2021

Digital Transformation and Application Security Posture in West and Central Africa

Nigeria | Senegal | Cameroon | Ivory Coast | Ghana

GEFONA DIGITAL FOUNDATION

hello@gefona.org
www.gefona.org

Table of Contents

Acknowledgments

By Tomslin Samme-Nlar

The report is a collaborative effort of the following individuals:

Primary researcher
Tomslin Samme-Nlar, **Director, Research**

Research team
Semi Yam, **Field Research Supervisor**
Lydie Nogol, **Reviewer**

Editorial and graphic design
Theryx Ndouken, **Graphic Designer**

Communications and web publishing
Theryx Ndouken
Cedric Abe

I. Introduction

Africa continues to see huge growth in digitization and the use of Information and Communication Technologies (ICT) to solve many of the challenges plaguing the continent. We've noticed rapid and ongoing growth in digitization in areas such as banking, farming, government, education and health. At the same time, we've noticed a significant rise in cyber-related attacks and crime on the continent.

The fast growth of digital and the increased dependency in technology comes along with cyber risks. The implication of these cyber risks/ threats in our day to day life is not always well perceived by all parties including companies and end users. In addition, very little data exists for both policy makers and the private sector to use in decision making, which is why we undertook this study.

Undertaking the study is also consistent with the objectives of GEFONA DIGITAL FOUNDATION. which are (1) building a database of the state of cybersecurity in Africa (2) providing information to help in decision making and (3) to trigger revision of policies based on in country facts.

After a successful study of the State of Application Security in Cameroon[1] which saw the production of a working report and the release of certain stylized facts regarding the state of applications in Cameroon, we thus considered the extension of this study to the wider immediate region. After discussions with some private sector players, we decided to extend the study to 5 countries (Nigeria, Ghana, Cameroon, Senegal and Ivory Coast) in West and Central Africa.
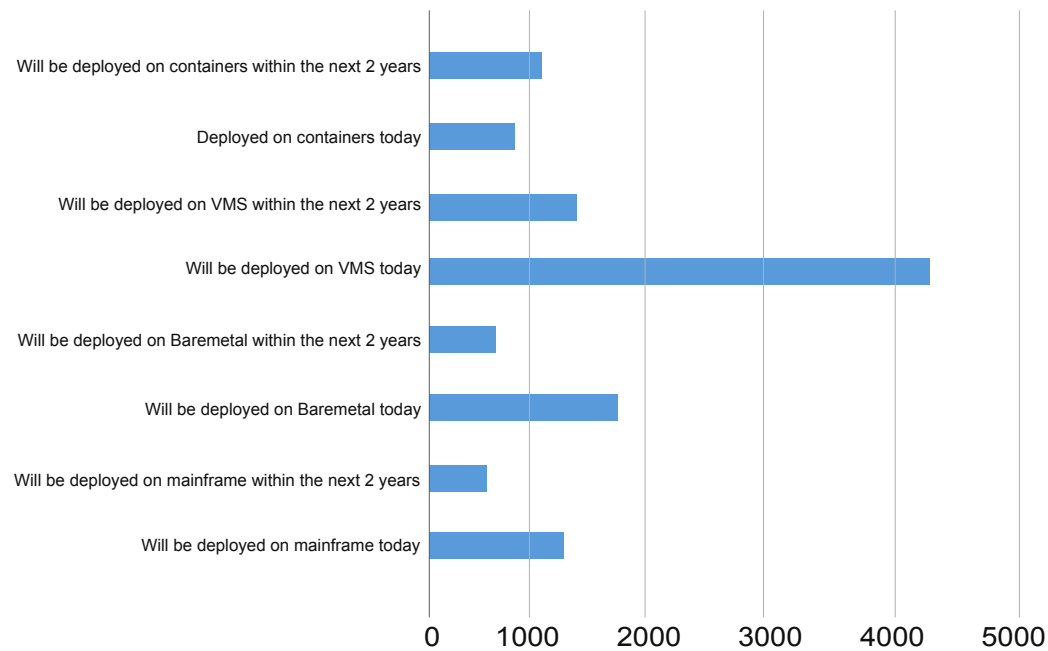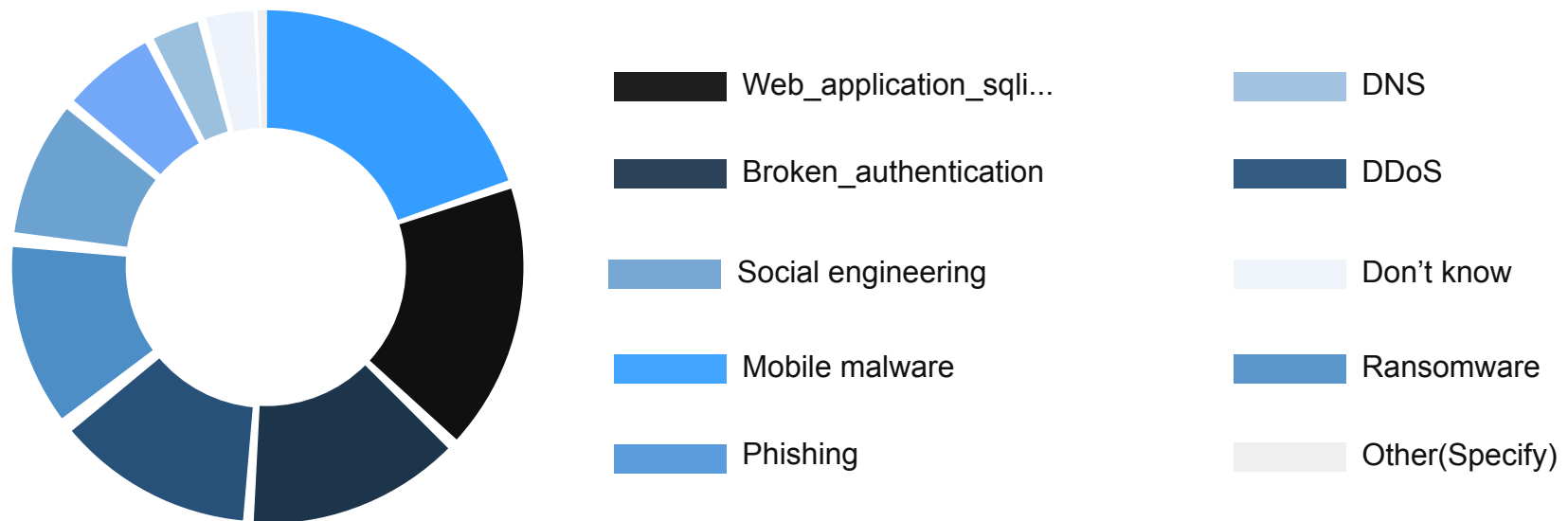
II. Key Findings

1. Cloud computing will be the most strategic technology trend for most organizations in West and Central Africa within 2-5 years.
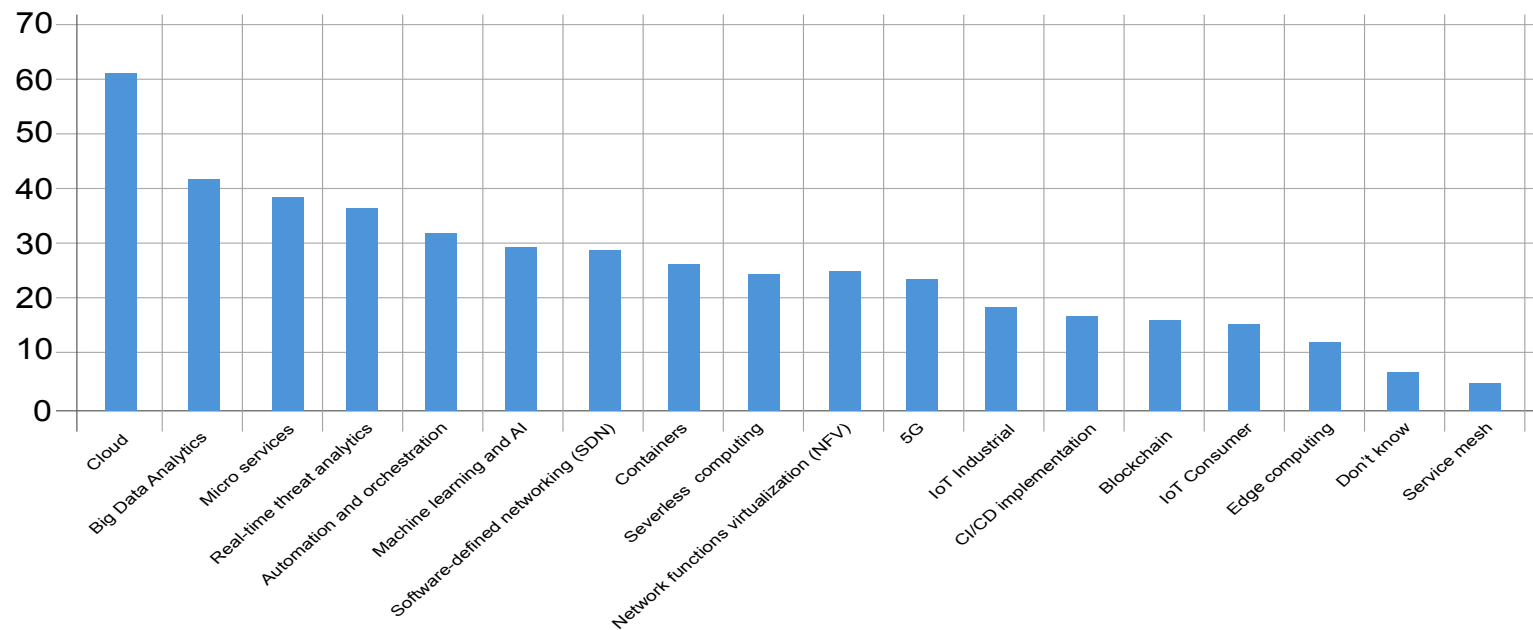
2. Virtual Machines (VMs) are still the predominant architecture used to deploy applications today.

Bar chart showing deployment architecture:
- Will be deployed on containers within the next 2 years
- Deployed on containers today
- Will be deployed on VMS within the next 2 years
- Will be deployed on VMS today
- Will be deployed on Baremetal within the next 2 years
- Will be deployed on Baremetal today
- Will be deployed on mainframe within the next 2 years
- Will be deployed on mainframe today

X-axis: 0, 1000, 2000, 3000, 4000, 5000

**3. Phishing (42.67%) and Web application attacks (SQLi, XSS, XXE, remote file inclusion) (36.67%) are the most common external attacks.**

Web_application_sqli...

Broken_authentication

Social engineering

Mobile malware

Phishing

DNS

DDoS

Don't know

Ransomware

Other(Specify)

4. When looked at from a regional perspective, most organizations don't think they have a security skill gap.

2021 Digital Transformation and Application Security Posture in West and Central Africa
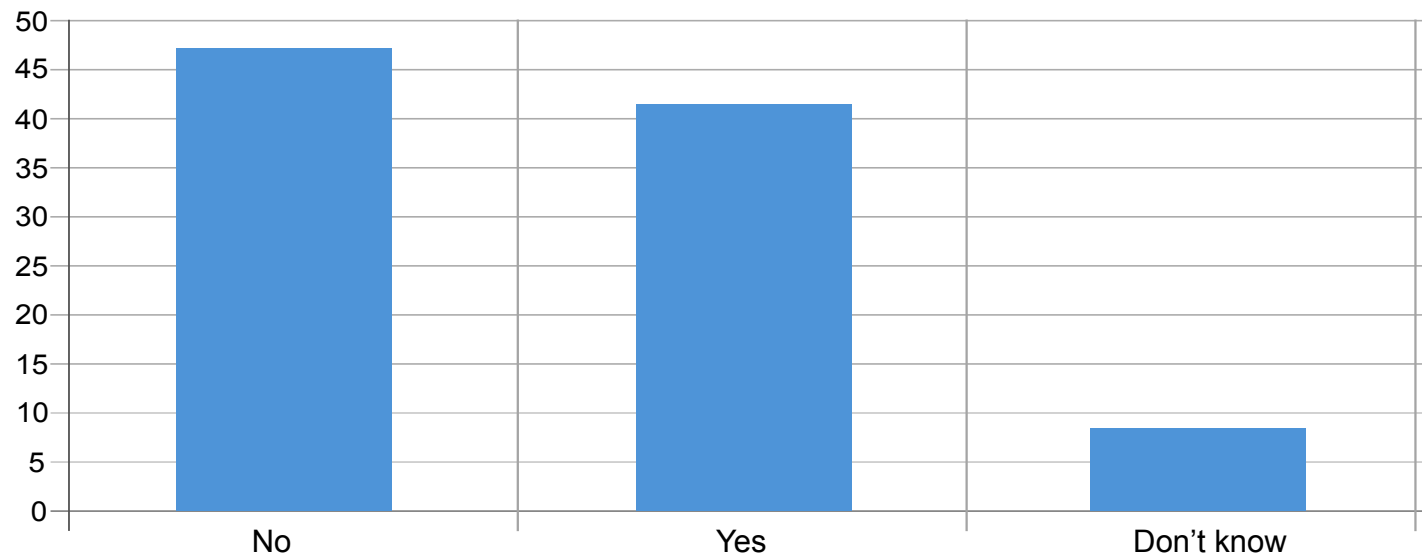
5. 24% of companies in the region will have up to 24% of their applications in the cloud by the end of 2022.
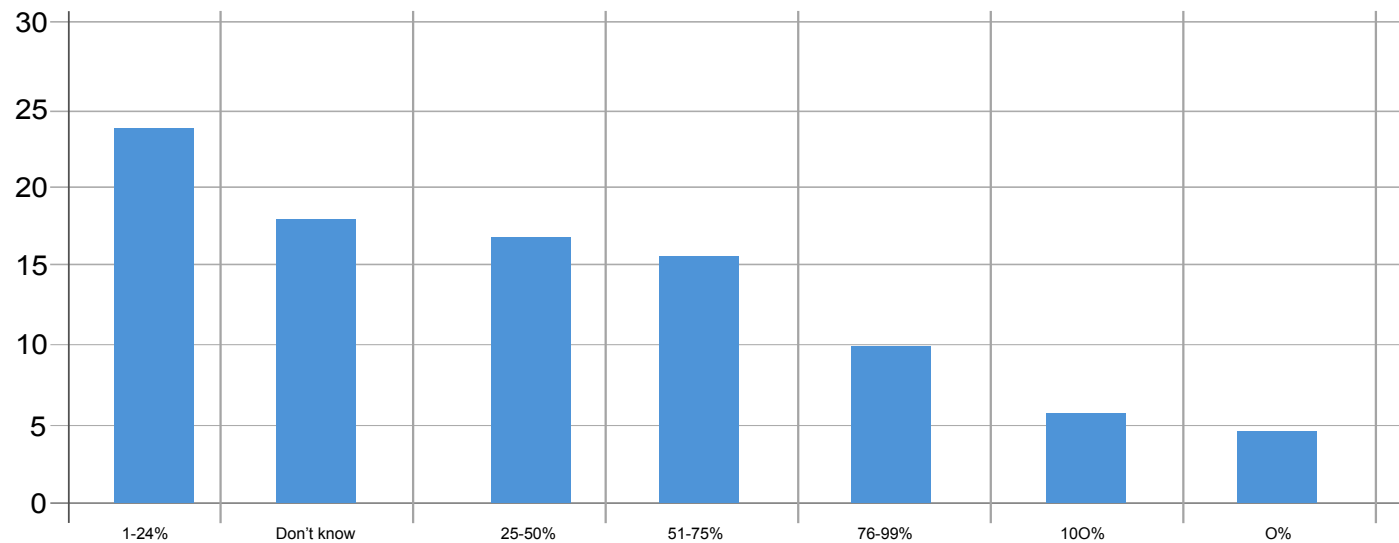
III. Digital Transformation

Most organizations today are undergoing some form of digital transformation. That is to say they are adopting digital technology to replace manual processes with digital processes or even replacing old digital technologies with newer ones, thereby transforming their businesses.

Besides the obvious advantages of digital transformation like efficiency, cost reduction and a competitive edge for the business, there is significant security benefit to be had from digital transformation. For example, cloud services are often more secure than most premise deployments of most organizations. This is because cloud service providers undergo accreditation programs like ISO/IEC 27001 or ISO/IEC 27017 to provide assurance to their customers that they have put all necessary controls in place to meet security best practices. Moreover, leveraging on security embedded on cloud services can be more cost effective for certain organizations than putting the same level of controls on premises. Finally, cloud service providers are often required to comply to various industry and government regulations.

Our research has shown that a high number of organizations are considering adopting cloud services in each of the countries studied.

60.6%

the majority (60.6%) of respondents were moving to the cloud.
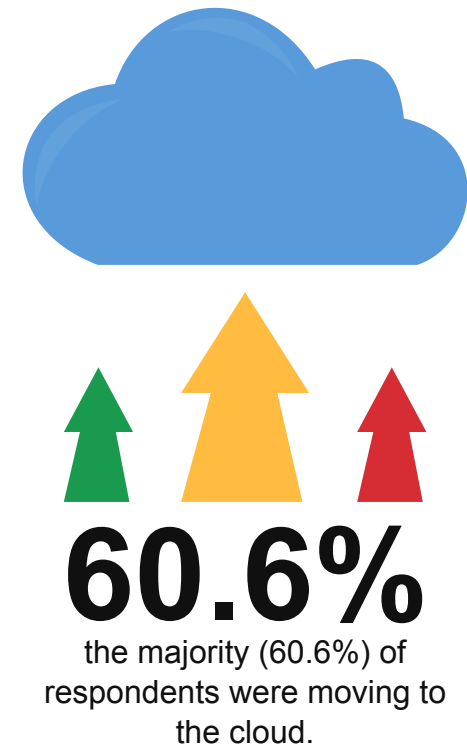
We Asked:

Which technology trends do you think will be strategically important for your organization in the next 2–5 years?
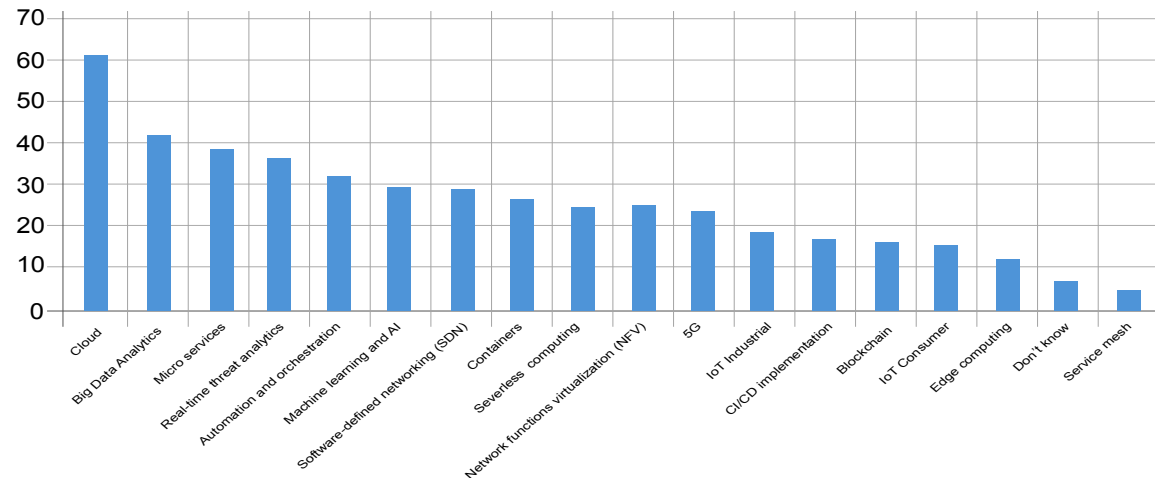
What we learned

60.67% of organizations in the region think cloud computing technologies will be strategic in the next 2-5 years.

There is however a little bit of differences in responses between the countries surveyed. The table below illustrates the differences:

| **Nigeria**	**Ghana**	**Cameroon**	**Senegal**	**Ivory Coast**
88.3% said cloud computing was strategically important in 2-3 years while 51.1% said Software-defined networking (SDN) & 5G will be strategic.	In Ghana 36.3% respondents said Cloud computing and new application development architectures will be strategically important for organizations in 2-5 years time.	Cloud (55.5%), big data analytics (44.4%) and AI/Machine learning (38.8%) are considered strategic in the next 2-5 years	Cloud (60.7%), Containers (46.4%) and newer application development architectures (42.8%) are considered strategic in the next 2-5 years	55.5% said cloud computing was ain 2-3 years

We Asked

Does your organization currently have or plan to have digital transformation projects in place?
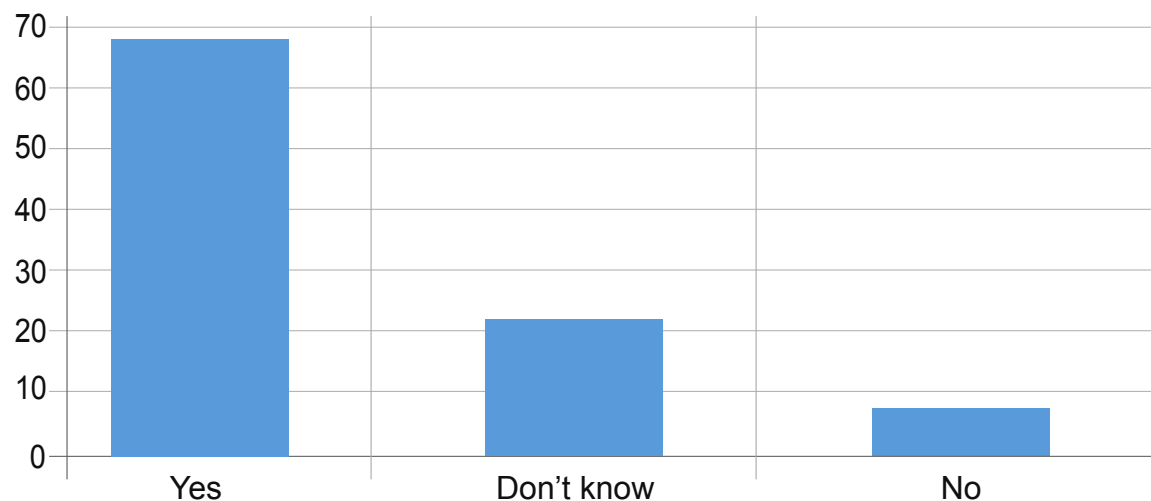
What we learned

67.33% of organizations have or plan to have a digital transformation project in the region.

In the different countries,

Nigeria

83.7% of businesses have started the digital transformation process.

Ghana

31.1% of organizations have or are planning to start their digital transformation journey.

Cameroon

45% of organizations have or are planning to start their digital transformation journey.
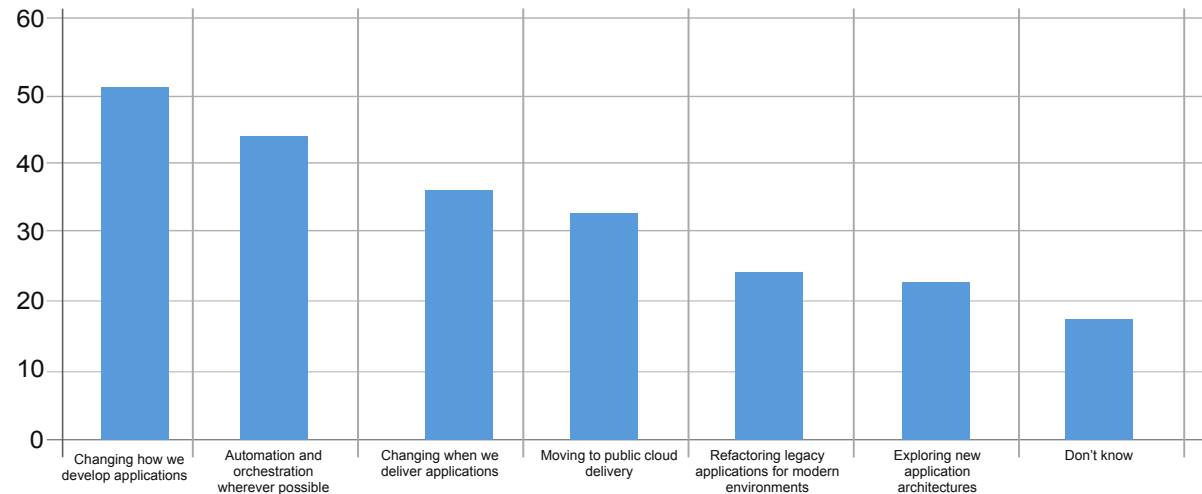
Senegal

44.4% of organizations have or are planning to start their digital transformation journey.

Ivory Coast

77.7% of organizations have or are planning to start their digital transformation journey.

We Asked

How is digital transformation influencing your application decisions?

What we learned

Digital transformation is changing how organizations develop applications, like moving to agile methods.

In the individual countries,

Nigeria

62.7% say digital transformation is predominantly changing how they develop applications while 55.8% said it is causing them to implement automation and orchestration wherever possible in their IT systems and processes

Ghana

57.5% say digital transformation is influencing how they develop applications and 45.4% say it is causing them to implement automation and orchestration wherever possible in their IT systems and processes

Cameroon

40.5% say digital transformation is influencing how they develop applications. An equal 35.1% said digital transformation is causing them to implement automation & orchestration and refactoring legacy applications for modern environments.
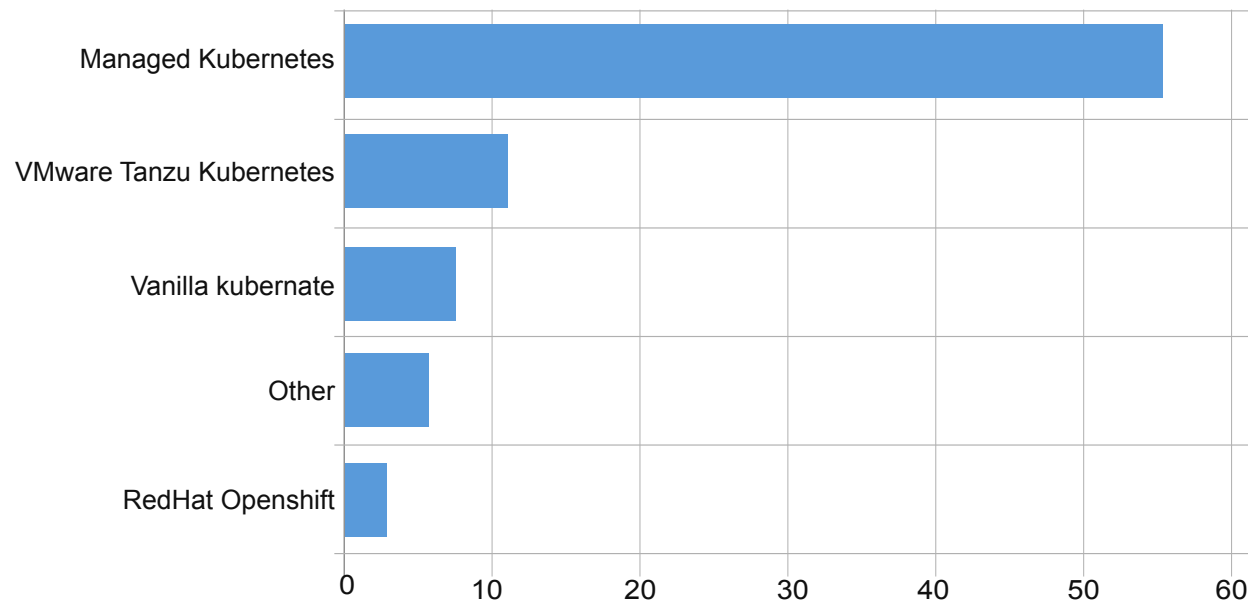
Senegal

46.4% said digital transformation is influencing how organizations develop applications

Ivory Coast

50% say digital transformation is influencing how they develop applications

We Asked

If you are evaluating or using container platforms, which platforms are you considering?

What we learned

Managed Kubernetes is the choice of container platform for those planning to move to containers.

In the countries studied:

Nigeria

77.1% organizations said they prefer a managed Kubernetes platform as their container platform.

Ghana

57.1% of organizations in Ghana prefer to use a managed Kubernetes platform
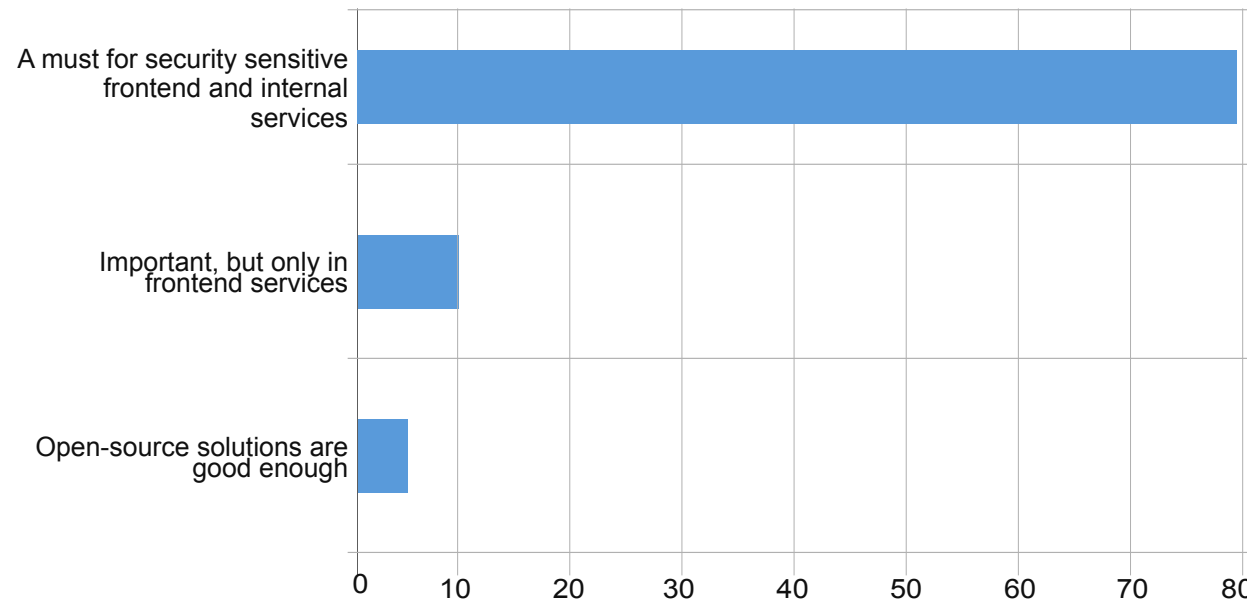
Cameroon

60.8% of organizations in Cameroon prefer to use a managed Kubernetes platform

Senegal

75% of organizations in Senegal prefer to use a managed Kubernetes platform

We Asked

How important is Web Application Firewall security to your organization?

What we learned

The majority of organizations thought Web application firewalls were a must for security sensitive front-end and internal services.

In the countries studied:

Nigeria

88.3% organizations in Nigeria consider Web Application Firewall security a must for securing sensitive frontend and internal services.

Ghana

93.9% of organizations said Web Application Firewall security is a must for securing sensitive frontend and internal services

Cameroon

83.3% of organizations said Web Application Firewall security is a must for securing sensitive frontend and internal services

Senegal

78.5% of organizations said Web Application Firewall security is a must for securing sensitive frontend and internal services

Ivory Coast

50% of organizations said Web Application Firewall security is a must for securing sensitive frontend and internal services

# IV. Infrastructure and Applications

In this section, we were interested in understanding the totality of applications that organization use across all deployment models.

Monolith applications continue to be run in the region. Containerization which allows developers to deploy applications faster, scaleably and more securely, is still a new concept in the region. Virtual Machines (VMs) are the predominant architecture used to deploy applications today.

We Asked:

As a rough estimate, how many applications is your organization, running/using?
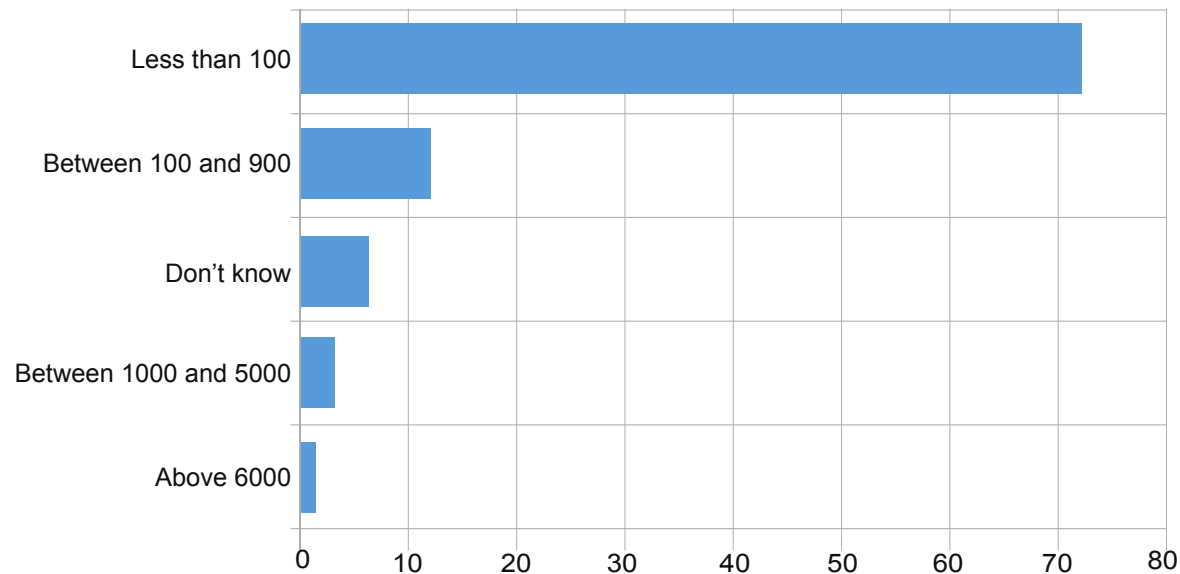
What we learned:

78.6% use less than 100 applications

In the countries we studied, the results were as follows:

| **Nigeria**	**Ghana**	**Cameroon**	**Senegal**
83.7% of organizations run or use less than 100 applications.	Only 15.1% of organizations use between 100 to 900 applications in their operations. Most use less than 100 applications.	Majority of the organizations (84.3%) run or use less than 100 applications.	78.5% run or use less than 100 applications.

We Asked:

Of those applications deployed today, roughly what share fit into the following categories? (1) Mainframes (2) Bare metal servers (3) VMs (4) Containers
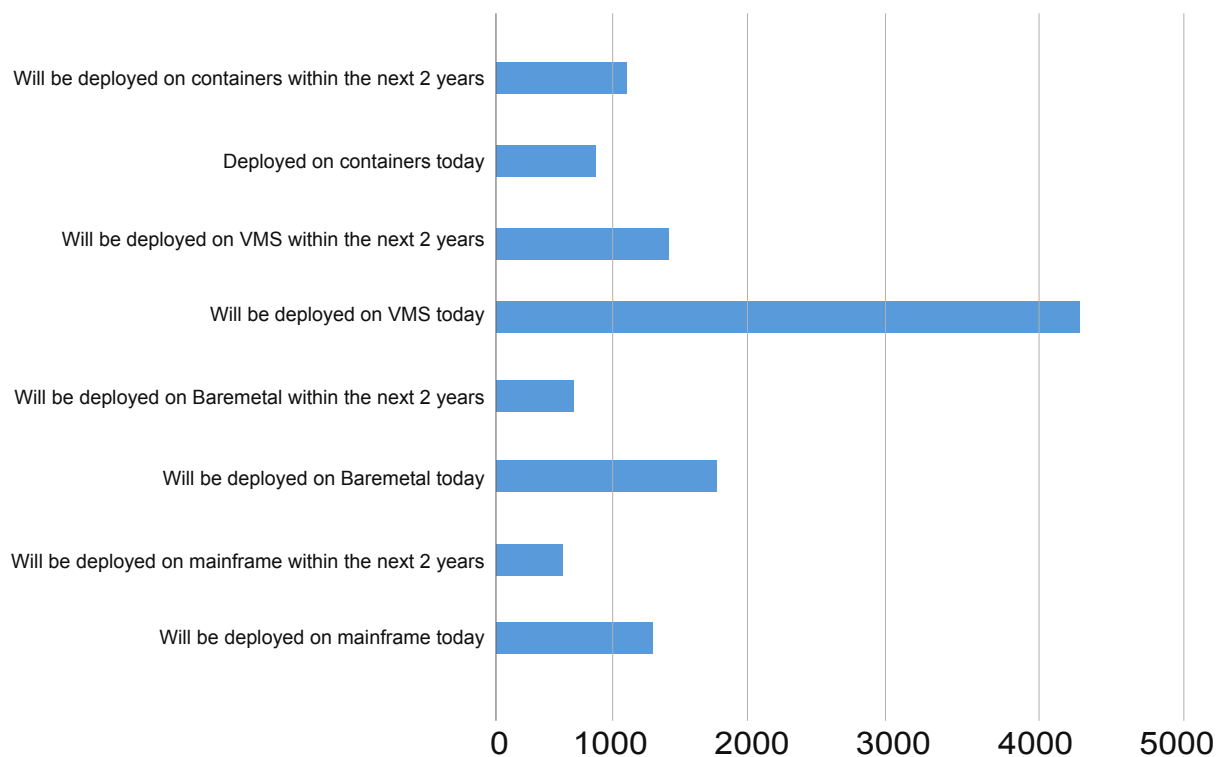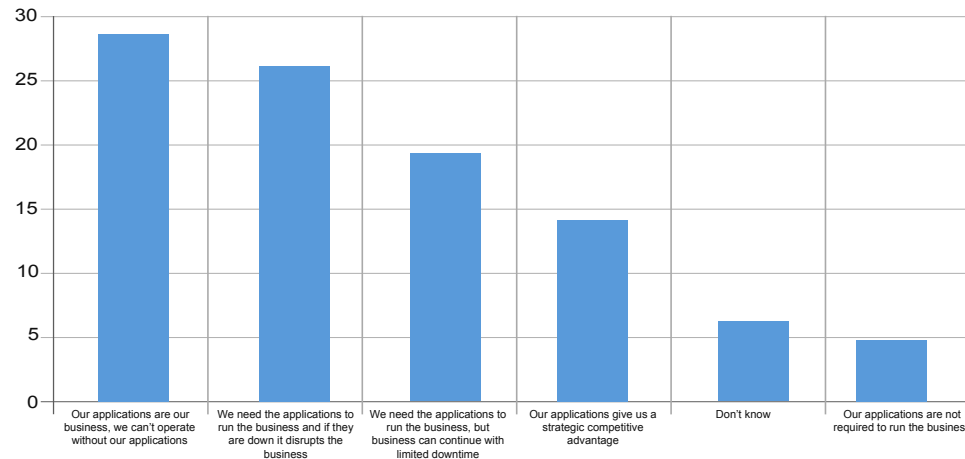

What we learned:

The majority of organizations predominantly use Virtual Machines (VMs) to deploy applications today.

We Asked:

Please select the statements that represent how your organization views/treats its application portfolio?

What we learned:

In the region, 28.6% viewed applications as core to their business, while 27.3% viewed applications as needed to run the business but not core to the business.

In the countries, we found the following:

Nigeria

41.8% of organizations view applications as important to run their businesses while 30.2% believe applications are their business, and therefore can't operate without them.

Ghana

45.4% said they can't operate without applications

Cameroon

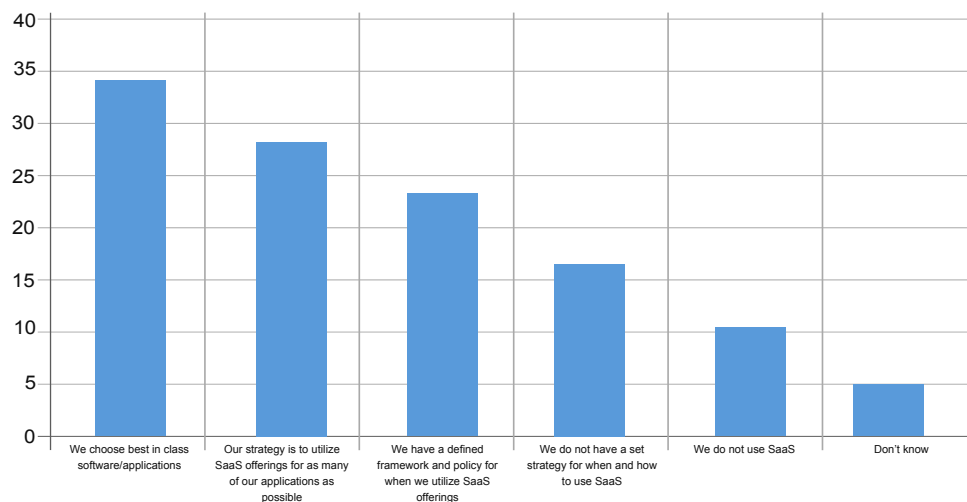46.8% need applications to run their business

Senegal

32.1% of organizations did not know, while only 17.8% said applications are core to their business.

Ivory Coast

37.5% of organizations did not know and 25% said applications are core to their business.

We Asked:

Please select the statement(s) that represent your organization's usage of Software as a service (SaaS)?

What we learned:

34% said they choose best in class software/applications

In the countries, we found the following

Nigeria

27.1% of organizations said that in their SaaS strategy, the operating and/or financial model is depending on the availability of the best solutions

Ghana

41.8% utilize SaaS to run as many of their applications as possible
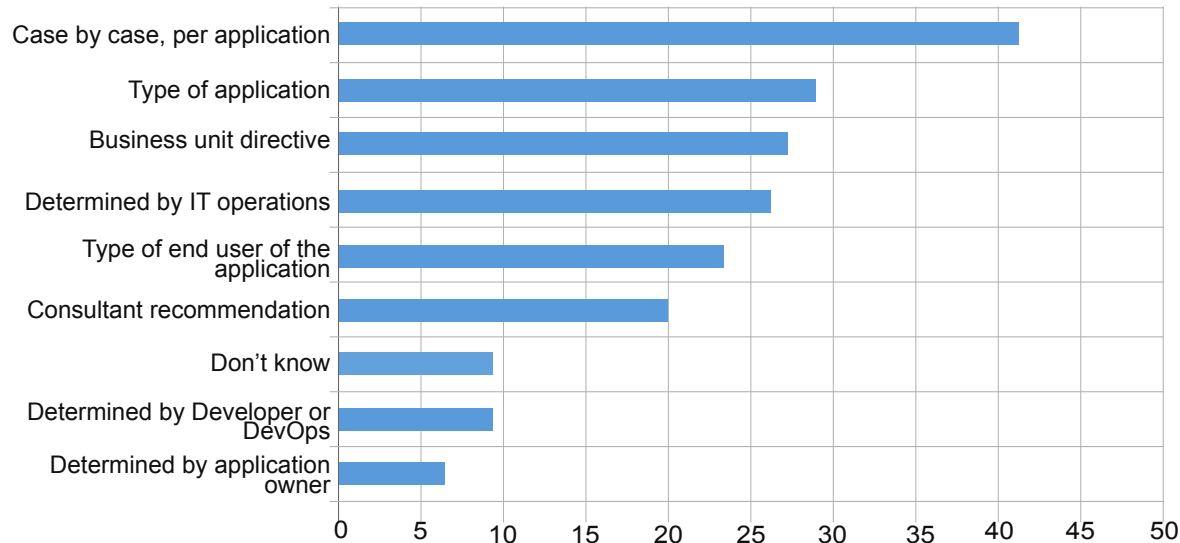
Cameroon

23.3% said they have a defined framework and policy for when they utilize SaaS offerings

Senegal

25.8% of organizations do not use nor have a set strategy for when and how to use SaaS.
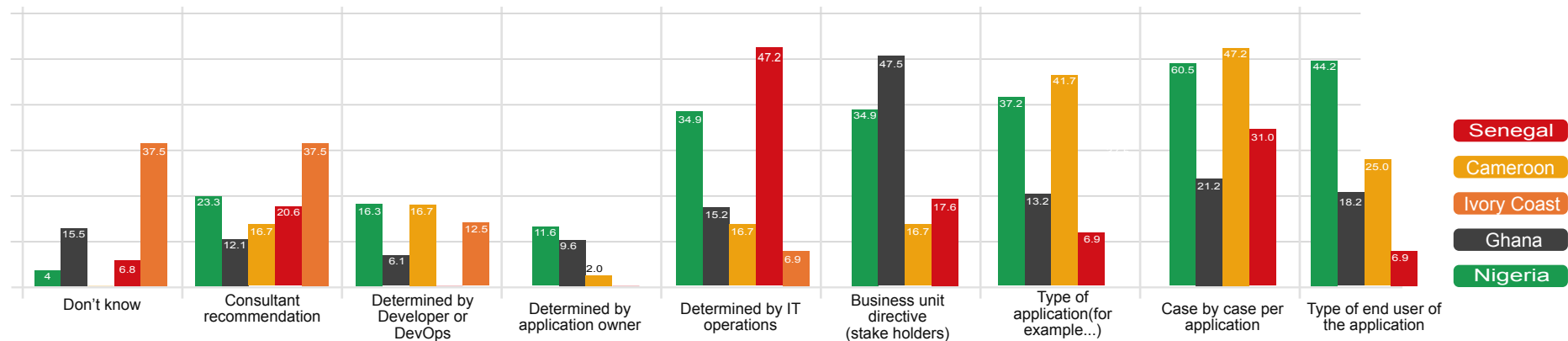
We Asked:

How does your organization decide which type of cloud is best for each application?
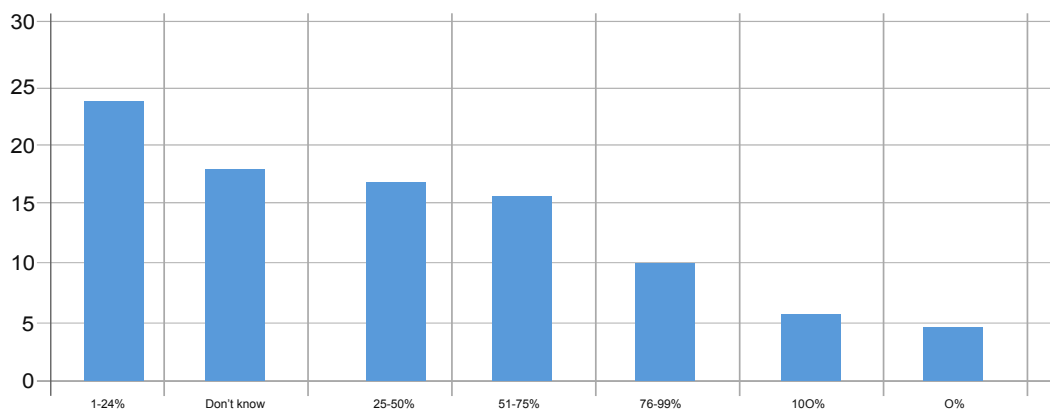

What we learned:

40.6% in the region said their organization decides which cloud is best on a case by case, per application basis.

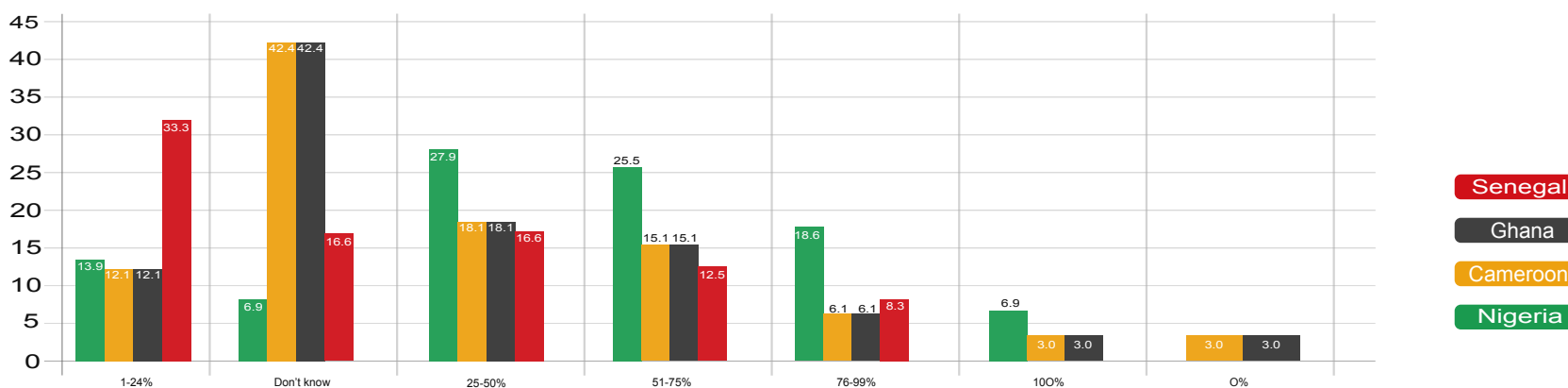The individual countries had different responses as shown below:

We Asked:

Either estimate the percentage of your organization's applications that will completely or some portion that will be operating in a cloud by the end of 2022.

What we learned:

24% said 1-24% of their applications will be in the cloud by the end of 2022.

In the individual countries,

V. Application Services

For the purposes of this survey, we define application services as network and security functions (often referred to as L4–L7 services or application delivery services) and are the broad set of capabilities covering availability, performance, security, and identity and access management.

We Asked:

When you are deploying application services, please select the most important characteristic of the offering.
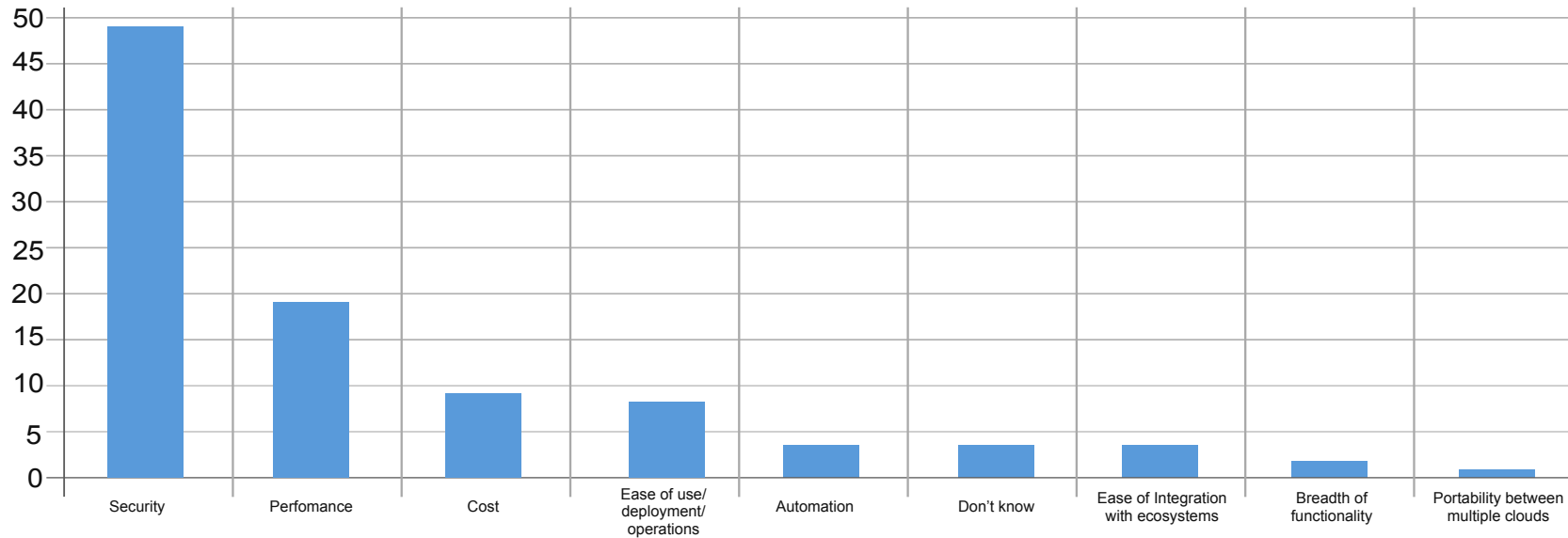
What we learned:

49% respondents believe security is the most important characteristic when deploying application services.

While it was generally the same theme, the percentages were a bit lower for most of the countries, except for Senegal and Ivory Coast.

Nigeria
39.5% of organizations in Nigeria consider security to be most important when deploying applications

Ghana
66.6% said security was most important when deploying applications

Cameroon
31.4% said security was most important when deploying applications

Senegal
71.4% said security was most important when deploying applications

Ivory Coast
50% said security was most important when deploying applications
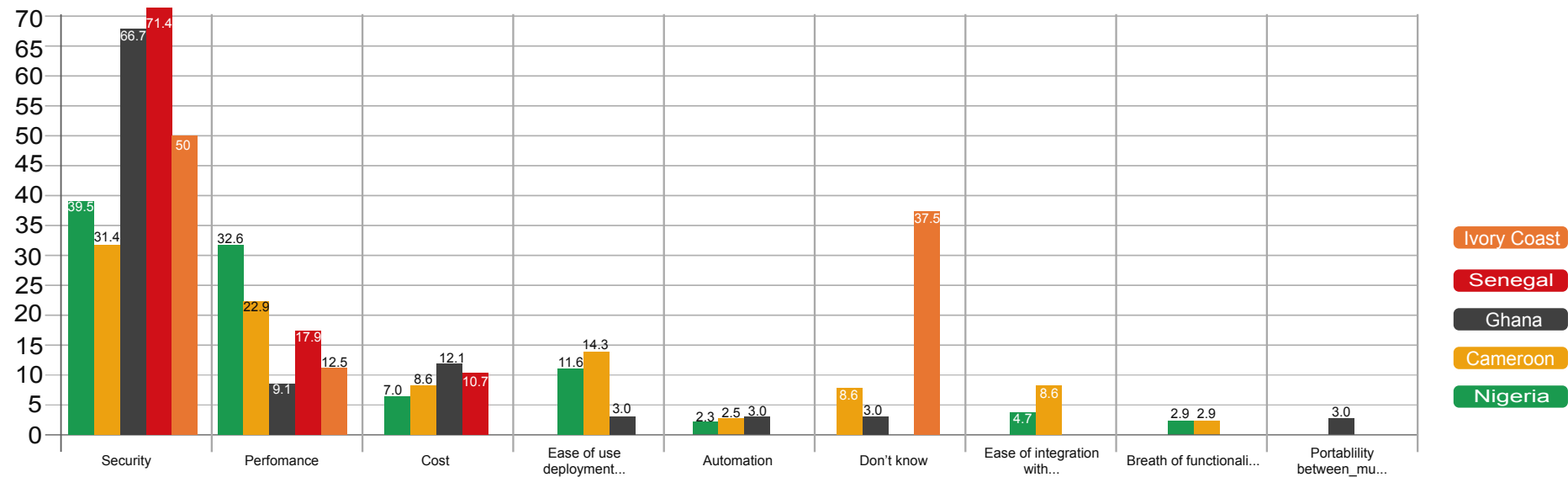
We Asked:

For application services, please select the most important characteristic in prioritizing your deployment decisions.

What we learned:

When it comes to prioritization of deployment decisions, consistency across all applications was popular amongst respondents as most important.

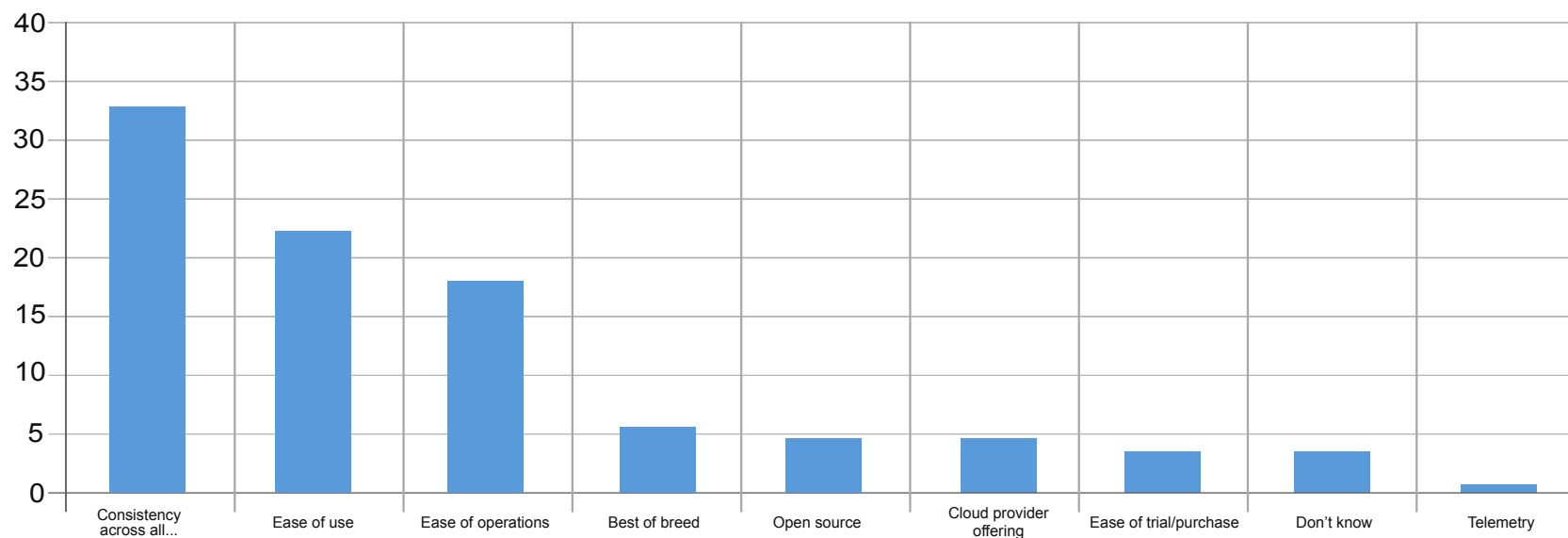Drilling down to the countries, the important factor remain same for most.

Nigeria
Consistency across all applications is considered most important characteristic in deployment decisions

Ghana
Consistency across all applications is considered most important characteristic in deployment decisions
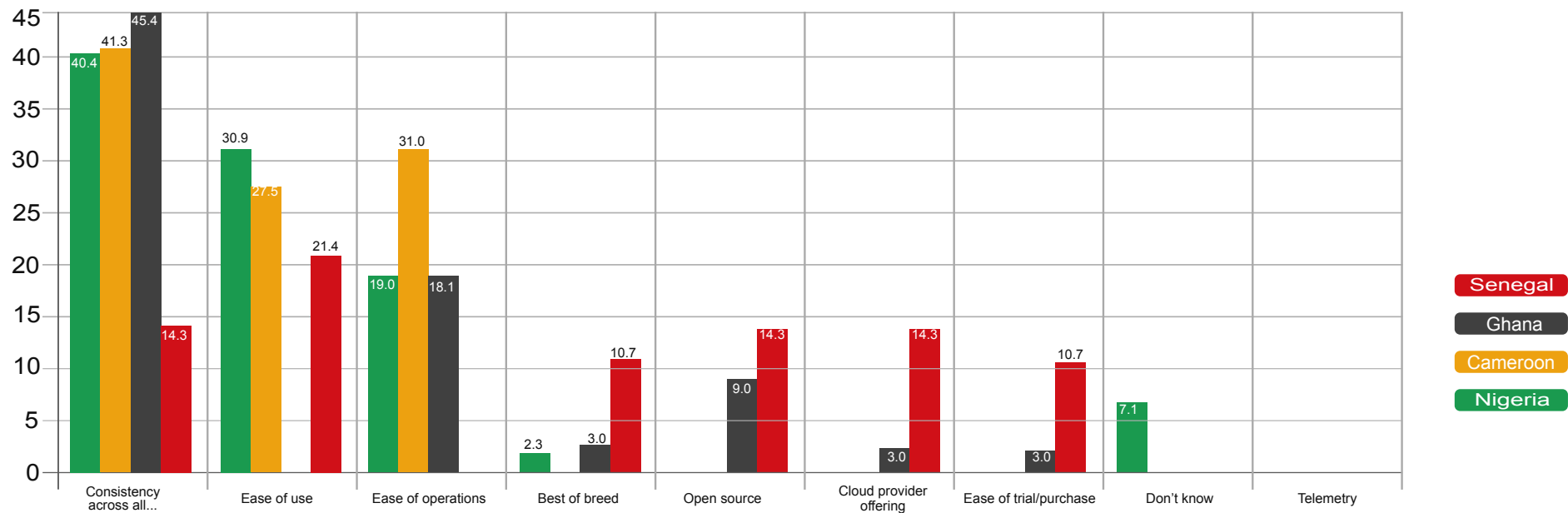
Cameroon
41.3% said consistency across all applications is most important while 31% said ease of operations was.

Senegal
Ease of use topped the list as most important characteristic in prioritizing application deployment decisions in Senegal

Ivory Coast
Most respondents in Ivory Coast said they didn't know

VI. Application Security

Information security is increasingly critical for all organizations and it is made even more critical with the introduction of complexities such as cloud computing, internet of Things (IoT) and Artificial Intelligence (AI).

Organizations tend to be reluctant to adopt the cloud due to the loss of premise control of data and security. And indeed, the majority of respondents said they trusted a private cloud (on-premise) more than the public cloud.
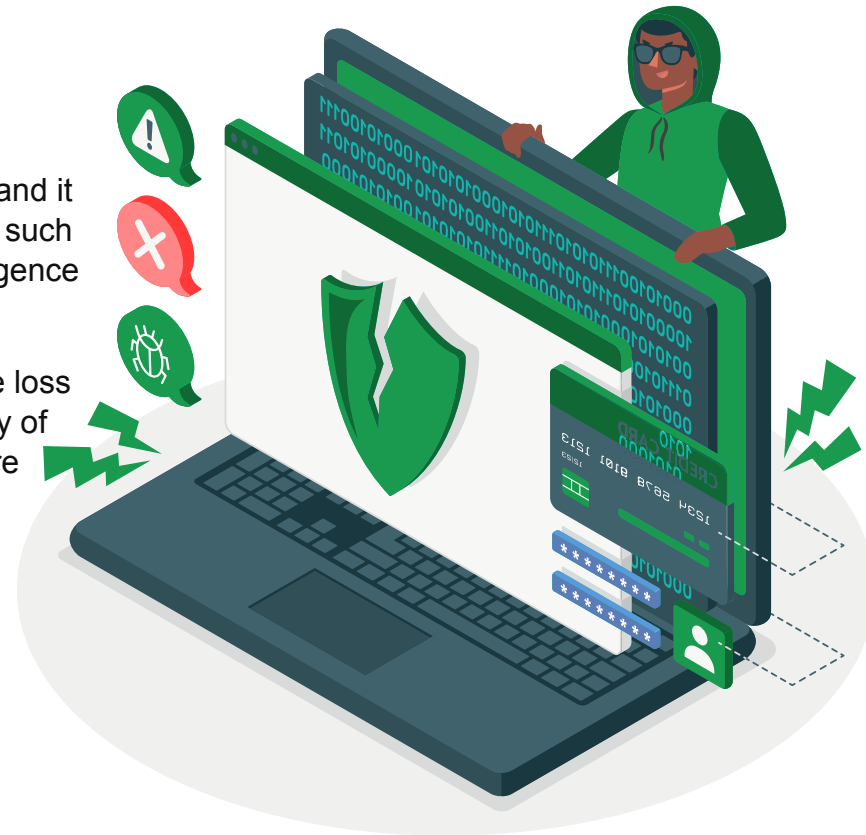
We Asked:

What are the most common external attacks carried out against your application?

A horizontal bar chart showing:
- Other(Specify): ~1
- Dont' know: ~7
- DNS: ~7
- Mobile malware: ~14
- Social engineering: ~20
- Ransomware: ~26
- DDOS: ~28
- Broken Authentication: ~30
- Web application sqli: ~32
- Phishing: ~42
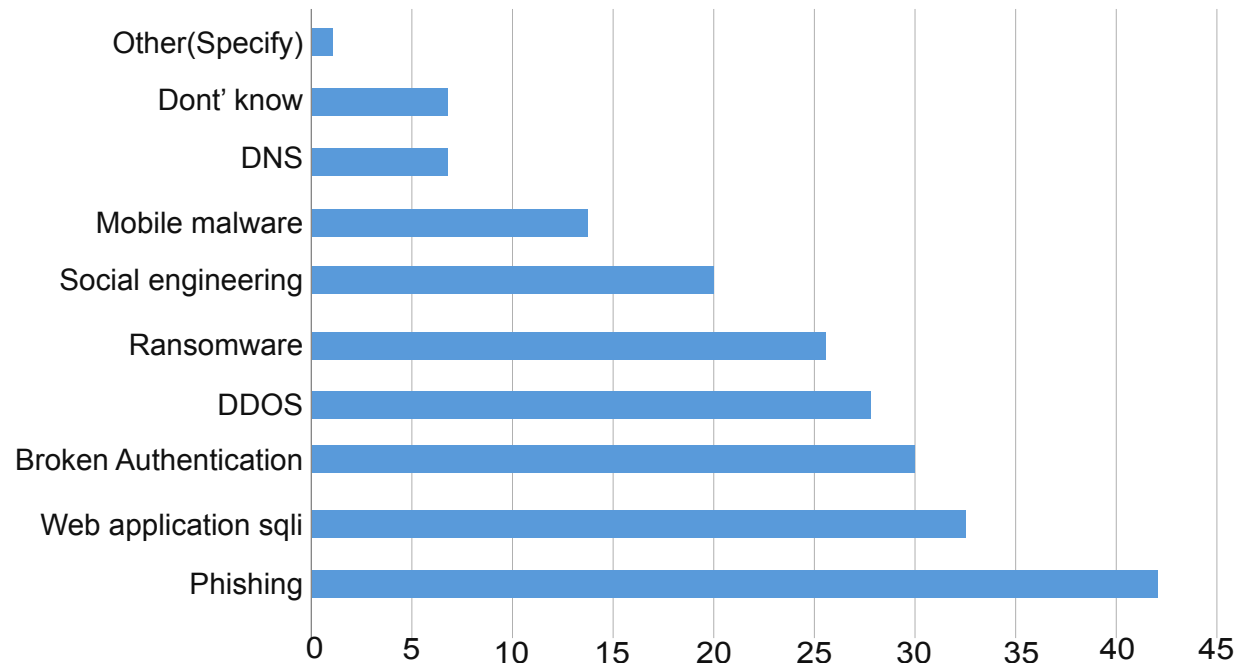
What we learned:

Phishing and web application attacks were the top attack vectors in the region. While ransomware wasn't at the top, it is worth noting however that it makes up to 26% of attacks, as reported by respondents.

We Asked:

The worst thing I could do is deploy an application without _____!
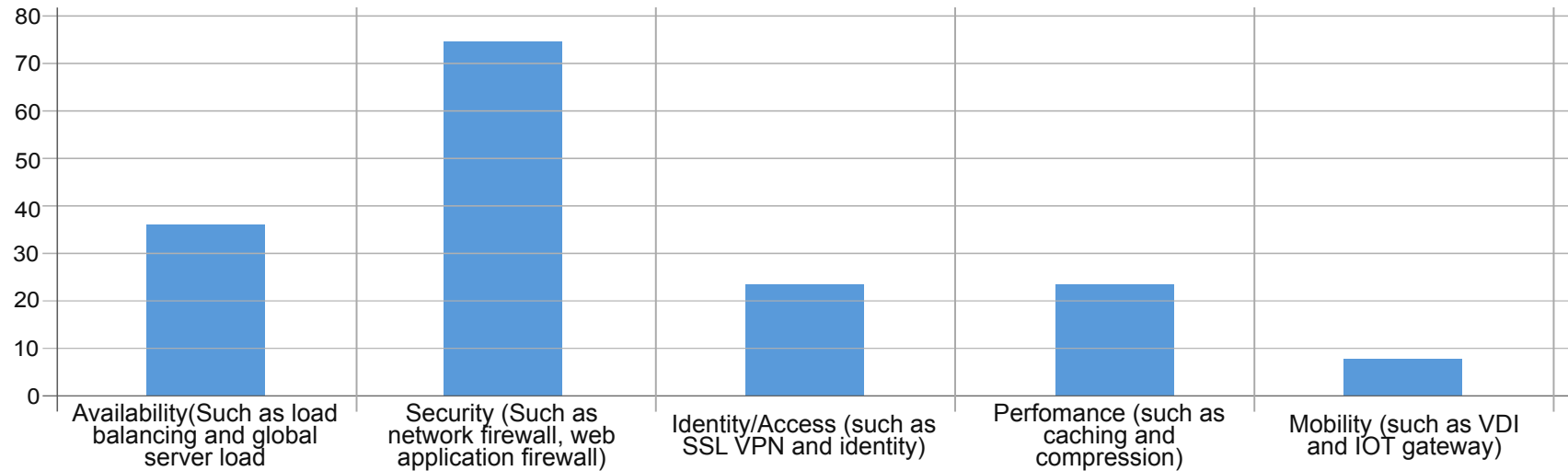
What we learned:

76.7% of organizations said security was what they couldn't live without. Availability and performance are secondary.

We Asked:

On a scale of 1 to 5, please rate your confidence in your company's ability to withstand an application-level security threat across the following application locations:

1. Private cloud (applications on premise)

2. Applications off -premises colocation data centers

3. IaaS, PaaS & SaaS (public cloud)

4. All Applications

What we learned:

Except for Nigeria where organizations were generally confident in their ability to withstand application-level security threats in both private and public cloud, for the rest of the countries, organizations are only confident in their ability to withstand application-level security threats on private cloud.

We Asked:

Do you believe you have a security skills gap in your organization?
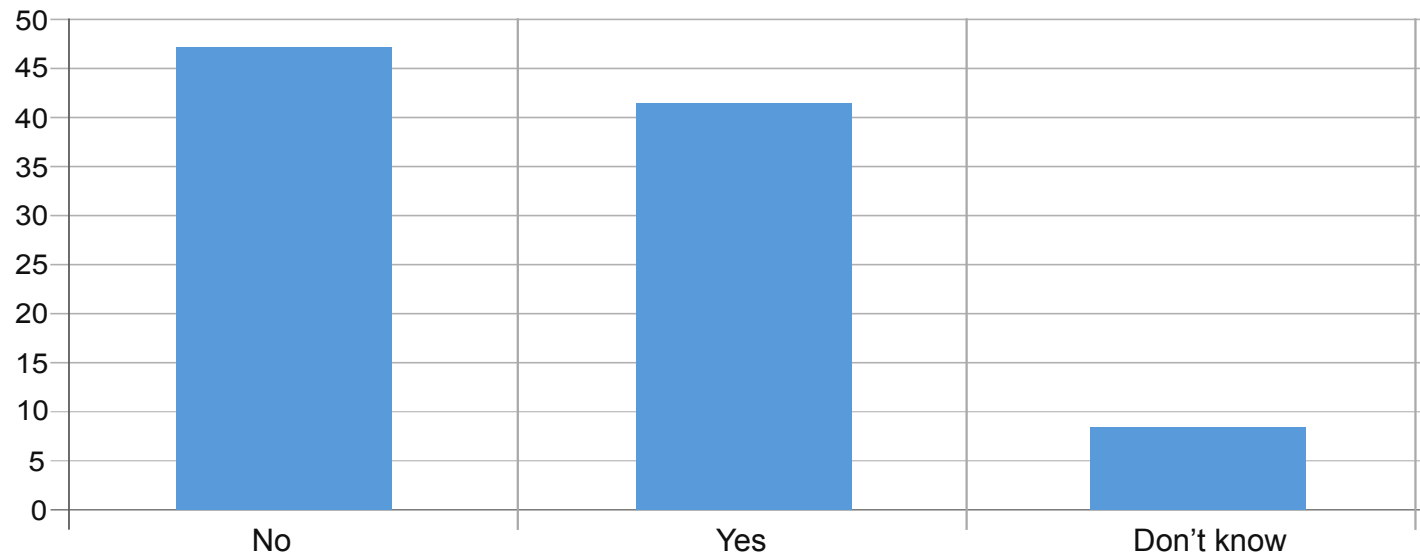
What we learned:

Interestingly, from a regional perspective, the majority of respondents said they don't have a security skill gap. It is unclear from the data why this is the case.

However, the results were different in the individual countries. Organizations in Nigeria and Cameroon said they had skill shortages while Ghana and Senegal said they didn't.

Nigeria — No: 40.5, Yes: 47.6, Don't know: 11.9

Cameroon — No: 37.1, Yes: 60.0, Don't know: 2.9

Ghana — No: 66.7, Yes: 24.2, Don't know: 9.1

Senegal — No: 57.1, Yes: 39.3, Don't know: 3.6

Nigeria   Cameroon   Ghana   Senegal
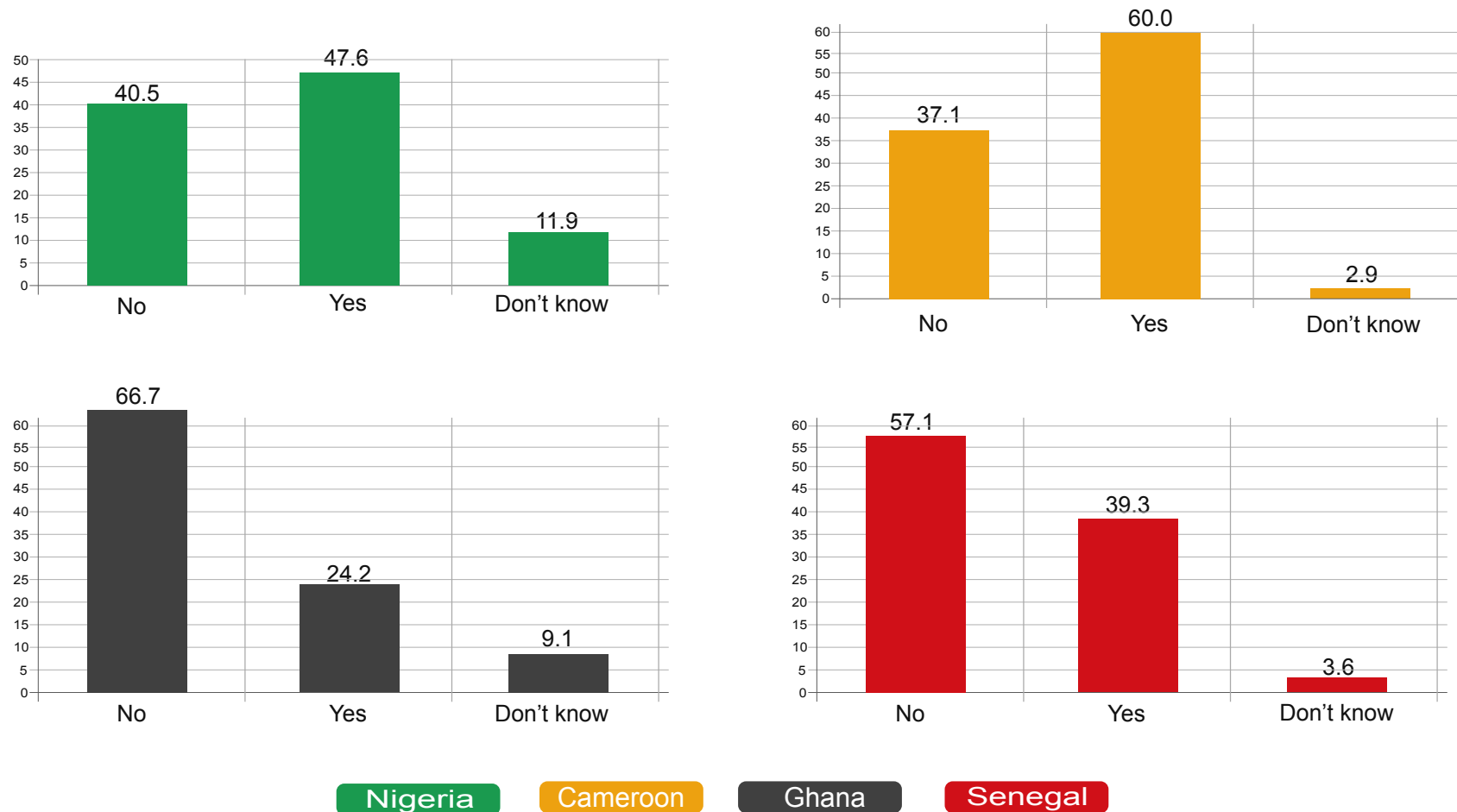
We Asked:

Which area do you have a security gap/deficit in skills in your organization?
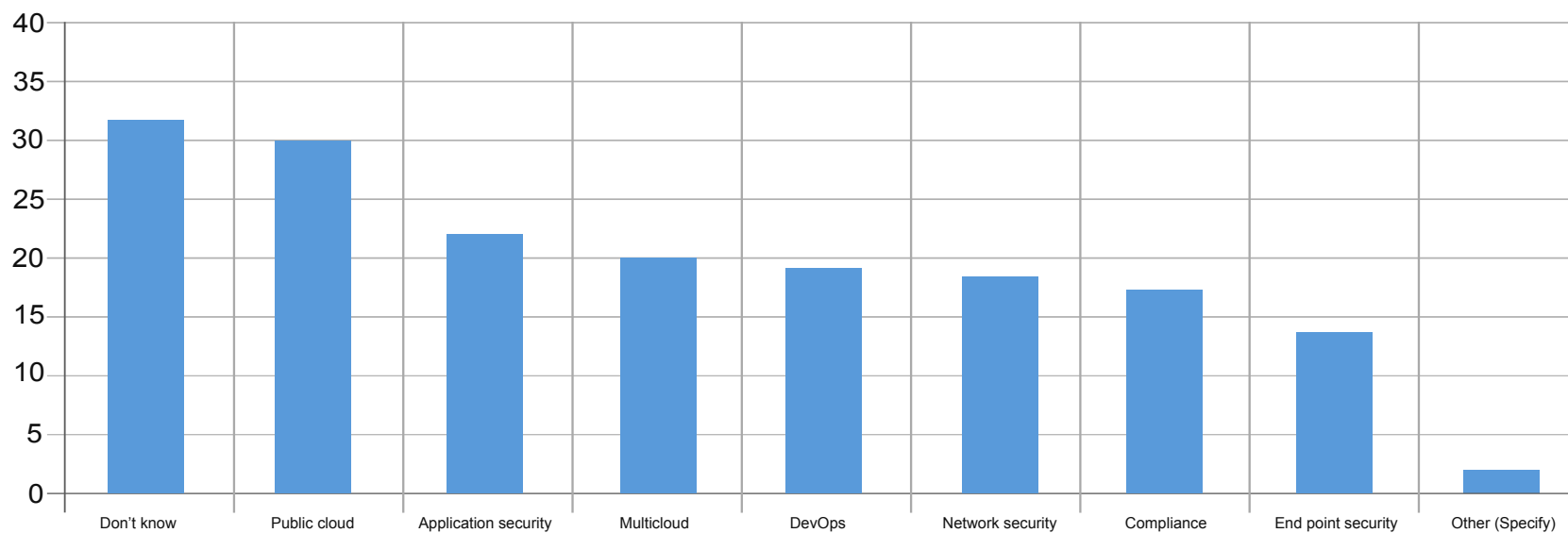
What we learned:

When asked which skills were short in organizations, from a regional perspective,most said they didn't know. 30% said cloud skills had the most shortage, followed by application security (22%).

However, the results were different in the individual countries. Organizations in Nigeria and Cameroon said they had skill shortages while Ghana and Senegal said they didn't.
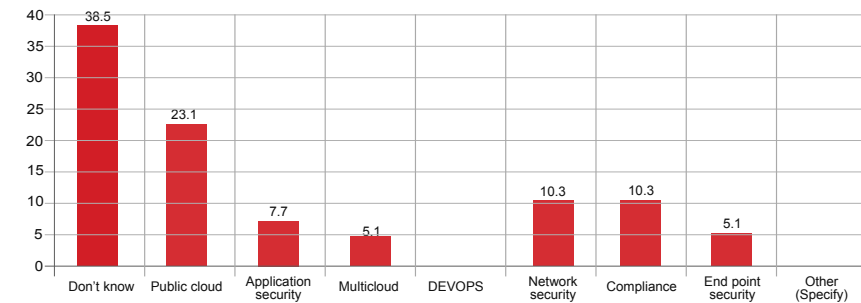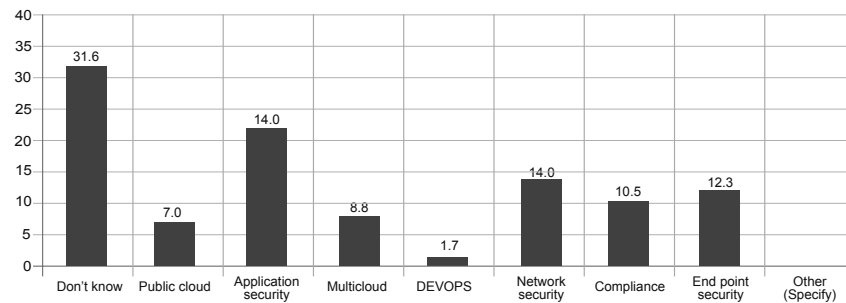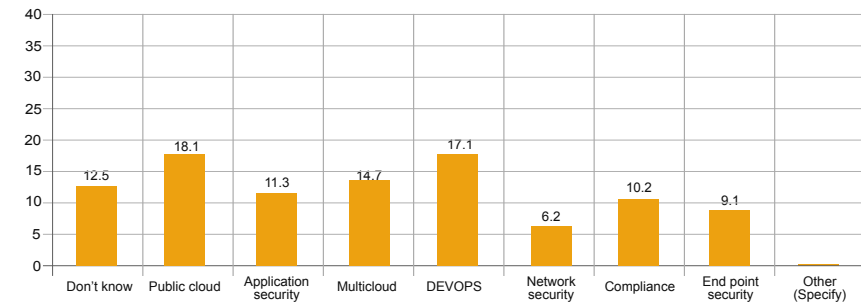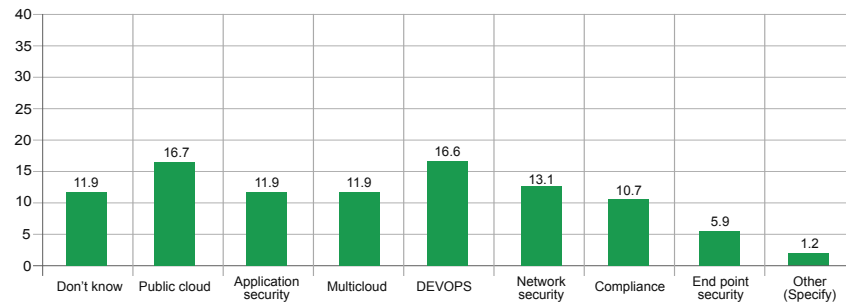

Nigeria (green)
Category	Value
Don't know	11.9
Public cloud	16.7
Application security	11.9
Multicloud	11.9
DEVOPS	16.6
Network security	13.1
Compliance	10.7
End point security	5.9
Other (Specify)	1.2

Cameroon (orange)
Category	Value
Don't know	12.5
Public cloud	18.1
Application security	11.3
Multicloud	14.7
DEVOPS	17.1
Network security	6.2
Compliance	10.2
End point security	9.1
Other (Specify)	

Ghana (black)
Category	Value
Don't know	31.6
Public cloud	7.0
Application security	14.0
Multicloud	8.8
DEVOPS	1.7
Network security	14.0
Compliance	10.5
End point security	12.3
Other (Specify)	

Senegal (red)
Category	Value
Don't know	38.5
Public cloud	23.1
Application security	7.7
Multicloud	5.1
DEVOPS	
Network security	10.3
Compliance	10.3
End point security	5.1
Other (Specify)	

Nigeria   Cameroon   Ghana   Senegal

VII. Conclusion & Recommendations

Organizations, both in the private and public sectors in Africa are adopting digital transformation. Awareness and use of technologies and concepts such as cloud computing, Internet of Things (IoT), machine learning and Artificial Intelligence is growing on the continent. As more processes get digitized and the infrastructure of organizations grow in complexity, information security will become even more critical than it is today. In that regard, here are our key recommendations based on the research.

- Based on the very high interest by organizations to move to the cloud, it is imperative that strategies are developed nationally to guarantee the confidentiality, integrity and availability of systems, especially those categorized as critical information infrastructure.

- Organizations must critically assess their individual needs, consider the benefits and risks of cloud computing before making the move to cloud.

- Considering the shortage of security skills as admitted by organizations in the research, it is very unlikely that organizations have a good security posture on their premise systems today. Therefore there may be significant improved security gains for moving to cloud computing in the region. However, organizations should be cognizant of the fact that cloud computing does not provide improved security by default, as there are still some security responsibilities that lie with the organization. New processes such as (1) contract management including Service Level Agreements (SLAs) for security, (2) access governance, (3) awareness, education, trainings, (4) insurance, (5) crisis management extended to the cloud provider, will become critical when going on the cloud.

- Organizations and policy makers should consider developing strategies to develop and grow skills in the areas of cloud computing, data analytics and security, to meet future demands.

- Leaders should consider immediate staff awareness programs alongside detection technologies, to effectively address the problem of phishing. It may seem like a relief to business leaders that phishing, not ransomware is the most common security threat, but leaders should be concerned since 91% of all cyber attacks start with a phishing email.

VIII. Methodology and Sampling
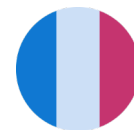
Research Methodology

The survey was conducted between February and May 2021 using both physical and online interview methods. The 150 respondents consisting of senior technical staff members and decision-makers in cybersecurity and IT were drawn from 5 countries in West and Central Africa regions.

Regional demographics

- West Africa (Nigeria, Ghana, Senegal, Ivory Coast): 76.7%

- Central Africa (Cameroon): 23.3%
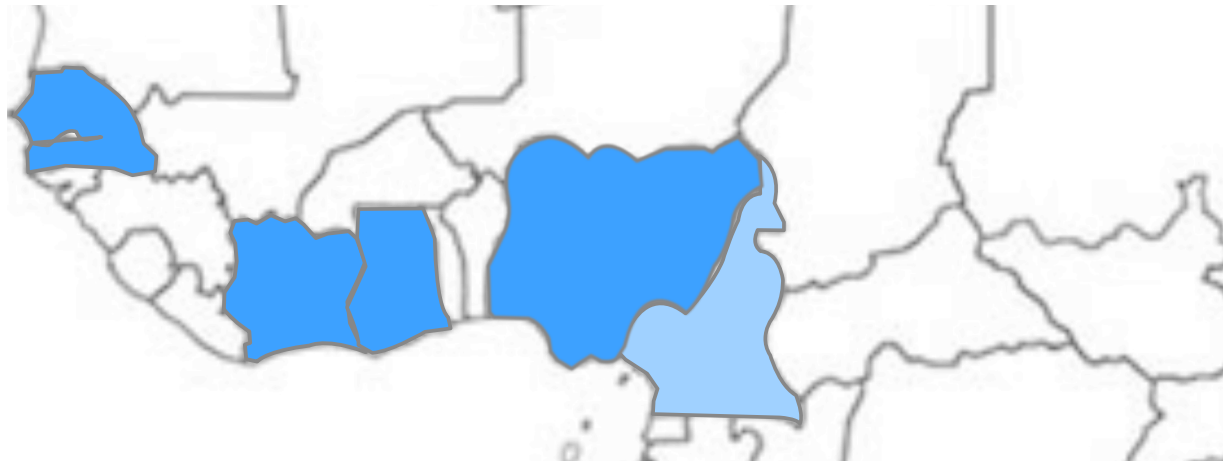
English speaking: 54.4%   French speaking: 45.6%

Industry demographics

24%
Financial services

3.3%
Manufacturing

1.3%
Mining and oil

1.3%
Energy and utilities

2%
Education

26.7%
Technology

5.3%
Public sector

2%
Agriculture

2.7%
Insurance

1.3%
Health

2.7%
Logistics and Travel

28%
Others

About GEFONA

GEFONA DIGITAL FOUNDATION is an independent, non-profit organization that aims to contribute to the development of Africa through original and policy-relevant research on digital technology, digital economy and cybersecurity, including the promotion of initiatives practices on digital development. Our vision is to contribute to the digital development of Africa.

Development Partners

This research is funded by F5 Networks.

Gefona is also grateful for the contribution and support of all its volunteers, without whom the operations of Gefona would not be possible.

2021 Digital Transformation and Application Security Posture in West and Central Africa