EMA
IT & DATA MANAGEMENT RESEARCH, INDUSTRY ANALYSIS & CONSULTING

Prepared for:

Progress®

How to Succeed with Load Balancing in a Hybrid Multi-Cloud World

October 2022 EMA Research Report

By Shamus McGillicuddy, Vice President of Research and Robert Gates, Senior Analyst

Table of Contents

Executive Summary

This report, prepared for Progress Software, explores how IT organizations are evolving their approach to load balancing and application delivery controllers to support hybrid cloud and multi-cloud. The research findings are based on a July 2022 survey of 152 North American IT professionals involved in their organization's data center and cloud load balancing strategies.

Hybrid Cloud is Driving Load Balancing Strategies

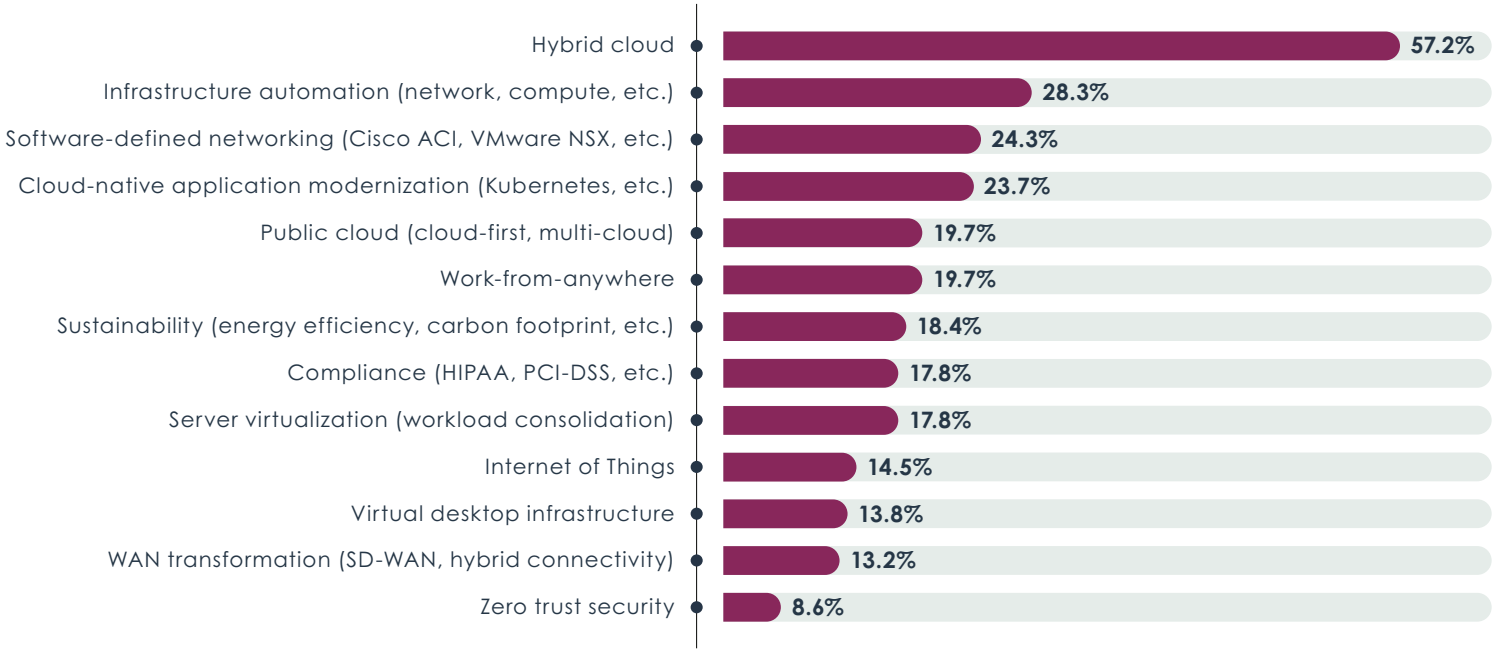
Load balancers and application delivery controllers (ADCs) are a critical part of application infrastructure. These devices distribute incoming application traffic across a pool of application servers to ensure individual servers are not overwhelmed by incoming traffic and that every application transaction is efficiently addressed.

In the past, load balancing was a data center technology. Today, IT organizations must take a hybrid, multi-cloud approach to the technology. As **Figure 1** reveals, hybrid cloud drives the majority of load balancing and ADC strategies today. This suggests that organizations should take a unified approach to the technology across their data centers and their public cloud environments.

Cloud-native applications are a secondary driver of strategy, but developers (39%) are much more likely than infrastructure and operations professionals (15%) to cite it. This suggests that developers are pushing IT organizations to extend their load balancing strategies into the containerized microservices platforms that they are using to transform applications in data centers and in the cloud.

EMA believes that IT organizations need to modernize and unify their load balancing architecture to meet the demands of hybrid cloud architectures and cloud-native applications.

Figure 1. Technology initiatives most influential on load balancer and application delivery infrastructure strategy



Sample Size = 152, Valid Cases = 152, Total Mentions = 421

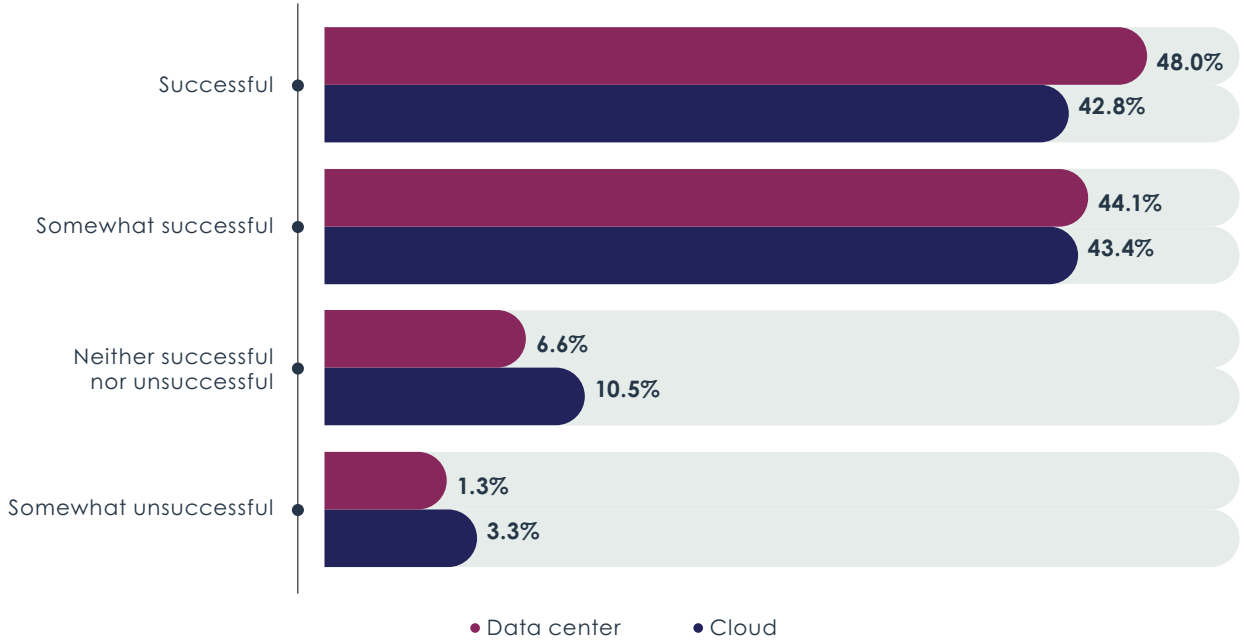
Most Enterprises Believe They Could Do Better with Load Balancing

Figure 2 reveals that only a minority of IT organizations believe they are fully successful with their use of load balancers and ADCs, in both their data centers and the cloud.

EMA found that IT executives are more enthusiastic than infrastructure and operations professionals and developers about success, suggesting a gap in awareness in the CIO suite. Personnel who work more closely with the technology are more pessimistic. This gap is a concern because IT leaders may make strategic decisions about infrastructure based on false assumptions about the effectiveness of their strategy. Members of network engineering teams, perhaps the one group most intimately familiar with traditional data center load balancing, expressed significant concern about their organization's success with load balancing in the cloud.

The following pages will explore how enterprises can optimize their hybrid multi-cloud load balancing strategies.

Figure 2. IT professionals rate their success with load balancer/application delivery infrastructure in data centers and the public



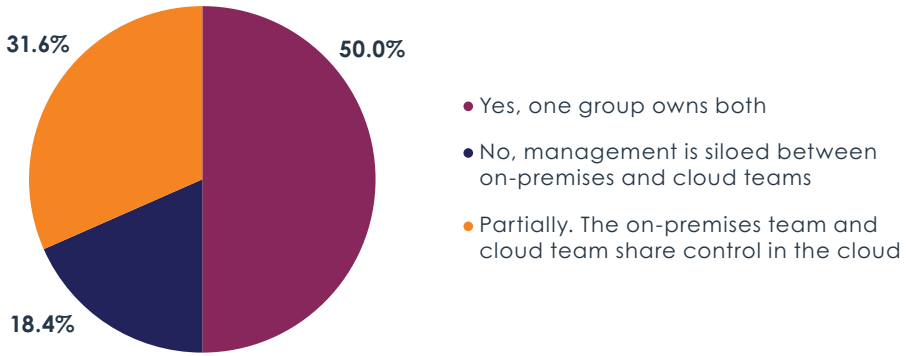
Sample Size = 152

A Roadmap to Load Balancing Success in the Hybrid Multi-Cloud

Get DevOps and NetOps on the Same Page

The network team has traditionally owned and operated load balancers in the data center, ensuring a consistent, effective approach to implementing and managing this infrastructure. However, as enterprises migrate applications to the cloud, application and DevOps teams have excluded the network team from load balancing decisions. EMA believes that IT organizations must adopt an cross-functional approach to load balancing across a hybrid multi-cloud architecture. Unfortunately, **Figure 3** reveals that many IT organizations are not quite there.

Figure 3. In your organization, does the team that owns and operates load balancers and application delivery infrastructure in your data center also own and operate such solutions in the cloud?



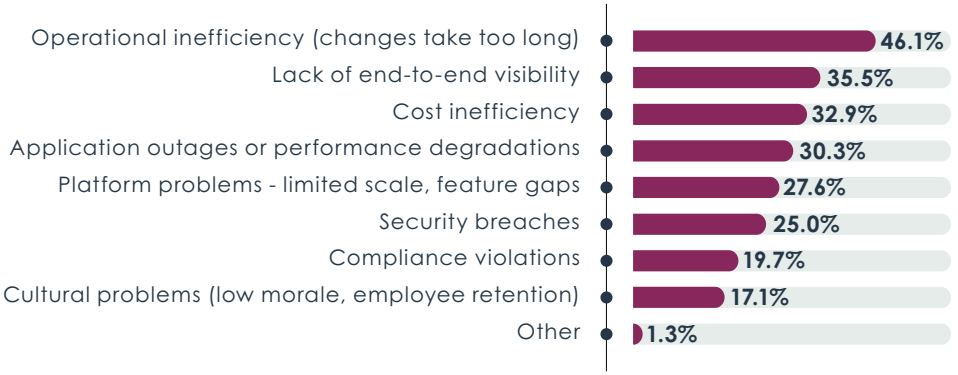
Only half of organizations have a single group that owns and operates load balancing across data centers and cloud infrastructure. Nearly one-third have partially unified two separate groups, and more than 18% remain completely fragmented. Midmarket enterprises (1,000 to 2,499 employees) were the most likely to have divided ownership across clouds and data centers.

EMA suspects that fragmented operations are more prevalent than this data reveals. Respondents who work in DevOps were much more likely (75%) to report a completely siloed approach to load balancing, suggesting that DevOps groups are often using their own load balancing platforms while developing and testing applications. Once they roll applications into production in a hybrid cloud, the infrastructure team will demand use of a standard load balancing platform.

Sample Size = 152

Figure 4 details the disruptions that occur when IT organizations fail to unify load balancer operations across hybrid infrastructure. Operational inefficiency is the major problem. Moves, adds, and changes take too long, which makes the organziation less responsive to the needs of a business.

Figure 4. Problems caused by divided administrative ownership of load balancing and application delivery infrastructure between public cloud and private data center environments



Visibility also suffers as tools struggle to collect consistent telemetry across end-to-end infrastructure. Larger enterprises especially struggle with visibility. Cost-inefficiency and application outages are also significant issues. One-quarter of companies claimed to have experienced a security breach as a direct result of fractured operations.

Sample Size = 76, Valid Cases = 76, Total Mentions = 179

Close Skills Gaps Through Cross-Silo Partnerships

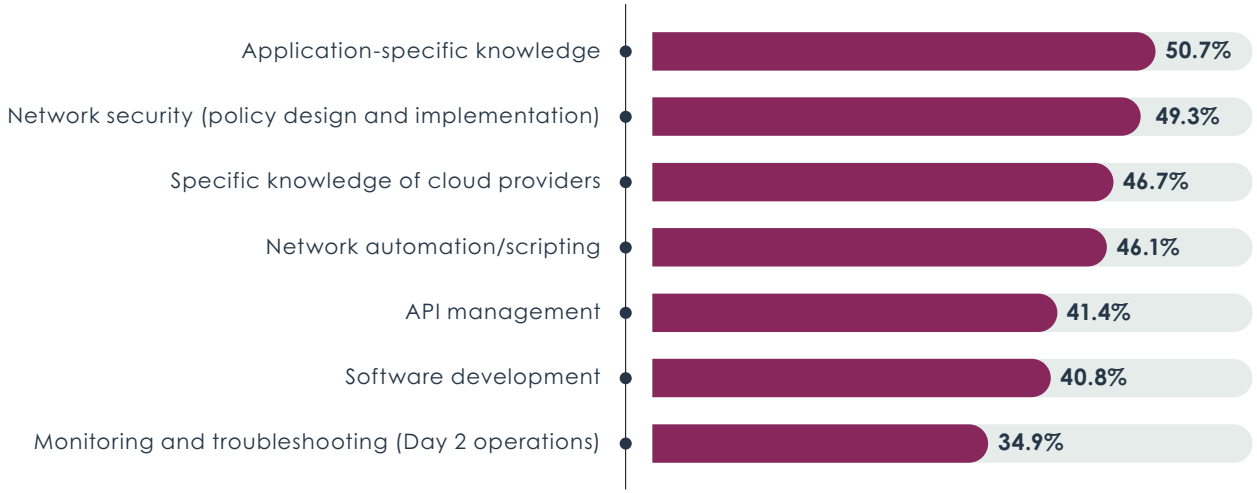
EMA found that 86% of organizations report at least some difficulty with hiring and retaining people with the technical skills and knowledge required to maximize the value of load balancers and ADCs. Organizations that struggle the most with this skills gap are less likely to report success with their use of load balancers and ADCs.

IT organizations should work with their infrastructure vendors on training personnel on the management of their solutions. Organizations should also adopt a standard load balancing and ADC platform so personnel don't have to learn multiple technologies.

Most importantly, organizations should forge cross-silo partnerships to close skills gaps. EMA found that many issues could be solved if groups worked together. For instance, **Figure 5** reveals that application-specific knowledge is the top skills gap. Network teams may lack this knowledge, but the DevOps team will have deep expertise with applications.

The second-biggest skills gap is around network security. The DevOps team might lack this expertise, but the security group and the network group can help them. Network and security groups might lack cloud provider expertise, but the DevOps team can bring it to the table. Network automation might be a foreign concept to security and DevOps, but network teams will have plenty of knowledge about network-specific automation solutions.

Figure 5. Load balancer and ADC skills that organizations most struggle to find in new hires



Sample Size = 152, Valid Cases = 152, Total Mentions = 471

Don't Rely on Cloud Provider Load Balancing Solutions

Cloud providers offer their own native load balancing solutions. EMA research found that 71% of organizations use cloud providers' solutions today, but 57% deploy virtual ADCs and load balancers from their traditional networking vendors in the cloud, too.

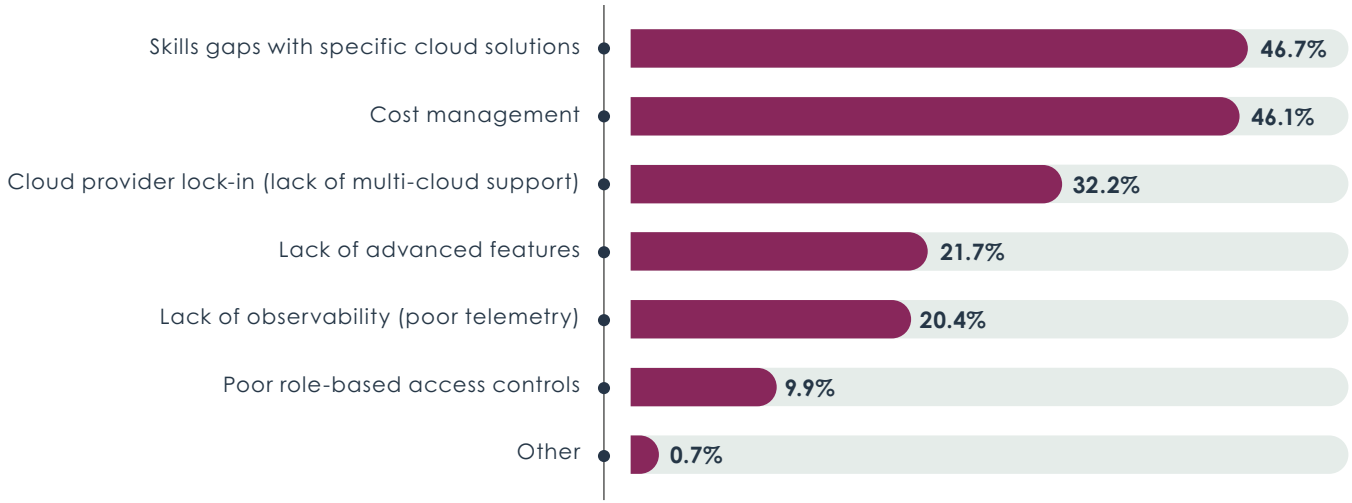
One major shortcoming of the load balancers that cloud providers offer is lock-in. These solutions are applicable only in a single-cloud environment. None of them offers multi-cloud support. With most enterprises using multiple cloud providers today, they are better off adopting a virtual ADC or load balancer that they can deploy in any cloud environment. In fact, EMA research found that adoption of virtual appliances increases with the number of cloud providers in use, from 38% in single-cloud enterprises to 73% in enterprises that use three providers.

Figure 6 reveals that cloud provider lock-in isn't even the biggest challenge associated with using a provider's native load balancing solution. Instead, a skills gap is the biggest issue. As organizations adopt multiple providers, personnel have to learn how to work with each provider's solution, including how to work with proprietary nomenclature and APIs.

Cost management is another major issue. The usage-based fees that many cloud providers charge may become more expensive than the licensing terms that load balancing vendors offer. This situation can challenge an organization's ability to plan and forecast budgets.

Finally, nearly 22% of organizations complained about the lack of advanced features offered by cloud providers. For instance, virtual ADCs offer web application firewalls, application acceleration, single sign-on, and more.

Figure 6. Most challenging issues with using native load balancing and application delivery networking features that cloud providers offer



Sample Size = 152, Valid Cases = 152, Total Mentions = 270

Treat Load Balancers as Part of Security Architecture

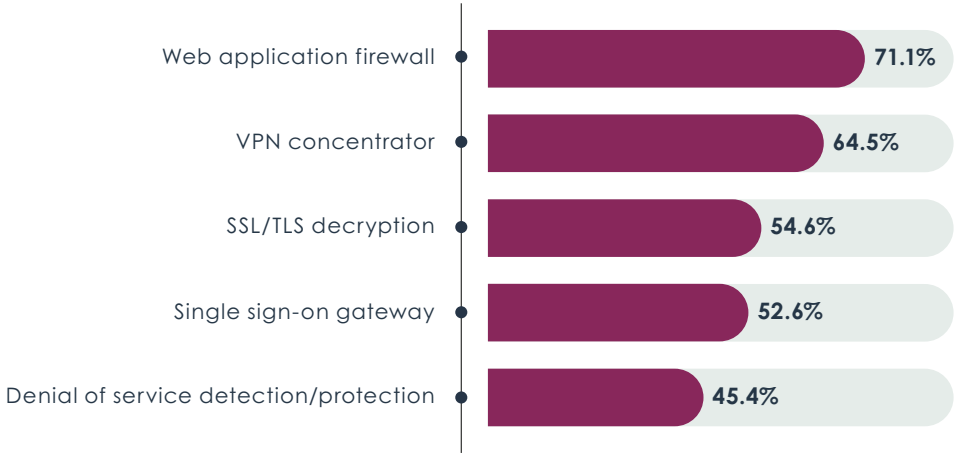
A key difference between a load balancer and an ADC is security. As application security requirements diversify, vendors consolidate a variety of security functions onto load balancers, rebranding them as ADC platforms, including web application firewalls and DDoS protection.

This research found that 89% of IT security teams consider ADCs to be part of overall security architecture. Network and DevOps teams may not fully appreciate the importance of ADCs to security. As these groups work together on a hybrid multi-cloud architecture, they should all embrace the idea of making ADCs an integral component of security.

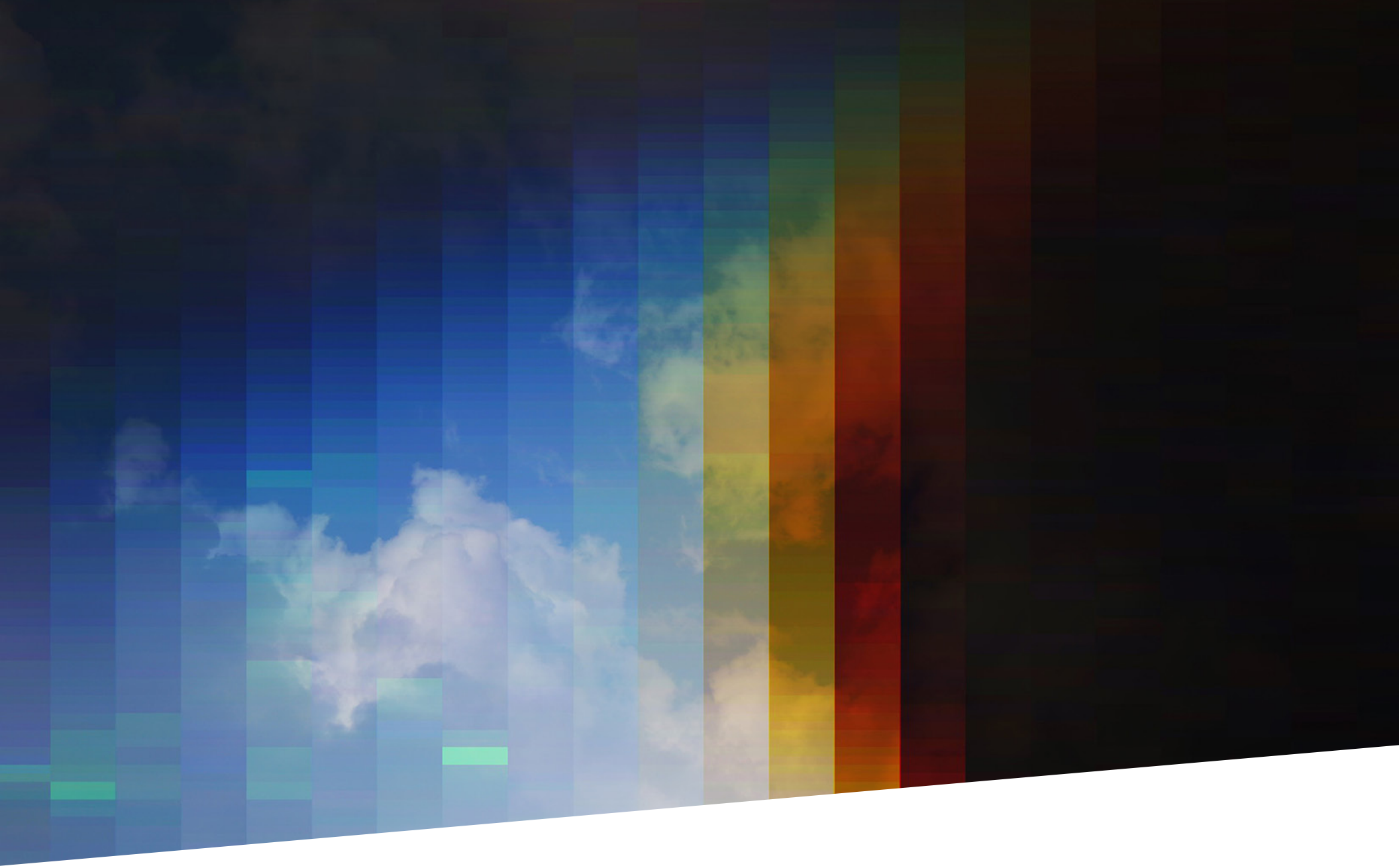
Figure 7 reveals that most enterprises are using four security functions in their ADCs today. The vast majority are using web application firewalls. More successful users of load balancers and ADCs are even more likely to use web application firewalls. Many are also using a VPN concentrator, SSL/TLS decryption, and single sign-on gateway functionality.

DDoS protection is less popular, but members of the security group are more likely to report using it. Thus, when security is participating in an ADC strategy, they enable DDoS protection on these platforms.

Figure 7. Security-related capabilities of application delivery controllers that organizations use



Sample Size = 152, Valid Cases = 152, Total Mentions = 438



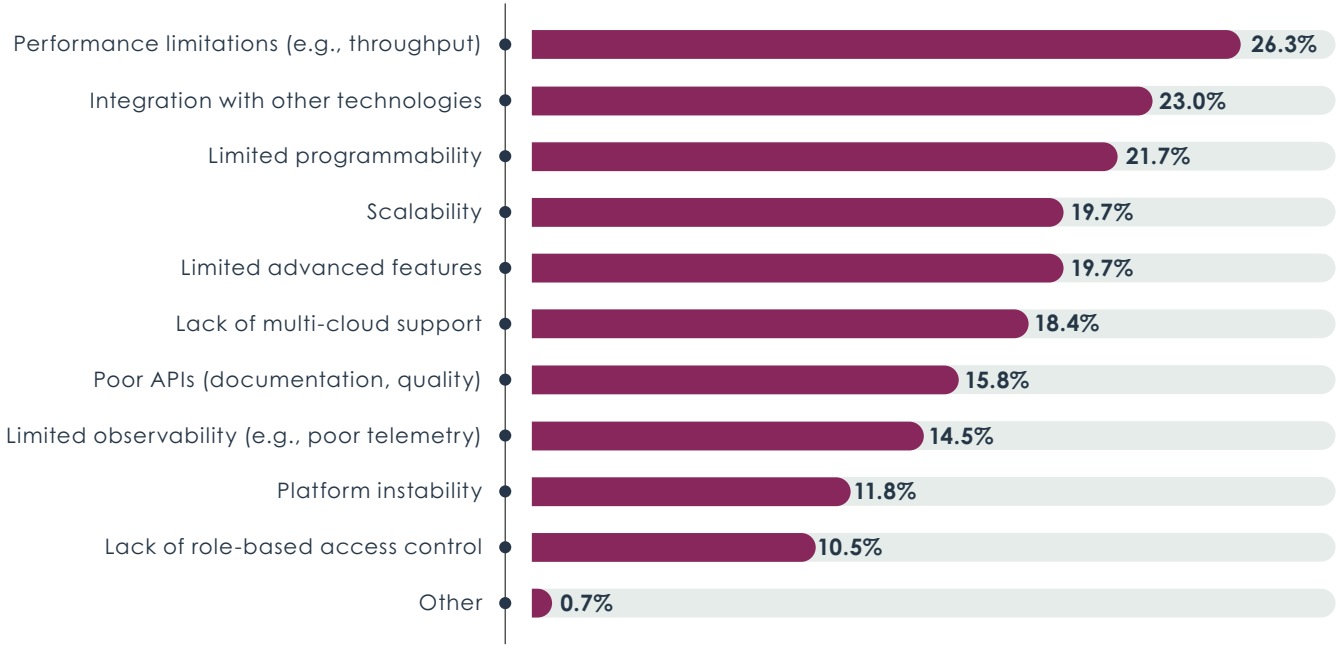
Load Balancing Pitfalls to Avoid

Now equipped with a roadmap for adapting load balancing strategies for hybrid cloud and multi-cloud, IT organizations should also recognize and avoid pitfalls that often undermine the successful use of this technology. If a technology team can navigate these problems well, its chances of success will increase.

Figure 8 details the technical problems that often derail load balancer and ADC strategies. The most prominent issue is platform limitations. For instance, the solution lacks the throughput and packet processing performance to support applications' needs. This points to the need for careful evaluation of platform requirements before designing and implementing a solution.

Integration with other technologies is also a major issue. Many organizations integrate infrastructure orchestration and automation, security monitoring, IT service management, and cloud management. Companies must ensure that they have sufficient expertise to execute this integration, and they should evaluate the APIs of any platform before they proceed. Multi-cloud enterprises were more likely to struggle with integration issues. EMA believes that using a single ADC platform across multiple clouds will reduce the complexity of integration.

Figure 8. Technical problems that most challenge an organization's successful use of load balancer/application delivery infrastructure



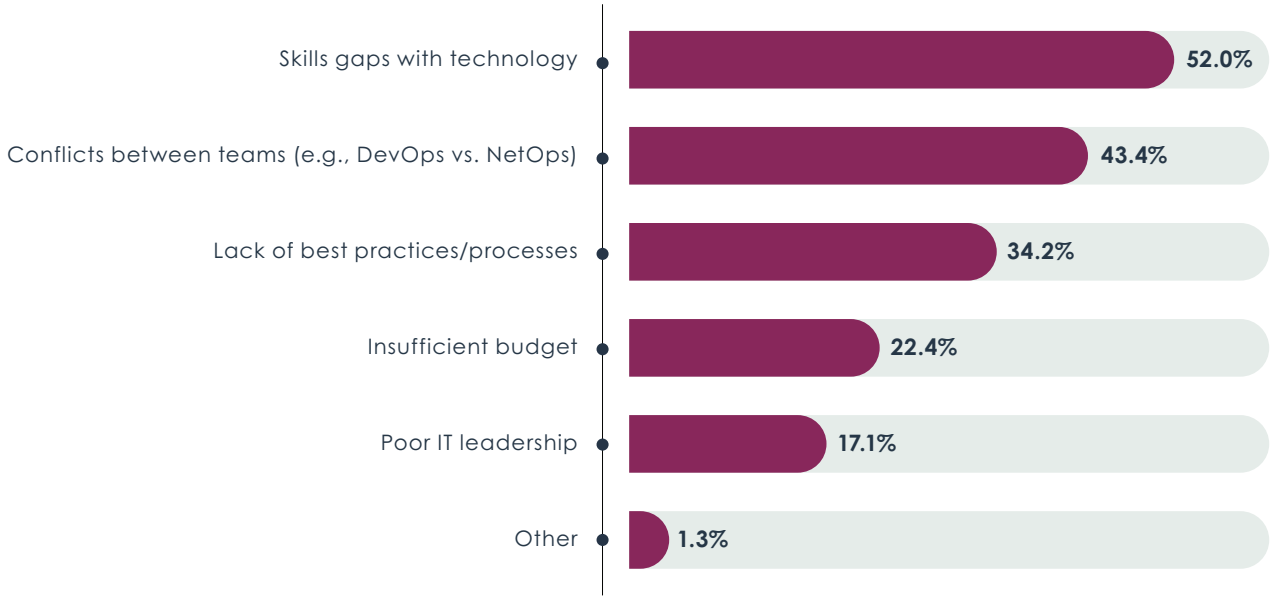
Sample Size = 152, Valid Cases = 152, Total Mentions = 277

Limited programmability is the third leading technical issue. Before adopting a new platform, an organization should evaluate whether the solution supports the use of scripting for automation and customization.

Figure 9 reveals that skills gaps are the biggest business issue when working with load balancers and ADCs, which is no surprise since this research already revealed that many enterprises struggle to hire skilled personnel.

Conflicts among teams are also a major problem. DevOps, network, and security teams must learn how to work together on a common platform. Finally, more than one-third of organizations are also struggling with a lack of best practices and processes. Cybersecurity teams were especially concerned about this issue. Operational errors can lead to security breaches, after all. Organizations should document processes for load balancer and ADC operations. This will reduce risk, but it will also reduce conflicts among individual groups.

Figure 9. Business issues that most challenge an organization's successful use of load balancer/application delivery infrastructure



Sample Size = 152, Valid Cases = 152, Total Mentions = 259

EMA Perspective

Ongoing EMA research consistently finds that hybrid multi-cloud architectures disrupt network and security operations. As IT organizations embrace the cloud, they must transform load balancer and ADC infrastructure and operations.

This research report reveals the risks and challenges that organizations encounter with this technology when they embrace the cloud. Complexity increases, operational processes fragment, and security risk rises. By taking a unified approach to load balancers and ADCs across hybrid and multi-cloud networks, organizations can improve their chances of success. Readers should use this paper as a high-level guide for adapting to the cloud era.

Appendix: Demographics

Figure 10. Job titles

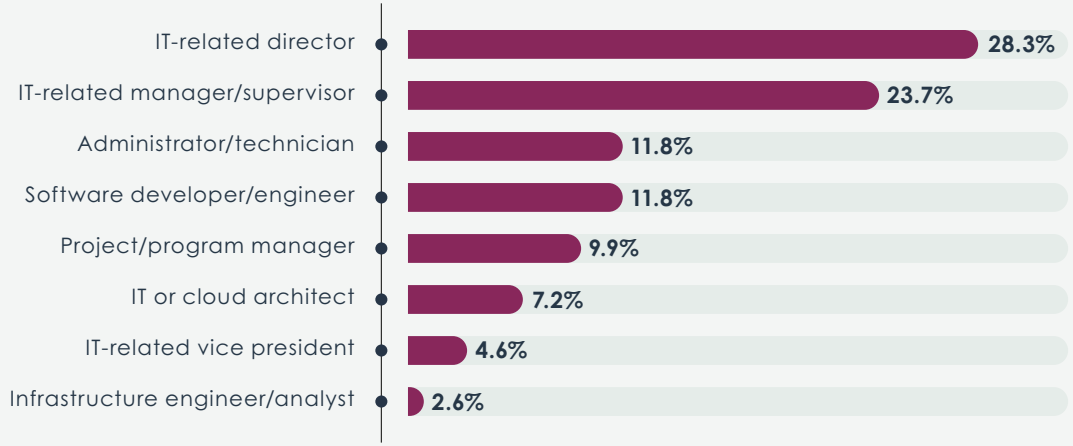
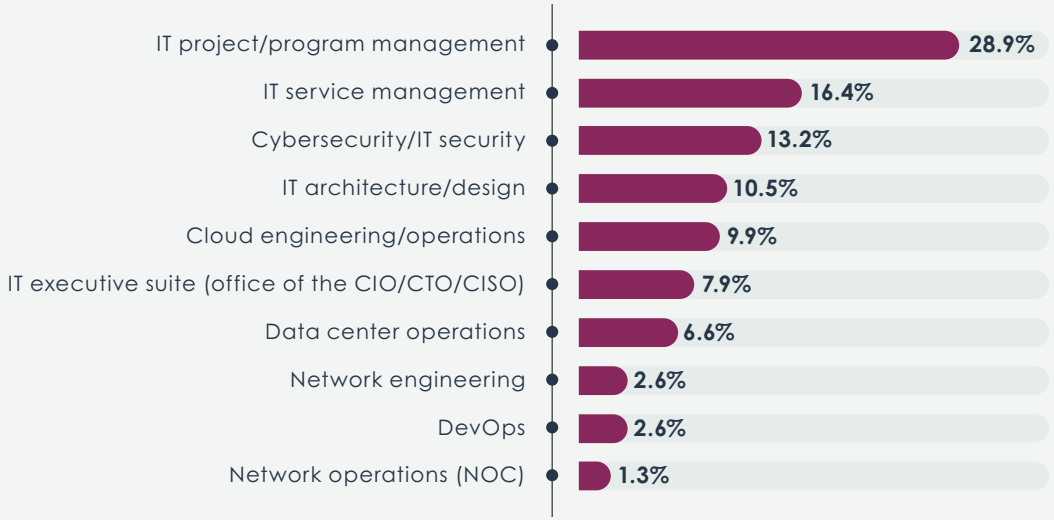


Figure 11. IT groups or departments



Sample Size = 152

Figure 12. Company size

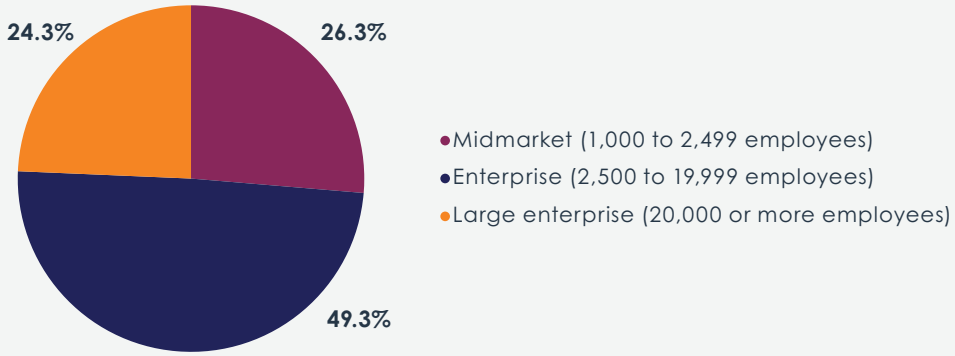
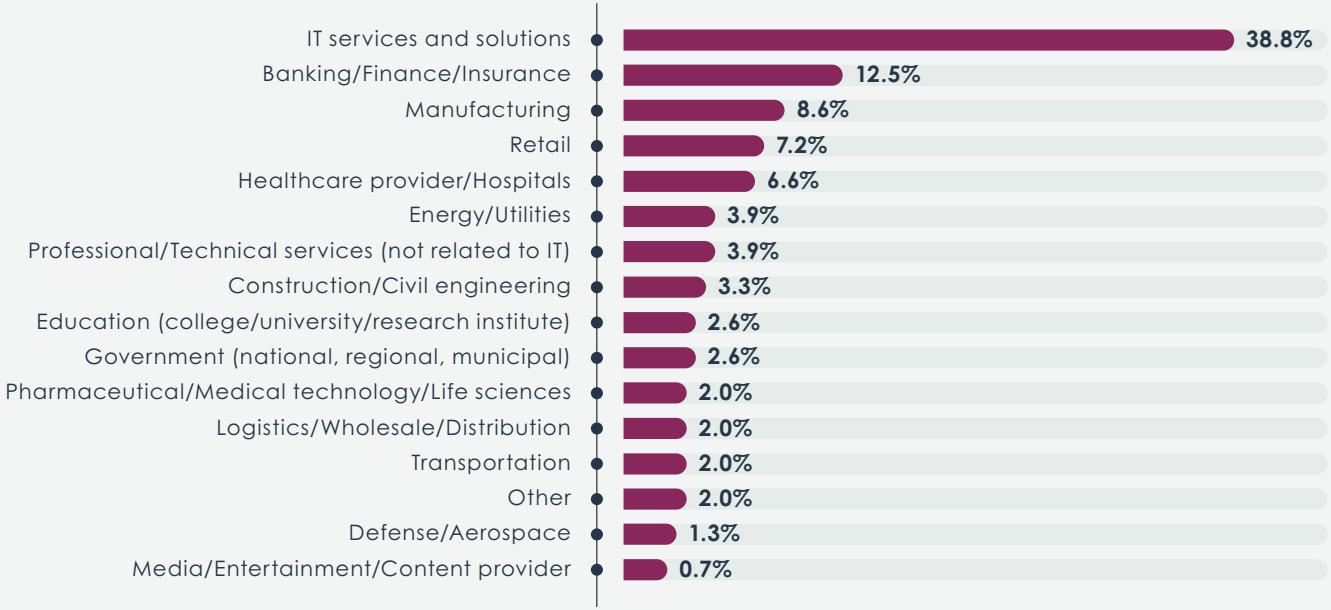


Figure 13. Industries



Sample Size = 152

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**. You can also follow EMA on **Twitter** or **LinkedIn**.

1995 North 57th Court, Suite 120, Boulder, CO 80301 +1 303.543.9500 **www.enterprisemanagement.com**

4228.102422