Top Attack Type

Meanwhile, the predominant attack vectors that introduce threats such as ransomware are old standbys—phishing and malicious exploits. Fifty-five percent of respondents say they fell victim to one (or both) of the two types of phishing emails last year: messages with malicious links or messages with malware-bearing attachments (see Figure 9).

Figure 9. Top Ten Most Common Cyberattack Vectors

Which of the following cybersecurity attacks – if any – has your organization experienced within the last 24 months? (Percent of respondents, N=450, multiple responses accepted, top 10 responses only shown below)





55%

have experienced at least one of the two types of phishing techniques

Email phishing runs the gamut from mass-market emails that are part of a broad attack campaign, through spear phishing that targets an individual, to whale phishing (i.e., "whaling") that focuses on compromising a company's executive team. In all cases, the prevalence of successful phishing attacks exploits human vulnerability with well-engineered emails that fool a user into taking swift yet unfortunate action. As such, ongoing security awareness training to help users identify fictitious emails and a focus on security controls such as those that detect and prevent cross-channel attacks—e.g., emails that include links to malicious emails—are essential.

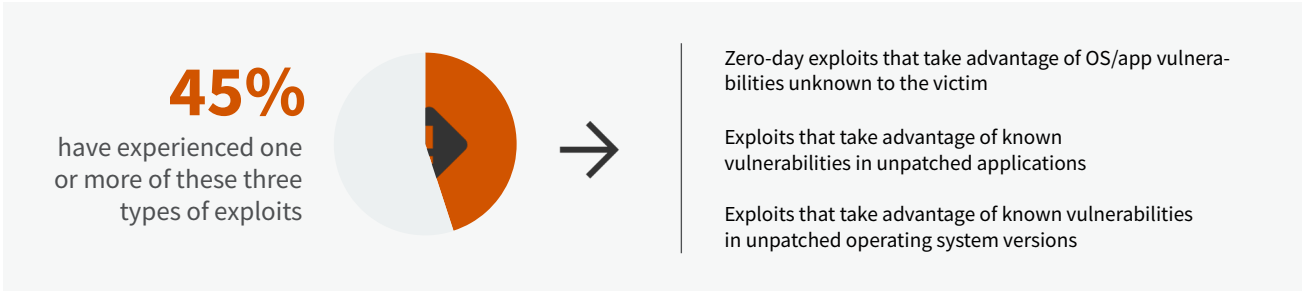
Organizations should also be aware that attackers are now employing other phishing vectors, including:

- **Vishing** – The use of voicemail to solicit a return call in which a user is convinced to share personal information.
- **Smishing** – The use of SMS text messages intended to lure recipients into clicking on a link that can lead to a webpage designed to steal credentials.

Because these newer types of phishing attacks are targeted not only directly at end-users, but also very often at their personal devices, security awareness training can prove most effective in mitigating these threats. Organizations should also be mindful that passwords in and of themselves, no matter how strong, will not fully mitigate the risk of phishing attacks that seek to steal credentials.

Exploited Vulnerabilities Are Prevalent

When it comes to exploits, 45% reported experiencing one or more attacks from an exploit of known vulnerabilities of unpatched applications, known vulnerabilities of unpatched operating system vulnerabilities, and/or new and unknown zero-day vulnerabilities.



A Diverse Range of Threats, Vectors, and Methods Are of Concern Moving Forward

Looking forward, our research reveals that businesses are concerned about a diverse range of attacks with respect to the type of threats and the methods employed by adversaries to introduce them (see Figure 10). Thematically, the concerns of our research participants include:

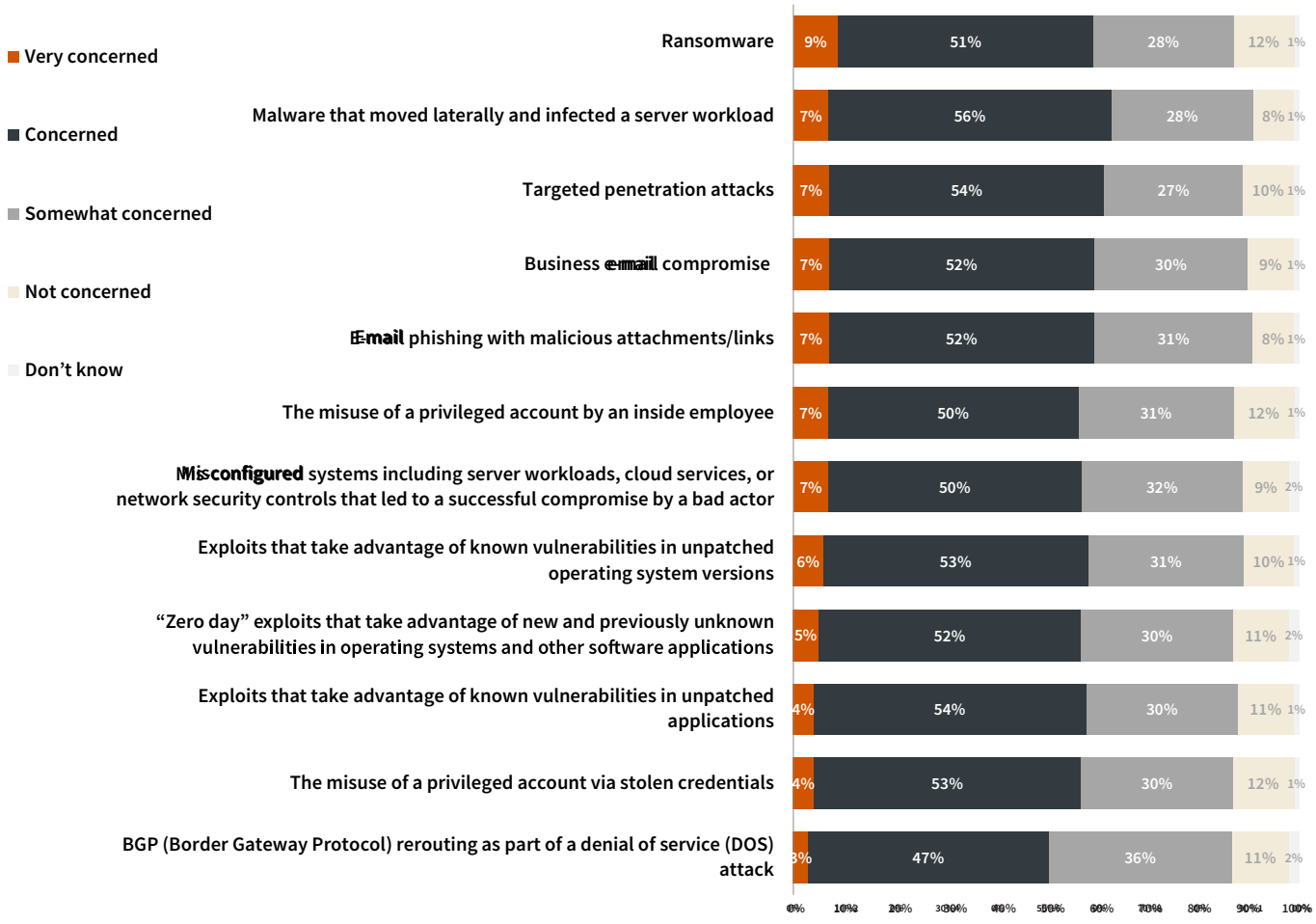
- **Threat types** from ransomware to malware and exploits.
- **Methods** such as targeted penetration attacks, business email compromises, and the theft and misuse of credentials.
- **Vectors** such as email phishing and misconfigured server workloads, cloud services, or network controls.

This research highlights that the frequency and volume of the combination of these vectors and methods employed by cyber adversaries to introduce a range of threats is, indeed, a challenge of scale.

“Of note is the concern about malware that moves laterally to infect a server workload...”

Figure 10: Top Concerns over the Next 12 Months

In terms of the risk level to your organization’s infrastructure, data assets, and business operations, how concerned are you with each of the following threat types over the next 12 months (regardless of any past attacks experienced)? (Percent of respondents, N=450)

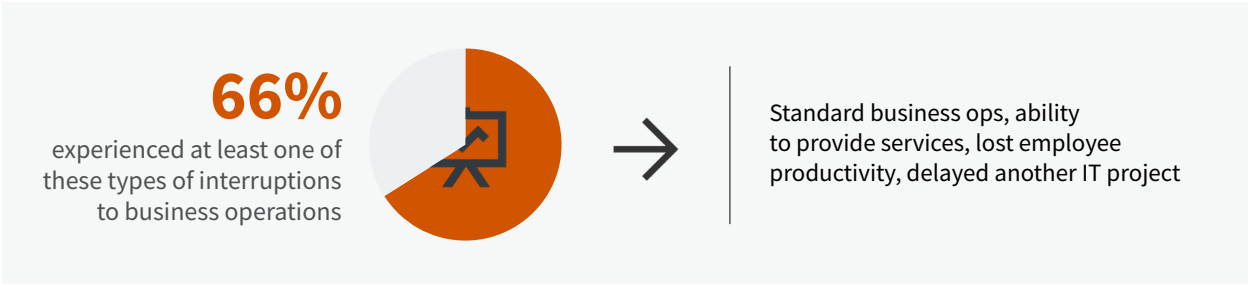


Of note is the concern about malware that moves laterally to infect a server workload, which indicates a focus on protecting an organization’s most critical business applications. Cloud-resident workloads are not immune to malware that moves laterally since attack chains that successfully introduce malware via a compromised endpoint could do the same via a cloud service such as an object store, or from another on-premises or cloud-resident server workload.

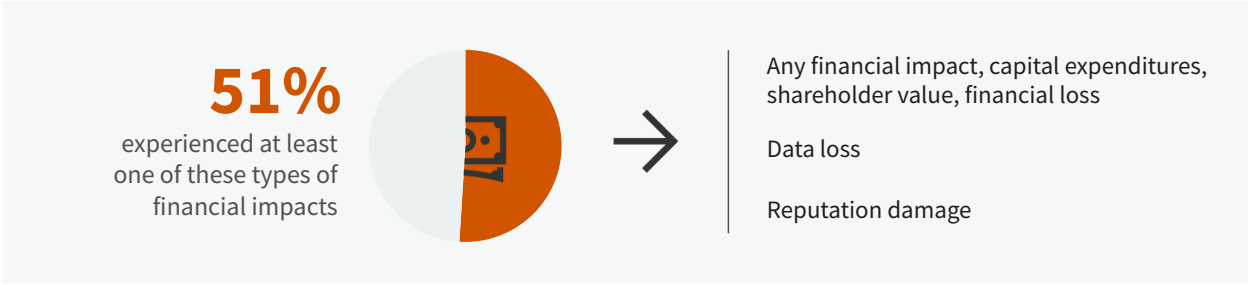
Beyond lateral malware, the negligible difference in survey respondents’ level of concern between the types of attacks punctuates the fact the organizations understand that bad actors are coming at them with a range of weapons. Later in this report, we share some of the defense-in-depth measures organizations are employing to protect themselves against such attacks.

Cyber Attacks Have Operational and Financial Impacts

Reports of high-profile cybersecurity incidents often highlight financial losses as the primary impact of the attack. But we found that disruptions to business operations are typically more frequent outcomes. Consider, for instance, that two-thirds (66%) of respondents say they experienced a cybersecurity incident that affected business operations over the past two years. These impacts include disruptions to standard business operations, disruptions in the ability to provide services, lost employee productivity, and delays in IT projects. The operational impact of cyber attacks can manifest in highly disconcerting situations, such as how ransomware, for example, has impeded the ability of some infected health care organizations to provide patient care.



Financial damages are certainly also a common outcome, however. More than half (51%) of respondents mentioned financial impacts such as financial losses, increased capital expenditures, or reduced shareholder value. Note that these outcomes are not mutually exclusive. Service interruptions and periods of reduced employee productivity often result in the direct loss of business for the organization.



One of the financial impacts of note is the need to incur capital expenditures for new technology. Some organizations rely on older systems to run their business, deferring the cost to upgrade hardware and update software. These older systems may simply not support a new version of an operating system, leaving them vulnerable to exploits. Other times, operating systems remain unpatched to maintain support for legacy applications that do not support new versions of the underlying operating systems. For some companies, a cybersecurity incident can serve as a catalyst to make the capital investments to upgrade older systems or move to the cloud as a necessary means to protect themselves from future attacks. Further adoption of cloud services, however, can obviate the need to make such capital investments.

3

Cloud Adoption Is Creating New Cybersecurity Challenges

Cloud realities create a visibility gap and policy enforcement challenges.

Cloud Adoption Has Created a Gap in Visibility

When it comes to today's most pressing cybersecurity challenges, the most frequently mentioned concern by far—cited by 38% of respondents—is the ability to detect and respond to security incidents in a cloud environment (see Figure 11).

Figure 11. Companies Report Their Biggest Cybersecurity Challenges

What are the biggest cybersecurity challenges currently experienced by your organization today?
(Percent of respondents, N=450, three responses accepted)

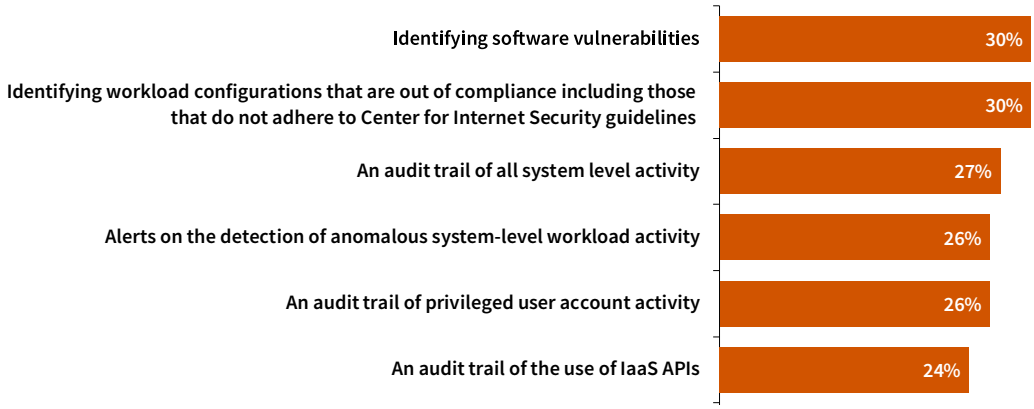
"Lack of visibility is a common refrain. It's rooted in the inability for customers to access the physical network layer and the self-service nature of cloud services."

The lack of visibility is a common refrain when it comes to securing the use of cloud services. It is rooted in some of the aspects that make securing cloud services fundamentally different than on-premises infrastructure, including the inability for customers to access the physical network layer, and the self-service nature of cloud services.

An ESG research study defined the lack of visibility in the cloud by assessing the specific areas that are the most important to improve security visibility for IaaS-hosted workloads.[5] Thematically, these research findings indicate a need to, first and foremost, understand whether any software or configuration vulnerabilities exist in cloud-resident workloads, and, then, a need to audit and alert on system activity, anomalies, and the use of privileged accounts. In total, this set of visibility requirements is indicative of a workload-centric approach.

Figure 12: Areas for Improving Security Visibility into Cloud-hosted Workloads

Which areas do you feel are the most important to improve security visibility for your organization's IaaS/PaaS-hosted workloads? (Percent of respondents, N=450, three responses accepted)



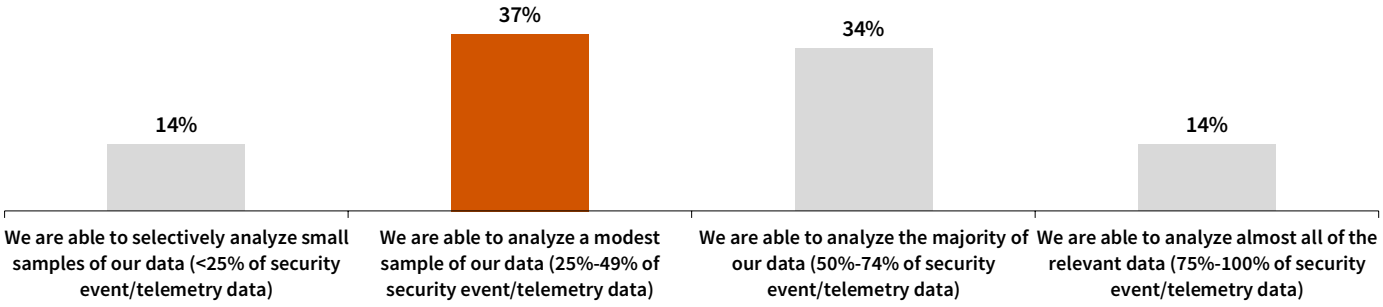
As shown previously in Figure 11, our research reveals that cybersecurity professionals are also concerned about a lack of visibility across their data center and endpoint attack surface, and for good reason. Models depicting the stages of cybersecurity attacks highlight how some attacks gain a foothold on an endpoint from which they move laterally across the data center to their target. For example, a phishing attack that successfully steals privileged account credentials puts critical systems at risk, whether on-premises or in a cloud. The ability to detect and evaluate anomalous endpoint activity provides visibility into the behavior of an attack chain, such as creating a connection to a remote command and control server. Such end-to-end visibility allows organizations to identify weaknesses in their cybersecurity defenses and make the necessary changes.

Analyzing Event Data Is a Challenge of Scale

The ability to collect and analyze a significant amount of security event and telemetry data, across the enterprise, remains another significant issue: Only 37% of respondents to this year's threat survey say they can analyze a modest sample of their data (defined as ranging from 25% to 49% of all data) and another 14% report they can only analyze small samples of their data (less than 25% of event data)—see Figure 13.

Figure 13. Ability to Analyze Security Event Data

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=450)



[5] Source: ESG Research, *Trends in Hybrid Cloud Security: Minding the Gap*, November 2017.

Back to Contents

This inability to analyze events is another aspect of the challenge of "keeping pace at scale"—the theme of this year's study. There are multiple factors that contribute to why so many organizations struggle to collect and analyze their event streams, including the fact that the adoption of cloud services has expanded the attack surface from which event data is generated.

Beyond sheer volume, the ability to triage events to prioritize analysis requires context from correlating event data. Without the use of advanced analytics solutions, including the application of machine learning, time-intensive manual processes are required. As organizations establish actionable context, the ability to automate responses and remediation steps will be instrumental in processing a deluge of telemetry data.

Cloud Security Policies Fail to Deter Shadow IT

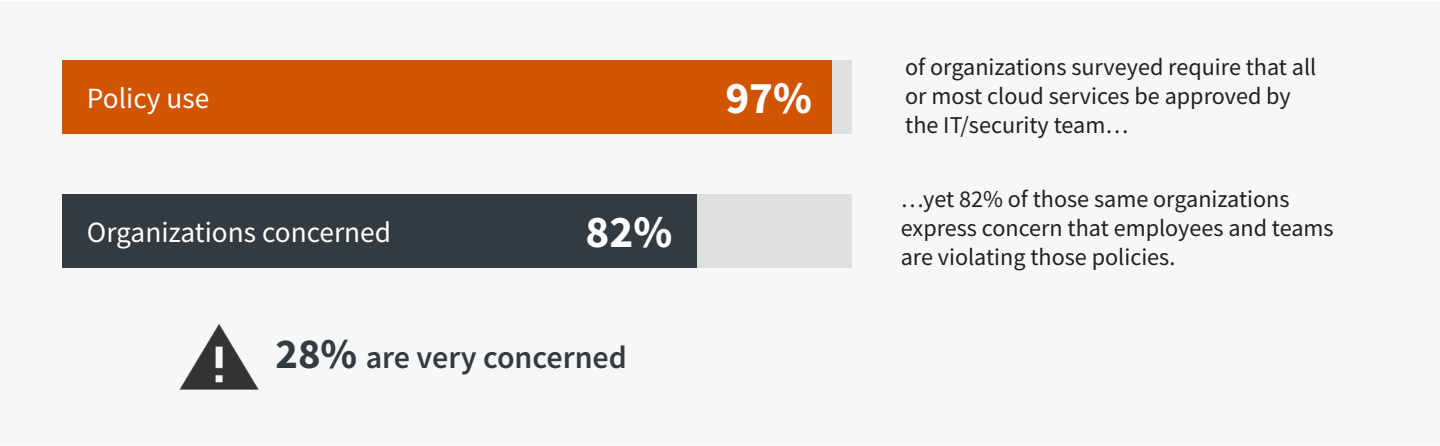
As competitive pressures push organizations toward more rapid delivery of products and services, companies have little choice but to allow line-of-business (LOB) managers to leverage cloud services. But IT and cybersecurity teams have attempted to make the use of cloud services secure as a matter of policy with little success.

We found that 50% of organizations say ***all*** cloud services must be approved by the IT/security team, with another 47% noting that ***most*** cloud services must be approved by IT/security. But, in reality, those policies are being widely ignored. While, in total, 97% have defined cloud-approval policies, an astonishing 82% of respondents are concerned that these policies are being ignored (see Figure 14).

Figure 14. Cloud Usage Concerns Remain Despite Established Policies

Which of the following best represents your organization's policy for the use of cloud services at your organization? (Percent of respondents, N=450)

How concerned are you that individuals, departments, and/or lines of business within your organization are in violation of your cloud services policies? (Percent of respondents, N=450)



The prevalence of shadow IT, in which individuals and business units sidestep cloud usage policies, is driven by a number of factors including a need for speed, personal preferences, and an increase in external collaboration. Work streams that entail a high level of collaboration, often with external parties via enterprise file sync and share (EFSS) applications, are a catalyst for the unapproved use of cloud applications. End-users who develop an affinity for a certain cloud application may be apt to use that service at work, and share corporate data via that same unauthorized and unsecured cloud service.

Shadow IT is caused by both the unauthorized use of a wide variety of SaaS applications by individual employees, and distributed development teams that can leverage IaaS and PaaS platforms for rapid application development. The perspective that the involvement of the IT and security teams impedes agility necessitates a new approach, one that embraces and enables the secure use of cloud services.

The Acute Shortage of Cybersecurity Skills Continues

Many businesses have not yet transformed their IT and cybersecurity operations to accommodate cloud security. In large part, that's because they haven't yet developed the requisite skills and addressed certain operational issues.

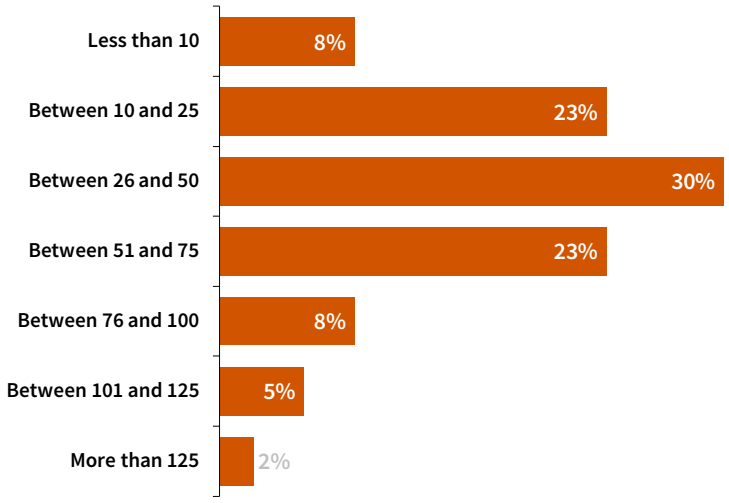
One of the biggest cybersecurity challenges cited in our research is the lack of skills and qualified staff, with 23% weighing in that this is one of their organization's biggest cybersecurity challenges (please refer back to Figure 11). This problematic shortage of skills is punctuated in an ESG research study in which 51% of respondents shared that their organization has a problematic shortage of cybersecurity skills.[6]

Spotlight: Point Tool Fatigue

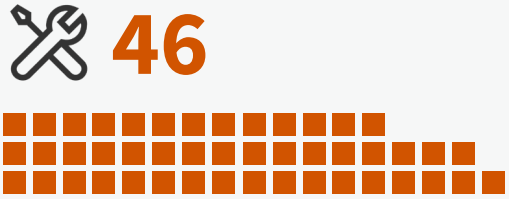
It's clear that enterprise cybersecurity professionals have their hands full. Consider that a cybersecurity professional manages an average of 46 security products (see Figure 15), leaving them very little time to master new cloud technologies, tools, and emerging best practices. Such acute point solution fatigue results in operational inefficiencies—an example of which is the finding in this study that cybersecurity teams struggle to process event telemetry at scale.

Figure 15. Average Number of Point Tools Managed by Cybersecurity Professionals

For approximately how many discrete or point cybersecurity products are you personally responsible? (Percent of respondents, N=450)



Number of different cybersecurity products (on average) managed by those in leadership roles (CISO, VP or security, etc.):



[6] Source: ESG Master Survey Results, *2018 IT Spending Intentions Survey*, December 2017.

4

Moving Identity and Access Management to the Forefront

The identity imperative of the cloud-enabled workplace

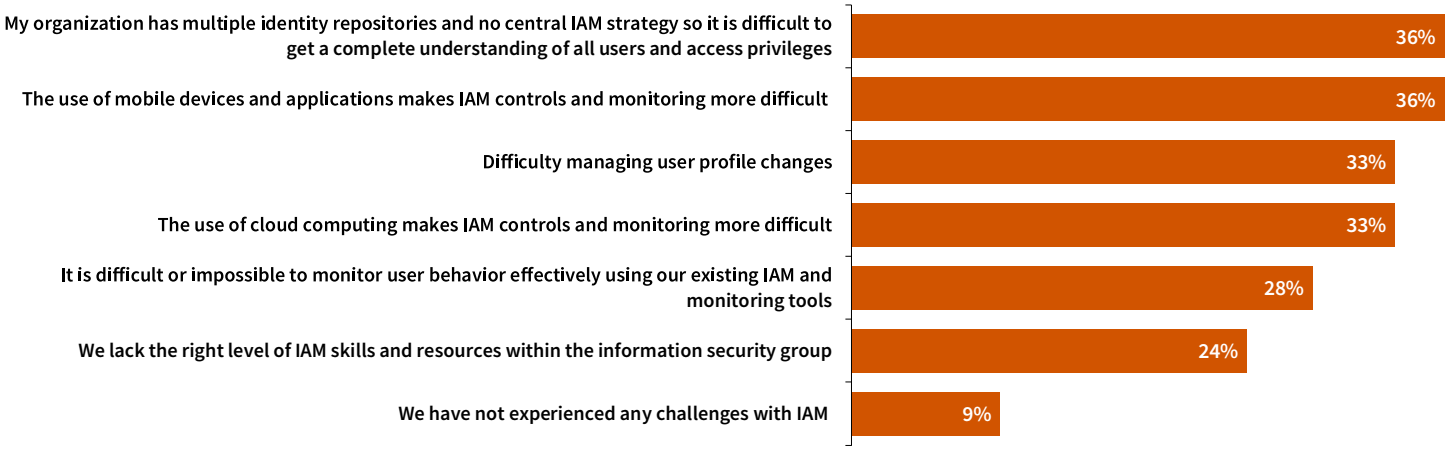
‘Anyone from Any Device at Any Time and Location’ Creates Identity-at-scale Challenges

A diverse set of knowledge workers now use mobile devices to access cloud-delivered corporate business applications, such as CRM, ERP, and HCM, as well as documents containing sensitive information. And they do so at any time and from anyplace. At the same time, applications and data are being accessed by sets of individuals broader than employees, including contractors, business partners, part-time workers, customers, and suppliers, making managing identity a challenging but critical aspect of securing the cloud-enabled workplace.

Indeed, the use of cloud services, alongside the increased mobility of knowledge workers, has challenged identity and access management systems and practices. It’s not surprising that the most frequently cited identity and access management challenges in our research highlight not only the mobility issue (i.e., more mobile users, devices, and applications) but also the need for organizations to manage multiple identity repositories (see Figure 16). As a result, the lack of a central IAM strategy makes it difficult to establish a single source of truth for authenticating identity and managing access privileges.

Figure 16. Identity and Access Management Challenges

Which of the following are your organization’s most significant identity and access management (IAM) challenges? (Percent of respondents, N=450, three responses accepted)



Businesses also say that it is difficult, if not impossible, to monitor user behavior with their existing IAM and monitoring tools. With respect to monitoring specifically, survey respondents say that the use of mobile devices and cloud applications has complicated the use of IAM controls and monitoring. But based on survey responses, businesses could benefit from more frequent reviews of employee entitlements. Currently, 45% say they review entitlements once a quarter, while 28% review them each month.

Entitlement review is especially relevant when comparing the process for removing a former employee's access to an on-premises application versus the one for terminating access to cloud-delivered applications. In the case of eliminating an ex-employee's access to an on-premises application, the IT organization typically follows an exit protocol that includes taking steps such as gaining possession of the employee's laptop, disabling VPN access, removing the user from the domain, and more. However, a former employee does not need a VPN connection to access a company's SaaS application and can do so from another device with his or her credentials. As such, eliminating a former employee's entitlement to use cloud applications makes decommissioning cloud application credentials a critical step in the employee exit process and one that is especially important for business-critical applications such as ERP and CRM systems.

Managing identity in the cloud-enabled workplace has become a challenge of scale that encompasses any user, device, and app at any location and time. That's why identity must be at the center of a cybersecurity strategy for the cloud-enabled workplace. While IAM has largely become operationalized, its heightened importance in today's complex IT infrastructure requires that organizations implement a complete, up-to-date identity strategy. After all, identity is the skeleton key that opens all the doors of enterprise applications and systems.

> **"identity and access management policies should be grounded in an alignment of business processes, roles, and permissions with an individual's HR profile following the least-privileged best practice"**

IAM Policies Must Align Roles and Permissions

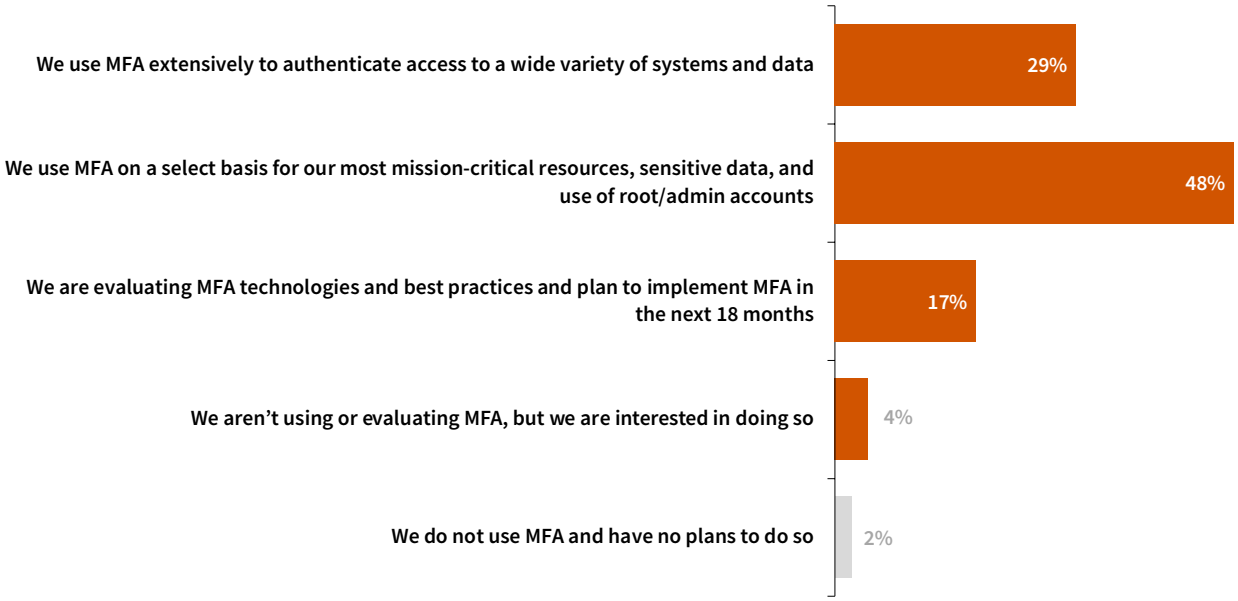
To get identity right, businesses must start with the understanding that IAM has evolved from abstracted identities and devices to a focus on people—that is, individual users—as the new perimeter. This will be particularly challenging to the 36% of businesses in Figure 16 that use multiple repositories for IAM because they have no single source of truth for what a person is allowed to access, and with what level of privileges.

Also influencing the evolution of IAM is increased employee fluidity in the workplace. Even at organizations with very low employee turnover, today's employees tend to have more roles over the course of their employment than in the past. To be effective, employee privileges should change with those roles. That is, identity and access management policies should be grounded in an alignment of business processes, roles, and permissions with an individual's HR profile following the least-privileged best practice, whereby the fewest number of individuals are granted access to the least amount of systems with the least amount of privileges required for them to effectively perform their jobs. However, as this research indicates, implementing least-privileged user account (LUA) management in cloud-enabled workplaces that lack centralized IAM repositories is challenging. Single sign-on (SSO) solutions that employ the Security Assertion Markup Language (SAML) as a means to federate access to multiple cloud services based on a centralized policy lexicon offers a means toward the LUA end.

Employ MFA for Access to Sensitive and Critical Assets

Fortunately, many businesses are embracing multi-factor authentication (MFA) to grant access to the organization's most sensitive and mission-critical assets. In fact, almost half (48%) of respondents rely on MFA to help lock down sensitive or mission-critical data and assets, with another 29% employing MFA to authenticate access to a wider variety of systems and data assets (see Figure 17). The use of MFA is also often a requirement for compliance with industry regulations such as PCI DSS.

Figure 17: Current Use of Multi-Factor Authentication



Spotlight: Adaptive Authentication

Beyond basic MFA, many organizations are adopting a more sophisticated, risk-based approach to requiring a secondary factor. "Adaptive authentication" evaluates the context of an authentication request, including a user's risk profile and behavior. For example, if an employee who typically logs in from a location in the United States attempts to access the corporate network or a cloud service from another country, and does not have a historical record of doing so, MFA solutions that utilize adaptive authentication will recognize this anomaly and trigger an additional factor of authentication. Such solutions can also be configured to evaluate such context for access to applications and data assets that the organization deems to be critical and sensitive. In short, this approach adapts the level of authentication to the level of risk based on context, without unnecessarily interrupting the user.

Adaptive authentication also serves as an anti-phishing control to prevent such attacks from using stolen credentials to access corporate assets. This form of authentication resonates strongly with our research base, as 66% of survey respondents indicated they are interested in exploring adaptive authentication to secure access to their corporate assets.

It's also effective to monitor user behavior not only to trigger a second factor of authentication, but also to understand normal access and use, and identify a potential malicious insider. This type of continuous monitoring will help businesses determine what employees are accessing which assets. This helps organizations better manage risks to these assets by implementing IAM best practices such as least-privileged access and adaptive authentication.

66%

are very or somewhat interested in triggering a second factor upon detecting an anomaly

5

Cybersecurity Best Practices for Modern IT Environments

Securing the cloud-enabled workplace requires a holistic and integrated approach across people, processes, technology, and business-critical assets.

The research findings of this study depict a modern IT environment comprised of:

- Cross-generational application stacks that require a reorientation around the definition of the perimeter.
- The use of multiple cloud providers across the entire stack of SaaS, PaaS, and IaaS.
- A pragmatic approach to securing the use of cloud applications.
- An ongoing focus on awareness training.
- A need to retool technical cybersecurity skills and roles.
- A characterization of patching as a configuration management best practice.
- The implementation of a defense-in-depth approach to protecting mission-critical applications.

If your company resembles, or is moving toward this modern IT environment, here are a few best practices that your organization can begin to implement today.

Think Beyond Perimeter Defenses

Network perimeters are now part of a broader perimeter made amorphous due to mobility and the prevalent use of cloud services. IT and cybersecurity leaders need to evolve their cybersecurity programs to an approach that augments network security controls with strategies, skills, and processes for the fluid nature of today's identity-based perimeter.

Adopt a Dose of Cloud Security Pragmatism

The speed and degree to which cloud apps and services are being adopted can be at odds with corporate cybersecurity programs that call for a more cautious approach. The reality—that the use of cloud services is often user-led, and born out of a sense of business urgency—creates a need for IT and cybersecurity leaders to strike a balance between enabling the secure use of the cloud and mitigating the associated risk.

A pragmatic approach of partnering with line of business leaders to gain alignment on such a balance requires an understanding and appreciation of the requirements that are driving the use of cloud applications in the first place. Such business discussions also serve to help business unit leaders to, in turn, understand and appreciate the cybersecurity policies, processes, and controls that are essential to ensure the secure use of the cloud. Implementing such a pragmatic approach requires adopting a series of best practices including:

Cloud Security Best Practices:

Coverage across cloud services, including SaaS properties and IaaS services, so that visibility and control policies can be applied across the breadth of services being used.

Contextual visibility that goes beyond the discovery of shadow IT applications to allow organizations to assess the risk associated with each app and service in use.

Data discovery and classification, another aspect of visibility, to provide insight into what types of data assets are being stored in conjunction with the use of cloud services.

Maintenance of system integrity by monitoring for configuration drift and automating the remediation of non-conformant workloads and cloud services, including, for example, the ACLs on object stores.

Threat prevention by inspecting in-transit traffic and at-rest content for malicious payloads to prevent cloud services from being employed as an attack vector.

Data loss prevention (DLP) policies to govern which users have access to classes of cloud-resident data.

Monitor user behavior for anomalous activity, such as non-standard login times and locations, as well as irregular data access actions.

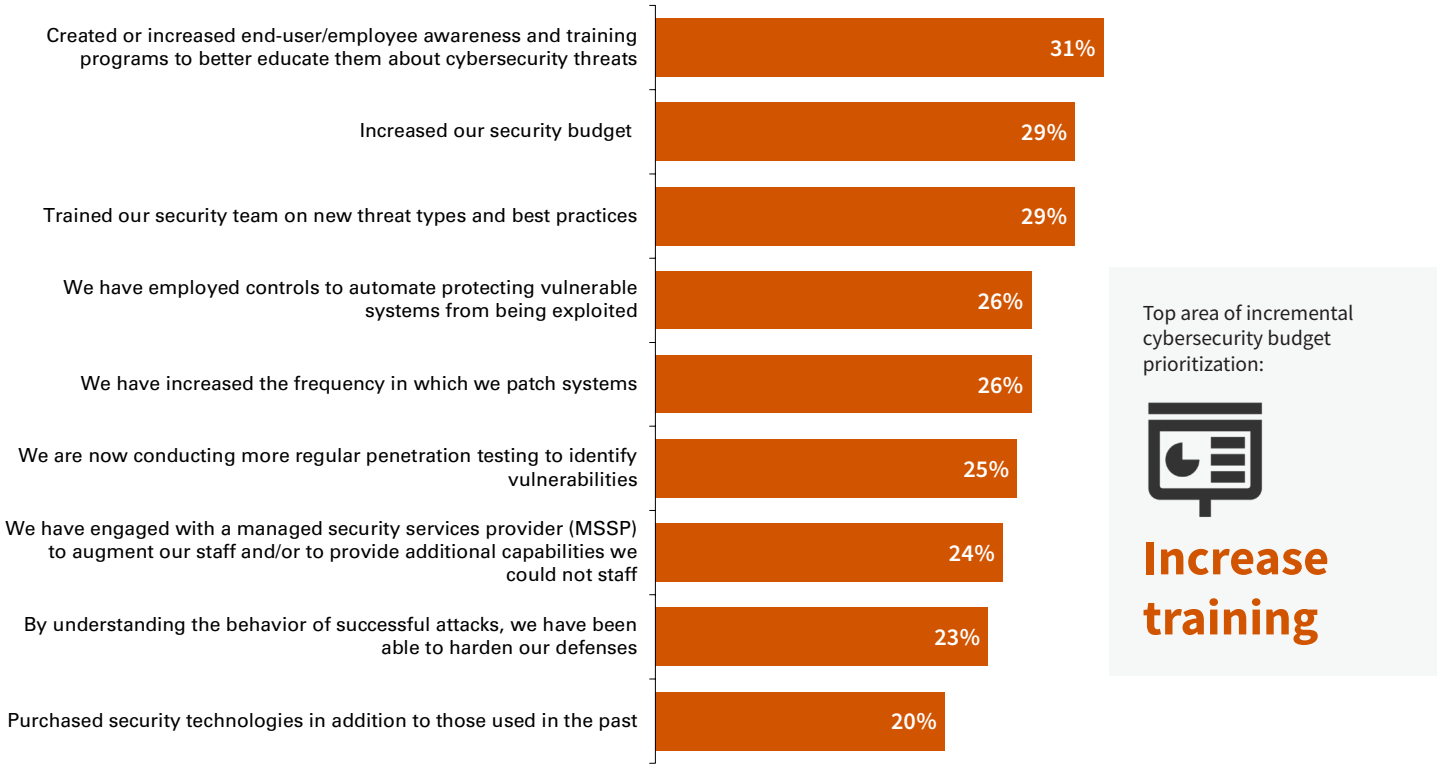
These best practices can be followed both for fully sanctioned cloud applications and services as well as for those that were unsanctioned, but are now being tolerated as a pragmatic approach to securing use of the cloud services.

Focus on End-user Awareness Training

Our research reveals that an approach that focuses on people and processes tends to deliver the most impactful results. When asked what actions have had the most positive impact on security in the last two years, respondents most often cite employee training programs for new threats (see Figure 18). In particular, the wave of phishing attacks over the past year illustrates the need for individual training on security hygiene so employees can be more adept at identifying phishing attempts. This research also highlights that the investment in people should include making security professionals more knowledgeable on the techniques, tactics, and tools employed by cyber adversaries.

Figure 18. Steps Taken to Improve Cybersecurity Posture

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=403, three responses accepted)

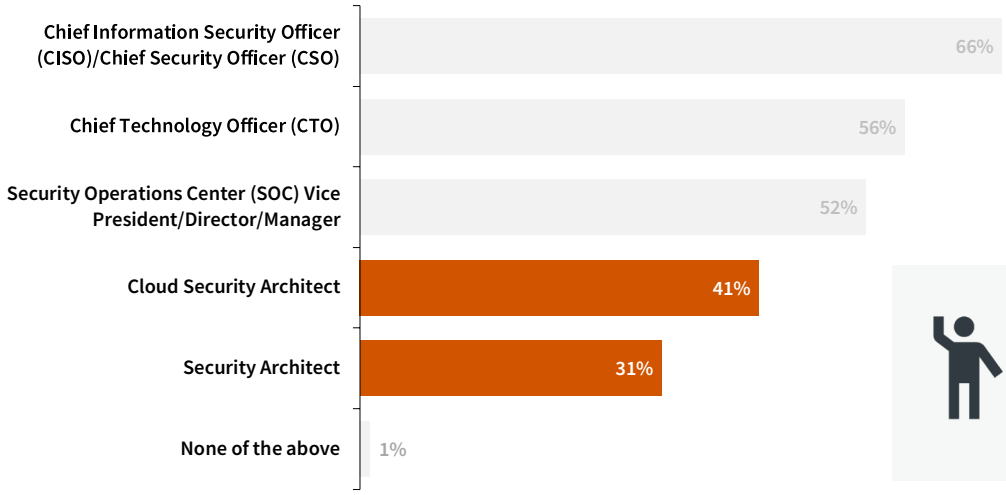


Spotlight: Retooling Cybersecurity Roles

The need to retool with a focus on people is evidenced by one of the notable findings of this research: the emergence of the cloud security architect. The fact that 41% of respondents say their organization now has a cloud security architect, compared with the 31% who have a security architect title, suggests that a new mindset has already set in (see Figure 19). The increasing prominence of the cloud security architect as a core member of new cloud security teams is indicative of the recognition for many organizations that the need to retool for the cloud means bringing on board not only individuals who can fill a technical skills gap, but also those who can strategically architect a cybersecurity strategy aligned with the speed of the cloud.

Figure 19. Common Cybersecurity Leadership Roles

Which of the following security leadership roles does your organization have? (Percent of respondents, N=450, multiple responses accepted)



More organizations have a dedicated **Cloud Security Architect** function than a traditional Security Architect

Dovetail Patching and Configuration Management

As cybersecurity exploits increase in technical sophistication and more workloads are deployed in public clouds, organizations should view patching and configuration management as two immutable practices to reduce their attack surface areas. As such, a coordinated patching and configuration management program is critical to effective server security—configuration management to close configuration vulnerabilities, and patching to close known software vulnerabilities. Our research reveals, however, that companies are taking different approaches to patching and configuration management.

> **A coordinated patching and configuration-management program is critical to effective server security.**

While patching is typically handled by IT operations, for some organizations, it can be ambiguous who owns patching responsibility between the IT and security teams. Regardless, a patching program should be designed using a risk-reduction perspective. For example, as new vulnerabilities become known, businesses should first investigate whether the specific vulnerabilities impact their more mission-critical systems, and whether any exploits in the wild are taking advantage of these vulnerabilities, and prioritize accordingly.

Even with such common-sense guidelines, patch and configuration management remains an uncertain discipline. Many organizations configure servers based on certified standard configuration benchmarks. But benchmarks can be moving targets, so organizations need to continuously assess and harden the configurations of the production systems. They may undertake patching as a result of periodic scanning for configuration and software vulnerabilities. The goal should be to operationalize patch management as part of an overall configuration management discipline that helps expedite patching of vulnerabilities based on risk assessment. Doing so can help businesses streamline a patching approach that reduces the risk that exploits pose to organizational assets.

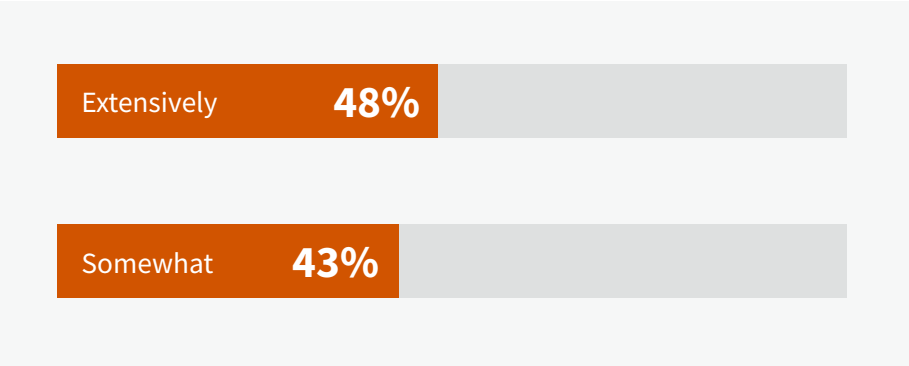
And that's critical because the scale of cloud computing can rapidly expand the attack surface, putting more assets at risk. Organizations with multi-cloud environments should consider cross-cloud patching strategies to ensure consistency of system integrity.

Secure Application Stacks with Defense-in-Depth

Businesses have been using detection and inspection technologies, such as network-based security controls and monitoring, for years. Now they are adopting emerging "defense-in-depth" tools that include User and Entity Behavior Analytics (UEBA) to detect anomalous activity, Endpoint Detection and Response (EDR), and deception technologies, which can help thwart cybercriminals. Our research indicates that a defense-in-depth approach also includes leveraging network performance monitoring (NPM) activity for breadth across horizontal attack surfaces as well as application performance monitoring (APM) depth for vertical visibility into the application stack. Our research reveals that many enterprises are, in fact, utilizing their NPM and APM solutions, with 48% doing so extensively to identify and analyze potential security threats and attacks (see Figure 20).

Figure 20. The Use of NPM and APM Tools for Cybersecurity Purposes

To what extent does your organization use network performance monitoring (NPM)/application performance monitoring (APM) tools and data to help identify and analyze potential security threats and attacks? (Percent of respondents, N=450)



"Our research indicates that a defense-in-depth approach also includes leveraging NPM and APM tools"...

The use of NPM and APM for cybersecurity use cases also fosters collaboration between IT operations management/Network Operations Center (NOC) teams who monitor network and application performance, and cybersecurity analysts in a Security Operations Center (SOC).

Figure 21. Collaboration Between NOC and SOC Teams

To what extent do your organization's NOC (Network Operations Center) and SOC (Security Operations Center) teams collaborate on cybersecurity matters? (Percent of respondents, N=450)

37%

Our NOC and SOC teams actively collaborate on defining network monitoring policies to detect threats and on the investigation and response to threats

24%

Our SOC team makes suggestions to our NOC team on network monitoring policies and they work together reactively to address cybersecurity incidents

17%

We have a single team that functions as both our NOC and SOC

Organizations that leverage feeds from their NOC into the SOC are gaining actionable visibility into security event activity related to utilization spikes across the network, including external connections that link remote sites. Such end-to-end network level visibility allows NOC and SOC teams to identify activity that could be indicative of a distributed denial of service (DDOS) or border gateway protocol (BGP) attack.

A broader and more holistic approach to monitoring includes leveraging APM solutions to track unusual underlying system activity. For example, the detection of anomalous CPU utilization, especially by a new and unknown process, can help detect the hijacking of systems enlisted for cryptomining operations.

These use cases highlight the compelling threat detection role NPM and APM solutions serve that enable NOC and SOC teams to protect their organizations from these and other types of attacks that put networks, applications, and data at risk.

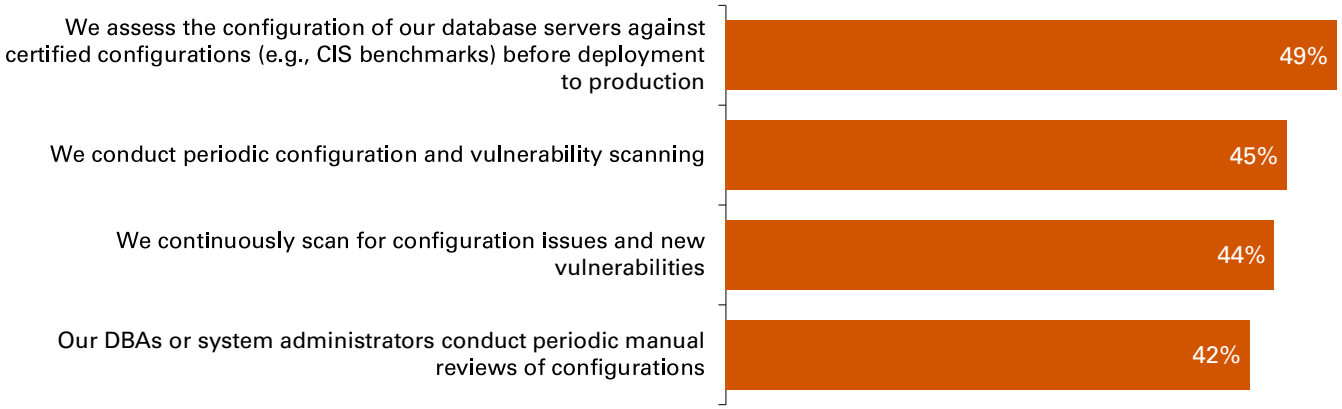
Secure the Database Tier with a Defense-in-depth Approach

Databases are foundational to business-critical apps. As such, a comprehensive database security strategy is essential to help reduce the attack surface, enforce access control policies, and perform 360-degree monitoring for anomalous behavior.

Database security begins with best practices for configuration management to reduce the attack surface area. Our research shows that, to achieve this, businesses assess their database servers against certified configurations, conduct periodic configuration and vulnerability scanning, and manually review configurations (see Figure 22).

Figure 22. Steps Taken to Ensure Proper Database Server Configuration

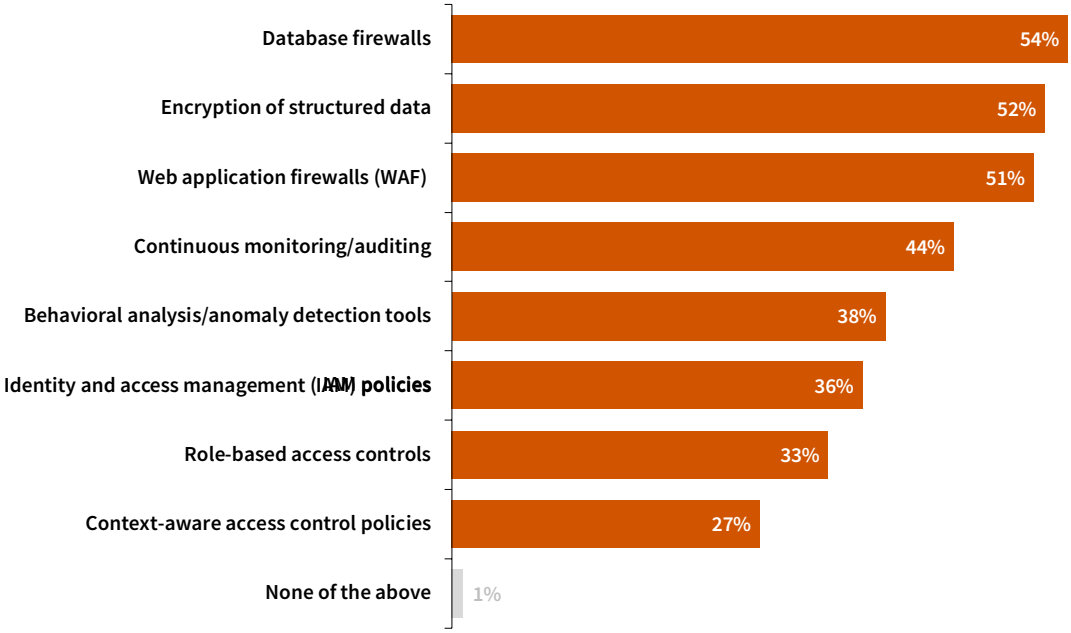
How does your organization ensure that its production database servers are properly configured? (Percent of respondents, N=450, multiple responses accepted)



Organizations are also protecting mission-critical databases through the use of access controls to help focus on people, and by extension, the application that is associated with the database. They do this through the use of database firewalls, encryption of structured data, application firewalls, and other controls (see Figure 23).

Figure 23. Security Technologies and Methods for Database Servers

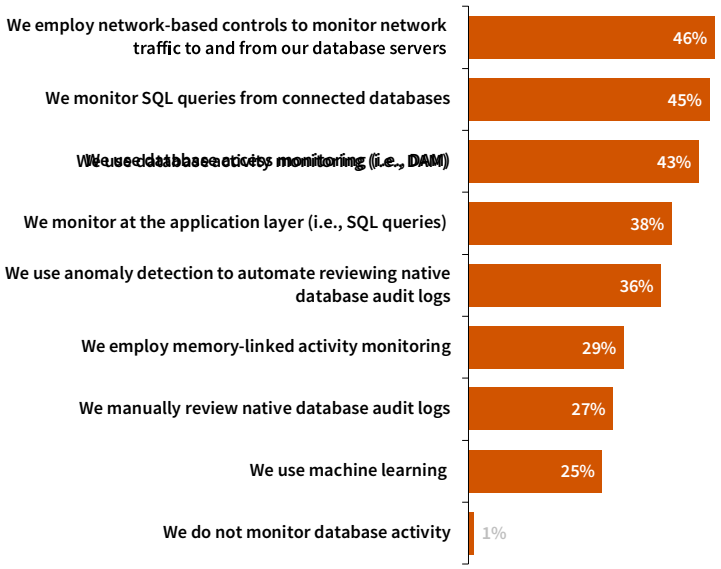
Which of the following technologies and methods does your organization use to prevent unauthorized access to your organization's sensitive and critical database servers? (Percent of respondents, N=450, multiple responses accepted)



Today's database security objectives extend beyond protecting against data loss to guarding against fraud and data corruption due to manipulation of systems. Multiple monitoring approaches can be used to mitigate such threats. Among survey respondents, the most common approaches include employing network tools to monitor traffic to and from database servers, monitoring of SQL queries from connected databases, and using database activity monitoring (see Figure 24).

Figure 24. Database Server Monitoring Approaches

How does your organization monitor its production database servers to detect suspicious activity? (Percent of respondents, N=450, multiple responses accepted)



Securing database servers is critical and is one of the essential cybersecurity best practices described in this section. The techniques outlined above offer a framework for how security teams and database administrators can collaborate to assure that database-resident assets are protected against unauthorized access, exfiltration, corruption, and other compromises. Going forward, the always-evolving array of cybersecurity best practices is likely to be altered by some very impactful new technologies. We now turn our attention to those.

6

Emerging Technologies Offer Hope for Improving Cybersecurity Outcomes

Technical advances on the fast approaching horizon are being utilized to improve cybersecurity outcomes.

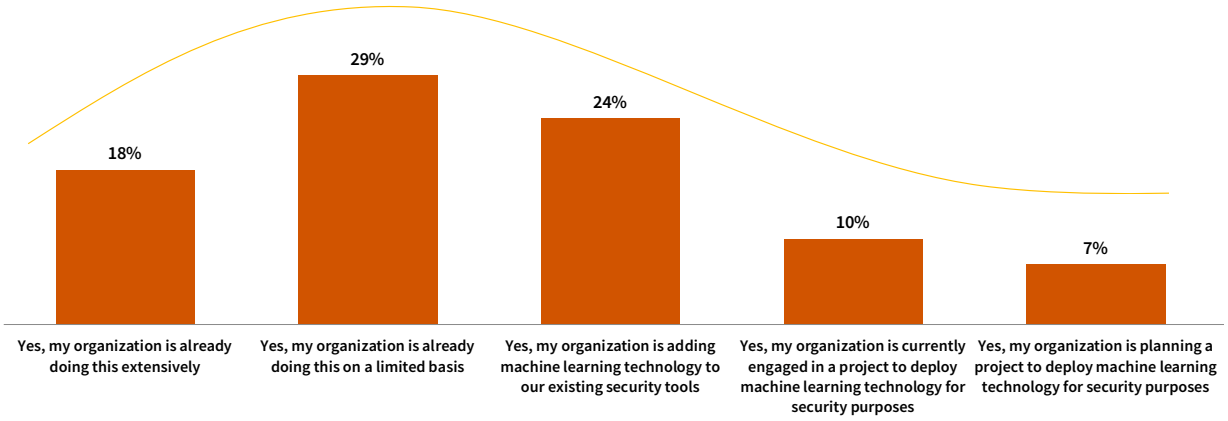
As organizations implement the security processes and technologies discussed in this report, it is worth noting that a number of highly promising new technologies are emerging. Historically, improving the efficacy of detecting and preventing threats and realizing greater operational efficiencies have often been mutually exclusive objectives. Machine learning and security automation are two technologies that offer potential to improve both of these outcomes simultaneously.

Machine Learning Promises to Improve Threat Protection Efficacy

Machine learning is already becoming a go-to cybersecurity technology to help identify zero-day threats. Machine learning employs models of behaviors and attributes as a mathematical basis for making predictions to identify new and previously unknown threats. While 29% of survey respondents are using machine learning on a limited basis, 18% say they do so extensively, and another 24% are now adding machine learning to existing security tools. Additionally, 27% of organizations are either currently deploying, planning to use, or interested in leveraging machine learning (see Figure 25). In total, that's a resounding endorsement of the role of machine learning as a foundational cybersecurity technology to improve the effectiveness of detecting and preventing threats.

Figure 25. The Use of Machine Learning for Cybersecurity

Has your organization deployed–or does it plan to deploy–machine learning technologies for cybersecurity purposes? (Percent of respondents, N=449)



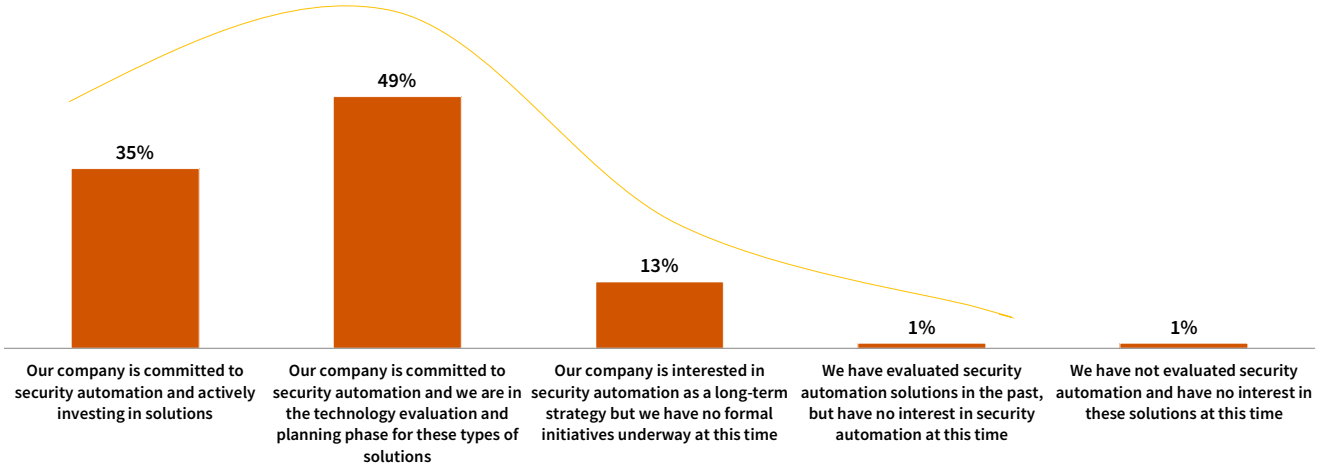
Machine learning is now being incorporated in a wide variety of cybersecurity controls to not only mitigate the threat posed by zero-day malware and exploits, but also to automate the analysis of the massive security event data sets many organizations struggle to analyze manually.

Security Automation Delivers Greater Operational Efficiencies

In the past, IT and cybersecurity professionals were often uncomfortable automating cybersecurity actions, including responding to alerts triaged by the SOC and updating firewall rules. Today, security automation is clearly viewed as a fundamental technology to efficiently respond to events and remediate weaknesses. In fact, almost half (49%) of respondents say they are currently evaluating and planning security automation; an additional 35% report they are actively investing in solutions (see Figure 26).

Figure 26. Companies Are Committed to Security Automation

How would you describe your organization's plans for/adoption of security automation solutions which automate remediation actions (e.g., updating firewall rules, quarantining an affected system, etc.)? (Percent of respondents, N=450)



In the context of many of the dynamics discussed in this paper, including the shortage of cybersecurity skills and increasingly complicated environments to be secured, automation promises to provide much-needed operational efficiencies and expedite closing security gaps.

On the Radar Screen: IoT

Identity challenges are quickly multiplying as the Internet of Things (IoT) expands the number of connected devices that store and share data across platforms and geographies. Already, according to ESG research, 25% of respondents say they have IoT initiatives under way, and an additional 43% plan to launch IoT projects within the next 12 to 24 months.[7] These deployments of connected devices will enable organizations to expand their products, services, and business models through the use of automation and telemetry delivered by sensor devices in the field, including at retail stores and at transportation hub kiosks.

As with the proliferation of cloud services, the build-out of IoT will increase risks by expanding the attack surface with the introduction of millions of connected devices that were not designed with strong cybersecurity in mind. The event telemetry these devices generate will further contribute to the challenge of processing security events discussed in this report.

[7] Source: ESG Master Survey Results, *2018 IT Spending Intentions Survey*, December 2017.

Back to Contents

IoT security starts with the IT and OT (Operational Technology) teams collaborating on making securing IoT devices a priority with the implementation of a set of best practices. IoT security best practices include:

- Profiling devices as part of an organization's onboarding process to assure no rogue devices are granted network access or permitted to set up shadow networks.
- Assuring only devices with approved configurations are allowed onto the network.
- Devices should be segmented when possible, and their outbound traffic monitored to detect hijacking from a botnet.
- Newer IoT devices should be vetted for adherence to security measures by the manufacturer to assure, for example, they do not include hard-coded passwords or ship with unsupported—and thus unpatchable—operating systems.

In Summary: Closing the Gap

Research conducted for the *Oracle and KPMG Cloud Threat Report, 2018* reveals a fundamental truth about protecting the cloud-enabled workplace: doing so is, indeed, a challenge of keeping pace at scale. We encourage the readers of this report to share with colleagues focused on these security and compliance challenges, and to engage with Oracle and KPMG for a strategic discussion on how to apply these best practices to secure today's cloud-enabled workplace.

The findings of this study also help define scale as a manifestation of multiple factors: the rate at which cloud services are being adopted, the diversity of the threat landscape, and the sheer volume of security event data that the expanded attack surface generates. We also learned that IT and cybersecurity leaders are meeting the challenge by not only funding cybersecurity initiatives, but also retooling their skills and approaches for the dynamics of today's IT model.

The adjustments being made to close the cloud security readiness gap span people, processes, and technologies with a focus on protecting critical applications—CRM, ERP, HCM—that enable business agility. With bad actors seeking to steal data, hijack CPU cycles to mine cryptocurrency, hold us hostage to extort monies, and disrupt business operations, cybersecurity professionals must be more vigilant than ever. Many of the proven best practices to prevent these threats need to be adapted to secure a perimeter that is now as much about users and data as it is about physical demarcations.

Adapting also requires aligning cybersecurity approaches with the reality of how cloud services are often consumed—user-led without adherence to policy. As such, the cybersecurity charter of protecting assets from compromise necessitates a willingness to move at the speed of the cloud. The emerging technologies discussed in this report—machine learning and security automation—promise to help cybersecurity teams be as agile as their line-of-business colleagues so they too can keep pace at scale.

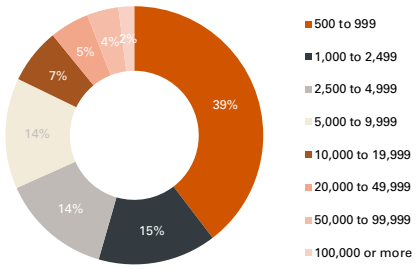
Appendix: Research Methodology and Demographics

The data presented in this report was collected via a comprehensive online survey conducted by Enterprise Strategy Group of 450 cybersecurity and IT professionals from private- and public-sector organizations in North America (United States and Canada), Western Europe (United Kingdom), and Asia (Australia, Singapore) between December 4, 2017 and January 10, 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.

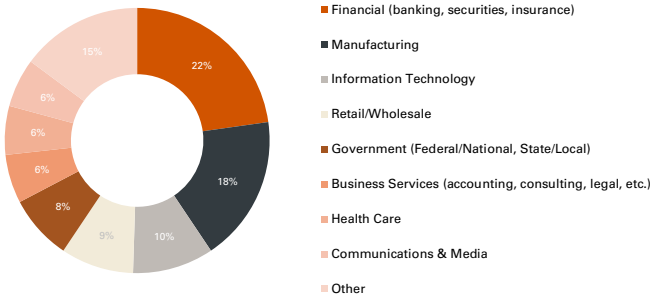
Note: Totals in figures and tables throughout this report may not add up to 100% due to rounding.

The following figures detail the demographics of the respondent organizations.

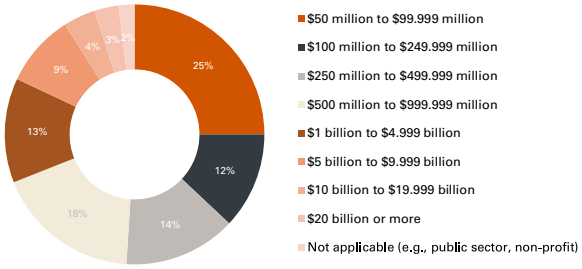
Respondent organizations by employees



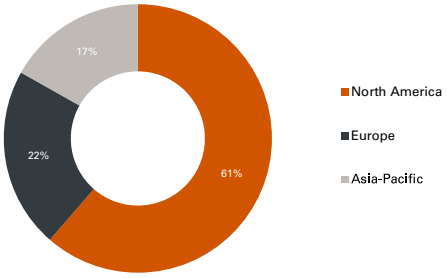
Respondent organizations by industry



Respondent organizations by annual revenue ($US)?



Respondent organizations by geographic region



Key Contributors

Mary Ann Davidson
Chief Security Officer – Oracle Corporation

Greg Jensen
Sr Principal Director Cloud Security Business – Oracle Corporation

Tony Buffomante
Principal – KPMG LLP

Laeeq Ahmed
Oracle Security & Controls Leader – KPMG LLP

Brian Jensen
Oracle Risk Consulting Sales Leader – KPMG LLP

Doug Cahill
Group Director and Senior Analyst – Enterprise Strategy Group

Special Thanks:
Akshay Bhargava, Suzanne Blackstock, Adam DeMattia, Troy Kitch, Mary Beth McCombs, John Hodson, James Finlaw, Peter Sinanian, Jennifer Gahm, Dan Koloski, Darren Calmen, Russ Lowenthal, Brendan Keane, Tim Stahl, Matt Flynn, Doug Madory, Sebastian Rovira, Josh McKibben, Rajan Behal, Eric Maurice, Sridar Karnam, Vidhi Desai