EXECUTIVE SUMMARY

As organizations undergo digital transformation and continue to increase their cloud consumption, more and more organizations are finding that a “multicloud” environment is the new norm. According to IDC’s 2017 CloudView Survey, most cloud users are running more than one type of cloud deployment and work with more than one major public cloud provider (i.e., PaaS, IaaS, SaaS, private, hybrid, and public) — and this new world of “multicloud” comes with new challenges and new priorities. There’s a significant difference between merely adopting multiple types of cloud and having the skills and processes in place to manage a hybrid IT environment. This white paper highlights best practices used to thrive in a multicloud world across operations and management, shares data from IDC’s CloudView Survey and Business Value Research illustrating multicloud adoption and associated business outcomes, and analyzes market growth, vendor tools, and pitfalls to avoid.

Multicloud adoption is an important part of IT organizations’ strategies; infrastructure and operations teams, cloud architects, and developers are growing more sophisticated in how they adopt and deploy cloud services from multiple public, private, and hybrid models. As of 2017, enterprise adoption of multicloud services has moved into the mainstream, with 85% currently using services from multiple cloud providers. Over the next 12 months, this number will rise to 93%.

CIOs and executive management teams are responding to the adoption of cloud services by creating cloud-first policies that drive the adoption of cloud services (including public and private/hosted private) and the execution of cloud-based IT delivery strategies. Fifty-four percent of C-level executives have made the cloud model their primary option for the delivery of IT capabilities. As the number of cloud providers used increases in the enterprise, so does the complexity of underlying processes and technologies that must be deployed, managed, and automated. In a multicloud
world, the proliferation and integration of traditional and modern applications (i.e., containers, DevOps practices, software-defined networks [SDNs], and microservices) require sophisticated management and orchestration capabilities. Effective management of containers and microservices enables infrastructure, operations, and cloud architects to adjust and scale to the increase in software deployment frequency that development teams deliver through multicloud channels. In addition, business executives have demanded new capabilities, often delivered through SaaS applications, that require IT management and control.

More mature adopters enjoy better business outcomes, including increased revenue and more strategic allocation of IT budget. The greater the level of cloud maturity, the more likely organizations will support advanced technologies including microservices architectures, containers, agile and DevOps practices, open source, and Internet of Things (IoT).

This white paper suggests that as companies continue to deploy more cloud services from multiple providers, the business benefits of increased agility, faster time to market, cost optimization, and product innovation are expected to increase. In fact, 56% of cloud adopters use cloud services to enable innovation, 50% expect the cloud to improve business agility, and 37% expect cloud services to improve their time to market. In addition, IDC expects that by 2021, the installed base of container hosts (physical and virtual) will reach nearly 50 million and the number of container instances concurrently installed will reach 3 billion (see Container Infrastructure Market Assessment: Bridging Legacy and Cloud-Native Architectures — x86 Software Containers Forecast, 2017–2021, IDC #US43661118, March 2018). Containers are expected to become ubiquitous in the datacenter. However, to achieve optimized results from cloud services, IT executives and their teams must invest to increase their level of cloud maturity across their staff, technologies, and processes. The more mature organizations have greater revenue and can more strategically allocate their IT budgets to keep more focus on innovation and less on activities necessary to “keep the lights on.”

IDC has identified five stages of cloud maturity: ad hoc, opportunistic, repeatable, managed, and optimized (in order of increasing maturity). While there are immediate benefits even from moving one step up from ad hoc to opportunistic, the benefits accrue and grow as you move further up the adoption curve. Only 44% of IT organizations have reached the repeatable, managed, or optimized phases of maturity, indicating that the industry has more work to accomplish in delivering business results in a multicloud world. This white paper provides CIOs, CTOs, infrastructure and operations teams, cloud architects, and DevOps executives with actionable advice and a risk mitigation blueprint for the effective evolution, management, and security of multicloud environments.
About This White Paper

This white paper is based on IDC’s 2017 CloudView Survey, for which IDC interviewed director-level and above respondents from a global sample of 8,188 executives knowledgeable about IT decisions. Of this sample, the full survey was conducted on the 6,084 respondents actively using cloud for multiple workloads. Thirty-six percent of the respondents were IT/C-level executives, and 15% were line-of-business (LOB) executives. The survey profiled companies’ overall use of cloud, deployment strategies, adoption drivers and benefits, and cloud requirements. Respondents came from North America (15%), Latin America (7%), EMEA (32%), and Asia/Pacific (46%) regions and spanned all company sizes.

Additional details behind the IDC methodology for the survey and business value analysis including key performance indicators can be found in the Appendix.

Cloud Adoption Continues to Increase

Cloud adoption is growing dramatically. IDC’s 2017 CloudView Survey revealed that enterprise adoption of cloud has continued to grow and expand, with 78.5% of organizations using some form of cloud, representing a 15% increase from 2016 (see Figure 1).

FIGURE 1:

Cloud Adoption Continues to Increase
Use of Public or Private Cloud

Q: How would you best describe your organization’s current or near-term plans to use public cloud or private cloud solutions to support production workloads and services?

- Currently using: 78%
- Firm plans to implement: 10%
- Educating/evaluating: 12%
- No interest: 9%
- 2016: 68%
- 2017: 78%

Source: IDC’s CloudView Survey, April 2017, n = 6,084
A very broad range of workloads are migrating to the cloud, and the most common workloads in each cloud deployment category include:

» **Public cloud.** Application workloads include email, enterprise social networks, and personal productivity (word processing, spreadsheets); data-oriented workloads include web content management, data backup/archiving, and test/development environments; and IT workloads include mobile device management and storage overflow capacity.

» **Private cloud (on-premises).** Application workloads include email, enterprise resource planning (ERP), supply chain logistics, and project and portfolio management (PPM); data-oriented workloads include database services (DBMS), enterprise search, and data integration; and IT workloads include mobile device management, network or application performance management, and security services.

» **Hybrid cloud.** Application workloads include product life-cycle management, customer resource management (CRM), and human resource applications; data-oriented workloads include enterprise content management (ECM), cloud testing/development, and IT operations analytics; and IT workloads include storage capacity and business continuity/disaster recovery.

### Why Multicloud?

The business reality facing IT executives is that sourcing cloud services from multiple vendors is no longer optional; it’s a requirement to stay competitive and scale capabilities for quickly enabling business growth. Additional reasons why multicloud adoption will continue to soar include:

» **The proliferation of roles (e.g., LOB, non-IT/CXO, developers, and DevOps) making technology decisions.** In turn, procurement of new cloud services has expanded. LOB executives are pushing for faster execution cycles and higher-quality customer experiences that drive revenue, profits, and competitive advantage.

» **Best-in-class, market-dominant SaaS companies (Salesforce.com, Workday, etc.) that are driving and entering the enterprise.**

» **Different stacks for different tasks.** New technologies (cognitive/machine learning, IoT, etc.) run from specialized stacks and clouds, such as Google Cloud Platform for AI, IBM for AI and machine learning, AWS Serverless Computing, and open source TensorFlow.
> Immediately beneficial client virtualization and client SaaS (Office365, desktop virtualization, etc.) adoption.

> Private cloud adoption and investments that continue to drive critical workloads for systems of engagement that support significant revenue.

> Industry and community clouds adoption such as GE Predix, athenahealth, or AWS GovCloud.

In addition, five major migration strategies are driving multicloud adoption. Every application allows different levels of workload portability, security, governance, risk, compute and infrastructure, network, and application management, design, and deployment capabilities. Mapping datacenter workloads to various cloud provider architectures is difficult and complex, notably when trying to preserve data, compliance, and security policies. These requirements often dictate which cloud strategy is a best fit for the application workload.

The Five Cloud Strategies

**Lift and shift:** Moving a legacy application from one environment to another, without redesigning it, often reducing hardware costs and improving disaster recovery capabilities

**Redevelop:** Developing an existing “traditional” or “legacy” application, often using DevOps, agile practices, and cloud-native tools

**Replatform:** Modifying and moving some elements of an existing custom-developed application to become cloud native, often by using cloud-native tools to take advantage of cloud-based functions such as IoT, BI, analytics, and automation

**Hosted SaaS-delivered applications:** Industry clouds and SaaS services, sometimes driven by LOB/non-IT/CXO stakeholders and used to obtain IT benefits such as a reduction in patching overhead and faster upgrade cycles

**Outsourced IT capabilities:** Leveraging third-party IT services in areas such as networking, security, and performance management
Maturity Matters in a Multicloud World

Despite the high level of cloud adoption, most organizations are still working to improve their cloud strategies, as challenges continue across people and organizational structures, operational processes, IT culture, and technology adoption. IDC defines five levels of cloud maturity:

» **Ad hoc.** These organizations are beginning the process of increasing awareness of cloud technology options and are turning to cloud because of the immediacy of their need, often in an unauthorized manner.

» **Opportunistic.** These organizations are experimenting with short-term improvements in access to IT resources through the cloud. They usually consider cloud for new solutions or isolated computing environments.

» **Repeatable.** At this level, organizations are enabling more agile access to IT resources through standardization and implementation of best practices. They rely on self-service portals to access cloud services.

» **Managed.** These organizations are implementing a consistent, enterprisewide best practices approach to cloud and are orchestrating service delivery across an integrated set of resources.

» **Optimized.** These organizations are delivering innovative IT-enabled products and services from internal and external cloud providers and driving business innovation through transparent access to IT capacity, based on the value to the business and transparent cost measures.

Our research revealed that 44% of organizations worldwide have repeatable, managed, or optimized cloud strategies — the three highest maturity levels (see Figure 2). The challenges of managing a multicloud environment are accelerating as more cloud services are utilized. Executives realize that automated operational processes are the only strategy to scale using multicloud-sourced services effectively. Additional critical points are:

» 15% of organizations already work with at least 10 different cloud providers.

» 58% work with at least 4 cloud providers.

The most cloud-mature organizations expect to be able to choose from multiple cloud providers based on location, policies, and governance principles and have implemented collaborative business and IT governance to do so.
Cloud Is Driving Significant Business Benefits

Increasing Cloud Adoption Drives Significant KPI Improvements

This white paper also shows that greater use of cloud is associated with improved business outcomes, specifically for increased revenue generation and lower operating costs. As shown in Figure 3, respondents expect business benefits in the form of risk mitigation, IoT enablement, faster time to market, and new customers. From a cost reduction perspective, the major benefits are infrastructure and IT operations cost reduction and business process improvements. In many cases, KPIs can also be improved by taking advantage of cloud services that cloud service providers offer.
More Mature Organizations Recognize Benefits Across the Board

The benefit per cloud-based application across organizations studied by IDC averaged $3 million in additional revenue and $1 million in reduced costs.

### Annual Benefit per Cloud-Based Application

<table>
<thead>
<tr>
<th>Benefit Category</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk mitigation</td>
<td>13%</td>
</tr>
<tr>
<td>Enablement of IoT</td>
<td>18%</td>
</tr>
<tr>
<td>Faster time to market</td>
<td>68%</td>
</tr>
<tr>
<td>New customers</td>
<td>2%</td>
</tr>
</tbody>
</table>

**$3 million**

**$1 million**

Source: IDC, 2017. 470 responses from 15 IDC Business Value Research studies from 2012 to 2016 covering cloud maturity levels, adoption of private cloud, implementation of private cloud and converged infrastructures in support of cloud and 35 respondents from a specialized study of optimized/managed cloud maturity organizations for Cisco in December 2014 and April 2016. Figures may not add to 100% due to rounding.

### Cloud-Mature Organizations Gain Greater Benefits from Containers, Microservices, and IoT Capabilities

Fully 100% of optimized organizations use microservices-based architectures to develop cloud-native applications, often utilizing Agile development processes and DevOps practices, up from 79% in 2016. Only 18% of ad hoc organizations utilize the same approach. IT executives realize that modern application delivery models often use a recipe that redefines their IT infrastructure and operations teams to increase their ability to scale due to faster application deployment frequencies. Infrastructure and operations teams must become a partner to the DevOps teams and provide self-service interfaces while providing capabilities on performance tuning for application services. DevOps approaches span the entire delivery pipeline and can increase deployment ease and frequency, providing a faster cadence to get applications out the door. For many organizations, DevOps allows for lower failure rates of new releases, shortened lead time between fixes and, potentially, faster mean time to recovery.

Microservices are essentially a design pattern supporting the DevOps principle of Agile, lightweight, and iterative development, changing how organizations build their application architectures and how they release new applications as well. Container usage continues to accelerate into production environments. IDC data shows that for IT organizations using containers, 85% are using containers for production applications. A benefit of containers is that they support full-stack deployments.
so that developer teams can work on the loosely coupled applications and then choose the technology stack best suited for their deployment requirements rather than the reverse. The added flexibility means developers spend less time and money on quickly and easily setting up development and test environments for burden, load, and function testing across deployment targets.

Infrastructure and operations teams must realize that developers generally view the modern application development and delivery world through three lenses:

- Developers often are held to stringent workflows that are difficult to change, such as Git workflows, user story templates, sprint planning, software testing and deployment, and scrum project management.
- Developers don’t like to be forced into new tools; they most often choose tools for themselves.
- Developers often are indifferent about the underlying infrastructure that supports their application services.

The most mature cloud adopters are nearly twice as likely to support IoT and other real-time initiatives through an event-driven architecture. This is likely driven by the need to have supply chain transaction visibility across private cloud, public cloud, and IoT sensor environments and the need to be able to detect, analyze, and resolve potential problems in real time in the supply chain before they impact the customer experience (see Figure 4).

**FIGURE 4:**

Cloud-Mature Organizations Also Take More Advantage of the Internet of Things (IoT)

**THE MOST MATURE CLOUD ADOPTERS**

are nearly twice as likely to support IoT and other real-time initiatives through an event-driven architecture.*

97%  
Most mature (Levels 4+5) Managed

53%  
Overall cloud adopters Optimized

*An event-driven architecture is geared toward detecting, consuming, and acting on events as detected by sensors or other agents. Typical cloud-based IoT use cases include instances where large and/or unpredictable amounts of data are involved or in which the sensors and agents are widely dispersed and accessible through public cloud. Source: IDC’s CloudView Survey, April 2017, n = 1,503
Cloud Maturity Continues to Lag

While the benefits of an optimized cloud strategy are clear, most organizations continue to lag in cloud maturity as they struggle with the changes required for operational processes, technology adoption, and staffing skills (see Figure 5). Many executives fail to recognize the importance of cloud planning, and that can result in their organizations being exposed. A good example is identifying the shared process responsibilities between cloud providers and the organization’s internal security and network teams or evaluating legal ramifications when the organization decides to end a cloud partnership earlier than anticipated. In addition, maturity also requires an increased focus on the multiple dimensions (IT and business collaboration, automated processes, DevOps, etc.) that drive cloud maturity (refer back to Figure 2).

FIGURE 5:
IDC’s Cloud Maturity Framework

While cloud has reached widespread adoption (78%+), cloud maturity — and in turn the level of business benefit organizations derive from cloud — continues to lag.

Overall cloud adoption
37%
19%
20%
13%
11%

Representative industries
• Healthcare/life sciences
• Retail/wholesale
• Professional services
• Oil & Gas
• Utilities

• Financial Services
• Manufacturing/tech

Source: IDC’s CloudView Survey, April 2017, n = 6,084; Respondents using public and/or private cloud for one or two small applications and/or have interest in using cloud sometime in the future (excludes no interest in cloud).
Overcoming the Barriers to Increasing Cloud Maturity

IT executives have made significant strides over the past three years in overcoming their public cloud adoption concerns. However, IDC research finds that there are six areas of concern with which executives remain challenged when attempting to mature their organizations, technologies, and processes to accelerate cloud adoption. The six areas, and recommendations for overcoming cloud maturity challenges, are shown in Table 1.

### TABLE 1: How to Increase Cloud Maturity

<table>
<thead>
<tr>
<th>Challenge</th>
<th>Actions to Improve Cloud Maturity</th>
<th>Common Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Business metrics</strong></td>
<td>• Executive leadership should clearly define and agree to business metrics that measure cloud outcomes.</td>
<td>• Business metrics include Net Promoter Score (NPS), time to market, profits, ROI, customer satisfaction, renewal rates, etc.</td>
</tr>
<tr>
<td></td>
<td>• Identify and benchmark technology and business metrics/ KPIs that drive team accountability and ensure progress mapping.</td>
<td>• Technical metrics include deployment frequency, lead time, MTTR, MTTF, ticket reduction, etc.</td>
</tr>
<tr>
<td><strong>Organizational structure and skills</strong></td>
<td>• Assess existing skills; determine required emerging skill sets for multicloud management, financial analysis, automation, and API development and integrations.</td>
<td>• Create DevOps CoE teams.</td>
</tr>
<tr>
<td></td>
<td>• Invest in training and development and create an organizational structure that delivers collaboration and teamwork.</td>
<td>• Hire site reliability engineers (SREs) for operations teams.</td>
</tr>
<tr>
<td><strong>Pace and rate of technology change</strong></td>
<td>• Determine whether the existing product selection diligence/ RFI process should be updated to reduce business risks.</td>
<td>• Drive investments in common metrics that trigger aligned behaviors and goals across development and operations teams.</td>
</tr>
<tr>
<td></td>
<td>• Consider the organization’s ability to adopt new capabilities as cloud-based product development cycles shrink. Invest resources into planning and cross-silo decision making.</td>
<td>• Revisit POC/RFI/vendor management processes and capabilities.</td>
</tr>
<tr>
<td><strong>Security</strong></td>
<td>• Map shared security responsibilities between the cloud provider and the IT organization; consider a multilayered security approach that uses proactive and automated capabilities across data, users, and application sources.</td>
<td>• Drive more collaboration across security and development teams by having formal “meet and greets.”</td>
</tr>
<tr>
<td></td>
<td>• For DevOps practices, include various security capabilities (i.e., application scanning, vulnerability assessment, etc.), processes, or policies earlier in the development life cycle.</td>
<td>• Share security policies, APIs, libraries, and tools that can be used across network and development teams.</td>
</tr>
<tr>
<td><strong>Process integration</strong></td>
<td>• Invest in network API management and integration skills to automate, control, and manage the infrastructure and network.</td>
<td>• Invest in integration skills across network and security teams, which is different from APIs used to integrate “platforms.”</td>
</tr>
<tr>
<td></td>
<td>• Create an integration road map and include policy, data, agent, and technology integration requirements.</td>
<td></td>
</tr>
<tr>
<td><strong>Data governance</strong></td>
<td>• Understand data governance and security requirements for data in motion, at rest, in storage, etc.</td>
<td>• Focus on the operating model (i.e., centralized, decentralized, or federated) and define roles and responsibilities for data across key enterprise stakeholders.</td>
</tr>
<tr>
<td></td>
<td>• Recognize government regulations across countries that drive different data integration requirements.</td>
<td></td>
</tr>
</tbody>
</table>
As executives decide which applications should reside on which cloud, multicloud becomes a fast, complex reality. A multicloud management strategy is fast becoming a necessary business requirement; solutions must work across different public clouds and with the private cloud.

Part of maturing in the use of cloud capabilities includes adjusting and managing multiple cloud providers. Increasingly, each cloud platform is fast becoming a technology silo. For example, each cloud platform has different requirements for application development, migration, and network process integrations. As such, IT executives must understand that each cloud platform should be approached differently and that each contract is a form of lock-in. The higher the number of cloud platforms in use, the higher the level of complexity — which generally leads to an increase in the total cost of ownership (TCO) because it becomes hard to optimize any singular relationship. As executives decide which applications should reside on which cloud, multicloud becomes a fast, complex reality. A multicloud management strategy is fast becoming a necessary business requirement; solutions must work across different public clouds and with the private cloud. With limited visibility between clouds, and a general inability to move workloads across various clouds, problems arise quickly, and identifying problems becomes very difficult across complex applications and compute and network environments. Executives should consider creating a risk mitigation plan for the multicloud challenges shown in Table 1.

**Creating a Risk Mitigation Plan for Multicloud Challenges**

Most executives using cloud infrastructures generally also deploy numerous other tactics to fully optimize cloud benefits. These practices include automation and orchestration tools, DevOps and Agile development practices, software-defined networks, continuous integration and delivery (CI/CD) containers and microservices and, increasingly, serverless technologies. As the number of cloud architectures in use rises, it becomes necessary for IT executives to create a risk mitigation strategy should a cloud provider be unable to deliver on service performance, security, or related contractual expectations. For example, some enterprise IT executives are realizing that their cloud costs are higher than expected or their public cloud services are not performing as expected via their defined service-level agreements (SLAs). These are the two most common reasons why cloud relationships sour.

Reducing business risks as multicloud relationships expand is critical for IT executives and their teams. To accomplish this, teams should consider the recommendations provided in the sections that follow.
Technology Recommendations

» **Data:** Create contract terms that answer specific exit questions on data storage and the role and responsibilities of the provider in data storage, confidentiality, migration, security, export formatting, data/application portability, recovery, and destruction. Clearly identify the lines of responsibilities of the provider.

» **Application strategy:** Application modernization is driving the executive suite to consider which cloud platform and strategy best fit each set of application requirements (i.e., security and compliance, performance, governance, and costs).

» **Application programming interfaces (APIs):** Cloud providers often use unique and proprietary APIs and databases. API integration is often required, and applications might need to be redeveloped to migrate to another provider. Recognize how much API and application customization is required to enter and exit a cloud platform.

» **Source code access:** Attempt to gain the provider’s application source code to reduce lock-in and make it easier to migrate off a platform. Insert escrows to reduce risk exposure and regulate what happens to a cloud vendor’s source code if the vendor ceases operations.

» **Standards:** Identify whether the underlying cloud platform is standards-based virtualized hardware or proprietary hardware and software infrastructure. Determine what this means for the potential lock-in risks and surrounding exit support costs (professional services, de-integration across billing, process, technology, etc.). Identify whether the cloud provider participates in standards bodies, creates or leads standards, or uses standards in its platform. This can help smooth an exit for certain standards-based capabilities (hardware, APIs, etc.).

» **Application portability analysis:** Conduct a risk analysis of the application workloads that will be migrated to the cloud and the steps necessary to move them off the cloud platform. In general, what level of technical and/or staff support will a provider offer if you exit its platform or decide to move an application from one provider to another?

» **Management and monitoring:** Incorporate capabilities that allow the IT team to monitor what’s happening in the cloud as easily as on-premises activities to enable visibility during an exit.

» **Work stream mapping:** While working with the legal team, map out the application work streams, processes, APIs, data, security, and other requirements to provide a clearer picture of the service, and think through what might be needed to reverse or change the work stream in case of an exit.
Contractual, Legal, and Internal IT Recommendations

» **Internal IT policies:** Establish cloud usage policies in security, compliance, data storage, migration, and recovery, and determine how those policies might have to change during an exit.

» **Compliance:** Create a compliance plan that identifies key validation requirements to track and report via executive dashboards; understand underlying data requirements and how data will be collected and where the data is stored.

» **Contract pricing:** Analyze the contract and the exit plan with regard to the potential impact of price increases as well as the breadth and depth of legal responsibilities, audit requirements, and compliance due diligence prior to purchase.

» **Scenario planning:** Conduct an audit of the provider’s operational practices and processes and scenario plan, or ask the provider about how it has managed other exits in the past. Develop a scenario that anticipates potential actions by the cloud provider, such as price increases, lock-in, competitive threats (due to an acquisition or a change in business strategy), or potential financial challenges to competition.

» **Internal skills analysis:** Prior to an exit and moving application workloads back into the private cloud, ensure you have the skills, infrastructure, management, process (change/operational), and applications and can reestablish the required licensing.

» **Disaster recovery because of compliance requirements:** Establish a cloud governance and business continuity program to create a data transport and transition framework that specifies a cloud disaster recovery plan and sheds light on potential compliance issues. Understand what happens to the backups (and related data) when the relationship sours and who owns the associated compliance responsibilities.

» **Legal education:** Partner and educate the legal team on specific terms and their meaning during review of the contract, and take a specific focus on the potential for an exit and the legal/contractual ramifications.

» **Contract:** Determine, from a contractual perspective, whether other services are contractually bundled together and the limitations or lock-in this might cause.

» **Transition period planning:** Be specific and detail which cloud services will be offered in perpetuity and what a potential transition period might look like. Recognize whether there are any shared overhead costs (i.e., development, billing, or patents). Cross-company systems and processes must be carefully unraveled (or shared by both companies for a transition period) to ensure effective separation.
Risk Mitigation for Modern Application Delivery: Containers

As executives continue to adopt modern application development, deployment, and management, the use of containers in production is increasing. Specific challenges for deploying applications on container-based architectures include those shown in Figure 6. IDC analysis finds that container management is a major inhibitor to bringing containers to production environments. Executives have the following challenges:

» There are few large-scale production container implementations; most deployments focus on development and test use cases (pre-production). Many executives don’t believe that pre-production environments require the use of sophisticated management and orchestration tools. The reality is they do, with tools that cover the broad spectrum of physical, virtual, and container-based application deployment models.

» The networking and persistent storage challenges from large, container-based stateless cloud-native applications are just beginning to be understood. Stateless containers often do not support storage features such as high availability (HA), replication, or clones.

» Administrators are still learning what management data matters in containerized environments. With application code abstracted from VMs, and containers frequently deployed onto public cloud environments, administrators who have historically focused on monitoring CPU, memory, and disk may need time to transition to an environment in which application performance and container performance are the priorities. The focus must be on the relationships between containers, the cloud and network infrastructure, and the health of the components inside a single container.

The reality is that IT executives, regardless of the group they manage, must create a management and orchestration strategy for containers or else risk minimized business outcomes, slower deployment cycles, and higher costs.
The network continues to be a critical factor in successful multicloud management and performance, as connectivity, latency, security, routing, policy management, monitoring, and orchestration capabilities play a significant role in multicloud architectures. Obstacles to greater cloud maturity include cost-prohibitive changes to network services and the lack of a consistent security model across all deployment types. The critical inhibitors are shown in Figure 7.

FIGURE 7:
Cost to Change and Security Are Primary Network Inhibitors to Public/Hosted Cloud Adoption

Network inhibitors to moving to/consuming public/hosted cloud services

Source: IDC’s CloudView Survey, April 2017, n = 1,503
Essential Guidance

IT executives should consider the following seven-step plan to mitigate multicloud risks:

1. **Identify and contain security threats** to meet compliance regulations and manage security policies across the organization for all users, data, and applications.

2. **Simplify global connectivity** between datacenters and public clouds to reduce maintenance and operations costs.

3. **Integrate performance monitoring and management** of legacy and cloud-native applications to deliver transparency and cost optimization across multiple clouds and to reduce customer impactful downtime.

4. **Plan for multicloud data collection and analysis**, including IoT sensors, for streamlined problem identification and resolution processes that prevent downtime and help identify problems faster across public and private clouds.

5. **Avoid cloud vendor lock-in** by planning for a cloud exit strategy before signing a contract. Recognize that each contract is a form of lock-in, and mitigate risks by upgrading the due diligence process and by spending time planning for new DevOps practices and new development and infrastructure and operations management tools and processes.

6. **Review SLA contracts and policies** to understand the critical availability and performance metrics spanning networks, applications, and related infrastructure; obtain assurance that dashboards will provide enough transparency and understand the outcomes if service levels are not met.

7. **Create an exit plan** before signing a cloud contract as potential cost increases and poorly performing services can affect outcomes and be a cause for exiting a relationship.

Cloud maturity requires integrated and automated capabilities that span a multicloud world and work across traditional and modern IT environments. Leverage the Cisco Multicloud Advisor Tool enabled by IDC to compare your cloud adoption efforts with those of other organizations in your industry, country, and size class. Understanding where you are on the adoption scale relative to competition can help you understand what you need to do to keep pace and/or gain advantage against competitors by lowering your costs, gaining greater levels of flexibility, reducing your capital footprint, or accelerating new product innovation.
Appendix

Business KPI Improvement Detail

Table 2 provides additional detail of the business benefits associated with moving up the cloud maturity scale according to the IDC cloud maturity model. For example, a company moving from the ad hoc level to the opportunistic level would expect to see an average improvement of 36% in time to provision applications, with a maximum expected improvement of 50% and a minimum expected improvement of 25%. Similarly, a company moving from the ad hoc level to the managed level would expect to see an average reduction in IT costs of 48%, with a maximum expected improvement of 60% and a minimum expected improvement of 18%.

**TABLE 2:**

<table>
<thead>
<tr>
<th>KPI</th>
<th>Ad Hoc to Opportunistic</th>
<th>Ad Hoc to Repeatable</th>
<th>Ad Hoc to Managed</th>
<th>Ad Hoc to Optimized</th>
</tr>
</thead>
<tbody>
<tr>
<td>Revenue growth</td>
<td>0.001%</td>
<td>0.05%</td>
<td>0.7%</td>
<td>1%</td>
</tr>
<tr>
<td>IT cost reduction</td>
<td>6%</td>
<td>13%</td>
<td>14%</td>
<td>13%</td>
</tr>
<tr>
<td>Improved IT staff allocation</td>
<td>4%</td>
<td>16%</td>
<td>18%</td>
<td>37%</td>
</tr>
<tr>
<td>Time to provision</td>
<td>25%</td>
<td>36%</td>
<td>50%</td>
<td>33%</td>
</tr>
<tr>
<td>Ability to meet SLAs</td>
<td>40%</td>
<td>43%</td>
<td>55%</td>
<td>57%</td>
</tr>
</tbody>
</table>

Source: 470 responses from 25 IDC Business Value Research studies from 2012 to 2016 covering cloud maturity levels, adoption of private cloud, implementation of private cloud, and converged infrastructures in support of cloud and 35 respondents from a customized study of optimized/managed cloud maturity organizations for Cisco in December 2014 and April 2016.
Methodology

The information for this white paper is sourced from IDC’s 2017 CloudView Survey (n = 6,084, full survey); 470 responses from a collection of 25 IDC Business Value Research studies from 2012 to 2016 covering cloud maturity levels, adoption of private cloud, implementation of private cloud, and converged infrastructures in support of cloud; and 35 respondents from a customized study of optimized/managed cloud maturity organizations for Cisco in December 2014 and April 2016.

The survey research provides a comprehensive and broad-based sample that was used to determine respondents’ level of cloud adoption as well as cloud needs and drivers. It collected demographics, cloud adoption profiles, expectations of benefits from cloud and drivers for cloud, and opinions on different types of cloud technology and standards.

The Business Value Research fuels a model that estimates business outcomes based on increasing levels of cloud maturity.