451 Research® | PATHFINDER REPORT

Secure Hybrid Cloud

THE STRATEGIC APPROACH TO ENTERPRISE IT

COMMISSIONED BY

IBM

MAY 2019

About this paper

A Pathfinder paper navigates decision-makers through the issues surrounding a specific technology or business case, explores the business value of adoption, and recommends the range of considerations and concrete next steps in the decision-making process.

ABOUT THE AUTHOR

JEAN ATELSEK

ANALYST, CLOUD TRANSFORMATION AND DIGITAL ECONOMICS UNIT

Jean is an analyst working across 451 Research's Cloud Transformation team and Digital Economics Unit. In addition to producing the quarterly Cloud Price Index deliverables, Jean covers vendors and cloud providers that offer technology or services to manage or improve public and private cloud TCO, performance or consumption. She has developed a niche in new private-cloud pricing models, including pay-as-you-go and build-operate-transfer.

OWEN ROGERS

RESEARCH DIRECTOR, DIGITAL ECONOMICS UNIT

As Research Director, Dr. Owen Rogers leads the firm's Digital Economics Unit, which serves to help customers understand the economics behind digital and cloud technologies so they can make informed choices when costing and pricing their own products and services, as well as those from their vendors, suppliers and competitors. Owen is the architect of the Cloud Price Index, 451 Research's benchmark indicator of the costs of public, private and managed clouds, and the Cloud Price Codex, our global survey of cloud pricing methods and mechanisms. Owen is also head of 451 Research's Center of Excellence for Quantum Technologies.

Executive Summary

The enthusiasm for hybrid cloud as an ideal structure for IT environments belies a complicated decision-making process around locations for various types of compute workloads and data stores. Though it may seem that today's enterprises have more choices than ever for where to host their applications, some workloads must remain on-premises for reasons related to data control, security, compliance and performance. At the same time, competitive pressures are pushing businesses to be more customer-responsive by taking advantage of the perceived scalability, flexibility and agility afforded by off-premises IT architectures. Enterprises must focus on business outcomes while deploying workloads and data in a way, and in a location, that ensures security and integration across increasingly distributed environments.

Key Findings

- **Workload placement is a critical factor in maximizing the value of IT environments.** As markets and technologies have matured, the choice of where to deploy data and applications has evolved as well. More than two-thirds (68%) of companies making strategic IT investments view hybrid IT and integrated on-premises/off-premises cloud environments as their default approach.
- **Public cloud is not a panacea.** Many enterprises have already migrated the applications and business functions that are 'low-hanging fruit' for off-premises deployment: productivity suites and customer relationship management systems, for example. But factors that may prevent migration include security and data protection, performance and cost.
- **Hybrid cloud is the new normal.** Data from 451 Research's Voice of the Enterprise service shows that hybrid cloud environments encompassing both on-prem and off-prem venues are the direction of travel for most organizations. Cloud transformation is occurring both within and outside the datacenter, and IT decision-makers plan to increase their use of both in the coming years.
- **Security must be baked in to IT evolution plans.** Maintaining security is paramount when migrating and refactoring IT systems to take advantage of the wealth of destinations available. Federation of identity and access management across public and private clouds is critical, and encryption of data is necessary to ensure that increasingly distributed systems remain tamper-proof while IT estates are upgraded and modernized to seize the possibilities of the next 20 years.

Cloud Adds Value When Data and Applications are Placed Where They Make the Most Sense

For most organizations, moving at least some applications and data to the cloud is not a matter of if, but when and why. The perceived benefits of lower cost, easier infrastructure management, and faster and more flexible provisioning ushered in a wave of business and IT transformation not seen since x86 virtualization made its appearance more than 20 years ago. As the market and technology have matured, however, businesses are changing their strategies.

In the past several years, cloud adoption has moved from being the province of early adopters into the mainstream. In many cases it began as a bottom-up phenomenon, with individual business units implementing 'shadow IT' – applications developed on platforms provisioned with the swipe of a credit card – to effect outcomes that made other departments (and IT management) take notice.

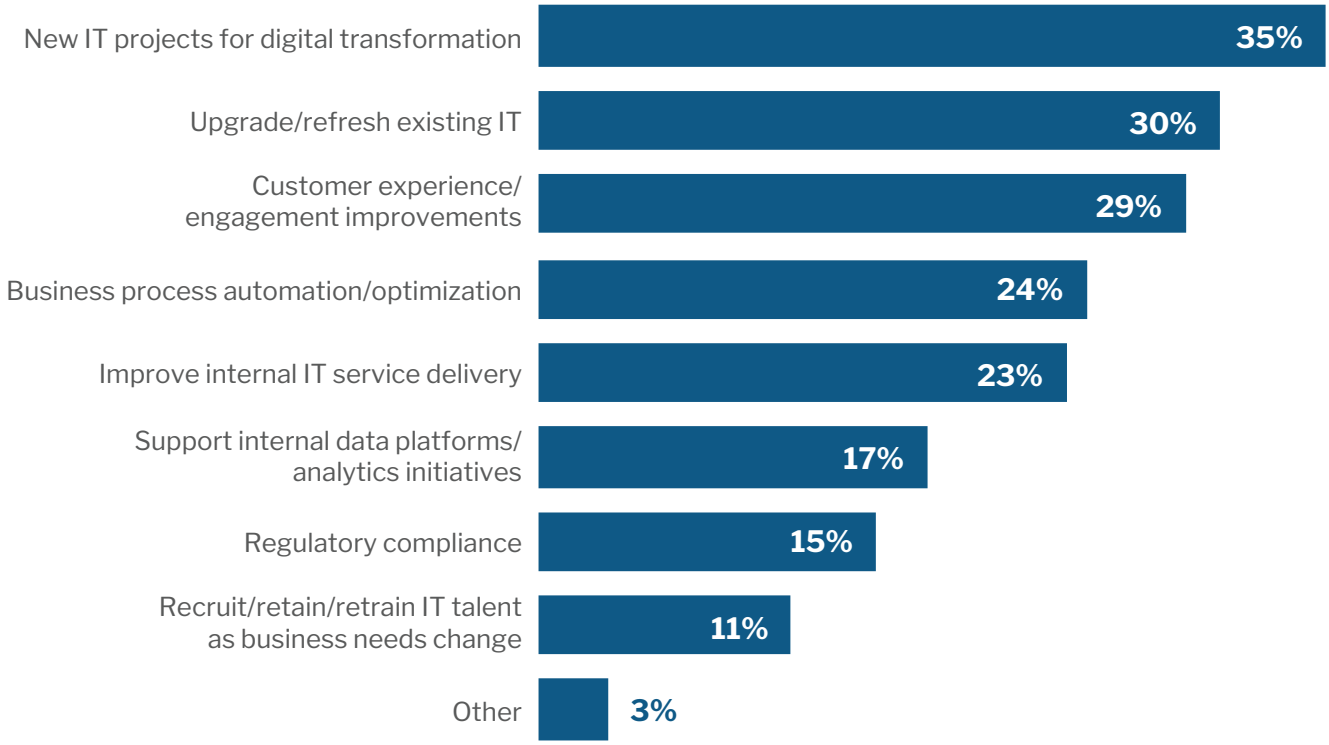
But the initial rush to cloud was not without complications and risks. Deployments that were impressive at small scale and in isolation created unacceptable exposure when moved into production, and establishing connections with on-premises data stores – in many cases the most valuable and differentiating IT assets in the organization – opened businesses to significant risk. Companies that were initially happy to lift and shift applications and data to the cloud soon learned that this approach, if applied indiscriminately, could be costly, complex and disruptive. This did not in itself make the organization more agile and flexible, nor did it necessarily make the applications more resilient or available.

The fact is, many workloads simply cannot or should not make the transition to cloud. Custom-built applications with core business dependencies are often mission-critical, especially in industries such as banking and insurance. These on-premises systems may be foundational, and abstracting away the underlying infrastructure would compromise the business itself. Workloads that require low-latency access to on-site data, such as financial services systems that need to process transaction details to and from customer accounts, are too sensitive for off-premises deployment; the business will rarely accept the increased risk in moving these apps and data off-premises. In all these cases, compliance demands – whether regulations restricting the geographic distribution of data, or industry or company-specific rules to ensure consumer information is protected – are needed to preserve access to lucrative markets.

The combination of these pressures – increasing business agility with cloud while maintaining on-premises control of sensitive data and regulated workloads – has led to the dominance of hybrid cloud as a key enabler of modern IT systems. Enterprises have accepted the idea of incorporating as-a-service infrastructure, platforms and software into their IT estates, but they need to do so in a selective, disciplined and secure way. This is reflected in IT spending priorities; digital transformation is the top spending focus for 2019, and cloud is a key enabler of this transformation (Figure 1).

Figure 1: IT spending priorities for 2019

Source: 451 Research's Voice of the Enterprise: Digital Pulse, Budgets and Outlook 2019
Q: Which of the following are your organization's top two IT spending priorities for 2019?



% of respondents (n=874)

Enterprise buyers are also looking to improve customer engagement and automate business processes to become more responsive to markets and opportunities. These initiatives tend to be part of cloud transformation efforts in a bid to migrate applications that support the business but are not critical to the core. These are also the areas where software-as-a-service offerings are selected. New app development and proofs of concept are also likely to start in cloud environments.

However, note that the second spending priority in the figure above is to upgrade or refresh existing IT, much of which is likely on-premises and will remain there for the foreseeable future.

"We try to separate and not say, 'We have a directive that we're going to move everything to the cloud or we have a directive that we're going to keep everything internally.' We just say, 'We find the application, and then we find out what is best from an economical, and a compliance, and security perspective and go that route.'"

– SENIOR MANAGER, $1-2.5BN FINANCIAL SERVICES BUSINESS

Among digital leaders – companies that are already executing on or strategizing their IT investments based on digital transformation – 42% are allocating more than half of their budgets on IT initiatives to grow or transform the business itself, and 68% view hybrid IT and integrated on-premises/off-premises cloud environments as their default strategic IT approach.

Challenges with an Exclusive Public Cloud

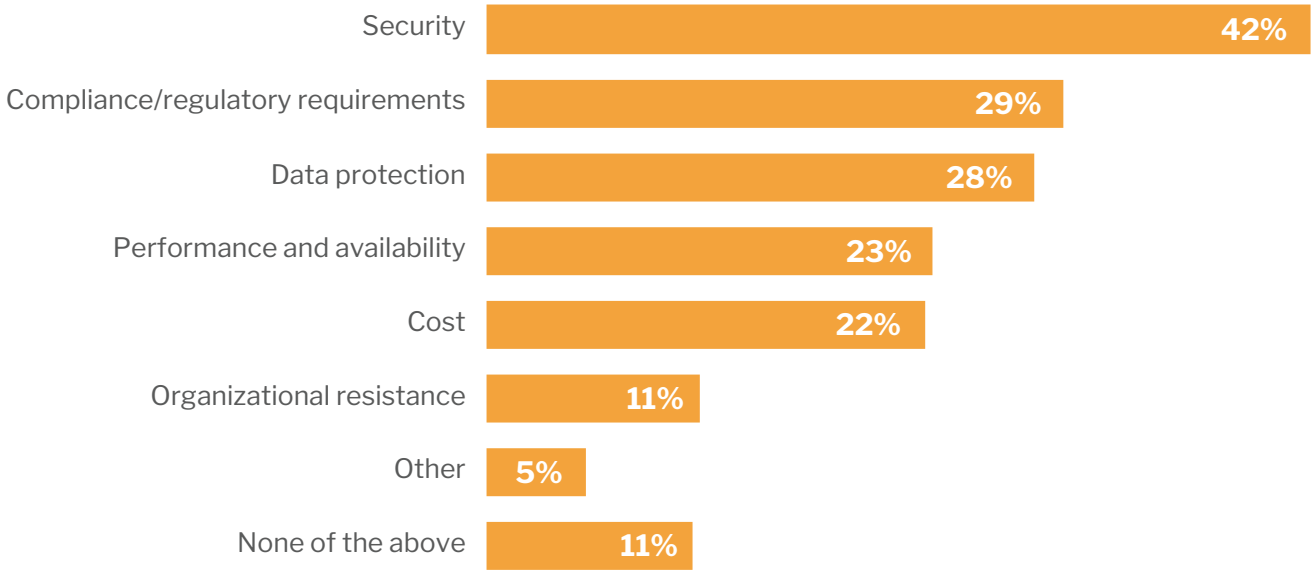
Although public cloud providers highlight customers that are going 'all in' on their platforms, these deployments are exceptions to the rule. Providers may position public cloud as a route to business agility, but the experience of large enterprises migrating applications and data to cloud justifies caution.

Many companies have already targeted applications for cloud migration: top candidates include email and document creation apps and systems of engagement such as customer relationship management and marketing platforms. Once these workloads have moved off-premises, however, continuing transformation becomes much more difficult.

IT decision-makers cited several high-stakes factors (Figure 2) that prevent them from moving workloads to public cloud, including security and data protection (including privacy), performance and cost.

Figure 2: Factors that make workloads unsuitable for public cloud

Source: 451 Research's Voice of the Enterprise: Cloud, Hosting & Managed Services, Workloads and Key Projects 2018
Q: Which of the following factors contribute most to your organization considering a workload unsuitable for running in a public cloud environment? Please select up to 2.



Security and data protection. Public cloud SLAs may guarantee the security of the infrastructure, but it is up to the customer to secure applications and data. If a public cloud security breach does occur, any compensation from the provider will likely pale in comparison to the customer's lost revenue, damaged reputation and regulatory fines. Enterprise stakeholders responsible for protecting a business's valuable intellectual property want to maintain strict visibility and control of the data, and in fact, restricting the physical movement of data is a top requirement of government and industry privacy standards.

"[Some of our data] requires security around the data, so it limits…like only US nationals can gain access. And the question was posed to the cloud vendors like, 'Who has access to the data?' and they couldn't really say who would have access to it. And so, of course, that fails the test basically, so that data cannot reside in the cloud … Legal said well, we can't sign off on that … so for the foreseeable future, it will stay on-premises."

– IT ENGINEERING/MANAGER, $1-2.5BN MANUFACTURING COMPANY

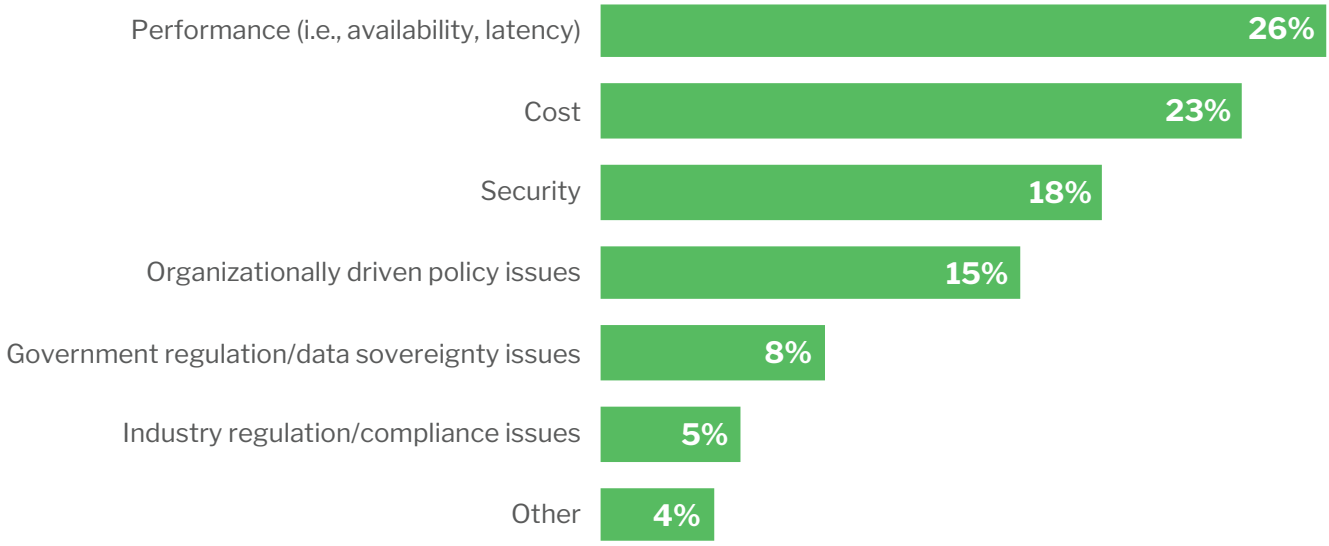
Performance. Public cloud providers tout the high availability of their services, but performance and latency issues continue to crop up. Few enterprises are willing to stake mission-critical operations on best-effort internet connections, and while high-speed direct connections can be provisioned, they come at additional expense. Customers have come to expect instantaneous access to their applications and data, but 'cloudifying' workloads in a way that increases the distance between source data and processing power can introduce unacceptable latency. Similar hang-ups can occur when application integrations need to be improvised as workloads are relocated, or when choke points develop due to inadequate provisioning or misconfigured policy engines.

"We know that there's going to be some stuff that we just can't move to the cloud for whatever reason: data security reasons or physical connectivity reasons, or things like this…We're not going to make any large strategic decision until we get a much better idea of what's going to remain on-site."

– IT/ENGINEERING MANAGER, $2.5-5BN EDUCATION AND TRAINING COMPANY

Figure 3: Drivers for migrating workloads from public to private cloud

Source: 451 Research's Voice of the Enterprise: Cloud, Hosting & Managed Services, Workloads and Key Projects 2018
Q: What was the primary driver for migrating workloads from a public cloud to a private cloud or non-cloud environment?



Cost. Ironically, cost has been both a top driver and a top inhibitor to cloud adoption. In the early stages, easy access to cloud technology and lower costs caused users to consume more. Although unit prices remained low, total spending increased. The convenience of consuming public cloud infrastructure exclusively encourages sprawl and waste; orphaned resources and overprovisioning can add up to unexpectedly high bills. Storing data in the cloud looks like a bargain until customers need to access, move or remove it, when bandwidth charges come into play.

"[For data stored in cloud] accessing the data, you're charged for that. You retrieve the data, you're charged for that. It's not really cheaper than being on-premises or a hybrid model."

–IT/ENGINEERING MANAGER, $1BN-2.5BN MANUFACTURING COMPANY

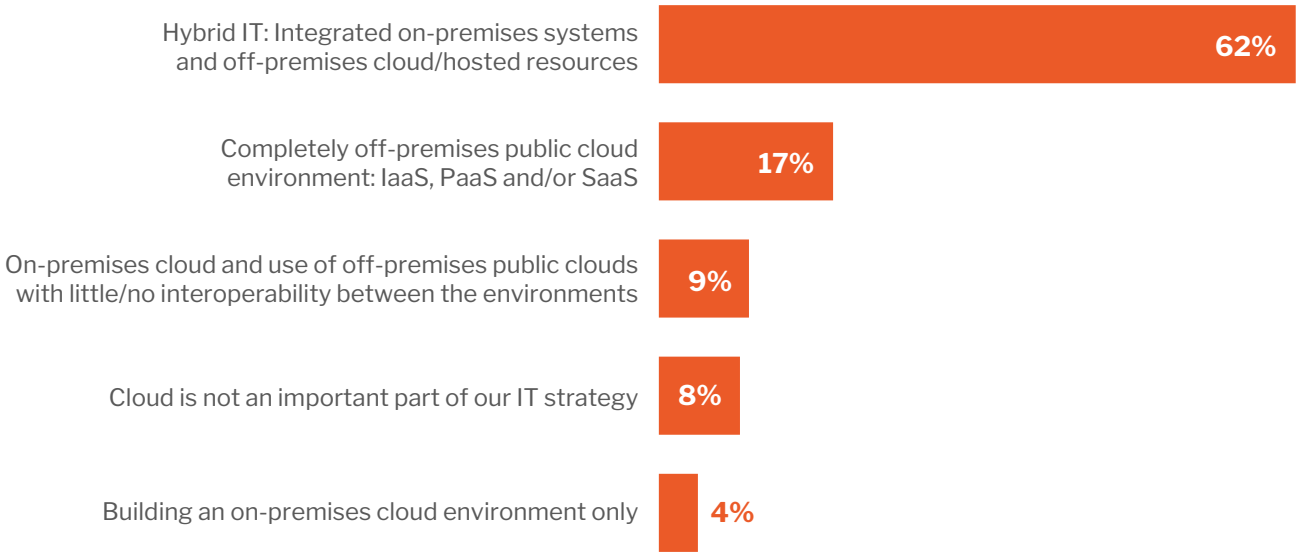
These factors can't be considered in isolation, and in fact, they should be adjusted in relation to each other for the sake of price and performance engineering. Enterprises are willing to pay more for more resilient and secure workloads that make up critical applications while building in flexibility for systems that can tolerate occasional downtime. Such decisions require assessment of the entire IT estate, service interdependencies, and regulatory and policy needs. IT and business decision-makers require different hosting environments for different workloads, but at the same time, they need to be able to secure, manage, integrate, govern, scale, deploy and update across multiple environments, and do so seamlessly and with confidence. There is no single solution that works across the board for all businesses.

Hybrid Cloud is the New Normal

451 Research's Voice of the Enterprise data underscores the prevalence of hybrid IT – meaning an integrated combination of on- and off-premises resources – as the direction for strategic IT (Figure 4). Behind this aggregate view is a more nuanced story. Not surprisingly, hybrid is the preferred (or in effect, default) approach for a greater proportion of large enterprises with more than 10,000 employees (69%) and government/education organizations (73%), while those going 'all in' on public cloud are more likely to be small organizations with fewer than 250 employees (27%).

Figure 4: Strategic approach to IT environments

Source: Voice of the Enterprise's Digital Pulse, Budgets and Outlook 2019
Q: Which of the following best describes your organization's overall IT approach and strategy?



The challenge of creating a secure, integrated hybrid environment is considerable, yet companies are pursuing it as a way to get the best of both worlds: the control and performance of on-premises IT with the pay-as-you-go offerings of public cloud. Large, multibillion-dollar enterprises are looking to modernize their IT estates and deliver services globally, complying with various regulations without having to maintain datacenters in each location. This requires security to be baked into the environment rather than applying it via perimeter hardening.

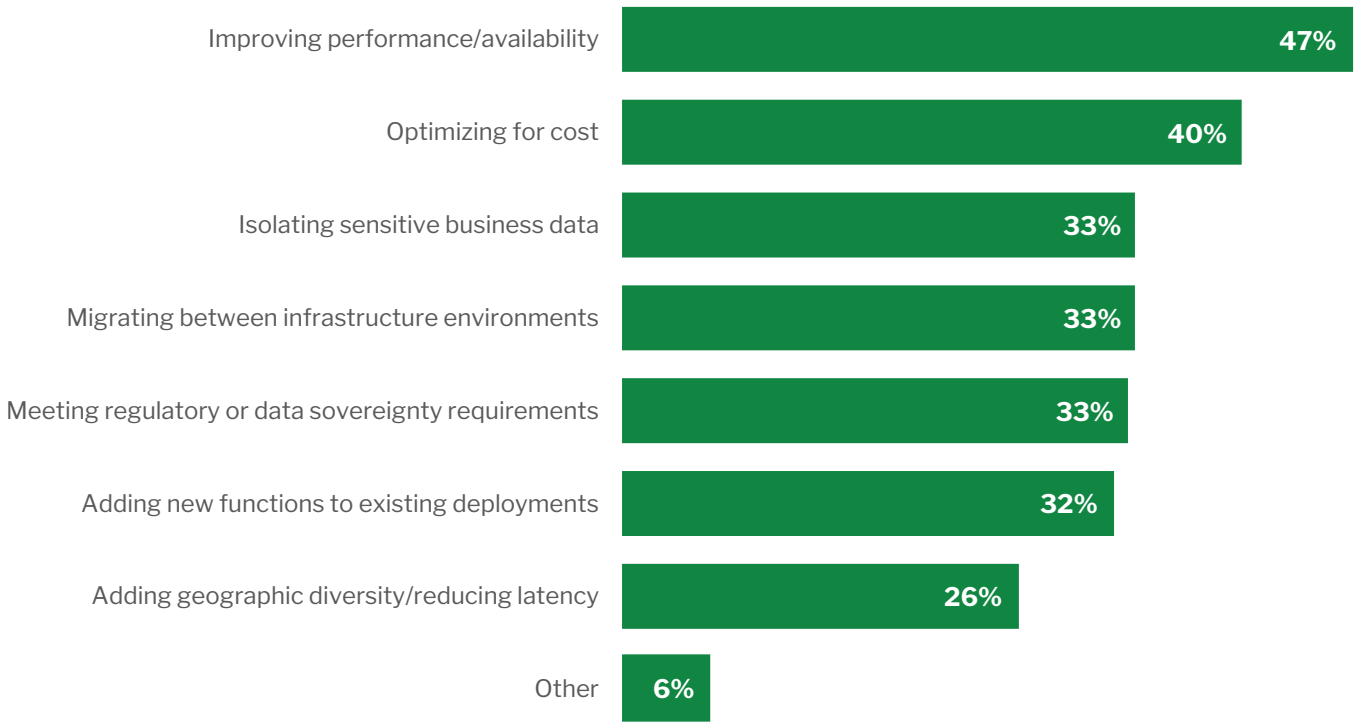
"The three things that govern how we make decisions on workloads – it's reliability, availability is number one; performance is number two; and then costs…[If] putting the content or the workload out into the cloud gives us higher reliability and availability for our customers while increasing performance and it's better, cheaper than doing it on-premises, then it will go to the cloud, as long as we're not Introducing any additional latencies to the customer…We're trying to get to a point to using a workload optimizer that actually looks at network latency as a decision-making process as to where the workload would be placed, whether it be on-premises or cloud."

– IT/ENGINEERING MANAGER, $1-2.5BN BUSINESS SERVICES COMPANY

Motivations for using multiple infrastructure environments highlight the benefits of on-premises and off-premises deployments (Figure 5). The primary factor – improving performance and availability – cuts both ways: popular use cases for public cloud include backup and disaster recovery to ensure availability, but performance concerns may necessitate keeping applications on-premises for quick access to on-site data. The same dual justification goes for the second reason: optimizing for cost. Keeping frequently accessed data stores on-site can save money in the long run, but moving batch workloads to cloud offers the financial advantage of being able to scale up and scale down costs as needed.

Figure 5: Reasons for using multiple infrastructure environments

Source: 451 Research's Voice of the Enterprise: Cloud, Hosting & Managed Services, Workloads and Key Projects 2018
Q: What, if any, of the following best describe your organization's reasons for using multiple infrastructure environments to operate? Please select all that apply.



Other factors point more directly to either on- or off-premises environments. Isolating sensitive business data and meeting data sovereignty requirements are common justifications for keeping data and applications on-premises, whereas adding new functions and adding geographic diversity (using content delivery networks) are common benefits of public cloud.

"We're bringing our first applications into the public cloud…At the same time, we're building up our private cloud within our datacenters…We also have multiple PaaS applications running… 5% of our applications are running in private. This will expand, so we're going to do a lot of migrations in the next couple of years. …[We'll also go] for a hybrid cloud setup. So not only having the different offerings next to each other, but also…load-balancing functionality that we can move workloads from private to public and vice versa."

– MID-LEVEL MANAGER, $10BN+ FINANCIAL SERVICES COMPANY

Conclusions

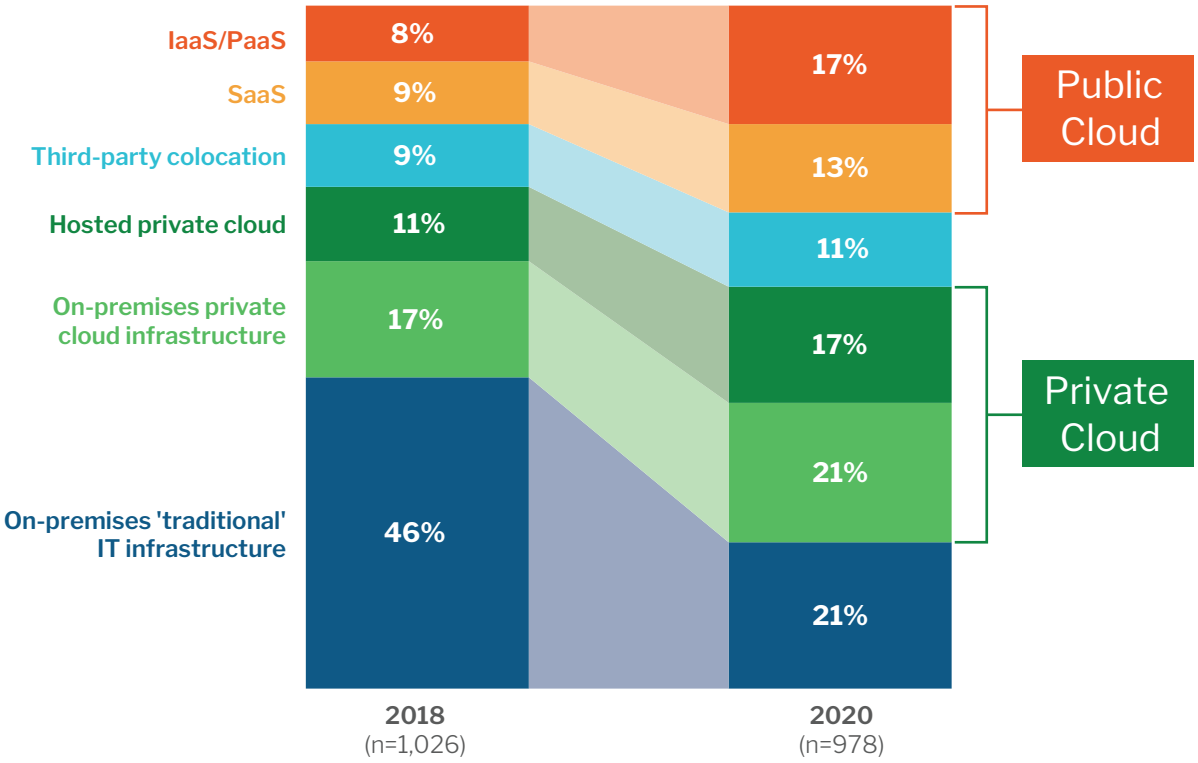
One size does not fit all when it comes to workloads and data hosting. Digital transformation requires a flexible approach to deploying workloads and data in a way, and in a location, that optimizes security, integration, flexibility, management, and agility, whether on- or off-premises or both.

Hybrid cloud environments encompassing both on-prem and off-prem deployments are clearly the direction enterprises are taking (Figure 5). Cloud transformation is occurring both in the datacenter and off-premises, and IT decision-makers plan to increase their use of both in the coming years.

Figure 6: Enterprises are headed toward cloud deployments

Source: 451 Research's Voice of the Enterprise: Digital Pulse, Workloads and Key Projects 2018

Q: Thinking about all of your organization's workloads/applications, where are the majority of these currently deployed? Where will the majority of these be deployed two years from now?



The challenge of workload placement will dominate the digital transformation conversation for the foreseeable future. Public cloud makes IT procurement and management easier for certain workloads, but this convenience comes at a cost. Not all applications and data can or should make the transition: compliance factors, dependencies and latency issues can underlie the decision to keep some resources on-premises. At the same time, cutting-edge cloud services and cloud-native development techniques are giving IT departments access to tools and innovation that can revolutionize service delivery and user experience.

Maintaining security is paramount when migrating and refactoring IT systems to take advantage of the wealth of destinations available. Federation of identity and access management across public and private clouds is critical, and pervasive encryption of data is necessary to ensure that increasingly distributed systems remain tamper-proof while IT estates are upgraded and modernized to seize the possibilities of the next 20 years.

Enterprises are adapting and optimizing for digital transformation, and to be successful, they need advanced security and privacy in both traditional and cloud technologies. A combination of highly scalable infrastructure and security-rich cloud services creates a reliable and dependable hybrid solution. IBM LinuxONE™ is an open source enterprise platform that sets new performance standards for today's cloud native applications. Learn how IBM LinuxONE offers advanced security and scalability for on-premises and off-premises cloud deployments at *ibm.com/linuxone/secure-cloud*.

Customers are looking for public cloud services that can help them build apps faster and with added security capabilities. That's why IBM put the LinuxONE platform in the IBM public cloud with a suite of solutions which includes dedicated cryptographic key management and database services, among others. Learn how IBM Cloud™ Hyper Protect Services puts you in total control of your public cloud environment at *ibm.com/cloud/hyper-protect-services*.

CONTENT PROVIDED BY

IBM

About 451 Research

451 Research is a leading information technology research and advisory company focusing on technology innovation and market disruption. More than 100 analysts and consultants provide essential insight to more than 1,000 client organizations globally through a combination of syndicated research and data, advisory and go-to-market services, and live events. Founded in 2000 and headquartered in New York, 451 Research is a division of The 451 Group.

NEW YORK
1411 Broadway
New York, NY 10018
+1 212 505 3030

SAN FRANCISCO
505 Montgomery,
Suite 1052
San Francisco, CA 94111
+1 212 505 3030

LONDON
Paxton House
30, Artillery Lane
London, E1 7LS, UK
+44 (0) 203 929 5700

BOSTON
75-101 Federal Street
Boston, MA 02110
+1 617 598 7200

451 Research®