ESG Research Insights Paper

Exploring Hybrid Cloud Adoption and the Complexity of Securing East-West Traffic

Consistent Controls Are a Prerequisite for Securing Hybrid Cloud Environments

By Doug Cahill, ESG Senior Analyst; and John Grady, ESG Analyst

January 2020

This ESG Study was commissioned by VMware and is distributed under license from ESG.

Contents

Executive Summary

In September 2019, the Enterprise Strategy Group (ESG) completed a research survey of 200 IT decision makers directly knowledgeable about their organizations' cloud priorities and perceptions. Additionally, organizations represented were all required to be using or planning to use public cloud infrastructure-as-a-service (IaaS) within the next three years. Further details of the research methodology and survey demographics are presented in the appendix section of this report.

Based upon the research conducted in this study, ESG concludes:

- **Hybrid clouds and applications are becoming pervasive.** Only 8% of organizations using multiple cloud service providers (CSPs) have no interest in hybridizing their applications, while a full quarter of respondents report multiple production applications utilizing a hybrid model. To ensure security, compliance, and performance in these complex architectures, organizations require tools that provide consistency in policy and management across disparate environments.

- **Companies that adopt data center-as-a-service (DCaaS) solutions will quickly transition their on-premises infrastructure to that model.** Early use cases must be proven out, but there is very strong interest in DCaaS (e.g., AWS Outposts, and Google Anthos). Of those organizations that expect to adopt DCaaS, most believe it will account for at least half of their on-premises infrastructure. The ability to consume IT services via a managed, on-demand, operational expense-based model while retaining data on-premises to mitigate security, compliance, and performance concerns is attractive to many organizations.

- **Enforcement of east-west policies will increase, but consistency is desperately needed.** The vast majority of organizations understand the importance of securing east-west traffic, but only 37% currently enforce east-west security policies today. There is strong interest from those who have not currently implemented solutions to do east-west enforcement, but based on infrastructure adoption trends, tools that provide consistency across multi-cloud, hybrid-application, and on-premises architectures are required. Three-quarters of organizations report this is a top security product purchase consideration.

Hybrid Cloud Adoption Has Become the New Norm, but Continues to Evolve

The continued growth in the adoption of public cloud infrastructure is well-documented. In fact, ESG research indicates the overall percentage of organizations using or planning to use infrastructure-as-a-service (IaaS) has grown from 21% in 2013 to 58% in 2019.[1] There are a variety of reasons for this.

- The agility and scalability provided by leveraging on-demand public cloud resources rather than procuring and deploying infrastructure on-premises play a critical role in digital transformation initiatives.

- Detaching applications from the underlying infrastructure allows organizations to focus resources and IT cycles on the application itself.

- The attractiveness of shifting infrastructure costs from a capital to operational expense continues to be an important factor in the adoption of public cloud services.

[1] Source: ESG Master Survey Results, *2019 Technology Spending Intentions*, March 2019.

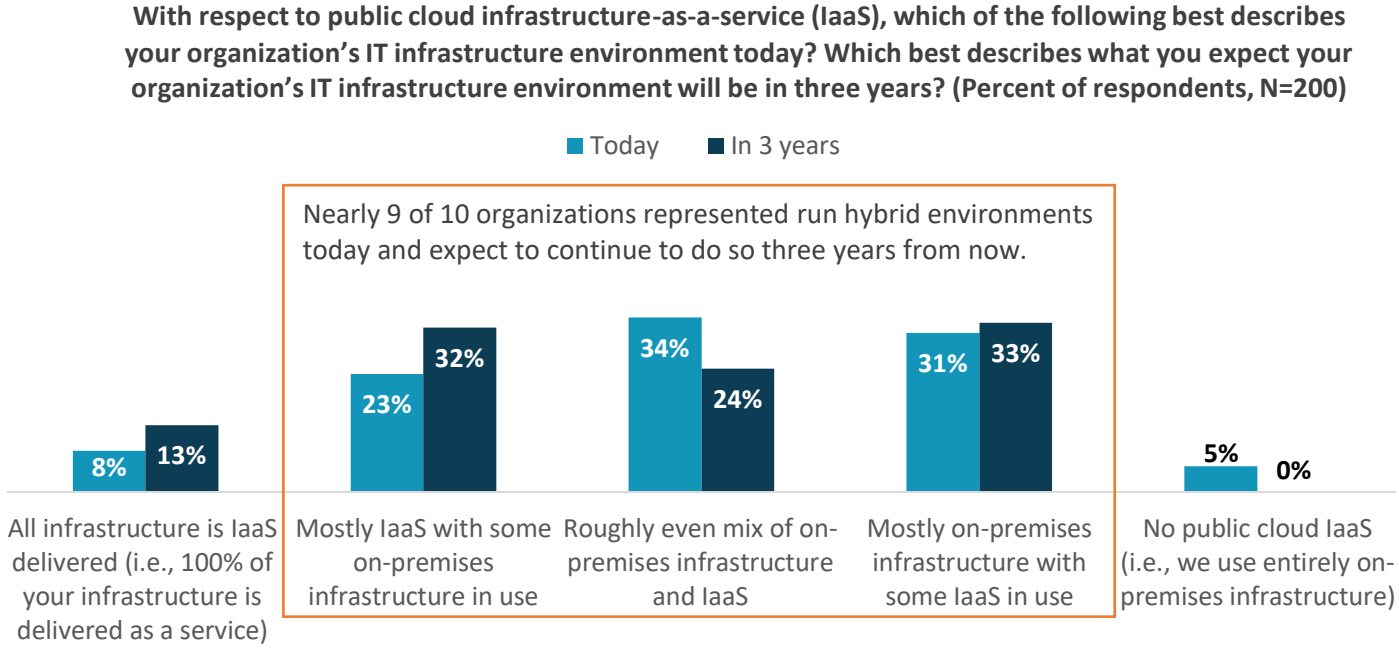
Multi-location Infrastructure Is—and Will Remain—Prevalent

However, despite the litany of benefits that public cloud services afford, most organizations will continue to employ a mix of cloud and on-premises infrastructure. Currently, 88% of survey respondents report using both IaaS and on-premises infrastructure (see Figure 1). This is expected to remain essentially unchanged over the next few years, with 89% of respondents expecting to use a mix of IaaS and on-premises infrastructure three years from now. However, while topline IaaS usage will stay constant, organizations' reliance on IaaS will increase. Whereas 32% of respondents currently use IaaS for most to all of their IT infrastructure, 45% report they will rely on IaaS for most or all of their infrastructure in three years.

Additionally, the usage of multiple CSPs will continue to grow, with the percentage of respondents using two or more CSPs expected to increase from 75% currently to 81% in three years. The specific characteristics of a multi-CSP approach can vary greatly.

- IaaS deployments may naturally sprawl across multiple CSPs over time due to the self-service nature of cloud and line-of-business involvement in development activities.
- One CSP may be used for external production applications, while development and testing environments for internal applications are maintained with a different CSP.
- Availability based on geography may play a role in the adoption of multiple CSPs.
- Some organizations seek to avoid vendor lock-in by spreading usage across multiple providers.
- For the most business-critical applications, spreading applications across multiple CSPs can improve disaster recovery.
- The specific capabilities of providers relative to the infrastructure requirements of legacy applications can also play a role in utilizing different CSPs for different applications.

Figure 1. Multi-location Infrastructure



Source: Enterprise Strategy Group

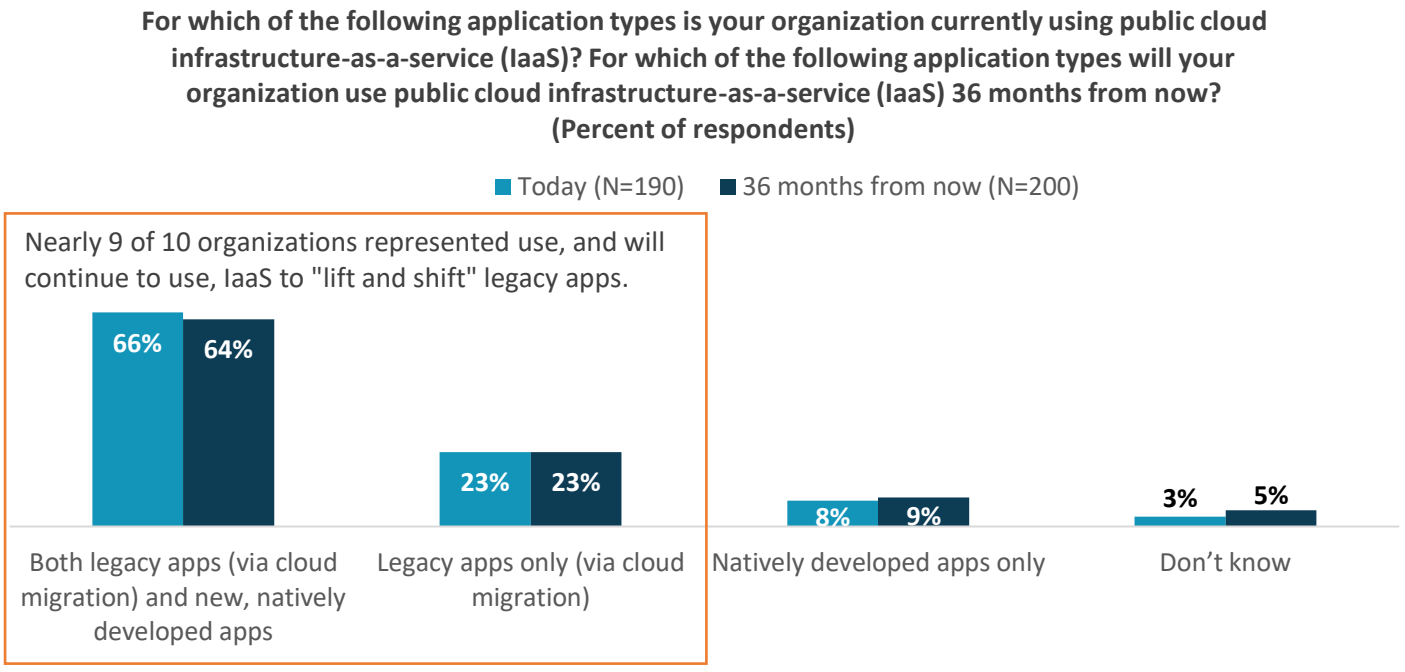
The Migration of Legacy Applications Introduces Additional Challenges

The logical follow-on question then becomes: With public cloud providing so many benefits, why are organizations maintaining an on-premises infrastructure? The reasons, as they often do, vary. To begin with, most organizations are not building an infrastructure from scratch; and moving the entirety of an established infrastructure and application environment to the cloud is typically not feasible. But beyond that, there are certain business reasons to maintain an on-premises infrastructure as well.

- Data residency and compliance concerns still play a role in organizations maintaining parts of their infrastructure on-premises.
- Similarly, questions about the shared security model can give organizations pause relative to pushing critically sensitive data to the cloud.
- For some legacy applications with specific requirements (like having to run them on mainframe systems, for example), the cost and difficulty in rearchitecting for the cloud is prohibitive.

Yet for IaaS adoption to be as robust as it is, it cannot solely be driven by the adoption of net/new, cloud-native applications; legacy applications must also be migrated. The survey results bear that phenomenon out, with 89% of respondents reporting that they use IaaS for the migration of legacy applications from on-premises infrastructure (see Figure 2).

Figure 2. The Use of Cloud Is Multifaceted



Source: Enterprise Strategy Group

While incorporating security into the continuous integration and continuous delivery (CI/CD) and DevOps process for natively developed cloud applications is a challenge that garners a lot of attention, migrating legacy applications to IaaS environments comes with its own set of challenges, both from a business and IT perspective. Refactoring monolithic applications to the microservices-based architecture of the cloud can result in higher complexity, longer time to market, and increased cost and risk; and ultimately limit some of the expected benefits and efficiencies of an IaaS deployment.

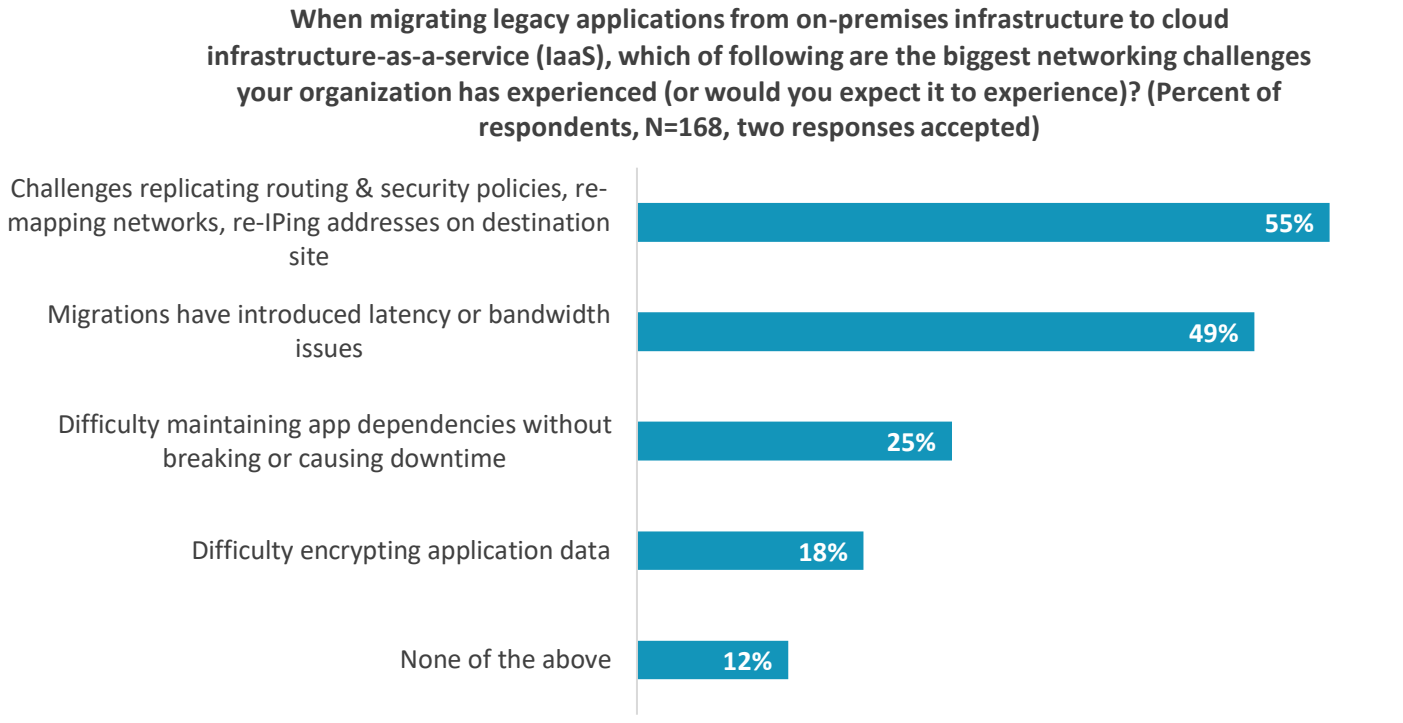
While the idea of "lift and shift" implies simplicity and that the application is left unchanged, issues can arise if applications are not properly reconfigured. In all, 88% of respondents cited at least one networking challenge when migrating legacy applications to IaaS.

- **Replicating consistent networking policy -** The most common challenge, cited by 55% of respondents, was difficulty replicating consistent networking policy when shifting to cloud (see Figure 3). This includes routing and security policies, remapping networks, and re-IPing addresses on destination sites. Specifically, incorporating geo-location, geo-proximity, failover, and other routing policies is necessary to ensure application performance and security, and can become a complex task.

- **Latency and bandwidth issues -** Nearly half of respondents (49%) reported that migrations have introduced problematic application latency or that they have had difficulties providing adequate bandwidth. With some applications being more latency-sensitive than others (like video conferencing and collaboration tools, gaming, and digital content), the distributed architecture of the cloud requires a thorough understanding of network routing paths relative to cloud data centers, as well as potential bottlenecks on those paths, and ultimately an intimate understanding of application performance relative to those factors. In some instances, the most mission-critical enterprise applications may require dedicated internet links to cloud providers to alleviate some of these issues.

- **Maintaining application dependencies -** The microservices-based architecture of the cloud is fundamentally different than the monolithic nature of many legacy applications. As such, 25% of respondents report challenges in maintaining application dependencies without breaking the application or causing downtime. Even with detailed dependency mapping, application reliance on the existing infrastructure can be overlooked until it has already been migrated.

Figure 3. Challenges in Migrating Legacy Applications



Source: Enterprise Strategy Group

Hybrid Applications Only Exacerbate the Difficulties

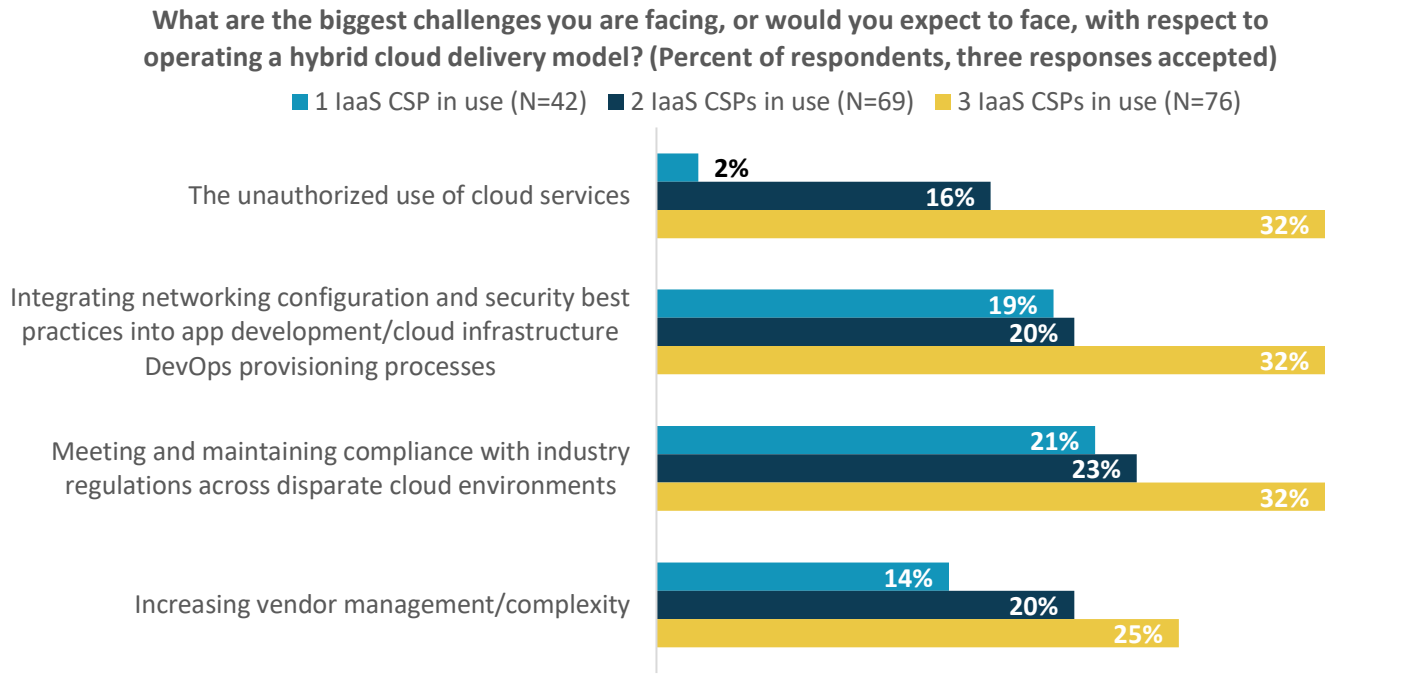
These challenges become more acute when accounting not just for hybrid environments (like public cloud services and on-premises) and multiple cloud providers, but hybrid applications as well. For the purposes of this study, hybrid applications were defined as an application hosting model where different tiers of an application are run in different locations and on different infrastructure. For example, the database tier of an application may run in an on-premises, customer-managed data center while the presentation/web tier might run on a public cloud infrastructure. As noted previously, over three-quarters of respondents use two or more CSPs.

Those respondents using multiple CSPs were then asked whether their organizations deploy tiers of production applications in different locations (i.e., use hybrid applications). Nearly all (92%) multi-cloud respondents have currently deployed, plan to deploy, or are interested in deploying a hybrid application model. Over half (52%) have already hybridized at least one production application, meaning this is not a future, but rather a current dynamic organizations must address.

Among those respondents interested in or using hybrid applications and three or more CSPs, the following challenges were reported (see Figure 4):

- 32% indicated they are concerned about the unauthorized use of cloud services.
- 32% reported that integrating network configurations and security best practices in the application development/cloud infrastructure DevOps provisioning process was a challenge.
- 32% said meeting and maintaining compliance with industry regulations across disparate cloud environments was difficult.
- 25% pointed to increasing vendor management and complexity as a concern.

Figure 4. Concerns about Hybrid Operating Models by Number of CSPs



Source: Enterprise Strategy Group

Data Center-as-a-service Appears to Be an Attractive On-premises Alternative

As the hybrid model continues to evolve, organizations must consider how their on-premises and cloud infrastructures integrate seamlessly. In fact, 73% of respondents indicated that it is critical or very important that public cloud vendors offer solutions that integrate with the user's on-premises environment.[2] To enable this integrated on-premises public cloud, or private cloud model, data center-as-a-service solutions have begun to gain traction.

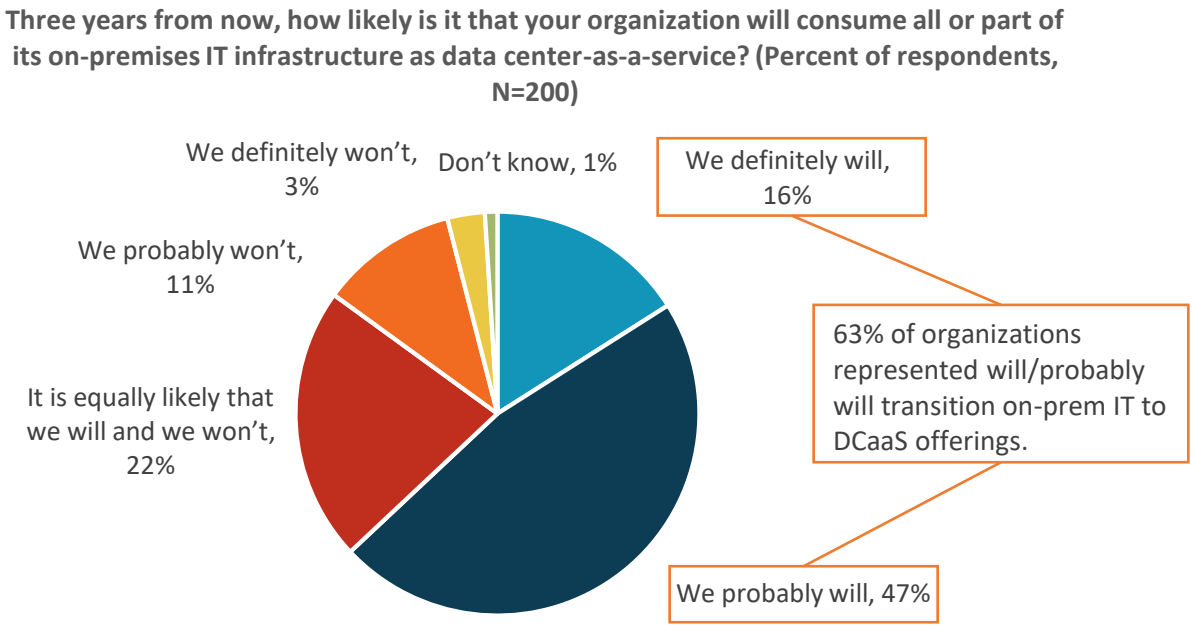
Data center-as-a-service is an on-premises infrastructure model where infrastructure resides in a data center owned by the customer but is consumed as a managed service. The customer does not own the physical resources (servers, storage, and networking), but rather consumes resources as if they resided at a cloud service provider's data center. DCaaS examples include AWS Outposts and Google Cloud Anthos.

Early Interest in Data Center-as-a-service Is High

When asked how likely their organization will be to use data center-as-a-service in three years, 63% of respondents reported it likely that some portion of their on-premises infrastructure would be DCaaS (see Figure 5). However, only 16% of respondents reported their organization would definitely use DCaaS. In other words, while interest is high, early adopters will have to prove out the benefits to push those on the fence toward adoption. If early use cases do not bear out the benefits, the high percentage of those organizations that are currently noncommittal may look to alternative solutions.

That said, if the benefits are as expected, expectations are high that DCaaS will account for a significant amount of on-premises infrastructure quickly. Of those respondents that indicated they may consume on-premises IT as DCaaS, 55% expect at least half of their on-premises infrastructure to be DCaaS in three years. Another 36% expect DCaaS to account for between a quarter and a half of their on-premises infrastructure.

Figure 5. Data Center-as-a-service Adoption Expectations



Source: Enterprise Strategy Group

[2] Source: ESG Master Survey Results, *Hybrid Cloud Trends*, May 2019.

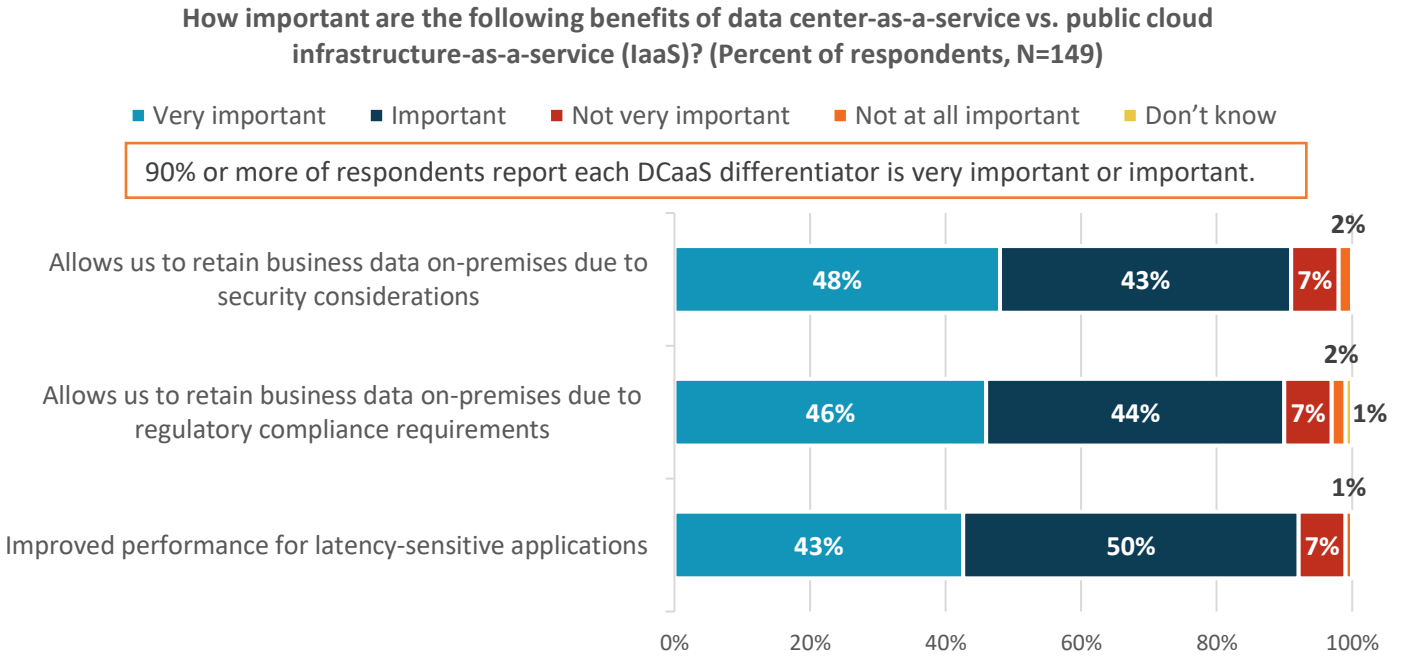
Data Center-as-a-service Is Viewed as Offering Superior Operational and Security Benefits

At a high level, DCaaS poses an attractive alternative for the majority of organizations that expect to retain a mixed infrastructure comprised of on-premises resources and public cloud services. DCaaS adoption better aligns the on-premises model to cloud and alleviates some of the complexities associated with hybrid multi-cloud environments, offering many benefits over legacy infrastructure. Moreover, the importance to respondents of these benefits relative to legacy on-premises infrastructure is noteworthy:

- 93% report uptime/availability improvements are important.
- 90% indicated reduction of time spent on infrastructure management is important.
- 90% say faster procurement and availability of IT services is important.
- 85% say the effectiveness of DCaaS as a means to refresh infrastructure matters.

Similarly, the stated benefits of adopting DCaaS over public cloud IaaS center on the perceived security, compliance, and performance concerns organizations have around public cloud services. Specifically, nine out of ten respondents said the ability to retain business data on-premises due to security or regulatory compliances issues and the improved performance for latency-sensitive applications are important advantages DCaaS holds over IaaS (see Figure 6).

Figure 6. Advantages of DCaaS versus IaaS



Source: Enterprise Strategy Group

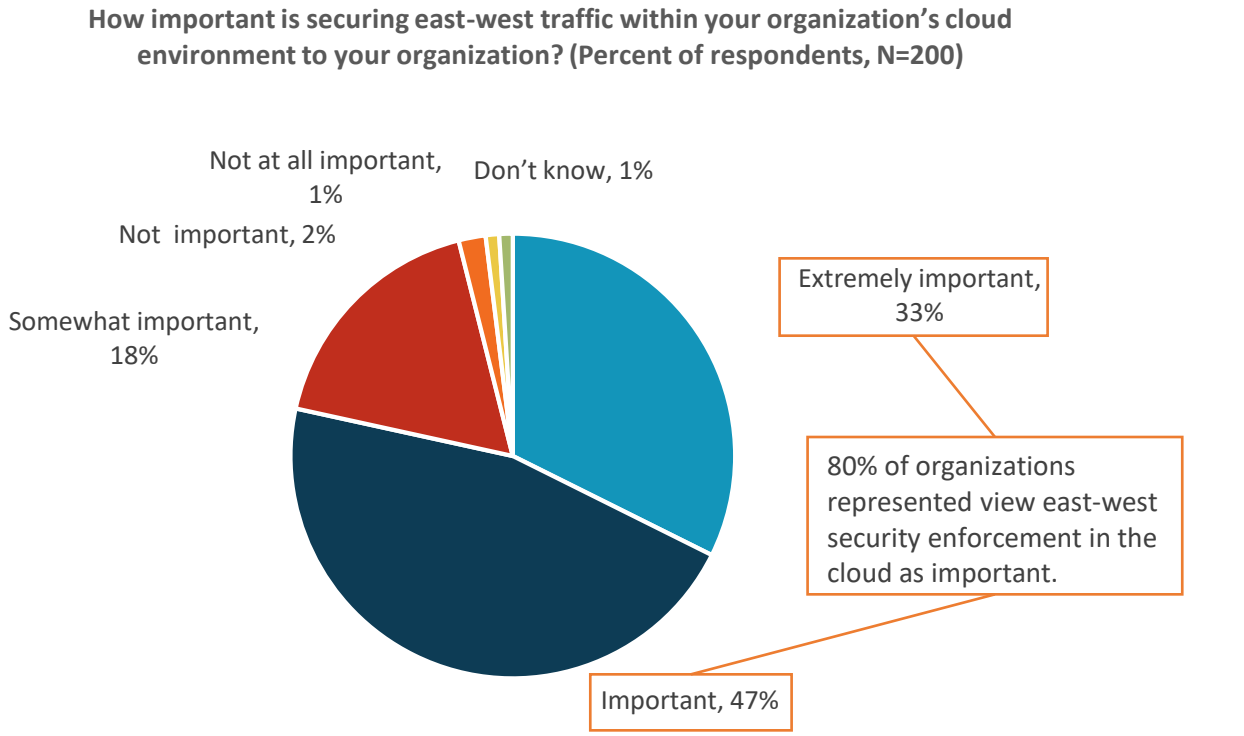
Security Importance Is Recognized, but Not Necessarily Enforced

Securing East-west Traffic Is Critical in a Hybrid, Multi-cloud World

Monitoring and controlling east-west traffic was an often-overlooked aspect of security programs when data centers were primarily on-premises. By implementing firewalls, intrusion detection/prevention systems, and other controls at the data center perimeter, organizations had control at least over the north-south traffic. However, with virtualization and then cloud adoption fundamentally changing the architecture of the data center, the amount of east-west traffic has exploded over the last decade. The expansion of hybrid multi-cloud environments only complicates the issue, with east-west traffic now moving in a north-south direction, on- and off-premises between the data center and cloud. The microservices-based nature of cloud-native applications by default contains more discrete tiers than traditional client-server applications, making inter-application east-west traffic an even greater security concern.

Yet because of this, securing east-west traffic takes on even greater importance, despite the increase in complexity. Limiting the lateral movement of attackers once they've gained a foothold in the environment and preventing malicious or curious insiders from taking advantage of broad access both require visibility and control over east-west traffic. The good news is that organizations recognize this, with 80% of respondents indicating that securing east-west traffic is important (see Figure 7).

Figure 7. The Importance of Securing East-west Traffic

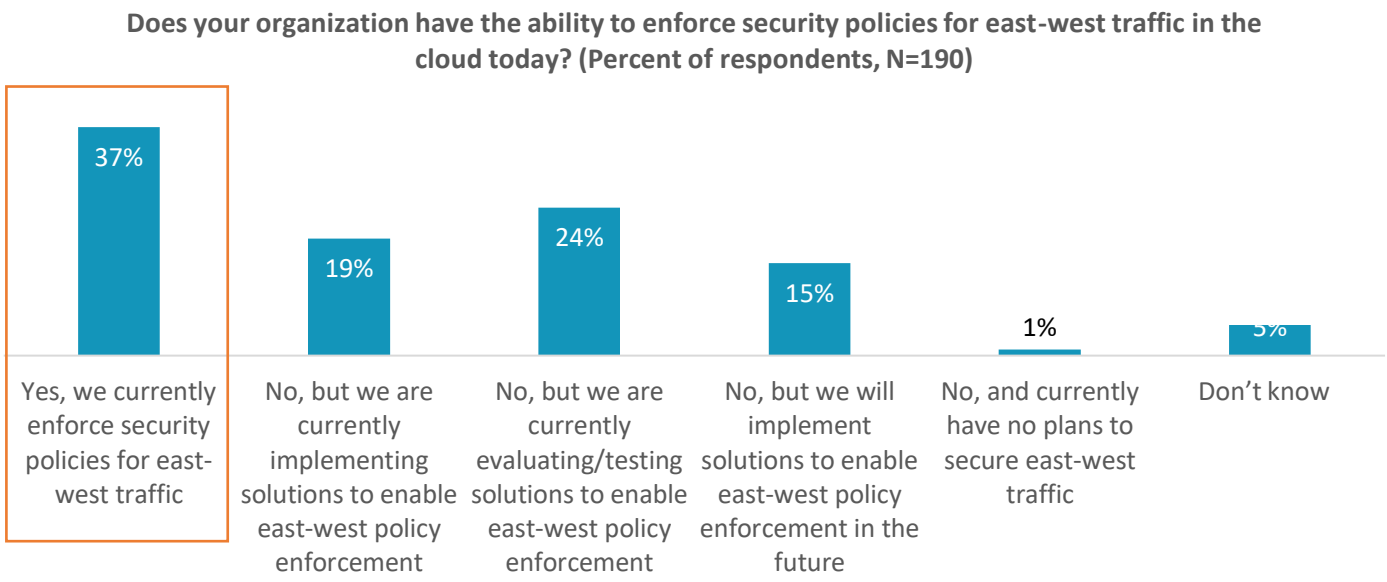


Source: Enterprise Strategy Group

Most Organizations Do Not Implement East-west Policy and Desire More Consistent Controls

However, the number of organizations actually implementing east-west security policies significantly lags those recognizing the importance of the practice. Only 37% of respondents currently enforce east-west traffic, less than half of those who indicate it is important. It is important to note that 19% of respondents are in the process of implementing, and 24% are currently evaluating, east-west policy solutions. So, organizations are moving in the right direction, but the disparity between current enforcement and recognized importance remains.

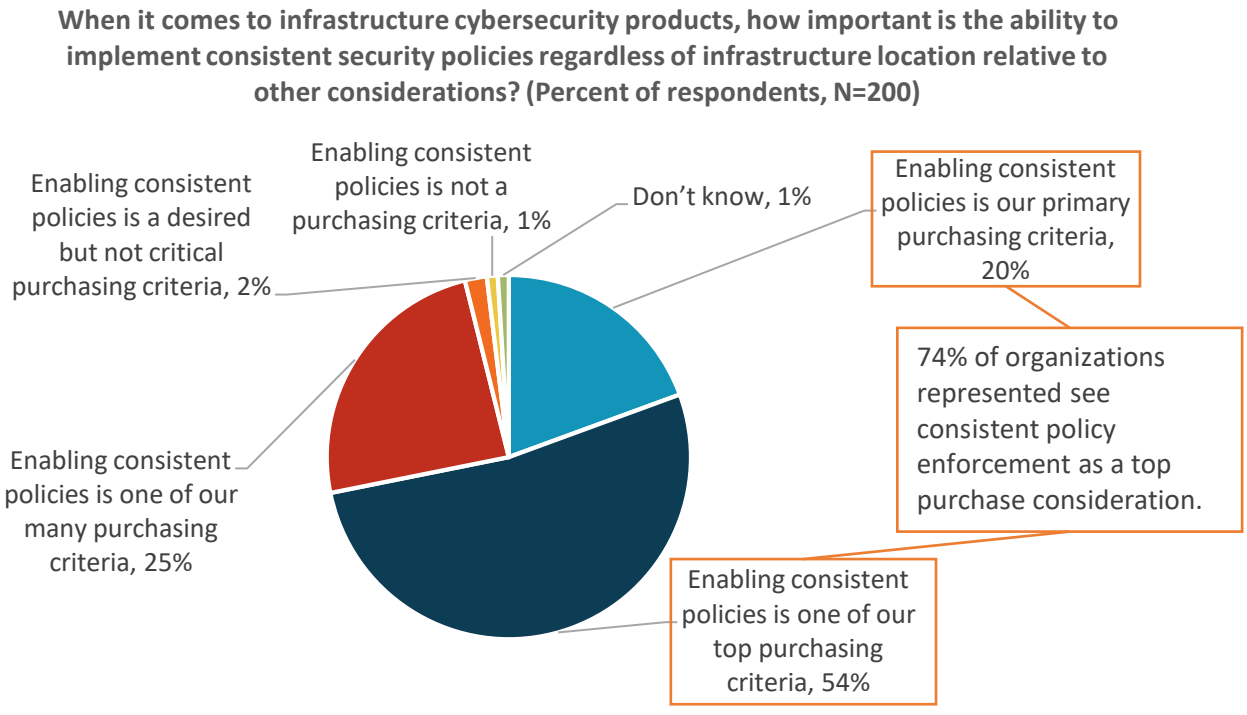
Figure 8. Implementation of East-west Security Policies



Source: Enterprise Strategy Group

One reason for this disconnect is the need for security tools to provide consistency across different environments. To secure and inspect east-west traffic, a majority of respondents use or plan to use host-based firewalls and/or distributed intrusion detection/prevention systems (IDS/IPS) as a means to implement micro-segmentation. Consistent policy and enforcement across different environments is crucial for these strategies to be successful. Therefore, it is imperative for these solutions to work across disparate clouds and on-premises environments. This is clearly a priority for buyers, with the ability to implement consistent security policies regardless of infrastructure location being listed as a top product purchase consideration for 74% of respondents (see Figure 9).

Figure 9. Consistent Security Policies



Source: Enterprise Strategy Group

The Bigger Truth

The IT environments of most organizations have become a patchwork of on-premise technologies, public cloud services, legacy applications and systems, and emerging technologies—and the situation is only becoming more complex. As organizations shift more resources to an increasingly diverse set of cloud providers and continue to spread more of their applications across multiple cloud environments, the idea of a traditional perimeter becomes a faint speck in the rearview mirror. As the security adage goes, you can't protect what you can't see.

In order to reduce the attack surface and limit the potential impacts of a breach, it is imperative to maintain deep visibility and granular control over east-west application traffic, regardless of location. In order to accomplish this, solutions such as distributed IDS/IPS and micro-segmentation that provide consistent enforcement and centralized control across disparate cloud and on-premises environments are prerequisites for organizations that have adopted a hybrid, multi-cloud approach to infrastructure.

Appendix: Research Methodology and Respondent Demographics

To gather data for this report, ESG conducted a comprehensive online survey of IT decision makers directly knowledgeable about their organizations' cloud priorities and perceptions. Nearly two-thirds of respondents held senior IT or security titles (i.e., CIO, CISO, VP of IT/IS, or equivalent) while the remainder held middle management and staff titles. All respondents were based in North America and employed at organizations with 100 or more employees. Specifically, 27% were employed at midmarket organizations (i.e., those with 100 to 999 employees) and 73% at enterprises (i.e., organizations with 1,000 or more employees). Respondents represented numerous industry and government segments, with the largest participation coming from information technology (19%), manufacturing (14%), healthcare (13%), financial services (12%), government agencies (9%), and education (9%).

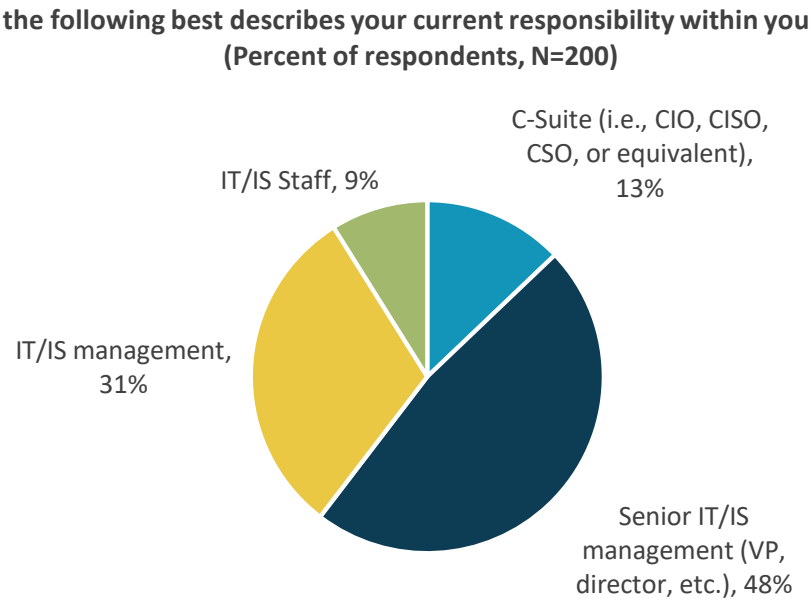
The survey was fielded between September 16, 2019 and September 21,2019.

After filtering out unqualified respondents, removing duplicate responses, and screening the remaining completed responses (on several criteria) for data integrity, a final sample of 200 respondents remained.

All respondents were provided an incentive to complete the survey in the form of cash awards and/or cash equivalents. Note: Totals in figures and tables throughout this report may not add up to 100% due to rounding.

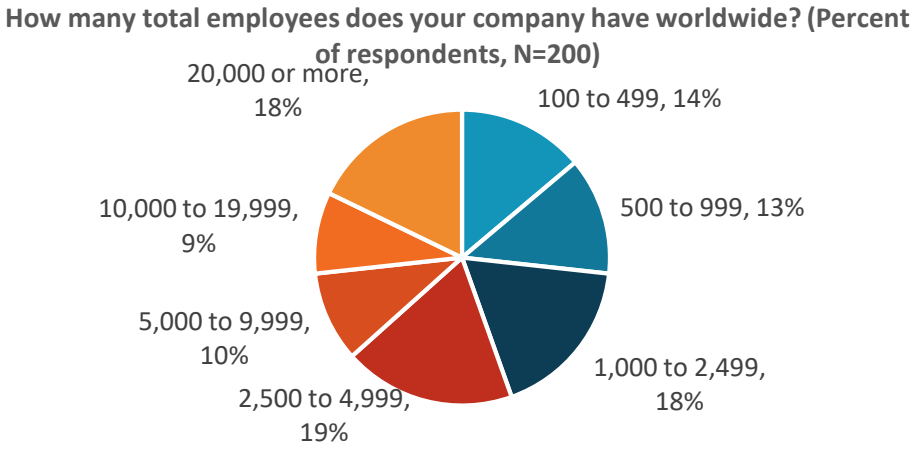
The figures below detail the full demographics of the respondent base: individual respondents' roles, as well as respondent organizations' total number of employees, annual revenue, and primary industry.

Figure 10. Survey Respondents, by Current Responsibility



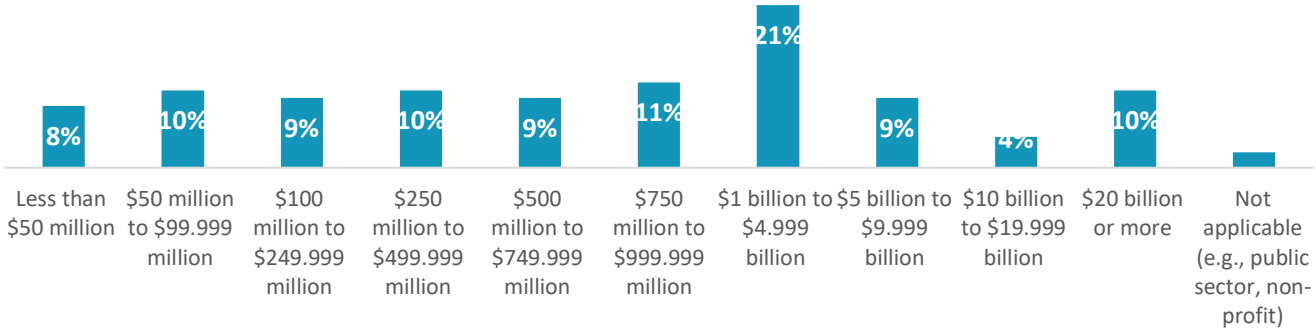
Source: Enterprise Strategy Group

Figure 11. Survey Respondents, by Company Size (Number of Employees)



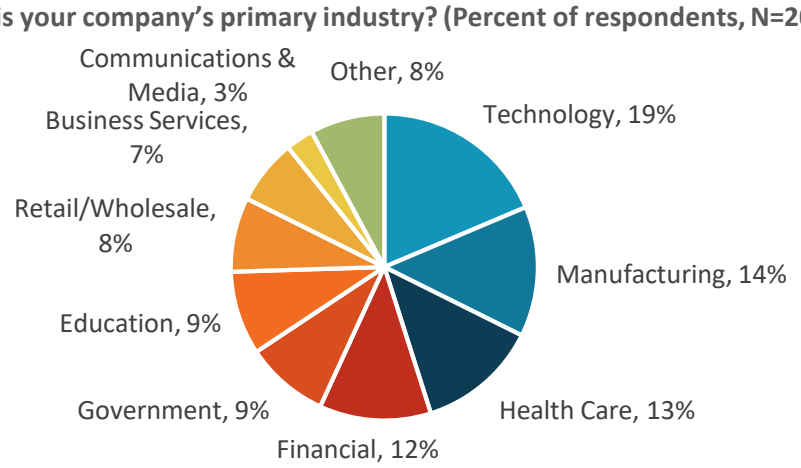
Source: Enterprise Strategy Group

Figure 12. Survey Respondents, by Company Size (Revenue)



Source: Enterprise Strategy Group

Figure 13. Survey Respondents, by Industry



Source: Enterprise Strategy Group

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides actionable insight and intelligence to the global IT community.

 www.esg-global.com

 contact@esg-global.com

 P. 508.482.0188