Making a secure transition to the public cloud

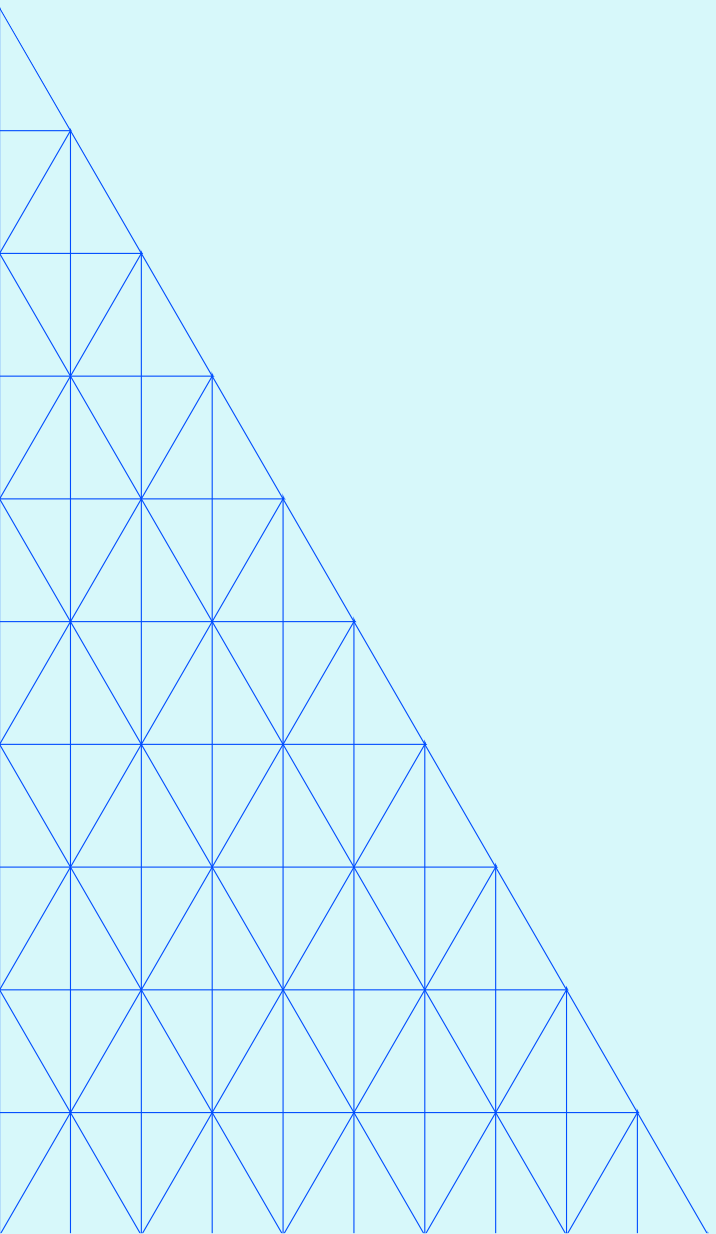
Arul Elumalai, James Kaplan, Mike Newborn, and Roger Roberts

Digital/McKinsey

Table of Contents

About the authors

Arul Elumalai and Roger Roberts are partners in the Silicon Valley office, James Kaplan is a partner in the New York office, and Mike Newborn is CISO for McKinsey Digital Labs in the Washington, DC, office.



Preface

Over recent years, cloud adoption has accelerated and a shift toward broader usage of public-cloud platforms has begun to build. This trend has made deploying and managing cloud-delivered technology solutions a far-reaching topic that touches every facet and function of an enterprise—not just the IT team. Today, business and technology executives are inundated by pitches and promises from vendors highlighting the value awaiting businesses that can integrate the cloud into their operations.

The reasons for the shift are straightforward. For many workloads and implementation scenarios, the public cloud offers more technical flexibility, simpler scaling, and lower operating costs. In response, many companies have altered their IT strategies to shift an increasing share of their applications and data to public cloud. However, using the public cloud disrupts traditional security models that many companies have built for years.

So, what cloud-security models are enterprises currently using as they consume public-cloud services, and what are the trade-offs for each model? What are cloud-security best practices, and how are these different from what enterprises are doing today?

To answer these questions, McKinsey conducted new research with cybersecurity executives at almost 100 companies, looking at factors such as barriers to cloud adoption, the steps enterprises are taking to safeguard their data in the public cloud, and how their cybersecurity choices affect the pace of the cloud adoption.

This report features the survey results as well as analysis and insights from executives and from our experience working with enterprise clients around the world on these issues. Our findings suggest a path forward for enterprises intent on capturing the benefits of the public cloud while ensuring that cybersecurity efforts adequately mitigate evolving risks.

We would like to acknowledge Yash Agrawal, Rich Cracknell, Srikanth Dola, Lisa Donchak, Matias Garibaldi, Dan Guo, James Manyika, Brent Smolinski, and Adam Tyra for their contributions to this article. We also wish to thank the security team at Google Cloud and the more than 100 security executives who shared their experiences and perspectives, without which this report would not have been possible.

Section

01

Public-cloud adoption and implications for cybersecurity

Companies are becoming more open to the public cloud, but using the public cloud disrupts traditional cybersecurity models.

After a long period of experimentation, leading enterprises are getting serious about adopting the public cloud at scale. Over the past several years, many companies have altered their IT strategies to shift an increasing share of their applications and data to public-cloud infrastructure and platforms.[1] As recently as three years ago, large enterprises were reluctant to move to the public cloud. They remained skeptical of public-cloud platforms due in large part to security and regulatory compliance concerns. In addition, many had spent significant time and resources building private-cloud platforms in-house and were typically not ready to jettison them, focusing instead on how to improve utilization of these assets.

Why move to the public cloud?

The reasons for executives' change of heart are straightforward. For many workloads and implementation scenarios, the public cloud offers more technical flexibility, faster scaling, and lower operating costs than on-premises servers or private cloud platforms. On flexibility and scaling, the major cloud-service providers (CSPs) now offer a wide range of cloud products and services across infrastructure, application platforms, application development and maintenance (ADM) tools, infrastructure management, and consulting. In addition, the number of third-party applications has exploded. Companies eyeing a move to the public cloud can take advantage of these solutions and applications to smooth the transition and support their operations.

Lower costs are another important benefit. Companies can reduce their operating costs by transitioning selected activities that deliver a lower total cost of ownership (TCO) in the public cloud. The amount of savings isn't a straightforward calculation, however; instead, costs can be highly variable, complex, and dependent on workload. For example, TCO of a server instance on the public cloud can be substantially lower than that of an on-premises server. However, TCO can rise significantly as large server instances are deployed to support computing-intensive workloads or the volume of data stored on the public cloud increases. Data transfer fees can also cause the TCO to increase dramatically for some data-intensive workloads.

Cybersecurity challenges

Despite the public cloud's agility and flexibility benefits, considerations around security have held companies back from migrating to the public cloud at the scale initially predicted. However, our research shows that chief information security officers (CISOs) have moved beyond the question, "Is the cloud secure?" In many cases they acknowledge that CSPs' security resources dwarf their own. Accordingly, CISOs are now asking how they can adopt cloud services in a secure way, given that many of their existing security practices and architectures may be less effective in the cloud. Using the public cloud disrupts traditional cybersecurity[2] models that many companies have built up over years. Cybersecurity technologies for on-premises IT systems, such as identity and access management (IAM) and data loss prevention, are unlikely to work as intended unless they are reconfigured to function effectively in the public cloud. Companies that have workloads with multiple CSPs must often reconfigure their IAM solution across multiple environments and invest additional resources to build a single universal directory to support access across hybrid environments.

Enterprises are still gaining an understanding of the shared responsibility model for cybersecurity. In this critical area, companies that lack the technical understanding to identify necessary actions and determine the level of CSP support can leave themselves more vulnerable to cyberattacks. Multiple parties—CSPs, tool vendors, managed-security-service providers (MSSPs)—jointly have a role in ensuring the security of data in the public

1 By cybersecurity this report refers to the full set of business and technology actions required to manage the risks associated with threats to the confidentiality, integrity, and availability of systems and information. Some organizations may refer to this function as information security or IT security.

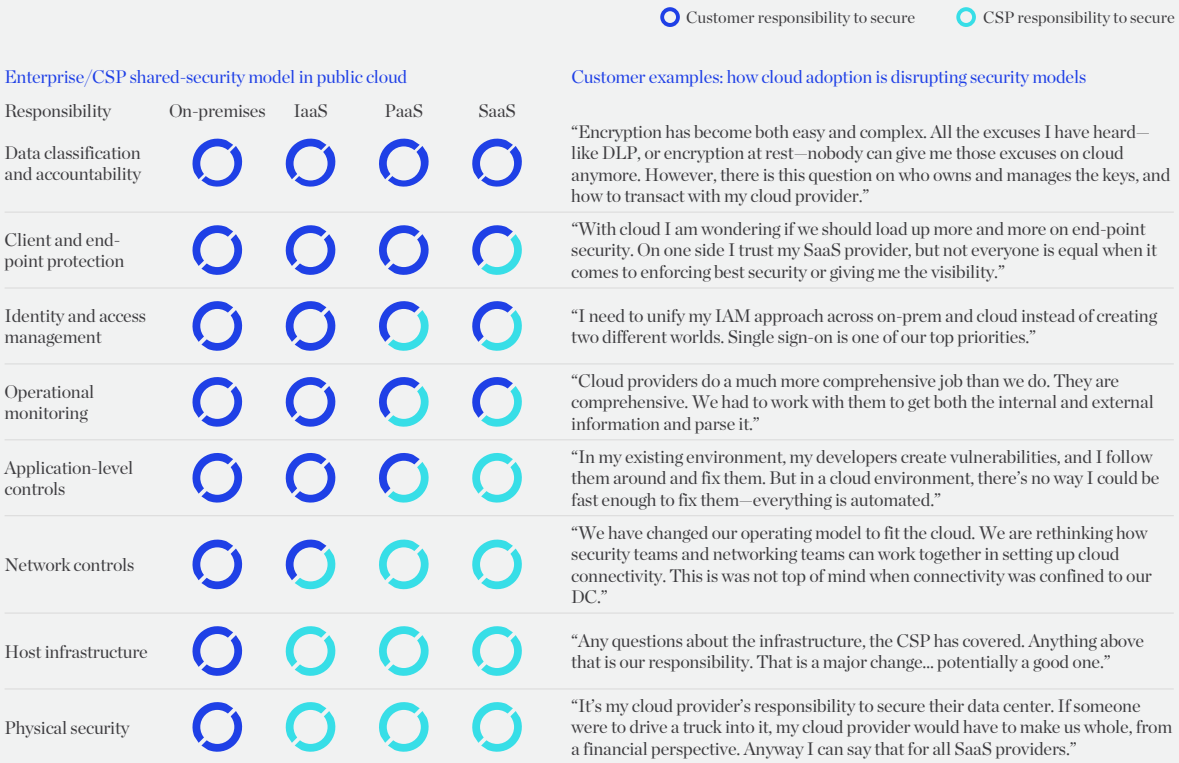
2 For more, see Nagendra Bommadevara, James Kaplan, and Irina Starikova, "Leaders and laggards in enterprise cloud infrastructure adoption," October 2016, McKinsey.com. Also see Arul Elumalai, Kara Sprague, Sid Tandon, and Lareina Yee, "Ten trends redefining enterprise IT infrastructure," November 2017, McKinsey.com, which primarily addresses the impact of infrastructure as a service (IaaS) and platform as a service (PaaS), rather than software as a service (SaaS).

cloud. Certain areas, such as IAM, operational monitoring, and application-level controls, can be particularly challenging, since responsibility is shared by the CSP, third-party solution providers, and the enterprise (Exhibit 1). One executive, for example, said, "I need to unify my IAM approach across on-premises and cloud instead of creating two different worlds. Single sign-on is one of our top priorities."

In such situations, tighter integration is needed across on-premises and public-cloud solutions. This model can complicate security for certain types of enterprises if they are unclear on the delineation of responsibilities between themselves (the tenant) and the CSP. In the face of such lack of understanding, many companies have chosen to stick with on-premises servers or private cloud despite the potential benefits of the public cloud. In a few other cases, respondents agreed that CSPs have better security expertise than their own, but challenges in understanding the shared responsibility model have prevented them from making the shift to public cloud. Embarking on a cloud migration inevitably forces companies to reexamine their own activities and, in some cases, become more comfortable with relying on CSPs for security. It requires companies to have a clear understanding of the division of responsibilities between themselves and the CSP—as one executive explained, "The CSP has the infrastructure covered. Anything above that is our responsibility. That is a major change."

Exhibit 1

Enterprise conversations showed that they are unclear about the shared responsibility model.



SOURCE: McKinsey global cloud cybersecurity research, 2017

A seemingly continual stream of major security breaches, where attackers are increasingly scanning for vulnerabilities and mistakes in user configurations, has also ratcheted up fears among executives—and adopting the public cloud can magnify some types of risk. For example, the speed and flexibility that cloud services provide to developers can, without appropriate configuration governance, lead to insufficiently protected environments, as a number of companies have already discovered to their embarrassment. In many of the high-profile breaches, misconfigured storage bucket settings were a common vulnerability, highlighting the need for enterprises to have the necessary in-house knowledge and capabilities to manage security in the public cloud.

CSPs offer a robust selection of security solutions and enablers, and the rollout of new technologies is simplified by the centralized nature of the public cloud. CSPs are also constantly evolving their security offerings to stay abreast of threats, and continuously refreshing the features and controls offered to tenants. Hence, enterprises are assured that they are getting the latest, most effective solutions. Moreover, there is safety in numbers—because cloud tenants share security responsibilities with the CSP, this potentially provides an additional pool of expertise to help secure the environment: the lessons from the experiences of one tenant are easily propagated to others, helping CSPs to learn and adapt their controls and operating model to benefit all.

Section

02

Securely consuming public-cloud services

Companies need bold, comprehensive strategies for public-cloud cybersecurity.

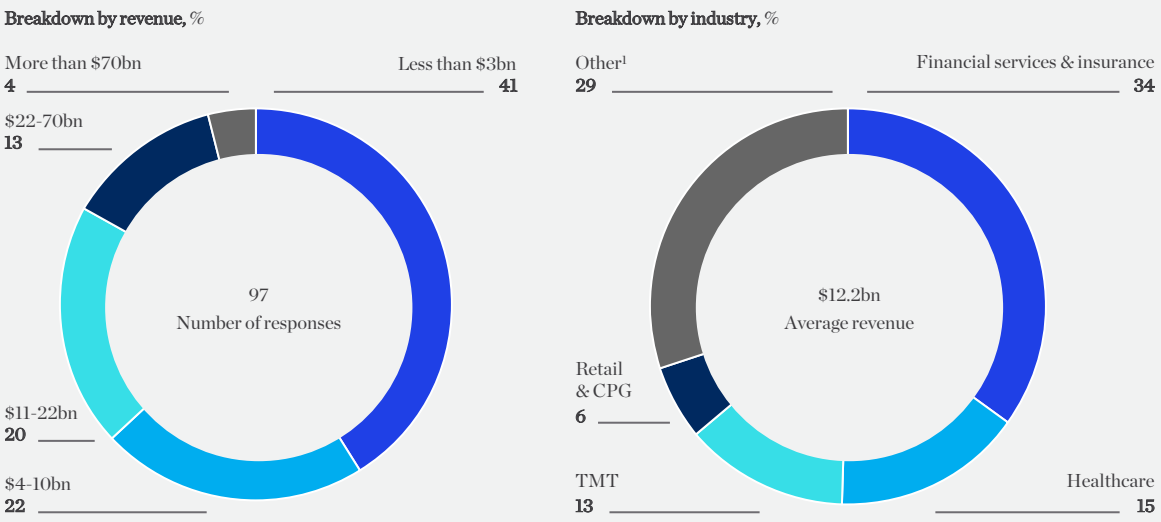
Although the public cloud is top of mind for many executives, the enterprises they work for show significant variation in their level of planned cloud adoption and the measures they are taking to prepare. McKinsey conducted research showing that companies have a high level of uncertainty about cloud security, so they are experimenting with a range of strategies and architectures (see sidebar, "About the research").

About the research

McKinsey conducted multiple rounds of interviews with cybersecurity executives at 97 enterprises across industries, including financial services and insurance; healthcare; retail and consumer packaged goods; and technology, media, and telecommunications to understand how organizations are approaching the public cloud (exhibit). The executives hailed from companies with a wide range of annual revenues. This research focused on four areas of cloud security: (1) customers' perceptions of security in a cloud environment and how it affects their security approach, (2) security models that enterprises are currently using in consuming public cloud, (3) cloud security best practices and how they differ from reality, and (4) gaps in the marketplace and how enterprises and CSPs can collaborate to address them. From these interviews, we identified trends and common challenges in cloud security and used them as a basis to develop perspectives. The survey and interviews were conducted from August to November 2017.

Exhibit

McKinsey interviewed approximately 100 enterprises about their cloud and cloud-security practices.



1 Other includes pharmaceuticals and medical products, aerospace and defense, advanced electronics, travel, and energy.

SOURCE: McKinsey global cloud cybersecurity research, 2017

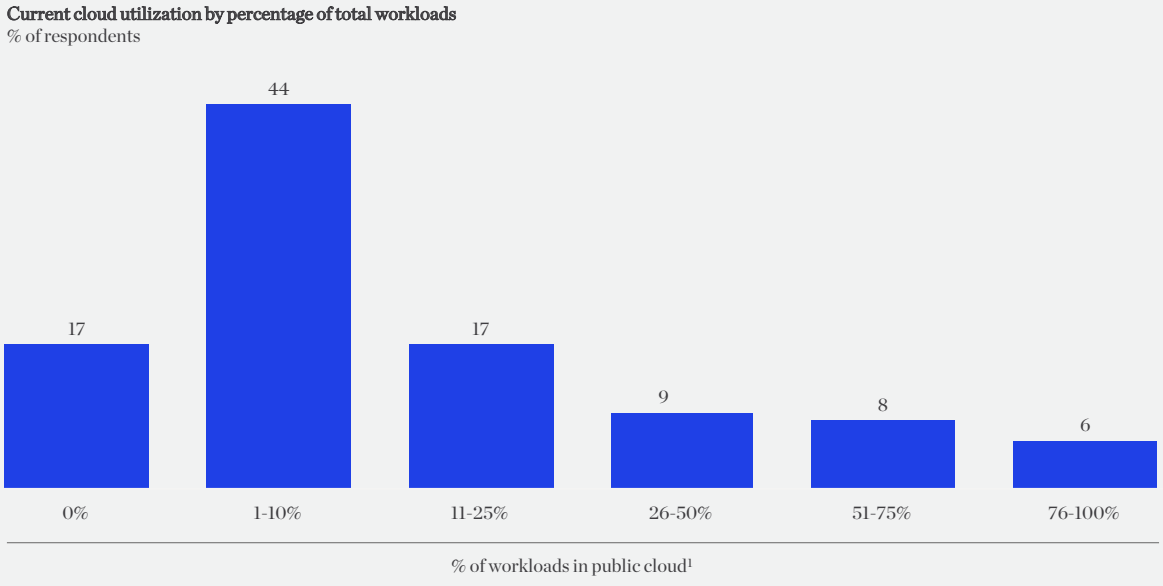
Public-cloud adoption trends

Enterprises are currently not only at different states in their adoption of the public cloud but also differ significantly in their aspirations for the future. More than three-quarters of survey respondents have yet to migrate the majority of their business activities to the public-cloud platforms. Overall, though, enterprises expect to double their cloud adoption in three years, from the current 19 percent of workloads (measured by the number of server instances running in public cloud) to 38 percent in the next 3 years.

Fewer than 15 percent of organizations had more than half of their workloads in the cloud, and they benefit from sophisticated security teams to guide the migration (Exhibit 2). One financial services executive said, "80 to 85 percent of our risk calculations occur in the cloud. In three years, 95 percent will be in the public cloud. The only things that won't be out are those for which it doesn't make financial sense." A subset of this category, five organizations, have more than 75 percent of their workloads in the cloud thanks in large part to a lack of legacy on-premises infrastructure to migrate.

Exhibit 2

Enterprises are at different states of cloud migration, with most organizations yet to migrate the majority of their workloads to the public cloud.



1 Measured as a percentage of server instances in the public cloud.

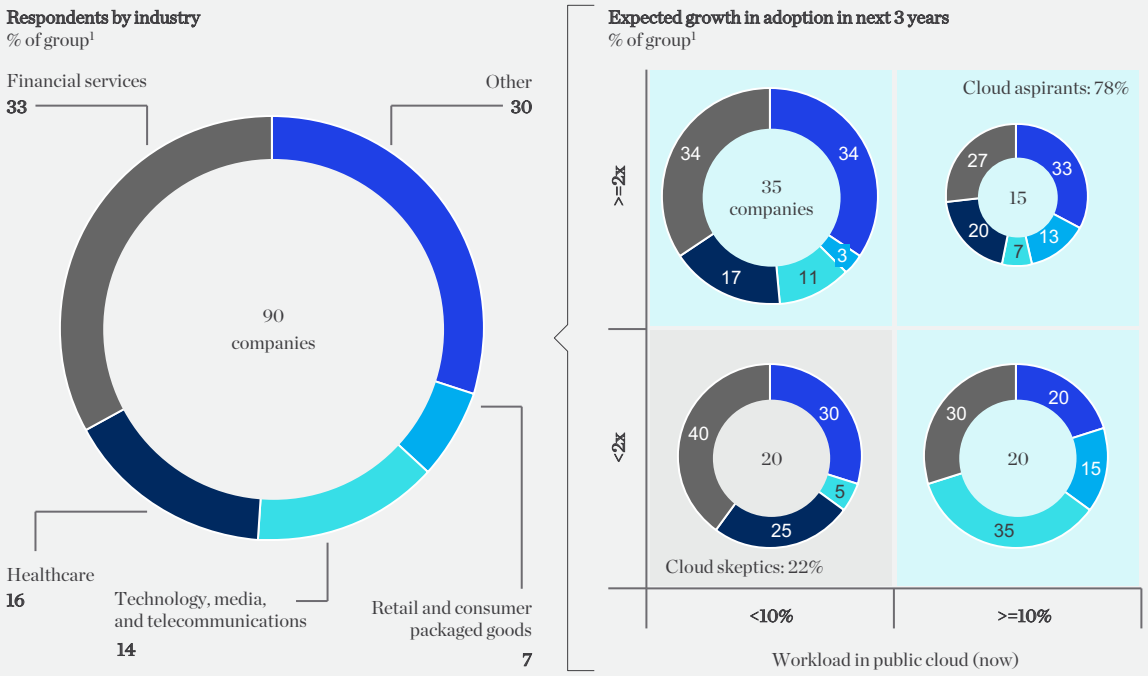
SOURCE: McKinsey global cloud cybersecurity research, 2017

Despite adoption of the public cloud being limited to date, the outlook for the future is markedly different. Today, just 40 percent of the companies we studied have more than 10 percent of their workloads on public-cloud platforms; within three years 80 percent plan either to have shifted over 10 percent of their workloads to public-cloud platforms or to double their cloud penetration. We refer to these companies as "cloud aspirants" (Exhibit 3).

For example, an insurance executive articulated his company's ambitions: "We see a future where it is almost complete cloud. There will always be a component of on-premises stuff, but I see more than 90 percent migration." Cloud aspirants have concluded that the public cloud offers more technical flexibility and simpler scaling for many workloads and implementation scenarios. In some cases, using the public cloud also reduces IT operating costs.

Exhibit 3

Cloud aspirants: Nearly 80 percent of companies plan to have 10 percent or more of their workloads in the public cloud or double their public-cloud use within three years.



1 Percentages may not sum to 100% due to rounding.

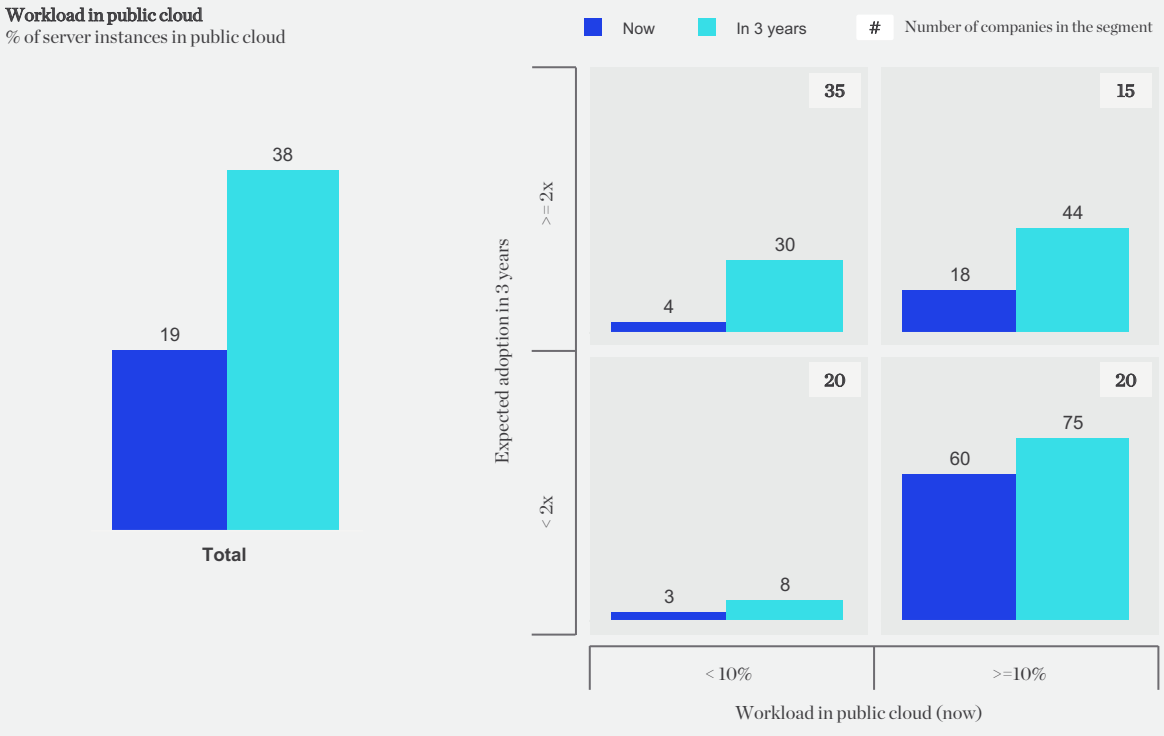
SOURCE: McKinsey global cloud cybersecurity research, 2017

In contrast, cloud skeptics (20 percent of respondents) reported that their enterprises have no plans to migrate activities to the public cloud at any scale. These enterprises have fewer than 10 percent of server instances running in the public cloud today and don't plan to change that share materially in the next three years. In most cases, the approach was influenced by a perceived lack of economic benefits. This category's approach was aptly summed up by one executive: "We have a pretty mature operating environment for how we manage and scale on-premises infrastructure, and translating those practices to a cloud provider is a pretty heavy investment that economically does not make sense for us."

Companies in every segment plan to increase their workload in the cloud, albeit to varying degrees. More than three-quarters of enterprises expect to at least double their use of the cloud in the medium term (Exhibit 4).

Exhibit 4

Overall, cloud adoption is expected to double over the next three years.



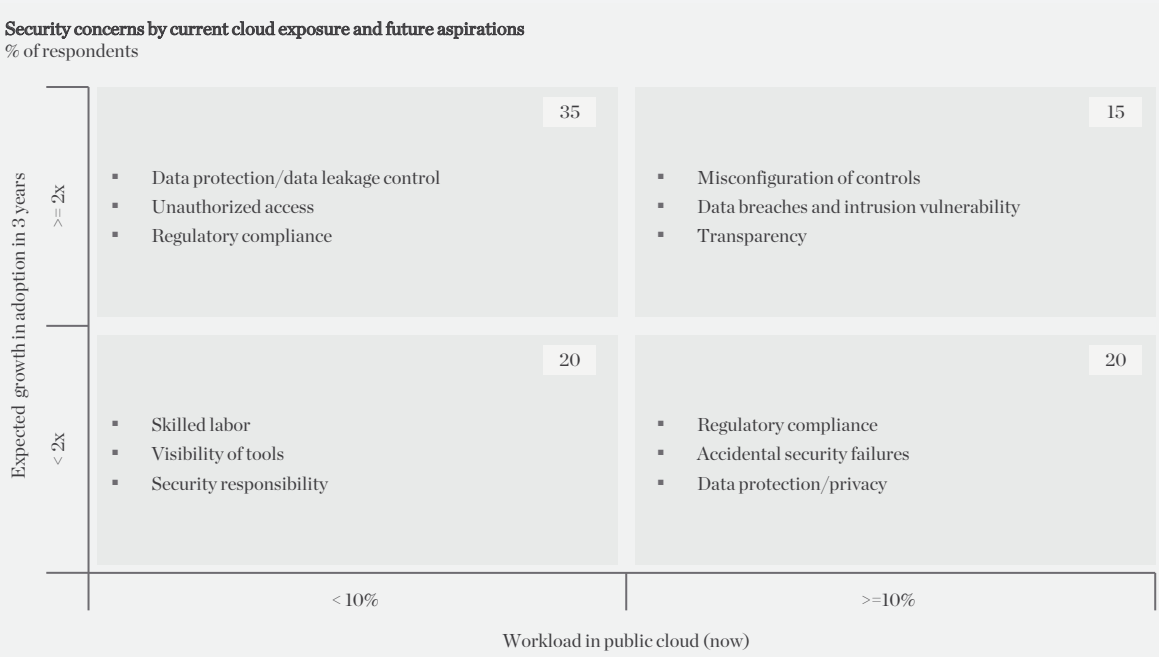
SOURCE: McKinsey global cloud cybersecurity research, 2017

Each category also identified different pressing issues based on their organization's capabilities (Exhibit 5). Cloud aspirants are more focused on CSP capabilities, with misconfiguration of controls, data breaches and intrusion vulnerabilities, and transparency being the key concerns. Meanwhile, the main barrier faced by cloud skeptics is a lack of organizational capabilities to support migration to the public cloud. Key shortcomings include a shortage of skilled labor to support migrations, the need for greater visibility into CSP tools, and lack of clarity around the shared responsibility model.

In short, what many enterprises need is a bold, creative, and comprehensive approach to adapt their cybersecurity strategy for the public cloud. Instead of trying to force-fit existing on-premises models to the public cloud, wrestling with the ambiguity around security responsibilities, or being constrained by fears of user errors and misconfiguration risks, enterprises are likely to benefit from taking a methodical approach to

Exhibit 5

Cloud skeptics identified lack of expertise as their main challenge, while cloud aspirants identified regulatory compliance.



SOURCE: McKinsey global cloud cybersecurity research, 2017

cybersecurity implementation—and evolving their operating model to support public-cloud adoption aligned to their overall cloud strategy. In many cases, the solution could include a mix of public- and private-cloud environments.

Enterprises can accelerate their move to the public cloud and the advantages it affords by focusing on four interrelated practices for cloud cybersecurity. Granted, every enterprise has its own unique needs and capabilities, so the best solutions must be tailored to the specific situation. That said, the following four practices offer a solid foundation for executives looking to develop and implement public-cloud cybersecurity strategies:

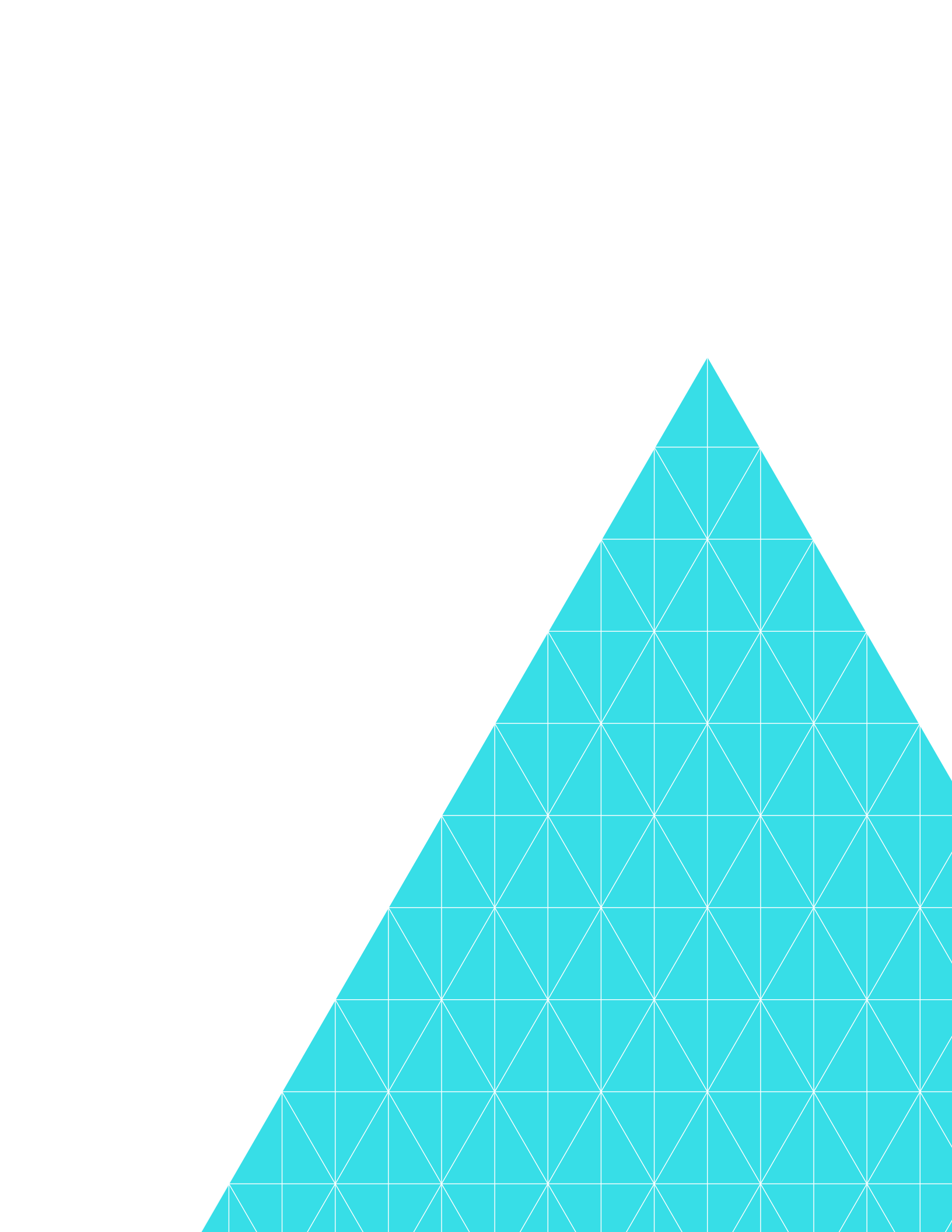
1. Developing a cloud-centric security model. In the hybrid-cloud/multicloud world, simply extending on-premises security controls to the public cloud will probably prove insufficient. Companies need to make choices about how to manage their perimeter in the cloud and how much they will rearchitect applications in a way that aligns with their risk tolerance, existing application architecture, available resources, and overall cloud strategy.

2. Redesigning the full set of cybersecurity controls for the public cloud. With their perimeter-design and application-architecture choices in place, companies can design controls. Security implementation can be defined as a combination of eight control areas: identity and access management, data security, perimeter security, operational monitoring and response, application security, hardware security, end-point security, and regulatory governance. Organizations have a choice of determining the level of security needed for control in each of these areas, selecting the control's location and provider, and tailoring implementation to fit the choice of archetype and the data or application needs. For each individual control, companies need to determine who should provide it and how rigorous it needs to be.

3. Clarifying internal responsibilities for cybersecurity versus what providers will do. Public cloud requires a shared security model, with providers and their customers each responsible for specific functions. Companies need to understand this split of responsibilities—it will look very different from a traditional outsourcing arrangement—and redesign internal processes accordingly. By working closely with CSPs, enterprises can gain better visibility and transparency into the security operating models to design and configure controls for multicloud deployments in a way that integrates with other tools, processing, and operating models.

4. Applying DevOps to cybersecurity. The public cloud offers developers unprecedented flexibility and scale, but too often traditional approaches to architecture and application design slow down the pace of migration and erode these advantages. Enterprises must therefore ensure that security processes support the application development velocity that public cloud offers. Enterprises need to develop a security DevOps model, which seeks to establish a more agile relationship between development and IT operations. This model makes security a core component of each step of the life cycle for application development and deployment.

The remainder of this report describes these four steps in greater depth, in order to provide guidance as companies position themselves to capture more value from public-cloud architectures and as they modernize their operating models to take full advantage of the possibilities that the technology offers.



Section

03

Developing a cloud-centric cybersecurity model

Companies need to make choices about how to manage their perimeter in the cloud and how much they will rearchitect applications in a way that aligns with their risk tolerance, existing application architecture, available resources, and overall cloud strategy.

For a company that has just begun to use the public cloud, it can be tempting to build a cybersecurity model using the controls it already has in place for on-premises systems. This approach can lead to problems, since on-premises controls seldom work for public-cloud platforms without being reconfigured. Even after taking this step, such controls won't provide visibility and protection across all workloads and cloud platforms. Recognizing this limitation in relation to on-premises controls, cloud aspirants are experimenting with a range of security strategies and architectures.

Enterprises intent on embracing the public cloud in coming years have developed a variety of approaches to protect their applications and data. The most effective approach, based on the experience of cloud aspirants, is to assess the company's cybersecurity model across two dimensions: how the perimeter is defined, and whether applications need to be rearchitected for the public cloud. The definition of the perimeter determines the topology and the boundary for the cloud cybersecurity model; choices regarding application rearchitecture guide the incorporation of security controls within the applications. These two dimensions also influence one another: for example, a company might opt to make its applications highly secure by adding security features that minimize the exposure of sensitive data during processing and making no assumptions about the security controls that are applied to a given environment.

Choosing a model for perimeter security

Enterprises that have favored on-premises servers or the private cloud have traditionally invested heavily in securing the perimeter; however, the transition to the public cloud necessitates a comprehensive reexamination of how to manage security across multiple environments. In this respect, the perimeter is the primary factor that influences cybersecurity approaches. Our analysis finds that among cloud aspirants, the following three models for perimeter security design stand out (Exhibit 6).

Exhibit 6

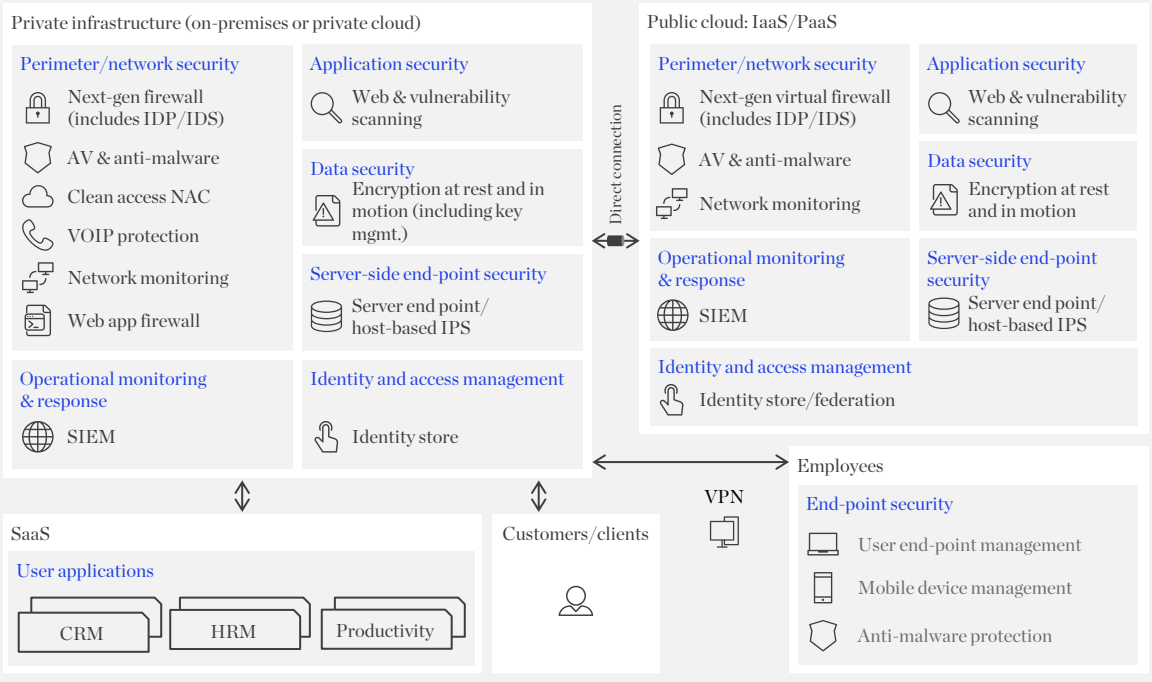
Architecture options: Three models for perimeter architecture stand out among cloud-aspirant companies.

Backhauling

In a backhaul architecture, the only external gateway to the public cloud is through private infrastructure, so when users want access to applications or data, they must go through their private cloud or on-premises data center, which reroutes the access to the public cloud: for example, through a virtual private network (VPN) connection or direct access supported by the CSP (Exhibit 7). This model provides the ability to use familiar controls with minimal need to learn new cloud-native controls. Organizations indicate decreased risk of misconfiguration by using familiar controls (often by routing most traffic to on-premises). Additionally, backhauling enables easier monitoring of traffic to the cloud providing better transparency and ease of debugging. The model also reduces time to full cloud implementation by alleviating the need to reconfigure all existing architecture. A backhaul strategy is a good fit for enterprises that lack cloud expertise, have a high level of comfort with and confidence in their security controls implementation in the private environment, or whose workloads are primarily accessed by internal users. Enterprises that are not adopting a multivendor strategy for CSPs are prime candidates for backhaul. As a result, these enterprises typically extend their on-premises controls to the cloud. However, one potential trade-off is that the model doesn't fully capture cloud benefits such as scalability. User experience is also likely to suffer due to potentially higher latency (versus using the cloud as intended), since network traffic is routed via on-premises infrastructure rather than directly to and from the cloud platform. Moreover, increased operational costs—possibly 20 to 30 percent higher—are likely to result from maintaining conflicting operating models concurrently in the on-premises environment and in the public cloud. Backhauling is how half of cloud aspirants manage perimeter security, but it might not remain popular for long: just 11 percent of cloud aspirants said they are likely to use the backhaul model three years from now.

Exhibit 7

Archetype: Backhauling public-cloud workloads through private infrastructure – Example architecture



Adopting CSP-provided controls by default

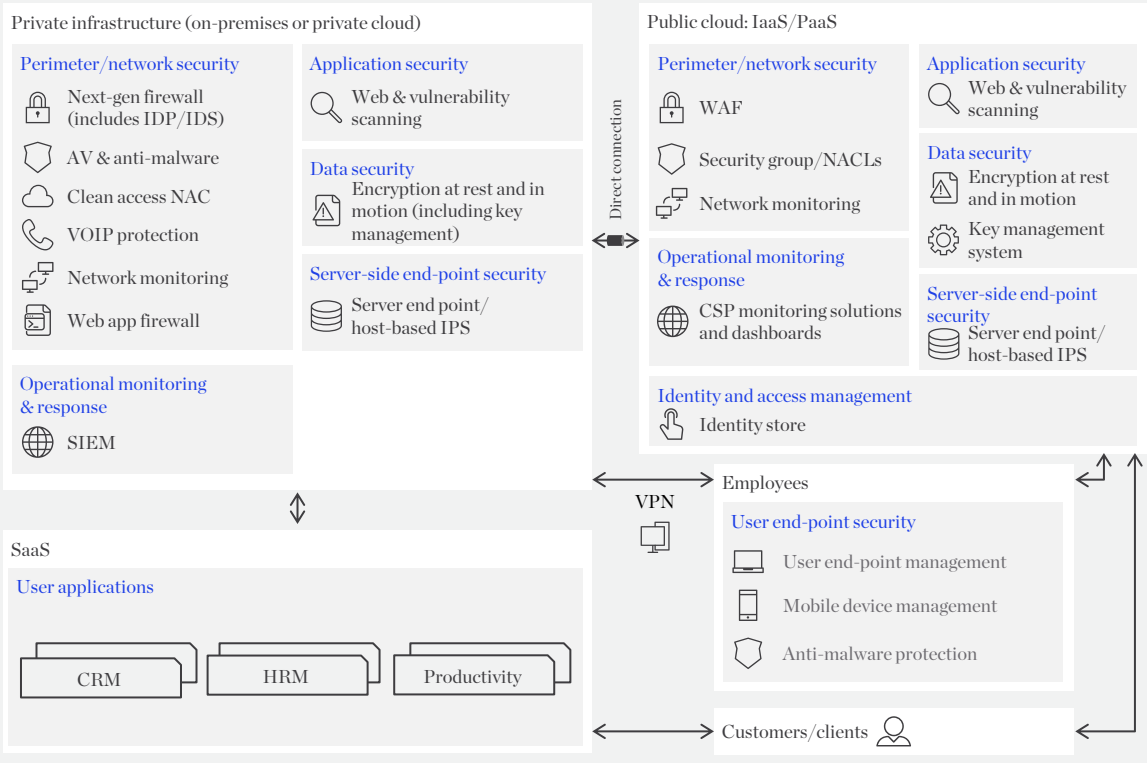
Enterprises might elect to cede responsibility for security to CSPs, an effective approach in scenarios where the CSP offers robust controls or the organization lacks the resources or expertise to design its own. In this approach, enterprises have the flexibility to rely on the CSP to manage security controls just for the public cloud while maintaining their separate security controls for on-premises workloads. CSP-provided controls are typically the lowest-cost option for workloads, and having a single source for security controls lowers complexity and potentially also cost. In addition, a large CSP can provide better services and controls than those that many small and midsize enterprises can develop on their own. Enterprises that have workloads with multiple CSPs are also candidates for this security perimeter approach (Exhibit 8). Overall, this model is the lowest-cost approach, as no additional investment is needed to use CSP-provided controls. At the same time, enterprises also see improved compatibility between controls and the platform: a CSP-provided control will work best on its own platform (compared with enterprise- or third-party–provided controls in the same cloud environment).

However, enterprises that fail to understand the limitations of CSP controls may create gaps. Additionally, CSPs may not offer the full set of controls needed to address the risk factors related to each workload or the needed flexibility to customize the controls to the unique requirements and constraints of an enterprise. This is because the CSP determines what security levers the institution can choose to implement. Moreover, the risk of misconfiguration can rise if in-house staff ignore CSP recommendations.

This model is the choice of 36 percent of cloud aspirants. For larger and more sophisticated organizations, defaulting to CSP-provided controls appears to be a temporary measure: 27 percent of cloud aspirants say they will use this model in three years (down from 36 percent today).

Exhibit 8

Archetype: Adopting CSP controls by default – Example architecture



Relying on CSP-provided controls

After two costly years getting ready for a move to the public cloud, an investment management company decided that default CSP controls were the most secure option. CSPs offer microservices that enable incredible agility on the public cloud, provide dependable customer service, and store keys in a cloud-provided key management service. In the company's view, the CSP controls are only vulnerable when misconfigurations create security loopholes. This security architecture has allowed the company to meet its ultimate goal of having more agile infrastructure. One executive noted, "The marriage of cloud and services means we can quickly spin up infrastructure to handle surges in the number of transactions without needing to scale up an entire application in a secure manner every time, because it is standard in the CSP environment." Satisfied with the experience thus far, the company aims to have up to 50 percent of its workloads in the public cloud by 2020.

Cleansheeting

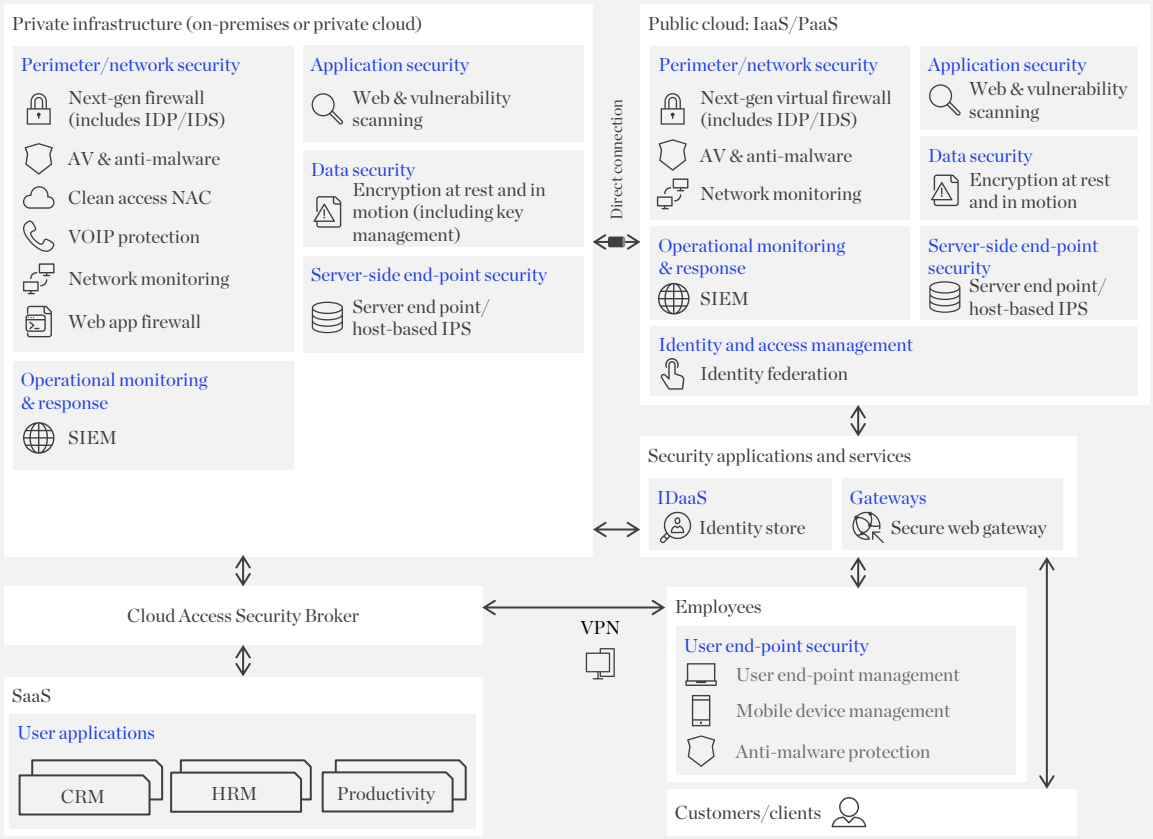
This involves designing a "virtual perimeter" and developing cloud-specific controls from solutions offered by various external providers. In this approach, enterprises evaluate and select multiple third-party security controls for public cloud as well as private infrastructure. The enterprise shares responsibility for the security perimeter with CSPs and third-party providers, which offer services that sit between an organization's on-premises infrastructure and a CSP's infrastructure. Enterprises that choose cleansheeting maintain the flexibility to replace point solutions as needs evolve without being tied to a certain vendor or product. Since changing solutions creates technical demands, companies typically practice cleansheeting when they have enough in-house cybersecurity expertise to select vendors and integrate their solutions.

Cleansheeting gives enterprises the option to harness multiple solutions for control and visibility as well as the ability to meet required security levels and assurances. User experience is enhanced in many cases because enterprises can select the best fit (for example, single sign-on and the option to support multiple device platforms) for their needs. Cleansheet architecture has the greatest opportunity to transform and modernize security operating models and is most likely to produce comprehensive and effective security controls. (Exhibit 9).

As noted, however, cleansheeting requires deep expertise in cybersecurity and cloud architectures; furthermore, its increased complexity and sophistication can result in higher security costs. The model requires a highly complex IT setup resulting from multiple vendor interdependencies and relationship management, so organizations without this capability may have to seek expertise and support from an MSSP. Used by some 15 percent of cloud aspirants, this approach enables companies to apply the best perimeter security solutions they can find and switch them in and out as needed. Although cleansheeting can slow down the migration of workloads into the cloud, this approach appears to be on the rise, with 47 percent of cloud aspirants saying they will use cloud-specific controls in the next three years.

Exhibit 9

Archetype: Cleansheeting – Example architecture



A progressive outlook on perimeter-security design

A pharmaceutical company is currently using backhauling as a stepping-stone with the intention of moving to cleansheeting in the near future. Its ultimate goal is to run on the public cloud with third-party tools. However, with so many on-premises applications and services, the process will take time, so the company has decided to make the move incrementally. During the migration process, the company is not worrying about its underlying architecture, since it has used a container strategy to develop its applications. The eventual move to cleansheeting reflects its belief that CSPs and third-party tools produce more secure technology than the firm can on its own. It values the shared responsibility of CSPs for security, though it plans to explore third-party tools that extend beyond default CSP capabilities.

Deciding whether to rearchitect applications for the cloud

The second choice that defines a company's cybersecurity posture is whether to rearchitect applications for the public cloud, by rewriting code or altering application architectures (or both). Just 27 percent of the executives we interviewed said their enterprise has taken this step. The benefits of rearchitecting applications are enhancing compatibility with CSP platforms to improve manageability (via container architectures, for example), stronger security (with changes such as encrypting data flows between calls), superior performance (for example, by allowing "horizontal scaling" in the public cloud) and lower operating costs (because application remediation and app-level security reduce the need for a company to choose the most expansive security solutions with a wide range of features and capabilities). However, the process of rearchitecting applications for the cloud can slow down a company's migration rate. Consequently, a large majority of enterprises—78 percent—migrate applications without rearchitecting them for public cloud.

Security rearchitecture approaches come in multiple forms to improve security (for example, implement encryption,or modify code to prevent SQL injection.) Organizations are also changing their application development process to improve security practices through code review, application scanning, penetration testing against apps and source code, cloud app scanning and regular penetration testing, vulnerability assessment, and automated patch scheduling.

Enterprises that have developed apps for on-premises or private cloud and who have not taken steps to assure workload mobility, face a dilemma: take the additional time and resources to optimize them for the public cloud or forgo this step and simply lift and shift the on-premises apps into the public cloud—potentially creating security risks or impeding performance. These choices and their rationales are explored in more detail in the following sections.

Defining six archetypes for public-cloud security

The choice of perimeter-security design, along with the choice about whether to adapt applications to the public cloud, create six archetypes for cloud cybersecurity (Exhibit 10). Backhaulers that rearchitect applications for the cloud and those using native CSP controls without rearchitecting applications are the two largest segments. Backhauling extends existing controls that companies are already familiar with to public-cloud implementations. Using default CSP controls is the simplest and most cost-effective approach. Cleansheeting controls calls for substantial security expertise but provides flexibility and support for multiple clouds. Organizations can use these criteria to choose the appropriate methods based on their specific needs.

Exhibit 10

Cloud aspirants can be divided into six archetypes based on their approach to application rearchitecture and implementing the security perimeter.

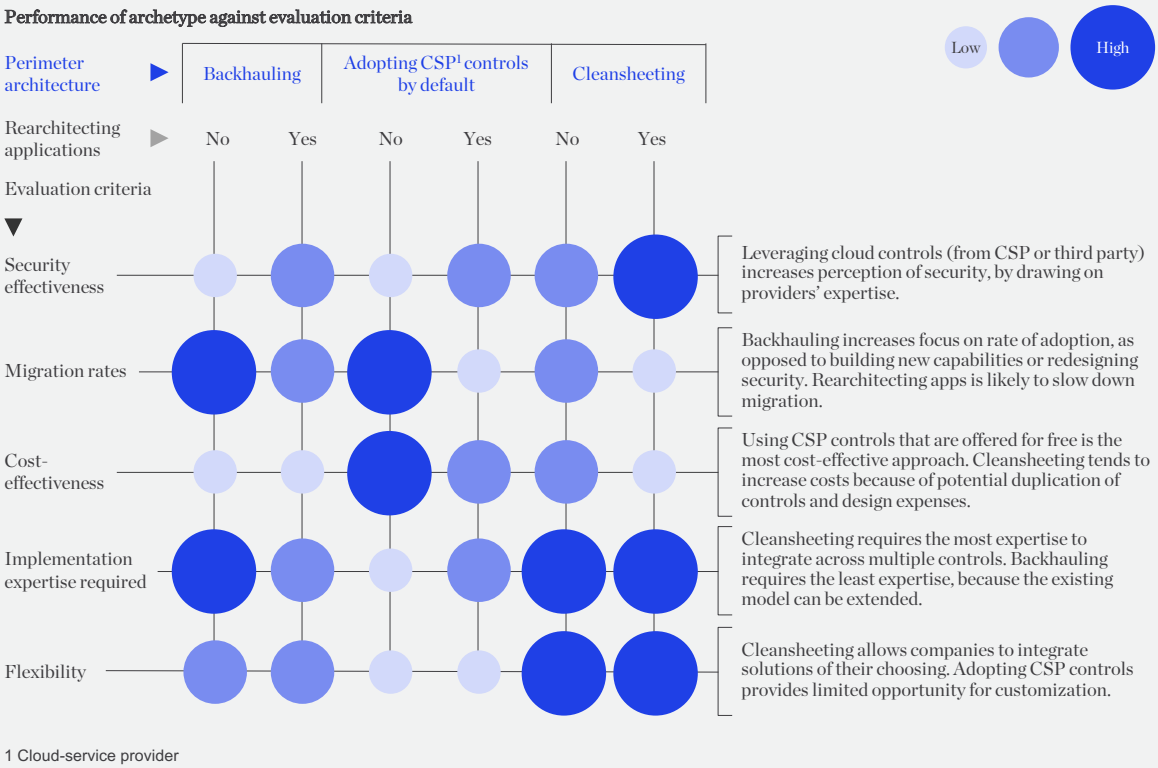
SOURCE: McKinsey global cloud cybersecurity research, 2017

Select your archetype early

Choosing the right model for cloud security depends on a number of internal and external factors. However, organizations need not confine themselves to a single archetype; instead, they can choose to classify applications and pick a different archetype based on workload. It is possible—even advantageous—to use different archetypes for applications with different requirements: for example, backhauling with a single CSP for a core transaction system to enable faster migration and familiar controls, while using CSP-provided security controls for low-cost, accelerated deployment of new customer-facing applications. In our experience, five primary criteria inform enterprises' decisions about their overall cloud-cybersecurity model: perception of security effectiveness, their desired cloud migration rate, their willingness to pay additional security costs, their expertise implementing new security programs, and the flexibility they desire from their security architectures (Exhibit 11).

Exhibit 11

Assessing architectures: Cloud-cybersecurity models generally follow six archetypes, which are defined by their designs for perimeter and application architectures.

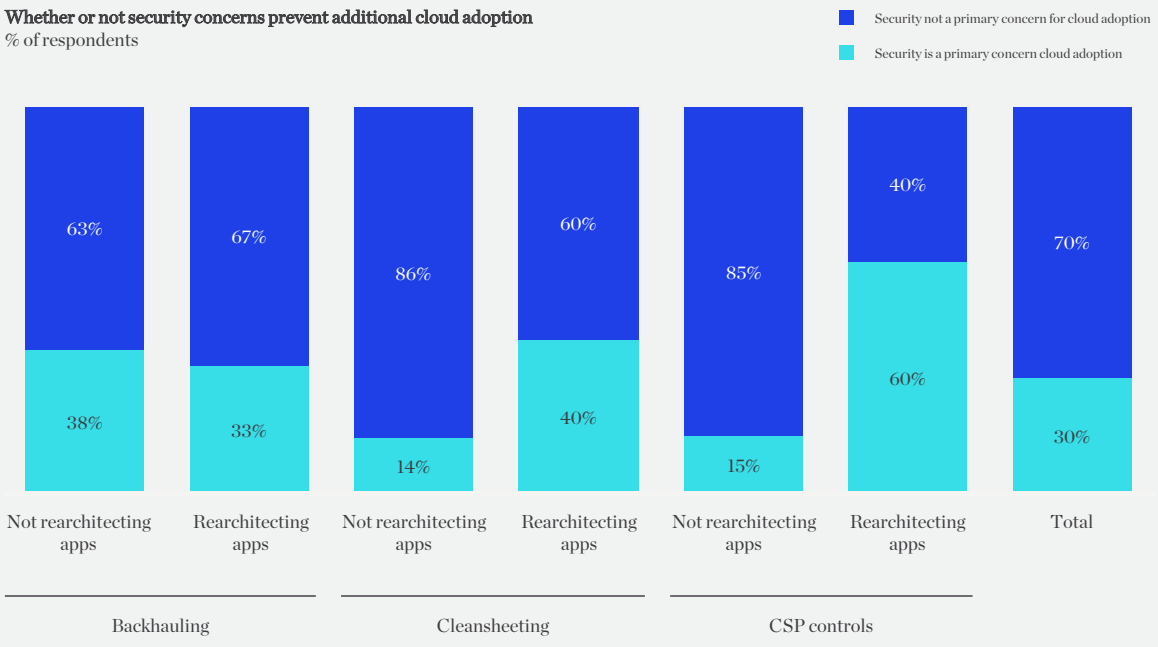


1 Cloud-service provider

Security effectiveness. Typically, enterprises with a heightened awareness of security issues redesign their security perimeter using a combination of public-cloud and third-party controls. Their reliance on CSP or third-party controls reflects a perception of greater confidence in providers' expertise and security controls. According to the survey, enterprises that chose both to use CSP security controls and rearchitect apps as an additional layer of protection indicated that they viewed security as an important concern and an obstacle to cloud adoption. This thorough approach to cloud security could thus be perceived as a necessary formula for addressing existing security concerns. By contrast, more than 85 percent of companies, which chose a cleansheet or CSP-default approach and did not rearchitect their apps, were not concerned about security as a barrier to migration because their greater knowledge and sophistication about the controls increased their trust in third-party providers (Exhibit 12).

Exhibit 12

Enterprises pursuing a cleansheeting strategy or using native CSP controls were rarely worried that security would slow cloud progress.

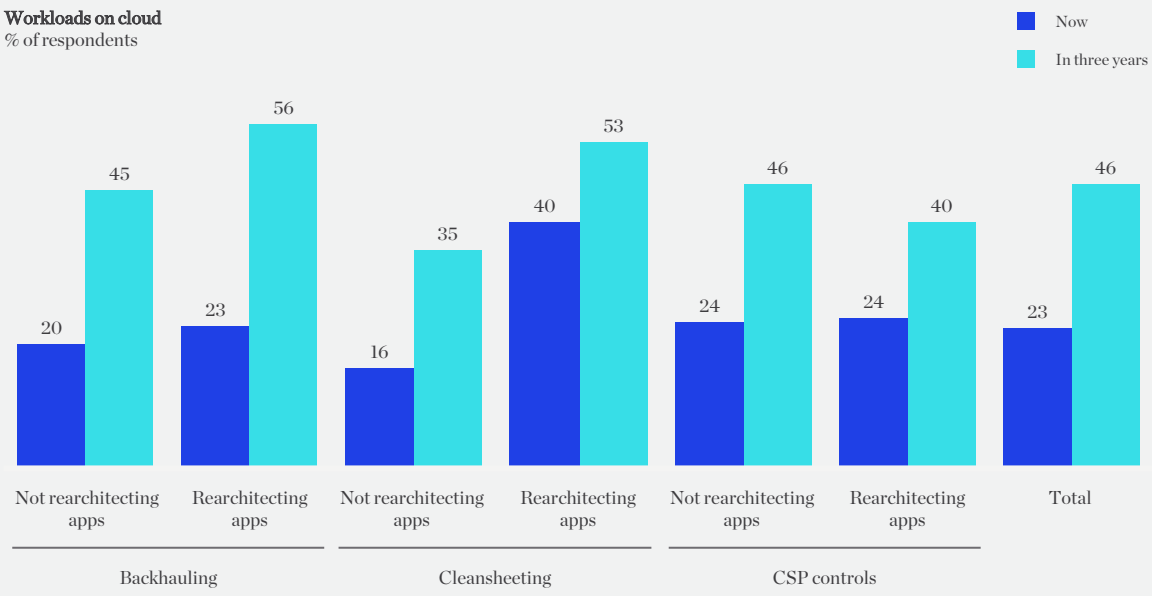


SOURCE: McKinsey global cloud cybersecurity research, 2017

Migration rates. Overall, cloud adoption among aspirants is set to double, rising from 23 percent today to 46 percent in the next three years (Exhibit 13). Within this group, enterprises that choose to maintain a private security perimeter and backhaul will have the highest relative increase in cloud adoption over the next three years. These organizations plan to move a higher percentage of workloads to the cloud than other cloud aspirants, a reflection of their familiarity and confidence in their on-premises security controls. Enterprises that default to CSP controls without rearchitecting apps also report a higher portion of their workloads migrating to the cloud than their counterparts, as these enterprises focus on cloud adoption over redesigning security controls or implementation.

Exhibit 13

Enterprises which backhaul today by routing traffic through their data centers are likely to see the highest growth in public-cloud adoption.

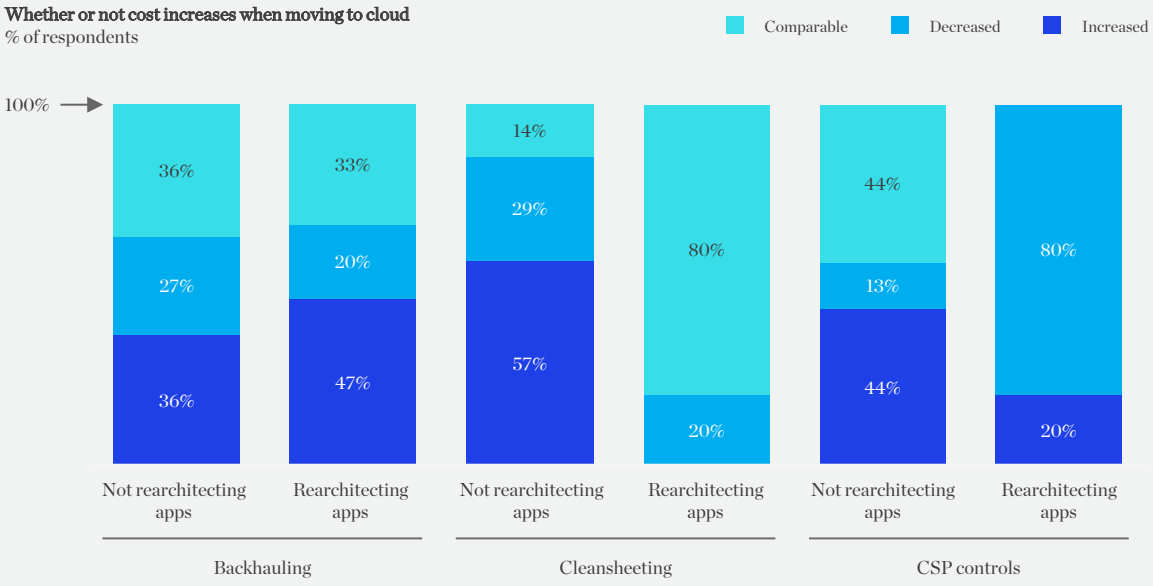


SOURCE: McKinsey global cloud cybersecurity research, 2017

Cost-effectiveness. Each archetype's TCO can fluctuate based on choices around perimeter security and app design. For example, 80 percent of enterprises using native CSP security controls while rearchitecting apps in parallel reported a decrease in security operating expenses (Exhibit 14). Although rearchitecting apps slows the pace of cloud migration, this step likely helps to keep costs low: tenants can take advantage of free or low-cost controls provided by CSPs, which are aggressively investing in updated controls. Hence, any increased investment in application rearchitecture to improve the security can be offset by the economies that enterprises gain from the free and native security controls that CSPs offer.

Exhibit 14

Enterprises see a decrease in security operating expenses when using native CSP controls and rearchitecting apps in parallel.



SOURCE: McKinsey global cloud cybersecurity research, 2017

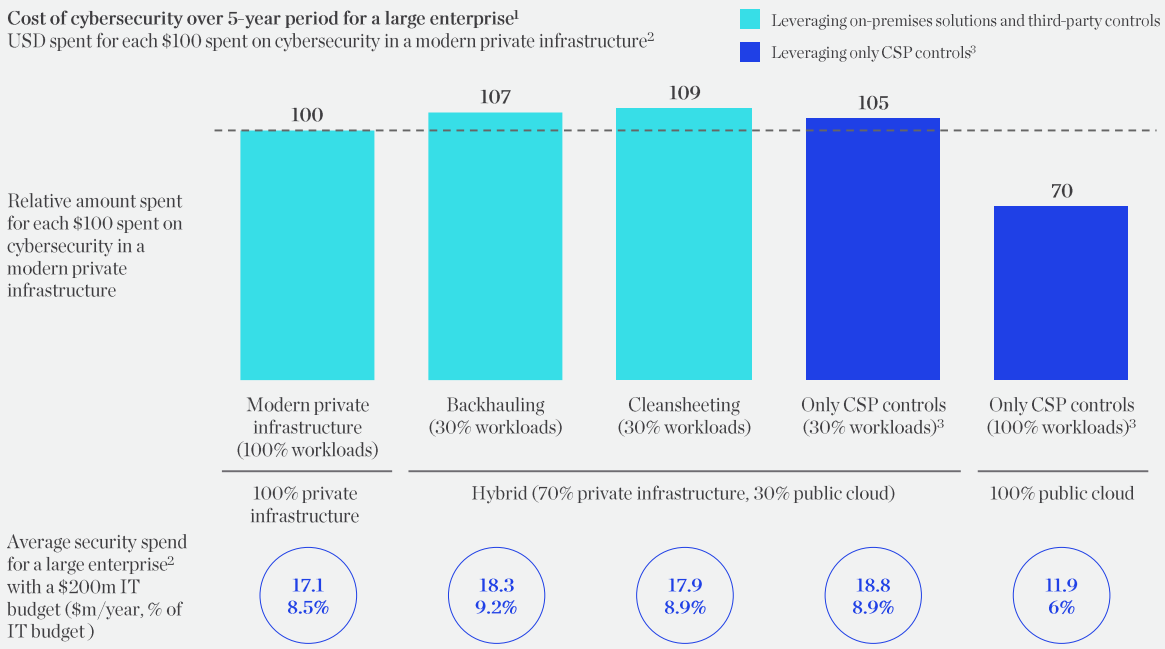
The economics of cloud security

The magnitude of available cost savings reinforces the implications of security perimeter choices and the lure of defaulting to CSP controls (exhibit). An enterprise with an annual IT budget of $200 million that relies on CSP-provided controls for security, for example, would spend on average $11.9 million a year on security—saving more than $5 million a year compared with private infrastructure (assuming that the enterprise has all its workloads on the public cloud). Maintaining a hybrid security architecture (one that draws on both public-cloud and on-premises controls) would also have cost benefits but at a reduced scale due to continued on-premises security costs. As organizations move more and more applications to the public cloud and lean toward using native CSP controls, a decrease in security operating and capital expenditure costs is likely. Of course, in the current threat environment CISOs are likely to reinvest this savings "dividend" to address other rising priorities (for example, end-user training and anti-phishing campaigns).

However, organizations should carefully evaluate the security offerings of different cloud players and go beyond just economics to make the right choices. Clearly, understanding the offerings of CSPs and third parties, including the gaps, is critical since variations are likely to exist across providers.

Exhibit

Costs of implementing cybersecurity

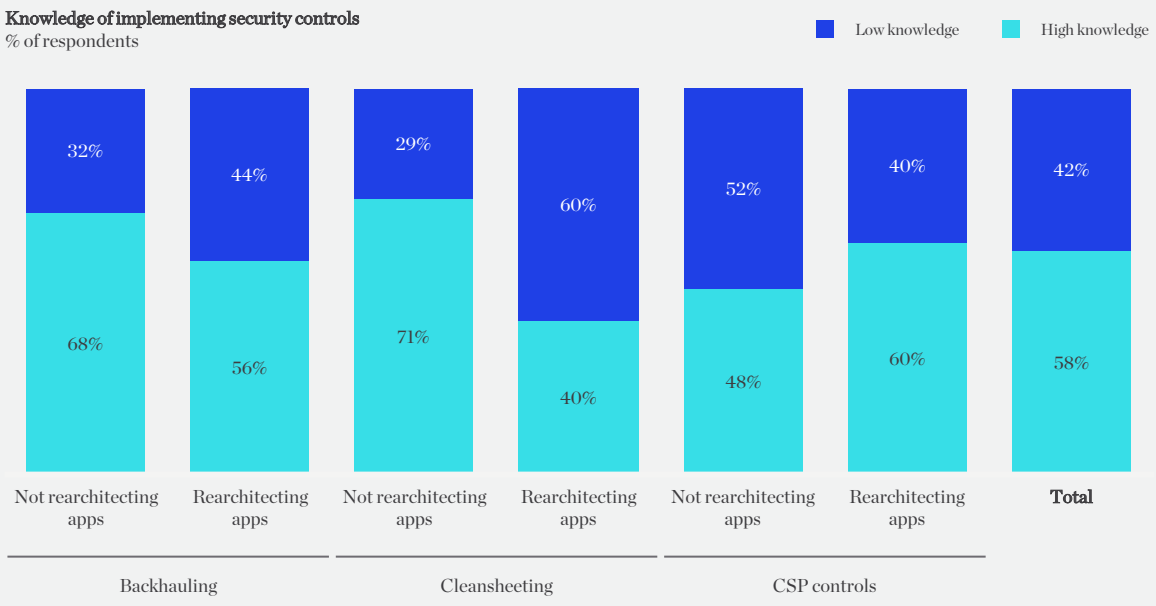


1 $20bn/year revenue, $200m/year IT budget, 40,000 employees, 35,000 end points, 300 locations, 10,000 VMs, 50 Gbps network bandwidth, 1 TB data storage, 50 web apps.
2 Includes data centers and private-cloud implementation.
3 Modeled for exclusively single CSP deployment; costs are expected to be higher when multiple CSPs are used due to integration costs; scope of controls deployed is not the same as with backhauling or cleansheeting.

Implementation expertise required. As noted previously, enterprises base their decisions on their security perimeter in part on their internal skills and capabilities. Cleansheeting the perimeter requires the highest knowledge of security implementation among all the approaches because of the need for integration expertise across disparate systems. However, this knowledge enables enterprises to take a more sophisticated approach to evaluate third-party providers and combine services in a portfolio designed to maximize security (Exhibit 15). In this context, some enterprises that want the benefits of cleansheeting but lack the internal capabilities seek the expertise of MSSPs to drive their security implementation. However, cleansheeting still requires implementation expertise (in-house or external) to integrate multiple providers and create a unified view of security posture and automated operations.

Exhibit 15

Enterprises with high knowledge of security controls are cleansheeting the perimeter.



SOURCE: McKinsey global cloud cybersecurity research, 2017

Flexibility. Cleansheeting provides the most flexibility in terms of implementing cybersecurity controls. Organizations have the option to choose different vendors for different controls based on how rigorous the controls need to be, and according to what features are of high value to them. As a result of using a combination of solutions, organizations also have the flexibility to swap out solutions as needed or to change them as their needs evolve. Further, cleansheeting allows for higher customization of the controls to meet the specific requirements of an organization. However, the trade-off for such flexibility is that cleansheeting requires organizations to spend more time and effort integrating controls in order to deliver an enteprise's target level of overall security effectiveness. In general, adopting default CSP controls tends to offer limited opportunities for customization and increase dependency on the CSP and its capabilities.

Section

04

Redesigning a full set of cybersecurity controls for the public cloud

Companies should consider the full set of security controls when building the security architecture, and for each individual control, companies need to determine who should provide it and how rigorous it needs to be.

Once enterprises have decided on a security archetype (or a mix of archetypes, with each archetype matched to a group of workloads with similar security requirements), they can turn to designing and implementing cybersecurity controls. Understandably, companies are experimenting with a variety of designs for each control and, given the pace of advancements, cybersecurity executives anticipate considerable change to these controls over the next three years. Cybersecurity controls can be categorized into eight broad control areas, and organizations need to think about all of these in combination. These control areas are listed below, along with observations from our research.

Identity and access management

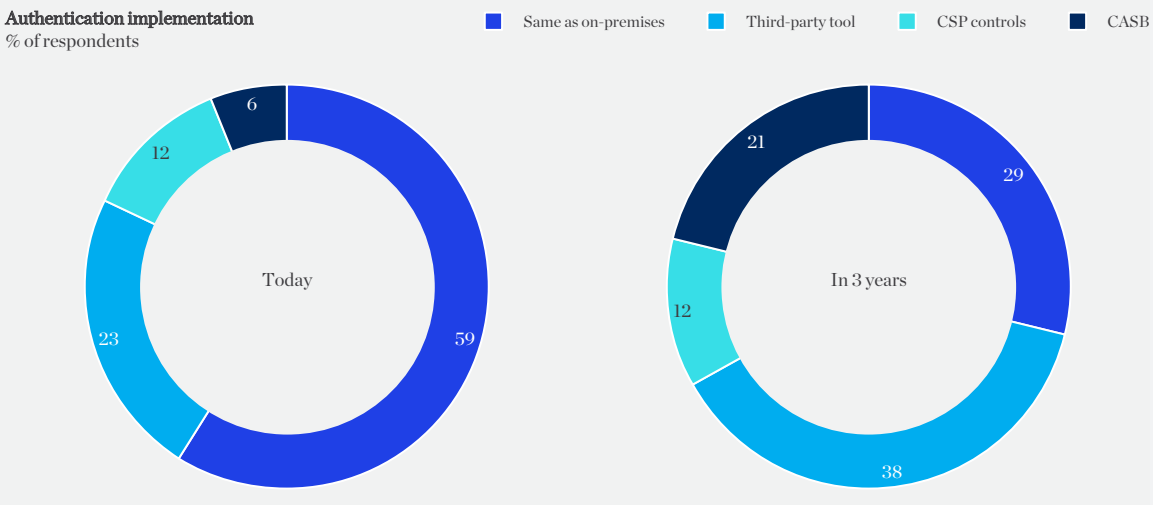
IAM is rapidly moving to the public cloud. Today, 60 percent of enterprises are using on-premises IAM solutions; in just three years our respondents expect that number to cut in half—an indication of fast-evolving sentiment toward the efficacy of cloud-based solutions (Exhibit 16). Currently, 30 percent of enterprises are using third-party solutions such as identity as a service (IDaaS) or a cloud access security broker (CASB). This figure is likely to double in the context of hybrid cloud and multicloud deployments: organizations planning to adopt cloud-based IAM solutions will do so to support hybrid cloud and multicloud deployments or to access advanced features offered by some IDaaS solutions when it is time to upgrade their on-premises IAM solution. For instance, one US-based financial services firm standardized an IDaaS solution to gain support for multicloud environments. The executive said, "We chose a third-party IDaaS control to consolidate IAM across multiple SaaS solutions. Then seeing how well it worked, we extended it to on-premises workloads." In a different approach, an executive at a leading media company noted, "We chose a CSP-provided IDaaS solution because it provides multifactor authentication. Our long-term strategy is to migrate everything to this solution eventually."

Data

Cloud data encryption is the new normal. Many leading CSPs are providing encryption for data at rest and in transit to support this requirement. As enterprises continue their march to the public cloud,

Exhibit 16

Most companies are leveraging their on-premises IAM solution now but plan to install a cloud-based tool in three years.



SOURCE: McKinsey global cloud cybersecurity research, 2017

Moving on to the next generation of IAM

One healthcare company aims to move up to 75 percent of its workloads to the public cloud by 2020. To enhance its security for the public cloud, the company completely upended its IAM paradigms. Its engineers sought to develop a stop-gap solution that could eliminate the human factor in provisioning access to its systems. The company transitioned from single-event authentication, such as typing in a password, to continuous authentication that could verify user access. This approach used behavioral authentication to develop an in-house risk model that compares a user's expected behavior and the functionality the user is trying to access via data from CSP monitoring. With this data, the model calculates a risk score to ultimately determine the appropriate level of access for each user. Exceptions triggered the generation of incident tickets. As a company executive told us in an interview,

> "Passwords are obsolete. Even multifactor authentication is a step backward. Behavioral authentication is the next generation. With the training data from CSPs, we are taking a risk-based approach and building continuous authentication."

As more behavioral data is collected over time, it will clearly enable this machine-learning-driven approach to refine and improve its performance versus systems based on simple rules. For security and data protection professionals, this will create yet another pool of sensitive data that needs to be governed and handled in accordance with clear policies, however.

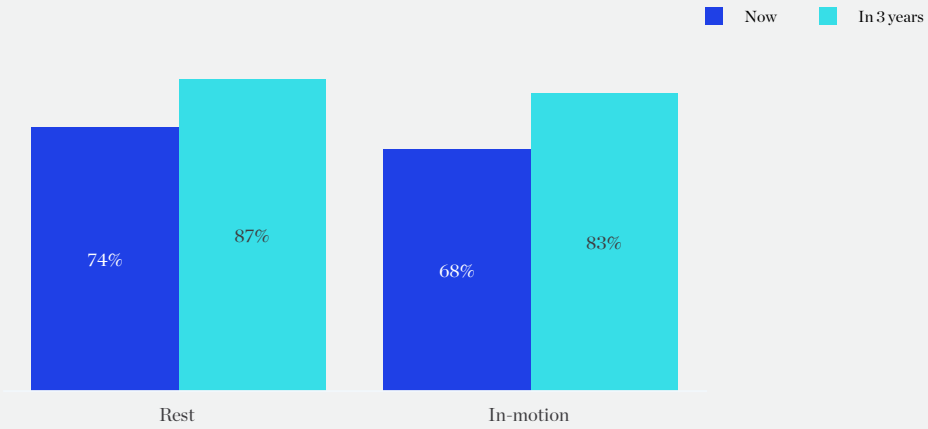
more than 80 percent of cloud aspirants expect that within three years they will encrypt the data they store in the cloud. Regulatory compliance is a contributing factor, as companies in industries such as financial services and healthcare need to be able to document and verify processes and controls for the handling and security of personal information. For a minority of enterprises, which are not encrypting data in the cloud, two factors—cost and performance—are barriers to adoption (Exhibit 17). On the former, some PaaS and SaaS providers charge for encryption services, and costs can quickly accumulate with higher volumes of data. One respondent from a financial services firm said, "My PaaS provider charges for encryption. Our costs went up 40 percent once we paid for it. So, we decided not to encrypt." Other enterprises have balked at the loss in performance, as searches in some cases are known to have slowed demonstrably due to encryption in the cloud.

Though enterprises overwhelmingly showed a preference for encryption, interviewees have different approaches to managing encryption keys for cloud workloads: 33 percent prefer to have CSPs manage keys, 28 percent keep them on premises, and 11 percent prefer to have third parties manage keys (Exhibit 18).

Exhibit 17

The use of encryption for data at rest and in motion will increase in three years.

Encryption of data in cloud
% of respondents

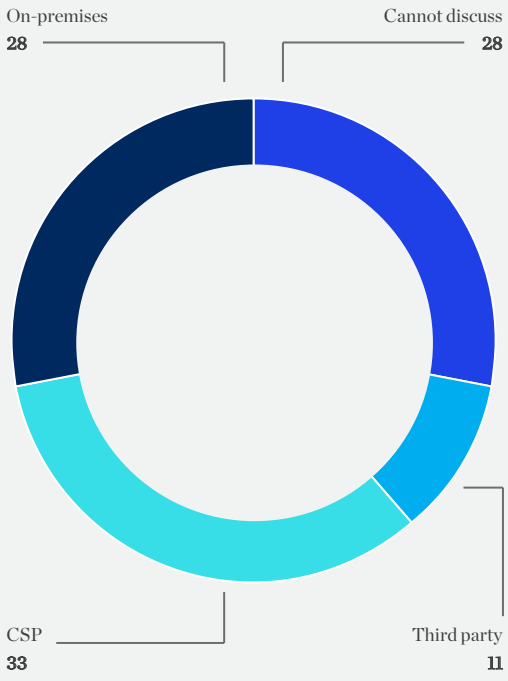


SOURCE: McKinsey global cloud cybersecurity research, 2017

Exhibit 18

Enterprises are divided in their approach to key management.

Key management ownership
% of respondents



SOURCE: McKinsey global cloud cybersecurity research, 2017

Why companies manage keys differently

Companies determine their key-management practices based on various factors, such as regulatory compliance and security benefits. Two examples from our interviews show why approaches differ. An IT services company has opted to generate and manage keys using a localized private system so it can use key ownership as a mechanism to stay in the loop if CSPs are forced to hand over data. The executive explained,

> "We are holding the key ourselves because it gives us and our compliance people confidence that only local employees have access to keys, and data cannot be accessed without our knowledge. That control gives peace of mind."

A pharmaceuticals and medical-products company takes a different approach, drawing on its CSP's key-management capabilities to improve cost-effectiveness and performance. The executive we interviewed said, "Our public-cloud application functionality is improved when keys are stored in the public cloud. Public-cloud applications need the keys to decrypt public-cloud data, and so we see less security benefit to storing keys privately. We get better performance having keys closer to apps, and encryption and decryption cost less with publicly stored keys."

Perimeter

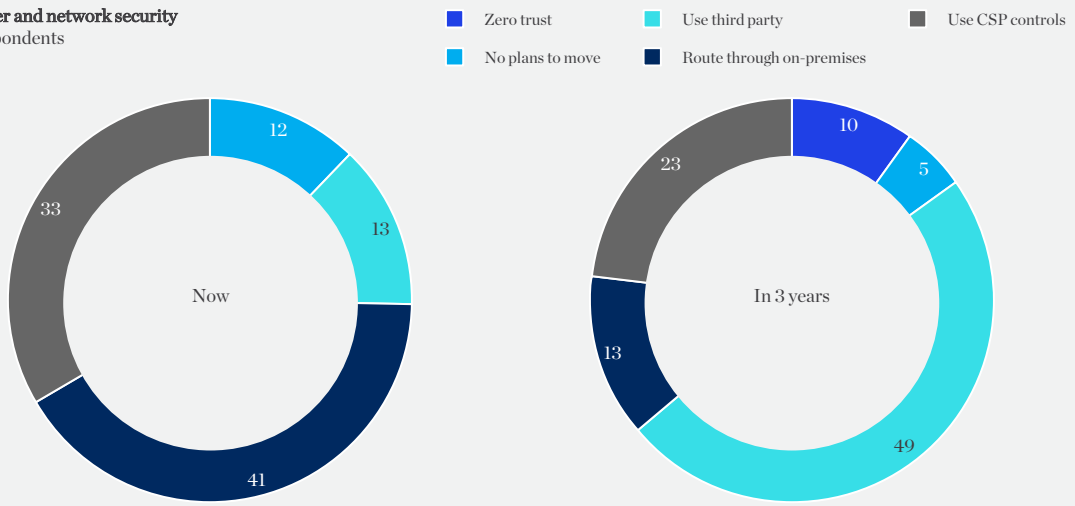
The choice of network security solutions is directly tied to the perimeter design model. As noted in the discussion on security model archetypes, enterprises are moving toward a "virtual perimeter" model. While a significant number of enterprises still favor the backhaul model as their path to the public cloud, this approach will become less popular in coming years. Approximately half of all organizations plan to adopt a cleansheet approach to perimeter control using a combination of services. To support this move, enterprises are choosing network security controls to align with their choice of perimeter design. Today, however, 40 percent of enterprises have chosen to backhaul data traffic and are using on-premises network security controls and routing traffic to the public cloud.

Top themes shaping the decision are the flexibility to select best-of-breed solutions and clarity on shared responsibilities (Exhibit 19). One insurance company currently using default CSP controls anticipates using a mix of CSP and third-party controls to gain better visibility, clarity regarding shared responsibility, and more transparency into security posture, because it is clear which solutions provider is offering which control. Some enterprises are considering "zero-trust" models, a radical alternative whereby the concept of a perimeter (and hence perimeter security) effectively ceases to exist. While these enterprises have expressed their intention to move to the zero-trust model in three years, it remains unclear whether this model will become mainstream.

Exhibit 19

Over the next three years enterprises expect to adopt a model of cleansheeting using third-party controls to define a virtual perimeter to cover their multicloud environments.

Perimeter and network security
% of respondents



Top themes driving migration to a cleansheet approach in the long term:

- Picking best of breed:
  A national player in the food industry foresees rapid development of security technology and has stuck to cleansheeting using a mix of solutions to keep pace with innovation; architecture provides flexibility to replace point solutions as needs evolve.
- Backhauling to cleansheeting for cost reasons:
  An energy company backhauls due to lack of cloud knowledge and leverages on-premises controls and has extended security stack to route to AWS. Increasing costs and aspiration to move to multivendor model drive need to cleansheet.
- Default CSP controls to third party for better visibility:
  An insurance company currently using default CSP controls anticipates leveraging best-of-breed solutions with a mix of CSP and third-party controls to get better visibility, clarity in shared responsibility, and more transparency into security posture.

SOURCE: McKinsey global cloud cybersecurity research, 2017

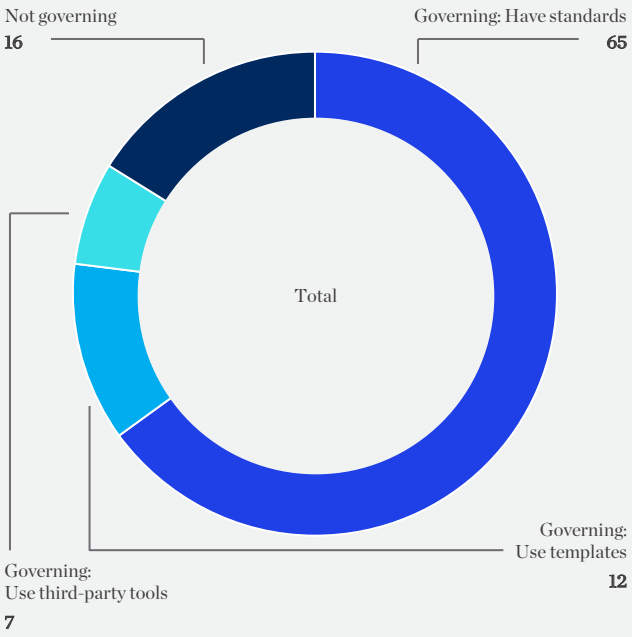
Applications

There is a need for increased developer governance as workloads move to the public cloud. Governance is even more critical in the public cloud because of the flexibility and ease of cloud development. One survey respondent noted, "With cloud, bad behavior propagates faster given the ease of developing and deploying code. It takes more effort to track down my developers. So, we emphasize governance." Although most interviewees (65 percent) define security configuration standards for cloud-based applications they do not enforce them using tools or templates—fewer than 20 percent are using tools or template-based enforcements (Exhibit 20). To avoid constraining developers while ensuring a modicum of governance, enterprises often define standards for application configuration and then rely on developers to implement them; however, 85 percent said their companies are likely to drive more developer governance as workloads move to the cloud. An executive at a payments provider said, "We have standards that we rely on the developers to implement, but they still have a lot of leeway." This type of soft enforcement represents the balance that enterprises are willing to strike while they gain greater familiarity with the safeguards and perils of cloud development. At the same time, CSPs grasp the importance of catering to developers, who are emerging as key influencers in the choice of public-cloud infrastructure vendors. As a result, CSPs are investing in building more application security templates and frameworks to attract developers to their environments.

Exhibit 20

A majority of enterprises has defined standards for application configuration, but compliance enforcement is not automated via tools or templates.

Governing developers in cloud
% of respondents



Enterprises indicate that governance is even more critical in the cloud due to the agility and ease of cloud development.

- Payments provider has standards but balances developer innovation with procedural controls:
  "With cloud, bad behavior propagates faster given the ease of developing and deploying code. It takes more effort to track down my developers. So we emphasize governance."

However, governance mechanisms tend to be soft enforcements.

- Payments provider has standards but balances developer innovation with procedural controls:
  "We have standards that we rely on the developers to implement, but they still have a lot of leeway."

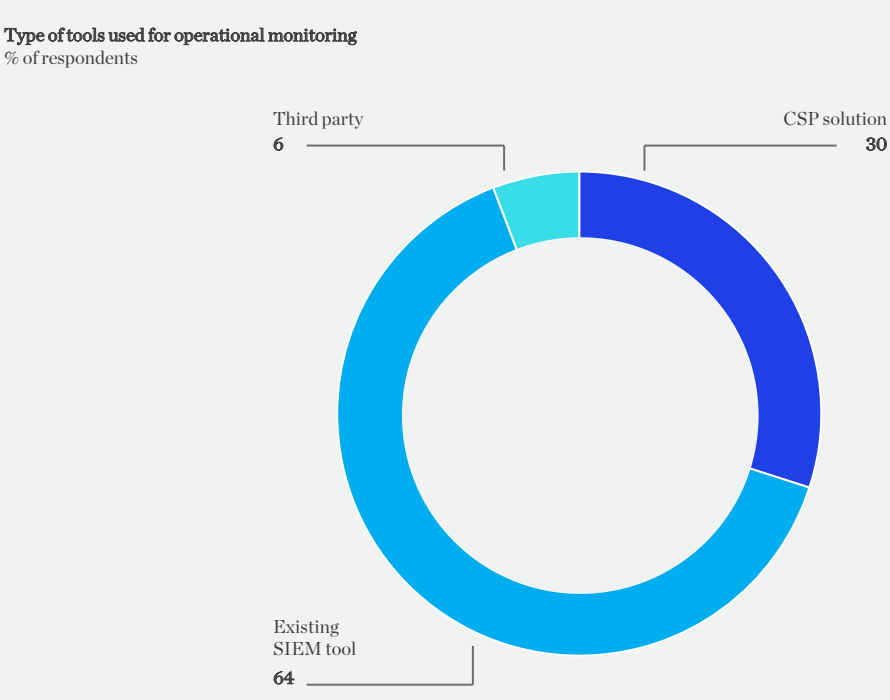
SOURCE: McKinsey global cloud cybersecurity research, 2017

Operational monitoring

There is continued reliance on existing security information and event management (SIEM) tools for operational monitoring. The hybrid nature of cloud deployments means that two-thirds of enterprises prefer to use their existing SIEM tools to monitor cloud apps rather than create an additional set for the public cloud (Exhibit 21). This stance is shaped by enterprises that have greater familiarity with current on-premises controls. According to one survey respondent, "Operational monitoring is a challenge in the cloud, and we don't know how the tools work. That's why we try to use our own tools. We still use our old SIEM." An additional 30 percent use other native monitoring tools provided by their CSPs or request CSPs to generate insights using proprietary data analytics solutions. These enterprises require CSPs to offer enhanced transparency into cloud operations and integrate solutions with their on-premises tool set. The ultimate preference is for tools that enable maintaining a common view across both on-premises and cloud environments.

Exhibit 21

Two-thirds of respondents continue to use their existing on-premises SIEM solution as they migrate into the cloud.



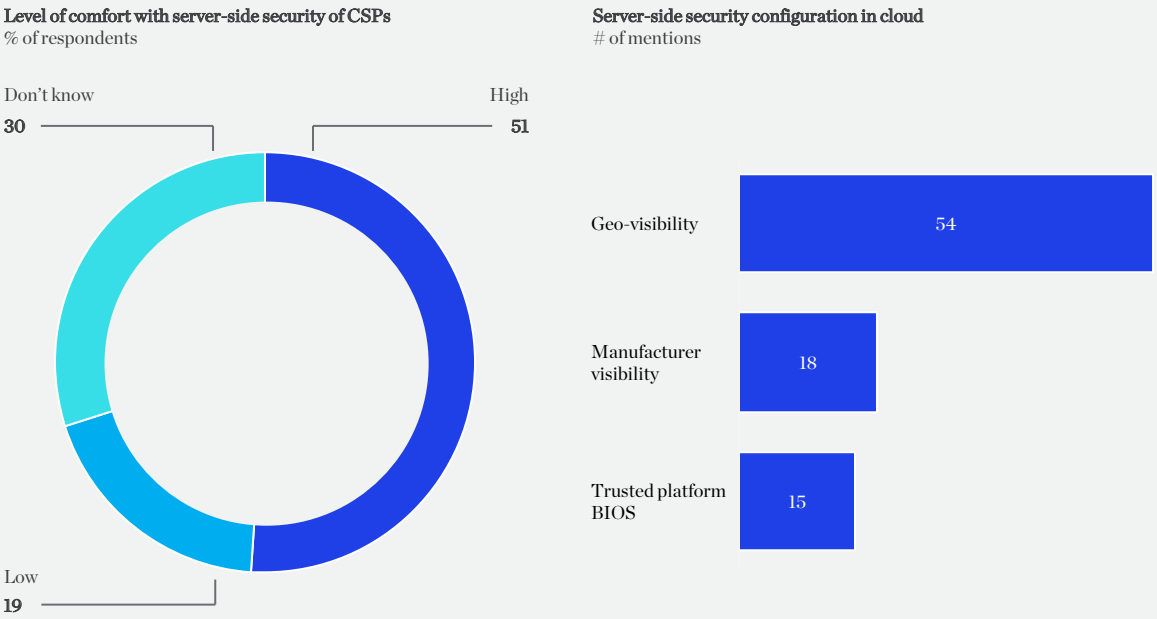
SOURCE: McKinsey global cloud cybersecurity research, 2017

Server-side end points

Cloud migration has reduced the burden of hardware and physical security for enterprises. Indeed, 51 percent of survey respondents are largely satisfied with CSP solutions and take comfort in the fact that CSPs take on the responsibility of server-side security and potentially the virtualization-layer security as well (Exhibit 22). Many companies, especially those with less sophisticated security programs, believe that CSPs have insight into and control over their server fleet that they could never achieve internally. One healthcare provider executive expressed his trust in CSP security tools: "In my opinion, the best server-side end-point security is provided by the CSPs."

Exhibit 22

Most enterprises are comfortable with the server-side end-point security offered by CSPs.



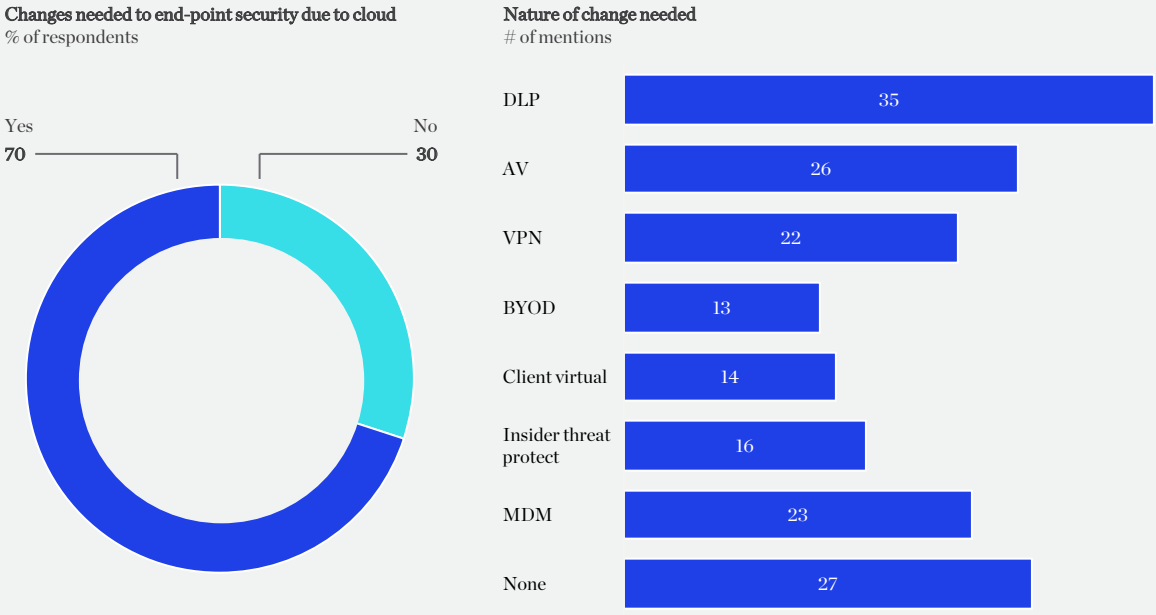
SOURCE: McKinsey global cloud cybersecurity research, 2017

User end points

Investments will be needed to enhance client end-point security. Moving workloads into the cloud ordinarily necessitates changes to controls for user devices, mainly for data loss protection (DLP) and safeguards against viruses and malware. Nevertheless, 70 percent of organizations believe that public-cloud adoption will require changes to user end points (Exhibit 23). Further, enterprises that are migrating activities to the cloud most aggressively in the medium term are also most concerned with DLP. As organizations migrate applications to cloud, it is also critical for them to reassess and fortify the security of end-user devices.

Exhibit 23

Seventy percent of organizations agreed that changes to end-point security were needed in the cloud, with updated DLP and antivirus most often needing changes.



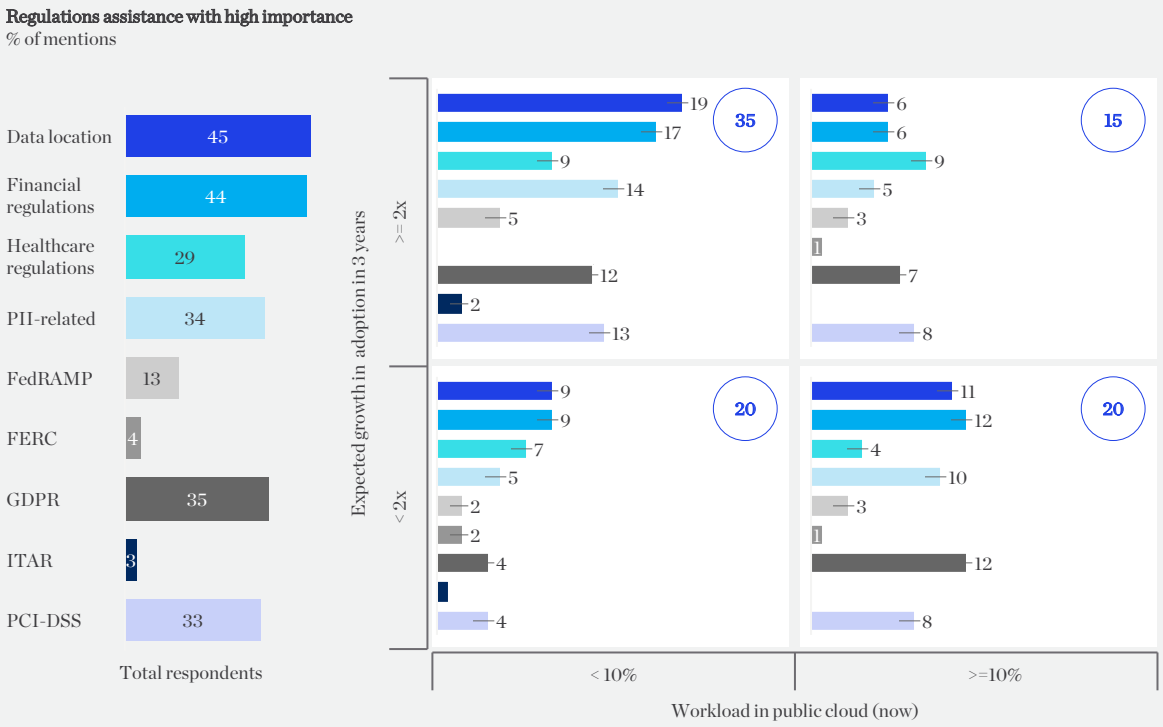
SOURCE: McKinsey global cloud cybersecurity research, 2017

Regulatory governance

Data sovereignty and compliance are set to become more pressing issues. New and existing regulations can be complicated by cloud adoption, and enterprises are seeking assistance in managing compliance. A majority of enterprises is looking to their CSPs to share responsibility for personally identifiable information (PII) and financial services compliance. In fact, data sovereignty is a primary reason why some enterprises are delaying their move to the public cloud (Exhibit 24). One university decided not to make the move because of a lack of visibility into data location. "Data sovereignty is a big concern for us; we have observed our CSP not being able to provide visibility into location of data processing, which creates compliance concerns." The European Union's General Data Protection Regulation (GDPR) is also top of mind: this regulation, which goes into effect in 2018, has led many enterprises with EU operations to be nervous about cloud adoption, so they are awaiting more clarity before determining the path forward. One European oil and gas company executive rates GDPR uncertainty as a deal breaker for cloud adoption, "GDPR has made EU enterprises nervous in moving to the cloud. We are waiting for rollout in 2018 to have more clarity before making a decision."

Exhibit 24

Data-sovereignty issues and compliance with financial and healthcare regulations were cited as top concerns by all segments of survey respondents.



SOURCE: McKinsey global cloud cybersecurity research, 2017

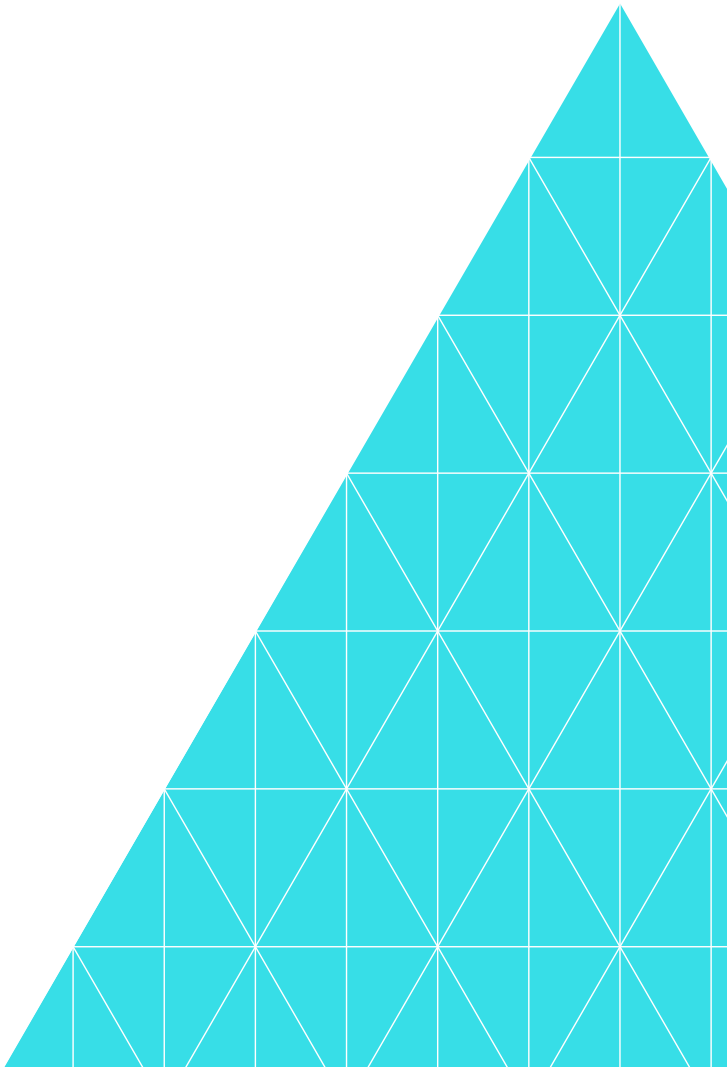
A comprehensive view of cloud-security controls

In selecting controls, organizations should start by identifying relevant threat scenarios and sources of potential countermeasures. This process, which analyzes all eight control areas in parallel rather than taking a piecemeal approach, includes the following three steps.

Design. Implementation can be carried out in phases, but designing in parallel ensures that the controls work in tandem to improve the overall security posture. By using the selected archetype as a lens through which to assess security options, enterprises can determine at a granular level the best security controls based on the archetype's features and limitations. Enterprises can then define the scope of control and explicitly assess what the control will cover. In defining IAM, for example, organizations will have to determine whether it covers only user access or if it will extend to application program interface (API) access. It is critical to design controls according to the risks inherent in each application slated for cloud deployment: in IAM, for example, does it make sense to implement single factor or two factor, since higher levels of security have cost and complexity implications? Enterprises should not only think about current applications and their requirements but also consider the future road map and overall cloud strategy when defining the scope.

Vendor selection. When selecting a provider, enterprises should consider the most suitable implementation option for each control according to available expertise and applicable cost-benefit trade-offs. This approach can help to determine which controls should be outsourced based on the selected security archetype. For controls that will be outsourced, enterprises should identify which ones will be provided by the CSP or a third party, and ensure that controls are adequate for the selected security archetype and risk appetite. As noted earlier, some organizations choose to outsource the encryption functionality to the CSP but retain key ownership and management.

Implementation. Organizations must determine how much to invest in standardization and automation of the controls. Not all controls can be standardized and fully automated. For example, within operational monitoring "log management" is a critical activity that covers how the application/host manages, secures, and maintains the availability of log files. It is a critical part of most security and compliance frameworks for supporting early identification of attacks, forensic investigations, and legal responsibilities. This control can be implemented on multiple levels: an enterprise can choose to standardize the operation by creating checklists that developers can use to guide log content and governance. To take it to the next level, organizations can also automate the implementation of logging functionality that different developers can invoke and also automate monitoring to ensure that application logging adheres to the standards defined in the checklist.



Section

05

Clarifying internal responsibilities for cybersecurity compared to what providers will do

The public cloud requires a shared security model, with providers and their customers each responsible for specific functions. Companies need to understand this split of responsibilities—it will look very different from a traditional outsourcing arrangement—and redesign internal processes accordingly.

When enterprises migrate applications and data to the public cloud, they must depend on CSPs and third-party providers for numerous security controls—but they should not depend on vendors to provide all of the necessary controls. Unless companies and CSPs clearly apportion all of the responsibilities for cybersecurity in public-cloud environments, some responsibilities could fall through the cracks. This makes it essential for companies to develop and maintain a clear understanding of what controls their CSPs provide, by having them provide a comprehensive view of their security operating models, along with timely updates as those models change. Individual CSPs organize their cybersecurity responsibility models differently, and take various approaches to sharing them, so each situation needs to be handled

carefully. That way, companies can design and configure controls that work well in multiple cloud environments and integrate well with various tools, processing models, and operating models.

Based on our experience and research, we find that enterprises can benefit greatly from understanding CSPs' responsibility across the full cybersecurity life cycle, from design to implementation and ongoing operations. However, four main areas emerged as top priorities in terms of understanding shared responsibility between companies and their CSPs.

Transparency on controls and procedures. Companies should ensure CSPs provide full visibility into their security controls and procedures, as well as any exposure incidents. Companies will also need to understand each CSP's willingness to allow security audits and penetration testing. CSPs that are reluctant or unwilling to let companies or trusted third parties conduct audits of their controls and procedures may not make good partners. One US health insurance executive noted, "SaaS solutions—that's where it becomes challenging. With turnkey solutions, we don't have that same level of transparency and control." However, in response to such requests, CSPs are developing better-defined written security practices, offering security architecture reviews, and permitting audits and providing the results of audits from trusted third parties against internationally recognized security standards.

Regulatory compliance support. Regulations on the handling and security of sensitive data present a thorny challenge. Enterprises in the financial services and healthcare industries for example, must comply with particularly stringent guidelines that are being updated on a regular basis—a time-consuming and complex undertaking. Companies should ask CSPs to provide detailed descriptions of the assurances they provide with regard to regulatory compliance and inquire about how they stay abreast of regulatory changes for each industry and update their compliance mechanisms accordingly. Then companies and CSPs can jointly determine how best to handle governance and sustain compliance with regulatory mandates.

Integrated operations monitoring and response. Companies will likely have to integrate their SIEM tools with CSP-provided services in a way that supports a centralized security administration. Companies should request that their CSPs provide them with comprehensive reporting, insights, and threat alerts on an ongoing basis. They can also pass on insights to help CSPs develop new capabilities for all their tenants and ensure that CSPs make their logs readily available in a format that companies can process using on-premises analytics tools.

Multicloud IAM capabilities. As enterprises increasingly move to an infrastructure with multiple cloud providers (nearly half of all enterprises that responded in the survey have more than one CSP), a greater awareness of security issues is leading them to consider more involved IAM solutions. The majority of enterprises currently requires two-factor authentication for cloud workloads. As one respondent noted, "Two-factor authentication is the new normal. If we don't get it, we will not select the vendor." CSPs should work to ensure security controls can function in different scenarios—for example, single sign-on across on-premises and public cloud, and consolidated monitoring capabilities. Those that are using IDaaS or on-premises IAM solutions will need to work with CSPs to integrate them properly, so they have adequate support for multiple public-cloud environments.

Section

06

Applying DevOps to cybersecurity

If a developer can spin up a server in seconds but has to wait two weeks for the security team to sign off on the configuration, that attenuates the value of the public cloud's agility. Companies need to make highly automated security services available to developers via APIs, just as they are doing for infrastructure services.

As enterprises migrate workloads to the public cloud, incorporating security controls and processes in the traditional deployment cycle regularly causes delays. Enterprises are finding that their traditional security operating models threaten to diminish the agility and speed promised by the public cloud. An in-depth look at the typical cloud-deployment cycle highlights how security challenges can dramatically slow movement to the cloud (Exhibit 25).

At each of the five steps of the cloud-deployment cycle, teams must interact with security professionals to obtain guidance and, sometimes, review and approval of their implementation decisions. Once a development team defines a

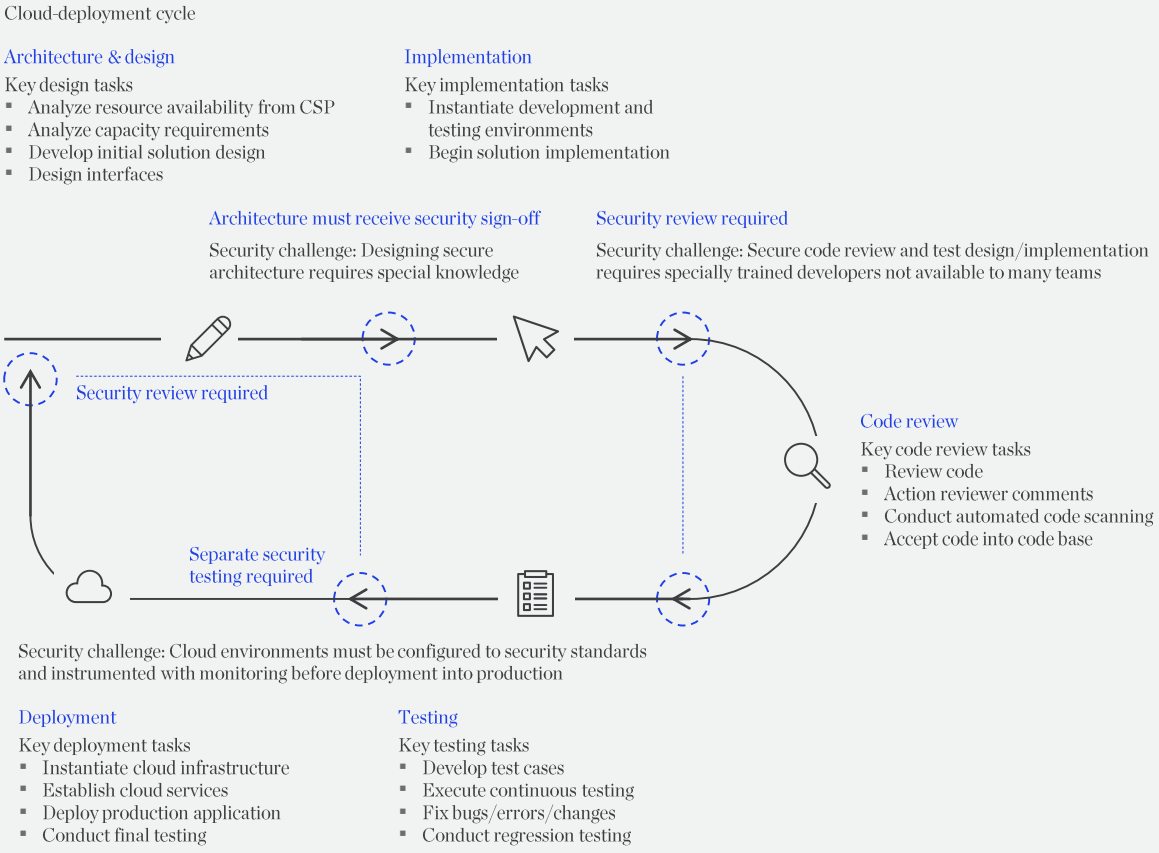
project's architecture and design, for example, the architecture must be evaluated and verified as secure before the process can move forward. Each review can add considerable time, often in the form of redesign and resubmission. Having the necessary talent can also be an obstacle, since many organizations do not have security teams large or sophisticated enough to keep up with regular security duties while simultaneously providing effective advisory support for developers. At the implementation and code-review steps, enterprises need specially trained developers to implement needed security mechanisms correctly, and these may be in short supply or attached to other projects. Then, in the testing and deployment phases, cloud environments must be configured to security standards and equipped with monitoring features.

Cumulatively, these security interactions can add substantial time and expense to cloud deployments.

To facilitate a smoother transition to the cloud, enterprises must align their approach to security interactions with the software-development and cloud-deployment cycles. DevOps is an increasingly prevalent approach to integrating development and IT operations, which supports continuous delivery of new software features, in part by providing developers with APIs to access operational services. Secure DevOps (sometimes called "SecDevOps" or "continuous security") integrates security reviews, implementation of security controls, and deployment of security technology with the DevOps approach that many teams have already adopted for

Exhibit 25

Traditional cybersecurity interactions can significantly delay cloud-deployment timelines.



movement into the cloud. Integration is achieved by automating security services across the full development cycle and making them available via APIs.

In our experience, secure DevOps enhances all categories of security controls for the cloud, leading to shorter deployment timelines and lower risk. A look at the eight control areas highlights its impact.

IAM. IDaaS enables transparent identity sharing between cloud and on-premises environments. Simplified IAM in the cloud shortens time to production for new cloud end points.

Data classification. All data receive a default classification based on predefined rules, resulting in a lower risk of breach or disclosure of sensitive data in cloud environments.

Network controls. Software-defined networks include robust controls by default at instantiation time, substantially reducing costs due to network security appliances and shortened time to production.

Application controls. Robust security controls are established during implementation, and delivered via secure DevOps, significantly reducing risks due to application vulnerabilities and cutting post-release maintenance costs.

Operational monitoring. All hosts and environments are instrumented to report status and enable monitoring immediately upon instantiation, giving enterprises greater situational awareness of the cloud while also decreasing maintenance overhead.

End-point protection. End-point protection systems are automatically installed in all end points during instantiation, greatly shortening production times for newly instantiated cloud end points.

Governance. Standardized checklists and a governance process for regulatory compliance are automated to prevent developer errors, deployment violations, and misconfiguration risks.

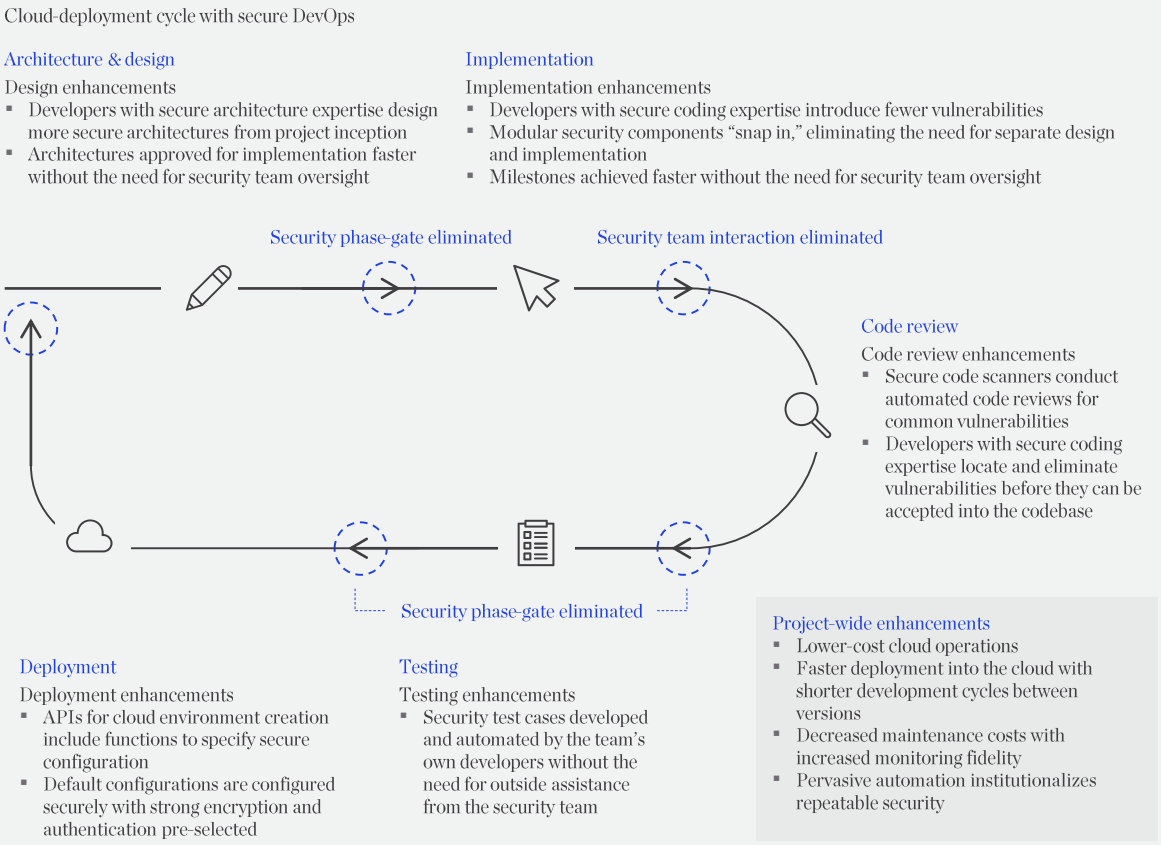
Host infrastructure. Hosts are instantiated with controls securely configured and activated by default, further shortening production times.

These enhancements to cloud migration can streamline each step of the process, accelerating the overall cloud-deployment cycle (Exhibit 26). In architecture and design, for example, greater definition of strategy and archetypes enables developers with secure-architecture expertise to design more secure architectures from the project's inception, leading to faster implementations without the need for security team oversight. Similarly, in implementation, developers with secure-coding expertise introduce fewer vulnerabilities and preapproved modular security components "snap in"—eliminating the need for separate design and implementation, as well as security team oversight. In the deployment phase, APIs for cloud environment creation include functions to specify secure configuration, and default configurations are deployed with pre-enabled encryption and authentication.

A secure DevOps model can help enterprises capture several benefits, including lower-cost cloud deployments and shorter development cycles between versions. In addition, increased monitoring fidelity cuts maintenance costs, while pervasive automation institutionalizes repeatable security.

Exhibit 26

By implementing secure DevOps, companies automate security controls and accelerate the cloud-migration process.



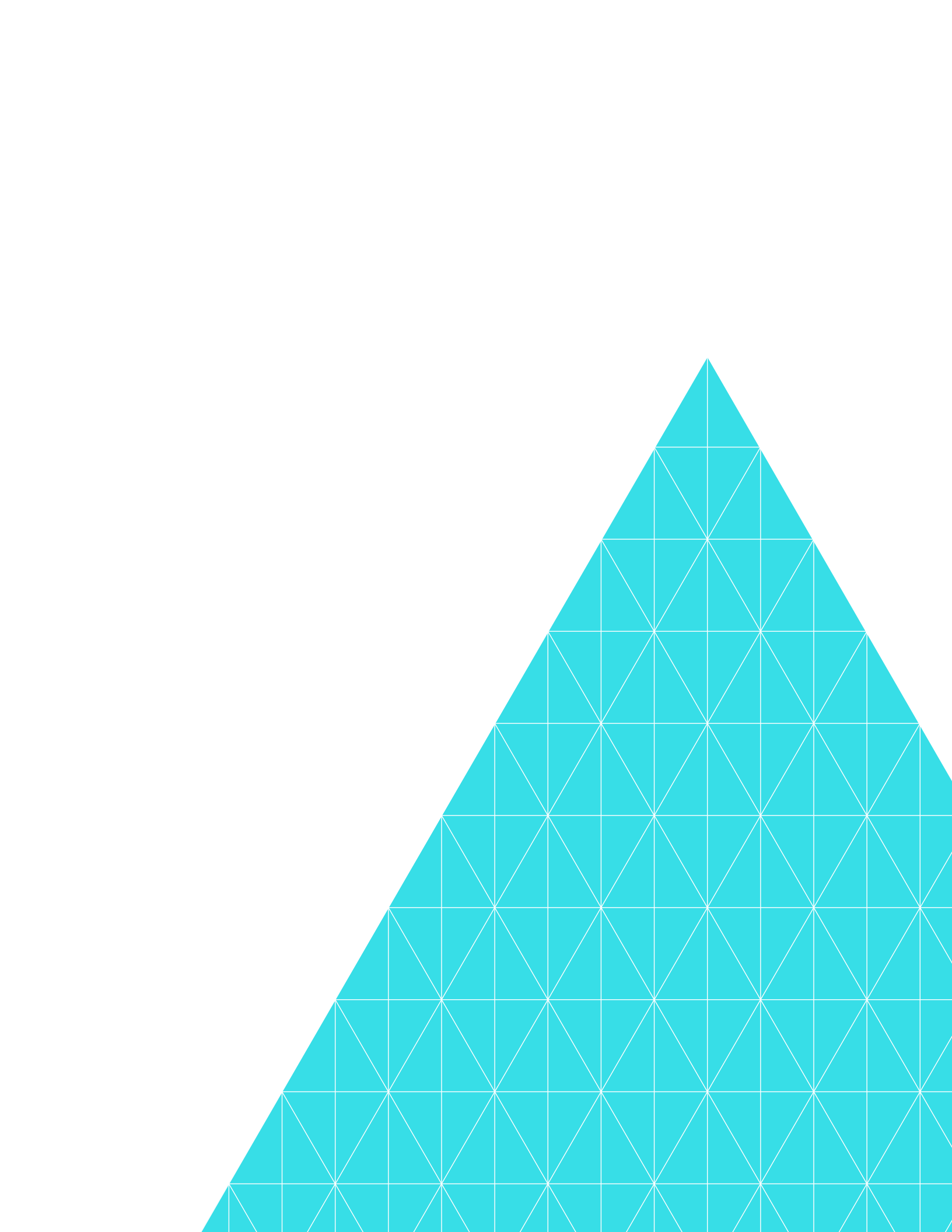
Speeding app development in the cloud with secure DevOps

A media and information company has adopted a secure DevOps approach to standardize and automate security controls. The company was motivated to make a change for several reasons: its applications development, R&D, security, and IT teams were all siloed. It had no standards for measuring security success, and it lacked insight into the security of its systems. And it was less agile than it wanted to be—developers were forced to move slowly, rethinking the same mundane security issues and reimplementing similar security solutions. Its target state with secure DevOps will feature both a standardized scorecard and automated verification of standards. With a well-defined set of standards, its team will have the ability to test application security controls against standards without manual intervention, allowing security controls to be configured at the click of a button. It will also support more rigorous compliance and offer efficient assurance that all cloud security rules and configurations are being followed.

Adopting secure DevOps methods requires companies to foster a culture in which security is a key element of every software project and a feature of every developer's work. Many developers will need additional security training in order to provide effective support during and after migration to the public cloud. Training also helps developers understand the security features of the tools they are using, so they can make better use of security APIs and orchestration technologies built into their existing security tools and build new ones when needed.

Companies should streamline their security governance procedures to make sure they do not cause delays for developers. As companies automate their security controls, they can make controls fully visible to developers. That way, developers can independently check whether controls are working properly in the background rather than delaying work to consult with security specialists. Automating the processes of auditing security mechanisms is also helpful. For example, companies can require that code is automatically scanned every night for compliance with policy, and integrate build-time checks of security components into applications to support a modern "continuous integration/continuous delivery" (CI/CD) process.

To implement secure DevOps, companies must also change their IT operating model so security implementation becomes a part of the cloud development and deployment process. Under such an operating model, a properly trained development team is the security team; no outside engagement is needed to obtain the right security expertise. Security experts will still act as coaches for the team as the members build and mature their secure DevOps capabilities and adapt to the new processes and mind-sets needed for success. Overall, embedding security expertise in the development team eliminates delays in the cloud-deployment process and permits the development team to iterate much faster than traditional security models allow.

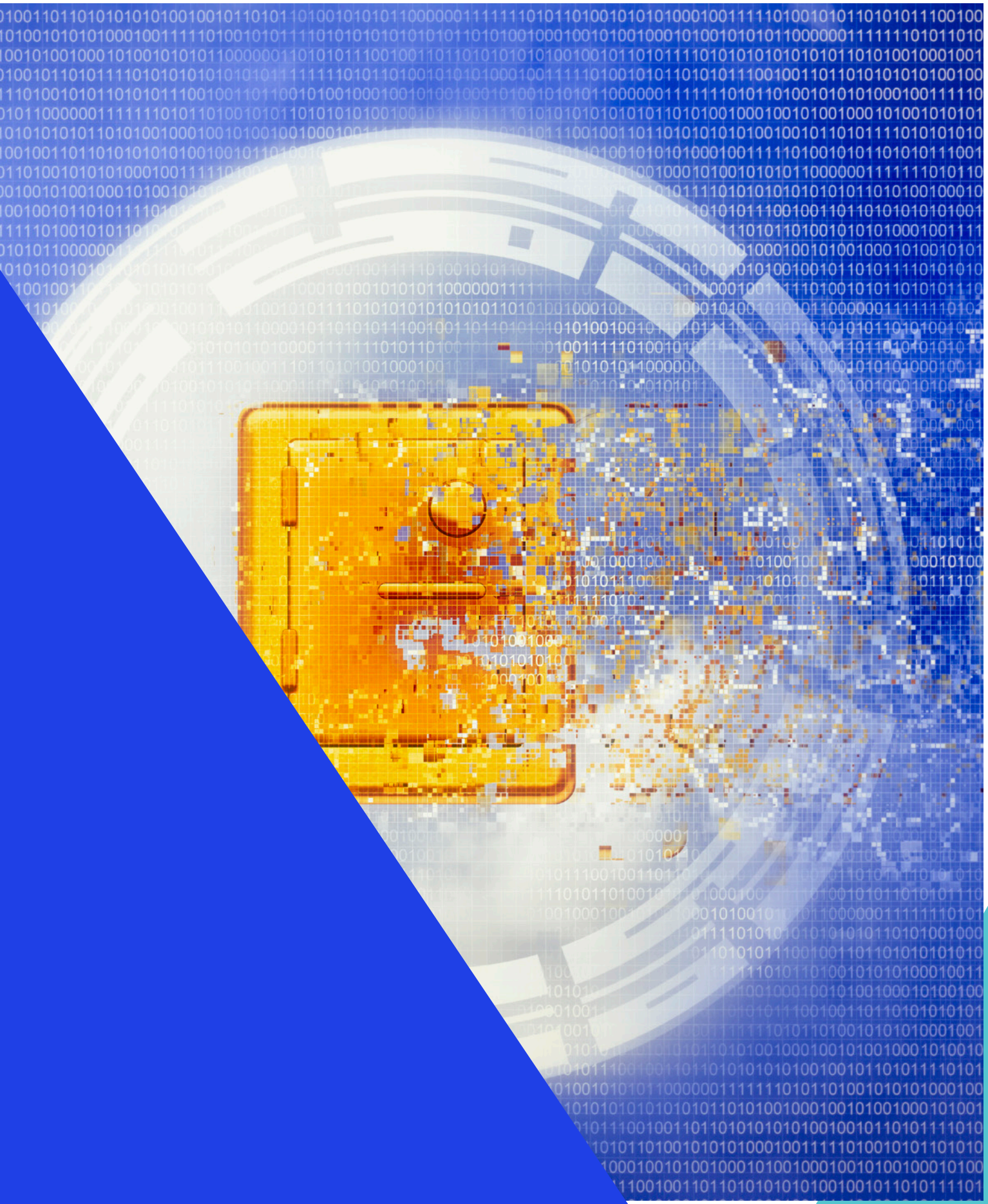


Section

07

How companies can begin strengthening cybersecurity in the cloud

Ten practical steps can kick-start the process of fortifying cybersecurity in the public cloud.



The four practices we have described for structuring a public-cloud cybersecurity program should enable companies to take greater advantage of public-cloud platforms. Nevertheless, setting up the program can be a complicated task, because companies have multiple cloud workloads, CSPs, on-premises and private-cloud capabilities, locations, regulatory mandates, and security requirements to address. This ten-step workplan will help companies stay coordinated as they move through design, development, and implementation of their public-cloud cybersecurity programs.

1. Decide which workloads to move to the public cloud. For example, many organizations choose to move test and development environments or analytical workloads to the public cloud initially, while keeping core transaction systems on premises. Then they can determine security requirements for workloads that are migrated.

2. Identify at least one CSP capable of meeting security requirements for the workloads. Companies may choose multiple providers for different workloads, but these selections should be consistent with the objectives of the companies' overall cloud strategies.

3. Assign a security archetype to each workload based on the ease of migration, security posture, cost considerations, and internal expertise. For example, companies can remediate applications and use default CSP controls for customer-facing workloads, and lift and shift internal core transaction apps without remediation while backhauling for data access.

4. For each workload, determine the level of security to enforce for each of the eight control areas. For example, companies should determine whether IAM should use single-factor authentication, multifactor authentication, or a more advanced approach such as behavioral authentication.

5. Decide which solutions to use for each workload's eight control areas. Given the capabilities of the CSP (or CSPs) identified for each workload, companies can determine whether to use existing on-premises security solutions, CSP-provided solutions, or third-party solutions.

6. Work closely with the CSP to implement the necessary controls and to integrate them with other existing solutions. This requires companies to gain a full understanding of CSP's security capabilities and security enforcement processes. CSPs need to be transparent about these aspects of their offerings.

7. Develop a view on whether each control can be standardized and automated. This involves analyzing the full set of controls and making decisions on which controls to standardize across organizations and which ones to automate for implementation.

8. Prioritize the first set of controls to implement. Controls can be prioritized according to their importance for the applications that are being migrated to the public-cloud environment.

9. Implement the controls and governance model. For controls that can be standardized but not automated, companies can develop checklists and train developers on how to follow them. For controls that can be both standardized and automated, companies can create automated routines to implement the controls and to enforce standardization using a secure DevOps approach.

10. Use the experience gained during the first wave of implementation to pick the next group of controls to implement. Drawing on this experience will also help to improve the implementation process for subsequent sets of controls.

Conclusion

Companies are steadily moving more of their applications and data from on-premises data centers onto public-cloud platforms, which can provide superior levels of cost-effectiveness, flexibility, and speed in many situations. But public-cloud migrations will only succeed if companies maintain the security of their applications and data—a task that some have struggled with to date.

As we have seen, making a secure transition to the public cloud is a multidimensional challenge. Our experience and research suggest that an effective public-cloud security posture is achievable with the right approach. By developing cloud-centric security models, designing strong controls in eight security areas, clarifying responsibilities with CSPs, and using secure DevOps, companies can shift workloads into the public cloud with greater certainty that their most critical information assets will be protected. Clearly this will be a top priority for CISOs as well as the wider range of business and technology leaders who steer their enterprises' IT strategies. We hope this research can inform and guide those journeys.