State of Application Services

2019 REPORT

Table of contents

TABLE OF FIGURES

Introduction

Welcome to the 2019 State of Application Services report. When we started this journey to understand the importance of application services within the context of emerging technologies such as cloud, IoT, and software-defined technologies more than five years ago, we knew we were shining a light on a future disruption.

What we didn't know was that applications themselves would become the very foundation of the digital economy—thus ushering in an even more prominent role for application services. It's these services that help organizations ensure that their applications can be quickly migrated and deployed with the confidence that they are always available, protecting their business from unforeseen threats, and scaling seamlessly around the world—no matter where their applications reside.

For our fifth annual survey, we asked nearly 2,000 respondents globally—across a range of industries, company sizes, and roles—about the challenges and opportunities presented by the ongoing process of digital transformation. This survey provides a uniquely comprehensive analysis of the trends shaping the application landscape—and how IT organizations are transforming to meet the ever-changing demands of the digital economy.

2019 Key Findings

01 87% of respondents have multi-cloud architectures, driven by an app-first methodology.

Most organizations evaluate cloud decisions based on what environment is best for each application, an app-first methodology that leads to multi-cloud architectures for nearly 90% of respondents. Multi-cloud has evolved from an experiment to a strategic concern, while enforcing consistent security and ensuring reliable performance are still challenging for most organizations.

02 69% of respondents are executing digital transformation–and app data reigns.

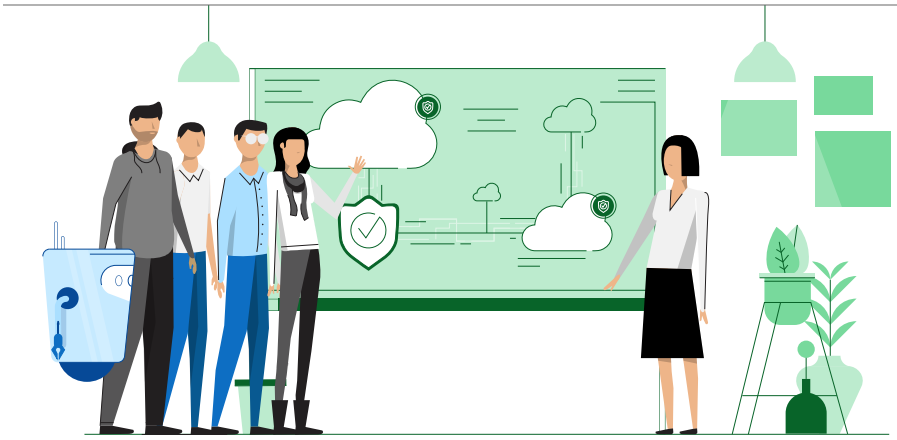
With more than two-thirds of survey respondents engaged in ongoing digital transformation initiatives, IT organizations are re-evaluating their structures, processes, and workflows to be more agile. As enterprises migrate applications to the cloud—and with them application data—the importance of data analysis and real-time threat analytics are emerging.

03 56% of respondents are employing containers; gateways, app security, and availability are growing in importance

The top application services currently deployed continue to be antivirus, network firewall, SSL VPN, and load balancing, but the list of services that respondents are planning to deploy includes some newcomers. The rise of containers has boosted deployment plans for SDN and API gateways, as well as service mesh, while respondents also report deploying some newly developed cloud-native app services to increase scalability.

04 62% of respondents are deploying automation and orchestration initiatives–and developer-oriented solutions are leading the charge.

Automating and orchestrating development and deployment pipelines helps organizations keep up with the rapid rate of change required for applications. With silos breaking down and cross-functional teams speeding innovation, organizations are standardizing on developer-oriented solutions to implement CI/CD practices throughout IT.



KEY FINDING 01

87% of respondents have multi-cloud architectures, driven by an app-first methodology.

Most organizations evaluate cloud decisions based on what environment is best for each application, an app-first methodology that leads to multi-cloud architectures for nearly 90% of respondents. While multi-cloud has evolved from an experiment to a key strategy, enforcing consistent security and ensuring reliable performance remain challenging for most organizations.

MULTI-CLOUD EVOLVES FROM EXPERIMENT TO STRATEGY

For most organizations, the adoption of multiple clouds has moved beyond the experimentation stages to become a deliberate strategy. A clear majority (87%) of respondents reported that they operate in a multi-cloud environment—and do so to drive business growth by reaping the benefits of public cloud platforms and associated technologies such as artificial intelligence and developer ecosystems.

Leading IT organizations understand that they need to assess each layer of their IT stack for standardization, scale, competitive advantage, and costs. In this assessment, they are choosing the application as the highest priority—underscoring the importance of a multi-cloud strategy. Respondents select their cloud platforms and locations by the types of applications (47%), by the intended end users of the applications (44%), and on an individual, case-by-case basis (44%).

All three considerations highlight the primacy of the application itself and the need to choose the best solution for each app. In some cases, the need to realize the benefits of collective, continuous innovation may lead to choosing a SaaS offering; in others, the opportunity to drive customer engagement at a global scale will lead to choosing a vertically integrated PaaS. In fact, nearly three out of four (71%) organizations reported that they are utilizing multiple cloud providers for IaaS and PaaS.

WITH CLOUD ADOPTION CONTINUING TO GROW, IT HAS A SEAT AT THE DIGITAL TABLE.

Treating each individual app as a unique asset while creating a unifying strategy is the role of the CIO and their organization. We find that IT helps guide this strategy, with 42% of respondents reporting that IT determines which type of cloud is best for each app. The role of IT in unifying application services, policy, and visibility is critical to the digital health and success of the organization.

WE ASKED

"How does your organization decide which type of cloud is best for each application? Select all that apply."

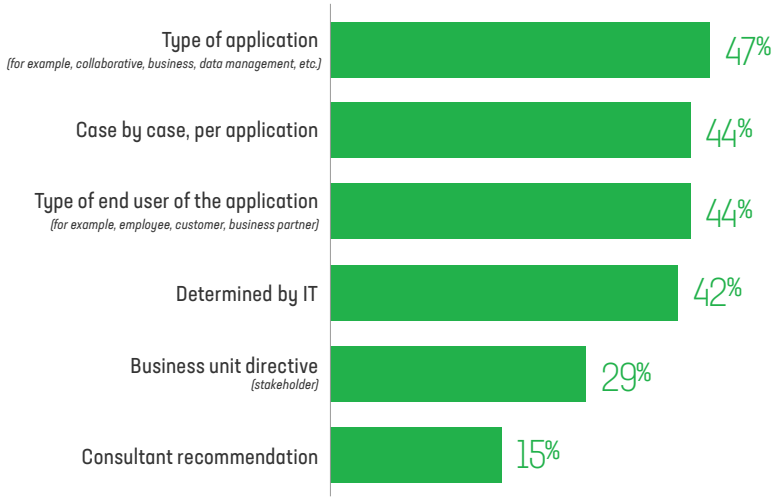


FIGURE 01: BEST CLOUD FOR THE APP

As has been the case for several years, cloud adoption continues to rise. Figure 2 illustrates the multiple types of clouds in use today, as well as those planned to be used in the next 12 months. With the exception of on-premises private cloud and colocation data centers, all cloud categories will see increases.

WE ASKED

"What types of clouds are you using now? What types do you plan to use in the next 12 months?"

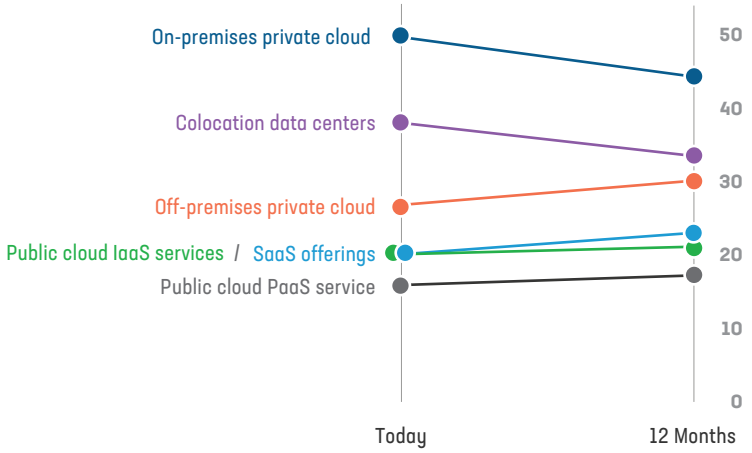


FIGURE 02: TRENDS IN CLOUD USAGE

SECURITY IS STILL A CHALLENGE FOR MULTI-CLOUD DEPLOYMENTS

The core challenge associated with these multi-cloud architectures remains enforcing consistent security across all applications. Nearly half of organizations (48%) with a digital transformation initiative are troubled by the difficulty of achieving consistent security for applications distributed among multiple cloud platforms.

Optimizing performance and gaining visibility into application health also remain high on the list of challenges. Even among those organizations without a digital transformation intiative, visibility and performance optimization were cited as top concerns with multi-cloud. All three challenges are real—particularly that of security, which displays its impact in the confidence organizations have in withstanding an application-layer attack.

WE ASKED

"As you think about managing applications in a multi-cloud environment (private, public, or SaaS), what part of managing the application do you find the most challenging, frustrating, or difficult? Select all that apply."

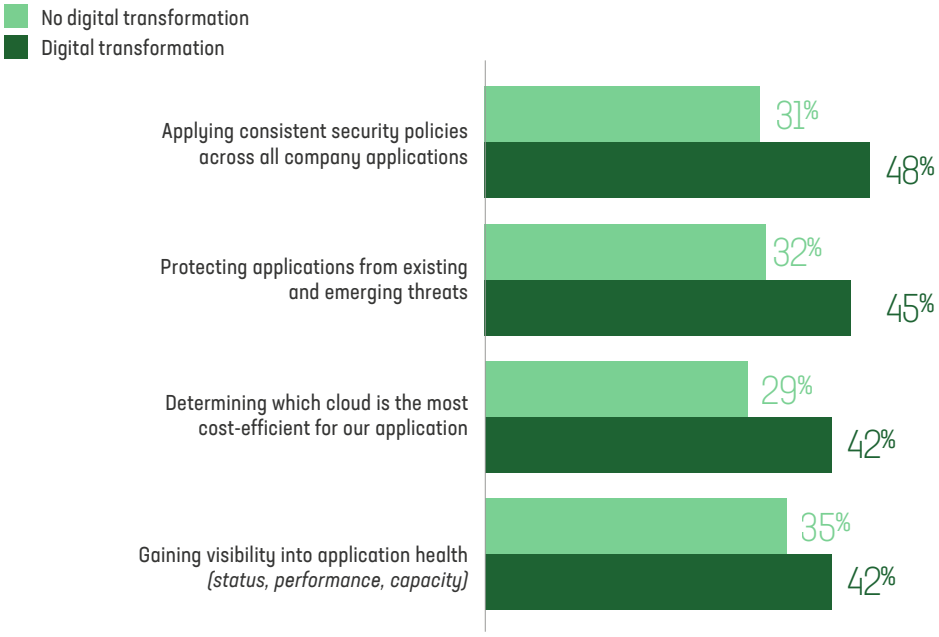


FIGURE 03: MULTI-CLOUD CHALLENGES

Overall, one in five (20%) respondents are not confident about their ability to withstand an application-layer attack this year, which is up 3 percentage points over 2018. As was the case last year, confidence rises with proximity to the app, with more than half (53%) more confident about protecting applications on premises than off premises in the public cloud (38%).

Confidence has fallen despite an increase in the use of application protection services over the past year. This year, 16% of organizations use at least one method of protection and 5% use six different services compared to 14% and 3%, respectively, in 2018. Increases were also seen in the use of cloud access security brokers (14% to 18%) and runtime application self-protection (11% to 16%), as well as a big jump in WAF usage (57% to 64%).

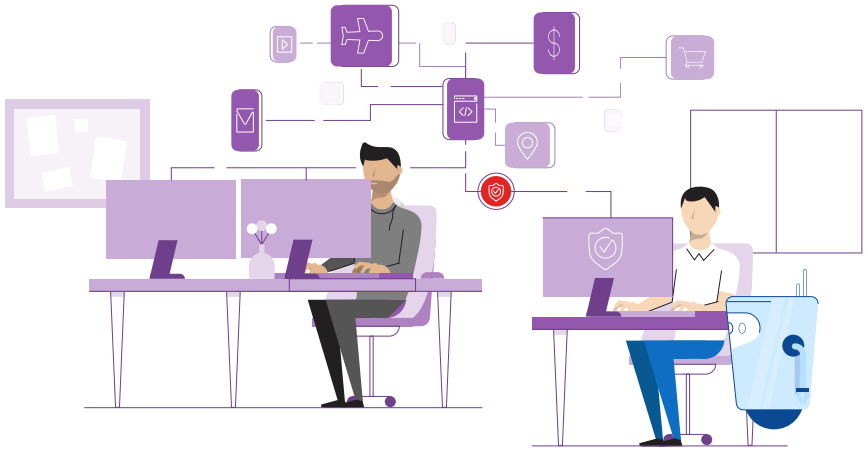
NETWORK FIREWALLS DON'T PROVIDE ADEQUATE APP-LAYER PROTECTION

Despite this increase in WAF deployments, 8% of organizations use only a network firewall to protect their applications—regardless of deployment location. That's distressing, and it's certainly a contributing factor to flagging confidence. The only environment in which users of network firewalls felt highly confident was on premises. In every other environment, the use of network firewalls did not seem to contribute to confidence at the application layer. This makes a great deal of sense. Network firewalls do not provide adequate protection against application-layer DDoS or infiltration attempts, nor can they detect or prevent credential stuffing attacks or probing attacks from bad bots, which have both increased dramatically in frequency over the past year.

Users of other application- and user-aware defenses—such as WAF, behavioral analytics, and application access control—were more confident they could withstand an app-layer attack in every environment.

F5 INSIGHTS FOR KEY FINDING 01

While public cloud adoption continues to rise, the disparity in application services deployments across environments contributes to the challenge of providing consistent security for the majority of multi-cloud organizations. The ability to enforce similar policy is enabled by the use of similar application services, which suggests that organizations would be well-served by standardization upon a common set of application services across all cloud environments.



KEY FINDING 02

69% of respondents are executing digital transformation—and app data reigns.

With more than two-thirds of survey respondents engaged in ongoing digital transformation initiatives, IT organizations are re-evaluating their structures, processes, and workflows to be more agile. As enterprises migrate applications to the cloud—and with them application data—the importance of data analysis and real-time threat analytics are emerging.

THE DIGITAL ECONOMY: APPLICATIONS, ANALYTICS, AND MACHINE LEARNING

In the digital economy, applications are an organization's most valuable capital. Employees are unable to do their jobs without applications facilitating all aspects of product creation, manufacturing, and delivery. Apps are also key in creating the first impression an organization makes with its customers—and they boost value by connecting a global network of customers, partners, and suppliers. In short, the business is driven by applications and, in an increasing number of organizations, the application is the business itself.

This new digital economy is changing the entire landscape of applications. We asked respondents which strategic trends will be important over the next 2–5 years and their answers were clear: the future is all about analytics and machine learning. For the more than two-thirds (69%) of the organizations that have or plan to have digital transformation projects in place, the top five strategic trends are big data analytics (53%), IaaS (53%), SDN (47%), machine learning and artificial intelligence (43%), and real-time threat analytics (42%).

WE ASKED

"Which technology trends do you think will be strategically important for your organization in the next 2–5 years? Select all that apply."

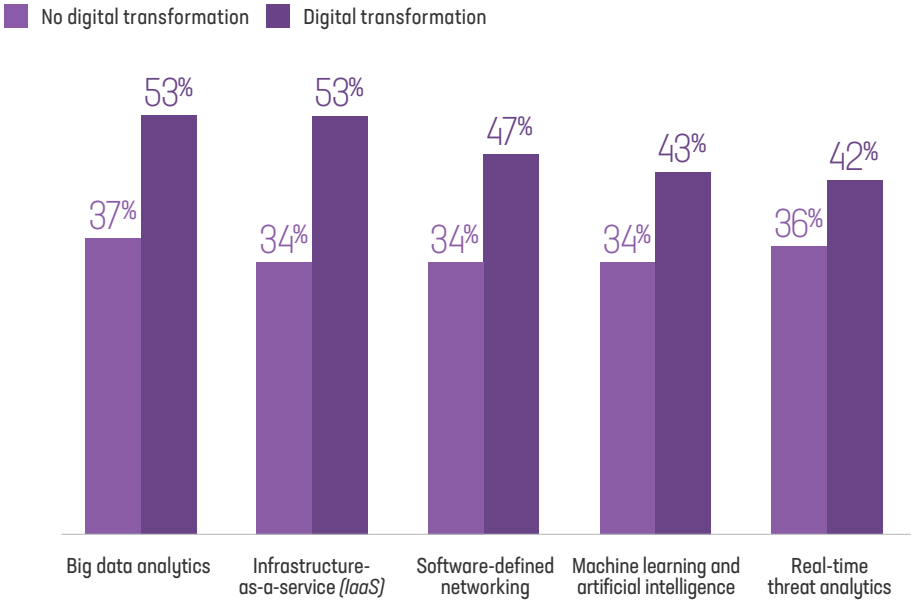


FIGURE 04: DIGITAL TRANSFORMATION DRIVING STRATEGIC TRENDS

ANALYTICS, CLOUD, AND SDN DRIVE IT OPTIMIZATION

These trends make sense. Similar to last year, the majority of organizations (69%) across every region and vertical ranked IT optimization as the number one benefit of digital transformation. The building blocks for IT optimization initiatives? You guessed it: analytics, smart cloud usage, and software-defined networking.

Next in line as the benefits of digital transformation were business process optimization (62%) and employee productivity improvements (57%), which means that the top three benefits of digital transformation this year are internal facing, neatly outpacing the external-facing benefits of competitive advantage (45%) and new business opportunities (45%). All indications are that IT organizations are studiously evaluating processes, workflows, and organizational structures to prepare for the onslaught of change to come.

WE ASKED

"What benefits do you want from your digital transformation projects? Choose all that apply."

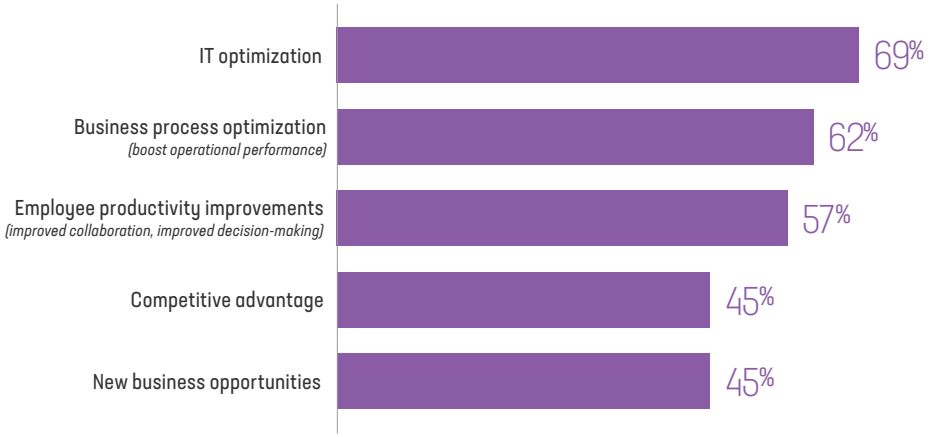


FIGURE 05: PRIMARY BENEFITS FROM DIGITAL TRANSFORMATION

NEW TEAM STRUCTURES SPEED TIME TO MARKET

To truly capitalize on digital transformation initiatives, leading organizations are finding they need to drive change in their organizational structures in addition to making new IT investments. Those organizations involved in digital transformation have transitioned away from siloed, single-function teams *(network, server, applications)* to either combined platform operations teams or collections of small, cross-functional infrastructure and operations (I&O) teams. These new team structures facilitate faster time to market and enable IT to collectively focus on the optimization initiatives that drive meaningful results for the business. These organizational structures are far more effective in providing key performance indicators that deliver insights to drive business performance and growth.

WE ASKED

"What is the structure of your IT team?"

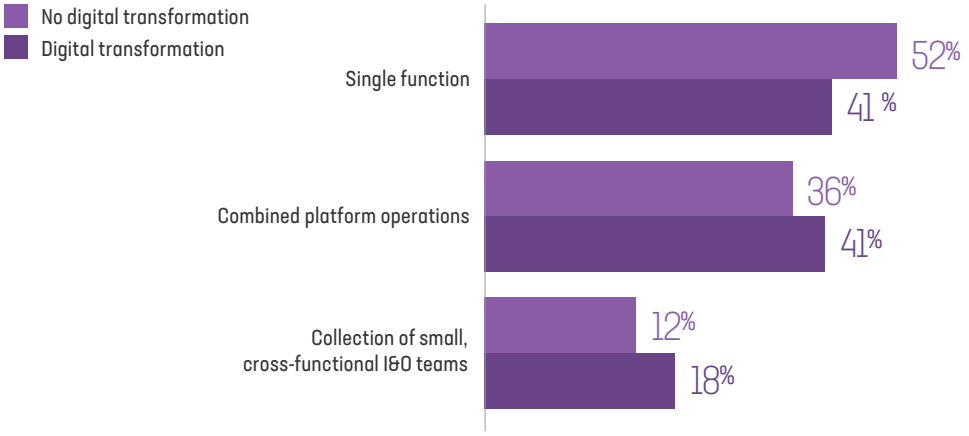


FIGURE 06: DIGITAL TRANSFORMATION DRIVING CHANGE IN IT ORGANIZATIONS

AUTOMATION AND ORCHESTRATION BECOME PARAMOUNT

Digital transformation influences every aspect of the application lifecycle—from development and delivery to deployment. As organizations look to transform, the need for automation and orchestration becomes ever more important, which is reflected in a 7% increase (from 55% to 62%) in the percentage of respondents who reported that they are implementing automation and orchestration this year. Organizations are taking advantage of agile development methodologies (52%) and increasing demand for more frequent delivery to production (48%), as well as exploring new application architectures such as containerization (42%). Taken together, these shifts all point to a changing application landscape which is automated, cloud-centric, and influenced by responsiveness to business priorities.

WE ASKED

"How is digital transformation influencing your application decisions? Select all that apply."

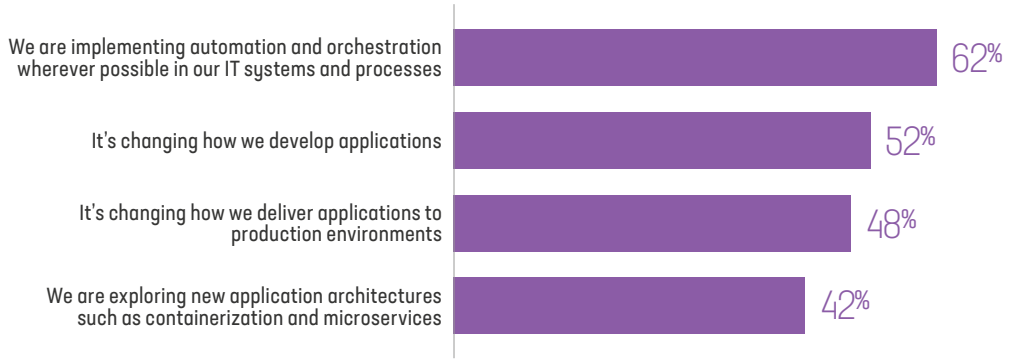


FIGURE 07: DIGITAL TRANSFORMATION INSPIRING CHANGE

F5 INSIGHTS FOR KEY FINDING 02

To prepare for the continued evolution of the digital economy, IT organizations are re-evaluating everything about how they deliver value to the enterprise. This year, the focus of digital transformation initiatives is analyzing and leveraging the monumental amount of data now available, while keeping that data safe through enhanced security and automation-based process improvement.

KEY FINDING 03

56% of respondents are employing containers; gateways, app security, and availability are growing in importance.

The top application services currently deployed continue to be antivirus, network firewall, SSL VPN, and load balancing, but the list of services that respondents are planning to deploy includes some newcomers. The rise of containers has boosted deployment plans for SDN and API gateways, as well as service mesh, while respondents also report deploying some newly developed cloud-native app services to increase scalability.

TOP APPLICATION SERVICES STAY CONSISTENT, WITH DDOS PROTECTION RISING

Over the past five years we've tracked the deployment of application services and noted that there is a consistent set that tops the charts every single year: antivirus, network firewall, SSL VPN, and load balancing.

WE ASKED

"For each of the application services below, please indicate your company's current deployment status."

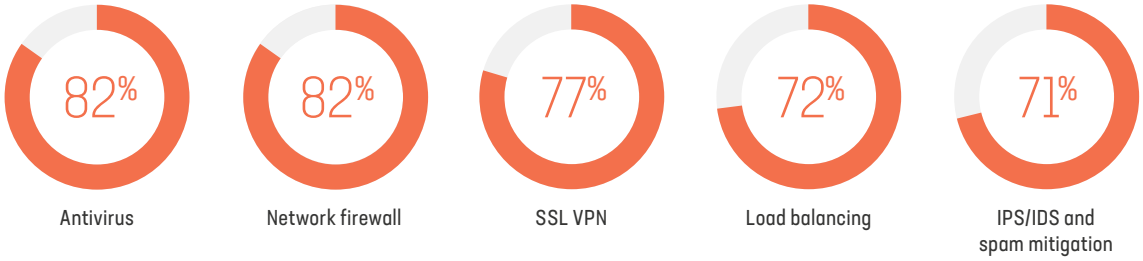


FIGURE 08: TOP FIVE APPLICATION SERVICES DEPLOYED TODAY

The remaining slot has been shared by spam mitigation, IPS/IDS, and, in 2017, DNS. There are few services that appear capable of unseating one of these power application services, but DDoS protection is a strong contender. While no other application service has seen increased deployment rates over the past five years, DDoS protection has risen from 53% in 2015 to an impressive 67% this year—enough to put it in the number six position and ready to challenge IPS/IDS and spam mitigation for their shared spot in the top five.

WE ASKED

"Please indicate whether you deploy DDoS protection."

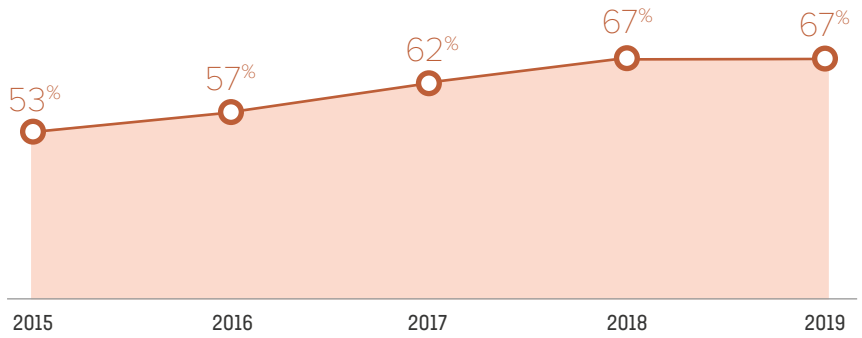


FIGURE 09: DDOS PROTECTION DEPLOYMENT RATES OVER FIVE YEARS

SECURITY AND IDENTITY ARE A BIGGER CONCERN FOR ORGS WITH A MAJORITY OF EXTERNAL-FACING APPS

It is unsurprising to note that the composition of an organization's app portfolio mix has an impact on the application services they have deployed. Organizations with more than 50% of their portfolios made up of external-facing applications deploy security and identity services at higher rates. They also focus more on app services associated with availability, such as API gateways, global and local load balancing, and DNS.

Given that a significant percentage of those applications are targeted at consumers and customers, it is understandable that these organizations are concerned about availability. However, business focus ignores the growing importance of productivity—usually achieved through the use of internal-facing apps—as a component of corporate financial health. Productivity and profit share the stage in determining corporate success, as productivity can have a profound impact on the bottom line. A decrease in productivity can negate gains in profit, and thus all organizations should be attentive to availability of all applications—the external-facing apps that serve customers and the internal-facing apps that empower employees.

WE ASKED

"For each of the application services below, please indicate your company's current deployment status"

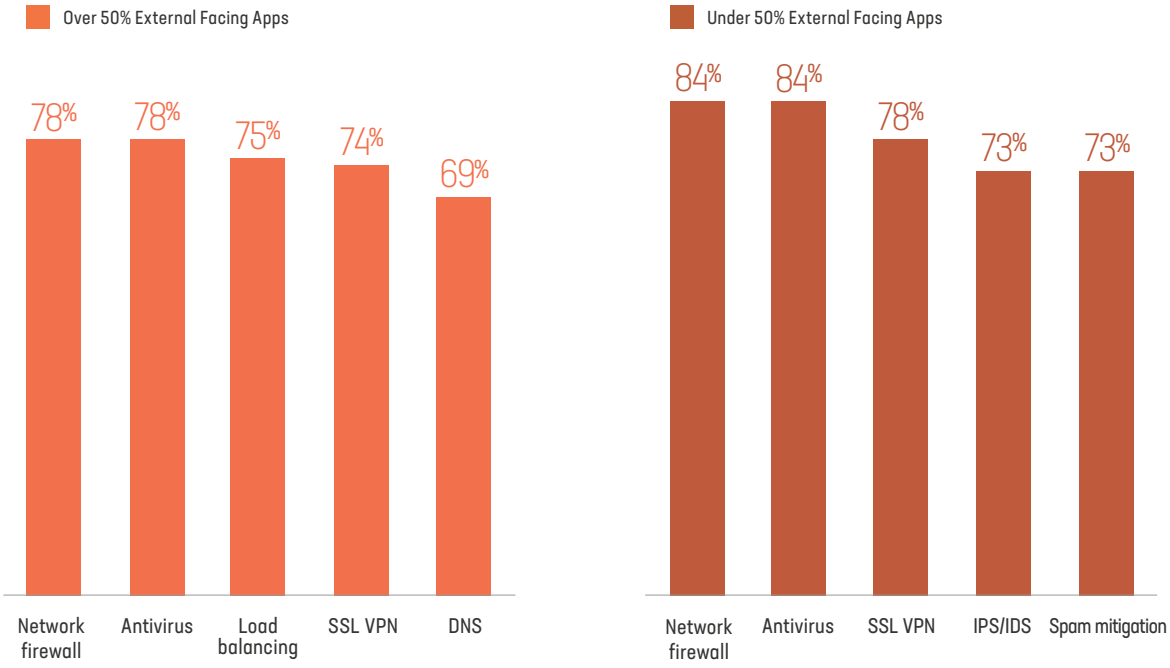


FIGURE 10: SECURITY AND IDENTITY ARE A BIGGER CONCERN FOR ORGS WITH A MAJORITY OF EXTERNAL-FACING APPS

Organizations with a portfolio composed of 50%+ external-facing applications are slightly more concerned about deploying applications without identity, mobility, and performance services than their counterparts with a portfolio made up of less than 50% external-facing apps. Both groups agree with the global results, however, that the worst thing they could do is deploy an application without security services. And regardless of app portfolio mix, antivirus and network firewall are at the top of the application services list and both groups deploy SSL VPN at significant rates.

While the top five application services deployed today remain fairly static, the top five to be deployed have shifted over the years along with strategic trends. Last year, we saw digital transformation influencing planned deployments, and this year that trend continues. Digital transformation still drives interest in and deployments of microservices and containers, and the impact can be seen in the application services that organizations plan to deploy in the next twelve months.

WHAT THE RISE OF CONTAINERS MEANS FOR SDN GATEWAY DEPLOYMENTS

Containers aren't coming to a data center near you—they're already here. More than half of respondents (56%) are employing containers today. Most of those are thanks to digital transformation initiatives, which drive the adoption of nascent and emerging technologies at impressive rates.

WE ASKED

"Have you adopted containers or do you plan to do it in the next 12 months?"

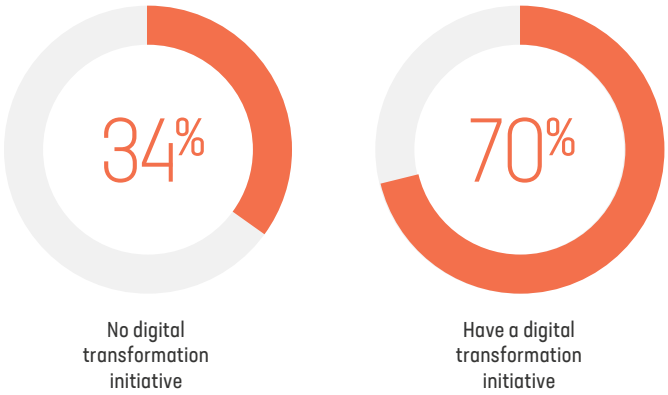


FIGURE 11: DIGITAL TRANSFORMATION DRIVING CONTAINER ADOPTION

The rise of containers is having an impact on application services, particularly in the area of availability. This is our first report including Ingress control (HTTP routing) as an application service—and it is already widely deployed. Nearly half (47%) of respondents have deployed Ingress control and another 23% plan to deploy it within the next twelve months. It's on track to match deployment rates of load balancing, which have remained fairly static at around 70% for the past five years.

The rapid and robust adoption of containers is also a significant factor in the rise of SDN gateways to near the top of the list of application services that will be deployed in the next year. In fact, while 56% of respondents globally are deploying containers, that rate rises to 72% for those that have deployed or plan to deploy an SDN gateway. This makes sense as Ingress controllers are used to route application traffic to containerized environments, and those environments increasingly rely on network overlay protocols like NVGRE and VXLAN—both of which are core capabilities of an SDN gateway solution. It is reasonable, then, to view the increasing strategic importance of SDN gateway services (at 31%, they come in at the top of the list of planned deployments for 2019) as an indicator of growing container deployments.

WE ASKED

"Which of the following application services do you plan to deploy in 2019?"

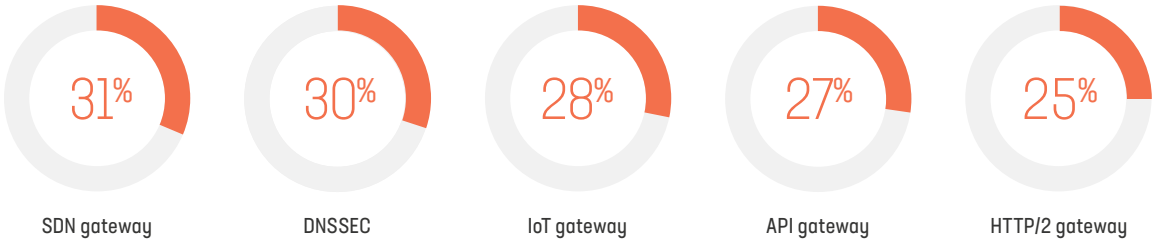


FIGURE 12: THE TOP FIVE APPLICATION SERVICES PLANNED FOR DEPLOYMENT IN 2019

The rise of containers can also be seen in responses stating preferences for application services form factors on premises. Over the past three years we've seen "containers" as a preferred form factor rise from 6% in 2017 to 9% in 2018 to 14% this year. Interestingly, this gain appears to be coming from a decline in desire for virtual appliances, which dropped to 26% this year from 30% in 2018. This trend is most likely propelled by multi-cloud adoption as containerized apps are viewed as being more portable across environments. Organizations also often cite management overhead as a factor driving the migration from virtual machines to containers.

DISPARITY BETWEEN ON-PREMISES AND PUBLIC CLOUD APP SERVICES DEPLOYMENTS LEADS TO SECURITY CONCERNS

This year, we explicitly asked about application services deployments in public cloud environments (IaaS). While the average number of application services in use overall is 14, that drops by half for public cloud deployments. This means that organizations are deploying apps in the public cloud, but they are not matching application services deployments at the same rate. Given the importance of application services in securing and scaling applications, this disparity is certainly an issue that bears further scrutiny.

This difference between on-premises and public cloud deployments may shed light on why organizations cite security as the top challenge with multi-cloud deployments. While 66% of respondents deploy a WAF, only 33% indicate that they use a WAF for production applications deployed in a public cloud. Other security-related application services suffer the same decline in use in the public cloud, which is troubling, because it is nearly impossible to achieve security policy parity without the application services that enforce it.

Almost every security and identity/access management-related application service has less than 33% adoption for production applications in the public cloud. Organizations' flagging confidence in their ability to withstand an application-layer attack against applications in the cloud makes these deployment rates confounding. Access control, botnet protection, DDoS protection, and WAF offer protection against a wide variety of application-layer attacks. The difference in confidence rates based on deployment of these foundational security services is dramatic. Those with high confidence in withstanding application-layer attacks targeting applications in the public cloud deployed these services at much higher rates than those with low confidence.

WE ASKED

"How confident are you in your ability to withstand an application-layer attack based on deploying the following app services in the public cloud?"

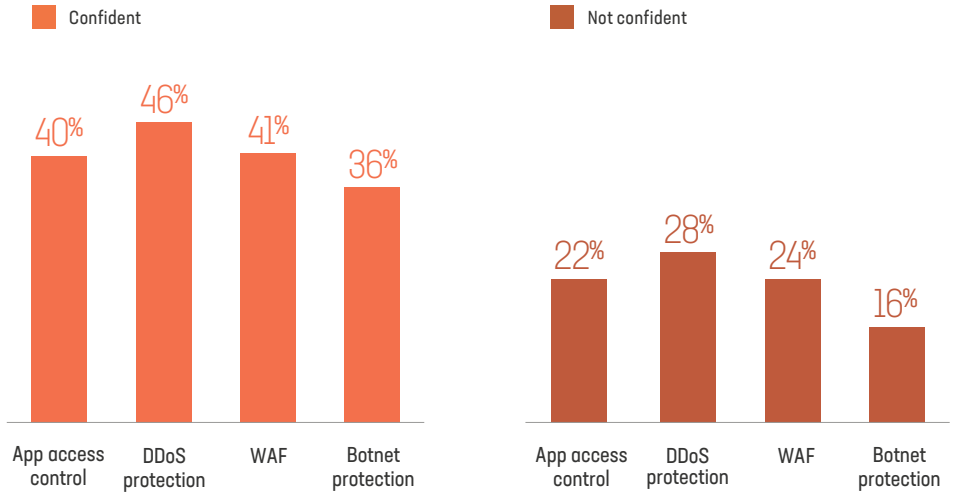


FIGURE 13: CONFIDENCE TO WITHSTAND AN APPLICATION-LAYER ATTACK BASED ON DEPLOYMENT OF KEY APP PROTECTION SERVICES IN THE PUBLIC CLOUD

ORGANIZATIONS ADOPT CLOUD-NATIVE APPLICATION SERVICES TO SUPPORT AVAILABILITY

In recent years, IaaS providers have developed a crop of cloud-native application services that focus primarily on scale and some forms of security. These services are enjoying respectable rates of adoption, with availability and SDN gateways leading the way. Cloud-native application availability services—encompassing both global and local load balancing—have been adopted by 58% of respondents. SDN and API gateways are close behind, with 47% and 42% respectively.

Of particular note is the adoption of service mesh, which is already being deployed by 27% of respondents. While that lags behind container adoption in general, we expect to see rates rise in both public cloud and overall as the technology matures.

F5 INSIGHTS FOR KEY FINDING 03

While cloud-native services provide some support for availability, the lack of consistent security application services deployment in the public cloud has caused many organizations to feel less than confident about their ability to withstand an application-layer attack. For on-premises deployments, containers continue to rise in importance, leading to the increased adoption of Ingress control and SDN gateway services to support containerized environments.

KEY FINDING 04

62% of respondents are deploying automation and orchestration initiatives—and developer-oriented solutions are leading the charge.

Automating and orchestrating development and deployment pipelines helps organizations keep up with the rapid rate of change required for applications. With silos breaking down and cross-functional teams speeding innovation, organizations are standardizing on developer-oriented solutions to implement CI/CD practices throughout IT.

AUTOMATION AND ORCHESTRATION HELP ORGANIZATIONS GET AHEAD

As a result of cloud and container disruptions, automation and orchestration grow in importance as essential components of digital transformation initiatives. Last year, 55% of respondents employed automation and orchestration as a direct result of digital transformation efforts. This year, it's 62%.

It is worth noting that—according to survey respondents—DevOps has never attained real strategic importance. It peaked in 2018 with 25% reporting it as a strategic concern, but lost its momentum, falling to a mere 14% this year. Even among those operating under a digital transformation initiative, CI/CD and DevOps could only manage 19%. This is not all that surprising, as strategic impact often implies competitive advantage. It seems that the automation and orchestration of development and deployment pipelines associated with DevOps is no longer about getting ahead—it's merely about keeping up.

The good news is that organizations are not only starting to keep up, but some are really moving forward. More than one-third have automated all four key components of the production pipeline:

WE ASKED

"Which of the following four key components of the production pipeline have you automated?"

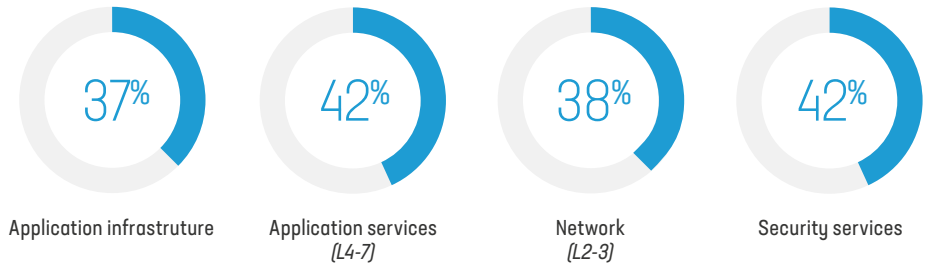


FIGURE 14: PERCENTAGE OF ORGANIZATIONS AUTOMATING COMPONENTS OF THE PRODUCTION PIPELINE

While a solid 35% are piloting or in production with self-service provisioning outside of IT, this number jumps to 46% for those organizations operating under a digital transformation initiative.

These numbers are highly influenced by the composition of applications being supported. Those with portfolios composed of more than 50% external-facing (customer, partner, consumer) applications exhibit higher adoption rates of automation across all four pipeline domains. Organizations understand that the rate of change required for external-facing applications can best be maintained with an automated deployment process.

Another factor in pipeline automation implementation is the structure of IT teams. More modern, DevOps-influenced, cross-functional teams and combined operational teams automate and orchestrate at a much faster pace than traditional, single-function teams. However, despite the rise of automation and orchestration, some challenges remain in automating the network, including a lack of skills, the difficulty of creating policies and governance, and having sufficient budget to implement new tools.

WE ASKED

"What do you find most frustrating or challenging about automating the network?"

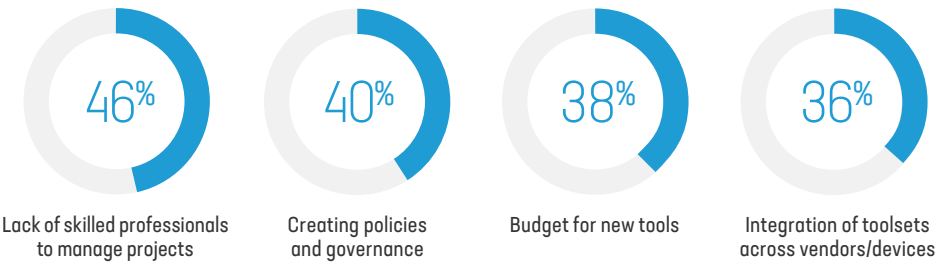


FIGURE 15: NETWORK AUTOMATION CHALLENGES

ORGANIZATIONS LEVERAGE DEVELOPER-ORIENTED SOLUTIONS TO AUTOMATE THE NETWORK

This lack of skills and an increasingly cross-functional/integrated IT organization are likely the primary factors influencing a shift away from network-centric automation tools toward developer-oriented solutions. In addition, many of the early traditional network automation offerings are unable to extend beyond simply managing devices and often leave holes that organizations need to fill with more comprehensive solutions for implementing their toolchains.

The maturity of existing solutions like GitHub Enterprise and Jenkins allows organizations to efficiently fill these holes and address the issue of skill scarcity in IT. Even if the market offers a viable network and infrastructure-focused alternative, we expect that the benefits of standardization on existing tools across an organization are likely to outweigh the appeal of such an offering.

WE ASKED

"Which of the following toolsets do you use or plan to use in the next 12 months to automate the network?"

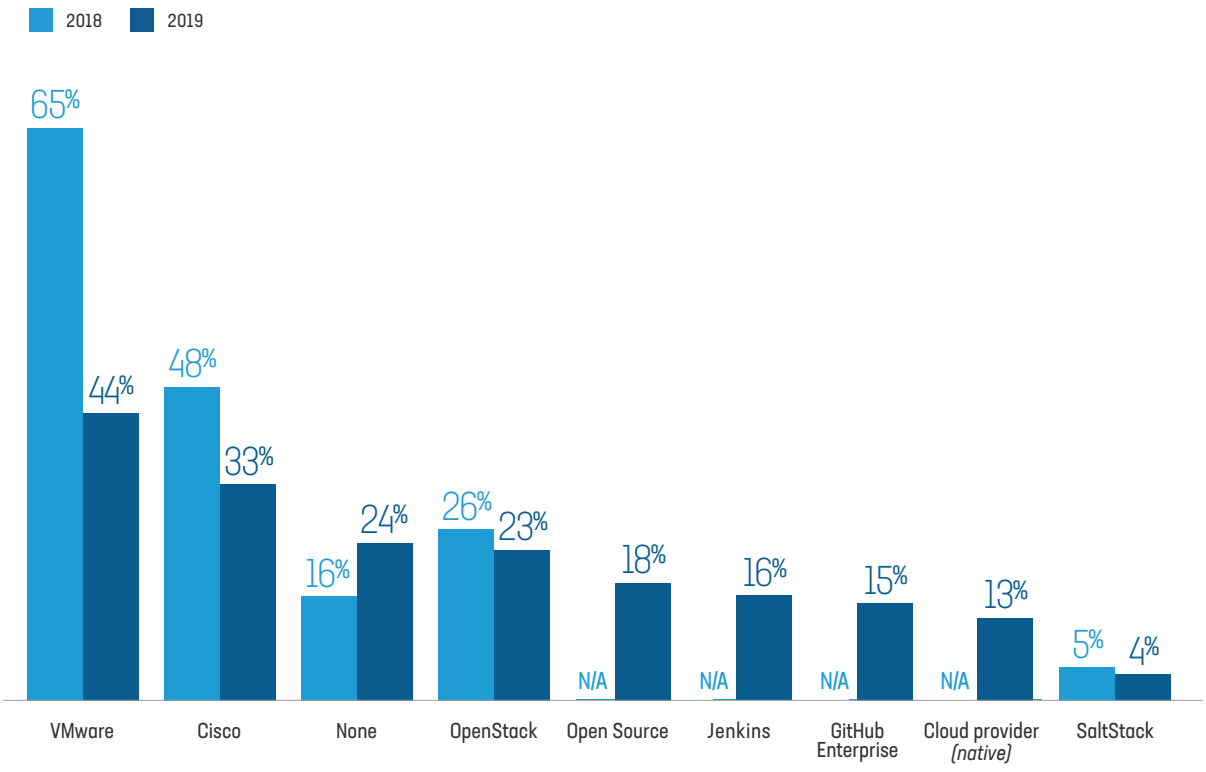


FIGURE 16: TOOLSETS TO AUTOMATE THE NETWORK

DEVOPS DRIVES NETOPS TO STANDARDIZE ON THEIR AUTOMATION TOOLS

With automation and orchestration being so important to the success of the enterprise, the pressure is on NetOps to deliver self-service provisioning and adopt configuration- and infrastructure-as-code methodologies. We are seeing DevOps drive NetOps toward those tools and team structures that have served to automate and orchestrate continuous delivery efforts. With a dearth of talent and a lack of skills, organizations will continue to look internally—to DevOps and developers—to realize the fully automated infrastructure pipelines necessary to satisfy business demands to deliver faster and more frequently.

This becomes evident when we glance at tool preferences by role. In network automation, VMware takes the crown—except where networking professionals and service reliability engineers are concerned. For them, it's Cisco and GitHub/Jenkins, respectively, that top their go-to list of network automation tools.

However, that's where the similarities end. Those in cloud-related roles and operations professionals agree: Cisco is second and OpenStack is third. Not a single SRE uses Cisco, and they also tend to avoid cloud-provider native toolsets, preferring OpenStack and open source as well as VMware to native offerings.

WE ASKED

"Which toolset do you prefer to use for network automation?"

	Cloud	Developer	Network	Operations	Security	Executive	SRE/DevOps
Cisco	44%	19%	56%	50%	40%	38%	
Cloud provider (native)	32%	19%	11%	9%	17%	27%	11%
Github Enterprise	24%	33%	13%	13%	19%	25%	56%
Jenkins	36%	43%	18%	14%	26%	18%	56%
Open source	8%	19%	23%	26%	27%	24%	44%
OpenStack	40%	38%	25%	29%	31%	32%	44%
SaltStack		10%	3%	1%	7%	9%	
VMware	72%	48%	55%	63%	55%	60%	44%

FIGURE 17: PREFERRED NETWORK AUTOMATION TOOLS BY ROLE

PYTHON RULES SUPREME

The one thing everyone agrees on—regardless of role or team structure or industry—is that Python is the go-to tool when it comes to overall automation and orchestration. It has occupied the top spot in every iteration of this survey, and we expect it to remain the favorite for the foreseeable future.

F5 INSIGHTS FOR KEY FINDING 04

For those engaged in automation and orchestration across a variety of roles, Python remains the scripting language of choice. In fact, the use of developer-oriented tools is spreading into the traditional domains of network automation solutions like those provided by VMware and Cisco. As automation and orchestration of the entire production pipeline becomes more and more important, organizations look to developers and DevOps groups to lead the way in standardizing on tools and team structures that enable faster development, deployment, and delivery of applications.

Conclusion

In some respects, the perception of application services as a critical component of success has come full circle since we started this report five years ago. When cloud and associated technologies such as software-defined infrastructure burst onto the scene—with the promise of solving the cost and agility challenges of IT operations—application services were relegated to the sidelines. Fast forward to today when multi-cloud has shifted from an experiment to a comprehensive strategy for innovation. In this application economy, app services have reclaimed their status as a key player in digital transformation and business success.

Organizations regard application services as vital for cloud and the full range of digital economy enablers to succeed. We see emerging application services such as Ingress control and IoT gateways skyrocketing from initial deployments into production. These new application services—in concert with existing services such as firewalls and global server load balancing—are adapting to the new platforms and requirements of our multi-cloud world.

As digital transformation continues to change the landscape, deploying consistent application services enables organizations to keep pace and thrive. By maintaining uniform policies, security, and availability across their entire portfolio of applications, organizations can best optimize their application capital—and continue to grow their business.

LEARN MORE

For more information about how application services can help your organization unlock the value of application capital, visit f5.com.

US Headquarters: 401 Elliott Ave W, Seattle, WA 98119 | 888-882-4447 // Americas: info@f5.com // Asia-Pacific: apacinfo@f5.com // Europe/Middle East/Africa: emeainfo@f5.com // Japan: f5j-info@f5.com