THE STATE OF APPLICATION DELIVERY

2016 REPORT

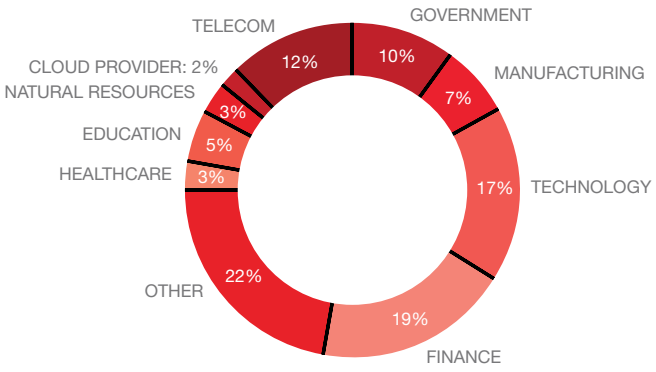
LOAD BALANCING
GLOBAL SERVER LOAD BALANCING
DNS
DDOS PROTECTION/MITIGATION
WEB APP FIREWALL
INTRUSION DETECTION/PROTECTION SYSTEM
ANTI-VIRUS
ANTI-FRAUD
ANTI-SPAM
DNSSEC
NETWORK FIREWALL
SSL VPN
IDENTITY FEDERATION
APPLICATION ACCESS CONTROL
SECURE WEB GATEWAY SERVICE
SINGLE SIGN-ON
APPLICATION ACCELERATION
COMPRESSION
SSL/TLS OFFLOAD
CACHING
TCP OPTIMIZATION
WAN OPTIMIZATION
ENDPOINT SECURITY
VIRTUAL DESKTOP INFRASTRUCTURE

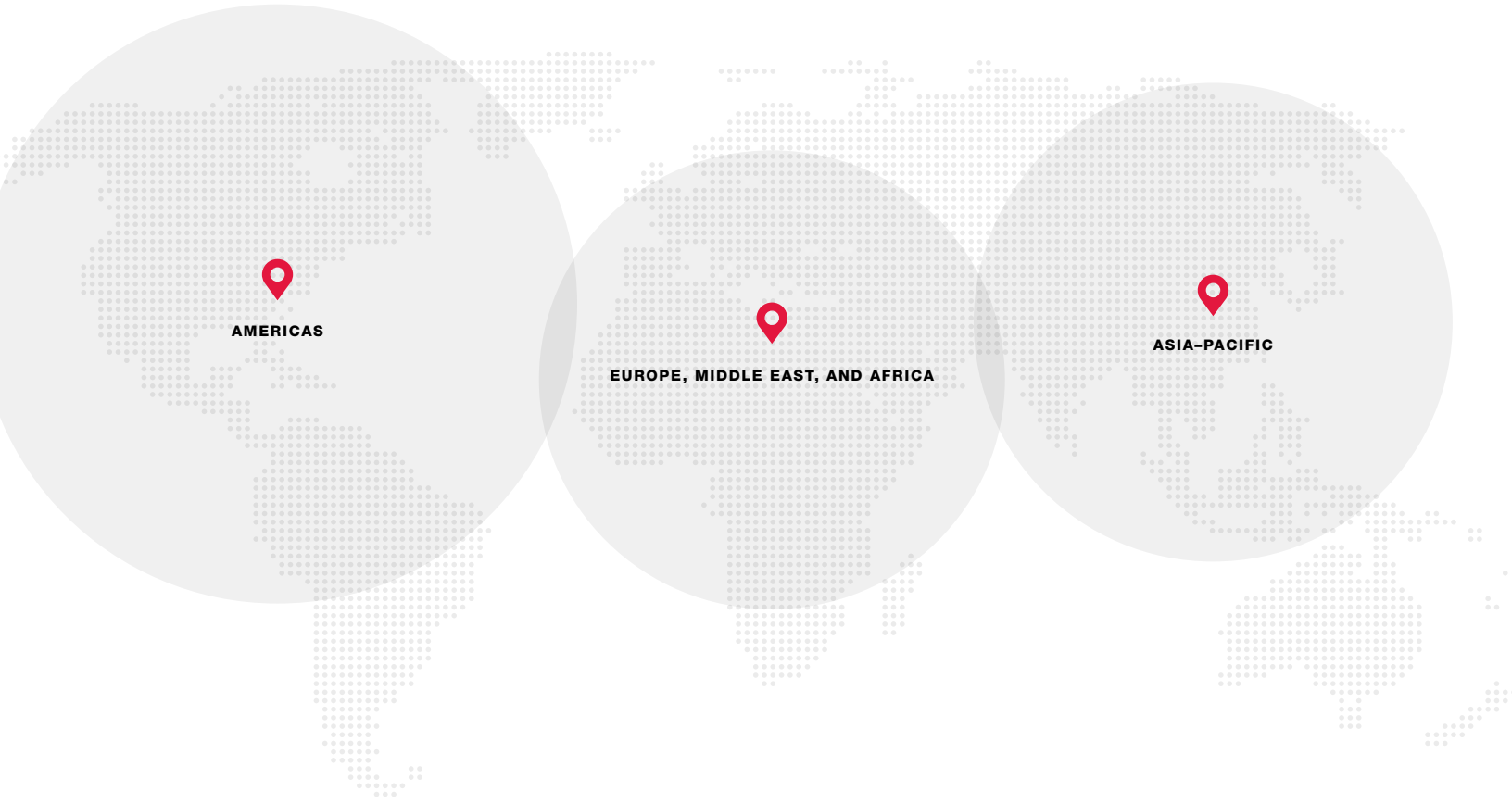
WHAT'S INSIDE

2016 SURVEY DEMOGRAPHICS

3,002

TOTAL RESPONDENTS





FROM THE CTO

In 2014, 300 of our customers in North America took part in a survey to help us understand the "state of application delivery." We wanted to know how emerging trends and technologies were affecting our customers' ability to deliver critical enterprise applications successfully. The results were published in our first State of Application Delivery report in January 2015. Little did we realize the amount of exposure, interest, and discussion this report would generate—so much so that we decided to make it an annual survey.

In 2015, we expanded the scope of participants to include customers throughout the globe. More than 3,000 people participated, giving us better worldwide insight into our customers' current practices and most pressing challenges, as well as their predictions and hopes for the future.

Although this year's broader global participation makes it difficult to draw direct comparisons to last year's data, it provides an opportunity for you to learn how your peers are handling some of the same complex challenges you and your organization face. We hope you'll find this year's report just as illuminating and useful as last year's as you plan for 2016 and beyond.

A sincere thank you to all of our customers for their generous participation.

Karl Triebes

Chief Technical Officer
and Executive Vice President of Product Development
F5

2016 KEY FINDINGS

KEY FINDING

01

APPLICATION SERVICES ARE ESSENTIAL AND PERVASIVE

Ten or more application services are used by well over half of respondents, who recognize that slow, unresponsive, and unsecured applications can have a substantial negative impact on revenue and operations.

KEY FINDING

02

HYBRID CLOUD IS THE NEW NORMAL

The vast majority of respondents (81%) are moving toward hybrid cloud environments to leverage the flexibility and potential cost savings it offers, especially for small and mid-sized organizations.

KEY FINDING

03

TODAY'S MOST VALUED SECURITY SOLUTIONS FOCUS ON PROTECTING USERS, DATA, AND APPLICATIONS

Security professionals who have the highest level of confidence in their ability to ward off attacks are protecting clients, requests, and responses—the critical points at which data can be easily compromised.

KEY FINDING

04

DEVOPS AND SDN ARE KEY TO IMPROVING OPERATIONAL EFFICIENCY

Because DevOps and software-defined networking (SDN) enable automation and orchestration, they are both seen as key factors for reducing operating costs and improving time to market.

INTRODUCTION

Twenty-five years ago, applications were monolithic software programs that ran in huge data centers and were used by the select few. Today, with the Internet and mobile devices—and increasingly, the Internet of Things—having transformed our lives, applications are everywhere and used by nearly everyone. Your business is driven by them, your customers connect with you through them, and your employees can't do their jobs without them.

Because we rely on them so heavily, applications must be available when we need them, able to respond within a split second to meet our demands, and secure enough to protect our confidential information.

To do that, applications need services. Without them, they are like cars without fuel, banks without vaults, and passports without pictures. Services do things like improve availability and performance to ensure that applications are always accessible and performing as users expect. They also help you protect your network, systems, users, devices, and confidential information, and give you the control you need to decide which applications users can access.

For this survey, we asked F5 customers to tell us about the number and types of applications and services they're using, what their greatest challenges are in delivering them, which services they need more of, and which ones they plan to deploy in the future. We also asked about trends in cloud, software-defined networking (SDN), and DevOps, and how these trends are changing their approach to IT.

Participants included F5 customers in the Americas (AMER), Europe, the Middle East, and Africa (EMEA), and Asia-Pacific (APAC) regions. Across industries, the broadest participation was among finance, technology, and telecom companies as well as government entities. By role, respondents included infrastructure architects, network managers, directors or vice presidents of IT, and security engineers, although application architects, developers, and managers as well as security architects and managers were also represented.

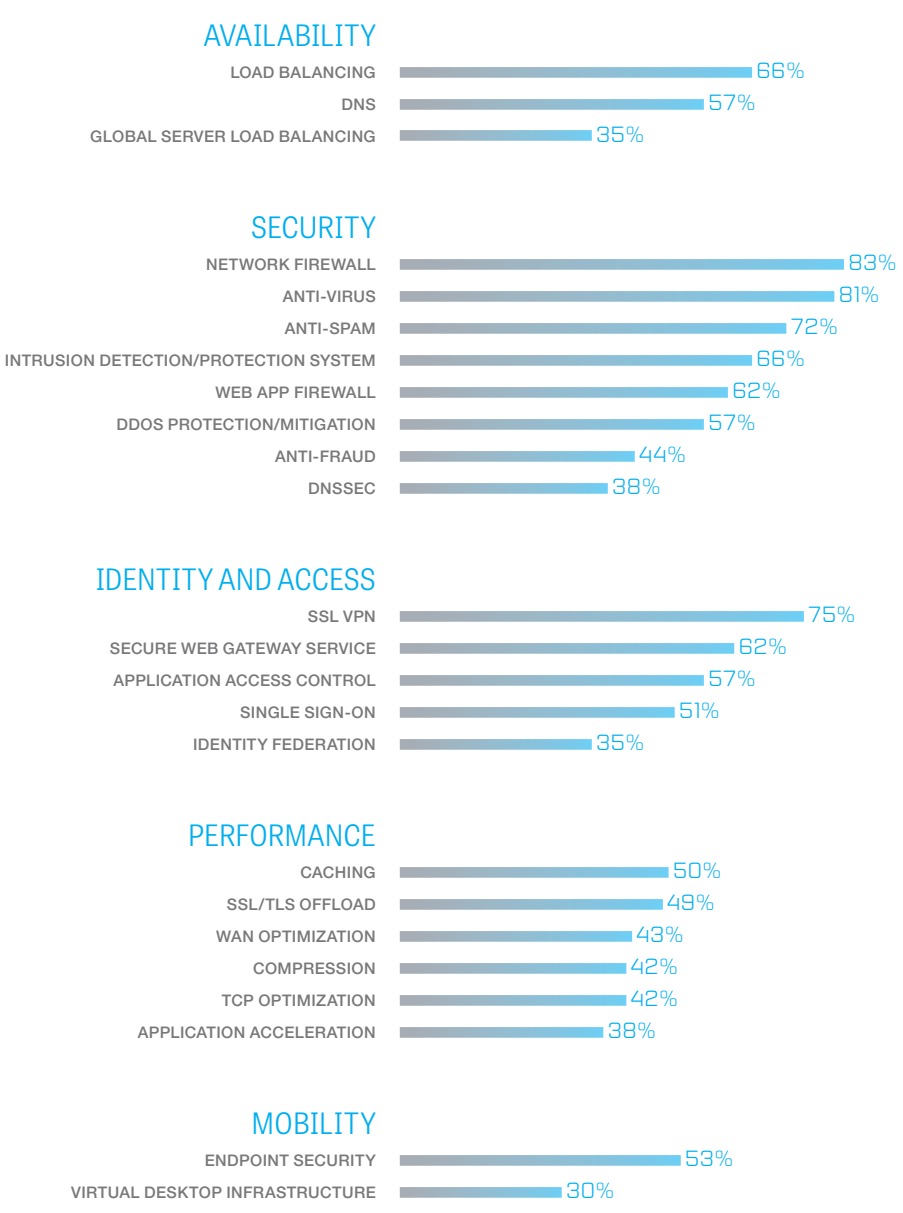
KEY FINDING

01

APPLICATION SERVICES ARE ESSENTIAL AND PERVASIVE

Application services are what make applications viable and useful, and that fact seems to be virtually undisputed by IT leaders as well as network and security professionals. We asked participants about numerous application services in five major categories: security, identity and access, availability, performance, and mobility. We were surprised to learn that as many as 30 percent of respondents use all 24 of the application services we asked about. Twice that number (60 percent) use 10 or more services, and all respondents use at least one. These numbers indicate not only how ubiquitous application services are but also how essential most respondents consider them to be.

Application services currently deployed



30% of respondents use all 24 of the application services we asked about.

60% use 10 or more of the services.

All respondents use at least one application service.

4/5

FOUR OUT OF THE TOP FIVE APPLICATION SERVICES MOST WIDELY DEPLOYED WERE SECURITY SERVICES.

83%

Network Firewall

83 percent of respondents employ a network firewall to stop illegitimate traffic from entering the network.

81%

Anti-Virus Solutions

81 percent use anti-virus solutions to detect and remove malicious software that enters the network uninvited.

75%

SSL VPN

75 percent use SSL VPN, giving users private, protected access to applications over public (usually Internet) networks.

72%

Anti-Spam

72 percent use anti-spam solutions to detect and stop unsolicited email.

SECURITY SERVICES TAKE CENTER STAGE

Security services were the most widely deployed of all types of application services. This isn't surprising, given the staggering increase in security threats and the growing number of ways in which confidential information can be compromised.

Eighty-three percent of respondents employ a network firewall to stop illegitimate traffic from entering the network, and almost as many (81 percent) employ anti-virus solutions to detect and remove malicious software that enters the network uninvited. Three-quarters of respondents also use SSL VPN, giving users private, protected access to applications over public (usually Internet) networks. And, 72 percent use anti-spam solutions to detect and stop unsolicited email. With these high percentages, organizations have clearly made it a priority to protect their resources, users, and data. Not far behind this array of security services, load balancing, which optimally distributes application load across multiple servers, was the fifth most commonly deployed application service.

While this data indicates which application services respondents currently have deployed, we also wanted to know which services they wouldn't consider deploying an application without. This question offers a slightly different perspective, indicating which services respondents consider most important—even essential—versus those they happen to be using already.

Consistent with last year's results, availability and security tied for the top spot at 32 percent. Organizations realize that all other application services have limited value if the application itself isn't available to users when they need it.

Applications that aren't available have a direct and immediate impact on employee productivity as well as customer engagement. Ensuring that applications are available depends in great part on the ability to intelligently manage application traffic (both locally and globally) and especially the Domain Name System (DNS), the Internet's "look-up" service that directs user requests to the correct web sites and applications.

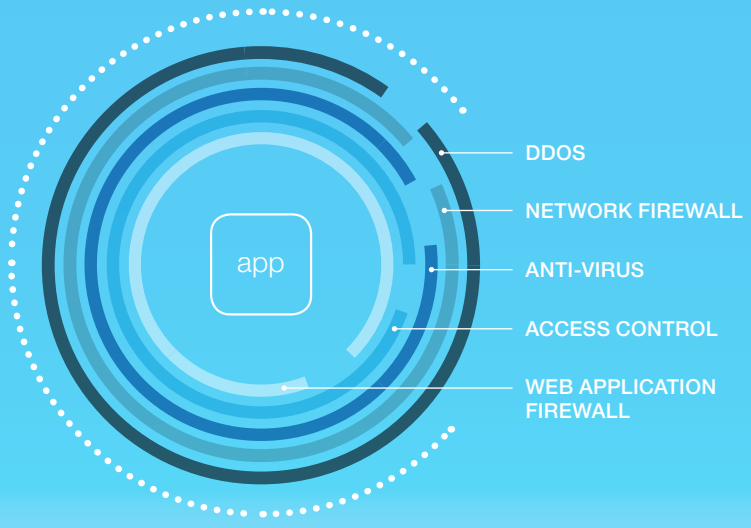
When it comes to security services, respondents named web application firewall, access control, anti-virus, network firewall, and distributed denial-of-service (DDoS) as those services they wouldn't deploy an application without. So, even though most organizations are already using multiple security solutions, given the opportunity, they would prefer to deploy new applications with an even broader range of security services.

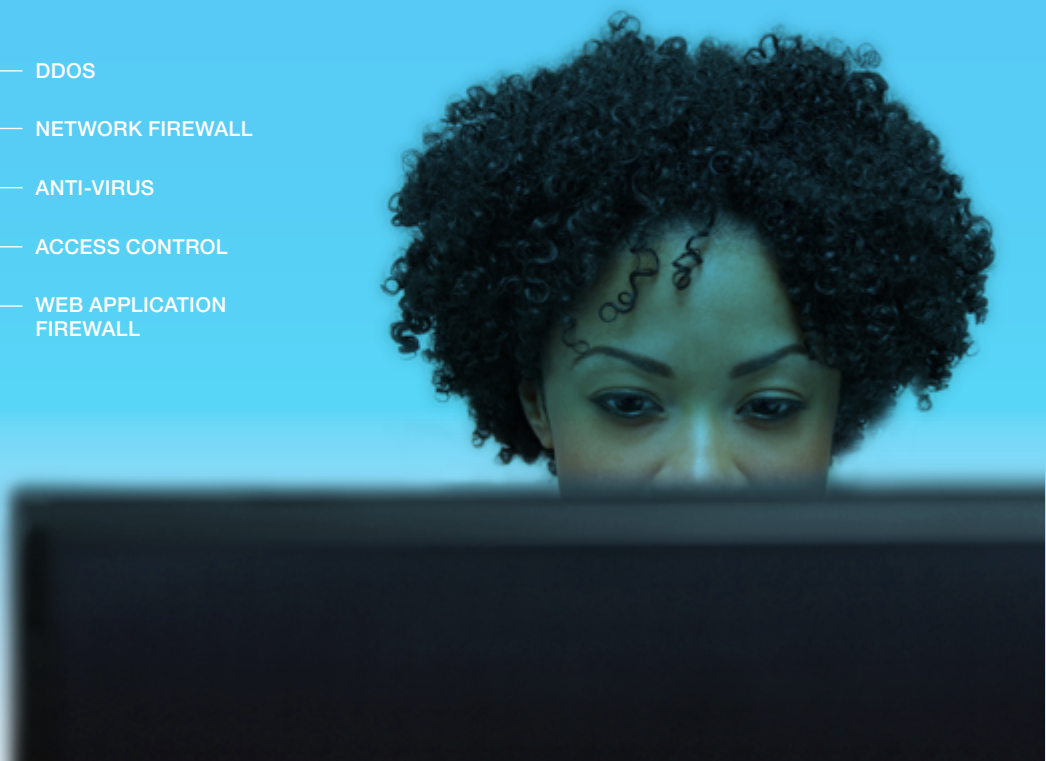
We were also curious which services respondents valued the most relative to network security, so we asked which services they would be willing to give up if it made their network more secure. Here, availability and performance were clearly paramount as only a very small percentage of respondents (4 percent and 8 percent respectively) was willing to forego these services in exchange for better security. Respondents were also reluctant to let go of programmability, the ability to change the behavior of application services using software. Programmability is an essential component of SDN and DevOps, and only 12 percent were willing to give this up for better security. Elasticity—the ability to scale up and down—was also highly valued, with only 16 percent of respondents willing to sacrifice this service.

Application services participants plan to implement in 2016

26%	26%	24%	24%	24%
DNSSEC	IDENTITY FEDERATION	GLOBAL SERVER LOAD BALANCING	SINGLE SIGN-ON	VIRTUAL DESKTOP INFRASTRUCTURE

Security services respondents wouldn't deploy an application without





The surprise answer to our "tradeoff for better security" question was ease of management, which 20 percent of participants said they *would* be willing to give up. We suspect the reason for this is that security concerns have risen to the very highest levels of the organization. The board of directors, chief executive officer, and IT organization are willing to accept some level of management complexity as long the company stays out of the headlines and both corporate and customer data are kept secure.

FASTEST GROWING SERVICES IN 2016

Finally, we wanted to know which services participants anticipate implementing in 2016. Twenty-six percent said they plan next year to deploy DNSSEC. The same number cited identify federation services, which lets IT maintain control of users' credentials when they access cloud-based applications. Nearly one quarter of respondents also plan to deploy virtual desktop infrastructure (VDI), single sign-on, and global server load balancing solutions. The nature of these services points to organizations moving toward a world of hybrid cloud or "multi cloud"—any combination of on-premises and cloud deployment models across one or more cloud architectures and providers.

F5 INSIGHT FOR KEY FINDING 01

The fact that organizations are continuing to deploy a greater number of application services every year indicates how vital they consider these services to be. Respondents' strong interest in availability and data integrity services points to the high priority they place on employee productivity and security. Services that directly support these priorities are powerful business drivers for lowering costs and increasing margins and therefore deliver the most value to the organization.

KEY FINDING

02

HYBRID CLOUD IS THE NEW NORMAL

The cloud clearly “arrived” as a viable and desirable deployment model in 2015—and it comes in many forms. Last year, 20 percent of North American respondents said they had a “cloud first” strategy, meaning their organizations are required to evaluate cloud-based IT solutions before making new IT investments. This year, that number jumped to 29 percent in North America, which reflects the trends we are witnessing worldwide. In fact, 42 percent of respondents in Asia-Pacific reported a strong preference for cloud first.

These three cloud operating models were identified as "strategically important"

43%

PRIVATE CLOUD consists of cloud infrastructure provisioned for exclusive use by a single organization.

40%

SOFTWARE AS A SERVICE (SaaS) enables an organization to use a cloud provider's applications on a pay-for-use basis. Office 365 and Salesforce are examples.

34%

PUBLIC CLOUD, also known as Infrastructure as a Service (IaaS), is provisioned for open use by the general public. Examples include AWS and Azure.

Three cloud operating models stood out as having strategic importance in the next two to five years: private cloud at 43 percent, Software as a Service (SaaS) at 40 percent, and public cloud at 34 percent.

We believe this environment of multi-clouds is emerging because business benefits are figuring heavily into IT's decisions about where best to locate applications and services. As an example, line of business owners are eagerly adopting SaaS alternatives over traditional on-premises solutions for functions like workforce, expense, and customer relationship management. Taking advantage of proven SaaS applications offloads IT and lets the business leverage subscription-based expense models. Likewise, specialty and short-lived applications (like those created for the Olympics or the soccer World Cup) require global access, mobility, and speed. In this case, public cloud, which offers agility and on-demand scalability, can be the best option. In contrast, for applications that have a high risk profile or are critical to a company's competitive advantage, private cloud is likely still the best option since it allows IT to maintain full custody and control of policies and data.

81%

RESPONDENTS PLANNING TO OPERATE IN A HYBRID ENVIRONMENT

One out of five respondents plan to migrate over half of their applications to the cloud.

Application services most likely to be deployed in a managed cloud

32% DDOS PROTECTION

29% ANTI-SPAM

28% GLOBAL SERVER LOAD BALANCING

27% DNSSEC

25% IDENTITY FEDERATION

One out of five survey respondents says they plan to migrate over half of their applications to the cloud while keeping the remainder on premises. And, when asked specifically about hybrid cloud—that is, any combination of public and private cloud infrastructures—as many as 81 percent of respondents say they plan to operate in this type of environment.

NO SINGLE HYBRID CHALLENGE IS UNIVERSAL

We asked participants what challenges they face as they adopt hybrid cloud. No single challenge affected a majority of respondents. Twenty-eight percent said they don't have the analytics to understand when it's most cost-effective to deploy applications in the cloud versus the data center. Slightly more (29 percent) said they haven't found a comprehensive identity and access management (IAM) solution. This challenge is especially important to solve because IAM solutions are essential to supporting a mobile workforce, the growing number of mobile applications, and the increasing use of cloud-based and SaaS applications. Only about one-sixth of respondents cited data security and application performance as hybrid cloud challenges.

APPLICATION SERVICES EMERGE IN THE MANAGED CLOUD

We're seeing the beginnings of a new trend, with a growing number of organizations showing an interest in deploying application services "as a service" in a managed, off-premises, subscription-based model. The most likely services to be deployed in a managed cloud were security-related, with distributed denial-of-service (DDoS) protection at 32 percent, anti-spam at 29 percent, and DNSSEC at 27 percent. Global server load balancing (28 percent) and identity federation (25 percent) completed the top five.

We think there are several reasons for this emerging trend toward managed cloud security services. One is the current talent shortage in information security, which prevents many organizations from adequately staffing on-premises data centers. Another is that many organizations don't have the on-premises resources to handle high-volume attacks. For those that do, the resources they need are costly and often underutilized, sitting idle when not under attack. And finally, organizations recognize that they must protect applications deployed in public clouds, particularly when they span multiple geographic locations.

F5 INSIGHT FOR KEY FINDING 02

Until recently, only the very largest enterprises could afford to build multiple data centers around the globe to make applications and data available to users everywhere. Cloud (in its many forms) introduces a whole new world of opportunities for small and mid-sized organizations, who can now enjoy the same kind of worldwide presence without sacrificing security and other critical services or incurring high infrastructure costs.

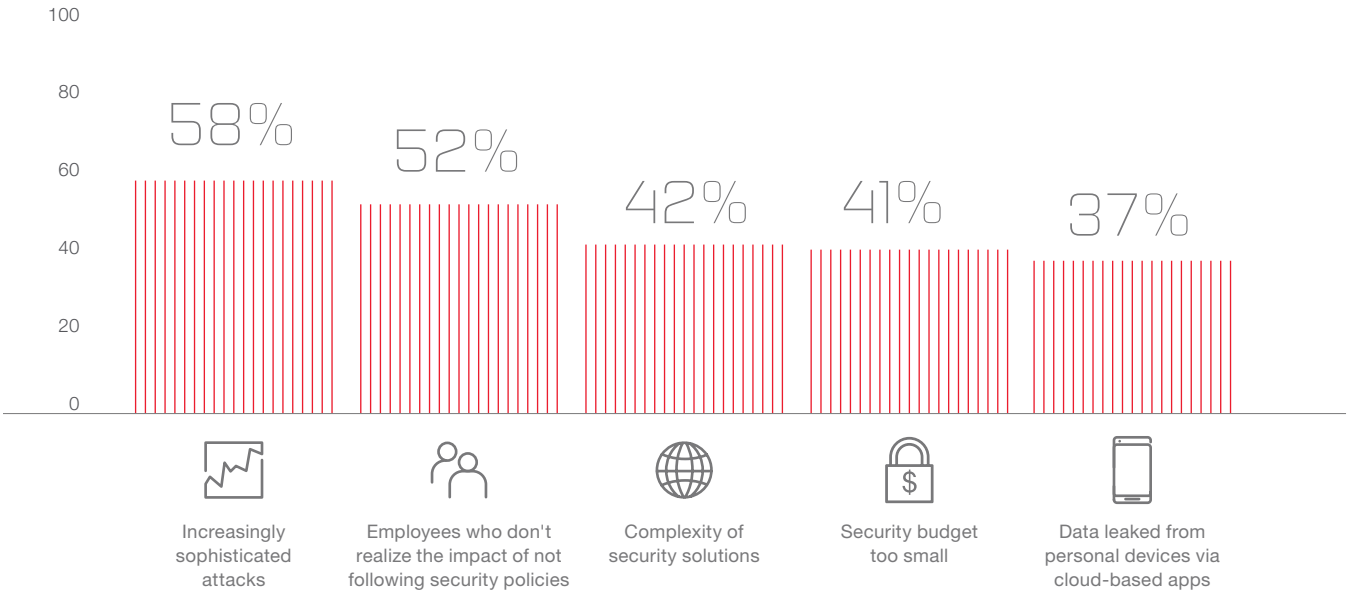
KEY FINDING

03

TODAY'S MOST VALUED SECURITY SOLUTIONS FOCUS ON PROTECTING USERS, DATA, AND APPLICATIONS

With security breaches in the news daily, it's no wonder that security remains a critical concern for most organizations. We wanted to know more specifically which types of concerns are keeping our customers up at night, so we asked them to rate their top five security challenges. The most frequent response (at 58 percent) was fear over the increasing sophistication of attacks. As many as 42 percent were also apprehensive about the growing complexity of security solutions.

Top 5 security challenges respondents face



Just as important, organizations are beginning to recognize that security is no longer just a technical issue. It has quickly risen to the level of business and operations, as evidenced by more than a handful of C-level executives losing their jobs over massive data breaches.

This shift away from strictly technical concerns is reflected in the fact that two of the top five security challenges focused on employees. More than half of respondents (52 percent) believe that employees underestimate the impact of not following security policies, which can expose the organization to potentially catastrophic vulnerabilities. Another 37 percent expressed concern about employees leaking confidential data while using cloud-based applications on their personal devices. This underscores the importance of applying protection where it's needed the most: with users, data, and applications. Budget was also a big concern, with 41 percent of respondents fearing that their IT budgets are too small for them to acquire the solutions they need to fend off attacks.

BROAD PROTECTION BOOSTS SECURITY CONFIDENCE

Remarkably, despite the growing sophistication of attacks, 85 percent of organizations are confident to highly confident that, in their current state, they can fend off application-layer attacks. This was especially true among the 67 percent of respondents who are using a web application firewall, which protects web-based applications and enables organizations to comply with regulatory requirements.

What would it take for participants to adopt cloud?

71 percent of respondents want data at rest (that is, data stored in the cloud) to be encrypted.

51 percent of participants want data in flight (that is, in transit across the Internet) to be encrypted.

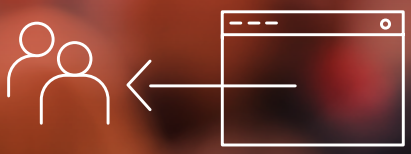
Participants who were most confident in their ability to withstand an attack protect multiple attack surfaces

57%

Client

53%

Request



44%

Response

In general, the level of confidence expressed by participants to withstand an attack correlates to the number of "attack surfaces"—the critical points at which data can be easily compromised—that organizations are protecting. In this context, attack surfaces refer to clients (such as smartphones), requests, and responses. Examples of protection include inspecting a smartphone for malware, preventing a request from being tampered with in order to extract data without authorization, and encrypting credit card information in a server response to safeguard a user's privacy. Participants who were most confident in their ability to withstand an attack were more consistent about protecting all three of these attack surfaces. Those who were less confident were more likely to respond "never" when asked about protecting clients, requests, and responses.

SECURITY CONCERNS HAMPERING CLOUD ADOPTION

When it comes to cloud specifically, we asked respondents which services were most important in order for them to move to the cloud. The highest number of responses concerned security or, more precisely, data encryption. With record amounts of confidential personal and corporate data now traversing the Internet, the idea of encrypting all Internet traffic by default was popular in 2015. Nearly three-quarters of survey respondents (71 percent) said they would require data at rest (that is, data stored in the cloud) to be encrypted before they would adopt cloud. Just over half (51 percent) said they would require data in flight (that is, in transit across the Internet) to be encrypted.

Many survey respondents are already well on their way to supporting the idea of an all-encrypted Internet. Sixty percent have already taken steps or plan to encrypt all Internet traffic by 2017, and a mere 2 percent have no plans to adopt this approach at all.

In addition to concerns about encryption, 48 percent of respondents also noted they need the same level of security and audit capabilities in the cloud that they currently have on premises. Until organizations are confident in a cloud provider's ability to deliver consistent and high-quality services, they will still show some level of reluctance to move to the cloud.

F5 INSIGHT FOR KEY FINDING 03

While traditional security solutions like firewalls remain valid and necessary, those that protect users, data, and applications are being seen as critical. This is especially true as organizations realize that security is as much a business and operations challenge as it is a technical one. Security professionals who are protecting all three (users, data, and applications) are most confident in their ability to fend off attacks and keep their environments secure.

KEY FINDING

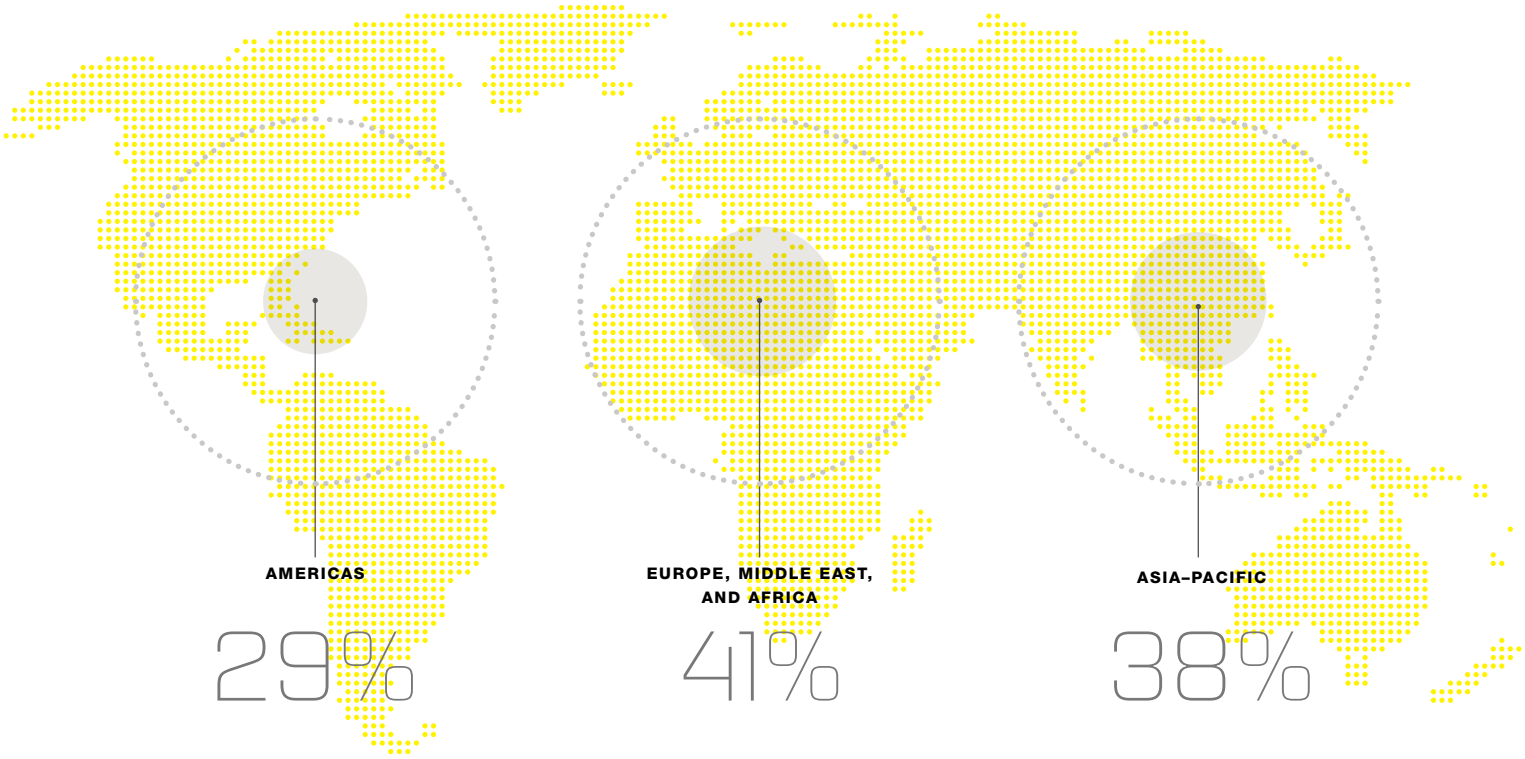
04

DEVOPS AND SDN ARE KEY TO IMPROVING OPERATIONAL EFFICIENCY

We asked respondents to identify which emerging trends they think will be strategically important to their organizations in the next two to five years. Alongside mobile apps, and as-a-service (both software and managed), we asked specifically about software-defined networking (SDN) and DevOps, since both are key to IT's ability to improve operational efficiency.

SDN separates the "brains" of the network from the physical devices, making the network more agile and easier to manage. DevOps is a model for developing software and services quickly by encouraging standardized communication and collaboration between application developers, IT, and networking professionals. DevOps also encourages the use of automation and orchestration.

Respondents who believe SDN will be strategically important in the next 2–5 years



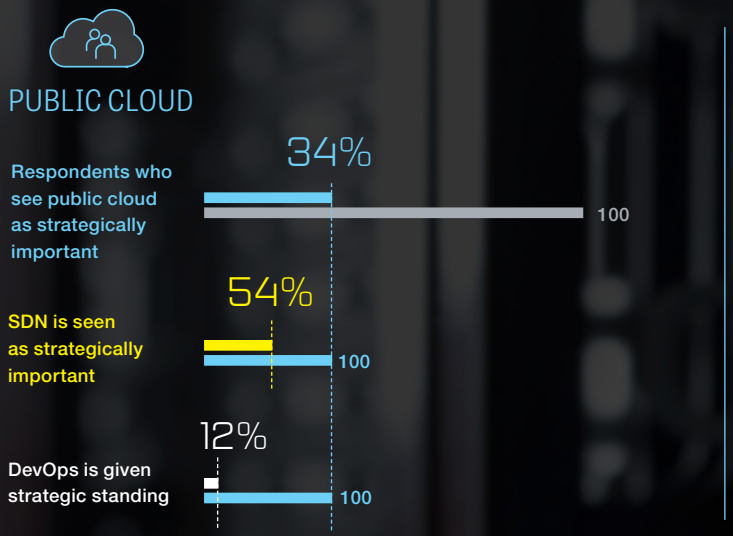
SDN ADOPTION VARIES BY REGION

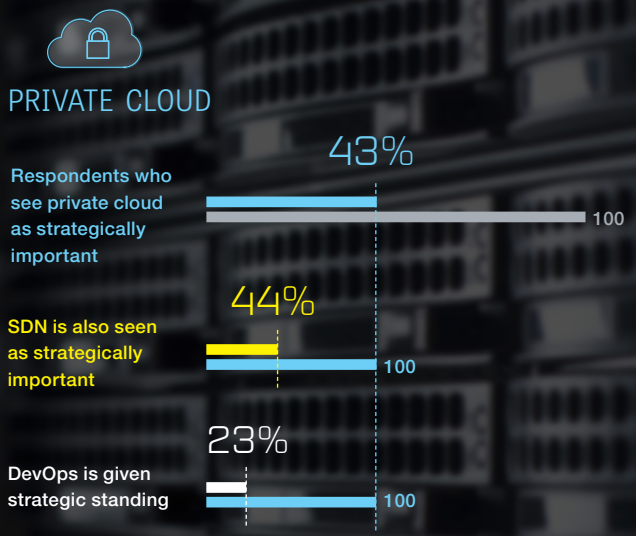
SDN continues a slow climb toward both relevance and adoption. Overall, 37 percent of respondents said that SDN will be strategically important to their organizations in the next two to five years. Across regions, the strongest response at 41 percent came from participants in EMEA. Their buying habits mirror this enthusiasm, with 26 percent planning to purchase SDN technology in the next 12 months. Participants in both Asia-Pacific and the Americas have similar purchasing plans at 26 percent and 22 percent respectively.

Of note, however, is that only 3 percent of respondents currently have SDN in production and 39 percent have no plans to deploy SDN at all. One reason this reluctance persists is because deploying SDN solutions often requires an organization to replace existing infrastructure. This is not only highly disruptive, it's a financial disincentive, considering that many organizations have significant existing investments in their network architectures.

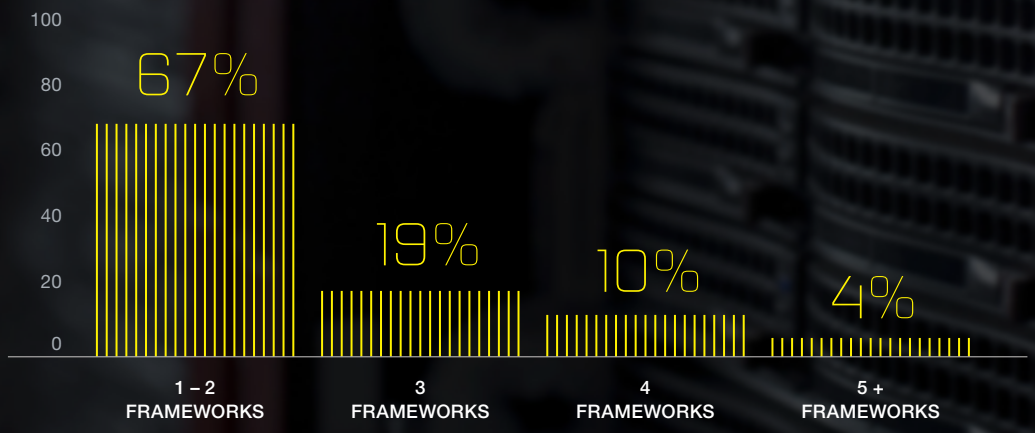
Among participants who are adopting SDN, the primary drivers across all regions were the need to lower operating costs (41 percent) and to improve time to market (27 percent). Yet, these objectives are difficult to achieve when IT is also being asked to expand operations, provide more services, step up security, and accommodate more users worldwide. The best way for organizations to reduce operating costs and improve time to market is to simplify their networks and make them easier to manage while also automating operations as much as possible. We see organizations increasing their focus in these areas in order to successfully reduce operating costs.

Strategic importance of SDN and DevOps to public and private cloud





The number of DevOps tools used for automation and orchestration



SDN AND DEVOPS RELATIVE TO CLOUD

We were interested in understanding how participants' answers regarding SDN and DevOps correlated with their thoughts about private and public cloud. Although cloud chatter about DevOps often focuses on public cloud, our survey respondents seem to associate DevOps more with private cloud. Of the 43 percent of participants who see private cloud as strategically significant, 23 percent also believe DevOps is significant, and almost twice as many (44 percent) believe the same about SDN. This seems to indicate that as organizations develop and deploy applications in their private clouds, they believe DevOps practices together with SDN implementations will give them the agile IT environments they need to meet their business requirements.

In contrast, among the 34 percent who said public cloud is strategically important, only 12 percent also believe DevOps is important while 54 percent believe SDN is. This is likely due to an increased focus on WAN-related SDN capabilities designed to improve the reliability and performance of applications that are hosted in the public cloud.

WHO'S DOING DEVOPS

DevOps itself continues to run under the radar. A mere 17 percent of respondents said that it will have significant strategic impact in the next two to five years. Yet, ironically, respondents certainly are doing a lot of it. As many as 67 percent of respondents are using one or two DevOps tools to help them automate and orchestrate the process of configuring, deploying, and scaling applications and servers; a third are using three or more.

Respondents continued to place high importance on tools that enable the automation and orchestration associated with DevOps and SDN, particularly programmability. Automation tools and frameworks rely on programmability features such as application programming interfaces (APIs) and templates that enable software-defined provisioning and configuration across application and network infrastructures. These speed deployment and reduce variations that can cause configuration errors. It was no surprise then that respondents rated as important to highly important all facets of programmability that enable automation: APIs (58 percent), templates (49 percent), and data path programmability (67 percent).

The survey results showed that these attitudes held across IT organizations, with the top five job roles—infrastructure architects, network managers, security engineers, IT director or VP, and application architect—placing high importance on programmability for automation and orchestration.

F5 INSIGHT FOR KEY FINDING 04

Although adoption is still slow, SDN is seen by many as a way to lower operating costs and improve time to market. The automation and orchestration tools that DevOps applies to application development are starting to filter up into the network. Both programmability and the use of frameworks are critical to an organization's ability to continuously deploy applications and services.

CONCLUSION

Respondents to our second annual State of Application Delivery survey provided new insights into the changing face of IT. More and more organizations have clearly embraced new deployment models—public, private, and hybrid cloud—as well as SaaS applications. Regardless of where or how they chose to deploy applications, organizations continue to rely heavily on services to ensure performance, availability, and security.

With many organizations leveraging new "multi-cloud" environments (often using multiple deployment models and cloud providers worldwide), the spotlight on security has shifted away from traditional location-based (data center) protection to protecting users and identity, data, and applications wherever they are located. Many organizations are still looking to SDN and DevOps to help them reduce capital expenses, streamline operations, and ensure continuous delivery through automation and orchestration.

Amid all this change, one outcome is clear: application services will remain the link that enables IT organizations to respond to requirements that are most vital to business unit owners. Performance, security, availability, and identity services improve employee productivity, reduce organizational risk, and drive positive customer engagement, as well as revenue growth.

MORE INFORMATION

For more information about the data in this report and what it means for your business, please join F5 for webinars featuring executives and subject matter experts. Visit f5.com/SOAD for details.

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-62569171