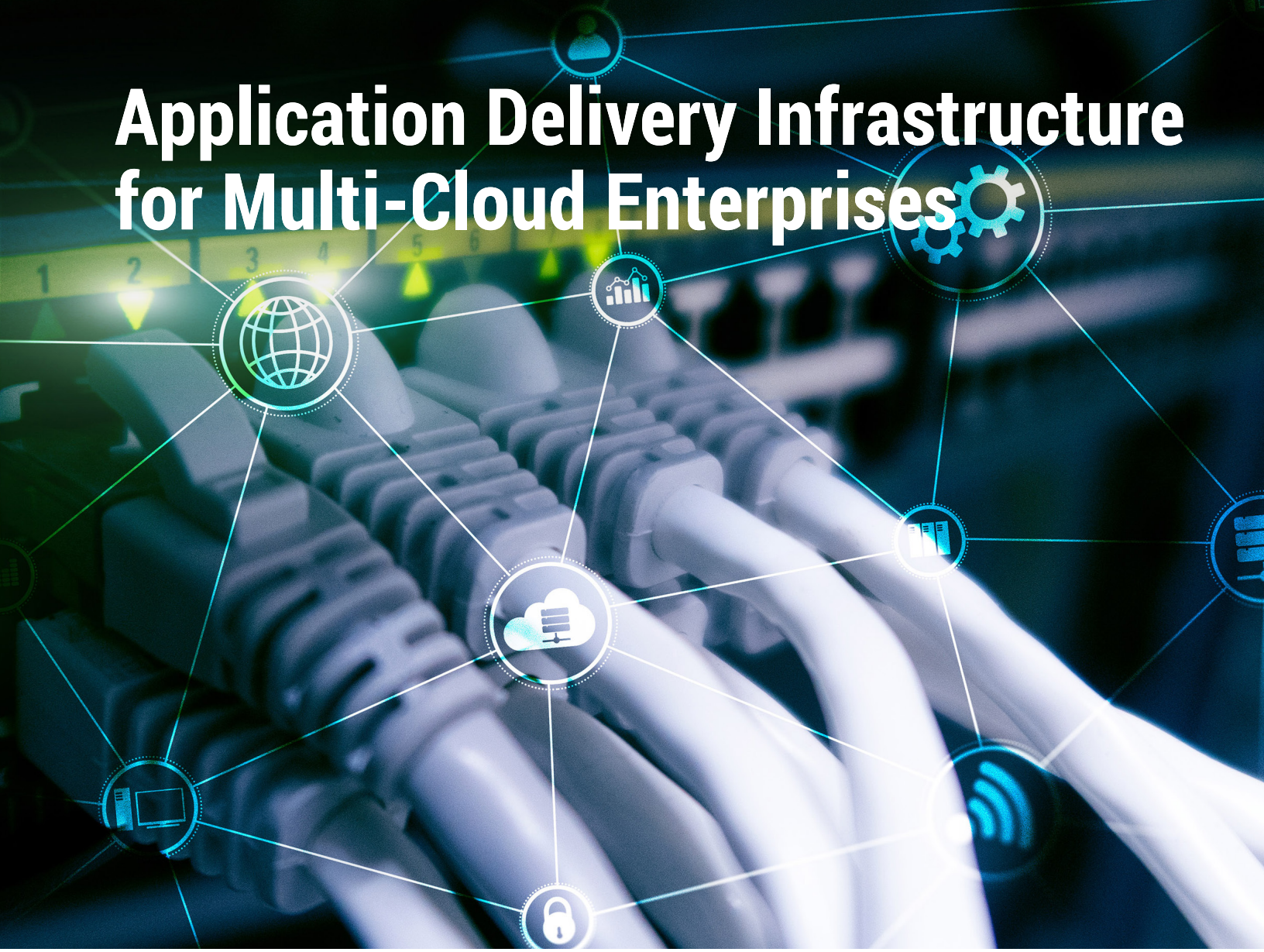
Application Delivery Infrastructure for Multi-Cloud Enterprises



An ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) Research Report Summary

By Shamus McGillicuddy

June 2020

Sponsored by:

NGINX
Part of F5

EMA™
IT & DATA MANAGEMENT RESEARCH,
INDUSTRY ANALYSIS & CONSULTING

Table of Contents

Executive Summary 1
Introduction 1
Key Findings 2

Demographics Overview 2
Strategic Drivers 5
Technical Initiatives 5
Application Architecture 6
The NetOps/DevOps Divide 7
Application Delivery Infrastructure Platforms: Today and the Future 10
Data Centers 10
Public Clouds 11
Application Delivery Infrastructure Requirements 13
Core Application Delivery Functions 13
Platform Requirements 15
Application Delivery Infrastructure Management 17
Telemetry and Observability 17
AIOps and Application Delivery Infrastructure 19
Infrastructure Automation 21
Infrastructure Automation in the Data Center 21
Infrastructure Automation in Public Clouds and Cloud-Native Application Environments 22
Service Mesh Perspectives 23
Management Integration Between Service Mesh and Application Delivery Infrastructure 24
The Impacts of the Coronavirus Pandemic 25
Succeeding with Application Delivery Infrastructure 27
Business and Technical Challenges 28
Conclusion 30
Case Study: Fortune 100 Tech Company Improves Website Performance, Resiliency, and Agility with NGINX 31
Benefits 31

Application Delivery Infrastructure for Multi-Cloud Enterprises

Executive Summary

This summary of an Enterprise Management Associates research report explores the state of the art of application delivery infrastructure. Based on a survey of 253 subject matter experts who work for enterprises and cloud providers, this research summary identifies emerging strategies and technology requirements for load balancers, application delivery controllers, and cloud-native software, such as service mesh.

Introduction

Since the early days of the internet era, application delivery infrastructure has been critical to ensuring application availability, performance, and security. The first generation of devices was comprised of load balancers with a narrow set of functional capabilities focused on distributing user traffic across multiple servers. As applications became more critical to business operations, load balancers evolved into application delivery controllers with an ever-expanding set of functions, from application acceleration and protocol optimization to SSL offload and web application firewalling.

Innovation in application architectures has driven the application delivery infrastructure industry to continuously reinvent itself. For a time, application delivery vendors focused on building massively scalable hardware platforms that could serve the needs of multiple applications from a single appliance.

The cloud computing era shifted application architecture from the monolithic client server model to three-tiered web and mobile applications, and more recently cloud-native, microservices-based applications. These new architectures changed the nature of traffic. So-called “east-west” traffic between application components outstripped the volume of north-south traffic between users and applications. This forced the application delivery infrastructure to shift toward a software-based, dynamic architecture, in which application delivery services are deployed where they are needed, rather than just in a DMZ in front of a monolithic server farm.

This Enterprise Management Associates (EMA) research report explores the current state of application delivery infrastructure strategy. Based on a survey of 253 technology professionals, this report identifies the technical requirements, management strategies, and infrastructure roadmaps of cloud-forward enterprises.

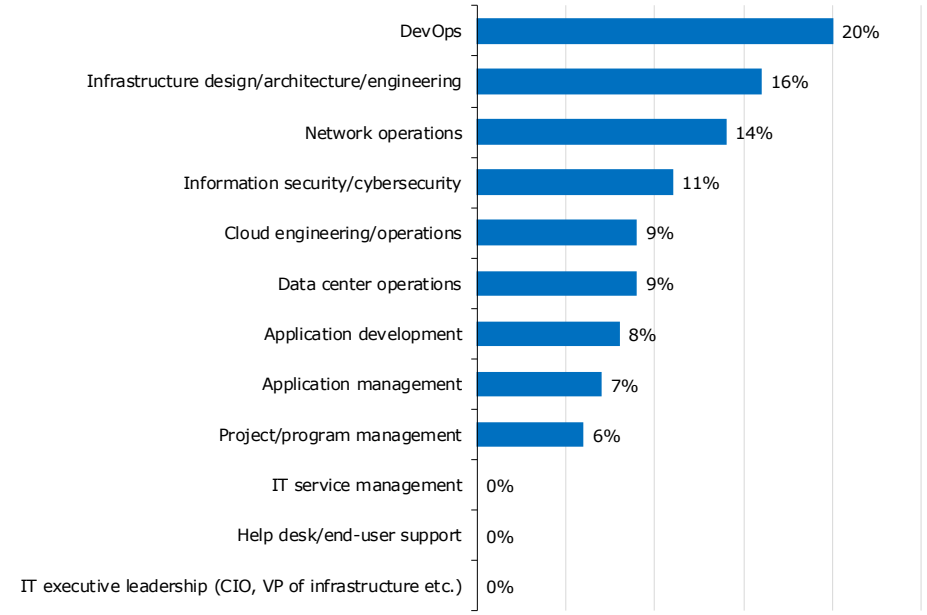
Key Findings

- 81% of enterprises have experienced fragmentation in operational and administrative ownership of application delivery infrastructure, leading to increased security risk, compliance challenges, and operational inefficiency.
- Enterprises identified cloud-native software as the application delivery platform of the future, both in private data centers and the public cloud.
- 82% of enterprises are collecting telemetry from application delivery infrastructure, primarily for security monitoring, capacity planning, and application troubleshooting.
- 95% of enterprises are interested in using AIOps solutions from their application delivery vendors.
- The vast majority of enterprises automate application delivery infrastructure management in both the data center and the cloud, but only a minority are satisfied with their ability to automate.
- 85% of enterprises are interested in using service mesh in their cloud-native application environments, and nearly all of them would like some management integration between service mesh and the rest of their application delivery infrastructure.
- 90% of enterprises have made changes to their application delivery infrastructure in response to the COVID-19 pandemic.

Demographics Overview

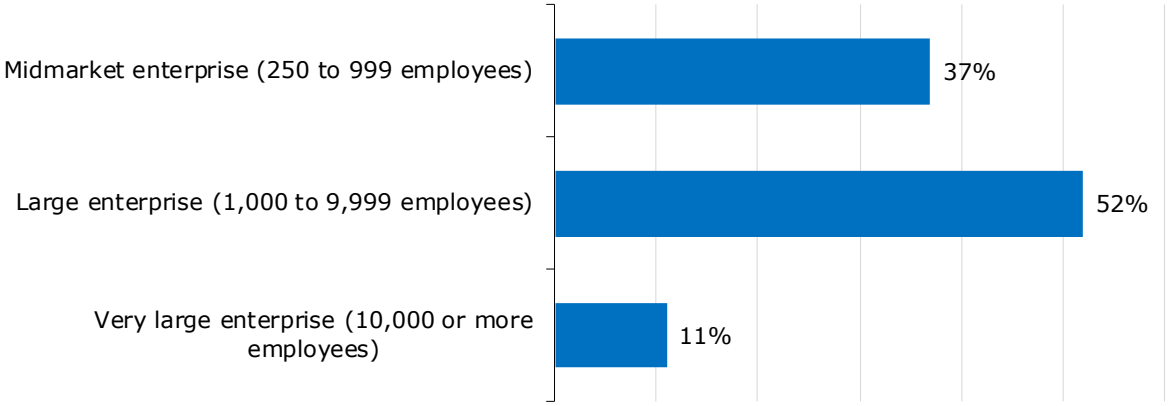
In April and May 2020, EMA surveyed 253 North American technology professionals who have direct and current experience with their employers' use of application delivery infrastructure. All of them work for companies with application delivery infrastructure deployed in their data centers and the public cloud.

The following charts reveal the demographic details of these research participants.



Sample Size = 253

Figure 1. Functional groups represented in the research



Sample Size = 253

Figure 2. Size of company (employees)

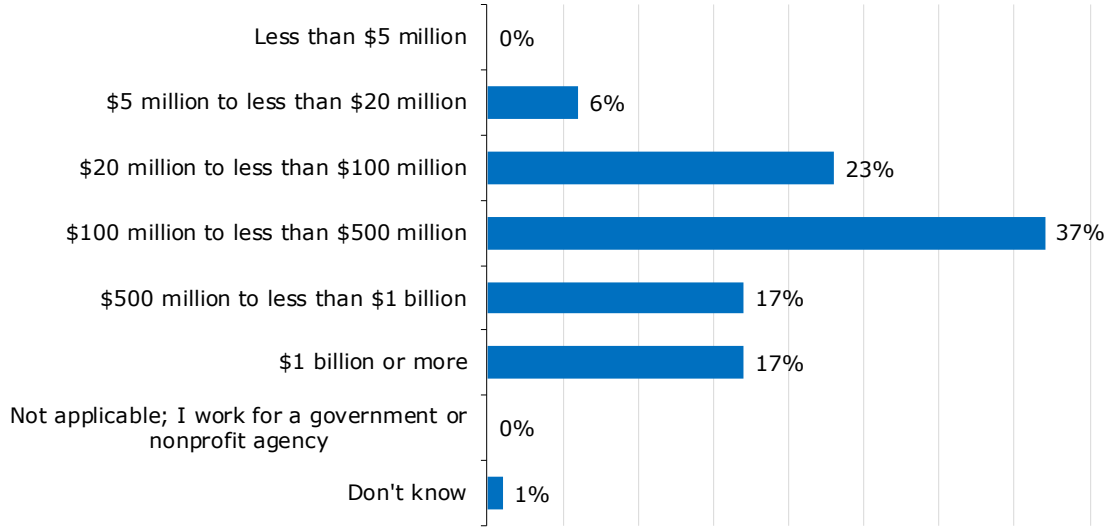
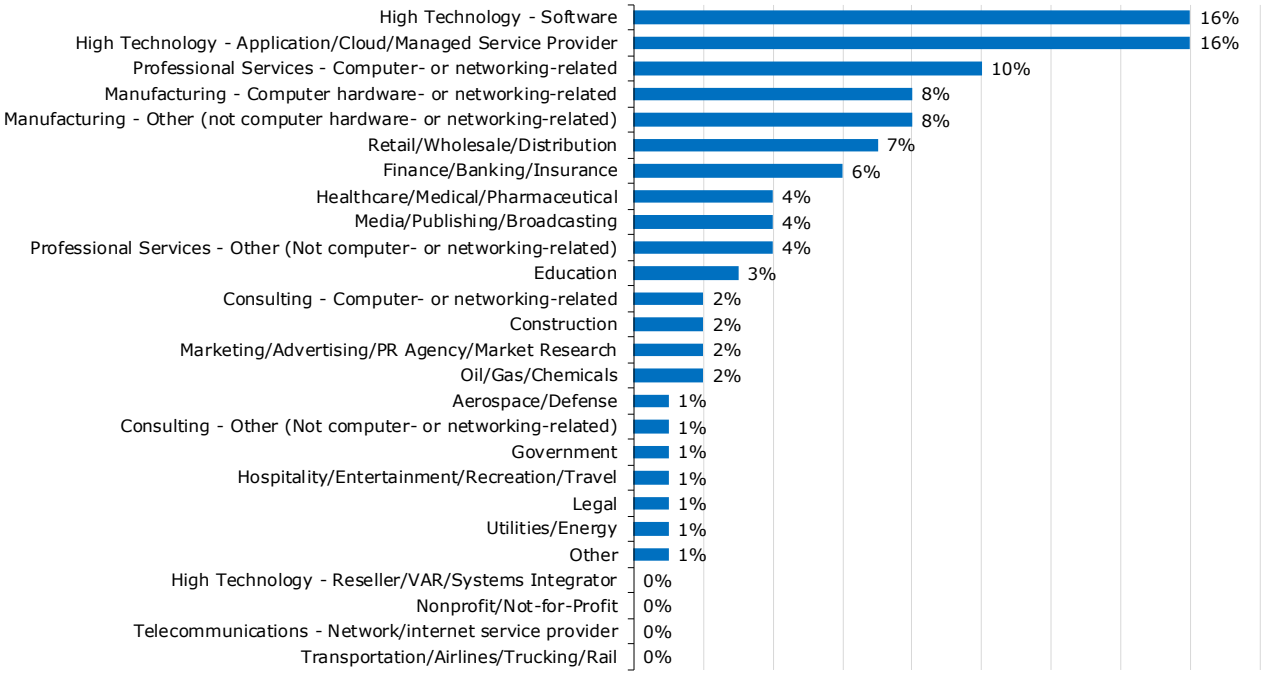


Figure 3. Revenue of represented companies



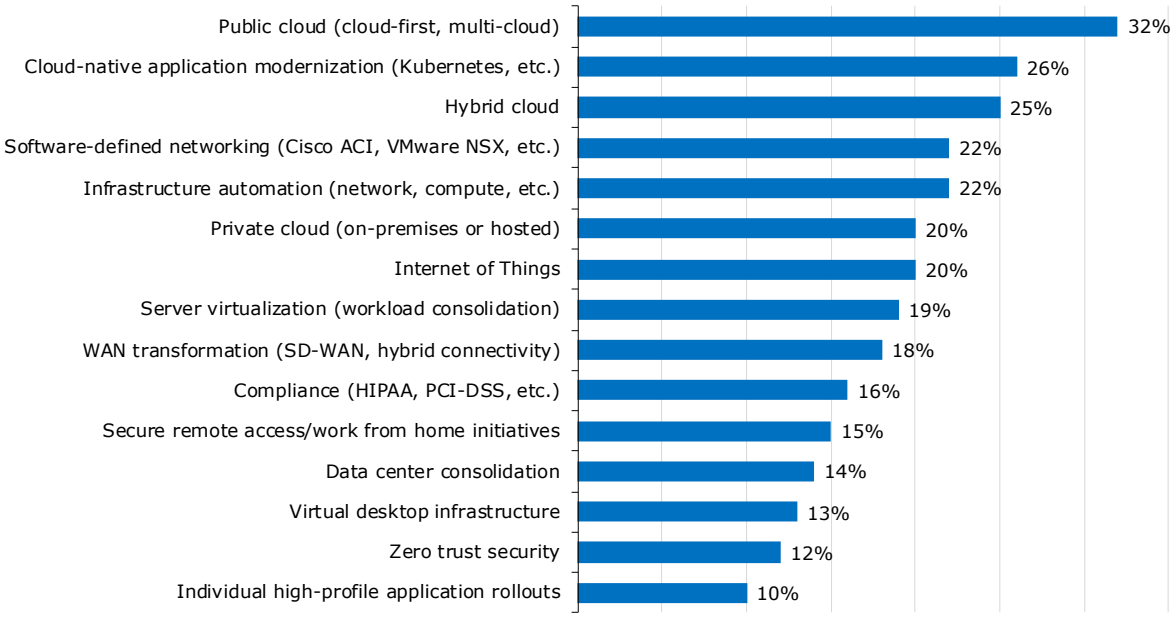
Sample Size = 253

Figure 4. Industries represented in the research

Strategic Drivers

Technical Initiatives

EMA asked respondents to identify up to three technical initiatives that are significantly influencing their application delivery infrastructure strategies. The public cloud is the biggest driver, followed by cloud-native application modernization efforts and hybrid cloud architectures. Data center SDN technology and infrastructure automation are also significant influences.



Sample Size = 253, Valid Cases = 253, Total Mentions = 717

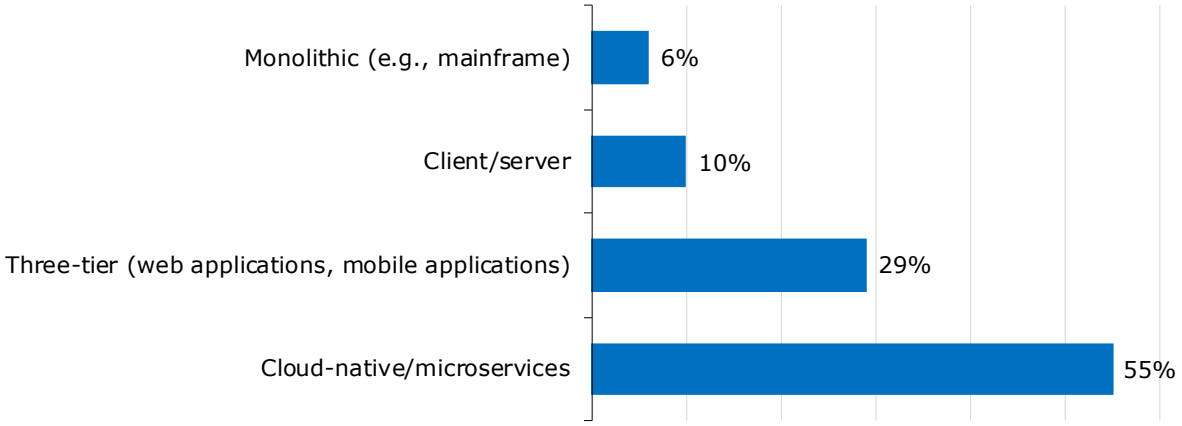
Figure 5. Technology initiatives most influential on application delivery infrastructure strategies

Overall, it's quite clear that cloud architectures, whether public, private, or a mix of the two, are driving application delivery infrastructure strategies.

Cloud architectures, whether public, private, or a mix of the two, are driving application delivery infrastructure strategies.

Application Architecture

Figure 6 examines which application architectures are steering application delivery infrastructure strategy. Clearly, architectures of the past, such as mainframe and client/server, are waning. Instead, the majority of respondents see cloud-native applications and microservices as the guiding architecture. A large minority are more influenced by three-tier web and mobile applications.



Sample Size = 253

Figure 6. Application architectures most influential on application delivery infrastructure strategy

These findings confirm that most technology organizations are moving into the future, orienting their application delivery platforms for cloud-native application architectures. Most enterprises will continue to maintain legacy applications, but cloud-native is the future and will drive most infrastructure strategies from now on.

The NetOps/DevOps Divide

IT organizations traditionally have well-defined siloes of responsibility, particularly when it comes to infrastructure. Load balancers and application delivery controllers are network devices. Therefore, IT engineering, network operations, and data center operations are typically responsible for installing and managing them.

81%
of enterprises are dealing with divided ownership of application delivery infrastructure.

As applications have migrated to private and public clouds, enterprises have shifted to using application delivery infrastructure software and cloud-based services. This shift has fragmented ownership of this critical technology across multiple administrative silos. The network infrastructure team still owns a good portion of infrastructure in data centers. However, cloud and DevOps teams have taken direct ownership of infrastructure in cloud environments, leading to divided operations.

Figure 7 shows that 81% of enterprises are dealing with divided ownership of application delivery infrastructure currently.

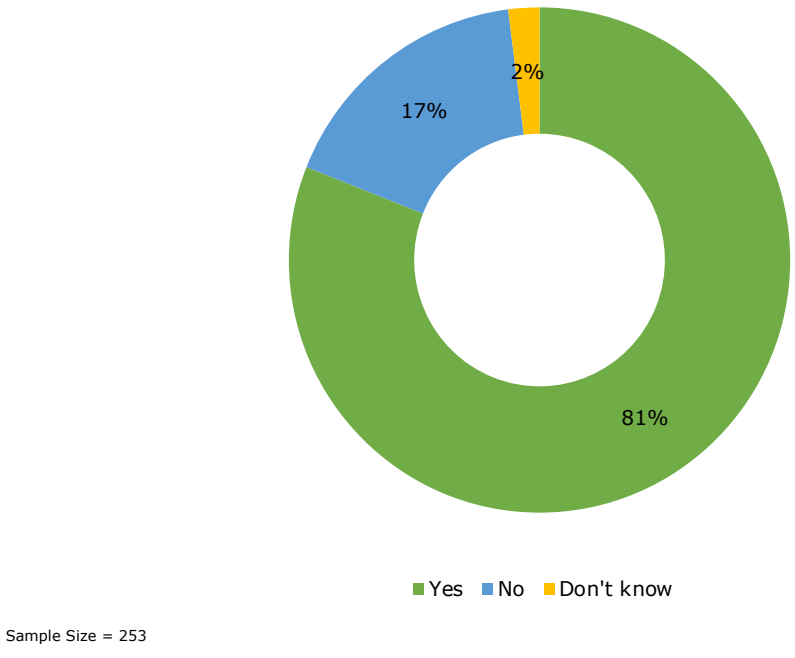


Figure 7. 81% of companies have divided ownership between traditional application delivery infrastructure and cloud-native and public cloud infrastructure

Most enterprises see the potential problems of this operational fragmentation. In fact, 85% have taken steps to close the gap and unify management.

EMA asked research respondents why they felt a need to close this gap in infrastructure ownership. Security risk is the top motivation, as **Figure 8** reveals.

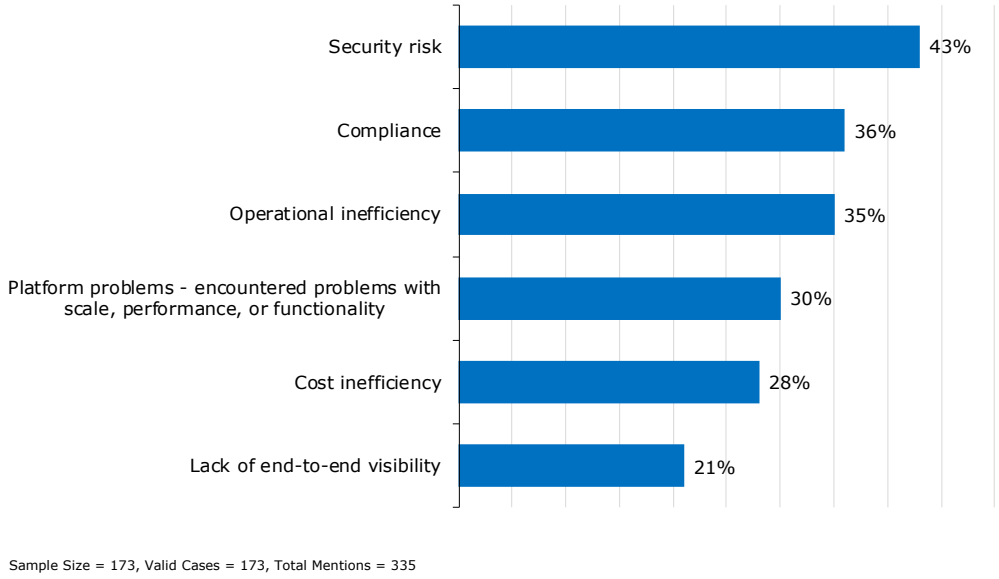
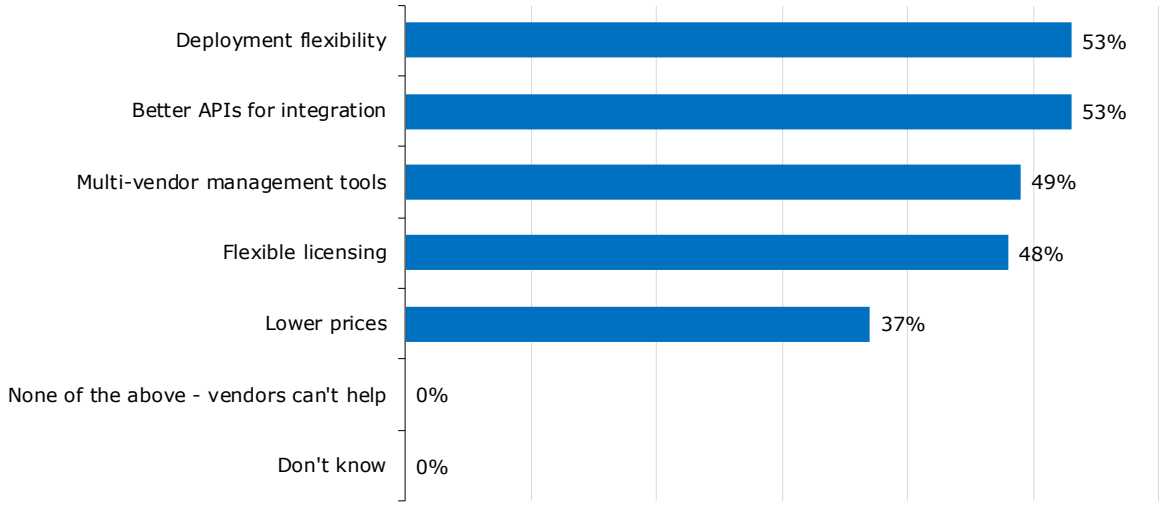


Figure 8. Why enterprises want to close gaps in ownership of application delivery infrastructure

Compliance and operational inefficiency are the chief secondary drivers of unifying infrastructure ownership. Some are also perceiving potential platform issues. For instance, the DevOps team might choose a load balancer that can't scale properly. The network operations team might choose a platform that cannot properly serve a microservices architecture.

EMA asked research participants if vendors could help unify this division of application delivery infrastructure operations. As **Figure 9** reveals, 100% of respondents said yes, their vendors could do something to help. Majorities of them said vendors could offer more deployment flexibility and better APIs for platform integration.



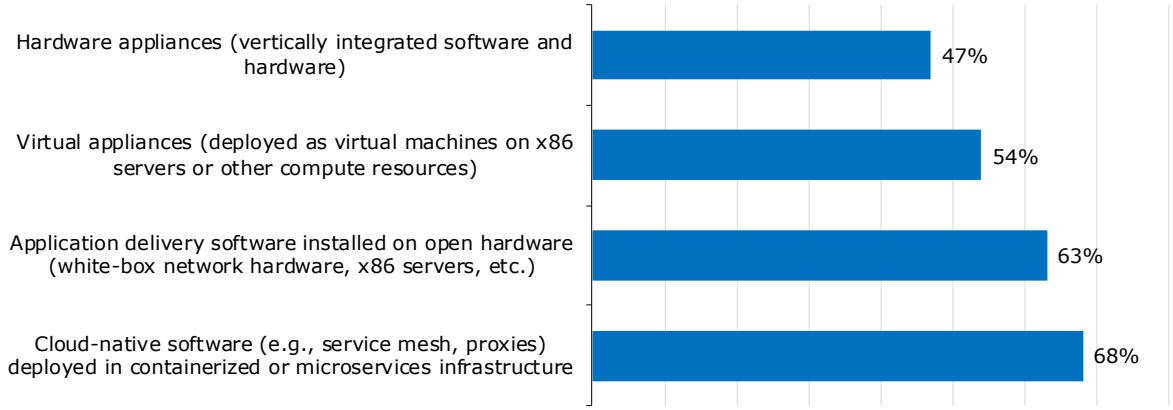
Sample Size = 204, Valid Cases = 204, Total Mentions = 490

Figure 9. Enterprises identify how vendors could help enterprises unify ownership of application delivery infrastructure

Application Delivery Infrastructure Platforms: Today and the Future

Data Centers

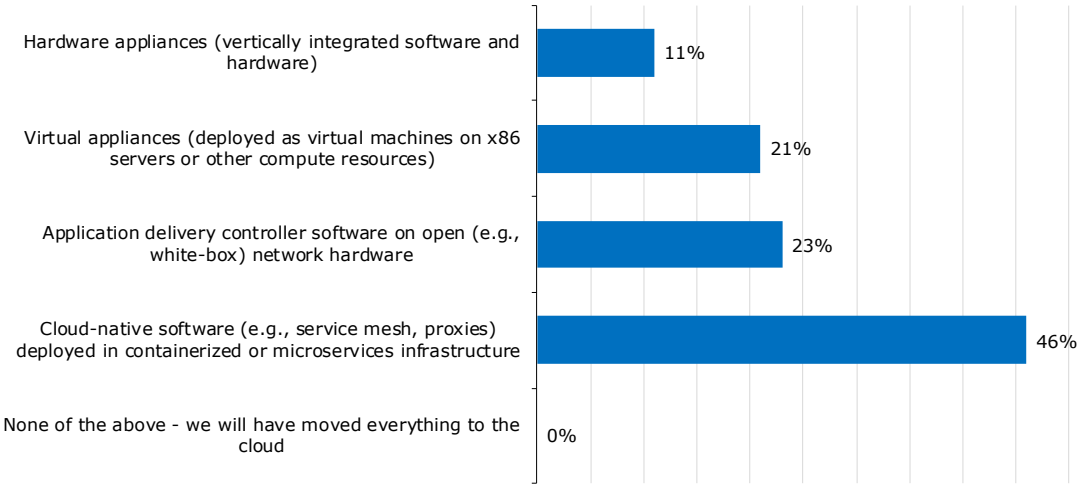
The majority of enterprises have a wide variety of application delivery platforms installed in their data centers, as revealed in **Figure 10.** Cloud-native software is the most common. This includes emerging technology, such as service mesh software, but it can also include lightweight, open source software solutions favored by DevOps organizations, like HAProxy and NGINX. Application delivery controller software installed on open hardware is also very common. A slight majority of enterprises have virtual application delivery controller appliances running on virtual infrastructure. Finally, slightly less than half are using vertically integrated hardware appliances. A decade ago, this last percentage would have been much higher.



Sample Size = 253, Valid Cases = 253, Total Mentions = 589

Figure 10. Application delivery platforms installed in the data center

EMA asked enterprises to project two years out and identify the class of platform that would be most important in their data centers at that time. **Figure 11** reveals that cloud-native platforms are the technology of the future. Only 11% believe hardware appliances will dominate their data centers in two years.

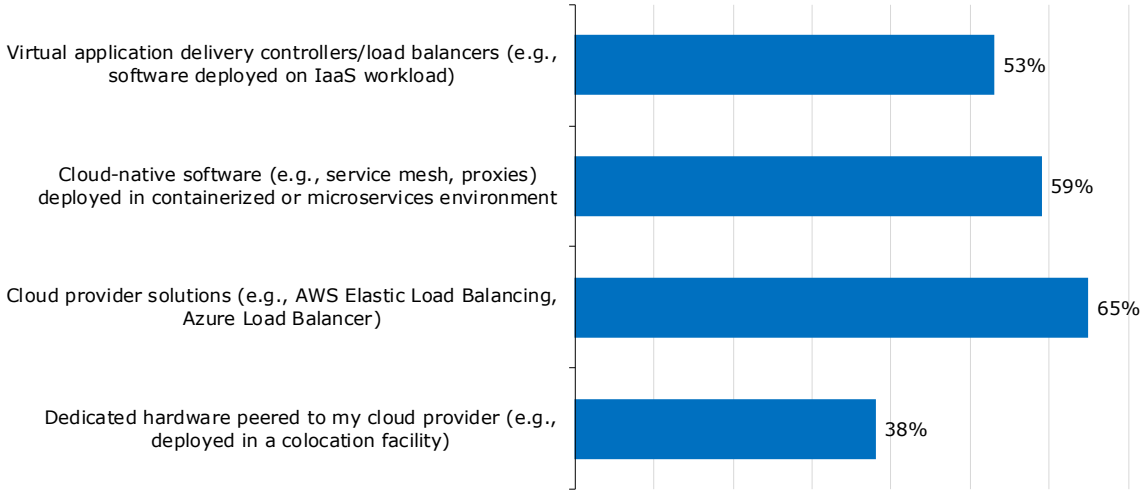


Sample Size = 253

Figure 11. Enterprises identify the platform expected to be most important to their data centers in two years

Public Clouds

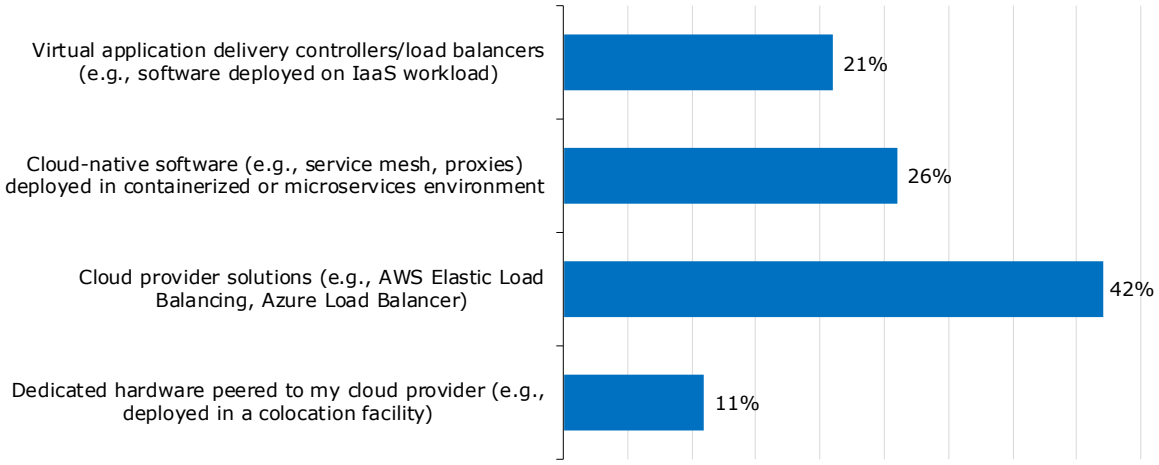
In the public cloud, most enterprises are using application delivery services offered by cloud providers. Smaller majorities are also using cloud-native software and virtual application delivery controllers.



Sample Size = 253, Valid Cases = 253, Total Mentions = 544

Figure 12. Application delivery platforms installed in the public cloud

EMA asked research participants to identify the one type of platform they expect to be most important to their public cloud infrastructure in two years. Application delivery services offered by cloud providers are the most popular. Many are looking at cloud-native software and virtual appliances.



Sample Size = 253

Figure 13. Enterprises identify the platform expected to be most important to their public cloud infrastructure in two years

Application Delivery Infrastructure Requirements

Core Application Delivery Functions

This section examines the application delivery functions that are most important to enterprises at the time of this report. As **Figure 14** shows, in the data center global load balancing, secure application gateways, data compression, and API gateways are the most valuable capabilities.

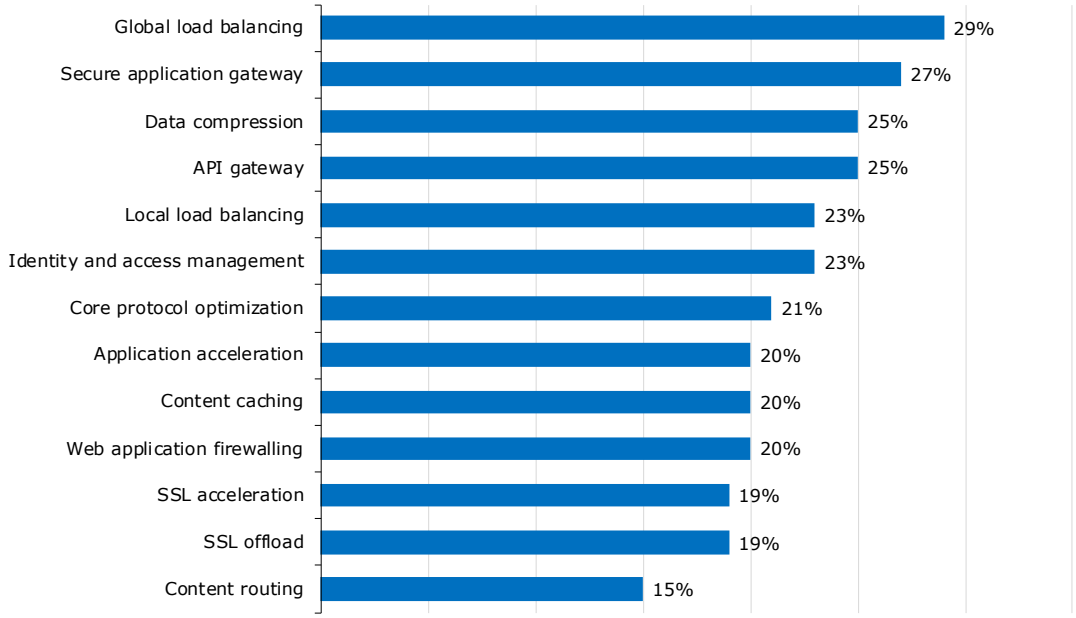


Figure 14. Most important application delivery functions in data center deployments

Enterprises have some different priorities in their public cloud infrastructure. Global load balancing remains paramount, and data compression also remains a top-three priority, as **Figure 15** reveals. However, local load balancing has much more value in the public cloud.

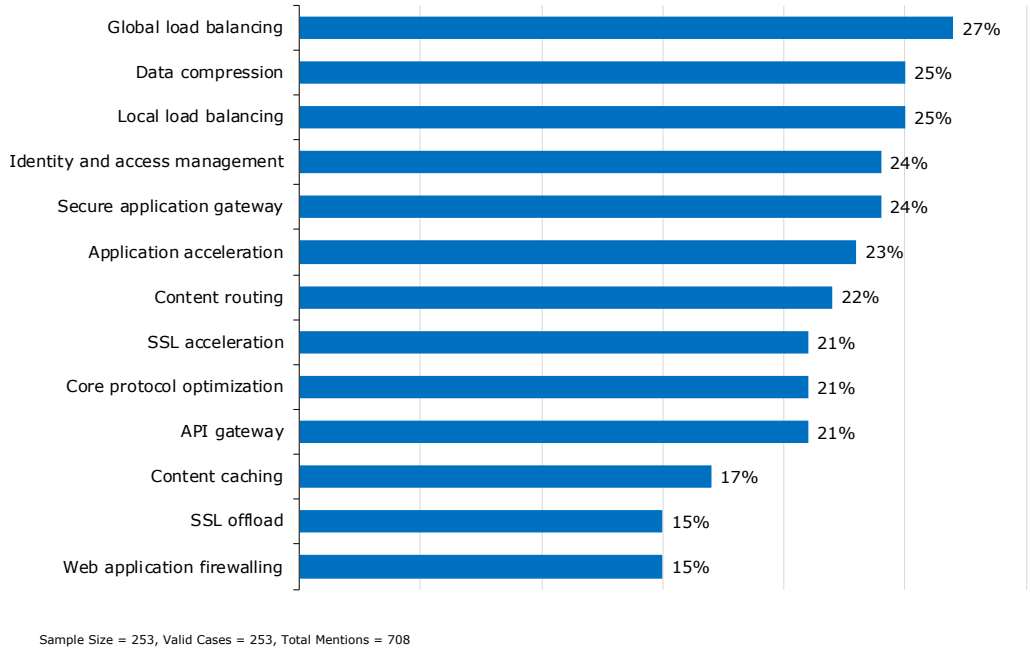


Figure 15. Most important application delivery functions in public cloud

Identity and access management and secure application gateways round out the top five, the latter being less important in the public cloud than it is in the data center. Content routing is more important in the public cloud, but web application firewalls are a lower priority.

Platform Requirements

EMA explored platform requirements for both data centers and public cloud environments. In the data center, enterprises have seven priorities, starting with multi-cloud support. In other words, enterprises want the application delivery infrastructure that they deploy in their data center to be deployable in their various cloud environments, too. This points to the need for a standard platform across public and private infrastructure. Very large enterprises are the most likely to value multi-cloud support.

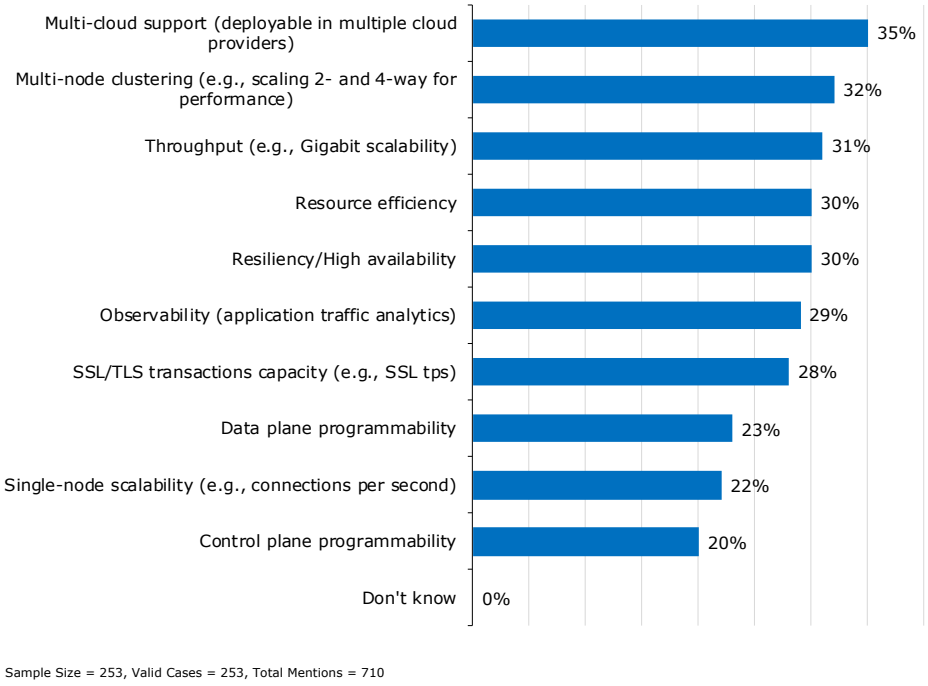
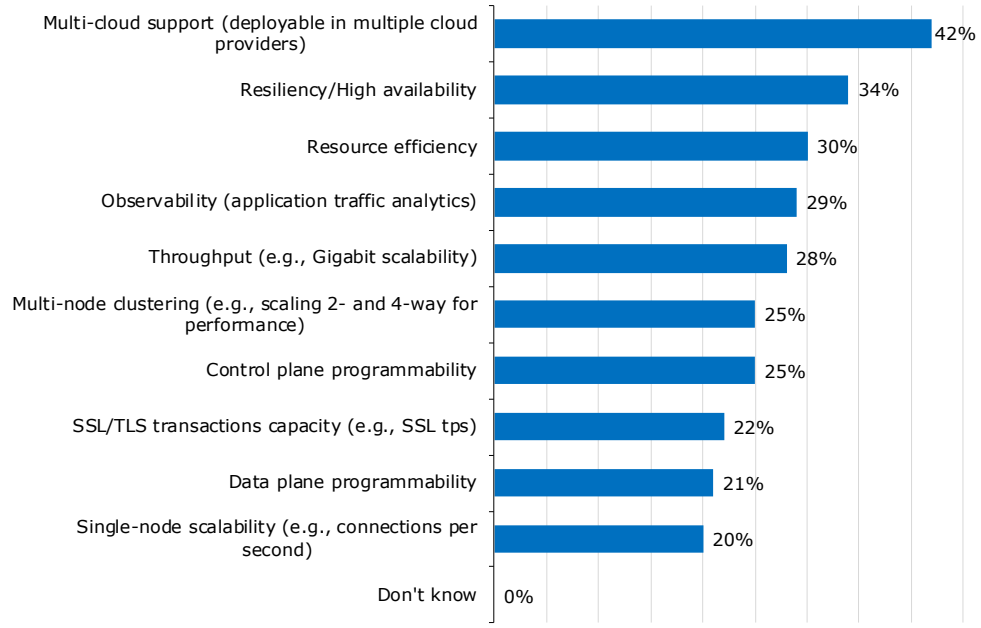


Figure 16. Platform requirements in the data center

In the public cloud, multi-cloud support is the most important platform requirement. This points to the fact that many enterprises want to standardize their application delivery infrastructure across multiple cloud providers.

Figure 17 shows that resiliency stands out as the chief secondary platform requirement. Resource efficiency, observability, and throughput round out the top five. Midmarket enterprises are the most likely to prize resource efficiency. Data plane programmability and single-node scalability remain low priorities, as they did in the data center. However, control plane programmability is a bit more important in the public cloud.



Sample Size = 253, Valid Cases = 253, Total Mentions = 702

Figure 17. Platform requirements in the public cloud

Application Delivery Infrastructure Management

Telemetry and Observability

Application delivery controllers and load balancers are well-situated for providing visibility into application traffic. Thus, enterprises can collect metrics and telemetry from this infrastructure to understand security, application performance, and network performance. **Figure 18** reveals that 82% of enterprises are collecting telemetry and statistics from their application delivery infrastructure.

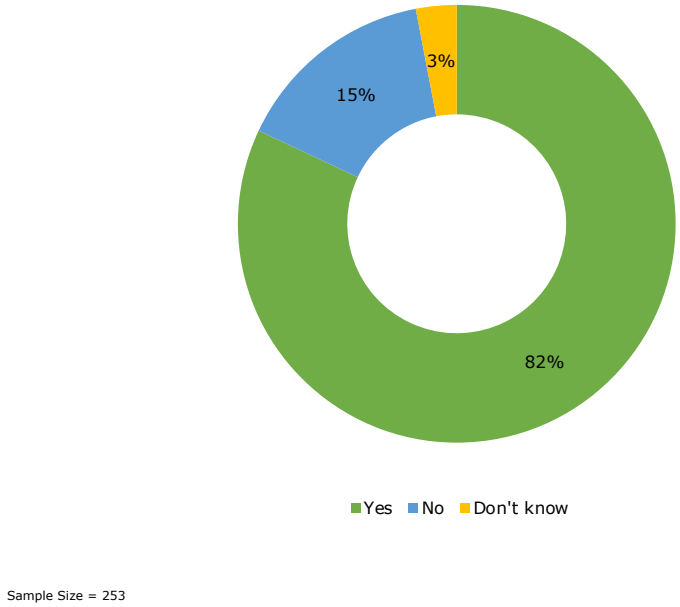


Figure 18. "Does your organization collect and analyze telemetry and statistics from your application delivery infrastructure?"

82%

of enterprises are collecting telemetry and statistics from their application delivery infrastructure.

EMA asked research participants to identify the tools they use to analyze this data. According to **Figure 19,** the average enterprise is using two different tools to analyze this data, and none of them stand out as the de facto choice. However, third-party security monitoring tools are the most popular. The second most popular approach is to export the data to a data repository for analysis by a standalone analytics solution, such as the popular open-source ELK stack (Elasticsearch-Logstash-Kibana).

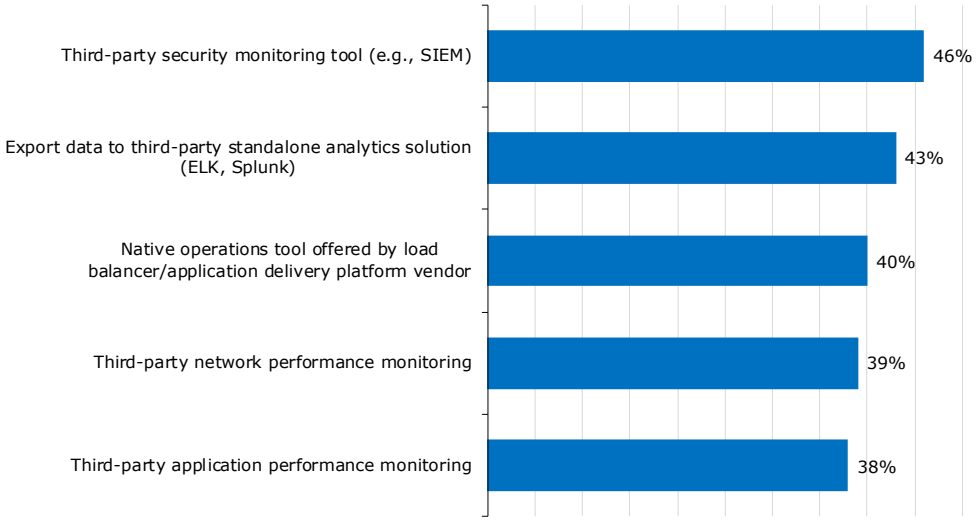
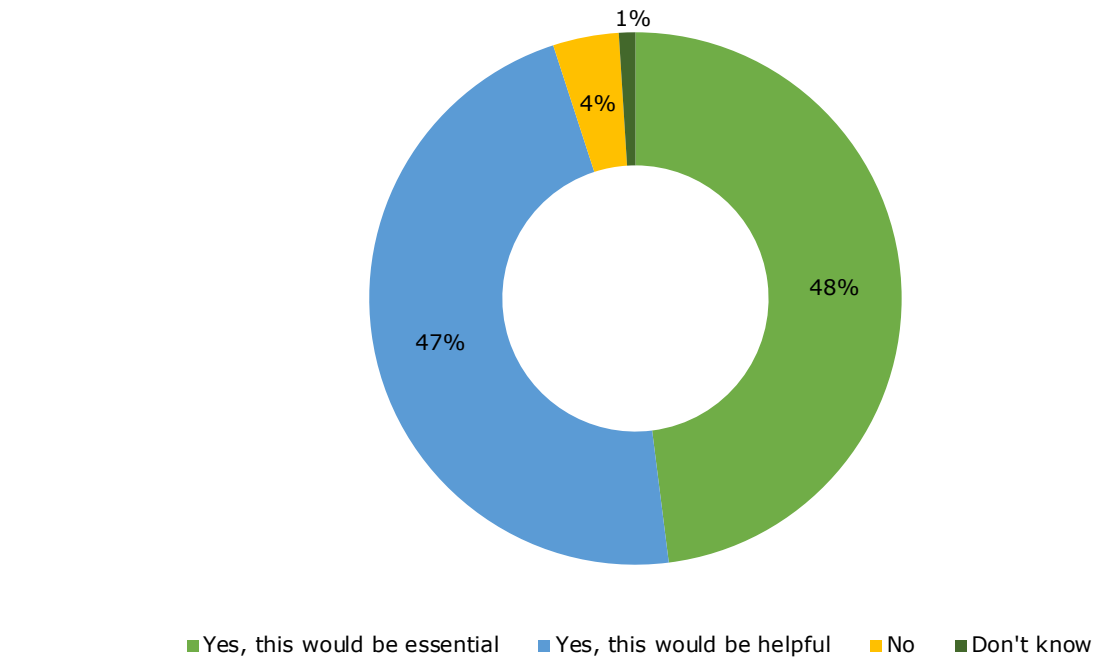


Figure 19. Tools used to analyze application delivery infrastructure telemetry

AIOps and Application Delivery Infrastructure

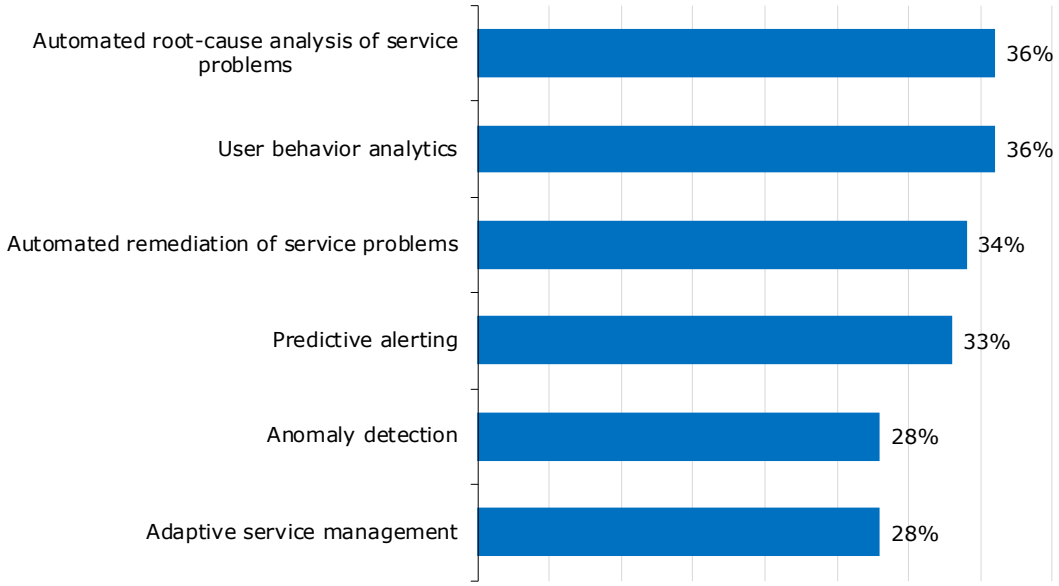
Some vendors of load balancers and application delivery controllers have started developing AIOps capabilities, applying machine learning and statistical analysis to the telemetry collected from their products. EMA asked research participants if they would use such offerings to enhance management and automation of their infrastructure. **Figure 20** reveals that 85% said yes, and nearly half of them said this capability would be essential to their operations.



Sample Size = 253

Figure 20. "If your application delivery infrastructure vendor offered AIOps capabilities to enhance management and automation, would you use them?"

Enterprises have four top use cases for these AIOps capabilities, according to **Figure 21.** First, they are interested in automated root cause analysis of service problems. Second, they are interested in user behavior analytics. Automated remediation of service trouble and predictive alerting round out the top four.



Sample Size = 239, Valid Cases = 239, Total Mentions = 468

Figure 21. Top use cases for AIOps solutions offered by application delivery vendors

Anomaly detection and adaptive service management are the lowest priorities. However, application management professionals consider anomaly detection a top use case, while network operations and infrastructure engineering teams are both very uninterested in this opportunity.

88%

of enterprises automate management of their application delivery infrastructure in their data centers, although only 31% have extensive automation.

Only 41% of enterprises that automate application delivery infrastructure in their data centersare satisfied with that automation.

Infrastructure Automation

Infrastructure Automation in the Data Center

EMA asked enterprises to characterize their automation of application delivery infrastructure in their data centers. While Eighty-eight percent of enterprises automate management of their application delivery infrastructure in their data centers, although only 31% have extensive automation. The majority automate only some management tasks.

Only 41% of enterprises that automate application delivery infrastructure in their data centers are satisfied with that automation. **Figure 22** shows that more than half are only somewhat satisfied, suggesting that they see room for improvement.

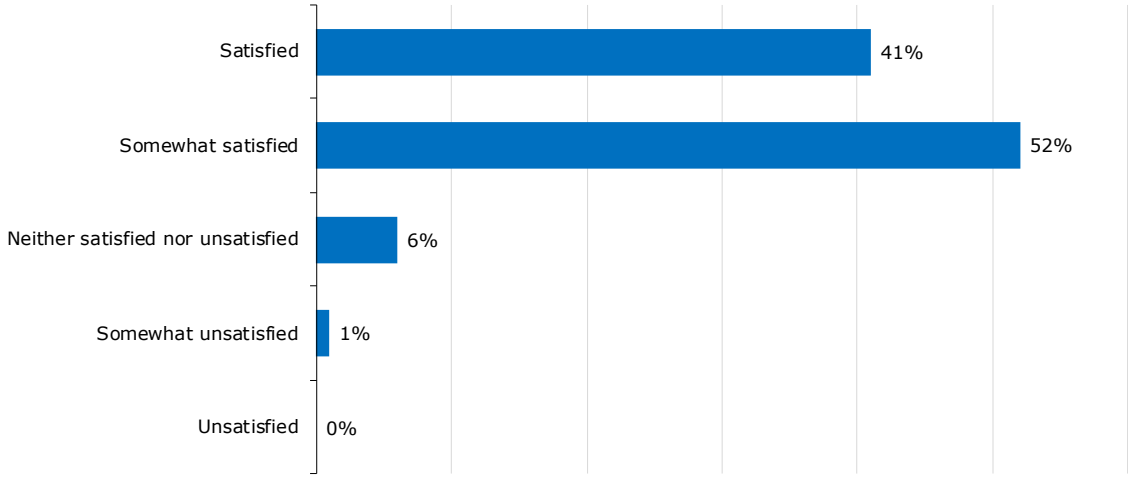


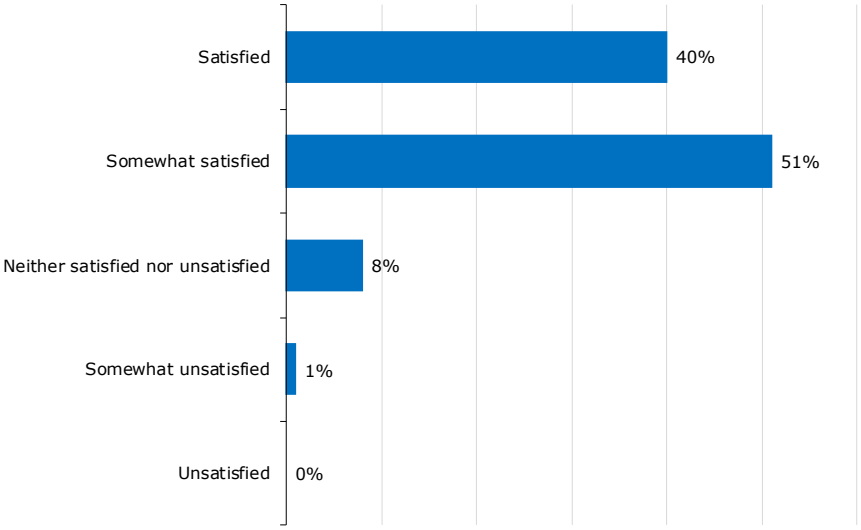
Figure 22. Satisfaction with data center infrastructure automation capabilities

Infrastructure Automation in Public Clouds and Cloud-Native Application Environments

Eighty-five percent of enterprises automate application delivery infrastructure in the public cloud, and 35% say that they use automation extensively.

Automation tool preferences are very different in the cloud, as described by **Figure 34.** Third-party commercial automation tools are the clear favorites. Whereas native automation tools offered by infrastructure vendors are the most popular class of solution for data center infrastructure, this capability is a distant second choice in the cloud. Half of all large enterprises in this survey rely on third-party commercial software. Midmarket firms were less likely to do so.

Satisfaction with cloud infrastructure automation is almost identical to satisfaction with data center infrastructure automation, as **Figure 23** verifies.



Sample Size = 215

Figure 23. Satisfaction with public cloud and cloud-native infrastructure automation capabilities

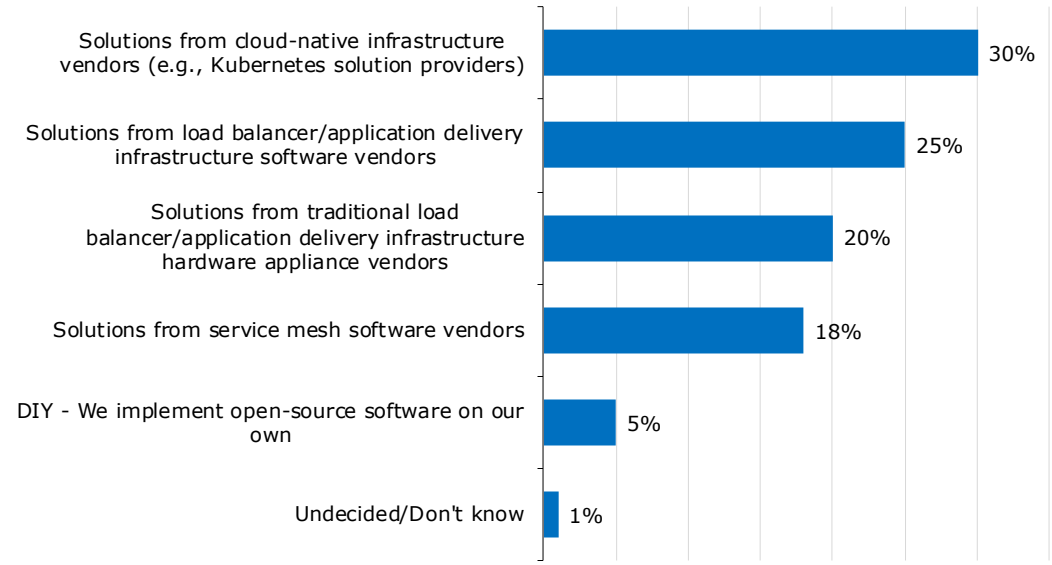
Service Mesh Perspectives

Service mesh is an emerging technology associated with cloud-native, containerized application platforms. It is essentially an infrastructure layer built into a microservices application architecture. In the classic service mesh deployment, service mesh proxies are deployed as "sidecars" side by side with the containers that comprise the application. In these environments, there isn't a standalone infrastructure layer of application delivery controllers and load balancers. The leading service mesh offerings today are open-source software, such as isitio and linkerd.

85%
of the enterprises in this survey have interest in using service mesh.

EMA found that 85% of the enterprises in this survey have interest in using service. Infrastructure engineering teams showed the strongest interest, while network operations teams showed less interest.

No vendors have necessarily claimed this space. Thus, EMA asked research participants who indicated interest in service mesh to reveal how they might prefer to consume service mesh solutions. The two most popular options are solutions offered by cloud-native infrastructure vendors (e.g., providers of Kubernetes solutions) and solutions from vendors of load balancer or application delivery software.



Sample Size = 214

Figure 24. How enterprises want to consume service mesh solutions

Solutions from traditional hardware vendors are the third-most preferred consumption option, followed by solutions from service mesh software specialists.

Management Integration Between Service Mesh and Application Delivery Infrastructure

EMA asked research participants whether they need to integrate management of service mesh with management of their traditional load balancer and application delivery controller infrastructure. Only 2% said no. Nearly half recognize this integration as critical, while another half see it as only helpful. Network operations teams, infrastructure engineering teams, and application management teams are more likely to say this integration is only helpful.

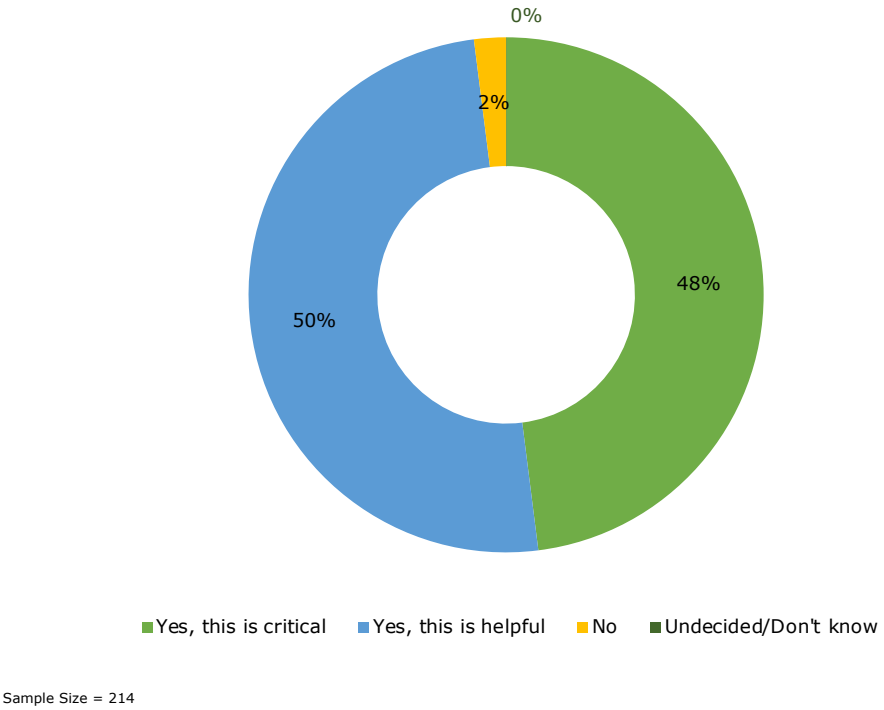


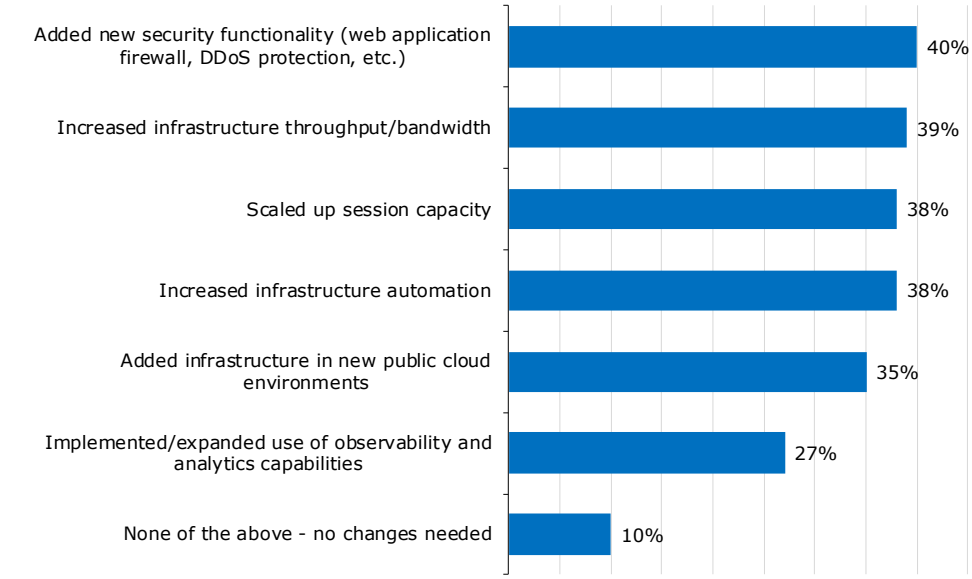
Figure 25. "Does your organization need to integrate management and orchestration of service mesh technology with management of traditional load-balancer/application delivery infrastructure?"

Infrastructure engineering, cloud engineering, application development, and data center operations teams were all more likely to single out observability. Very large enterprises expressed stronger interest in policy enforcement, while very few midmarket companies were particularly interested in this capability.

The Impacts of the Coronavirus Pandemic

EMA started work on this research just as the World Health Organization declared a pandemic of the COVID-19 virus. Thus, EMA added some questions to the survey about how the public health response has impacted application delivery infrastructure, particularly given the massive surge in people forced to work from home.

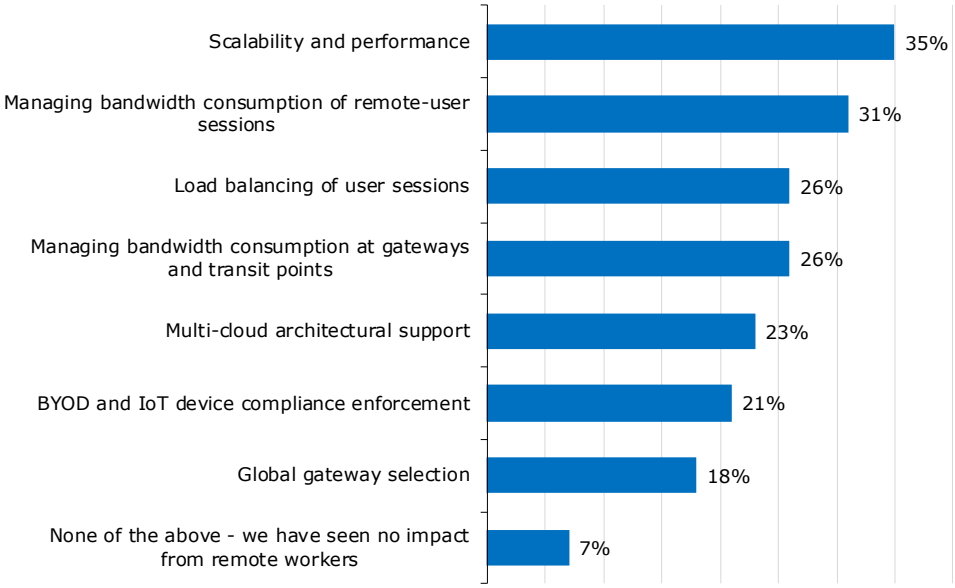
First, EMA asked respondents to indicate what changes they made to this infrastructure in response to the business conditions dictated by the pandemic.Figure 26 shows that only 10% claimed to have made no changes in response to the situation. Overall, the average enterprise is taking two actions. The most common responses are the addition of new security functionality, increased infrastructure throughput, scaled up session capacity, and increased use of automation. Many are also adding infrastructure to a new cloud provider, suggesting that they are scaling out overall services in the cloud.



Sample Size = 253, Valid Cases = 253, Total Mentions = 575

Figure 26. Changes made to application delivery infrastructure in response to the COVID-19 pandemic

EMA also asked respondents to describe how they are using this infrastructure to ensure business continuity and the productivity of users working from home during the pandemic. First, enterprises are relying more on the scalability and performance that this infrastructure delivers to applications, as **Figure 27** reveals. Second, they are using this infrastructure to manage the bandwidth consumption of individual remote user sessions. Network operations teams are especially likely to manage bandwidth consumption of remote users, while DevOps and information security are not.



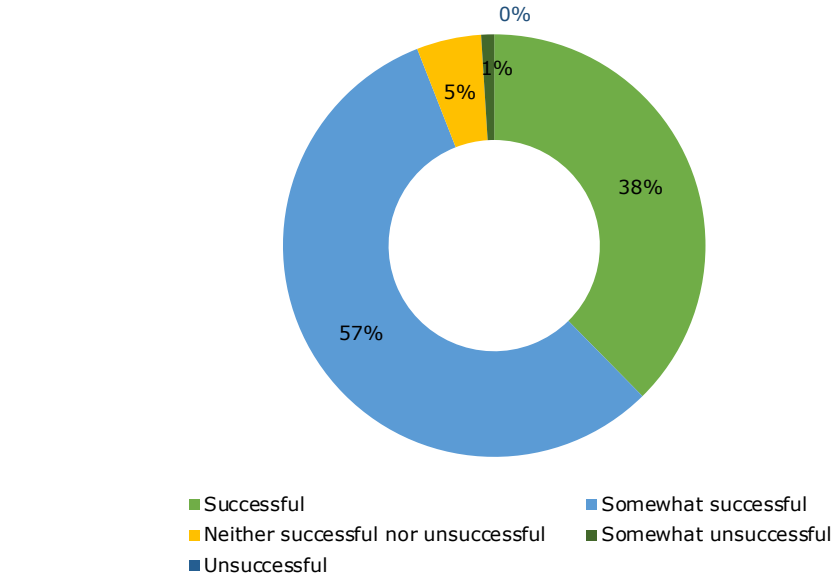
Sample Size = 253, Valid Cases = 253, Total Mentions = 473

Figure 27. Aspects of application delivery infrastructure most important to ensuring business continuity and productivity of users working from home during the COVID-19 pandemic

Load balancing of user sessions and managing bandwidth consumption at gateways and transit points are the secondary capabilities.

Succeeding with Application Delivery Infrastructure

Only 38% of enterprises are fully successful with their use of load balancers and application delivery infrastructure. More than half are somewhat successful, meaning they see room for improvement.



Sample Size = 253

Figure 28. Overall success with load balancer and application delivery infrastructure

Enterprises must be willing to spend on this technology. Success with application delivery infrastructure correlates strongly with budget growth. Those with the highest rates of budget growth are the most likely to be successful with this infrastructure. Companies with flat or shrinking budgets are much less likely to succeed.

Only 38% of enterprises are fully successful with their use of load balancers and application delivery infrastructure.

Business and Technical Challenges

Figure 29 reviews the top business challenges that enterprises encounter with their application delivery infrastructure. A skills gap is the biggest challenge with application delivery infrastructure. Some of the various teams that work with this technology lack the expertise to manage it properly. Change control/role-based access, budget shortfalls, and conflicts between teams are the chief secondary challenges.

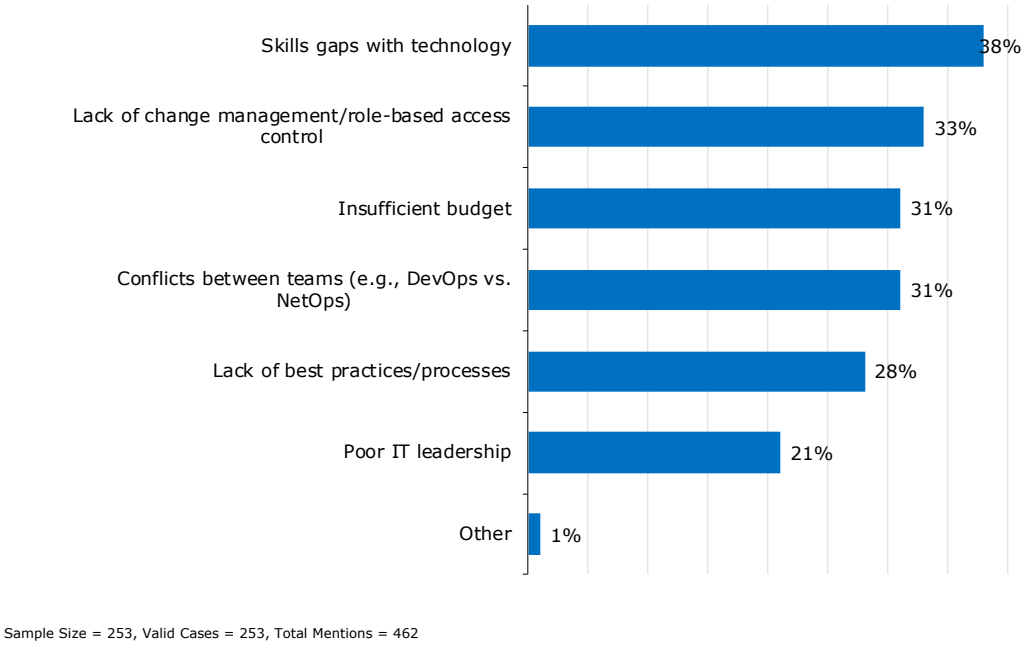
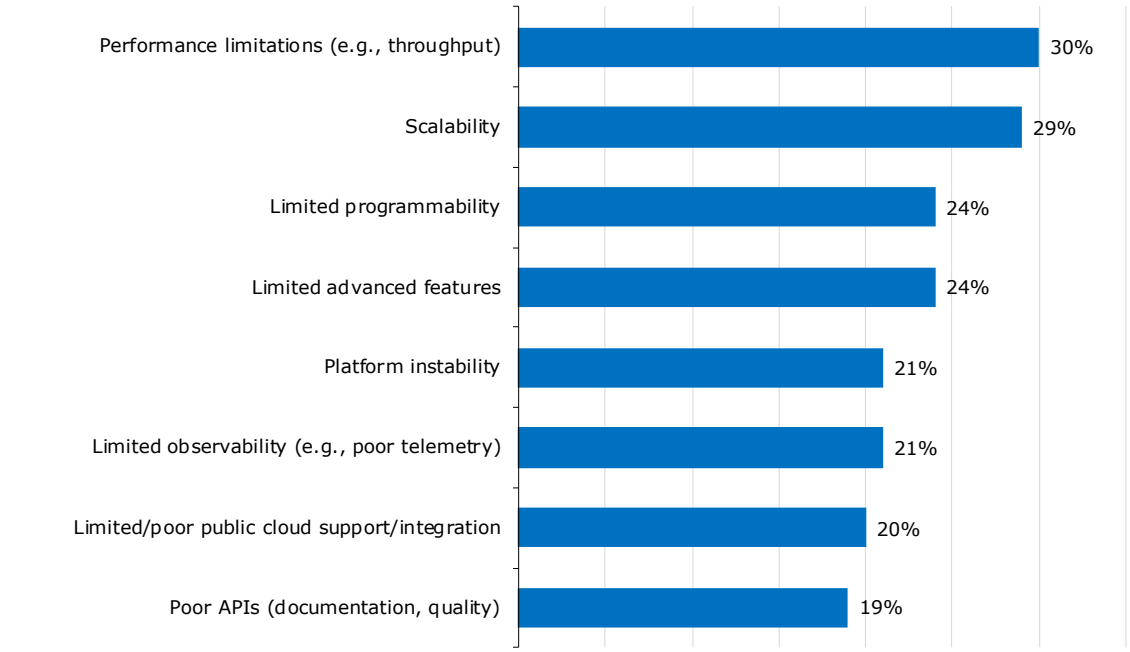


Figure 29. Business challenges associated with load balancers and application delivery infrastructure

Poor IT leadership is the least prominent business challenge. Data center operations are more likely to perceive such a problem, while infrastructure engineering and DevOps teams are less likely to see this issue.

A skills gap is the biggest challenge with application delivery infrastructure.Some of the various teams that work with this technology lack the expertise to manage it properly.

Figure 30 reviews the technical challenges that companies grapple with in application delivery infrastructure. First, enterprises are struggling most often with the performance limitations of their application delivery infrastructure, which suggests that they need to upgrade the throughput of these solutions. Next, they are struggling with infrastructure scalability.



Sample Size = 253, Valid Cases = 253, Total Mentions = 479

Figure 30. Technical problems associated with load balancers and application delivery infrastructure

The two leading secondary challenges are limitations with programmability and advanced features.

Conclusion

This research shows that the days of appliance-based application delivery infrastructure are over. Enterprises are embracing cloud-native software, both in the data center and the cloud. Furthermore, service mesh is top of mind for most enterprises.

This transition to software and the cloud has fragmented infrastructure engineering and operations, but enterprises are working to close this gap, particularly because it presents a security risk. Infrastructure vendors can help with this issue by adding multi-vendor support to their own management tools and increasing deployment flexibility. The former will be particularly helpful as enterprises adopt service mesh.

Enterprises are particularly interested in application delivery infrastructure automation. They also want to leverage the telemetry that is available within this infrastructure. Beyond simple telemetry generation, enterprises would welcome AIOps capabilities from their infrastructure vendors to improve operations and security.

EMA was disappointed to find that only a minority of companies are fully successful with this infrastructure, although automation and AIOps appear to be paths to improving this issue. Enterprises must press forward with finding ways to advance their success with application delivery infrastructure because it remains critical, even as application architectures evolve and migrate to the cloud. In fact, this research found that this infrastructure has proven itself indispensable to business continuity during the current COVID-19 pandemic. It's good that most enterprises are expanding their budgets for this technology.

EMA will continue to follow this market and adjacent markets closely with its ongoing research into infrastructure and operations.

Case Study: Fortune 100 Tech Company Improves Website Performance, Resiliency, and Agility with NGINX

A Fortune 100 technology company generates a significant portion of its revenue through its website. As the company adopted a product-oriented approach to operating the website, it needed to modernize its application delivery infrastructure to support increased demand for resiliency and agility.

The company had a monolithic, hardware-centric application delivery cluster (ADC) deployed in front of its website infrastructure to handle application request routing. This reverse proxy cluster had 12,000 lines of code in a single configuration file, presenting a complex, single point of failure for this critical website.

“The cluster was quite brittle,” said the senior principal engineer for the company’s site reliability team. “This introduced the potential for a small error in a change to have a very negative impact on a wide range of applications.”

Given that minutes of downtime could cost the company millions of dollars, any change applied to the ADC cluster went through several layers of approvals that typically required weeks of lead time. This slow pace of change flew in the face of product-oriented teams’ efforts to apply a continuous integration and continuous deployment (CI/CD) pipeline. The website’s 30 application development teams working across multiple continents found themselves waiting in line to implement changes.

“Any new feature or any defect that required a change was locked into someone else’s timeline that could take two or three weeks to turn around,” the engineer said. “We wanted to break down this monolith and give responsibility to individual product teams. We wanted the product teams to own and maintain the routing rules for their products. By breaking the routing responsibility into smaller clusters, teams gained the flexibility to release changes at a pace that better suited their product lifecycle.”

The site reliability team made the strategic decision to migrate from its legacy ADC hardware cluster to software-driven clusters of NGINX ADC instances running on virtual machines. This ADC software could integrate directly into the CI/CD pipeline. The team worked with the NGINX division of F5 Networks to migrate to this new infrastructure. The changeover has been gradual, but the majority of the website’s traffic is now traversing NGINX infrastructure.

Benefits

With NGINX in place, the company has experienced improvements in operational efficiency, risk management, application performance, and monitoring.

The site reliability team integrated NGINX with its DevOps pipeline and gave individual application development teams the ability to provision their own services on NGINX instances, rather than rely on the infrastructure team to handle change requests. The days of managing a configuration file with thousands of lines of code were over. This shortened lead times from weeks to potentially turning around changes within a few hours.

The company reduced risk by eliminating its ADC cluster governed by a single configuration file with thousands of lines of code. Now, each product team working on the website has access to a cluster of specialized NGINX instances. When product teams push a change to NGINX, it only affects a small group of applications or services, rather than the whole website. Also, product teams can tie their NGINX instances to their own CI/CD pipelines, allowing them to run several layers of validation and testing against the changes before pushing them into production.

The shift from a monolithic hardware infrastructure to a cluster of ADC software dedicated to individual products on the website drove resource efficiency and led to reduced latency throughout, the engineer said. Finally, NGINX's dashboards provided critical visibility into infrastructure, health, and performance.

"We can see upstreams listed out on the dashboard and see what's performing and what is not in real time, which is a level of visibility we didn't have in our old solution," he said. In particular, this visibility revealed last year that the legacy reverse proxy infrastructure was failing to log routing errors in some cases. "We were losing customer traffic, but we had zero record of it."

The migration to NGINX will continue throughout this year, and the site reliability team is also exploring the use of NGINX Controller, a central management and monitoring tool, to orchestrate and test websites' business continuity plans. It is exploring how NGINX Controller can support the testing and implementation of live data center failovers.

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates® (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help EMA's clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals, and IT vendors at www.enterprisemanagement.com or blog.enterprisemanagement.com. You can also follow EMA on Twitter, Facebook, or LinkedIn.

Corporate Headquarters:
1995 North 57th Court, Suite 120
Boulder, CO 80301
Phone: +1 303.543.9500
www.enterprisemanagement.com

3990RRSummary-4009.08062020-CS