2018 REPORT

# The State of Application Delivery

LOAD BALANCING
GLOBAL SERVER LOAD BALANCING
DNS
DDOS PROTECTION/MITIGATION
WEB APP FIREWALL
APPLICATION ACCELERATION

ANTI-VIRUS
ANTI-FRAUD
ANTI-SPAM
DNSSEC
NETWORK FIREWALL
SSL VPN

IDENTITY FEDERATION
APPLICATION ACCESS CONTROL
SECURE WEB GATEWAY SERVICE
SINGLE SIGN-ON
COMPRESSION
CACHING

TCP OPTIMIZATION
WAN OPTIMIZATION
ENDPOINT SECURITY
API GATEWAY
SDN GATEWAY
IOT GATEWAY

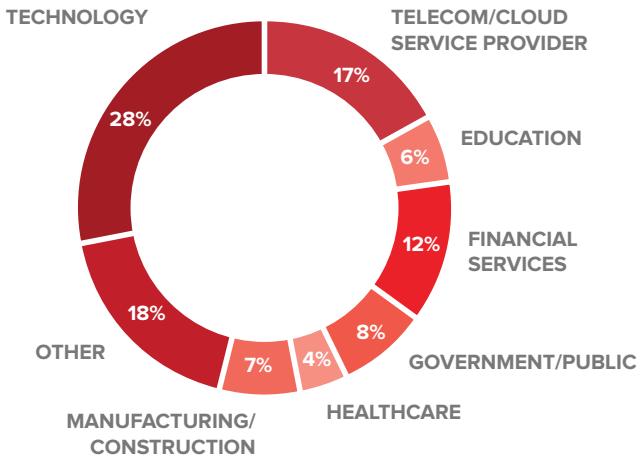
# What's Inside

# 2018 Survey Demographics

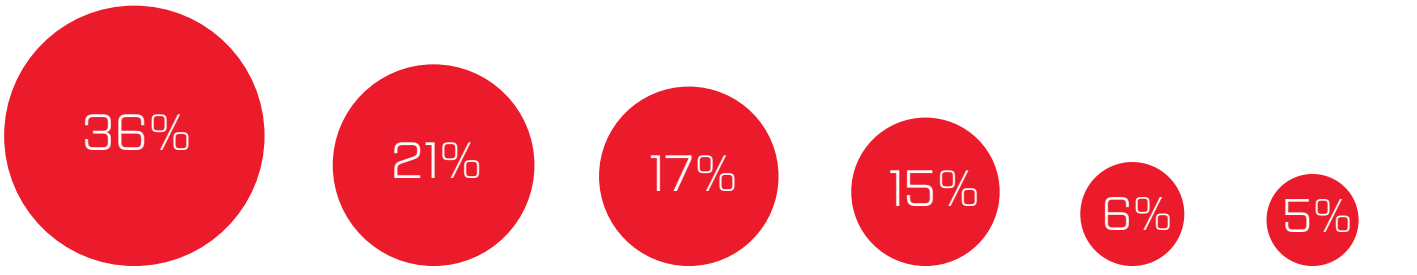
3,460

TOTAL NUMBER OF RESPONDENTS

## Industry




## Respondent role




**NETWORK**
Manager, Engineer, Architect

**OPERATIONS**
Engineer/Manager

**SECURITY**
Manager, Engineer, Architect

**EXECUTIVE**
C-level, IT Director/VP

**CLOUD**

**APP DEVELOPER/ DEVOPS**

# Introduction

With digital transformation reshaping the modern enterprise, applications represent a new class of assets and an important source of differentiation. The ever-more-competitive digital economy requires that your applications be delivered with unprecedented speed, scale, and agility, which is why more and more organizations are turning to the cloud.

This explosive growth of apps hosted in the cloud creates a world of opportunities—and a whole new set of challenges for organizations that must now deploy and manage a vast portfolio of applications in multi-cloud environments. Automation and orchestration systems can help streamline and standardize IT processes across traditional data centers, private clouds, and public clouds. But with rapid innovation come concerns about security and delivering a consistent experience across environments.

Enter application services, which can help organizations boost performance, maintain availability, improve network and application security, and gain visibility into the behavior and health of their apps wherever they are deployed. In this dynamic technology ecosystem, the only law is change. As a result, the types of application services, the way they are deployed, and the environments they serve are constantly evolving.

In this, our fourth year, the State of Application Delivery report continues our journey to understand customer motivations underlying the deployment of application services. We explore current business imperatives and how they are shaping the decisions IT is making—including the location of the application itself, the security required to protect it from a variety of threats, and the benefits that come from automating tasks. We surveyed over 3,000 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 our world.

This year's research revealed five key findings that, taken together, represent a detailed picture of the global application delivery landscape today. Here's an inside look at the State of Application Delivery in 2018.

**4 out of the top 5 application services currently deployed are security services.**

# 2018 Key Findings

01

## Digital transformation inspires new architectures and IT optimization initiatives.

Optimizing IT infrastructure and processes remains the primary driver for digital transformation projects. Cloud adoption and automation provide the speed, space, and scalability required by organizations.

02

## Multi-cloud enables the “best cloud for the app” strategy.

Most organizations pursue a best-of-breed strategy for each application deployment, leading to multi-cloud architectures. Nonetheless, IT organizations are still required to provide their distributed application portfolio with ubiquitous security and performance—no matter where each app resides.

03

## Application services are the gateways to the future.

On average, organizations take advantage of 16 different application services to keep their apps fast, safe, and available. Security is still the most important application service, but application gateway services emerged as key services to be deployed in the next 12 months.

04

## Security confidence falls as multi-cloud rises.

Digital transformation drives organizations to deliver more apps from the cloud, yet organizational confidence to withstand an attack has taken a hit due to lack of experience and expertise in securing applications deployed in public clouds. Organizations that deployed web application firewalls (WAFs) were most confident in their security—both in public and private clouds.

05

## Automation and orchestration: Full steam ahead.

IT is embracing programmability—and is standardizing their automation and orchestration environments—to realize leaner IT with the goal of reducing OpEx. The use of containers ticks up as organizations seek faster, smarter scale through new application architectures and deployment models.

KEY FINDING

01

# Digital transformation inspires new architectures and IT optimization initiatives.

The digital economy is reshaping every industry across the globe, from the small business now accepting mobile payments to the Global 2000 incorporating transformative technologies such as robotics and virtual reality. CIOs not only have a front-row seat to the ramifications of a spectrum of business processes and strategies—they are the driving force of change in the organizations they serve. As with any structure, system, or process, the foundation needs to be solid to facilitate long-term success, and CIOs are building that foundation with digital transformation initiatives.

## IT Optimization Primary Benefit from Digital Transformation

72%
**IT OPTIMIZATION**

56%
**COMPETITIVE ADVANTAGE**

49%
**BUSINESS PROCESS OPTIMIZATION**

48%
**EMPLOYEE PRODUCTIVITY IMPROVEMENTS**

## Digital transformation mandates—and drives—IT optimization

IT optimization provides the foundation of digital transformation initiatives, and is also viewed as the primary benefit according to 72% of respondents. Optimizing IT processes was the leading response in every region, for every vertical, and at the executive level. Competitive advantage came in second, and is viewed as a benefit by 56% of the organizations, as innovative new applications utilizing data analytics support customer interaction and the ability to respond quickly to changing business requirements. Business process optimization (49%) and employee productivity improvements (48%) rounded out the top four. Interestingly, verticals that tend to have higher customer interaction—such as financial services, education, and healthcare—ranked employee productivity improvements ahead of business process optimization, likely because employees are on the front line of customer satisfaction. The Americas and Asia Pacific agreed with the results on the top four benefits. However, EMEA reported a slightly stronger desire to support new business opportunities (47%), bumping employee productivity improvements (45%) to the number five spot.

## Digital Transformation Inspiring Change

**55%**

**WE ARE AUTOMATING AND ORCHESTRATING IT SYSTEMS AND PROCESSES**

**49%**

**WE ARE DELIVERING OUR APPLICATIONS FROM THE CLOUD**

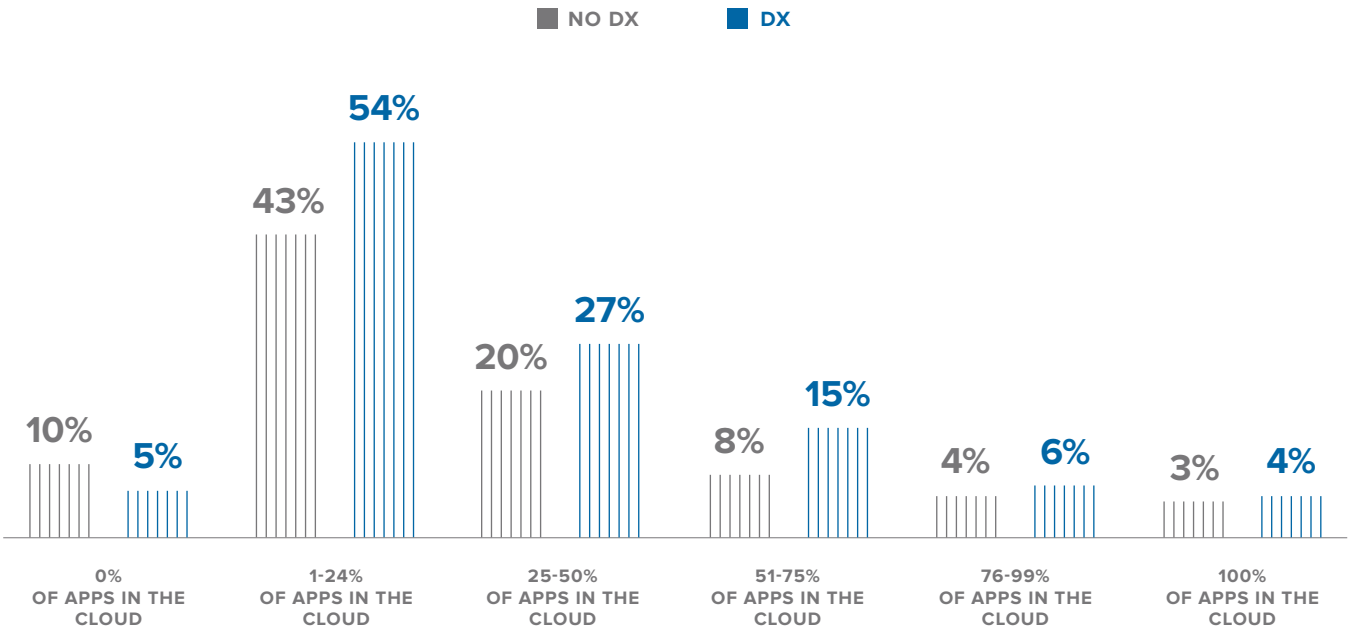
**47%**

**WE ARE CHANGING HOW WE DEVELOP APPLICATIONS**

**41%**

**WE ARE EXPLORING NEW APPLICATION ARCHITECTURES SUCH AS CONTAINERIZATION AND MICROSERVICES**

## Digital Transformation Leading Cloud Adoption



# 41%

**Forty-one percent reported exploring new application architectures such as containers and microservices.**

## Automation, orchestration, and new development environments help speed IT optimization

Digital transformation is driving the need for automation and orchestration to IT systems and processes, according to 55% of the respondents. Digital transformation also holds profound implications for application architectures and environments. According to 49% of respondents, digital transformation is encouraging the delivery of applications from the cloud. Furthermore, 47% stated that it is changing how they develop applications, and 41% reported exploring new application architectures such as containers and microservices.

## Cloud facilitates needed speed, space, and scale

Organizations are relying on the cloud to deliver the agility necessary for digital transformation projects. A quarter (25%) of organizations with digital transformation projects in place have over 50% of their applications in the cloud compared to only 15% of organizations without digital transformation projects. When we look specifically at public cloud infrastructure, the trends are similar across application types—digital transformation companies report higher usage of public cloud infrastructure.

### F5 INSIGHTS FOR KEY FINDING 01

**Organizations of all sizes are adapting to the new digital economy through digital transformation projects. Optimizing IT infrastructure and processes, gaining a competitive advantage, and improving employee productivity are all driving these major shifts. As organizations evolve, they look to the cloud to provide the flexibility necessary to succeed in an increasingly crowded marketplace.**

KEY FINDING

02

## Multi-cloud enables the “best cloud for the app” strategy.

As cloud platforms continue to evolve and offer more robust services, organizations find themselves selecting the cloud platform that is best for each application or category of applications. While prioritizing based on the most appropriate features for an application offers best-in-class business value, it also increases the challenges for IT organizations of maintaining security and delivering a positive customer experience.

## Best Cloud for the App

**CASE BY CASE, PER APPLICATION**

56%

**DETERMINED BY IT**

30%

**TYPE OF END USER OF THE APPLICATION**

26%


**TYPE OF APPLICATION**

25%

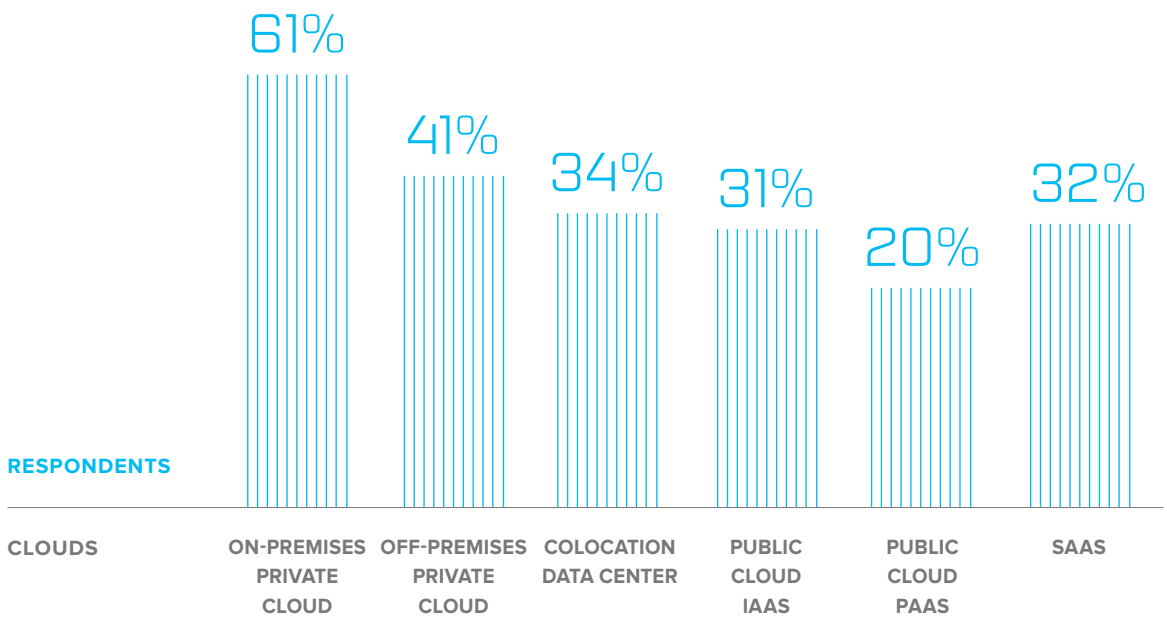
**BUSINESS UNIT DIRECTIVE**

22%

## App-centric business necessitates multi-cloud architectures

Applications streamline processes, provide new services and offerings, and enhance customer experiences—they're the core of the business. With the application itself paramount, IT decisions get made based on app requirements. At the same time, the speed and scale required from the digital economy is moving IT off premises and into the cloud. This means that cloud decisions are made on a case by case, per-application basis according to 56% of the respondents. As customers have on average over 200 applications, with varying requirements, it's no surprise that most respondents are operating in multi-cloud environments (this year, nearly nine out of ten (87%) reported that they use multiple clouds). On average, respondents reported that they have deployed applications in 2.1 clouds, up from an average of 1.8 clouds in 2017. Over half (59%) reported they are in two to six clouds.

## Multiple Different Types of Clouds



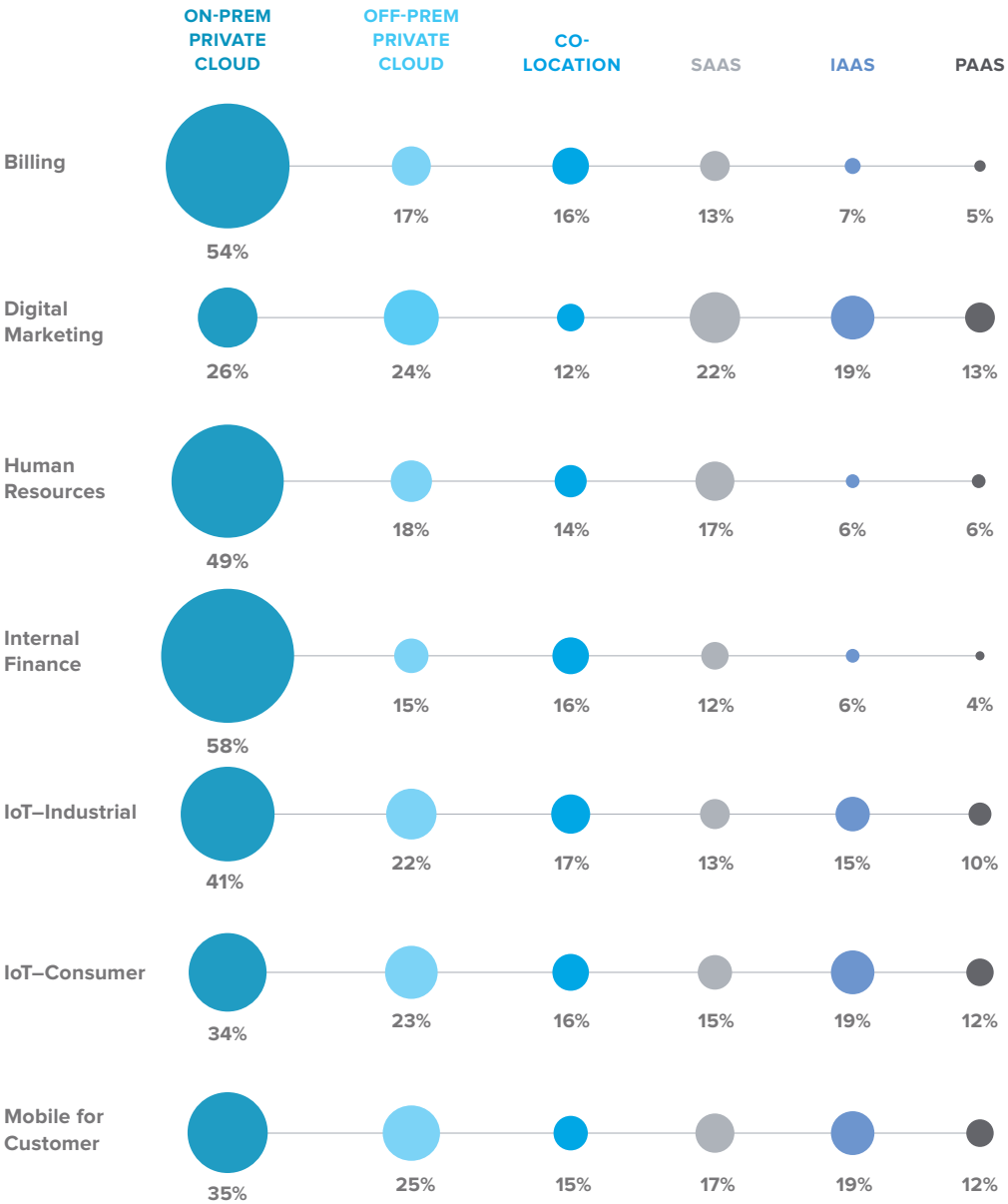

## Organizations use different cloud models for different kinds of applications

We wanted to understand the choice of cloud by application category, so we dug deeper. Applications that serve remote users and that must adapt quickly to changing market dynamics and trends had the highest preference for IaaS: digital marketing (19%), consumer IoT (19%), and consumer mobile (19%). Similar to last year's findings, the applications with the highest on-premises private cloud footprints are internal finance (58%), billing (54%), and human resources (49%).

## Multi-cloud presents challenges

While multi-cloud architectures undoubtedly increase agility, they also present very real organizational challenges. This year, respondents reported they were primarily concerned with security and the ability to have visibility into the health of their applications—no matter where those applications reside. Applying consistent security across all company applications was reported as a challenge by 42%, while protecting applications from existing and emerging threats came in right behind at 40%.

## Cloud Models Preferred for Different Application Categories



# 87%

**Eighty-seven percent reported that they used multiple clouds.**

## Multi-Cloud Challenges


**Applying consistent security policy across all company applications**


**Protecting applications from existing and emerging threats**


**Optimizing the performance of applications**


**Gaining visibility into application health**

Respondents were also concerned with optimizing the performance of their applications in the cloud (34%) and gaining visibility into application health (31%). The solution for these challenges? Application services are the secret ingredients that help organizations overcome the challenges they face in delivering applications across a globally distributed world of networks, locations, and users.

### F5 INSIGHTS FOR KEY FINDING 02

**As applications drive business, organizations make IT decisions based on the needs of the app, leading many to leverage multiple cloud platforms. While multi-cloud environments offer many benefits in terms of speed, scale, and flexibility, challenges include providing consistent security across clouds, protecting apps from a variety of threats, and gaining visibility into application health.**

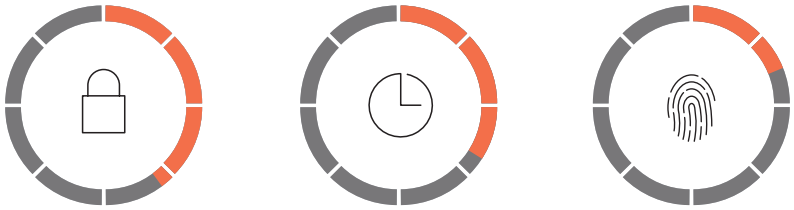
KEY FINDING

03

# Application services are the gateways to the future.

Application services are the unsung digital heroes of the application delivery chain, ensuring that apps are as fast as they can be while protecting them and their valuable cargo—data and credentials—from exposure or theft. They are also the services filling up public cloud marketplaces, and increasingly the means by which many cloud providers seek to differentiate themselves from competitors. A newcomer to 2018's "most likely to be deployed" list are app services that bridge generational gaps in protocols, environments, and app architectures, smoothing the path to success for organizations embracing the digital economy.

## The Worst Thing I Could Do Is Deploy an Application Without



43%
SECURITY

33%
AVAILABILITY

14%
IDENTITY/ACCESS

## The application services landscape evolves

Every year we look at the app services landscape and find that new services have appeared in response to challenges arising from the evolving digital environment. We are now tracking 30 distinct application services across five categories: availability, identity and access, performance, security, and mobility. This year saw the addition of gateway services for IoT, APIs, and HTTP/2, along with botnet protection. Organizations, on average, take advantage of 16 different application services—from load balancing, caching, and compression to access control, WAN optimization, and DDoS protection—in their quest to deliver on their promise to keep apps safe, fast, and available.

The pervasive use of these services always leads to the question, “Which one is most important?”

## Security services continue to rise in importance

Two years ago, respondents tagged both availability and security as equally important. But last year, security moved ahead of availability. And this year, that lead was extended with 43% of respondents declaring the worst thing they could do was deploy an app without security services. Availability still garnered a respectable 33%, the same as in 2017, and 1% higher than in 2016.

## Planned gateway services deployments show organizations embracing emerging technologies

The real surprise this year is the dominance of gateway services in the list of app services that organizations plan to deploy in the next twelve months. While the top five app services deployed now remain in line with results from previous years, when we asked about which app services organizations planned to deploy in the next 12 months, we saw a new trend emerging.

In fact, four of the top five services organizations plan to deploy are gateway app services. These foundational components of technology transitions can bridge gaps between existing and emerging protocols and technology. The breadth of gateways that respondents plan to deploy—including SDN, API, IoT, and HTTP/2—speaks to the profound impact digital transformation is having on organizations.

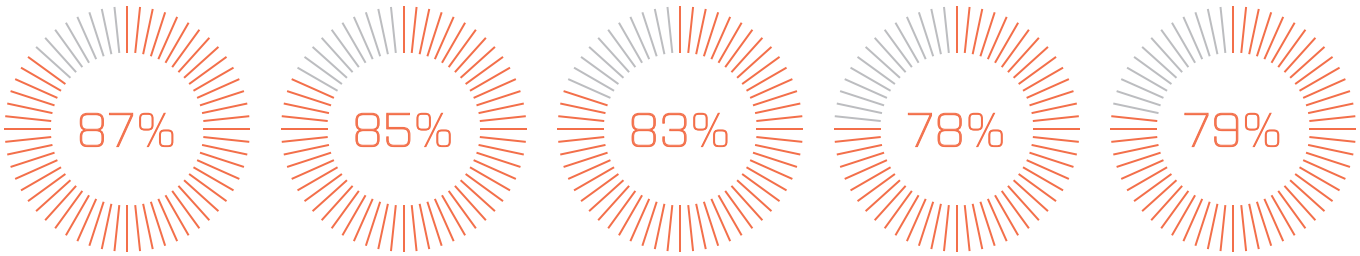
By embracing modern application architectures, cloud models, and a wide diversity of devices, organizations strive to capitalize on the digital economy. The deployment plans for gateways clearly show that respondents are putting in place the technologies and tools they need to confidently move forward into an increasingly digital future.

## Digital transformation changes deployment preferences

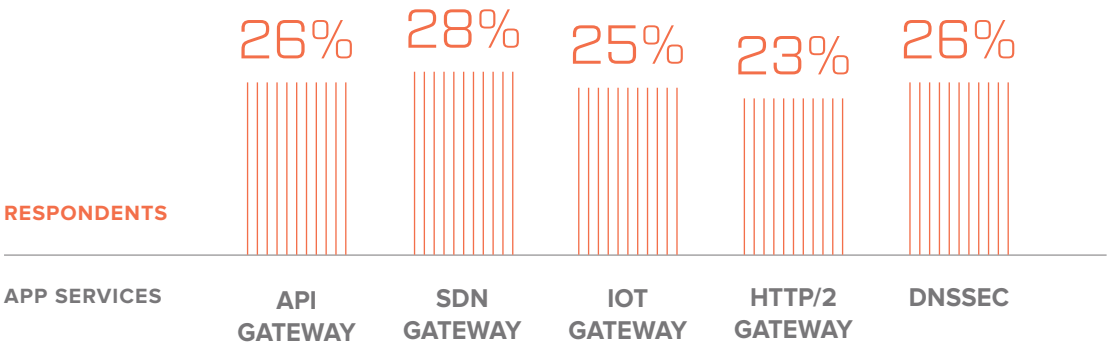
Ongoing digital change isn't just affecting the kinds of app services organizations deploy; it's also changing the way they deploy them. When it comes to on-premises deployment, organizations operating under a digital transformation initiative were more likely to want deployment of app services in containers at the expense of virtual machines. Almost a third (32%) of those without digital transformation initiatives preferred virtual machines for deploying app services and only 6% desired containers. Nearly twice as many (11%) operating under a digital transformation initiative indicated a preference for containers, with the increase coming at the expense of virtual machines, which dropped to 27%.

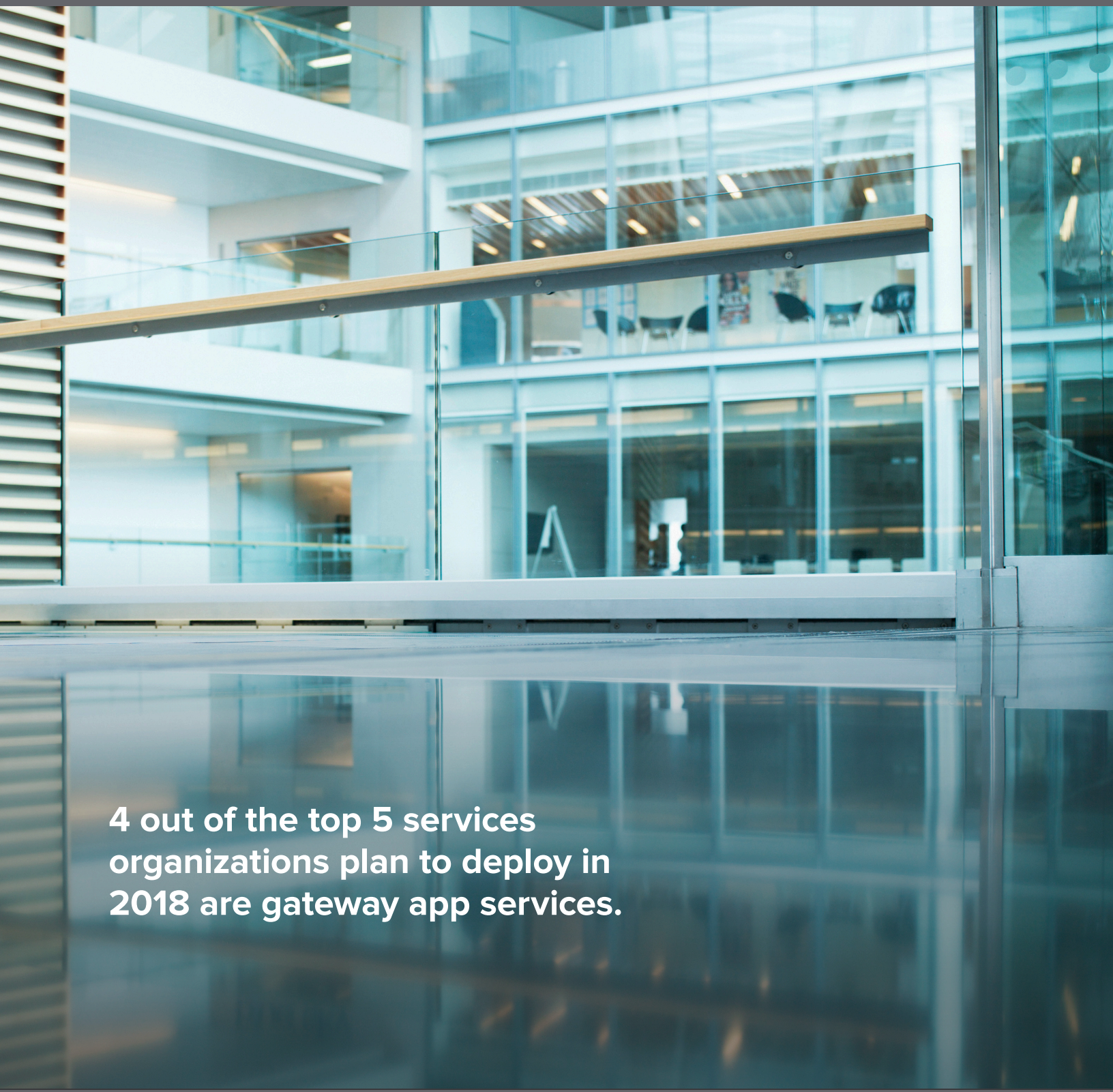
This increase in preference for containers is not surprising, as 56% of the respondents with current digital transformation projects told us that these projects are driving them to deliver applications from the cloud. Containers are natively more portable than virtual machines, and their orchestration environments are being designed with multi-cloud deployments in mind.

## Top Five App Services Deployed Now




## Top Five App Services Planned for Deployment in 2018





**4 out of the top 5 services organizations plan to deploy in 2018 are gateway app services.**

Given that 59% of respondents already employ 2–6 different cloud providers, we expect to see containers continue to rise as a preferred form factor given the greater ease with which application services can be standardized across multi-cloud environments.

## F5 INSIGHTS FOR KEY FINDING 03

**Security held the top position in the list of services that organizations consider mandatory to deploy in support of their apps. However, four of the top five app services that organizations plan to deploy in the next twelve months are gateway services, which help bridge gaps between existing and emerging technology. Finally, organizations undergoing digital transformation were nearly twice as likely to prefer deploying app services in containers.**

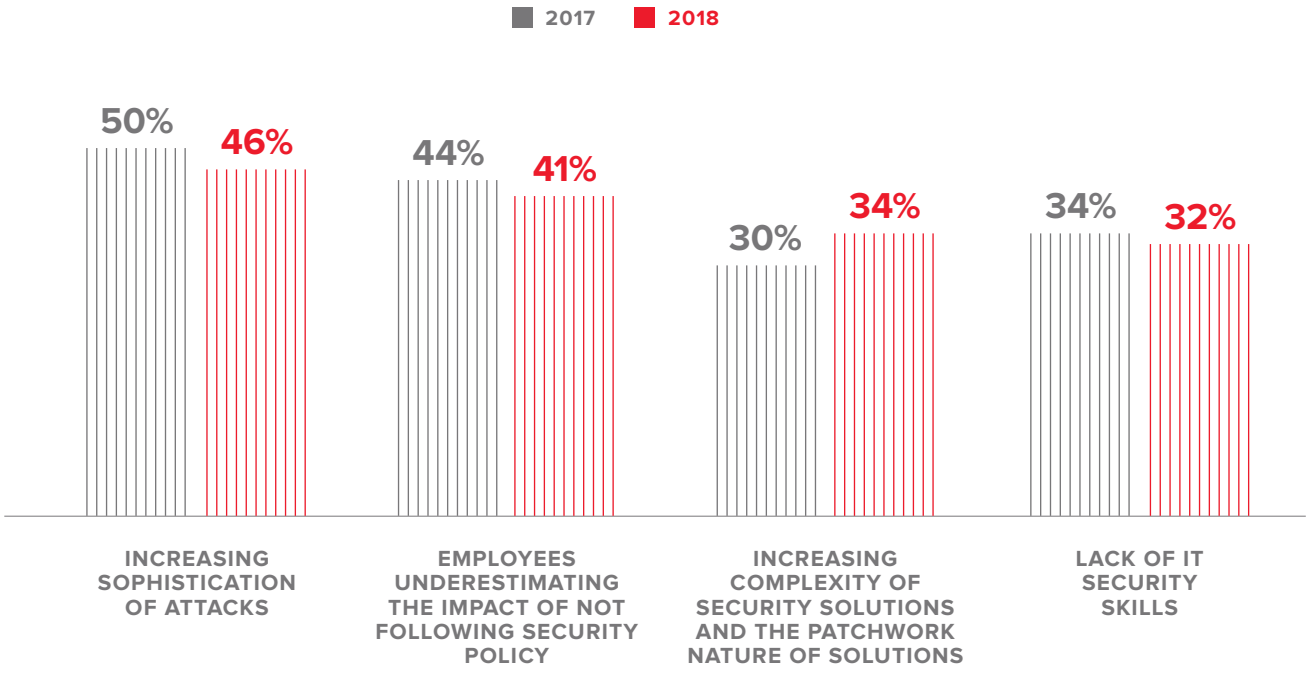
KEY FINDING

04

# Security confidence falls as multi-cloud rises.

In the past year, we've seen the rise of Death Star–sized botnets and the number of breaches has soared. With more breaches comes less confidence in security solutions and strategies to protect the ever-increasing amount of personal data that organizations process and hold. And while threats affect applications in every environment, organizations continue to be less confident in their ability to protect applications in public cloud or multi-cloud environments.

## Top Security Challenges Remain Largely the Same Year Over Year




## Challenge of protecting apps is on the rise

While the names of critical vulnerabilities and insidious malware may have changed, the underlying threat remains the same—consumer and corporate data is at risk. Complicating the task of protecting that data is the reality that organizations are fighting the security battle on multiple fronts.

Digital transformation is having a significant impact on where applications are deployed, with nearly half (49%) of respondents indicating it is driving them to deliver apps "from the cloud." That means apps in multiple locations and environments must be managed, monitored, secured against intrusion, and protected against attack.

Moreover, the challenge of successfully protecting apps is on the rise. In 2017, less than one in four (23%) respondents noted the difficulty in securing applications as a top security challenge. In 2018, that figure rose to 28%. While not enough to propel it into the top five security challenges this year, it is not far behind.

## WAF deployments trend up, but still only protect a portion of apps

The difficulty of protecting distributed applications is behind the rise in the deployment of web application firewalls (WAFs). Today, the majority of respondents indicate they have a WAF deployed, with another 19% planning to deploy one in the next twelve months. This continues a four-year upward trend in WAF deployments, growing consistently from 56% in 2015 to 70% in 2018.

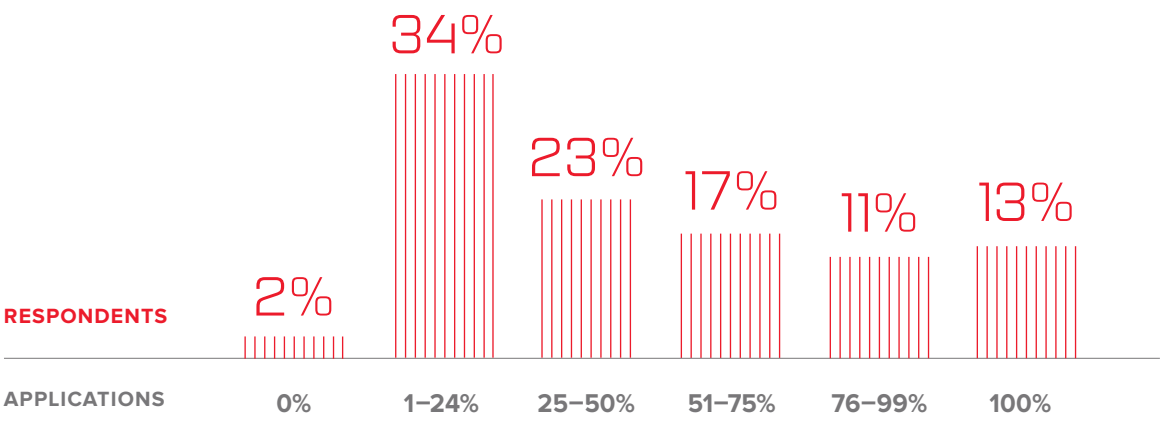
Despite this growth in WAF deployments, the percentage of applications that will be protected by the critical service remains lackluster. One in three (36%) plan on protecting less than a quarter of their applications with a WAF. Coverage continues to decline at each quartile, with just over one in ten (13%) indicating protection of 100% of their applications.

While this seems disheartening on the surface, the percentage of an organization's applications that are exposed to the Internet or partners varies. The urgency for security services like a WAF for applications not exposed to external clients is certainly lower than those deployed in the cloud and intended for public consumption. Also, nearly one in three (31%) respondents cited budgetary constraints as a significant security challenge for the coming year, which may be contributing to fewer applications being offered the protection of a WAF service. Of course, WAFs are not the only technologies organizations use to protect applications. We asked what respondents used and noted a strong preference for controlling access to the network (firewalls at 83%) and the application (access control at 75%). Web application firewalls rounded out the top three with 57% of respondents. A surprising 5% of respondents used none of the technologies we asked about, which also included cloud access security brokers (14%) and runtime application self-protection (11%) in addition to user behavior analysis (26%).

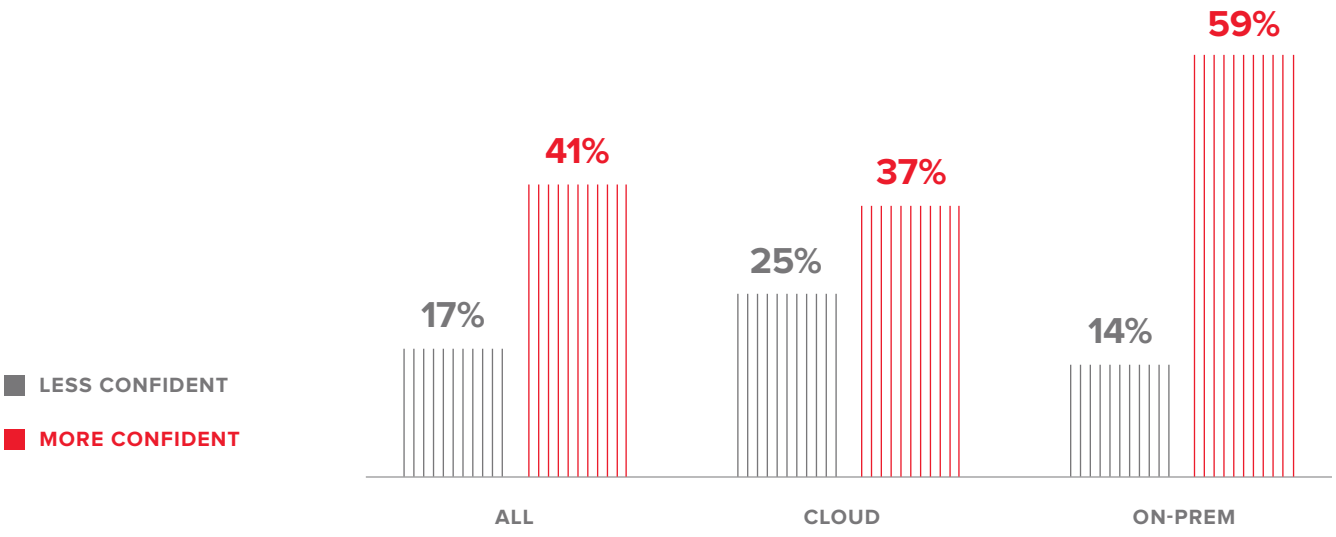
We suspect the heavy reliance on access-based methods of application protection contributes to the reduced confidence in protecting apps against attack in the public cloud. Interestingly, the use of technologies to protect applications has a more profound impact on confidence levels on premises than in the public cloud.

For example, of those with very low confidence in protecting on-premises applications, a mere 6% used a WAF. Of those with very high confidence, 37% employed the services of a WAF. The same relationship holds true in the public cloud, but the impact was less striking. Of those with very low confidence in protecting public cloud applications, 18% employed a WAF. Of those with very high confidence, 28% used a WAF.

## Percentage of Applications Protected by a WAF




## Confidence to Withstand an Application–Layer Attack




70%
Seventy percent of respondents indicated they have a WAF deployed.

## Security confidence wanes as public cloud adoption waxes

We suspect two culprits are responsible for shaking up confidence levels. First, traditional security strategies are often centered on controlling access to the application through the network. That accounts for the heavy reliance on network firewalls, which primarily restrict access at the network layers. Moving to the public cloud challenges that traditional approach and requires organizations to move from network-centered solutions and policies to an application-centered security strategy. This heavier focus on the application, its platform, and its protocols can be challenging as it requires greater collaboration between IT and developers and, in particular, security professionals who may or may not have expertise securing applications and their architectures.

Second, the increasing prevalence of APIs is forcing security and network professionals up the network stack to the application layer. Application–layer expertise has typically not been a requirement for security and network professionals, but we suspect that this will soon change. A lack of experience and skills at the application layer contributes to reduced respondent confidence in their ability to protect apps in the public cloud.

### F5 INSIGHTS FOR KEY FINDING 04

**With consumer and corporate data at risk due to persistent and emergent threats, organizations are ramping up WAF deployments to protect their apps. Respondents who have a WAF currently deployed tend to feel more confident in their ability to withstand application-layer attacks, although this confidence is more pronounced for on-premises deployments. Organizations with applications deployed in the cloud are challenged to move from network-focused security to application-centric solutions.**

KEY FINDING

05

# Automation and orchestration: Full steam ahead.

It has become popular to create technical mash-ups by combining operational domains within IT with DevOps, such as SecNetOps, DevNetOps, and NetSecDevOps. Beyond all these buzzwords lies the simple truth—programmability of the network and the security infrastructure that makes up the production app delivery chain is no longer a nice-to-have—it's a requirement. With pressure from Dev and Ops mounting, thanks to increasing use of containers and adoption of cloud, traditional IT is embracing programmability to enable the automation and orchestration required to succeed. However, organizations seeking to optimize IT through automation and orchestration need to standardize before speeding ahead.

## Use of Automation in Production


## IT optimization drives use of automation

Nearly three in four (74%) of respondents declare the use of automation in the operation of IT infrastructure to be “somewhat” or “very” important. That holds true across all roles in the organization—including C-level executives and security professionals. More than just viewing automation as important, respondents are embracing it. Over half (53%) are using automation partially or fully in production, and another 31% are piloting its use. Only 17% indicate they are not using automation in production at all.

Those that use automation are driven by factors that align with digital transformation benefits, particularly the desire for IT optimization. The majority (70%) are using automation to realize leaner IT with the goal of reducing OpEx. Over half (51%) are looking to scale to meet demand. Both are appropriate responses in the face of the law of diminishing returns, which is just as applicable to operational scale as it is business.

To this end, respondents indicate considerable use of automation for incident response as well as major and minor changes in production. Over half of respondents report that they use automation in all three cases in production "sometimes," with one in four "always" employing automation for major or minor changes in production. Incident response teams are least likely to use automation. This is not a surprise, given that incidents are far less predictable and therefore not as well suited to being codified as the well-established processes that govern changes in production.

This considered embrace of automation is encouraging, as it indicates a more strategic operational view. Remember that tactical and accidental use of automation can actually be a net negative. A strategic approach evaluates the long-term sustainability of automation systems and scripts, and is critical to realizing the optimization and scale desired.

## Organizations work to standardize; OpenStack, Cisco, and VMware hold their places

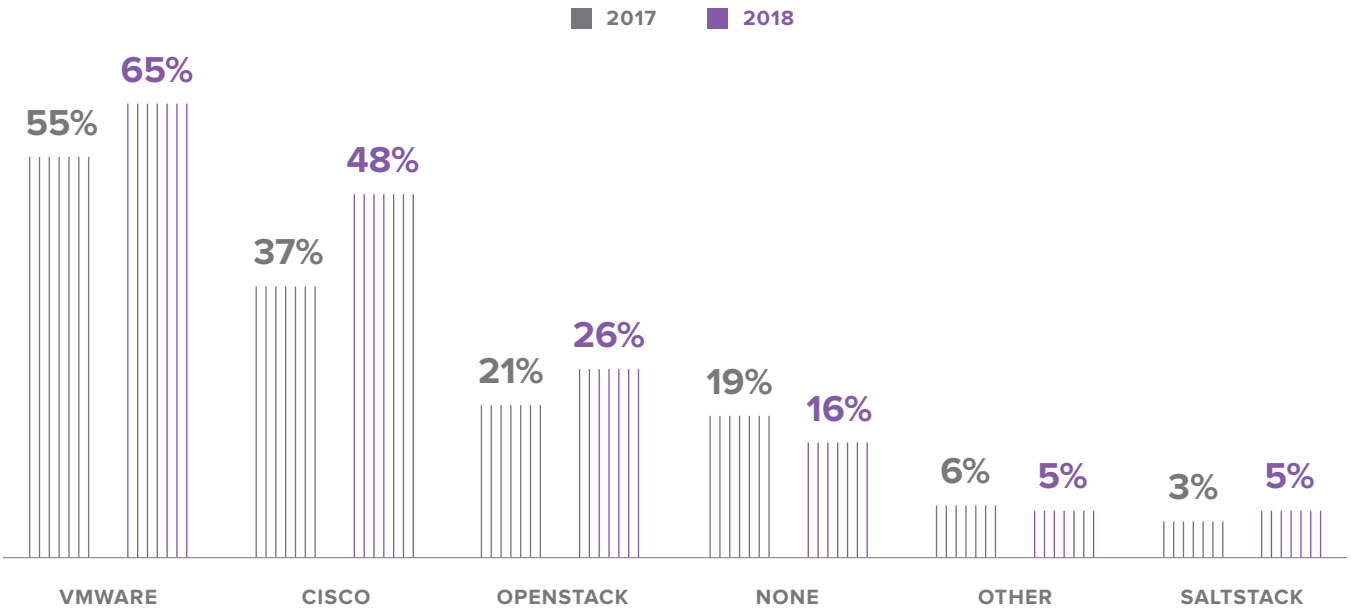
The good news is that organizations are beginning to standardize their automation and orchestration environments. That's important because the benefits of reducing operational costs are hard to achieve when you're accumulating technical and architectural debt from maintaining multiple frameworks, tools, and systems.

Half (50%) of all respondents have settled on a single network automation toolset. Just over a third (36%) are using two toolsets. Of those toolsets, the "big three"—VMware, Cisco, and OpenStack—continue to dominate the network automation landscape. All made significant gains with Cisco and VMware boasting 11% and 10% increases year over year, respectively. OpenStack rose from 21% in 2017 to 26% in 2018.

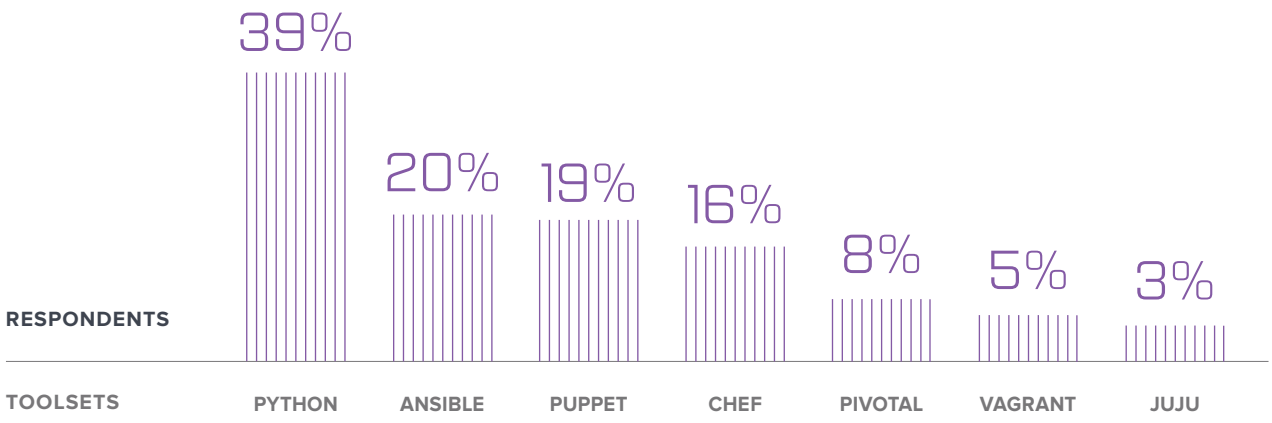
When it comes to scripting and deployment, 67% have also standardized on a single toolset, with Python scripts (39%) taking a definitive lead over more formalized frameworks like Ansible (20%), Puppet (19%), and Chef (16%).

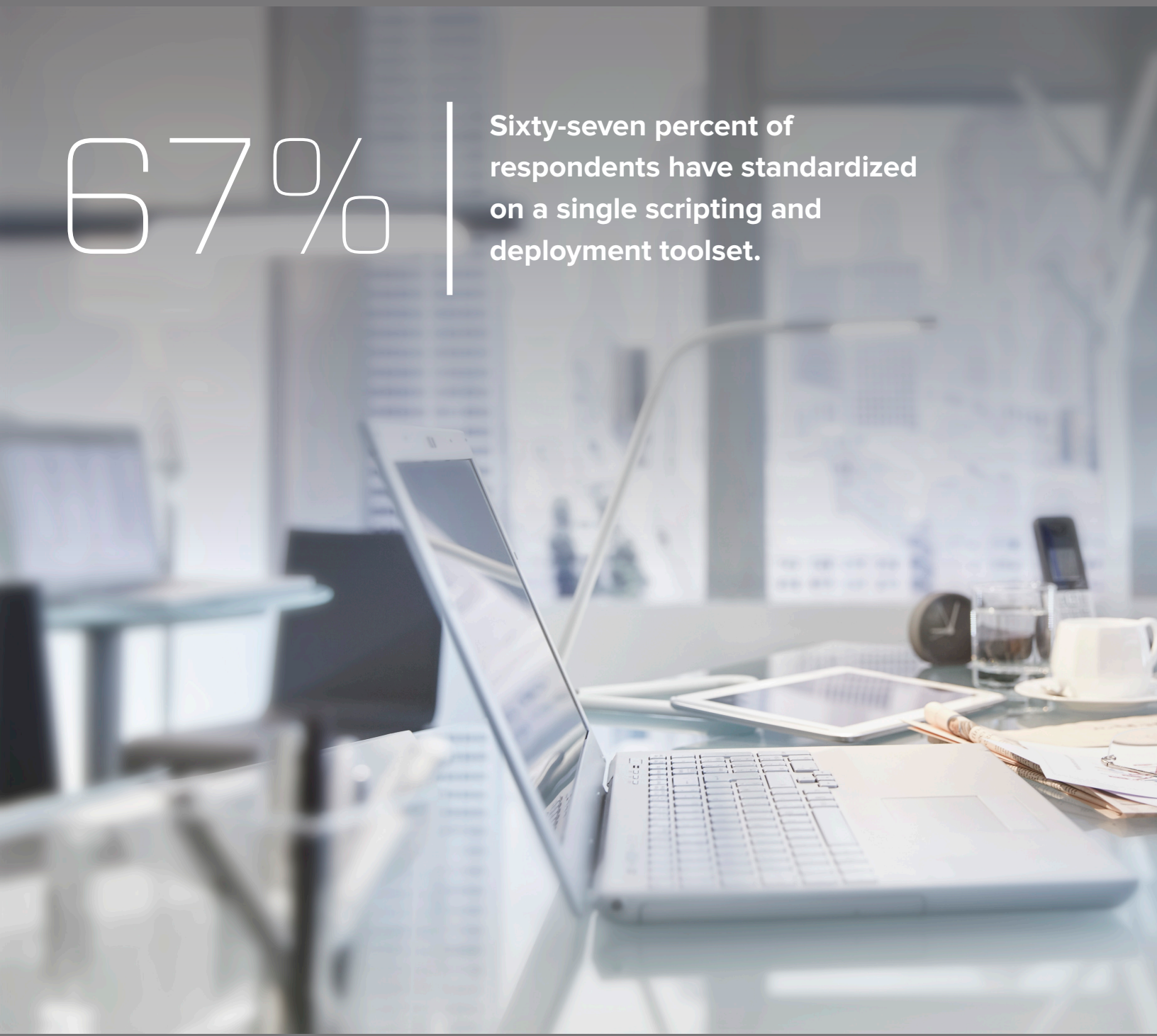

**Fifty percent of all respondents have settled on a single network automation toolset.**

## Network Automation Frameworks in Use




## Automation and Orchestration Toolsets





# 67%

**Sixty-seven percent of respondents have standardized on a single scripting and deployment toolset.**

## Kubernetes is not winning, but it's not losing either

Not to be ignored is the increasing use of container orchestration systems as developers push containerized applications and microservices into production. While Kubernetes dominates Twitter and the conference circuit, Docker Swarm is the clear favorite among respondents with 27%. Twenty-one percent (21%) prefer Red Hat OpenShift. Although Kubernetes might not be winning, it's not losing either; 16% of respondents are using the open-source darling.

Overall, the interest in container orchestration is unsurprising. In 2017, 4% of respondents indicated a preference to deploy app services in containers. This year, that surged to 9%, an upward trend we expect to see continue as containers push their way further into production, and organizations migrate faster and faster to the public cloud.

### F5 INSIGHTS FOR KEY FINDING 05

**Nearly three out of four respondents cite automation as being important to their IT operations, and they are taking a strategic approach to leveraging it to optimize processes, scale to meet demand, and respond to incidents. Almost half have settled on a single automation framework, while two-thirds have standardized on a single scripting and deployment toolset. Container orchestration through proprietary and open-source systems continues to grow in popularity.**

# Conclusion

Last year, we noticed the influence of the digital economy on application services. This year, the proof is clear—organizations are building the foundation to support digital transformation by embracing cloud, automation, and orchestration. Furthermore, businesses are adjusting their security strategies to focus more on the application and are considering new offerings that are better suited to support applications deployed across multiple clouds.

Organizations leverage a suite of application services to provide the security, availability, and performance that their critical applications require to satisfy the needs of businesses and customers alike. With the percentage of apps being delivered from the cloud growing, maintaining a robust and consistent suite of application services will become more and more important.

This year, respondents were heavily focused on internal requirements to support the digital economy. As they become confident in the foundation they are building, we expect IT organizations will reinvent themselves as platforms for competitive differentiation and innovation, helping drive business success in this continuing digital transformation.

### MORE INFORMATION

**For more information about the data in this report and what it means for your business, please visit f5.com/SOAD.**

F5 Networks, Inc. | 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

RPRT-SOAD-183861188