2017 REPORT

The State of Application Delivery

LOAD BALANCING
GLOBAL SERVER LOAD BALANCING
DNS
DDOS PROTECTION/MITIGATION
WEB APP FIREWALL
INTRUSION DETECTION/PROTECTION SYSTEM

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

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

SSL/TLS OFFLOAD
CACHING
TCP OPTIMIZATION
WAN OPTIMIZATION
ENDPOINT SECURITY
VIRTUAL DESKTOP INFRASTRUCTURE

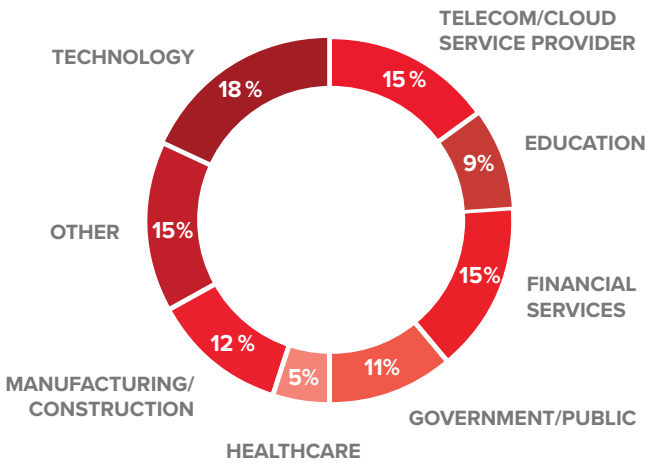
What's inside

2017 Survey Demographics

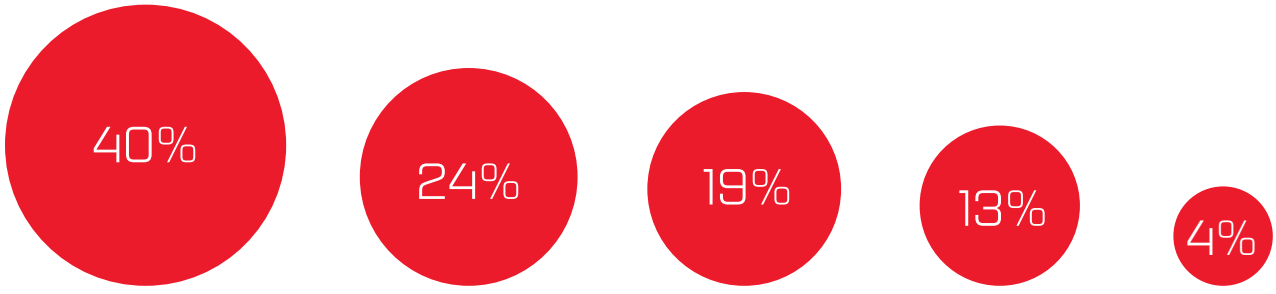
2,197

TOTAL NUMBER OF RESPONDENTS

Industry



Respondent role



INFRASTRUCTURE / NETWORK
Engineer/Manager

EXECUTIVE
C-level, IT Director/VP

SECURITY
Manager, Engineer, Architect

APPLICATION ROLES
Developer, Architect, Manager

CLOUD ARCHITECT/ DEVOPS

Introduction

The modern world runs on applications. Your employees require apps to do their jobs, while your customers rely on them to connect with your business and advance their own. Expectations are high. All your users demand immediate, uninterrupted, and secure access to the applications they need when they need them.

In order to thrive in today's fast-moving, hyper-connected digital world, your applications need the support of a robust set of application services that boost performance, maintain availability, bolster network and application security, and deliver the visibility you need to ensure success. And whether you're deploying critical apps in the cloud or in the data center, using virtualized machines or containers, every organization feels the pressure to reduce costs and increase scalability.

Our intention in conducting the State of Application Delivery survey over the past three years has been to understand not only the deployment landscape for app services, but also the market trends and drivers behind the use of and need for those services. We investigated cloud computing adoption and strategies, future investment plans and application portfolios, as well as security challenges. And, finally, we explored questions of operational efficiency by digging into automation and orchestration with a focus on DevOps and SDN. By collecting answers from more than 2,000 respondents globally across a range of positions and industry verticals, we explored the challenges of the digital transformation organizations are currently undergoing.

With that data firmly in hand, it is our pleasure to present our findings on the State of Application Delivery in 2017.


17
The average organization
is planning to deploy
17 application services
in the next 12 months.

2017 Key Findings

01

The digital economy is driving increased reliance on application services.

As pressure mounts to deliver applications faster, smarter, and more securely, businesses are responding with increased usage of key application services. Three-fourths of respondents have 10 or more services deployed–up from 60 percent who reported 10 or more services in 2016. The average organization is planning 17 deployments in the next 12 months.

02

Cloud expertise is vital.

With one out of five respondents planning to have more than half of their applications in the cloud by 2017, and four out of five adopting multi-cloud environments, organizations are expanding cloud computing deployments in the face of a continuing gap in related skills.

03

Deployments of security application services grow more sophisticated.

Globally, organizations with the most confidence in their ability to withstand an attack have expanded beyond a simple perimeter approach to security. Many plan to deploy DDoS mitigation, DNSSEC protection, and a web application firewall in the next year.

04

Operational benefits have become the main attraction for DevOps and programmability.

Scalability and operating expense reduction are the top two drivers for the interest in DevOps and programmability. This scale is necessary to thrive in the digital economy.

KEY FINDING

01

The digital economy is driving increased reliance on application services.

While applications are the engines that run today's enterprises, application services are the fuel that keeps them on the road. We asked customers about their use of application services, from network firewalls and antivirus protection to SSL/VPN, load balancing, and DNS services. Of the respondents, nearly three-quarters have 10 or more services deployed today, with the average organization planning to deploy 17 services in the coming year.

Top 5 application services companies have deployed today

83% NETWORK FIREWALL

83% ANTIVIRUS

78% SSL VPN

72% LOAD BALANCING

72% SPAM MITIGATION

App services deployment is on the rise

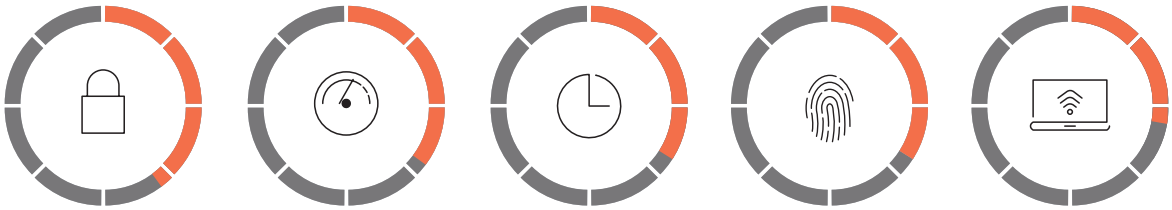
With the increasing importance of applications as the currency of the digital economy, it is no surprise that the average number of app services in use by organizations increased from 11 in 2016 to 14 today. That's more than half of the 26 services we asked about, spanning availability, mobility, performance, security, and identity and access. The percentage of organizations that rely on 10 or more of these app services rose to 74 percent in 2017, up 14 points from last year. Nearly half (49 percent) of organizations deploy between 11 and 20 app services.

The top five of those app services deployed remained relatively stable compared to 2016. The continued reliance on applications to drive revenue growth as well as the vital necessity of continuing to provide a positive customer experience contributed to the growth in load balancing deployments from 2016.

We also recorded a steady rise in the number of planned deployments for app services, with the average organization planning 17 deployments in the next 12 months.

Globally, the top individual security services planned for deployment in the next year are DDoS mitigation (21 percent), DNSSEC protection (25 percent), and web application firewall (WAF) services (20 percent).

App services respondents will deploy in the next 12 months

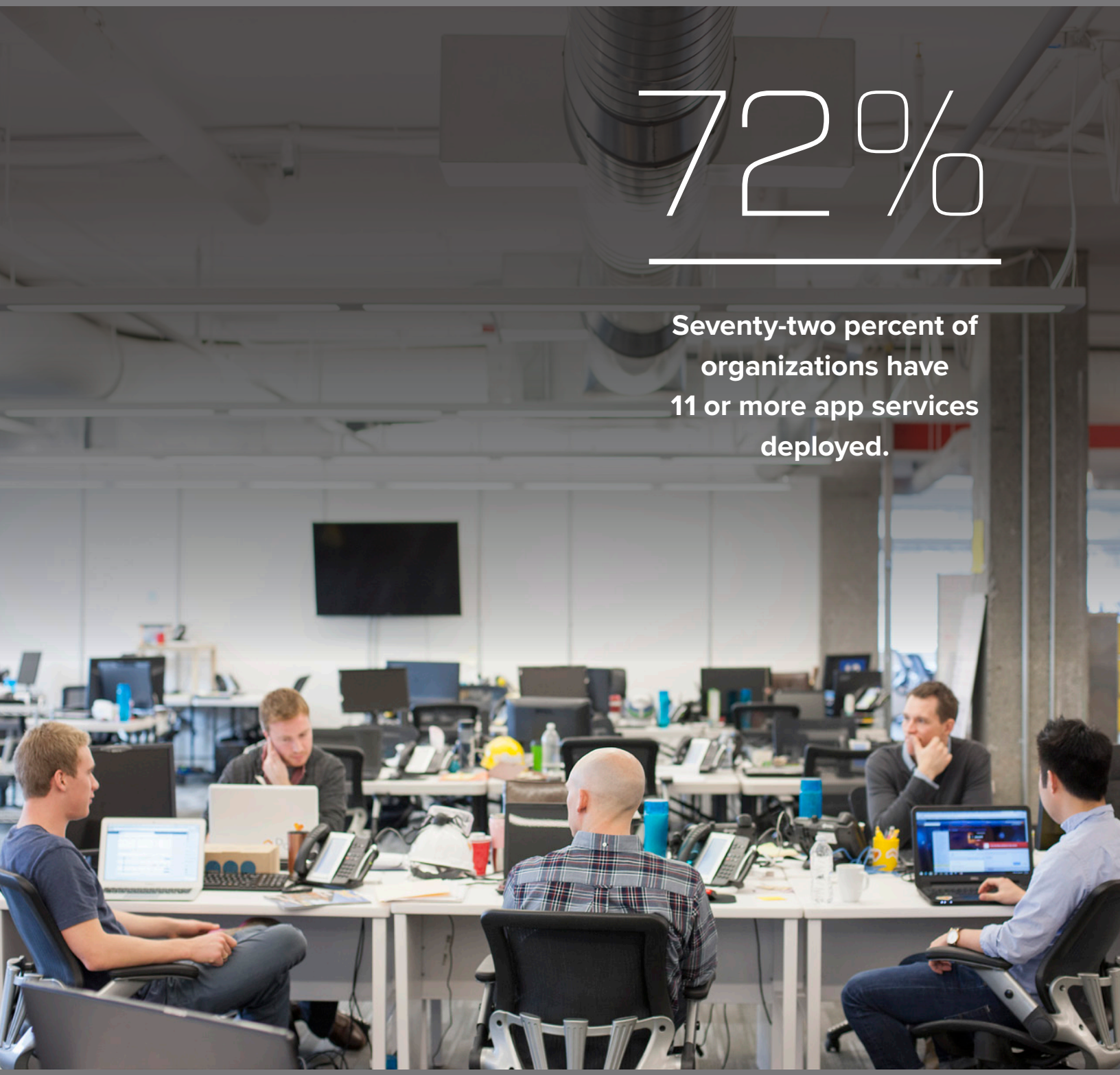


A closer look by region shows a similar story, with the exception being Japan, where anti-fraud services led the list of those being deployed at 17 percent. DNSSEC (12 percent) and DDoS mitigation (11 percent) also made the top three. Interestingly, this does not appear due to an overwhelmingly large existing deployment of DDoS protection in Japan (61 percent). Instead, the divergence seems to highlight a focus on application and data protection in Japan.

What apps can't live without

As in past years, we attempted to answer the question "what's the most important app service" by encouraging respondents to identify the worst thing they could forget to deploy with an app. We've seen this change from availability in 2015 to security in 2017. By a margin of almost 6 percent, respondents this year said it is worse to deploy an app without security than without availability. Given the fanfare with which security breaches are announced, and the subsequent negative impact on organizations to their brand and their bottom lines, this should not be surprising.

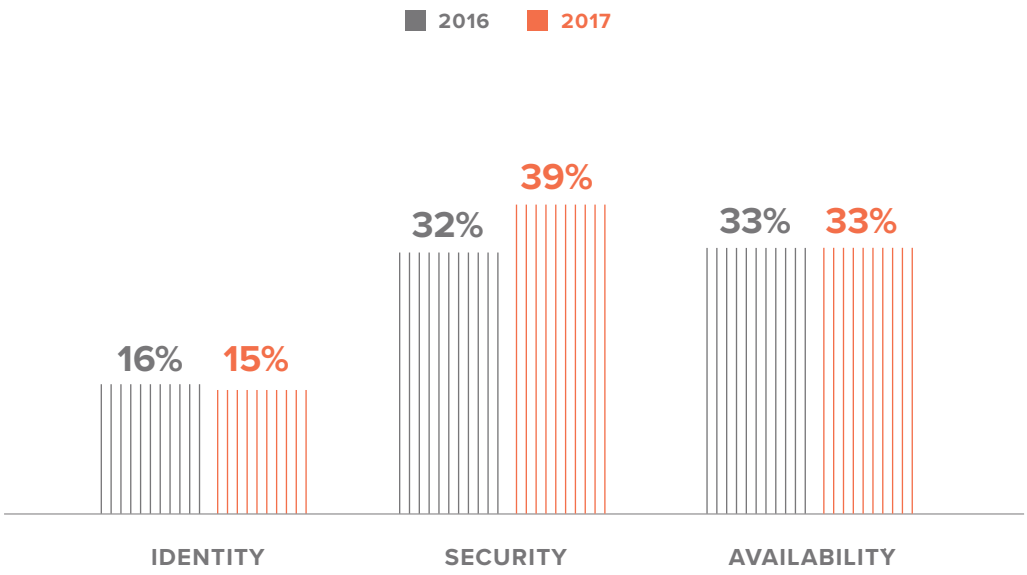
Still, many might argue that the security of an application is irrelevant if it is unavailable. A failure to scale is as detrimental to a brand's reputation as a security breach, and often it is just as costly in terms of lost revenue and customers. Splitting apart the app services categories and digging deeper into the data, we found that on an individual basis the single most important app service turns out to be one associated closely with availability: load balancing, with one out of five reporting this as the most important application service.



72%

Seventy-two percent of organizations have 11 or more app services deployed.

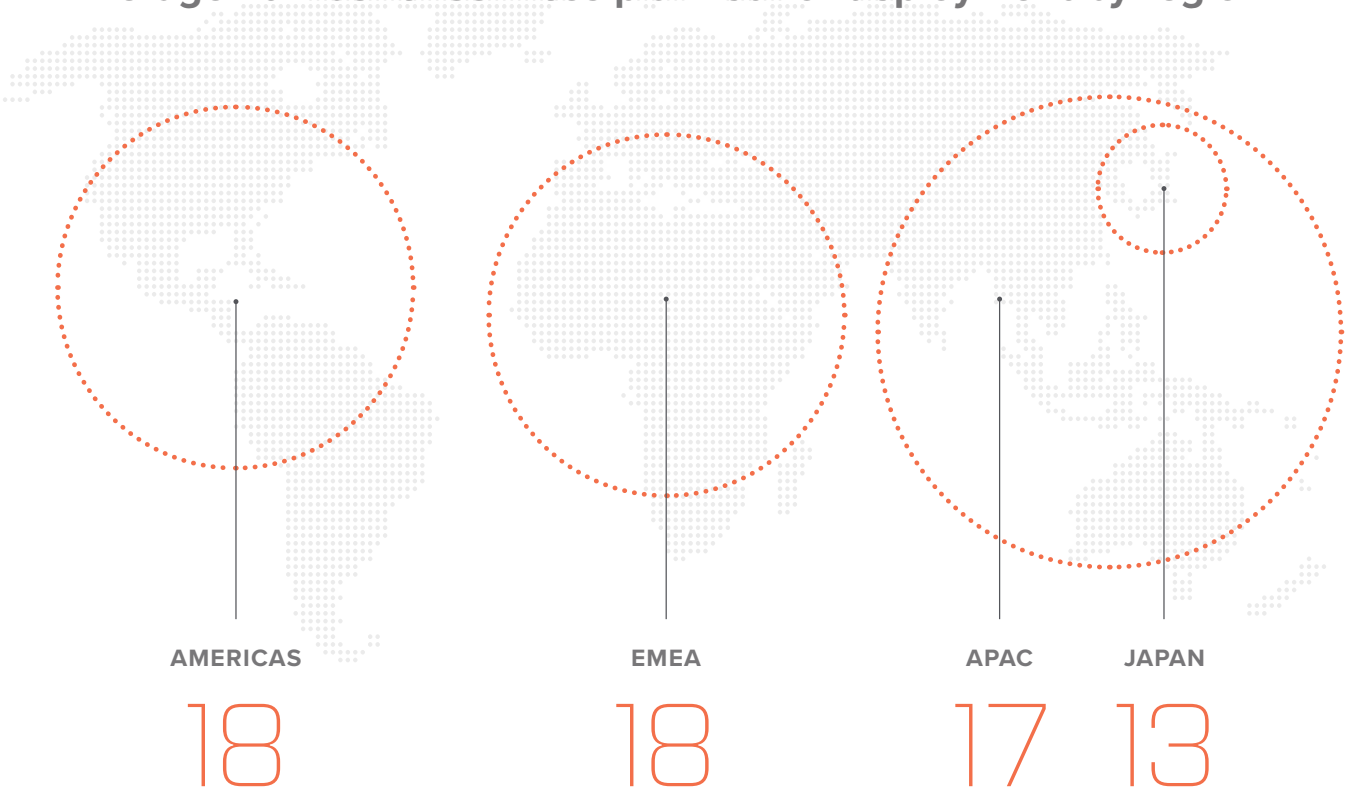
The worst thing I could do is deploy an app without...



Top 3 security services planned worldwide

Top 3 security services planned in Japan

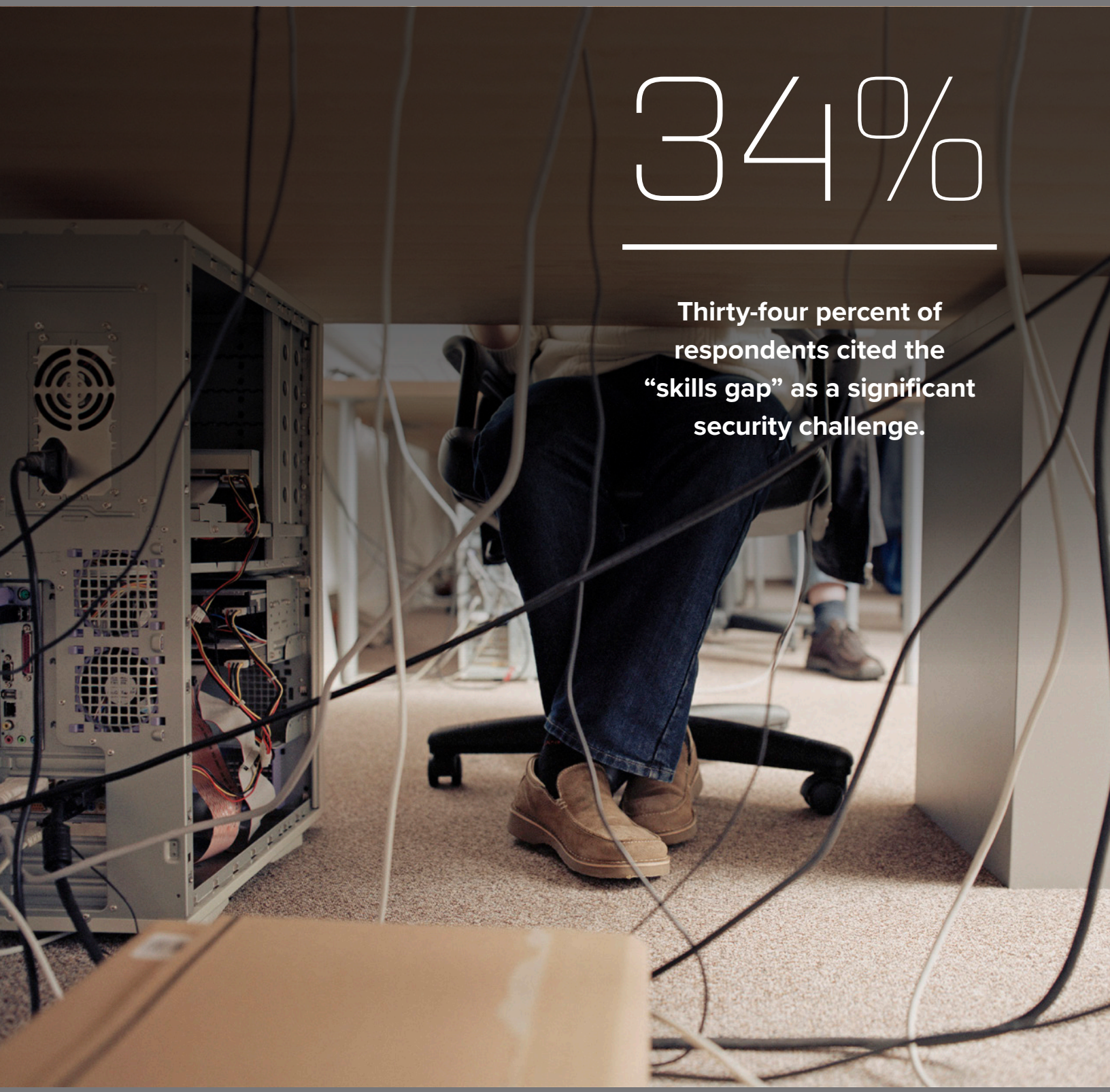
Average number of services planned for deployment by region



Vying for the second and third spots on the list of apps respondents can't live without were application access and WAF, both of which are ultimately important to maintaining the security of application. Some differences appear when viewing app services from the different perspectives of role and responsibility within the organization. Those in application roles, for example, considered a WAF far more critical than access control. On the other end of the spectrum, those in executive roles felt exactly the opposite, tagging access control as more important.

Regional differences did have an impact on the results. In Japan, for example, anti-fraud topped the "worst thing to deploy without" list at 19 percent, followed by network firewall at 15 percent and load balancing at 14 percent.

The majority of the services respondents tagged as being critical are directly related to the safety of both consumer and corporate data through controlling access and interactions. These overarching concerns were mirrored in service deployment plans for 2017.



34%

Thirty-four percent of respondents cited the “skills gap” as a significant security challenge.

App services follow applications to the cloud

Deployment of services in the public cloud continues to increase across the board, year over year. The 26 app services showed an average increase of 4 percent over last year in public cloud deployment preference. On-premises preferences were a mixed bag of decreases and increases. With the exception of DDoS protection and spam mitigation, all security services also show a similar decrease in on-premises preferences.

Eighteen percent of organizations reported challenges optimizing performance in their hybrid cloud environments, so it is not surprising that three of the top services preferred for public cloud deployment were related to performance: HTTP2 (16 percent), caching (15 percent), and acceleration (15 percent). This is close to the percentage of respondents who also indicated a preference for public cloud for marketing apps (12 percent) and mobile apps (13 percent).

The "skills gap" was cited by 34 percent of respondents as a significant security challenge. So it makes sense that most of the app services respondents indicated they'd like to deploy "as a service" were security related. One in four respondents preferred a service model for deployment of DDoS protection, DNSSEC, and spam mitigation. One in five included global server load balancing (GSLB), anti-fraud services, and identity federation in their "most wanted to deploy as a service" list.

Respondents continue to report a preference for "on premises" followed by "as a managed service." Given the preferences for deployment of all application types in an "on-premises, private cloud," it is no surprise that respondents' preferences for deploying the app services needed to deliver fast and secure apps would also be strongly on premises as well.

As app services tend to follow applications by design, we suspect that as app deployment preferences drift toward public cloud, we will continue to see gains in preferences for deploying app services in the public cloud.

F5 INSIGHTS FOR KEY FINDING 01

Over the past three years, security has supplanted availability as the most important application service according to respondents. Private and public cloud deployments are growing and no matter whether apps are deployed on-premises, in a private cloud, or in a public cloud, organizations will continue to rely on app services to keep their critical apps secure, available, and performing up to expectations.

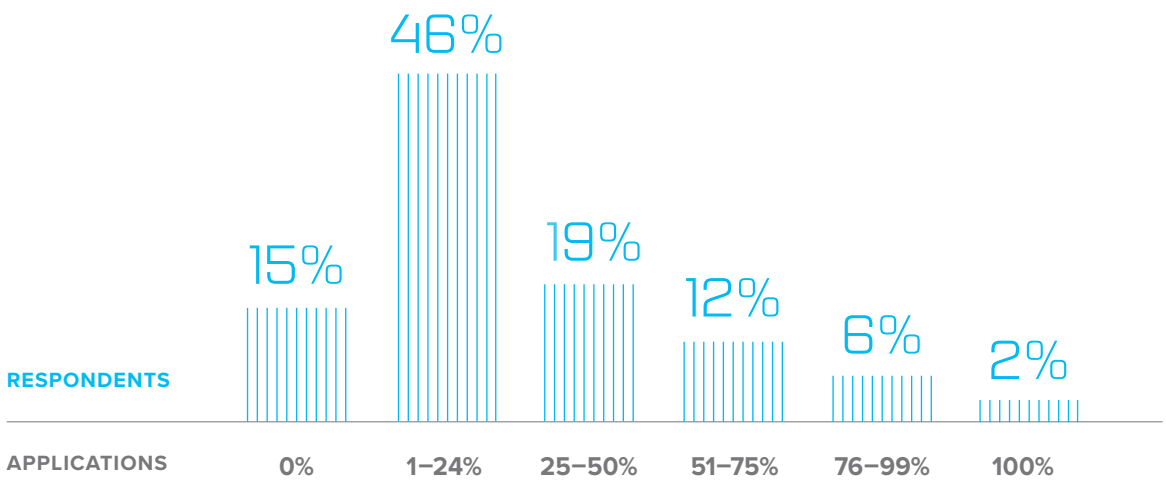
KEY FINDING

02

Cloud expertise is vital.

Whether it be public, private, or a hybrid model, the cloud is thriving, with more and more organizations evaluating cloud-based solutions before making new IT investments. In this multi-cloud world, organizations find themselves making choices about the cloud today that will affect their business for years to come. We asked survey participants how this explosive growth in cloud computing has affected their IT strategy, whether they are a cloud-first organization, and where they are planning to make investments in cloud technology in the coming year.

Percentage of apps respondents will move to the cloud by 2017



Cloud opportunities and investments

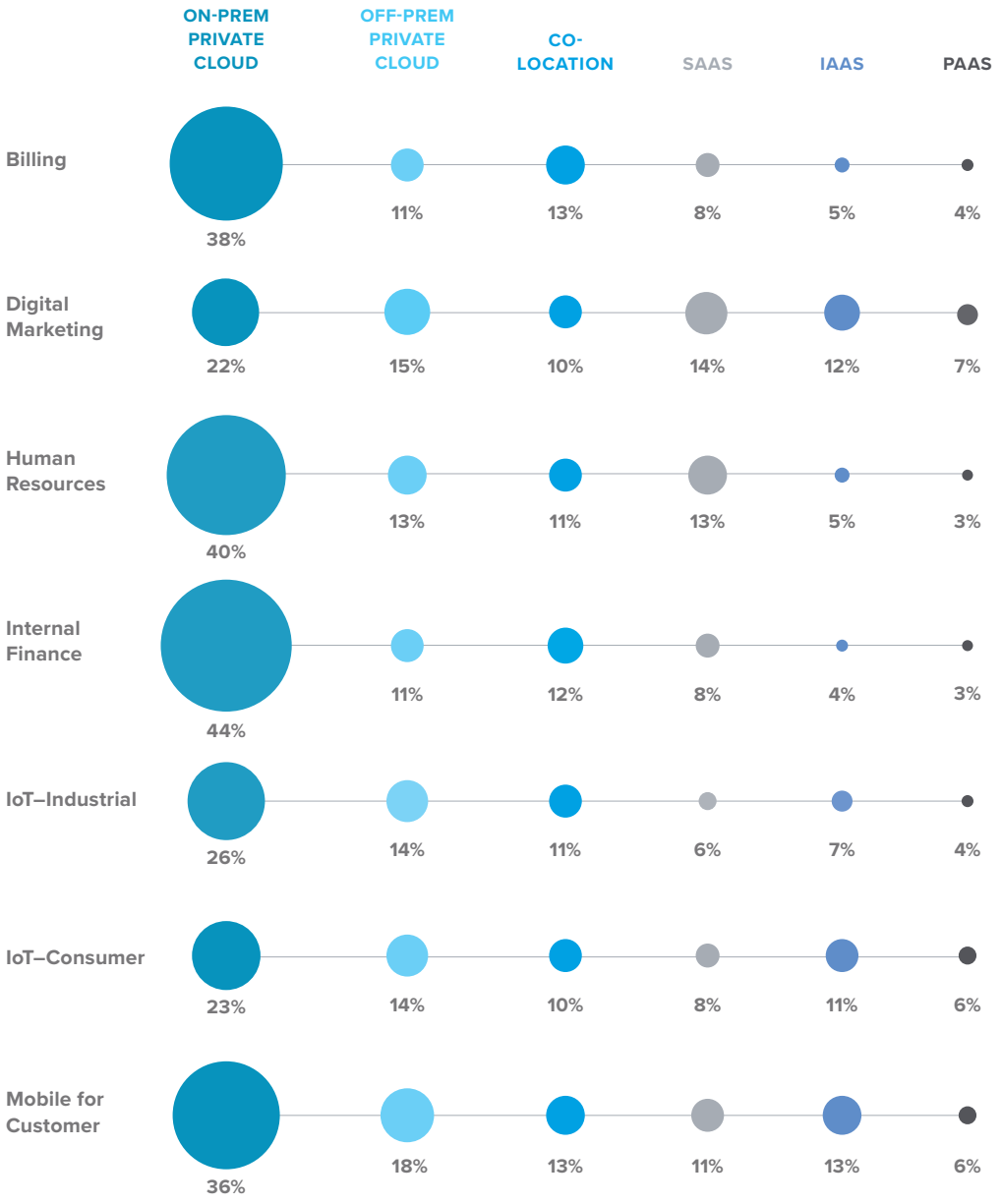
Cloud computing entered the mainstream with early beta releases in 2006. Now, with a decade of experience and more and more cloud-based solutions available, respondents are clearly embracing cloud computing. Customers are moving more apps to the cloud; globally, 1 out of 5 respondents will have over 50 percent of their apps in the cloud by 2017.

We noted slight variations by vertical and company size with the most striking trend aligned with the number of applications deployed. The respondents with the largest number of applications (3,000+) reported the highest percentage of apps in the cloud.

The more applications a company has deployed, the greater motivation to reap the operational benefits of the cloud. These organizations also tend to have the most maturity with respect to IT investments and are often leaders in many technology trends.

This year, we expanded the survey to understand the choice of cloud by application category. The applications with the highest on-premises private cloud footprints are, not surprisingly, internal finance (44 percent), human resources (40 percent), and billing (38 percent).

Cloud models preferred for different application categories



These three cloud operating models were identified as “strategically important”

PRIVATE CLOUD

39%

PUBLIC CLOUD

38%

SAAS

37%

Additionally, customers reported a strong preference for on-premises private cloud for industrial IoT apps. The amount of data industrial “things” are transmitting means it makes more sense to have the alerts and computation of this data happen closest to the greatest concentration of the devices, be it the systems on the manufacturing floor, the trackers in the fields, or the equipment in the hospital. As a result, over a quarter (26 percent) of respondents plan on using an on-premises private cloud for industrial IoT apps.

Respondents reported a strong preference for all cloud types for mobile applications used by their own customers. The preference for on-premises private cloud was the highest for mobile applications at 36 percent, and this workload also saw the highest percentage of all the workload types for public cloud IaaS (13 percent) and PaaS (6 percent).

Globally, respondents reported that on-premises private clouds will see the largest amount of investment this year according to 46 percent of the respondents. This is true across every region; Americas (41 percent), EMEA (46 percent), Asia-Pacific except Japan (49 percent), and Japan (47 percent).

Customers are making investments today in on-premises private clouds, and, as they look to the future, they believe that private clouds, public clouds, and SaaS will all have strategic importance in the next two years.

Public cloud as a strategic priority has increased from 34 percent last year, largely because of increased interest in the Americas and EMEA. Whereas last year, Asia-Pacific was ahead in viewing public cloud as strategic, all three regions appear to have similar strategic intent in 2017 with the Americas at

+4%

Respondents showed an increased preference (+4 percent) for deploying the app services we asked about in the public cloud.

41 percent, EMEA at 38 percent, and Asia-Pacific at 36 percent.

Solutions are entering the market that lower the barrier to public cloud IaaS adoptions. Nearly one-third (32 percent) of respondents will purchase public cloud solutions this year, which is dramatically up from 25 percent in 2016. Additionally, when we asked which deployment model would see the largest amount of investment, 10 percent reported public cloud IaaS.

The cloud is thriving and more and more organizations are embracing "cloud first" strategies, meaning their organizations are required to evaluate cloud-based IT solutions before making new IT investments. This year, the number of cloud-first organizations jumped to 47 percent globally, from just 33 percent in 2016. Asia-Pacific leads the regions in cloud-first strategies with over half (54 percent) reporting a cloud-first preference, which is up from the 42 percent who reported a strong preference last year.

Cloud challenges

We live in a multi-cloud world where customers are choosing the platform, data center location, and ecosystem that best meet their specific application requirements. Consistent with 2016 results, 4 out of 5 of the respondents reported that their organizations are adopting hybrid cloud. This hybrid environment is not without its challenges, however. Respondents cited the inability to have consistent security policies across multiple environments (28 percent) and lack of analytics (25 percent) as the top two challenges.

Cloud expertise also remained a concern for respondents, with 23 percent reporting that they don't have in-house or readily available external expertise in public cloud. We noted some regional differences, as almost one-third (32 percent) of Asia-Pacific respondents logged concern with implementing consistent security policies. Additionally, similar to last year's results, Asia-Pacific respondents reported a much higher concern with application performance across hybrid cloud deployments (21 percent), compared to only 13 percent in the Americas and 14 percent in EMEA. Given the geographical distances in the region, these performance concerns remain an ongoing challenge for pan-Asia-Pacific customers.

F5 INSIGHTS FOR KEY FINDING 02

As organizations grow more comfortable with cloud computing, more and more are moving their critical applications to the cloud. While on-premises clouds will see the most investment this year, respondents also cited the strategic importance of the public cloud and SaaS offerings. Cloud expertise remains a challenge for many organizations attempting to manage the increasingly complex world of applications deployed across multiple cloud deployments.

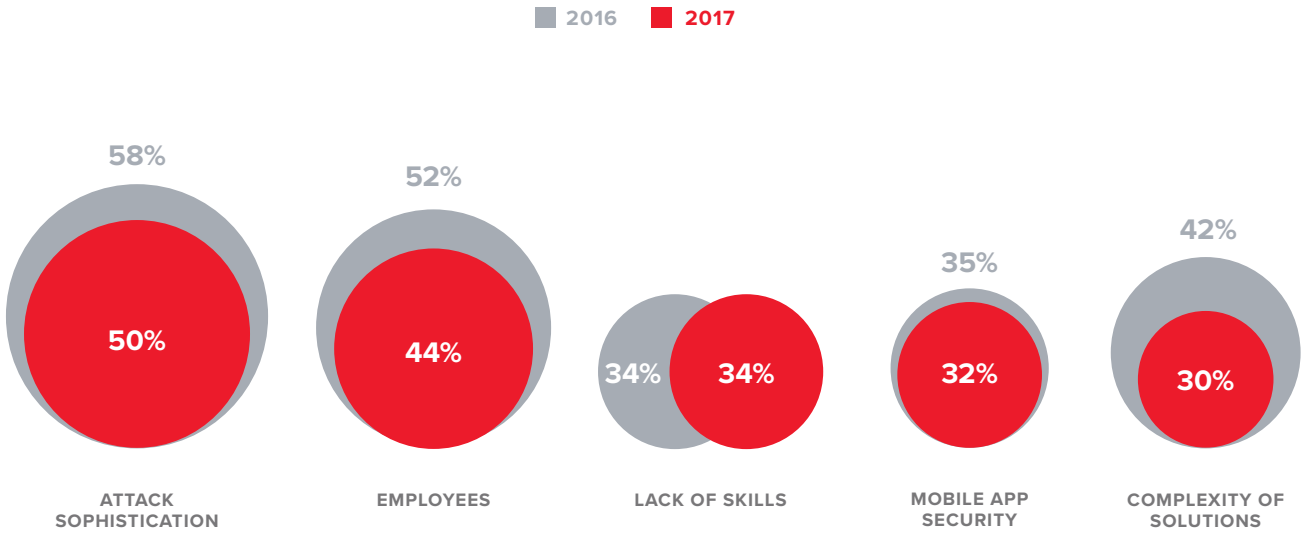
KEY FINDING

03

Deployments of security application services grow more sophisticated.

As attacks on applications become ever more complex, organizations are responding by redrawing the traditional perimeter to encompass the new reality of users accessing applications from anywhere, at any time, and from any device. There's a focus on a holistic approach to application security that protects the app from DDoS and DNS attacks and defends the company from fraud, as well as mitigates traditional application security flaws. We asked survey participants about their strategies to defeat emerging threats, secure their applications, and protect their data.

Top security challenges



The security landscape today

The increasing sophistication of attacks remained the top security challenge in the next 12 months for respondents (50 percent), with employees' understanding of the importance of security policies next at 44 percent, and the security skills gap at 34 percent. Interestingly, this is an improvement over 2016 when attack sophistication was cited as the top challenge for 58 percent of respondents and employee understanding was second. Only the skills gap remained unchanged from 2016 to 2017, which illustrates a continuing challenge for organizations.

We've seen increases in preferences for managed/as-a-service offerings with respect to security (DDoS, WAF, etc.), which likely arise as a result of organizations' inability to find staff to address security struggles. All other challenges saw reductions, including budgetary concerns, which dropped from 41 percent in 2016 to 30 percent in 2017. We suspect that this is due to security budgets rising across industries as the importance of securing data and applications becomes more critical to the success of the business.

Security reactions to external pressure

The devastating consequences of security breaches seem to be reflected in the plans for security service

deployments over the next 12 months. DDoS, WAF, and anti-fraud protection—all of which help ensure the availability and protection of corporate and consumer data—topped the list of planned deployments. Given the number and frequency of high-profile breaches during past two years, it is understandable that organizations would turn to those app services able to help them make applications safer through smarter security and deployment models.

For example, 25 percent of respondents preferred to deploy DDoS protection/mitigation as a service. This deployment model not only serves to address the security skills gap currently plaguing the entire industry by providing expert, managed security services, but further expands protection to applications deployed off premises in public, private, and colocation environments. That protection is increasingly important given that the majority of organizations (4 in 5) are operating in a hybrid cloud model, and 20 percent plan on delivering more than half of their applications from the cloud by 2017. Both WAF and anti-fraud services saw 5 percent gains in preferences for public cloud deployment.

The deployment of app-centric security services like WAF, anti-fraud, and DDoS protection on premises for applications deployed off premises is not architecturally optimal. We expect we will continue to see a rise in deployment of security-related app services in public clouds and managed/as-a-service offerings as organizations continue to develop apps for and migrate apps to the public cloud.

App services boost confidence

Confidence in withstanding an application-layer attack overall remained fairly high this year. Nearly half (45 percent) of all respondents were “confident to very confident” in their organization’s readiness to withstand such an attack. Only 17 percent were “not at all or less confident.”

Real differences began to appear when we dug into security practices with respect to app services. Among those organizations with a WAF deployed today, confidence was much higher (53 percent) than those without a WAF deployed today (32 percent). Similarly, only 11 percent of those with a WAF deployed today were less confident in their ability to mitigate an attack, whereas 25 percent among those who did not have a WAF deployed today were less confident.

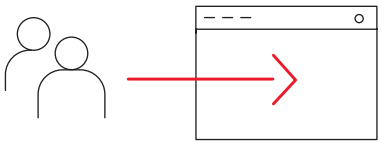
Confidence levels were similar when viewed against organizations with/without DDoS protection deployed today. Those with DDoS protection were more likely to feel somewhat/very confident in their ability to withstand an application layer attack (43 percent) versus less/not at all confident (11 percent). Of those without DDoS protection deployed today, 35 percent were somewhat/very confident while those less/not at all confident more than doubled to 24 percent.

Similarly, the level of protection afforded applications impacts corporate confidence in withstanding an attack. Of the three primary app attack surfaces (request, response, client), confidence was highest among those who always protect all three surfaces

When a WAF is deployed, 53% are confident in their ability to withstand an attack

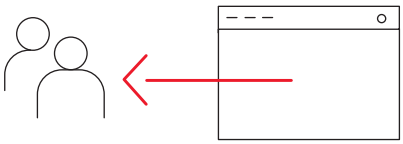
When DDoS protection is deployed, 43% are confident in their ability to withstand an attack

Respondents who always protect all three primary attack surfaces are most confident



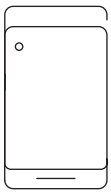
69%

Request



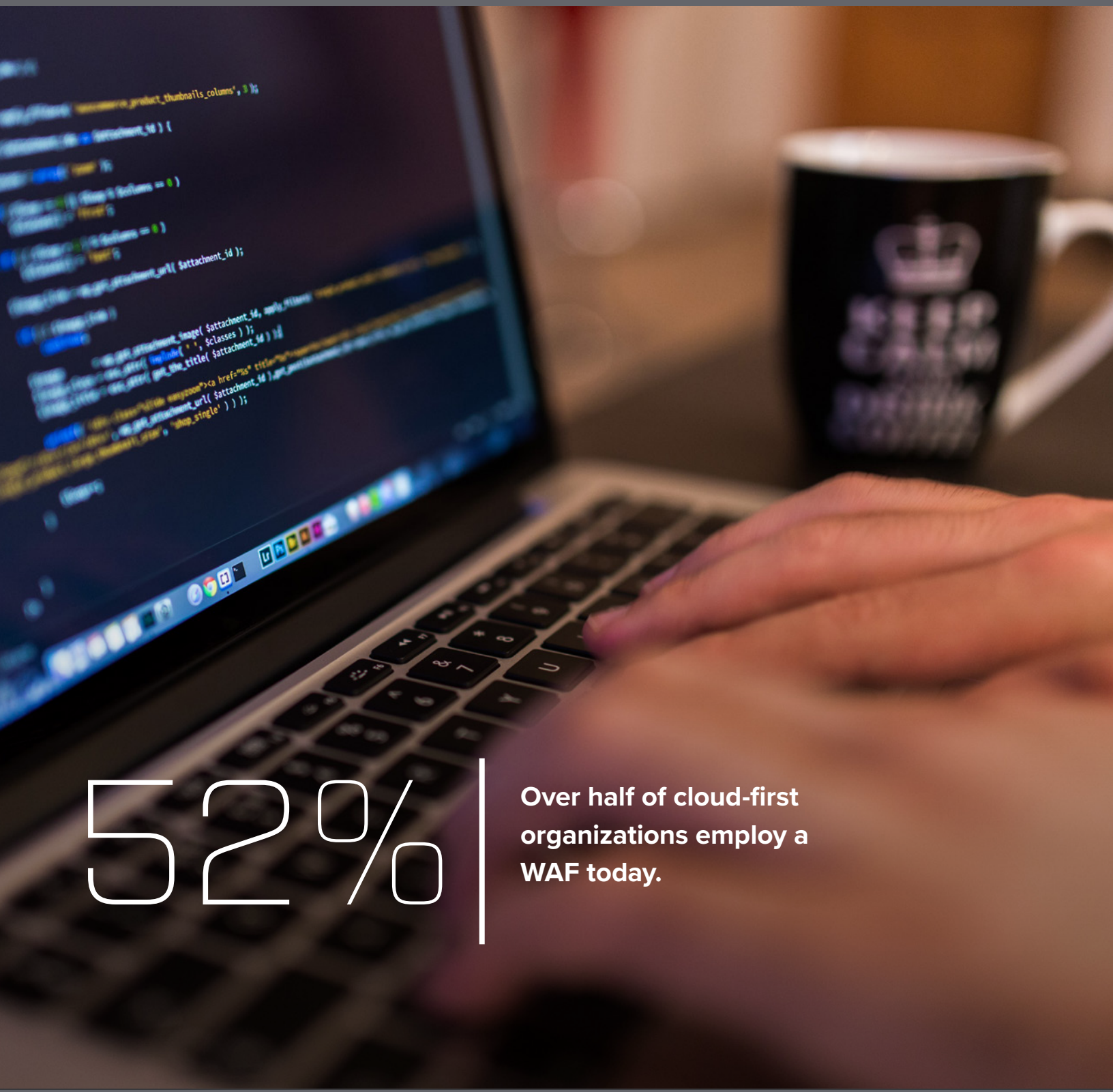
63%

Response



68%

Client



52%

Over half of cloud-first organizations employ a WAF today.

against exploitation and attack. Those with lower confidence were found to always protect surfaces half as often, with only 33 percent protecting inbound (request), and even fewer (29 percent) protecting outbound (response). Appropriately, perhaps, those with lower confidence were twice as likely to never protect surfaces.

Cloud-first security

An interesting thing happened on the way to the cloud. In spite of security being regularly cited as a risk that hinders cloud adoption, organizations employing a cloud-first strategy (47 percent) had more confidence in their ability to withstand an application-layer attack than those without, by a margin of nearly 10 percent. Digging in deeper, we found that over half (52 percent) of cloud-first organizations employ a WAF today. Conversely, only 45 percent of those that do not identify as a cloud-first organization do so.

We suspect that the difference in confidence may be related to the WAF deployment status given the impact it appears to have on confidence in general. The stronger use of a WAF with cloud-first organizations may also be the result of fewer traditional network security services available in public cloud environments. WAFs are readily available in a wide variety of cloud environments today, and may be seen as the most viable option for protecting applications when moving to the cloud.

F5 INSIGHTS FOR KEY FINDING 03

Attacks continue to grow in sophistication and size, but organizations are also evolving their strategies to address the security of their applications. With security budgets rising in the wake of public attacks, DDoS mitigation solutions, WAFs, and anti-fraud protection are among the top app services that organizations plan to deploy over the next 12 months. Respondents who have a WAF and DDoS protection solutions currently deployed—as well as those identifying themselves as representing cloud-first organizations—tend to feel more confident in their ability to withstand application-layer attacks.

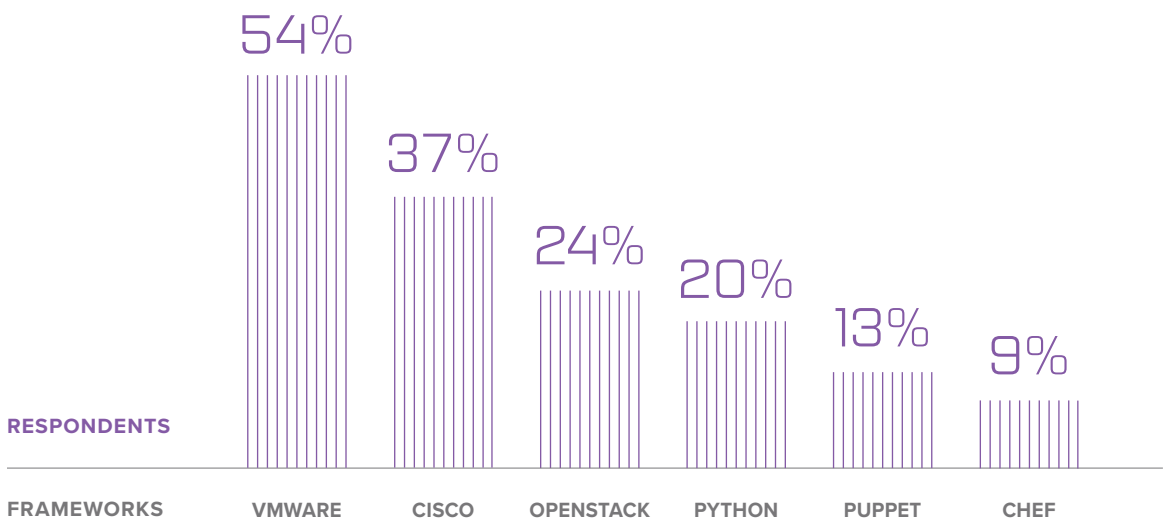
KEY FINDING

04

Operational benefits have become the main attraction for DevOps and programmability.

As the pressure to deliver more apps more frequently increases, some organizations are finding their answers in a move toward more automation and orchestration. We asked survey participants what, if any, strategic impact the DevOps methodology had on their organizations, including what the top drivers were for the use of frameworks, and the level of importance placed on a programmable infrastructure. The answers were somewhat surprising, as the majority of organizations still don't see DevOps as having a strategic impact, despite their widespread adoption of its aspects of automation and orchestration.

Frameworks in use and planned for use



DevOps and the use of frameworks

The number of respondents using at least one framework doubled over 2016, moving from around 20 percent to nearly 50 percent. Accordingly, frameworks saw gains in adoption—some significantly so—over 2016. Interestingly, overall, DevOps was selected as having strategic impact by just 20 percent of respondents. Among those in executive roles, DevOps was identified by only 17 percent, well below front-running SaaS (42 percent), big data (41 percent), and public cloud (IaaS) (39 percent). Among those identifying as having DevOps and cloud-related roles, DevOps took third place with 39 percent behind SaaS (44 percent) and big data (42 percent). This is in spite of evidence that organizations are engaging in at least the automation and orchestration aspects of DevOps.

We've also noted changes in the number of frameworks in use year over year. The increase in those using only one framework seems indicative of a move toward standardization, which is an important step toward automating and orchestrating processes with greater speed and success.

It is, however, interesting to note the slight increase in the average number of frameworks in use when viewed against number of applications deployed. There appears to be a definite trend toward

greater variety in framework use as the number of applications in production grows. We suspect this is a result of the reality of mergers and acquisitions and divisions across lines of business where different groups are responsible for different applications and environments and have settled on dissimilar frameworks for automation and orchestration.

Of those relying on only one framework, 47 percent were using VMware, 26 percent Cisco, 9 percent OpenStack, and 7 percent Puppet. Interestingly, Python scripts—which point to a roll-your-own approach to automation and orchestration—were the only technology in use by 7 percent of respondents.

Across industries, Cisco and Puppet's biggest users came from financial services/insurance organizations. OpenStack's came from technology and telecommunications, while VMware use was strong in technology firms.

The driving need for automation

A closer examination of the reasons behind respondents' use of frameworks provides some insight into the nature of how they view DevOps.

Overwhelmingly, use of automation and orchestration frameworks was driven by scalability needs and reduction of OpEx. Contrary to the overriding mantra of time to market being a critical force for DevOps adoption, very few respondents viewed their use of these frameworks as being driven by the need to improve this measure. Neither scalability nor OpEx savings are strategic in nature; instead, the use of frameworks to achieve these goals is a tactical response, which may explain why so few organizations view the adoption of DevOps principles as strategic.

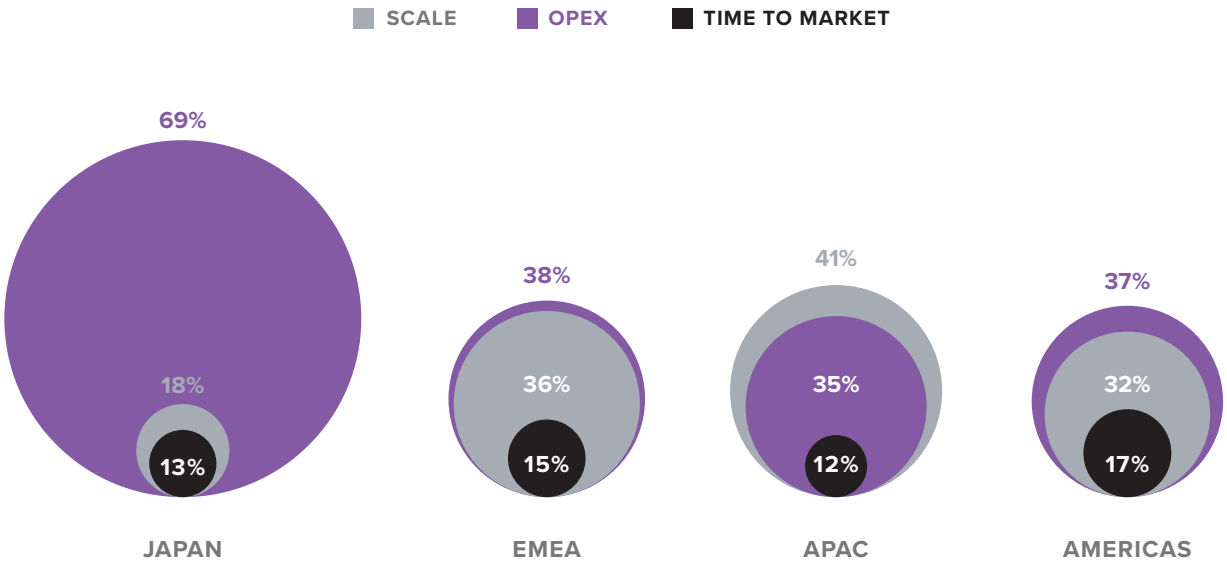
These drivers were also closely reflected in responses regarding complementary software-defined networking (SDN), in which the overwhelming driver for adoption is reducing OpEx (62 percent) followed by a reduction in CapEx (36 percent), and, finally, improving time to market (33 percent). Thirty-seven percent of respondents were looking to automate configuration of the network with SDN, and 29 percent hoped to enable agile network provisioning.

The importance of programmable infrastructure

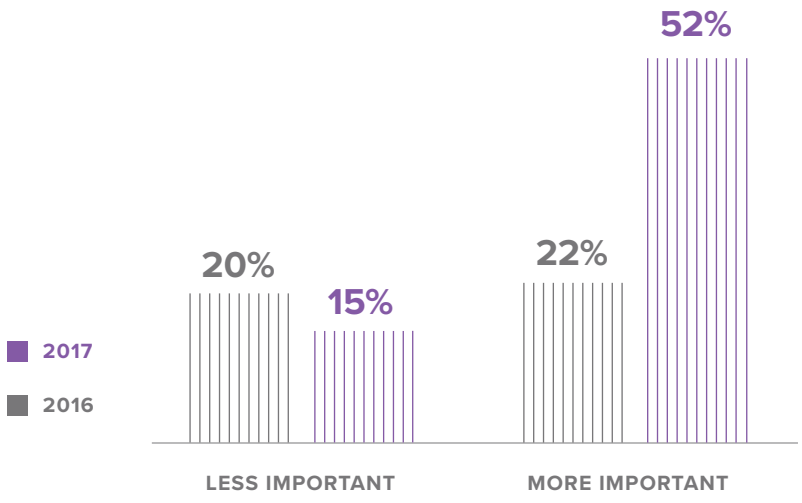
It should be no surprise that as automation and orchestration become more prevalent in organizations, programmability—which enables automation and orchestration—would also rise in importance. Lacking an API-enabled infrastructure, automation and orchestration are incredibly difficult to achieve with the same diversity of tools and technologies with which organizations approach these efforts today. Indeed, APIs are the means by which organizations seize the freedom to choose their own path toward a more automated and efficient data center. Without them, organizations are forced to select solutions from a limited set of pre-existing integrations.

There were some differences in the overall importance placed on APIs and templates based on the form factor of appliances preferred by

Framework drivers by region



52% of companies think templates are important in 2017–up 30 percentage points from 2016



62%

Sixty-two percent of respondents view the reduction of OpEx as the overwhelming driver for adopting SDN.

respondents. For example, among those who preferred containers or virtual machines for app services, 60 percent considered APIs highly important. Of those who preferred hardware only, that number dropped to 50 percent.

The difference with regard to templates was even more striking, with 67 percent of respondents who prefer container or virtual app service form factors tagging them as highly important. Only 53 percent of those who prefer hardware-only deployments considered templates as highly important. Framework use appears to have little impact on the importance placed on APIs and templates. OpenStack users were more likely to place high importance on templates (65 percent) and APIs (63 percent) than other framework users, likely because of the nature of the open-source solution and its high reliance APIs and templates to provide the broadest support possible.

F5 INSIGHTS FOR KEY FINDING 04

Despite being traditionally tied to increased speed to market, the key drivers for the use of DevOps-related frameworks and toolsets remain scalability and reduction of operational expenses. As organizations continue to focus on automation and orchestration, programmability becomes even more important, especially for respondents who use containers or virtual machines for app services.

Conclusion

As the digital economy matures, organizations rely on applications to bring innovation to life. The results of the 2017 State of Application Delivery survey demonstrate that application services will continue to be a vital link enabling IT organizations to respond faster, smarter, and safer to the needs of the business.

Respondents to our third annual survey reinforced the dominance of cloud as a response to the increasing pressure of digital transformation. Organizations continue to embrace a variety of cloud deployment models and show similar preference to deploy app services in those environments to address their challenges with security and performance. The strong preferences for those cloud models that offer the right mix of control and choice—private and colocation models—indicate organizations are strongly invested in the promise of cloud as a model, and they are unwilling to sacrifice the control required to enforce compliance with corporate and regulatory security policies. As public cloud continues to expand its ability to address these concerns, we anticipate higher rates of migration and adoption.

With security and cloud-related skills in high demand and short supply, organizations are turning to automation and orchestration as well as service-based offerings to address security and scalability. The efficiencies achieved by leveraging DevOps and SDN-related technologies support respondents' need to reduce operational costs, and we anticipate that will drive sustained growth in both the adoption of and importance placed on APIs and templates in the coming year.

As organizations push forward with digital transformation efforts, app services will continue to provide the security, performance, and availability apps need to meet the expectations of businesses and consumers alike. Whether deployed on-premises or off, in cloud environments or as a service, app services continue to aid in delivering the profit and productivity gains business seeks to achieve in the digital economy.

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-105658244