REPORT REPRINT

This report, licensed to Orca Security, developed and as provided by 451 Research, LLC, was published as part of our syndicated Technology & Business Insight subscription service. It shall be owned in its entirety by 451 Research, LLC. This report is solely intended for use by the recipient and may not be reproduced or re-posted, in whole or in part, by the recipient without express permission from 451 Research.

451 Research

S&P Global
Market Intelligence

THOUGHT LEADERSHIP

NOV 2020

Cloud Security Is a Team Sport

Fernando Montenegro, Principal Research Analyst, Information Security

Hiding underneath the surface of discussions about cloud security is a massive realignment of security functionality and needs, both in terms of what is offered by technology vendors and how customers are likely to consume it. This will impact all stakeholders and will require much higher degrees of collaboration, in context of vendor collaboration as well as internal collaboration with customers.

©2021 451 Research, LLC | WWW.451RESEARCH.COM

About the Author

Fernando Montenegro

Principal Research Analyst, Information Security

Fernando is a Principal Research Analyst on the Information Security team at 451 Research, a part of S&P Global Market Intelligence. He is based out of Toronto, Canada. He has broad experience in security architecture for enterprise environments. He currently focuses on covering primarily the endpoint security and cloud security markets.

Prior to joining 451 Research, Fernando worked in pre-sales and delivery roles with both startups and established security vendors focusing on different aspects of enterprise security. His areas of interest include security economics (particularly behavior economics), security-focused data science, and cloud-native security. Fernando holds a BSc. in Computer Science and several industry certifications.

©COPYRIGHT 2021 451 RESEARCH. ALL RIGHTS RESERVED.

Key Findings

- Concerns related to securing cloud environments or data security are regularly listed by IT practitioners as top issues preventing or delaying cloud adoption. Cloud service providers have responded with significant capabilities and guidance, and third-party vendors have also positioned themselves to address this need.
- Approximately 72% of respondents to our *Voice of the Enterprise (VotE): Cloud, Hosting and Managed Services, Workloads and Key Projects 2019* survey indicate that their organizations use services from two or more cloud providers. While this is common, it is more likely that individual project teams within organizations focus on a single cloud environment.
- Security teams indicate that they currently face gaps in cloud platform skills and are concerned with issues related to runaway cloud usage, how to verify controls and how to report compliance. Many customers indicate they plan to use cloud provider services, but many also plan to use third-party tools.
- Inside organizations, modern DevOps teams indicate that they recognize security as a key stakeholder in DevOps adoption and are working toward including better security capabilities within their projects, something that more established teams can achieve more often.

©COPYRIGHT 2021 451 RESEARCH. ALL RIGHTS RESERVED.

Executive Summary

Introduction

This report investigates topics, trends, challenges and recommendations for securing cloud-based environments. The crux of the matter is that, given the increasingly distributed nature and increased agility of modern IT, there's no way to address these demands without thinking carefully about how the different teams work together. More than at any other time, cloud security truly becomes a team sport.

The notion of team-like collaboration manifests itself in two key scenarios. First, there is a need for collaboration between vendors such as cloud service providers (CSPs), third-party security vendors and, potentially, services firms as customers indicate they are looking to secure their cloud deployments via a combination of methods involving all three types of partners.

Second is the idea of cloud security as a team sport, which is meant to reflect the deep levels of collaboration that organizations must achieve internally. Our research shows both that key practices such as DevOps are highly distributed within the organization and that security teams indicate a gap in having sufficient cloud platform expertise. These two factors, coupled with what is likely a risk management model that still places a heavy responsibility on security teams, dictates that building and operating cloud security practices should be a very collaborative exercise.

This report touches on the different areas of cloud security but focuses on customer efforts for securing infrastructure built on top of what is generally considered IaaS and PaaS. We look at two key 'megatrends' – the increased presence of security functionality in broader technology products/services, and the distributed nature of work within organizations – that highlight more tactical trends affecting cloud security. This report then considers the impact of these trends on different types of stakeholders and lists potential challenges moving forward.

©COPYRIGHT 2021 451 RESEARCH. ALL RIGHTS RESERVED.

Methodology

This report includes observations on cloud security trends derived from a combination of two key sources: briefings with numerous stakeholders – security, cloud security and cloud management vendors, CSPs, managed services providers, selected executive-level and technical-level practitioners at different organizations, among others – and the results from our various VotE surveys that focus on data from 2019 and 2020. The data is presented alongside our interpretation of these trends in the context of impact to different stakeholders and discussion of possible future challenges.

Reports such as this one represent a holistic perspective on key emerging markets in the enterprise IT space. These markets evolve quickly, though, so 451 Research offers additional services that provide critical marketplace updates. These updated reports and perspectives are presented on a daily basis via the company's core intelligence service, 451 Research Market Insight. Forward-looking M&A analysis and perspectives on strategic acquisitions and the liquidity environment for technology companies are also updated regularly via Market Insight, which is backed by the industry-leading 451 Research M&A KnowledgeBase.

Emerging technologies and markets are covered in 451 Research channels including Applied Infrastructure & DevOps; Cloud & Managed Services Transformation; Cloud Native; Customer Experience & Commerce; Data, AI & Analytics; Datacenter Services & Infrastructure; Information Security; Internet of Things; and Workforce Productivity & Collaboration.

Beyond that, 451 Research has a robust set of quantitative insights covered in products such as Voice of the Enterprise, Voice of the Connected User Landscape, Voice of the Service Provider, Cloud Price Index, Market Monitor, the M&A KnowledgeBase and the Datacenter KnowledgeBase.

All of these 451 Research services, which are accessible via the web, provide critical and timely analysis specifically focused on the business of enterprise IT innovation.

For more information about 451 Research, please go to: *www.451research.com*

©COPYRIGHT 2021 451 RESEARCH. ALL RIGHTS RESERVED.

Table of Contents

©COPYRIGHT 2021 451 RESEARCH. ALL RIGHTS RESERVED.

©COPYRIGHT 2021 451 RESEARCH. ALL RIGHTS RESERVED.

1. What's In a Name?

Shakespeare may have written that "A rose by any other name would smell as sweet," but our reality in modern organizations is that we must be precise in our usage of terminology, lest our troubles be much ado about something, indeed.

When discussing cloud security with different stakeholders, particularly those such as senior IT leadership or those with a broader view of technology, part of the conversation invariably must include a disambiguation step: Are we talking about cloud security as meaning "how we secure our corporate actions using cloud services," or is cloud security about "creating IT functionality on the cloud and securing those environments"? In one case, this leads organizations down the path of cloud access security brokers (CASBs) and security for SaaS applications, while another leads down the path of securing back-end infrastructure that the organization is creating within public cloud providers such as Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP), among others, or even within their private clouds or hosted private clouds.

We think this differentiation is essential. While ultimately both areas can – and should – be rolled up into a cohesive security architecture for the organization, each area has very distinct needs, workflows and operating tempos.

When thinking of security for SaaS applications, CASB and others, the typical security architect is looking inward to the organization: how do the totality of the organization's users – IT teams and regular business users – consume cloud resources? How are they interacting with external services – some of which the architect may know nothing about? Are they leaking business information, knowingly or not? How does the organization govern access to data hosted on those cloud services? Making changes to the decisions around these topics is something that may be done as new services are consumed, new business units formed and teams hired and so on. The threats against this usage will vary, but are more typically associated with theft or loss of business records, or information pivoting from compromised single user accounts or application administrator accounts.

©COPYRIGHT 2021 451 RESEARCH. ALL RIGHTS RESERVED.

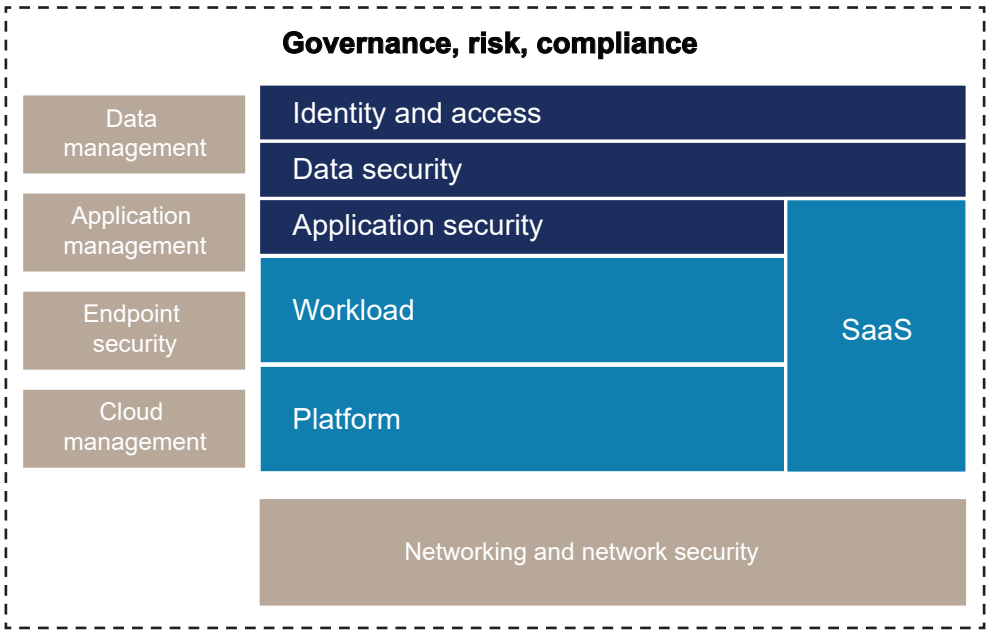
In contrast to this, the other use case is about the protection of environments, data and applications associated with IT infrastructure that the organization is deploying within cloud services environments. Rather than just consuming services, the organization's users – primarily those associated with IT development and operations, though not always – are creating environments leveraging building blocks from cloud providers, including VMs, container execution and orchestration environments, serverless functions and much more. As an added complication, there may be further access to external services, but from the perspective of application integration via APIs, rather than users reaching out to services. Here, things may move much faster – a business unit or team might be leveraging automated integration and delivery pipelines that can make changes to production environments multiple times a day. When thinking about threats, the external presence of the organization is exposed to those seeking not only to obtain business records, but to abuse infrastructure for further gain, and to do so from the perspective of infrastructure administration abuse.

The cloud infrastructure aspect – which is the focus for this research report – can be further subdivided into security for the underlying cloud platform itself and security for the workload that will execute on that platform.

Naturally, cloud security doesn't exist in a vacuum and is adjacent to several other areas both within security and broader IT disciplines. Figure 1 illustrates how we see these key cloud security areas not only in relation to each other, but also as they touch other aspects of IT.

Figure 1: Cloud Security and Adjacencies

Source: 451 Research, 2020



©COPYRIGHT 2021 451 RESEARCH. ALL RIGHTS RESERVED.

In Figure 1, 'cloud as IT infrastructure' is depicted as workload and platform. In this context, platform refers to the underlying execution environment, typically the configuration associated with the services consumed from cloud providers such as creation of VMs, container execution environments, network connectivity, various forms of storage, and more. Workload, in contrast, refers to securing more application-centric constructs, processes (such as integration pipelines) and concerns such as container workloads, function execution (serverless) and more. SaaS refers to the security for applications.

Figure 1 also shows other key areas with close adjacencies, both within security and in other, broader IT practices. Application security concerns are directly tied to and increasingly overlap with workload security. Data security, which includes concerns such as data encryption, data governance and more, is relevant across both pillars and reaches deep into both workload- and platform-related topics. Identity and access management (IAM) is not only a key discipline within cloud platforms (more on that later), but it is a broad field by itself, and the organization should look at it as touching both main pillars of cloud security.

Outside this immediate area, other key adjacencies appear: cloud management platforms start to offer considerations for security use cases, endpoint security vendors start to offer functionality covering workload aspects, application management (particularly observability) and data management (storage) also start having support for cloud use cases. As the diagram shows, the entire area of networking – and the associated large practice of network security – are foundations on interacting with cloud resources. Lastly, every organization is considering its use of IT resources under a broader umbrella of governance, with strong ties to operational risk management and compliance.

Lastly, Figure 2 illustrates how common terms and recent trends in cloud security approximately map to this model. While areas such as CASB, cloud security posture management (CSPM), cloud workload protection and identity as a service are relatively well understood, two key new areas are being discussed.

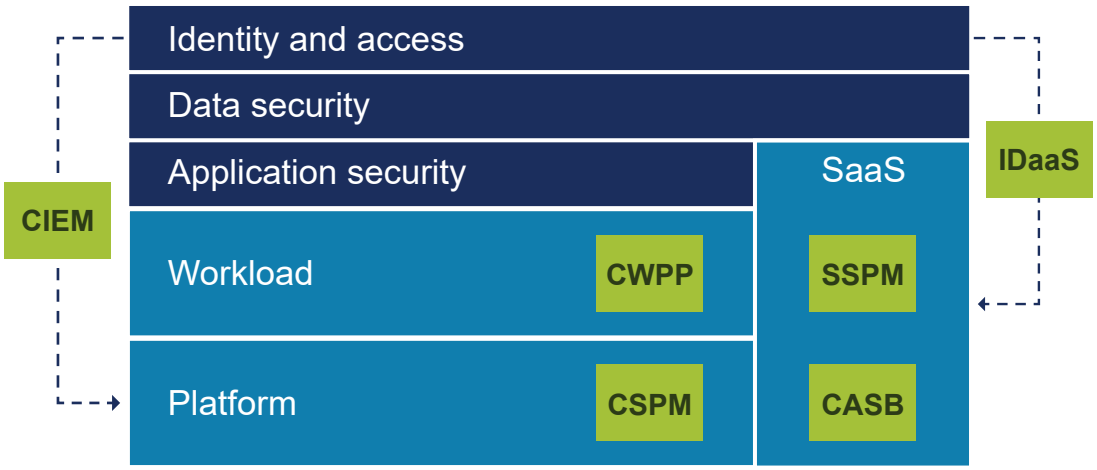
One area is named cloud identity and entitlement management (CIEM). This new area focuses on vendors offering a set of capabilities used for controlling the explosive number of permutations – and issues – associated with identities and permissions when configuring cloud platforms. The typical issues being looked at include overtly permissive configurations on resources, user accounts with excessive permissions and a lack of separation of duties, among others.

The second new area is named SaaS security posture management. In this case, it refers to the relatively new effort to control security posture across SaaS environments, not unlike a combination of CSPM with CASB.

©COPYRIGHT 2021 451 RESEARCH. ALL RIGHTS RESERVED.

Figure 2: Mapping Current Categories

Source: 451 Research, 2020



This report is not aimed to be a market map of vendors in the cloud security space with a detailed analysis of specific vendors, but focuses more on the workload and platform aspects of cloud security.

With this in mind, Figure 3 provides a partial list of vendors with offerings around cloud security focusing on use cases around cloud platform security and cloud workload security; the list is not exhaustive.

Figure 3: Cloud Security Vendors

Source: 451 Research, 2020

AREA	RELEVANCE	VENDOR
CIEM	These vendors focus primarily on adding capabilities to manage identities and entitlements for underlying cloud platforms.	• CloudKnox • Ermetic
CSP	These vendors offer a wide variety of cloud security tooling covering identities, configurations, data protection and more.	• AWS • GCP • IBM Cloud • Microsoft Azure • Oracle Cloud

©COPYRIGHT 2021 451 RESEARCH. ALL RIGHTS RESERVED.

AREA	RELEVANCE	VENDOR	
ESTABLISHED SECURITY VENDORS	Security vendors have incorporated functionality for both cloud platform and cloud workload security, among others.	• BMC • Check Point • Cisco • FireEye • McAfee • Netskope • Palo Alto Networks	• Qualys • Rapid7 • Sophos • Trend Micro • VMware • Zscaler
NEWER VENDORS – FOCUS ON PLATFORM	These newer vendors have offerings around cloud platform security. Some also have offerings covering cloud workload security, identity and other use cases.	• Accurics • Bridgecrew • CloudCheckr • Concourse Labs • disruptOps • Fugue • JupiterOne	• Lacework • Orca Security • Soluble • Sonrai Security • Threat Stack • Tufin • Turbot
NEWER VENDORS – FOCUS ON WORKLOAD	These newer vendors have offerings around cloud workload security, primarily containers and Kubernetes. Some also have offerings covering cloud platform security, identity and other use cases.	• Anchore • Aqua • Capsule8 • NeuVector • Portshift • StackRox • Styra • Sysdig	• Tigera • Lacework • Orca Security • Soluble • Sonrai Security • Threat Stack • Tufin • Turbot
OTHER VENDORS	These vendors cover different aspects of cloud security, including close adjacencies such as application security, identity management, and more.	• Github (Microsoft) • Gitlab • Hashicorp • Hewlett Packard Enterprise • jFrog	• Snyk • Sonatype • Synopsys • Veracode • Whitesource

Famed statistician George Box is known for quipping that "all models are wrong, but some are useful." This cloud security model is no different, but it should help stakeholders better understand the key trends and likely participants in the future of cloud security.

©COPYRIGHT 2021 451 RESEARCH. ALL RIGHTS RESERVED.

2. Understanding Key Trends

There are two megatrends associated with cloud infrastructure, which are then reflected on more specific customer behavior trends.

More Security in the Platforms Themselves

While it may not be readily apparent from listening to discourse within the information security public sphere, the first key megatrend is that the broader information technology industry has slowly, haltingly, sometimes clumsily, but inexorably moved toward adding increasing sets of security capabilities to offerings, either at no additional cost or packaged in a cost-effective or efficient manner. This is nothing new: We estimate that this trend has been developing over the past 20 years or so.

All that effort is paying off. The incorporation of security is now visible across the broader infrastructure, from endpoint and mobile operating system vendors (Microsoft, Apple, Google and others) that have evolved their designs to include ever-increasing security features, to built-in security capabilities in all manners of networking technologies (wired and wireless) and, not surprisingly, within the broad set of offerings coming from major cloud service providers.

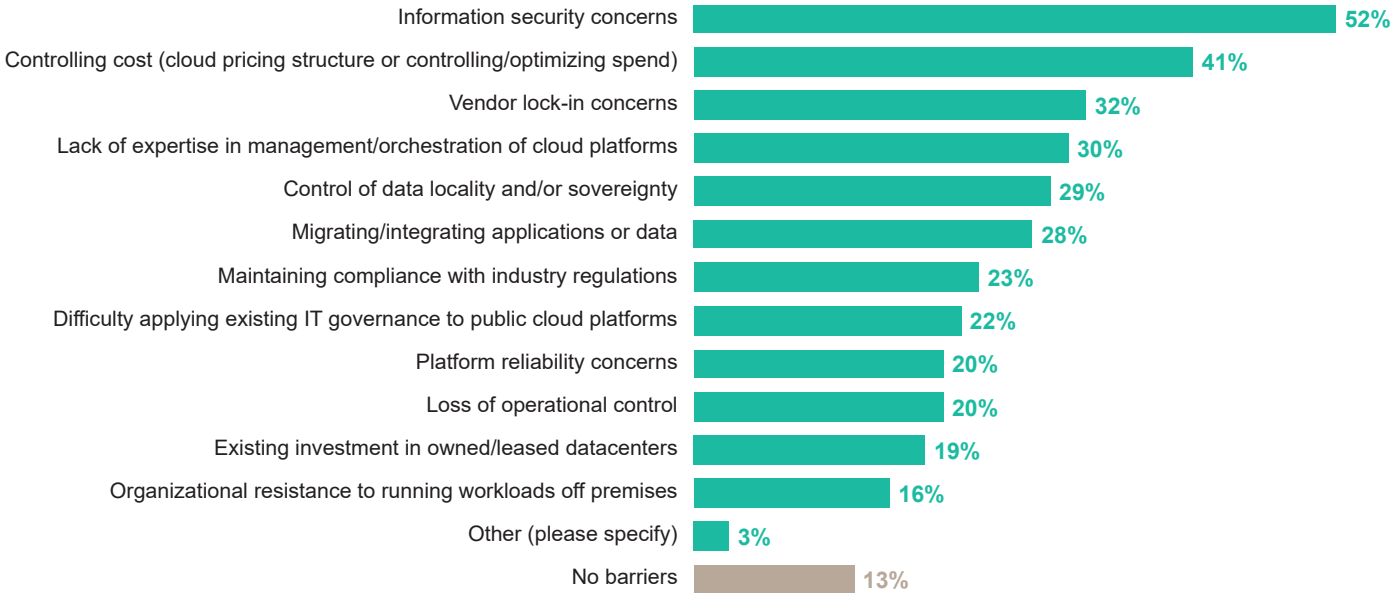
One can look at this phenomenon from the perspective of evolution, where Leigh Van Valen's Red Queen hypothesis (picking up on Lewis Carroll's Queen of Hearts, who exclaimed "now, here, you see, it takes all the running you can do, to keep in the same place!") might explain this as just evolving practices. There's also the perspective of Austrian economist Joseph Schumpeter, where innovation and 'creative destruction' are critical for economic change. Regardless of perspective, one thing is clear: Given customer insights and demands, when it comes to cloud security, making sure you are addressing security concerns make perfect, rational economic sense.

According to our VotE: Cloud, Hosting and Managed Services, Workloads and Key Projects 2020, information security concerns is the top barrier for further adoption of IaaS/public cloud services (see Figure 4).

©COPYRIGHT 2021 451 RESEARCH. ALL RIGHTS RESERVED.

Figure 4: Barriers to Adoption

Source: 451 Research's Voice of the Enterprise: Cloud, Hosting and Managed Services, Workloads and Key Projects 2020
Q. Which of the following challenges - if any - are the greatest barriers to broader implementation of IaaS/public cloud for production applications at your organization? Please select all that apply.
Base: All respondents (abbreviated fielding) (n=69)



Cloud service providers have responded enthusiastically to this demand and have adopted a multitude of cloud security services. Figure 5 lists the number of security and identity services, or offerings, from each of the major cloud providers. Since each provider may choose to offer different capabilities – which are then included possibly under a security and identity category, but also in other areas such as compute, networking, storage or databases – this table is not meant to be used for counting which provider has more or less services. Rather, it is an indication that every provider has responded to this demand with different components and packaging that cover the spectrum including IAM, data protection, infrastructure protection, incident response and compliance.

Figure 5: Number of Services Offered by Major CSPs

Source: 451 Research, 2020

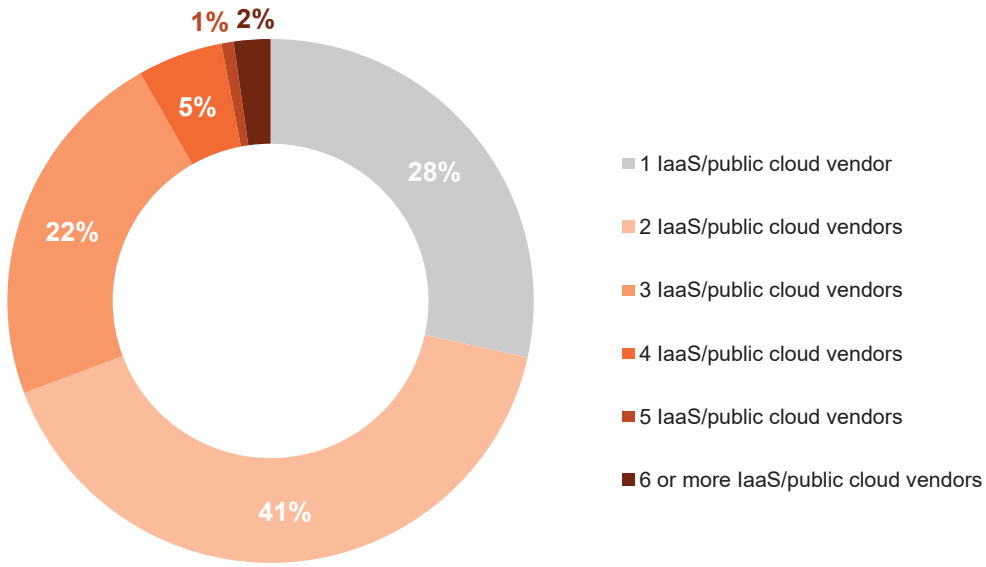
CLOUD SERVICES PROVIDER	NUMBER OF SECURITY/ IDENTITY SERVICES LISTED
AWS	23
GCP AND GSUITE	26
MICROSOFT AZURE	16
IBM CLOUD	9
ORACLE CLOUD	20+

©COPYRIGHT 2021 451 RESEARCH. ALL RIGHTS RESERVED.

Therein lies one of the key challenges facing organizations. Each cloud provider is unique in their approach to cloud infrastructure security, from how the provider defines identities, to which privileges exist and how they can be assigned, and more. This would not be so much of an issue if organizations were concentrated on one single provider, but the reality is that organizations are, on aggregate, multicloud, even if individual teams may not be. As can be seen from Figure 6, 72% of respondents indicate they use two or more IaaS/public cloud vendors.

Figure 6: Number of Cloud Providers Used

Source: 451 Research's Voice of the Enterprise: Cloud, Hosting and Managed Services, Workloads and Key Projects 2019
Q. How many different IaaS/public cloud vendors does your organization currently use?
Base: All respondents (n=267)



The other key challenge in the context of cloud security as offered by providers is that there's a rethinking of the security model for controlling resources. While providers have started adding controls in terms of restricting changes more closely aligned with how enterprises typically think of access control – such as restricting access from specific locations or network addresses for the purpose of configurations – there is a fundamental conceptual gap. Absent specific controls, cloud resources can usually be changed from anywhere in the world, if someone has the right access credentials. If one can extract access credentials from somewhere – say, a container image or mobile app – and those credentials happen to have wide permissions within the environment, the potential impact can be significant.

©COPYRIGHT 2021 451 RESEARCH. ALL RIGHTS RESERVED.

Not all news is bad, though. There are at least two key benefits that the prevalence of security controls within cloud providers brings: local consistency and agility. While yes, the differences across providers are an issue, things change within the same provider. In that case, the APIs are generally consistent across the entire environment – usually there are regional differences in services being offered – so it becomes possible to more easily automate wide swaths of one's cloud estate. The other aspect is that the same elasticity and agility that make cloud environments so different from on-premises environments can also work in the benefit of security organizations – processes can be revisited to take these benefits into account.

More Agile, Collaborative and Distributed Work Within Client Organizations

The second key megatrend concerns the nature of modern IT work within organizations. The sheer explosion in use of technology across an organization's entire value chain – not specifically cloud, but just technology in general – has resulted in a combination of work that is at the same time operating at a faster tempo and is more collaborative, always in support of business objectives. When considering cloud technologies, though, this stands out. Figure 7 from 451 Research's *VotE: Cloud, Hosting and Managed Services, Organizational Dynamics 2020* study clearly brings out agility as a key objective for those pursuing cloud initiatives.

Figure 7: Benefits from Cloud

Source: 451 Research's Voice of the Enterprise: Cloud, Hosting and Managed Services, Organizational Dynamics 2020
Q. Which of the following has been the most significant benefit from use of cloud?
Base: Experienced multiple benefits from cloud services (n=262)

©COPYRIGHT 2021 451 RESEARCH. ALL RIGHTS RESERVED.

How is this agility obtained? On one hand, it has everything to do with the technical nature of provisioning – what would normally require significant planning and expense for procuring hardware and software can now be automated in simple API calls that execute in minutes if not sooner. More than that, though, agility also comes from the adoption and support of methodologies that favor fast feedback loops and improved communication between teams – enter DevOps.

There has been significant research and evidence that organizations adopting DevOps practices obtain numerous benefits in terms of agility and quality (*Accelerate: The Science of Lean Software and DevOps: Building and Scaling High Performing Technology Organizations* by Forsgren, Humble and Kim is a good reference). The field is not static, with refinements coming in constantly both in technology and, importantly, organizational design. Many of these improvements are aimed at reducing teams' cognitive loads and improving inter-team collaboration. Pais and Skelton, for example, argue in *Team Topologies: Organizing Business and Technology Teams for Fast Flow* for organizing teams along four main topologies:

- **Stream-aligned teams**: Teams aligned to single stream of work with fast feedback loops.
- **Enabling teams**: Teams aligned to growing capabilities of stream-aligned teams via new approaches, methods, and more.
- **Complicated-subsystem teams**: Teams tasked with addressing areas with heavy demand of specialist knowledge.
- **Platform teams**: Teams that are tasked with creating the platform to allow stream-aligned teams to function independently.

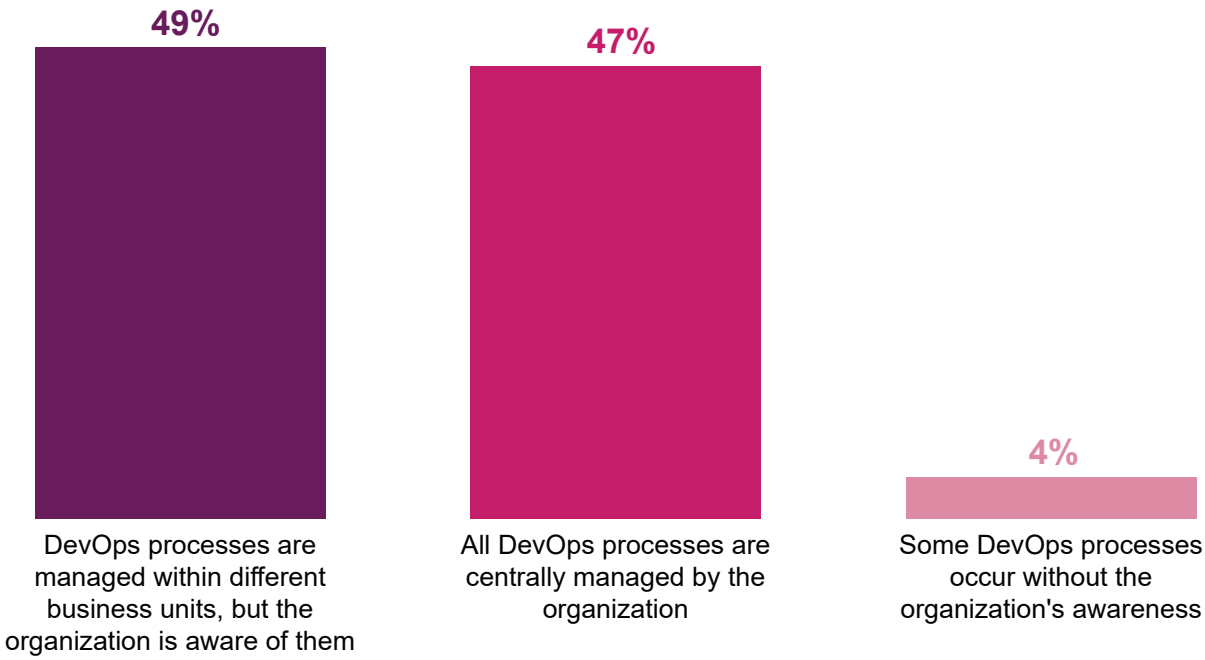
That this type of transition is happening in organizations is disruptive enough as it is – for example, how does the shift in internal structure for organizations that are looking to disrupt Conway's law affect everything from career progressions to budgeting? There is, though, one more aspect that can be deeply disruptive for centralized teams such as security: the increasingly distributed nature of work.

According to the *VotE: DevOps, 2H 2019* survey, 49% of respondents indicate that DevOps processes are being managed within business units, but IT is aware of them (see Figure 8).

©COPYRIGHT 2021 451 RESEARCH. ALL RIGHTS RESERVED.

Figure 8: DevOps Management

Source: 451 Research's Voice of the Enterprise: DevOps 2H 2019
Q. Which of these statements is most accurate regarding DevOps process at your organization?
Base: All respondents (n=476)



Where does this leave security teams? There is a well-known aphorism that says that "for every 100 developers in an organization, there are 10 people in IT operations, and one security person." That security team was already stretched out, dealing with a barrage of topics from end-user security awareness to application security, compliance and more. Now, the increasingly distributed nature of DevOps means that the security team needs to accommodate not only a large volume of work, but a large volume of distributed work, which brings with it a plethora of challenges.

©COPYRIGHT 2021 451 RESEARCH. ALL RIGHTS RESERVED.

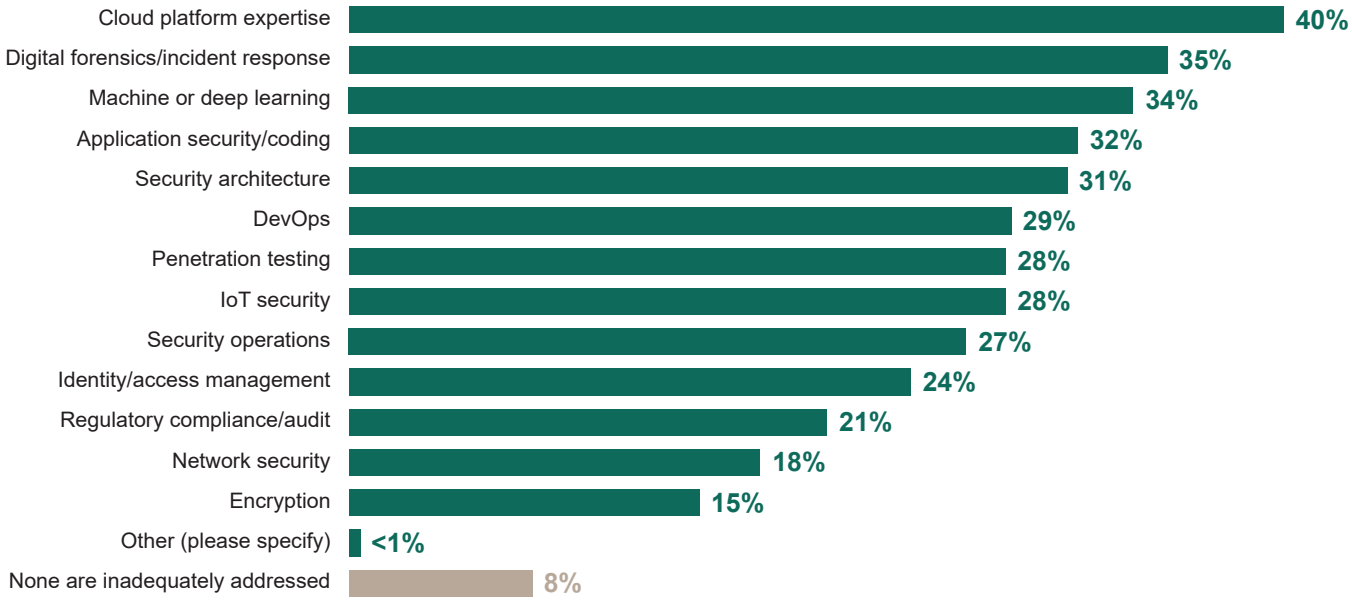
Additional Trends

KEY GAPS IN CLOUD PLATFORM EXPERTISE

As organizations embrace cloud, there is a consistent and relatively widespread skills gap in cloud platform expertise (see Figure 9). This finding is coming both from our more general research (see our VotE: Cloud, Hosting and Managed Services, Organizational Dynamics 2020 report) and from security-focused studies (see our *VotE: Information Security, Organizational Dynamics 2020*). This is particularly relevant as security teams are being asked to participate in cloud implementations and may struggle to properly assess the true exposure of assets to threats or to collaborate with other stakeholders on remediations that may apply.

Figure 9: The Skills Shortage

Source: 451 Research's Voice of the Enterprise: Information Security, Organizational Dynamics 2020
Q. And which skillsets are inadequately addressed at your organization today? Please select all that apply.
Base: All respondents (n=415)



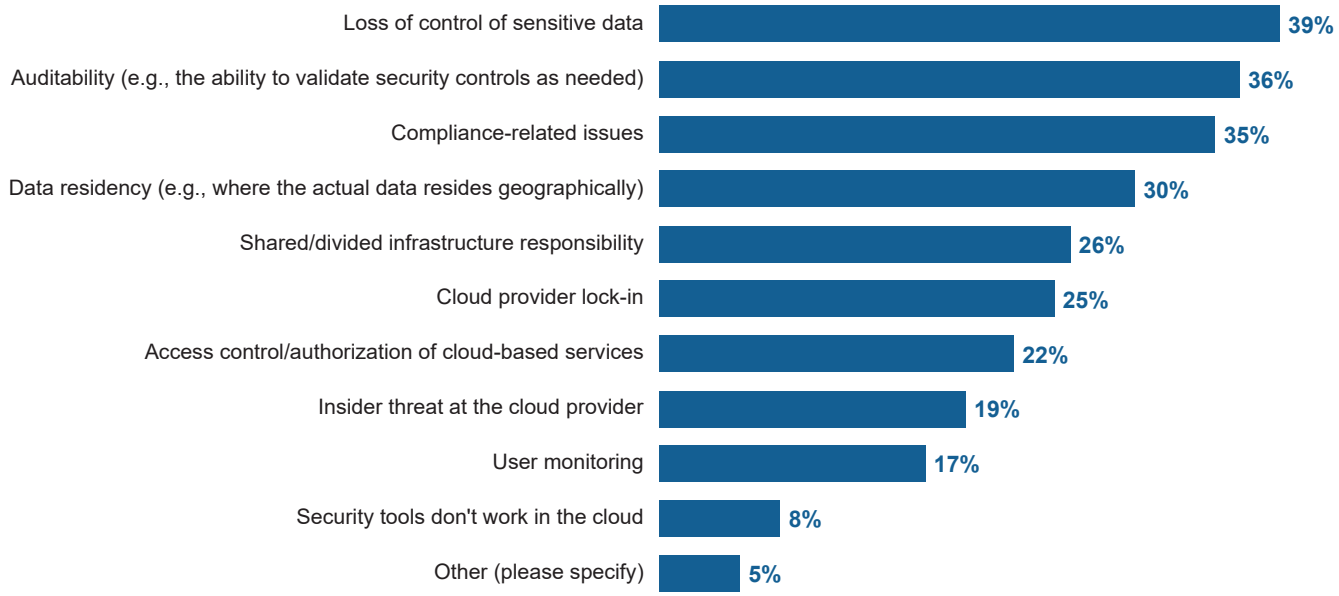
©COPYRIGHT 2021 451 RESEARCH. ALL RIGHTS RESERVED.

KEY CONCERNS BY SECURITY TEAMS

Even as teams are looking to improve their capabilities, cloud implementations are not idly waiting by. As teams push forward, security teams appear to be feeling the pressure. Looking at Figure 10, security teams indicate their main concerns when it comes to cloud usage hover around a combination of loss of control of data, auditability and compliance. This is a pressing issue as, given how public cloud misconfigurations may be exploited more easily than flaws on-premises, organizations may be exposing themselves beyond what their risk appetites would dictate. Furthermore, unless organizations have shifted traditional risk management responsibilities, security teams are likely to be held accountable for these issues, even if they're not able to address them directly.

Figure 10: Areas of Concern

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



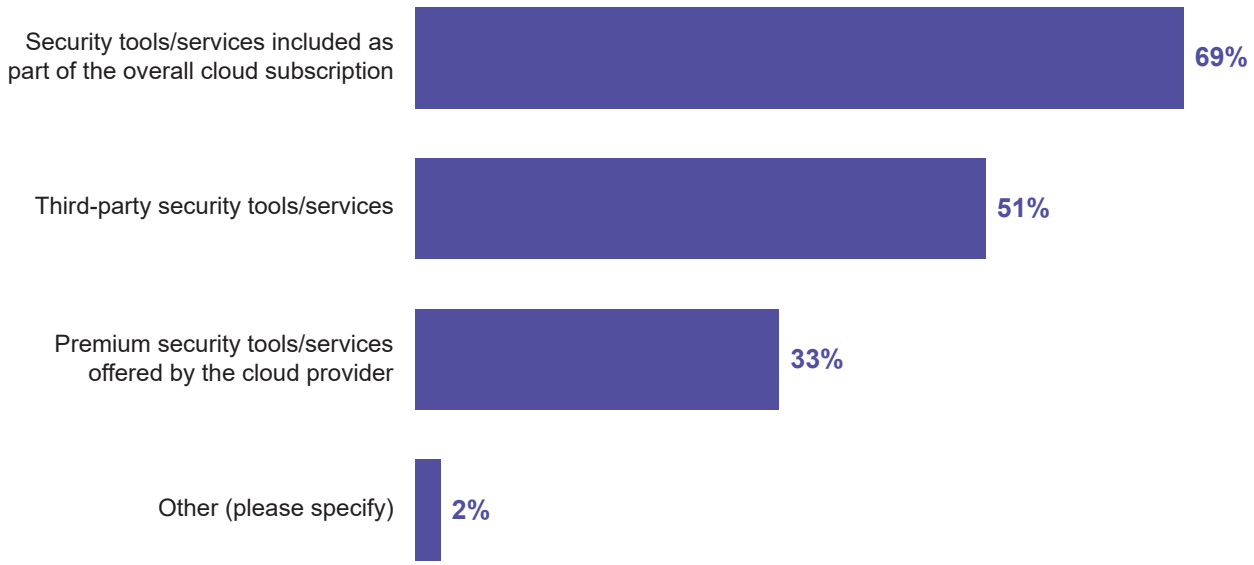
©COPYRIGHT 2021 451 RESEARCH. ALL RIGHTS RESERVED.

CUSTOMERS USING COMBINATION OF TOOLING

Faced with the challenge of figuring out cloud security, security teams are looking at bringing in resources both from the cloud providers and from third-party vendors. As Figure 11 shows, a sizeable proportion of respondents indicate they will use security capabilities offered by the provider, but approximately 52% of respondents also indicate that they plan to use third-party services or tools. Interestingly, a deeper look into this question indicates that, compared to the 52% of respondents who will use third-party offerings, only 28% of those that self-identify as digital transformation laggards plan to do so. This finding is compatible with additional observations that show lack of experience with cloud often translates into inflated expectations of capabilities.

Figure 11: Use of Cloud Security Tools

Source: 451 Research's Voice of the Enterprise: Information Security, Budgets and Outlook 2020
Q. Which vendor-based security tools does your organization currently use for its off-premises cloud architectures? Please select all that apply.
Base: Respondents who use hosted cloud architectures (n=134)



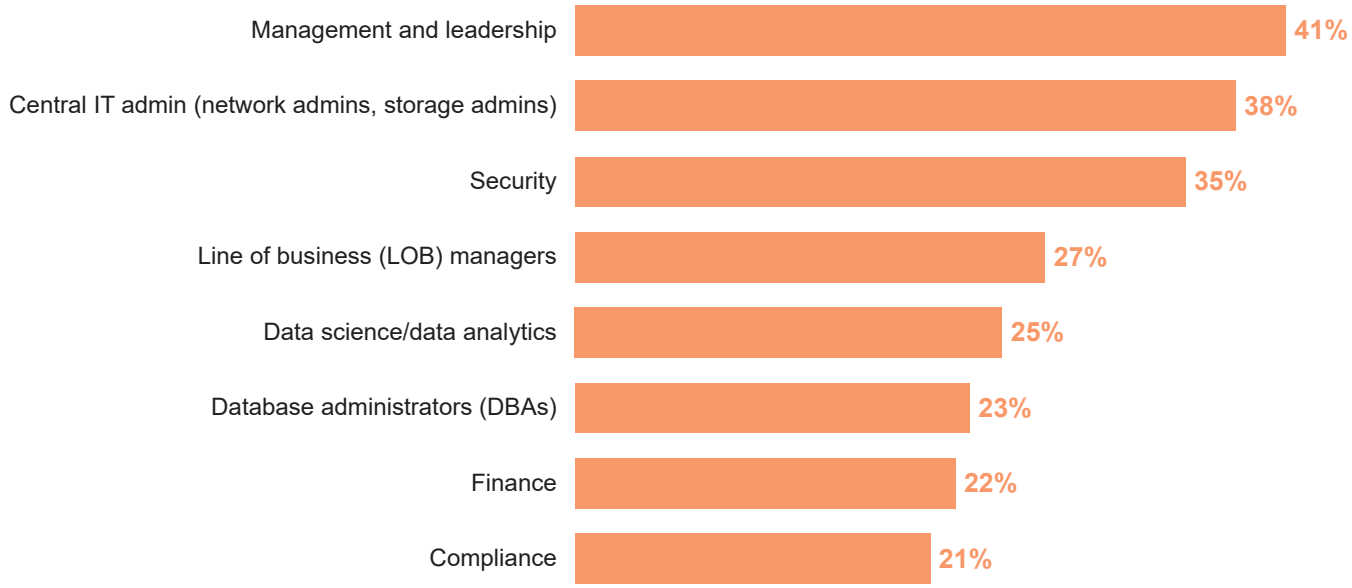
©COPYRIGHT 2021 451 RESEARCH. ALL RIGHTS RESERVED.

SECURITY IS A KEY STAKEHOLDER, SAYS DEVOPS

While some of the data may point to a negative outlook for cloud security, there's notable elements of positive developments. First, as can be seen in Figure 12, DevOps practitioners, when asked who the key stakeholders are for DevOps implementations, list security as one of the top choices. This is evidence of growing synergies between security teams and other teams within the organization. We also have anecdotal evidence of DevOps practitioners actively engaging with security teams to adjust processes and tools for better collaboration.

Figure 12: DevOps Stakeholders

Source: 451 Research's Voice of the Enterprise: DevOps 2H 2019
Q. Beyond developers and IT operations, who are the primary stakeholders in your DevOps implementation? (Choose up to 3)
Base: All respondents (n=482)



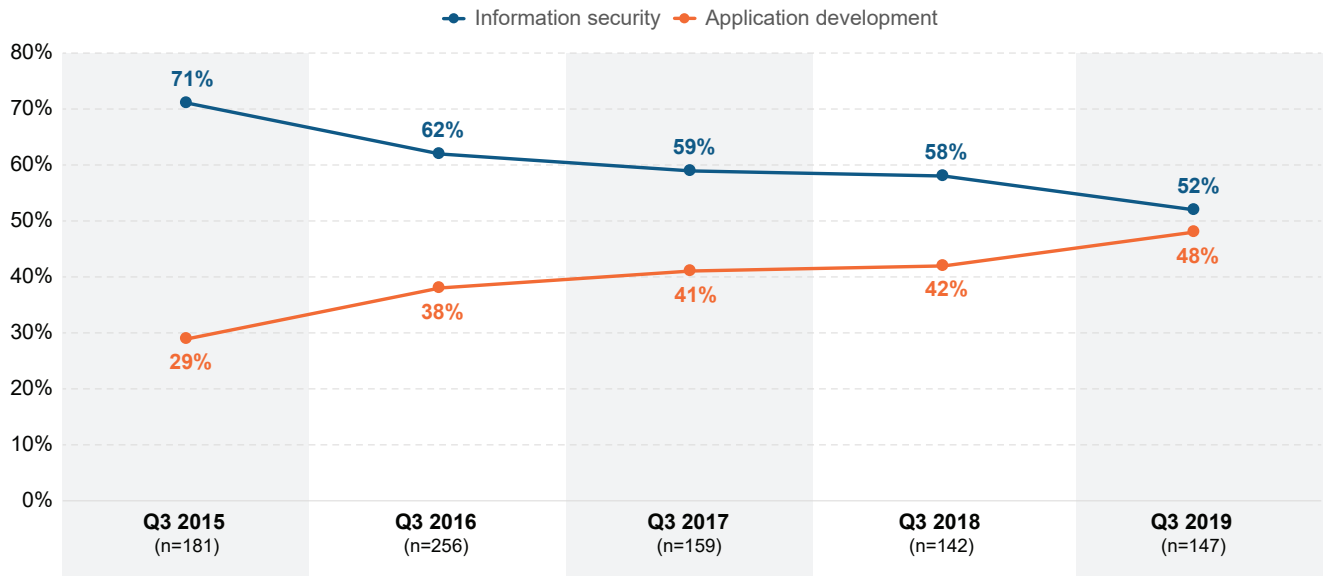
©COPYRIGHT 2021 451 RESEARCH. ALL RIGHTS RESERVED.

ENGAGEMENT WITH APPLICATION TEAMS GROWS

One more interesting – and positive – development has been the trend of increased usage of application security tools (AST) not by security teams, but by the application development teams themselves (see Figure 13). This represents not only the possibility that security concerns are increasingly shifting in terms of being addressed earlier in the lifecycle, but that there may be increased interaction and collaboration between teams. As the work on cloud initiatives is undertaken by those application development teams, the practice of using security may already be familiar to them.

Figure 13: Usage of AST

Source: 451 Research's Voice of the Enterprise: Information Security, Vendor Evaluations 2019
Q. How is the usage of application security tools allocated across the following two teams in your organization?
Base: Respondents currently using application security



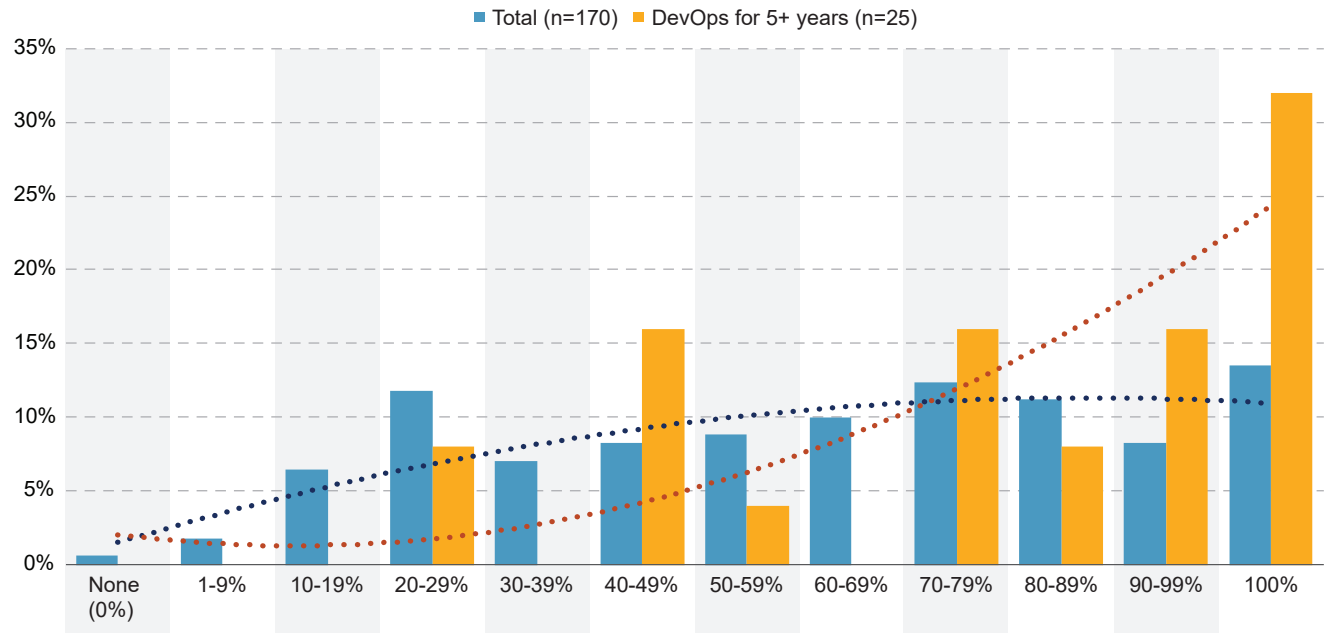
©COPYRIGHT 2021 451 RESEARCH. ALL RIGHTS RESERVED.

SECURITY EXPERTISE IMPROVES WITH TIME

Lastly, we have some indications that as teams embrace DevOps, security outcomes – or at least intentions around security outcomes – improve. This is important as it represents an understanding and potential rearrangement of security priorities and responsibilities. Figure 14, taken from our *VotE: DevOps, Workload & Key Projects* survey in late 2019, shows how respondents grade the use of security within their DevOps processes by asking what percentage of their DevOps workloads include security features. What we can see from Figure 13 is that, compared to the total number of respondents, which are somewhat uniform across percentages, those respondents who indicate they have been practicing DevOps for longer than five years are skewed, citing that a higher proportion of their DevOps workloads includes security.

Figure 14: DevOps Security Improvement

Source: 451 Research's Voice of the Enterprise: DevOps, Workloads & Key Projects 2020
Q. Approximately what percentage of your DevOps workflow implementations include security elements?
Base: Organization uses DevOps at some level, abbreviated fielding (n=170)
Note: Base sizes below n=30 should be interpreted anecdotally.



©COPYRIGHT 2021 451 RESEARCH. ALL RIGHTS RESERVED.

3. Evaluating the Impact

With a broad understanding of the key trends as described above, it is now possible to consider what the impact of these trends – and the interaction between them – may mean in the context of cloud security. Cloud security becomes a team sport in the context of numerous interactions between multiple stakeholders, both within and between organizations, CSPs and third-party vendors.

Impact to Technology

MULTICLOUD GLOBALLY, SINGLE CLOUD LOCALLY

The first consideration on technology patterns is that, except for all but corner cases (typically smaller organizations), the reality at the aggregate level is that the organization will be multicloud. It may use one or two or three hyperscale providers, but it will likely also have on-premises assets either on its own datacenters or arranged via a partner. This is not surprising, but it should be called out because, when put in conjunction with the reality of distributed workstreams within the organization, it may mean that, on aggregate, the organization will be multicloud but individual projects will much more likely be restricted to one environment. Why does this matter? Well, if that project/team is only aligned to one environment, it may make sense for that team to consider 'native security' functionality from that environment, even if, at a larger scale, the organization needs to support multiple environments.

THE NEED FOR AGGREGATION LAYERS

The other consideration is that as cloud providers work to remove security barriers for workload adoption, they're likely to concentrate their efforts on offering security features outside of their environments – one does not normally expect Google Cloud, for example, to provide security functionality around securely using Microsoft Azure or AWS. This dynamic opens the opportunity for third-party vendors to offer a consistent multicloud experience, acting as an aggregation layer between cloud service providers. Indeed, this has been one of the key use cases of the CSPM space and should continue to be so in the near term.

Still, potential disruption is afoot: Microsoft has recently announced that it will start supporting security configuration functionality for workloads residing on other cloud environments via its Azure Arc product. We feel this represents a special case since Microsoft, unlike AWS and Google Cloud, can act both as a CSP and as an enterprise security vendor. This new functionality appears more closely aligned with following its 'enterprise vendor' playbook, which will put it in competition with other security vendors offering cloud platform security support.

©COPYRIGHT 2021 451 RESEARCH. ALL RIGHTS RESERVED.

RISE OF INFRASTRUCTURE AS CODE

As organizations scale up their usage of cloud resources, they mostly do so programmatically. Rather than clicking away at a provider's web interface, the bulk of work is being done increasingly via automation pipelines. All providers have released comprehensive capabilities for automation, and Hashicorp's Terraform has gained popularity as a common language to implement infrastructure-as-code (IAC) workflows. The impact for security teams is that they may be able to be proactive in inspecting the codified instructions for modifying cloud environments, rather than just detect flaws via periodic scan of an organization's cloud estate. This has been picked up by numerous vendors, including but not limited to Palo Alto Networks, Aqua Security, Accurics, Bridgecrew, disruptOps and others.

Impact to Vendors

BEWARE WHITESPACE IN CLOUD SECURITY

The first key impact of current cloud security trends for third-party vendors is that they're operating in an environment where the incumbent (or CSP) is happy to coexist only so far as interests are aligned. All large CSPs have clearly articulated that they make decisions based on customer needs and, should there be a gap that the market is not addressing those needs, they may step in and implement it. Amazon's Jeff Bezos is famous for saying "your margin is my opportunity."

What whitespace remains then? We see three key areas for possible vendor-led services specifically in the context of security focused on cloud platform and cloud workload security:

- Provide aggregation services (as described above) that tie more easily into a customer's existing workflow, bringing together functionality across multiple environments.
- Cover additional data sources, innovation and specific use cases – vendors can pursue coverage above and beyond what the CSP offers. Perhaps it may be industry-specific mandates or challenges, or novel techniques that incorporate additional contextual information, or additional sources.
- Work alongside the CSP to add threat intelligence and/or telemetry that can be used by the provider.

©COPYRIGHT 2021 451 RESEARCH. ALL RIGHTS RESERVED.

NEED TO WORK WITH DIFFERENT STAKEHOLDERS

While discussing whitespace is more of a consideration when dealing with external factors, the internal aspects of customers also deeply impact vendors moving forward. Here, the key factors are the reality of where cloud engineering and security teams are on their respective cloud security journeys, how they interact with each other and how senior management assigns security risk decisions within the organization. While each situation will be unique, common patterns we expect vendors to find are needing to support a security team with obtaining broader understanding of cloud security details and/or relationships with the right stakeholders across the aisle, needing to demonstrate to security decision-makers that their offerings can meet security requirements, and navigating the nuances of project budgeting and risk management to move initiatives forward.

RECOGNIZE THE TRUE CHALLENGE IS GOVERNANCE, NOT JUST SECURITY

Lastly, vendors may have to deal with a scenario where customers looking to obtain positive outcomes in cloud security may be much more constrained by internal governance challenges rather than by not having a toolset that implements specific technical capabilities. In these scenarios, the obstacles the customer may be experiencing could be related to inter-team communications, team capabilities, budgeting, risk management and a variety of other topics. In this context, a third-party vendor can potentially act as a common layer between different stakeholders within the customer, and the value it can provide will be in terms of clear reporting, or flexibility around competing requirements, or flexible configuration delegation to address customer needs such as multi-tenancy, multiple reporting requirements and more.

Impact to Customers

IMPORTANCE OF COMMUNICATIONS

The first clear impact of modern work trends is that it exposes the need for security teams and cloud engineering teams to collaborate. This collaboration must account for the needs of each team: security teams may need to catch up on cloud technologies and capabilities, while cloud engineering teams may need to understand how the organization performs risk management. In many anecdotal conversations we've had, too often the disconnect between teams resulted in scenarios from security teams being unaware of critical cloud deployments already in production, to cloud engineering teams being hampered in adopting delivery of business value because of security process roadblocks.

©COPYRIGHT 2021 451 RESEARCH. ALL RIGHTS RESERVED.

UNDERSTAND ROLE AS SUPPORTING TEAM

What role does security itself play? This will vary for each organization – indeed, it is a function of both culture and how risk management responsibilities are currently allocated – but, following on the theme of team sports, it needs to coordinate plays with cloud engineering, acknowledging that there's value in being a supporting team member. In some scenarios, security teams can act as enablers for cloud engineering, teaching teams how to be self-sufficient in performing threat modeling exercises. In other situations, security teams can act as escalation paths during security incidents. Lastly, security teams can also own and operate underlying platforms or libraries that provide value to more stream-oriented cloud engineering teams, such as IAC scanning capabilities, shared libraries for authentication and monitoring or even support of workload-level constructs such as secure service meshes.

UNDERSTAND OVERARCHING SHARED RESPONSIBILITY MODEL

Many discussions around cloud security bring up the concept of the shared responsibility model (SRM) as a way of crystallizing how the CSP and the client should split up responsibilities in the design, implementation and ongoing operations of cloud-based environments. While the overall idea of a shared understanding is positive, each provider takes a slightly different approach to defining the division of responsibilities.

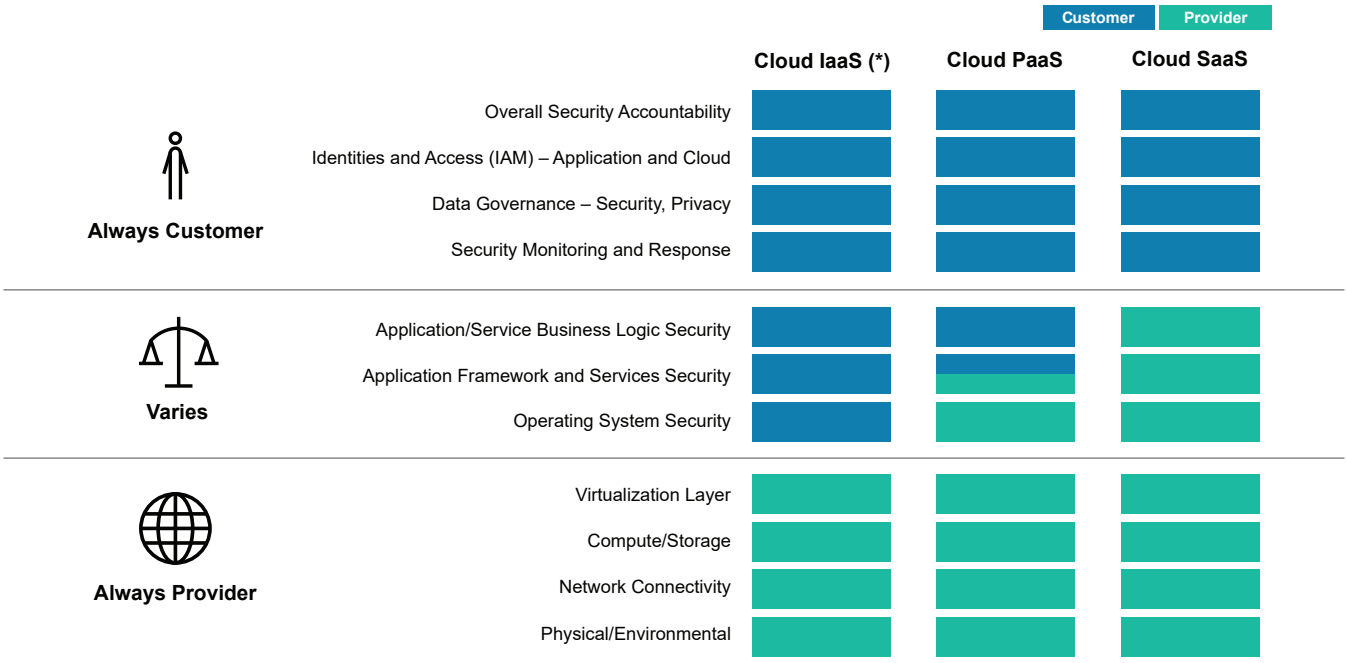
One of the consequences of the differences between providers is potential confusion. We have observed that some stakeholders within organizations – particularly those not deeply involved with cloud security efforts – may overestimate the role of the service provider in ongoing security operations.

With that in mind, Figure 15 captures the nuances of the key elements of the security architecture – overall accountability, IAM, data governance, and overall monitoring – that consistently remain with the customer.

©COPYRIGHT 2021 451 RESEARCH. ALL RIGHTS RESERVED.

Figure 15: Shared Responsibility in SRM

Source: 451 Research, 2020



EMBRACE CLOUD SECURITY CAPABILITIES

As customers understand their responsibilities under the SRM, the next step is to acknowledge and embrace cloud-delivery models, looking for opportunities to use some of the key characteristics of cloud environments – the agility, the well-defined APIs, the robust control plane and others, not to mention the security services offered by the providers – to the benefit of security operations. There are many options for improving operations and architecture, including but not limited to:

- Reducing blast zones for incidents by using account-based segregation of assets and tightly controlled virtual execution environments (or VNets).
- Use of out-of-band management methods, reducing the exposure to potential attackers.
- Use of immutable components that, in combination with automated pipelines and modern deployment strategies, reduce the burden of patching components.
- Simplify forensics and investigations by using snapshot capabilities from cloud providers.
- Consider architectural changes to applications to remove dependency on common network protocols, further reducing attack surface.
- Consolidation of security alerting and information via centralized alerting capabilities offered by providers.

©COPYRIGHT 2021 451 RESEARCH. ALL RIGHTS RESERVED.

EMBRACE ITERATIVE IMPROVEMENTS

At a broader level, security teams can consider their efforts to upskill in cloud security alongside the well-known observe, orient, decide and act (OODA) loop popularized by Air Force Colonel John Boyd. In this context, teams may need to iterate over different instantiations of:

- Observing current cloud practices within the organization, both independently and via collaboration with other stakeholders.
- Orienting themselves in terms of contextualizing the observations alongside recommended practices for cloud security and organizational objectives.
- Deciding what actions must be taken in the context of any potential gaps from a desired state.
- Act, either directly or again via collaboration, with other stakeholders.

This cycle can be improved over time – as teams better understand technologies, likely threats and possible remediation methods – and can also be codified to be implemented efficiently across the organization.

©COPYRIGHT 2021 451 RESEARCH. ALL RIGHTS RESERVED.

4. Challenges Ahead

CSPs

For cloud services providers, the trends do indicate that customers will heavily favor using security functionality provided by the platform, including, in some cases, premium services. That said, customers expect cloud providers to continue innovating in how they deliver security capabilities, in a way that is amenable to integration into the rest of a customer's overall security architecture. For those larger customer organizations, the expectation is that a provider's feature set will be one of many that the customer's security team may be dealing with.

Third-Party Vendors in General

As we have seen in the trends discussed in this report, customers are looking to catch up on cloud security, and they're considering using not only capabilities from providers (including premium features), but also offerings from third-party vendors. This is particularly interesting for vendors that are already part of a customer's existing technology stack, especially if they can easily demonstrate how to support cloud environments within the same workflows.

That said, there is one caveat to keep in mind: More than other technologies in the past, there's the potential for organizations to arrange themselves to maximize provider services, use community/open source offerings or even roll out their own.

This is, naturally, a new round of build versus buy, which is not a new debate in IT. This time, the decision is not about building an entire new endpoint security agent or building a custom database security feature; rather, this is about using the building blocks already being provided by a cloud provider that is properly incentivized to remove security roadblocks.

Cloud engineering teams are already amply skilled at using cloud resources to achieve their ends. The question on cloud security is whether the diversion of one's engineering talent to generate security outcomes is the best use of an organization's resources.

The key challenge for vendors becomes clearly articulating their value propositions, both in terms of functionality and value for money. The very nature of API-driven integration makes switching costs potentially lower.

©COPYRIGHT 2021 451 RESEARCH. ALL RIGHTS RESERVED.

Security Vendors

The key challenge ahead for security vendors is the realization that, with the distributed nature of modern work, some of the key stakeholders for cloud security are outside the security team. While a chief information security officer (CISO) may still be the executive in charge of cloud security and the ultimate buyer or budget holder, they will decide considering the input from their cloud engineering customers. Security vendors must then either enable existing security champions to articulate the value of their offerings to these new stakeholders or build those relationships themselves.

On a more practical level, a security vendor needs to ensure that they're able to support these new stakeholders throughout the lifecycle of their engagement. This may mean that pre-sales and sales teams need to potentially build new relationships within prospect accounts and must do this with authenticity, or that customer success/support teams need to provide information and support in a manner that is easily consumable by new stakeholders. It can also mean adjusting channel relationships, packaging options and more.

Technology Vendors

A technology vendor without a long-standing offering in the security space will face different challenges. In this case, they likely already have support within the cloud engineering or cloud operations team and now need to win over the security team. This will require understanding, for example, of what compliance mandates the organization is targeting to comply with, or how the organization expects to incorporate external threat intelligence into its cloud security tooling. How does an offering integrate not only with cloud engineering development or operations, but also within security workflows happening in the security operations center – typically with SIEM/security orchestration, automation and response integration or, more recently, with trends such as extended detection and response (XDR)? Supporting other enterprise-level features – such as single sign-on and providing detailed auditing capabilities, among others – is also likely to be a factor.

Customers

What our research has shown is that for many organizations, the path forward will include a great deal of collaboration – indeed, a team approach – both in the context of working alongside CSPs and trusted third-party vendors, but also emphasizing the much deeper collaboration inside the organization as well.

The key challenge to be aware of is how to simultaneously improve collaboration between disparate teams – cloud engineering and security, in this example – while upskilling those teams with the necessary cross-domain expertise. Furthermore, how do you do this while the organization reconsiders how it performs not only cloud governance itself – who's accountable and who's responsible for securing specific cloud resources – but also potentially realigning how it does operational risk management?

©COPYRIGHT 2021 451 RESEARCH. ALL RIGHTS RESERVED.

5. Conclusions

What does the future hold for cloud security? We see a few key themes persisting.

First and foremost, the quest for agility and automation in cloud adoption in general, not just cloud automation, should drive more organizations to continue adopting cloud services in response to their business needs. As organizations become more experienced in cloud security, we expect to see additional demand for more efficient automation across delivery pipelines, leveraging security capabilities from the cloud provider and from third-party vendors where appropriate.

Delivering security functionality within a project will increasingly fall on cloud engineering teams, but they will work in conjunction with security teams. This will take the form of enablement activities such as threat modeling, security testing and more. Security teams will be able to articulate and translate organizational security goals into manageable constraints for cloud engineering teams and will insert functionality into the development and deployment pipelines to provide faster feedback to teams about potential security issues. From there, the operational model for teams will likely be to independently verify if the security decisions within their projects are compliant with policy, occasionally receive input from independent scans or verifications by the security team and incorporate any security fixes within their existing workload tracking systems.

Over time, the changes brought about by cloud deployments – the agility, the automation, the autonomy and more – will be normalized within IT, much like other trends have been. Until then, cloud security remains explicitly a team sport, and clear communication and collaboration between stakeholders remains essential.

©COPYRIGHT 2021 451 RESEARCH. ALL RIGHTS RESERVED.

6. Further Reading

Cloud Security Market Monitor 2020

2020 Trends in Information Security

Meditations on the Next Decade of Cloud Platforms, June 2020

Container Security Market Map, March 2019

Voice of the Enterprise: Cloud, Hosting and Managed Services, Workloads and Key Projects 2020

Voice of the Enterprise: Cloud, Hosting and Managed Services, Organizational Dynamics 2020

Voice of the Enterprise: Information Security, Organizational Dynamics 2020

Voice of the Enterprise: DevOps, Workload & Key Projects 2020

©COPYRIGHT 2021 451 RESEARCH. ALL RIGHTS RESERVED.

7. Index of Companies

©COPYRIGHT 2021 451 RESEARCH. ALL RIGHTS RESERVED.

©COPYRIGHT 2021 451 RESEARCH. ALL RIGHTS RESERVED.

Appendix A: Select M&A Transactions

There has been significant M&A activity over the past two years in relation to acquisition of vendors with capabilities around securing cloud platforms and cloud workloads.

DATE	ACQUIRER	TARGET	AMOUNT ($M)
2020-06-05	IBM	Spanugo	n/a
2020-05-13	VMware	Octarine	n/a
2020-04-28	Rapid7	DivvyCloud	145
2020-04-09	Zscaler	Cloudneeti	n/a
2020-02-03	Hewlett Packard Enterprise	Scytale	n/a
2020-01-21	FireEye	Cloudvisory	13.2
2019-12-10	Acronis	5nine Software	n/a
2019-12-02	Check Point	Protego Labs	n/a
2019-11-12	Aqua Security	CloudSploit	8
2019-10-21	Trend Micro	Cloud Conformity	70
2019-08-21	VMware	Intrinsic	n/a
2019-08-09	McAfee	NanoSec	n/a
2019-05-29	Palo Alto Networks	Twistlock	410
2019-05-29	Palo Alto Networks	PureSec	47
2019-01-08	Sophos	Avid Secure	15
2018-10-30	Qualys	Layered Insight	12
2018-10-24	Check Point	Dome9 Security	n/a
2018-10-03	Palo Alto Networks	RedLock	173
2018-07-12	Netskope	Sift Security	n/a
2018-03-14	Palo Alto Networks	Evident.io	300
2018-02-14	VMware	CloudCoreo	n/a

©COPYRIGHT 2021 451 RESEARCH. ALL RIGHTS RESERVED.

451 Research

S&P Global
Market Intelligence

About 451 Research

451 Research is a leading information technology research and advisory company focusing on technology innovation and market disruption. More than 100 analysts and consultants provide essential insight to more than 1,000 client organizations globally through a combination of syndicated research and data, advisory and go-to-market services, and live events. Founded in 2000, 451 Research is a part of S&P Global Market Intelligence.

© 2021 451 Research, LLC and/or its Affiliates. All Rights Reserved. Reproduction and distribution of this publication, in whole or in part, in any form without prior written permission is forbidden. The terms of use regarding distribution, both internally and externally, shall be governed by the terms laid out in your Service Agreement with 451 Research and/or its Affiliates. The information contained herein has been obtained from sources believed to be reliable. 451 Research disclaims all warranties as to the accuracy, completeness or adequacy of such information. Although 451 Research may discuss legal issues related to the information technology business, 451 Research does not provide legal advice or services and their research should not be construed or used as such. 451 Research shall have no liability for errors, omissions or inadequacies in the information contained herein or for interpretations thereof. The reader assumes sole responsibility for the selection of these materials to achieve its intended results. The opinions expressed herein are subject to change without notice.

NEW YORK
55 Water Street
New York, NY 10041
P 212.505.3030
F 212.505.2630

SAN FRANCISCO
One California Street
31st Floor
San Francisco, CA 94111
P 212-505-3030

LONDON
20 Canada Square
Canary Wharf
London E14 5LH, UK
P +44 (0) 203.929.5700
F +44 (0) 207.657.4510

BOSTON
75-101 Federal Street
5th Floor
Boston, MA 02110
P 617-598-7200
F 617-428-7537

©2021 451 Research, LLC
WWW.451RESEARCH.COM