

[Webinar] November 19, 2020

Trends in Cloud and Security



Fernando Montenegro
Principal Research Analyst
451 Research – Information Security

Drew Daniels
CIO/CISO
Druva

Avi Shua
CEO & Co-Founder
Orca Security

Sachin Jain
CIO/CISO
Evalueserve

Dmitriy Sokolovskiy
CISO
Avid



Research[®]
Now a Part of

S&P Global Market Intelligence

Copyright © 2020 S&P Global Market Intelligence.
Permission to reprint or distribute any content from this presentation requires the prior written approval of S&P Global Market Intelligence.

Today's speakers


Fernando Montenegro

Principal Research Analyst

451 Research – Information Security


Drew Daniels

CIO/CISO

Druva


Avi Shua

CEO & Co-Founder

Orca Security


Sachin Jain

CIO/CISO

Evalueserve


Dmitriy Sokolovskiy

CISO

Avid



Agenda

Introduction

Context for transformation

Cloud adoption patterns

The impact on security

Panel discussion

Research methodology

451 Voice of the Enterprise

Quarterly Insights:

- Budgets & Outlook
- Workloads & Key Projects
- Organizational Dynamics
- Vendor Evaluations

Additional Surveys:

- DevOps (2H 2019, 1H 2020)
- Coronavirus Flash Surveys
 - Mar 2020, June 2020, Oct 2020

Briefings, Inquiries, Research

100s of hours

- Enterprise IT
- Service providers
- Security vendors
- Finance professionals

Qualitative research

Independent

COVID-19, Digital Transformation, Security

451

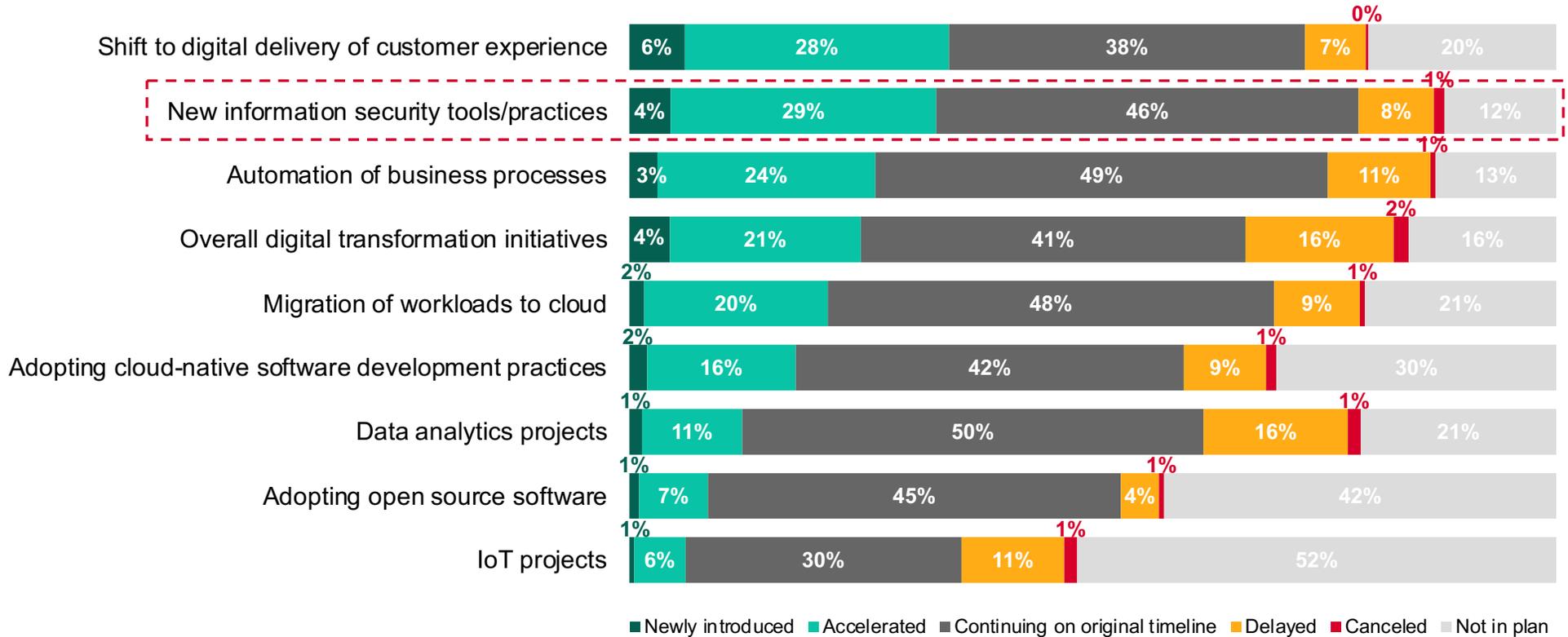
Research

Now a Part of

S&P Global Market Intelligence

Even faced with COVID-19, security investments continue

Q. Some organizations have seen IT initiatives accelerated or delayed as a result of the coronavirus (COVID-19) outbreak. For each of the following types of technology initiatives, please indicate how they were affected at your organization, if at all.



Base: All respondents (n=356-368)
Source: 451 Research's Voice of the Enterprise: Digital Pulse, Coronavirus Flash Survey June 2020



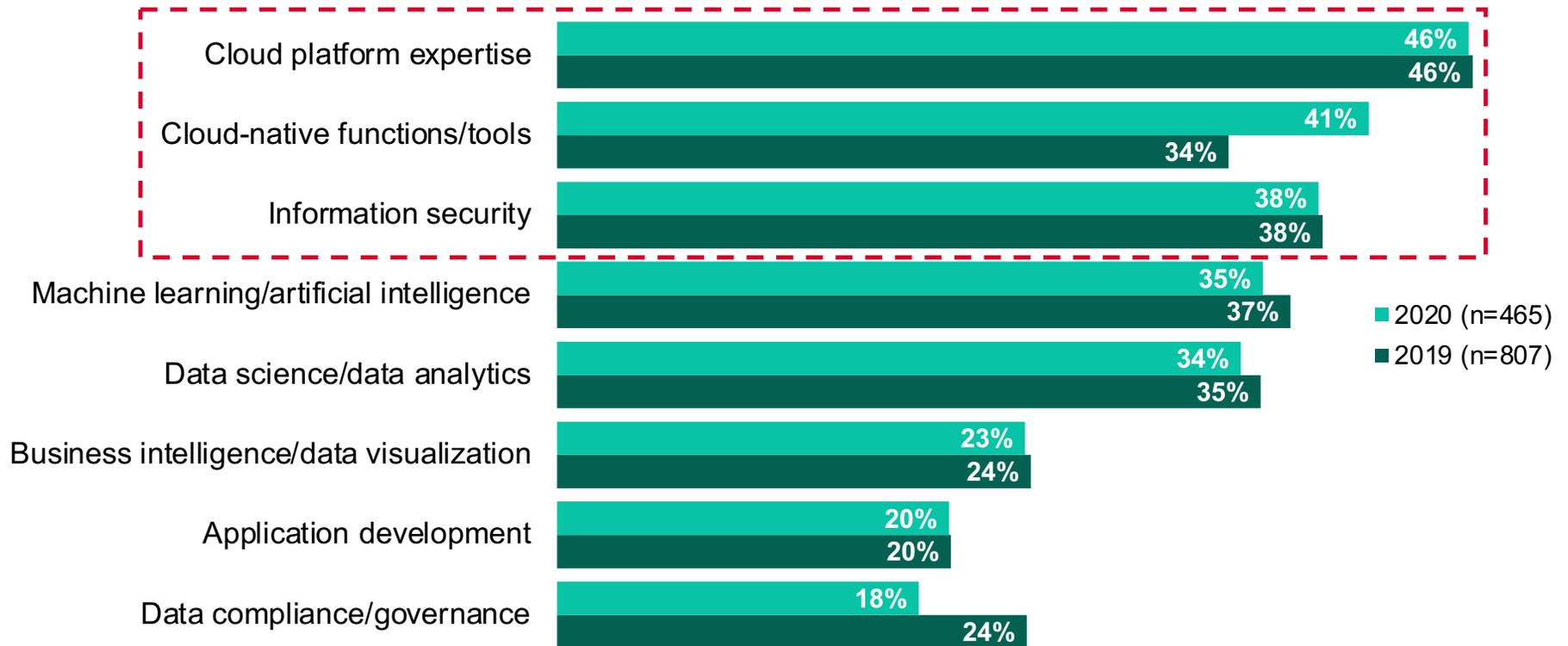
IT is on a journey

Digital transformation is real for **over 90%**

- Nearly 50% executing
- The rest in planning/evaluating

Aiming for larger strategic role (~60%)

In which of the following IT categories, if any, is your organization currently facing an acute skills shortage? Please select all that apply.

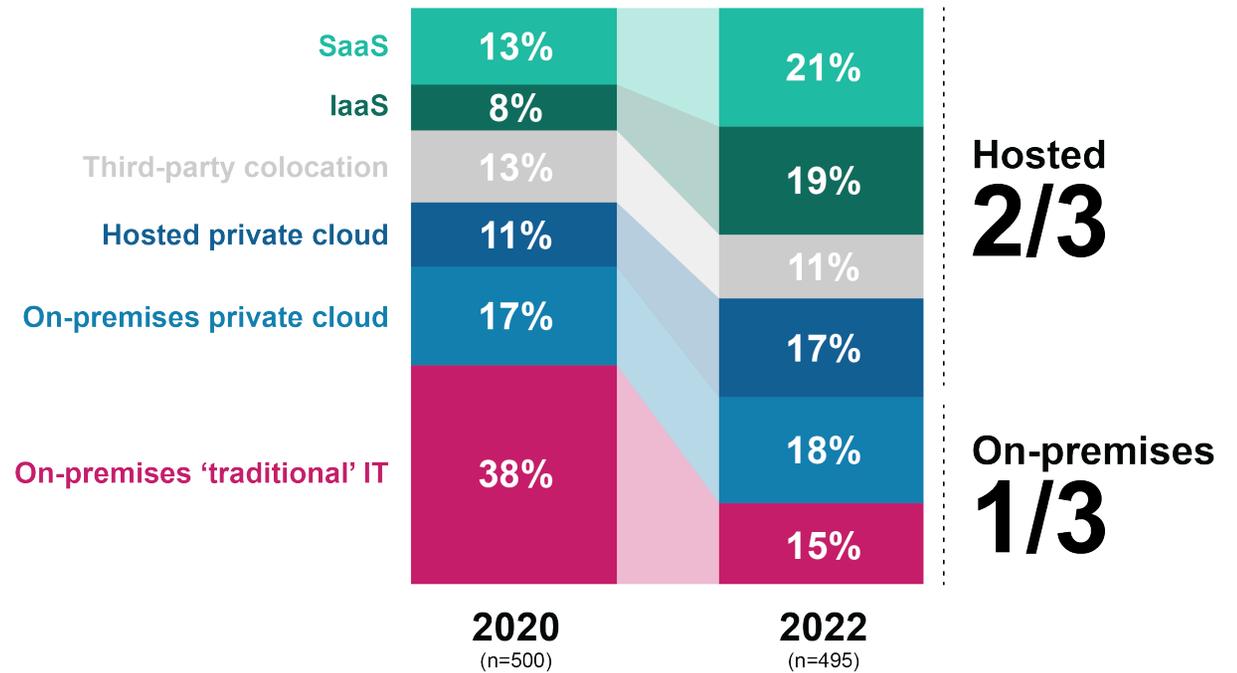


Base: All respondents (n=465)
 Source: 451 Research's Voice of the Enterprise: Digital Pulse, Organizational Dynamics 2020

Adoption Patterns

The future looks...cloudy

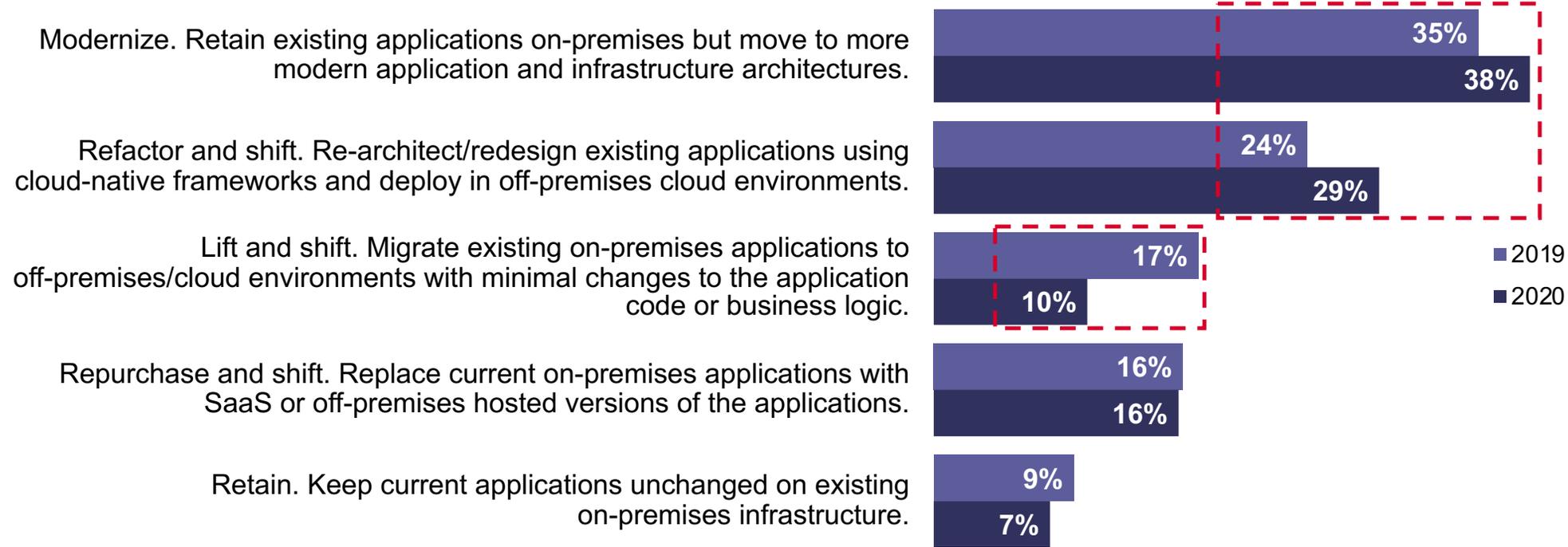
Deployment Location for Workloads/Applications



Q. Thinking about all of your organization's workloads/applications, where are the majority of these currently deployed?
 Q. And thinking about all of your organization's workloads/applications, where will the majority of these be deployed two years from now?
 Base: All respondents
 Source: 451 Research's Voice of the Enterprise: Digital Pulse, Workloads & Key Projects 2020

More nuanced view of modernization destination

Q. Which of the following best describes your organization's approach to mission-critical legacy applications and workloads going forward?

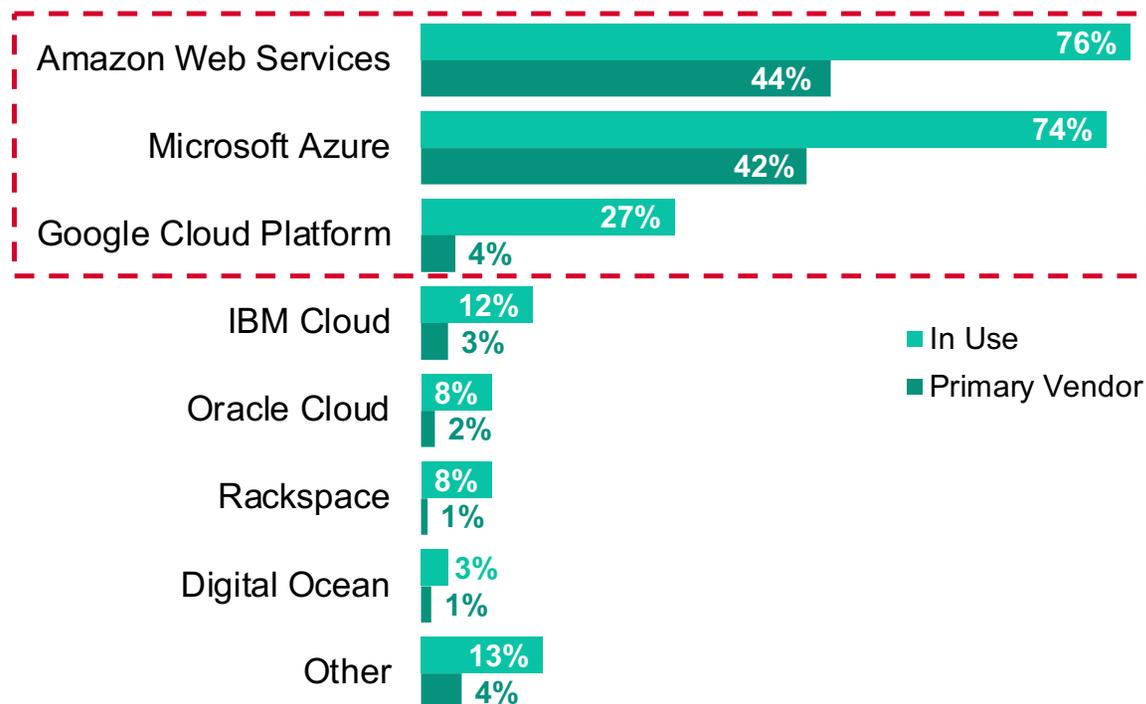


Base: All respondents (n=496)
 Source: 451 Research's Voice of the Enterprise: Digital Pulse, Workloads & Key Projects 2019 & 2020

AWS and Azure dominate the primary public cloud role, with Google Cloud in a complementary role

- Multicloud approaches to using public cloud are common, but the **role of primary vendor is concentrated with AWS and Microsoft Azure** (nearly 90% of public cloud customers identify one of the two as primary).
- AWS holds slight leads over Azure in both usage and primary vendor role. However, it has **significantly larger leads in both categories among businesses with the greatest rates of public cloud spend**, which helps account for its more dominant share of revenue.
- Google Cloud, though rarely cited as primary vendor, is in use by **nearly a third of customers**.
- IBM and Oracle fill more **specialized roles** among the large vendors. Both see **higher usage among top spenders**.
- The **multi-vendor preference** leaves room for alternative clouds, such as Rackspace's cloud, Digital Ocean and others.

Public cloud vendors, in use and primary



Q. Which of the following vendors is your organization currently using for IaaS/PaaS public cloud? Please select all that apply.

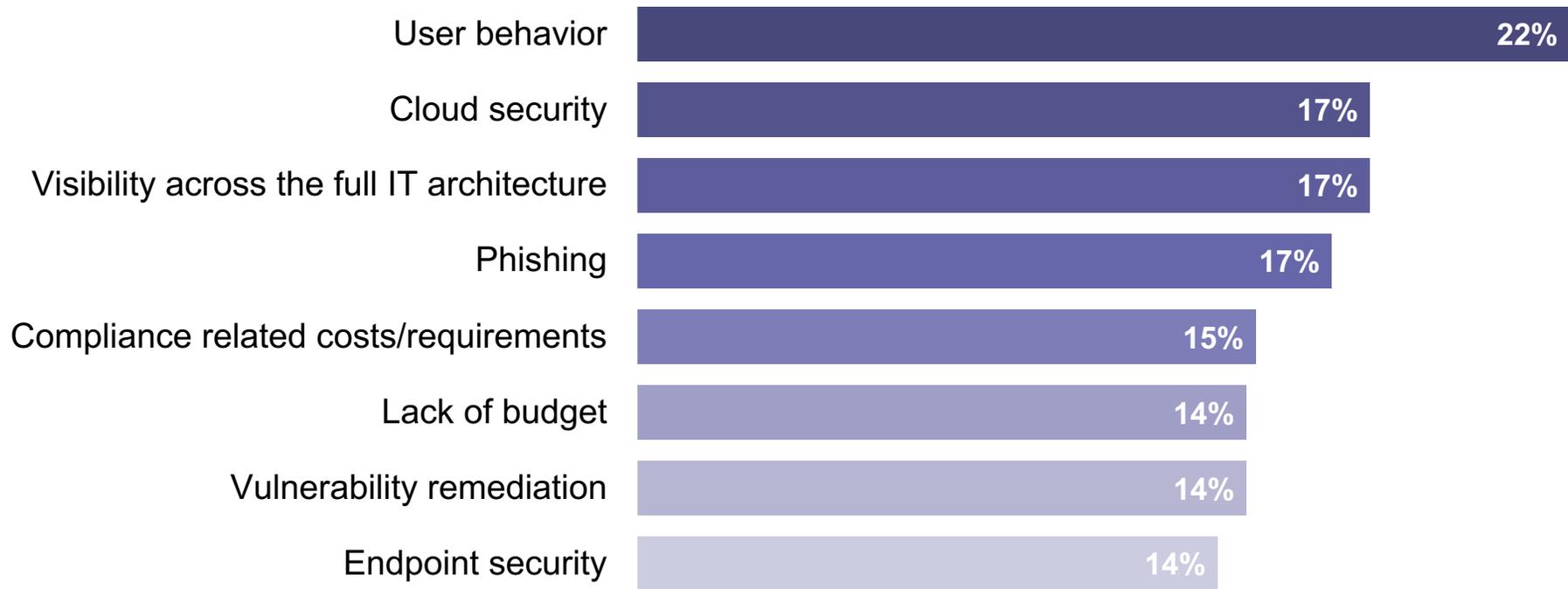
Q. Which of the following vendors do you consider your primary vendor of IaaS/PaaS public cloud?

Base: Selected one or more IaaS/PaaS vendors (n=272)

Source: 451 Research's Voice of the Enterprise: Cloud, Hosting & Managed Services, Vendor Evaluations 2019

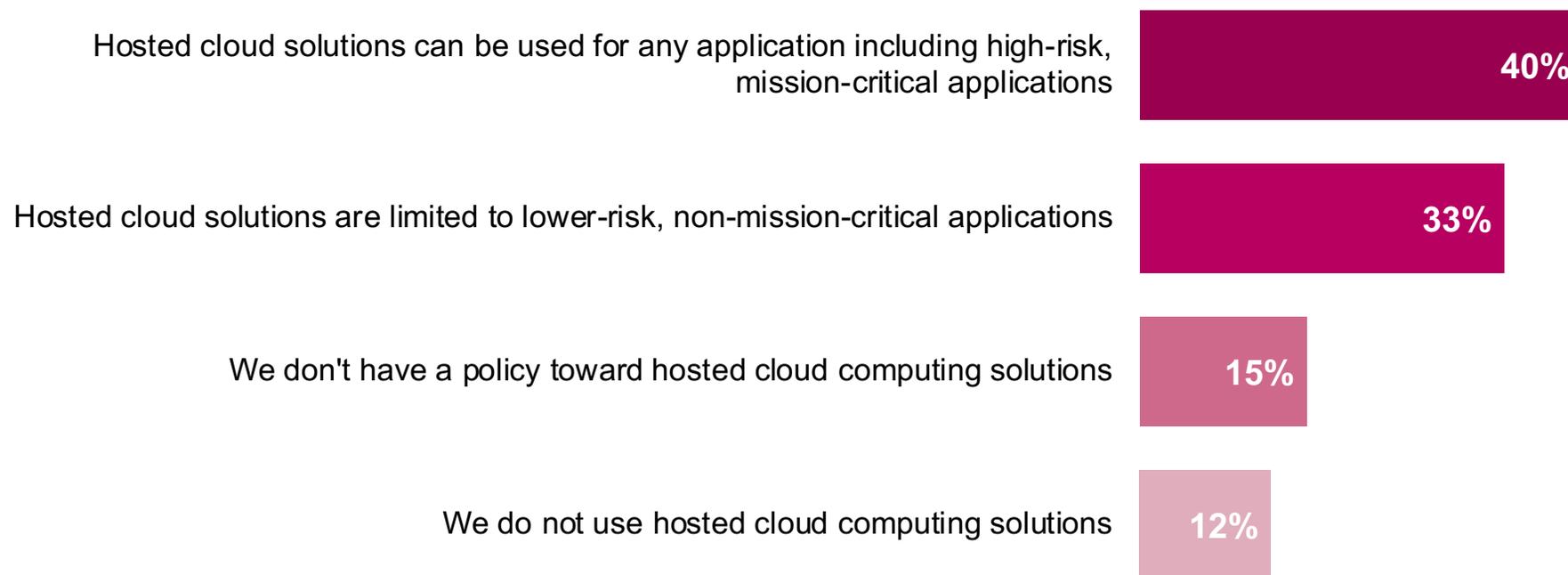
The Impact on Security

What are your organization's top three information security pain points? Please select up to three.



Base: All respondents (n=442)
Source: 451 Research's Voice of the Enterprise: Information Security, Workloads and Key Projects 2020

How would you best describe your organization's policy toward usage of hosted cloud computing solutions (hosted private cloud, IaaS or PaaS) today?



Base: All respondents (n= 464)
Source: 451 Research's Voice of the Enterprise: Information Security, Budgets and Outlook 2020



What is the most likely way you would find out that your hosted cloud solution had been breached?

Our security monitoring infrastructure as applied to the cloud would tell us

48%

Our cloud provider would tell us

38%

Third parties (e.g., a credit processing company, the FBI) would tell us

11%

Other (please specify)

3%

Base: Uses hosted cloud computing architectures (n=352)

Source: 451 Research's Voice of the Enterprise: Information Security, Budgets and Outlook 2020

Copyright © 2020 S&P Global Market Intelligence.

Permission to reprint or distribute any content from this presentation requires the prior written approval of S&P Global Market Intelligence. 16

451

Research

Now a Part of

S&P Global Market Intelligence

Shared responsibility model in context

Customer | Provider

		Cloud IaaS (*)	Cloud PaaS	Cloud SaaS
 Always Customer	Overall Security Accountability	Customer	Customer	Customer
	Identities and Access (IAM) – Application and Cloud	Customer	Customer	Customer
	Data Governance – Security, Privacy	Customer	Customer	Customer
	Security Monitoring and Response	Customer	Customer	Customer
 Varies	Application/Service Business Logic Security	Customer	Customer	Provider
	Application Framework and Services Security	Customer	Shared	Provider
	Operating System Security	Customer	Provider	Provider
 Always Provider	Virtualization Layer	Provider	Provider	Provider
	Compute/Storage	Provider	Provider	Provider
	Network Connectivity	Provider	Provider	Provider
	Physical/Environmental	Provider	Provider	Provider

(*) – Most deployments, except for 'bare metal' and similar offerings

Panel Discussion



Today's speakers


Fernando Montenegro

Principal Research Analyst

451 Research – Information Security


Drew Daniels

CIO/CISO

Druva


Avi Shua

CEO & Co-Founder

Orca Security


Sachin Jain

CIO/CISO

Evalueserve

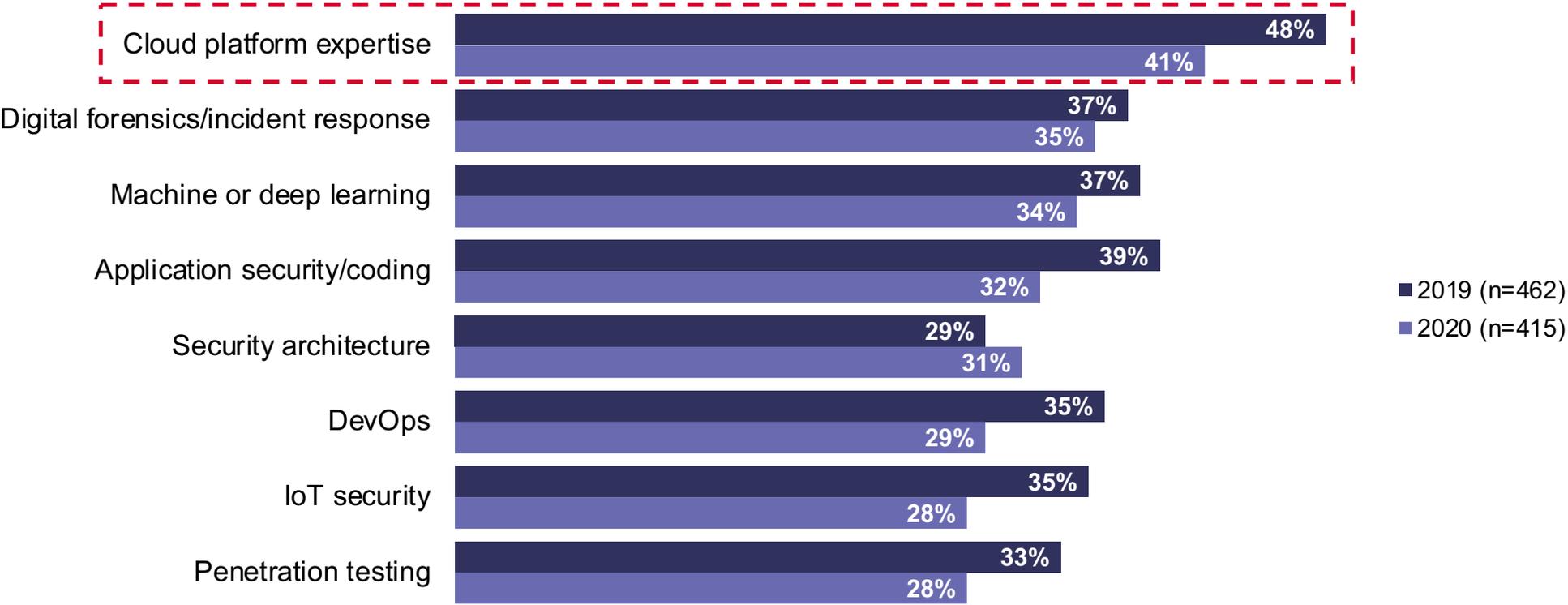

Dmitriy Sokolovskiy

CISO

Avid

Cloud remains current significant gap for infosec

Skillsets inadequately addressed at organization today



Q. And which skillsets are inadequately addressed at your organization today? Please select all that apply.
 Base: All respondents
 Source: 451 Research's Voice of the Enterprise: Information Security, Organizational Dynamics 2019 and 2020

Q1

How are you handling the demand for cloud expertise?

451

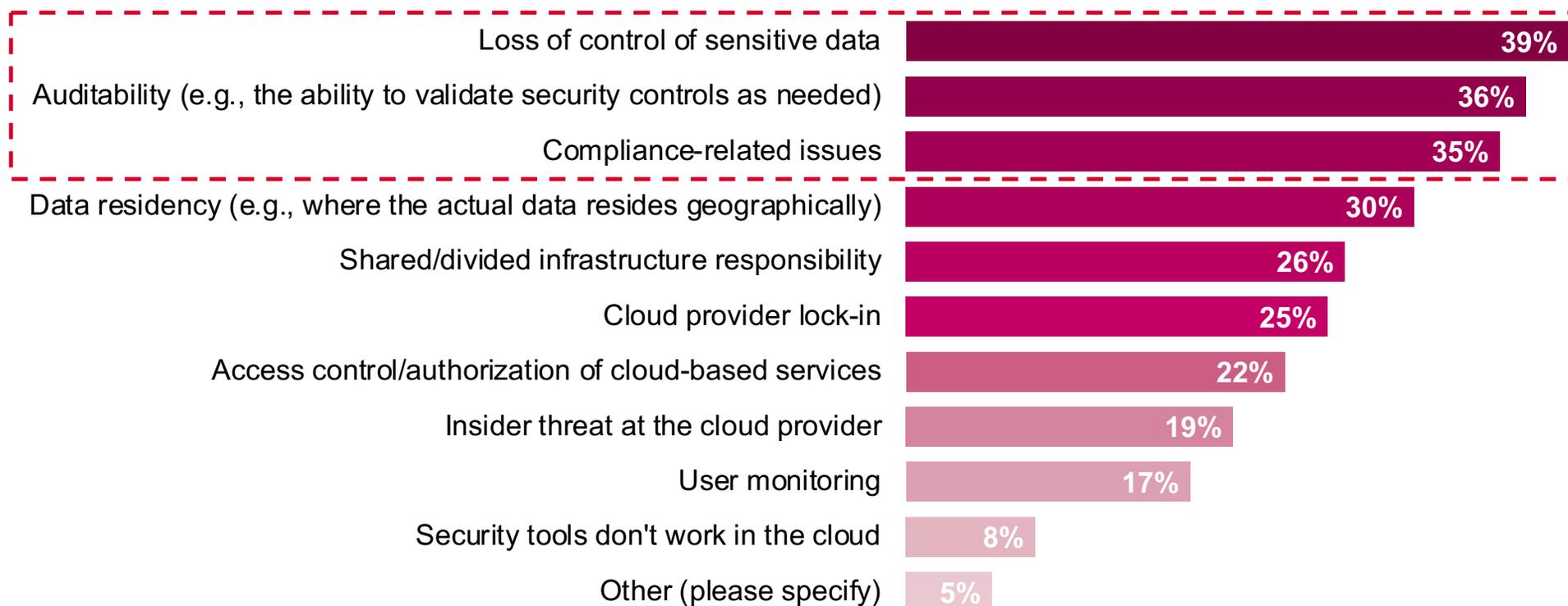
Research

Now a Part of

S&P Global Market Intelligence

Infosec is concerned with runaway cloud usage

Q. What are the top potential issues with hosted cloud solutions (hosted private cloud, IaaS or PaaS)? Please select up to 3.



Base: All respondents (n=199)
Source: 451 Research's Voice of the Enterprise: Information Security, Budgets & Outlook 2020

Q2

What concerns you most about adoption of cloud services?

451

Research

Now a Part of

S&P Global Market Intelligence

The incredibly distributed nature of DevOps

Q. Which of these statements is most accurate regarding DevOps process at your organization?

DevOps processes are managed within different business units, but the organization is aware of them

49%

All DevOps processes are centrally managed by the organization

47%

Some DevOps processes occur without the organization's awareness

4%

Base: All respondents (n=476)
Source: 451 Research's Voice of the Enterprise: DevOps, 2H 2019

451

Research

Now a Part of

S&P Global Market Intelligence

Copyright © 2020 S&P Global Market Intelligence.

Permission to reprint or distribute any content from this presentation requires the prior written approval of S&P Global Market Intelligence. 24

Q3

**How do you work alongside
your cloud engineering team?**

451

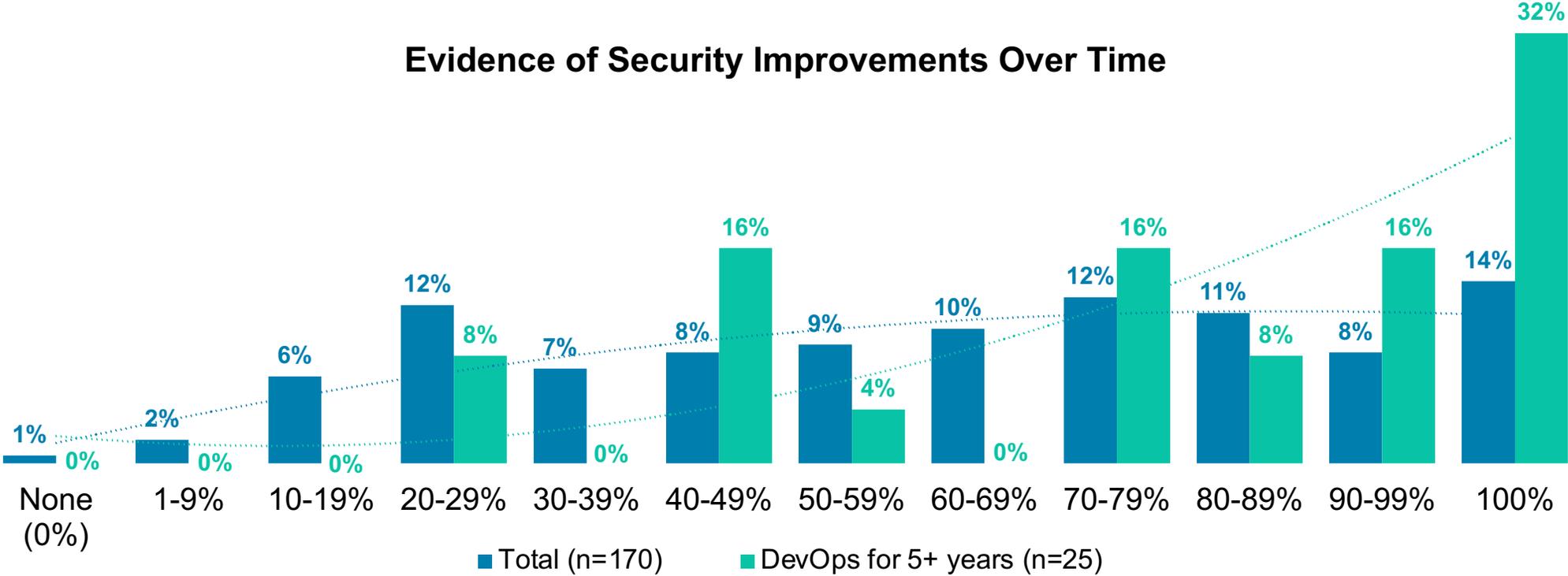
Research

Now a Part of

S&P Global Market Intelligence

Security comes from experience

Evidence of Security Improvements Over Time



Q. Approximately what percentage of your DevOps workflow implementations include security elements?
 Base: Organization uses DevOps at some level, abbreviated fielding (Note: Base sizes below n=30 should be interpreted anecdotally)
 Source: 451 Research's Voice of the Enterprise: DevOps, Workloads & Key Projects 2020

Q4

**What have been
interesting learnings
that you want to share?**

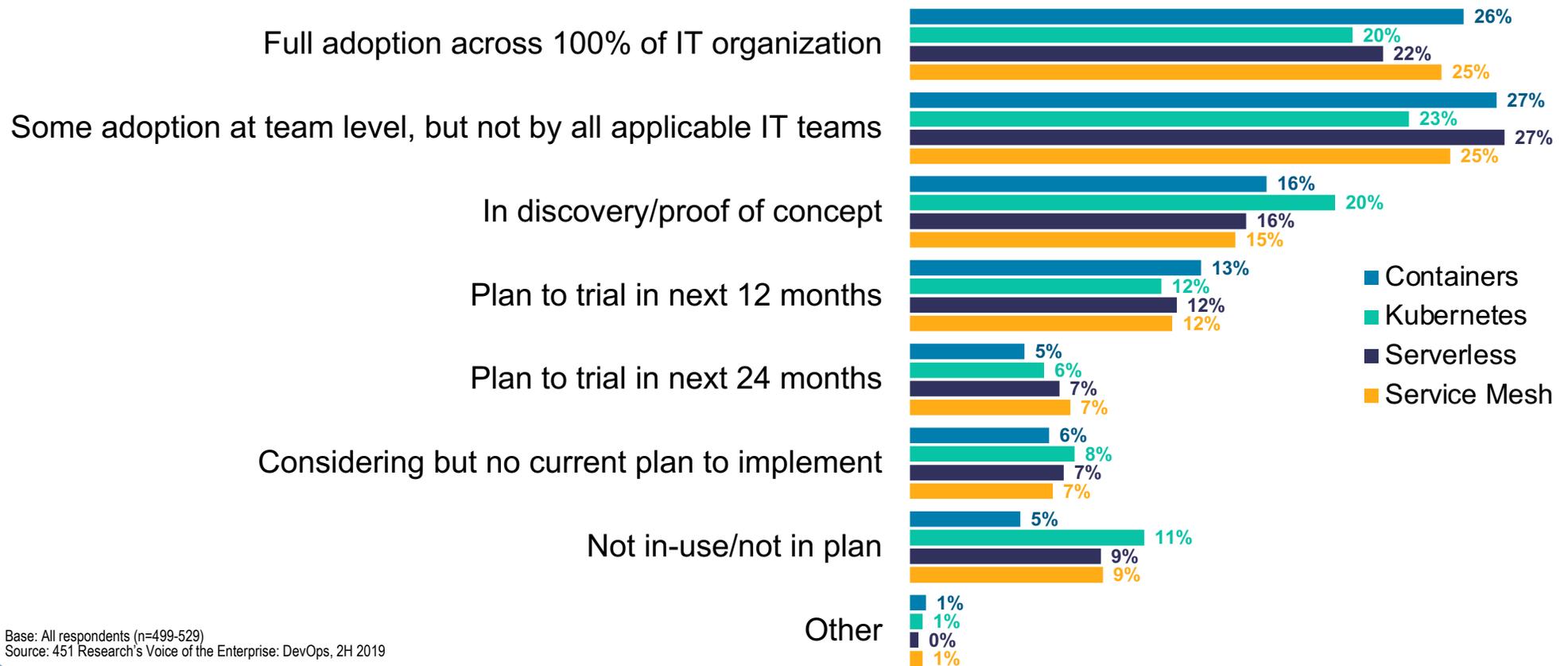
451

Research

Now a Part of

S&P Global Market Intelligence

What is your organization's adoption status for the following technologies? Please select one for each technology.



Base: All respondents (n=499-529)
 Source: 451 Research's Voice of the Enterprise: DevOps, 2H 2019

Q5

What's next for you in terms of cloud adoption?

451

Research

Now a Part of

S&P Global Market Intelligence



SECURITY AND COMPLIANCE FOR AWS, AZURE, AND GCP

- Workload-deep
- Context-aware
- 100% coverage
- No agents

SAMPLE CLIENTS



Enterprise

Top 10 Global
Consultancy

Top 5 Private
Equity Firm

Big 4 Professional
Sports League

Top 5 Global
Hotel Chain

Nasdaq-traded
Internet Services
Firm

Mid-Market



Cloud



Fintech



EVOLUTION OF SECURITY VISIBILITY

HOSTS



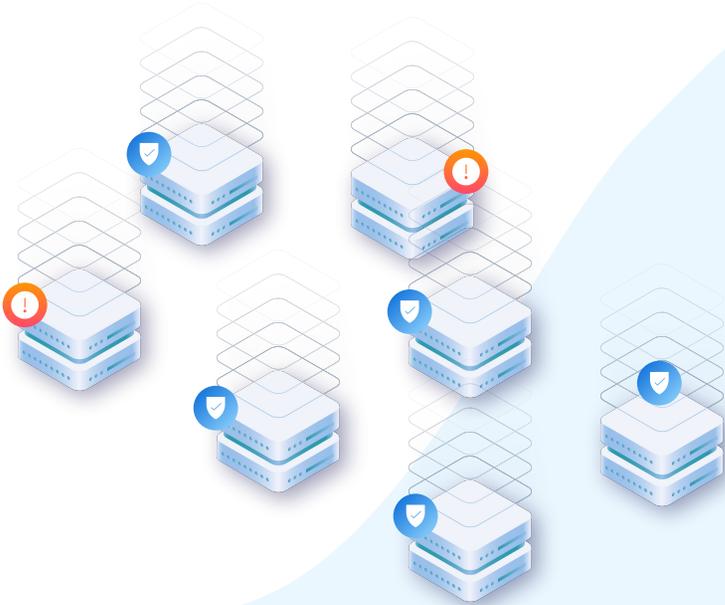
AGENTS



Reside on the Host

Full visibility to OS, Apps and Data

Look for rogue activity



EVOLUTION OF SECURITY VISIBILITY

DATA CENTER



AGENTS

Reside on the Host

Full visibility to OS,
Apps and Data

Look for rogue activity

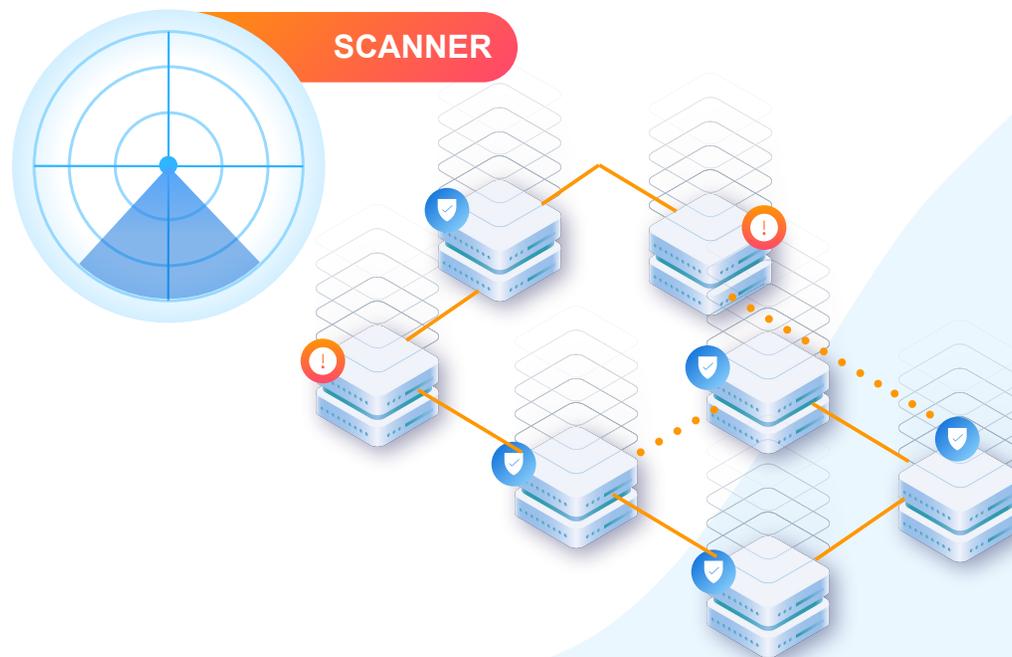


SCANNERS

Reside on the Network

Scan applications like
an adversary

Look for improper response



EVOLUTION OF SECURITY VISIBILITY

DATA CENTER



AGENTS

Reside on the Host

Full visibility to OS,
Apps and Data

Look for rogue activity

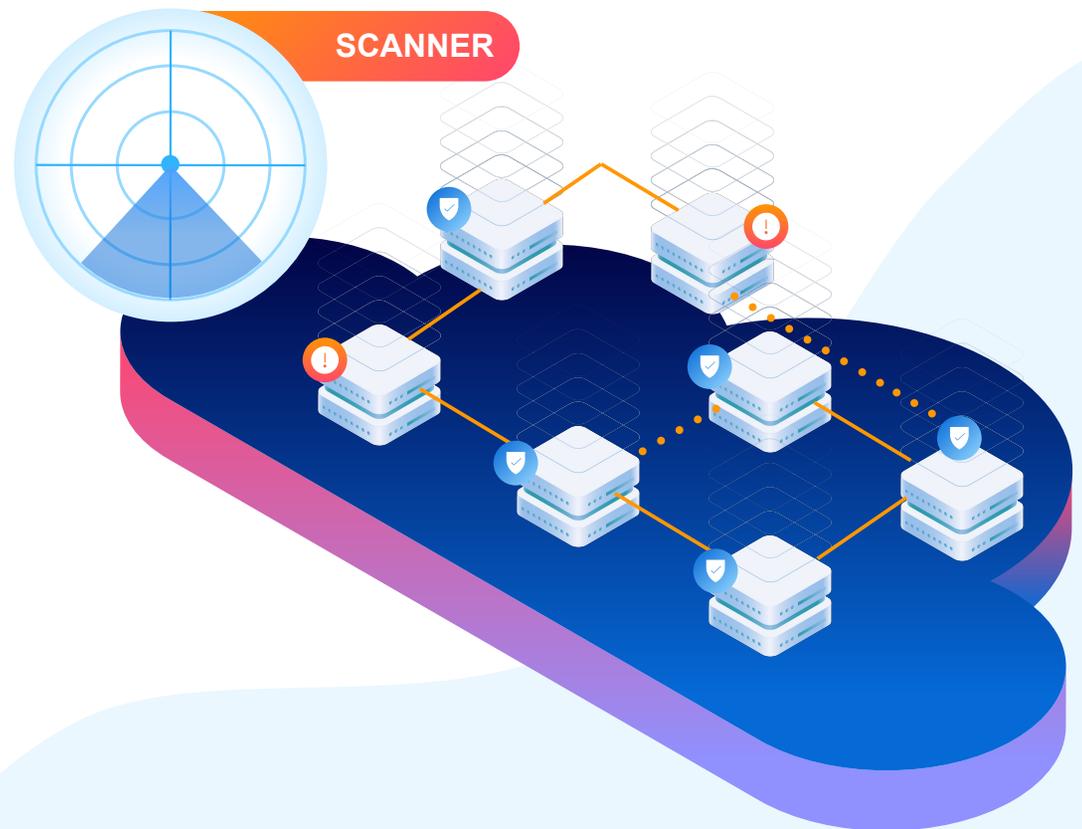


SCANNERS

Reside on the Network

Scan applications like
an adversary

Look for improper response



EVOLUTION OF SECURITY VISIBILITY

DATA CENTER



AGENTS

Reside on the Host

Full visibility to OS,
Apps and Data

Look for rogue activity

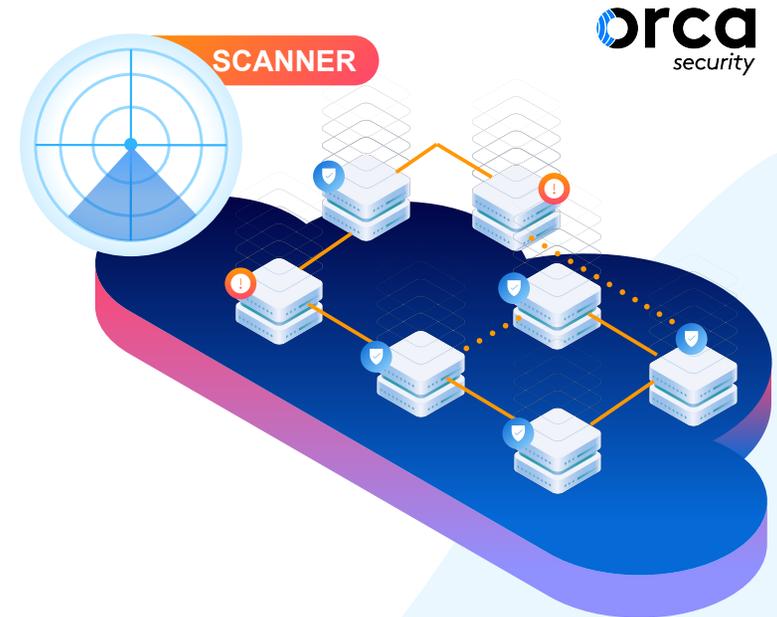


SCANNERS

Reside on the Network

Scan applications like
an adversary

Look for improper response



EVOLUTION OF SECURITY VISIBILITY

CLOUD



AGENTS

Reside on the Host

Full visibility to OS, Apps and Data

Look for rogue activity



SCANNERS

Reside on the Network

Scan applications like an adversary

Look for improper response

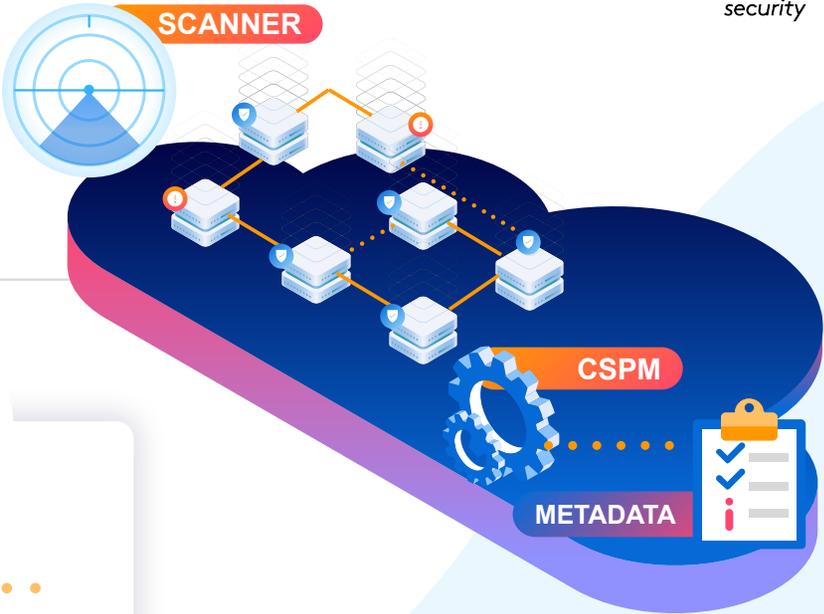


CSPM

Reside in the Cloud

Examine Cloud metadata

Look for deviations and misconfigurations



HOWEVER, IN REALITY

AGENTS DO NOT SCALE

FACT

On average less than 50% of cloud assets are covered by host security solutions

-
- Virtually impossible to deploy everywhere
 - Requires DevOps cooperation

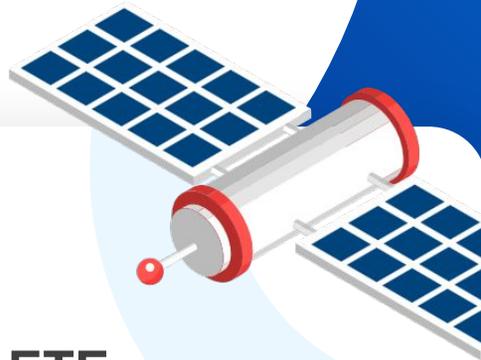
OVERLOAD OF SECURITY ALERTS

FACT

For every 100 assets there are on average 10,000 vulnerabilities detected

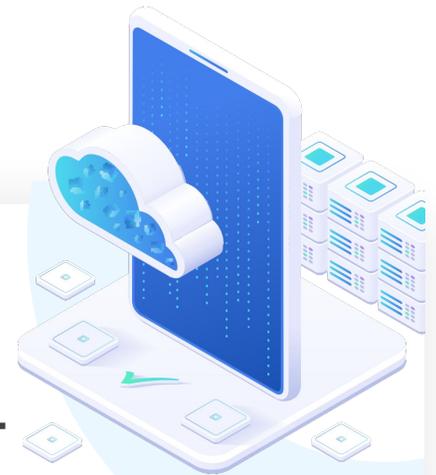
-
- Multiple tools working in silos
 - Prioritization is difficult

INTRODUCING OUR PATENT-PENDING
SIDESCANNING™



—
**COMPLETE
COVERAGE**

Entire estate covered
within minutes



—
**CONTEXT
AWARE**

Automatically de-prioritize
99.9% of the alerts



SIDESCANNING™

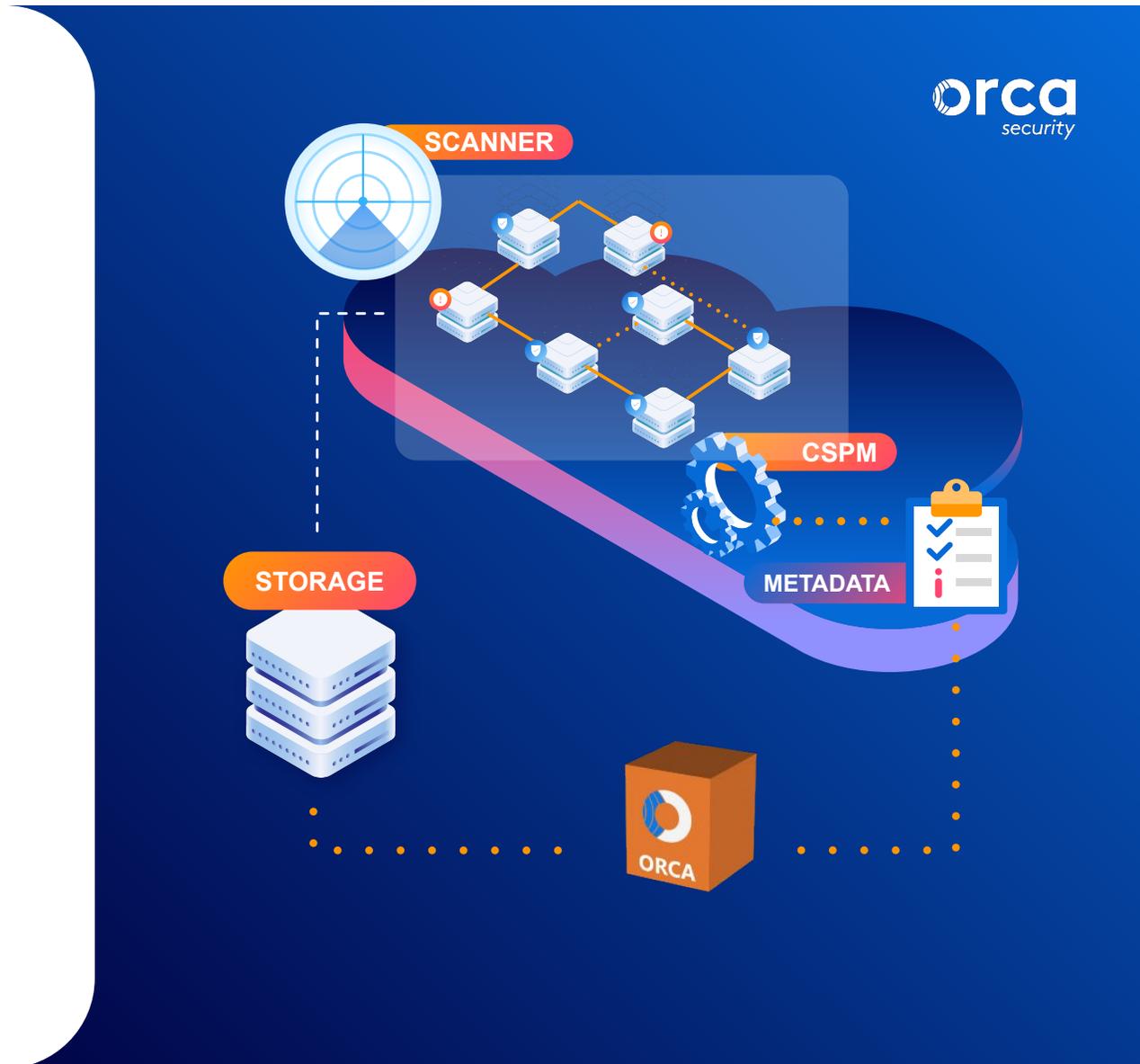
HOW?

**Eliminate the need for Agents,
Scanners and CSPM**

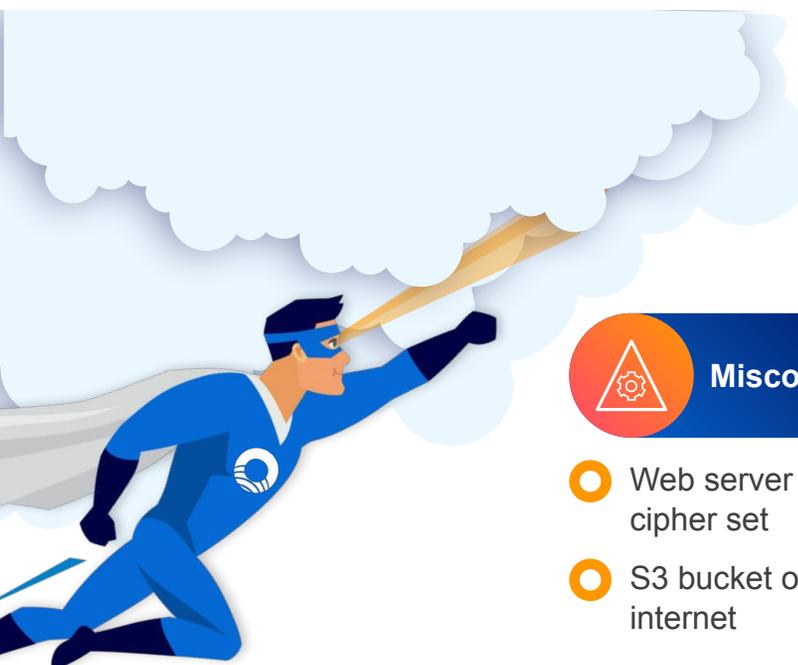
Collect data directly from

- Workload runtime block storage
- Cloud metadata

**Gain immediate understanding of
entire estate security deficiencies
and their relative importance**



COMPLETE SECURITY



Misconfigurations

- Web server using weak cipher set
- S3 bucket open to the internet

Vulnerabilities

- OS, Packages and libraries
- E.g. Vulnerable tomcat server

Misplaced PII

- Customer data not properly secured
- e-mail addresses, users lists, credit card data

Full stack asset inventory

- Cloud native and workload constructs
- Down to the application version

Compromised Assets

- Malware infection
- Unexpected changes

Lateral Movement Risk

- Insecure keys
- Improper segmentation

Authentication risks

- Weak and leaked credentials
- Overly privileged roles

SIDESCANNING™ BENEFITS



**SEAMLESS
DELIVERY!**



COMPLETE VISIBILITY

- Sees exactly what the workload sees



IMMEDIATELY ATTACHED

- New workload automatically scanned
- No need for DevOps cooperation



ZERO IMPACT

- Read-Only access
- Scanning occurs on the Orca host
- No performance penalty
- No potential side effects to workload



CONTEXT

- Risks are prioritized according to your environment



TAMPER PROOF

- Even if the workload is compromised, Orca is not

UNDERSTANDING CONTEXT



CLOUD METADATA

Logs

Policies

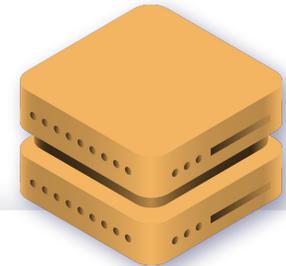
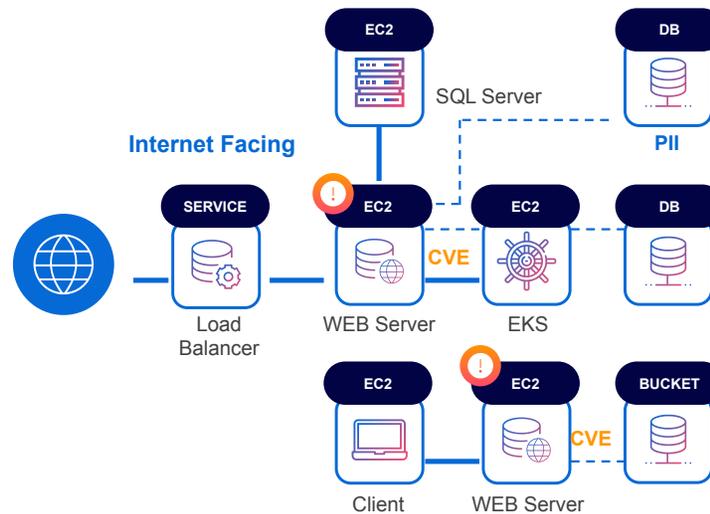
VPCs

Networking

IAM Roles

Security Groups

ORCA CONTEXT MAP



SHARED STORAGE BASED VMs

Running Services

Reverse Proxies

App Config

Firewall Config

Docker Config

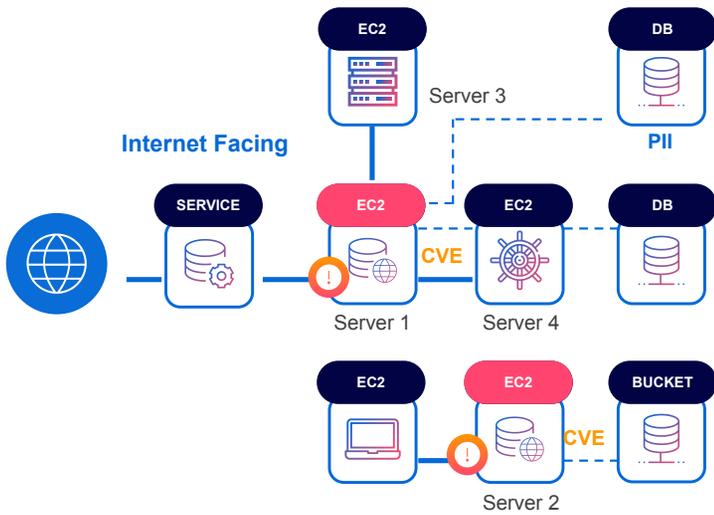
Discover Cloud assets

Identify asset roles

Identify connectivity and trust

Identify risk

UNDERSTANDING CONTEXT



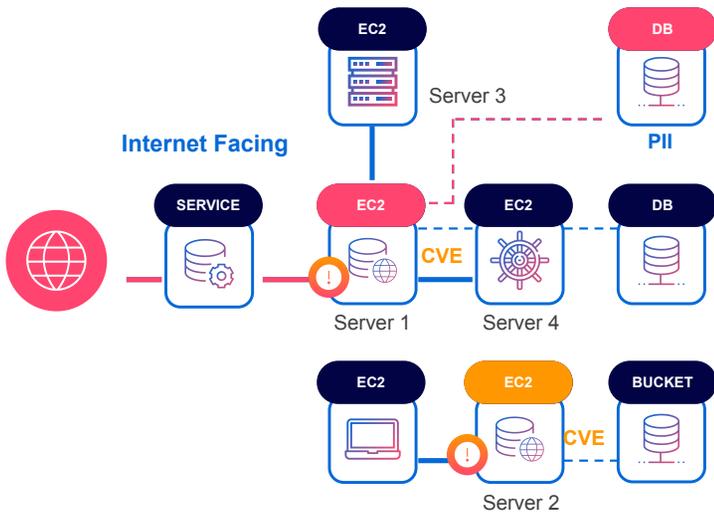
AGENT APPROACH



	Asset	Service	Issue	Type	Score
!	Server 1	Apache	CVE-2018-1176	RCE	High 8.8
!	Server 2	Apache	CVE-2018-1176	RCE	High 8.8
✓	Server 3	SQL	--	--	None
✓	Server 4	EKS	--	--	None

Identical Severity Score

UNDERSTANDING CONTEXT



ORCA SECURITY



	Asset	Service	Issue	Risk	Score
🚨	Server 1	Apache	CVE-2018-1176	Internet-facing PII Exposure	Imminent
⚠️	Server 2	Apache	CVE-2018-1176	Internal server	Medium
🛡️	Server 3	SQL	--	--	None
🛡️	Server 4	EKS	--	--	None

Severity Score According to Context

CONTEXT BENEFITS



BETTER PRIORITIZATION

EXAMPLE

A Host that's connected to the Internet is more at risk than those that aren't



IDENTIFY HIDDEN BREACHES

EXAMPLE

Unexpected differences between clustered hosts can indicate a breach



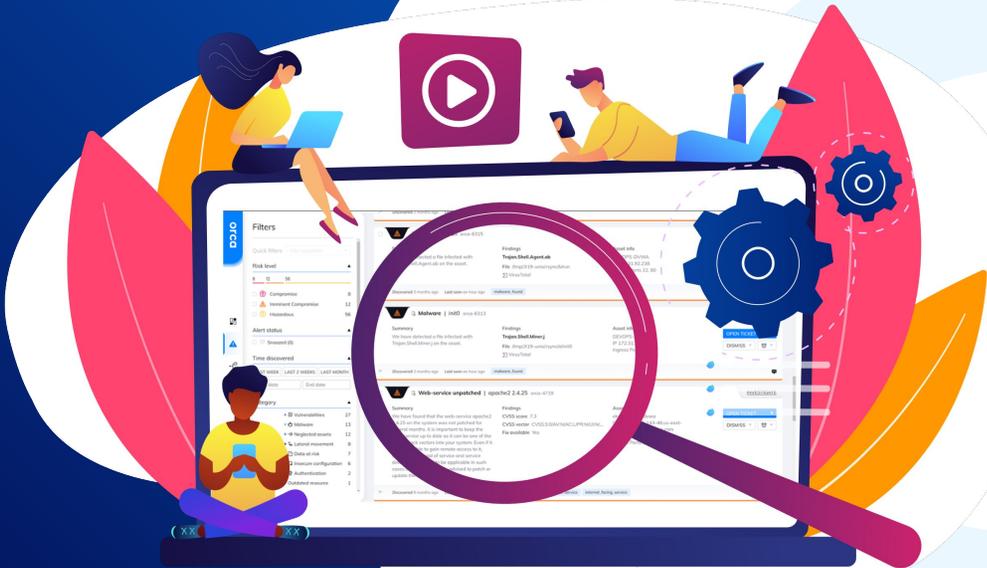
DATA MISPLACEMENT

EXAMPLE

Over privileged IAM role found on a host, lateral movement risk



CONTEXT MATTERS!



ORCA SECURITY PRODUCT DEMO



THANK YOU!

Free trial demo at: orca.security

Thank you

Fernando Montenegro
Principal Research Analyst
451 Research – Information Security

Drew Daniels
CIO/CISO
Druva

Avi Shua
CEO & Co-Founder
Orca Security

Sachin Jain
CIO/CISO
Evalueserve

Dmitriy Sokolovskiy
CISO
Avid

Contact Us:

451 Research:
US +1 212.505.3030
EUROPE +44 (0) 203.929.5700

S&P Global Market Intelligence:
US +1 877.863.1306
EUROPE +44 (0) 20.7176.1234

451research.com
spglobal.com/marketintelligence

451

Research

Now a Part of

S&P Global Market Intelligence

Copyright © 2020 S&P Global Market Intelligence.

Permission to reprint or distribute any content from this presentation requires the prior written approval of S&P Global Market Intelligence. 30

Copyright © 2020 by S&P Global Market Intelligence, a division of S&P Global Inc. All rights reserved.

These materials have been prepared solely for information purposes based upon information generally available to the public and from sources believed to be reliable. No content (including index data, ratings, credit-related analyses and data, research, model, software or other application or output therefrom) or any part thereof (Content) may be modified, reverse engineered, reproduced or distributed in any form by any means, or stored in a database or retrieval system, without the prior written permission of S&P Global Market Intelligence or its affiliates (collectively, S&P Global). The Content shall not be used for any unlawful or unauthorized purposes. S&P Global and any third-party providers, (collectively S&P Global Parties) do not guarantee the accuracy, completeness, timeliness or availability of the Content. S&P Global Parties are not responsible for any errors or omissions, regardless of the cause, for the results obtained from the use of the Content. THE CONTENT IS PROVIDED ON "AS IS" BASIS. S&P GLOBAL PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, FREEDOM FROM BUGS, SOFTWARE ERRORS OR DEFECTS, THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED OR THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION. In no event shall S&P Global Parties be liable to any party for any direct, indirect, incidental, exemplary, compensatory, punitive, special or consequential damages, costs, expenses, legal fees, or losses (including, without limitation, lost income or lost profits and opportunity costs or losses caused by negligence) in connection with any use of the Content even if advised of the possibility of such damages.

S&P Global Market Intelligence's opinions, quotes and credit-related and other analyses are statements of opinion as of the date they are expressed and not statements of fact or recommendations to purchase, hold, or sell any securities or to make any investment decisions, and do not address the suitability of any security. S&P Global Market Intelligence may provide index data. Direct investment in an index is not possible. Exposure to an asset class represented by an index is available through investable instruments based on that index. S&P Global Market Intelligence assumes no obligation to update the Content following publication in any form or format. The Content should not be relied on and is not a substitute for the skill, judgment and experience of the user, its management, employees, advisors and/or clients when making investment and other business decisions. S&P Global Market Intelligence does not endorse companies, technologies, products, services, or solutions.

S&P Global keeps certain activities of its divisions separate from each other in order to preserve the independence and objectivity of their respective activities. As a result, certain divisions of S&P Global may have information that is not available to other S&P Global divisions. S&P Global has established policies and procedures to maintain the confidentiality of certain non-public information received in connection with each analytical process.

S&P Global may receive compensation for its ratings and certain analyses, normally from issuers or underwriters of securities or from obligors. S&P Global reserves the right to disseminate its opinions and analyses. S&P Global's public ratings and analyses are made available on its Web sites, www.standardandpoors.com (free of charge) and www.ratingsdirect.com (subscription), and may be distributed through other means, including via S&P Global publications and third-party redistributors. Additional information about our ratings fees is available at www.standardandpoors.com/usratingsfees.