White Paper

Retooling Cybersecurity Programs for the Cloud-first Era

Strategies for Protecting Cloud-resident Data and Cloud-native Applications

By Doug Cahill, ESG Senior Analyst

September 2019

This ESG White Paper was commissioned by Capsule8, Obsidian, and Signal Sciences and is distributed under license from ESG.

Contents

Executive Summary

Cloud-first, The Cloud Era, The Cloud Generation, Cloud-smart, Cloud-native, and other such refrains all scream, "To the cloud or bust!" The proverbial cloud horse is, indeed, out of the barn, leaving cybersecurity teams to adapt to the new world order. Is new world order too draconian of a situational analysis? No, and not just because of the level of cloud adoption, but because of *how* cloud services are being consumed.

One of the fundamentals of the cloud paradigm shift is the changing role of the corporate IT department, not just the cybersecurity team. Out of a need to realize business agility, lines of business are leading the cloud charge, with or without the involvement of their corporate IT and cybersecurity teams. Call it Shadow IT, if you like, but business units are no longer hiding their use of clouds, be they SaaS, IaaS, or PaaS, including software development projects that utilize the microservices of cloud-native apps and DevOps processes to expedite continuous integration and delivery. How does this impact cybersecurity?

This reality results in a need to retool the people, process, and technology pillars of organizations' cybersecurity programs, starting with a cultural shift to treating security as a shared responsibility and fully embracing a broader definition of the perimeter.

Because lines of business are going directly to the cloud, cybersecurity and IT teams are losing control over both the administration and security of cloud-delivered applications. This decoupling, in which the consumer of the cloud service is administering its use, means that security teams are losing centralized visibility and control over the data assets associated with those services and the users who have access. This reality results in a need to retool the people, process, and technology pillars of organizations' cybersecurity programs, starting with a cultural shift to treating security as a shared responsibility and fully embracing a broader definition of the perimeter. This paper explores these trends based on primary, peer-level research and offers a set of prescriptive best practices for securing cloud-native applications and the expanded perimeters of cloud-first businesses.

Cloud Adoption Is Broad-based and Business-critical

The complexion of cloud adoption has evolved with respect to not only the types of cloud services in use but also the business-critical nature of those services. No longer merely a backup target, or just for dev and test environments, the cloud is now the center of computing gravity for many businesses. Cloud adoption has also led to a shift to an iterative software development approach and a correlated preference for microservices that enable rapid app development and delivery.

Cloud Consumption Is Leading to Data Migration, and New Perimeters

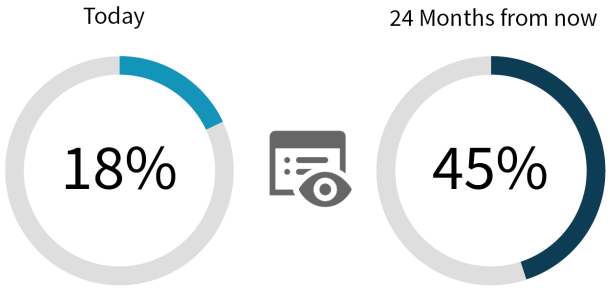
The broad use of software-as-a-service (SaaS) applications and an appreciable increase in the use of infrastructure-as-a-service (IaaS) services are leading more corporate data to be cloud-resident. Almost one-quarter (24%) of respondents to a research survey conducted by ESG said that more than 40% of their corporate data resides on public cloud services today This is expected to more than double to 58% of organizations within 24 months.[1] This migration of data to cloud stores, coupled with remote user access outside of the network perimeter, has created a human perimeter comprised of identity, privileges, and data classification.

With respect to data classes, the amount of cloud-resident data that research participants shared is sensitive is notable and a proxy for the criticality of cloud services. In fact, nearly one in five (18%) respondents said that more than 40% of their

[1] Source: ESG Master Survey Results, *Trends in Cloud Data Security*, January 2019.

corporate data that resides on public cloud services today is sensitive. This is expected to more than double to 45% of organizations within 24 months (see Figure 1).[2]

Figure 1. Cloud-resident Sensitive Data



Source: Enterprise Strategy Group

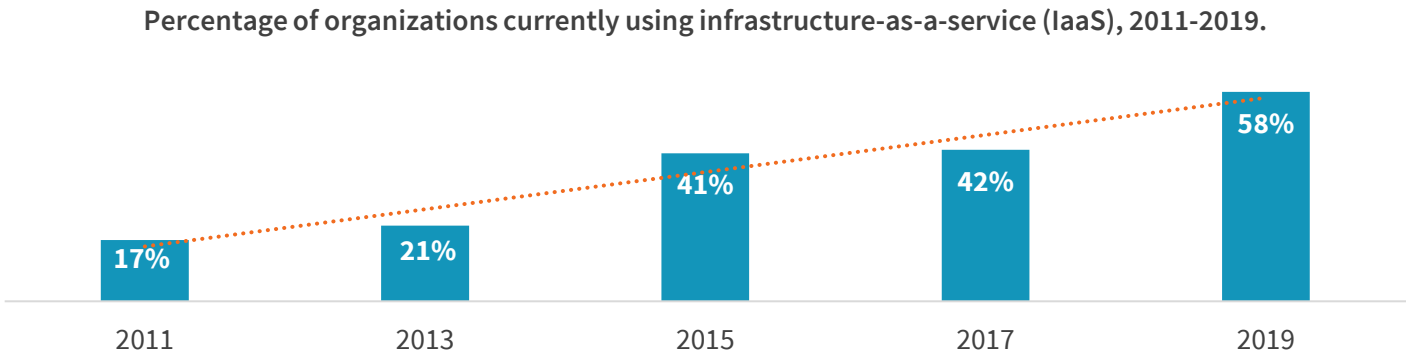
Of concern is the number of respondents who share that an appreciable percentage of their cloud-resident sensitive data is not secure, with three-quarters of research participants noting that more than 20% of that type of data is insufficiently secured.[3]

Cloud-first Initiatives Are Driving Breadth and Depth of Cloud Use Cases

A term coined by the United States Federal Government to encourage its agencies to adopt cloud services, "cloud-first" is now a leading indicator of cloud adoption across private and public sector organizations alike. According to ESG research, those organizations with a cloud-first policy have become more prevalent in just the last year, with 39% of research participants stating that their organization has a cloud-first policy in 2019, up from 29% in 2018.[4]

All types of cloud services are now broadly adopted, including the breadth of SaaS usage with two-thirds (67%) of participants in ESG research sharing that more than 20% of their applications are now SaaS-based, a notable increase from 38% of organizations who cited the same level of SaaS usage in 2013. Also of note is the appreciable increase of IaaS usage from 42% of organizations consuming IaaS services in 2017 to 58% in 2019 (see Figure 2). And, of those consuming IaaS services, over three-quarters (76%) are doing so from more than one cloud service provider (CSP).[5]

Figure 2. Use of Infrastructure-as-a-Service (IaaS)



Source: Enterprise Strategy Group

[2] ibid.
[3] Source: ESG Master Survey Results, *Trends in Cloud Data Security*, January 2019.
[4] Source: ESG Master Survey Results, *2019 Technology Spending Intention Survey*, March 2019.
[5] ibid.

Cloud-native Applications Transcend Technology

When thinking about cloud-native applications, there are multiple dimensions to consider, including the heterogeneous composition of cloud-native apps, where they are currently deployed, and where they will be in the future, as well as the processes employed to develop, deliver, and, of course, secure them. As such, for the purposes of this paper, cloud-native applications encompass both an on-demand, elastic microservices-based architecture and an iterative agile DevOps approach to continuous integration and continuous delivery (CI/CD).

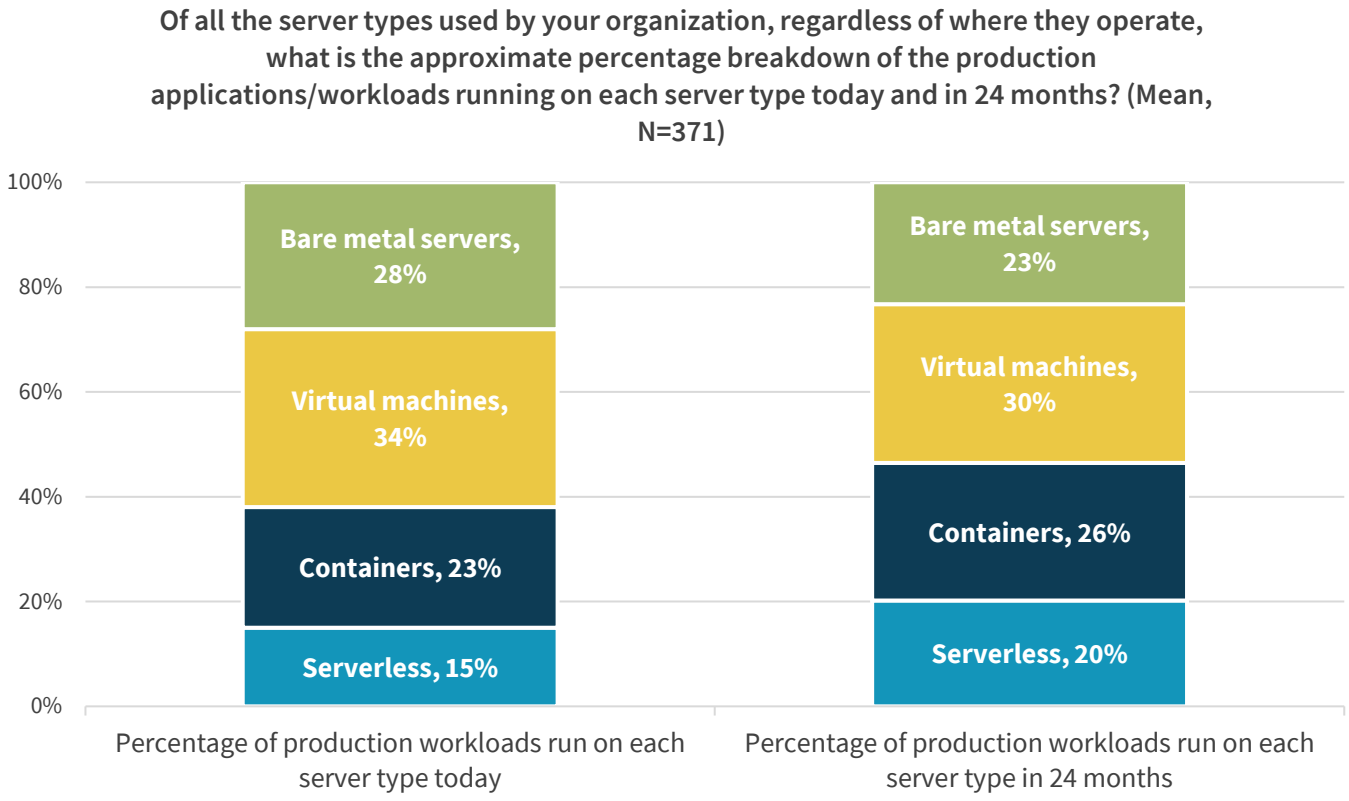
Cloud-native applications encompass both an on-demand, elastic microservices-based architecture and an iterative agile DevOps approach to continuous integration and continuous delivery (CI/CD).

Cloud-native Applications Are Heterogenous

Comprised of a Disparate Set of Technologies

There is strong adoption of the microservices that comprise cloud-native apps, including containers and serverless functions. Of those organizations that are already on their journey to cloud-native applications, 52% are using serverless functions to some extent.[6] But old applications and the technology stack they run on do not get decommissioned overnight. As such, the microservices of cloud-native apps will coexist with fleets of virtual machines, as well as bare metal servers, representing a heterogenous mix of server workload types (see Figure 3).

Figure 3. The Heterogenous Mix of Server Workload Types



Source: Enterprise Strategy Group

[6] Source: ESG Master Survey Results, *Leveraging DevSecOps to Secure Cloud-native Applications*, to be published. All ESG research references and charts in this white paper have been taken from the master survey results set, unless otherwise noted.

Use Different Linux Distributions

Whether the workload vehicles are bare metal, VMs, or containers, Linux is typically the operating system of choice for cloud-native applications, with software developers often empowered to choose their Linux distributions of choice. As a result, while the operating system type may become more homogenous, the multitude of Linux distros represents another dimension of heterogeneity and leads to a requirement for Linux-focused security controls.

Deployed across Hybrid, Multi-clouds

The portability of containers and data center-as-a-service (DCaaS) offerings, such as Outpost, Azure Stack, and Anthos, lead to increased runtime location options for cloud-native applications.

Cloud-native as a term is arguably a misnomer in that not all cloud-native apps are, or will be, hosted in and delivered from a public cloud platform. On the heels of failed OpenStack projects, Kubernetes and containers represent the path forward for some organizations to standing up customer-managed, on-premises private clouds. To this point, 46% of research participants shared that their container-based applications will be deployed in a combination of public cloud platforms and private data centers in the future, double the percentage of those who cited doing so for their current container deployments. Why the relatively large numbers of those who cite being location-agnostic in the future for containerized apps? The portability of containers and data center-as-a-service (DCaaS) offerings, such as Outpost, Azure Stack, and Anthos, lead to increased runtime location options for cloud-native applications. The heterogeneity of environments and the "public by default" nature of the public cloud have made identity and access management a critical security control in addition to the network.

Cloud-native Applications Are Developed via Agile, Delivered via DevOps

The shift to cloud services and cloud-native apps is about more than a heterogenous mix of technologies. The tight coupling of agile software development and DevOps methodologies as the means by which cloud-native apps are developed by the former and delivered via the latter represents modern methodologies. In fact, nearly three-quarters (74%) of research participants who cited an extensive use of DevOps also indicated that they use agile software development extensively, representing a fundamental shift in business processes. Understanding, and thus fully embracing, agile and DevOps is fundamental to implementing a secure DevOps program to protect cloud-native apps, the specific use case of which this paper explores later.

Hand in hand with the rise of DevOps and automation in the development and deployment of cloud-native applications is the proliferation of trusted identities with excessive privileges (e.g., service accounts, API keys, automation bots, third-party contractors, and admins). These high-privilege accounts pose a significant risk to cloud infrastructure and cloud-native applications.

Cloud Security Challenges Span Attack Types and Visibility Gaps

While the cloud has promised to get organizations out of the data center provisioning and management business, IT has, in fact, become more complicated at a time when there is an ongoing acute shortage of cybersecurity skills. Two-thirds of respondents in a research study conducted by ESG said that IT has become more complex over the last two years, with 53% citing a problematic shortage of cybersecurity skills. The top contributors to this perceived increase in complexity most often cited by respondents include an increase in the number of endpoint devices, higher data volumes, and an increase in the number of applications used by employees.[7]

[7] Source: ESG Master Survey Results, *2019 Technology Spending Intention Survey*, March 2019.

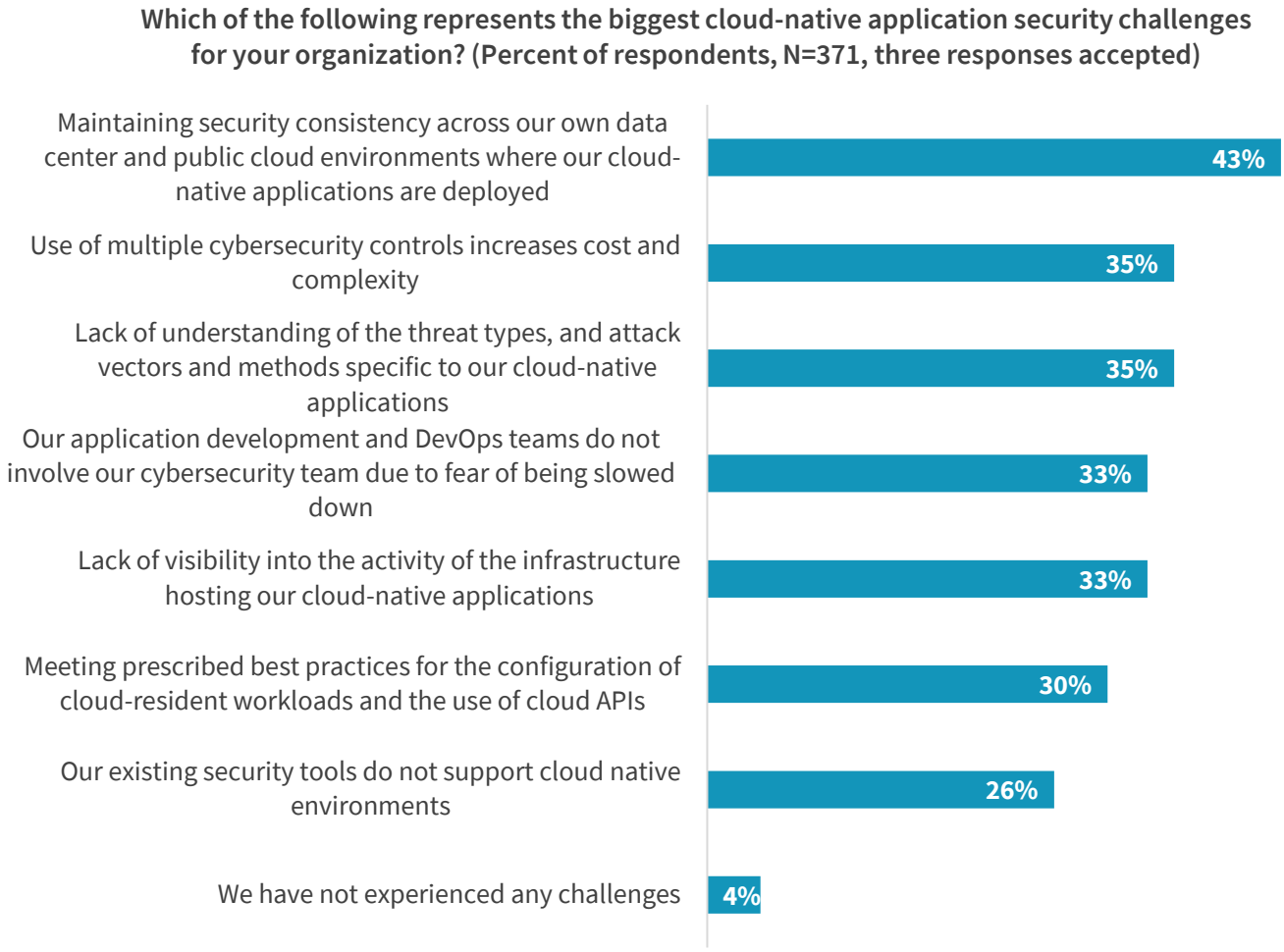
Siloed Approaches Lead to Lack of Consistency and Increased Complexity

A typical approach for managing and securing new environments and technologies is to do so off-to-the-side with different personnel and a unique set of controls. Such a siloed approach has been the modus operandi for securing cloud-native applications, creating a set of operational challenges.

According to ESG research, the challenge in securing cloud-native apps most-cited by respondents (43%) is maintaining consistency across the disparate infrastructures of hybrid, multi-cloud environments where cloud-native apps are deployed (see Figure 4). Another 35% shared that the use of multiple cybersecurity controls has led to increased costs and complexity with other top responses indicating a need to better understand threat models specific to cloud-native apps and a lack of visibility into the activity on the infrastructure hosting those applications.

The challenge in securing cloud-native apps most-cited by respondents (43%) is maintaining consistency across the disparate infrastructures.

Figure 4. Top Challenges Securing Cloud-native Applications



Source: Enterprise Strategy Group

The Shared Responsibility Model Can Be Challenging

The shared responsibility model of cloud security depicts the division of labor between the cloud service provider (CSP) and the customer for securing cloud services. While the line of demarcation changes based on the type of cloud service being

used, a few constants remain: data security and identity and access management, including privileges, are always the customer's responsibility. However, the fact that so many organizations experience data loss indicates that the customers of cloud services are struggling to keep their end of the bargain.

A Varied Set of Threats Puts Cloud-native Apps at Risk

When it comes to the types of attacks that are of concern to participants in ESG's research, there are, not surprisingly, many. The list of top-of-mind threats includes tried and true exploits that take advantage of known vulnerabilities in unpatched operating systems and applications with zero-day exploits.

Another threat of foremost concern is indicative of a visibility gap into how cloud services are provisioned, per the 90% of research respondents who indicated they are concerned about misconfigured cloud services, sever workloads, network security, or privileged accounts. With respect to the latter, 83% also report concern with the misuse of privileged accounts by an inside employee. Security teams are concerned about ensuring that the infrastructure and platform services used by cloud-native applications are configured according to security best practices such as the benchmarks published by the Center for Internet Security (CIS).

Container Security Concerns Include Deployment Flexibility

The complete set of application container security concerns is indicative of a need to secure the container lifecycle from pre-deployment to production.

The portability of containers has respondents thinking through the need to align locality with the architectural implementation of container security controls, the container security concern most-cited by respondents (32%).[8] Also cited by 32% of respondents as one of their container security concerns is the need to verify the integrity of registry-resident images with respect to vulnerabilities and compliance with standard configurations such as the benchmarks published by the Center for Internet Security (CIS). The complete set of application container security concerns is indicative of a need to secure the container lifecycle from pre-deployment to production and to keep pace with the rate at which containers are deployed without the inclusion of the appropriate runtime security controls.

Lack of Consolidated Visibility into Authorizations and Activity Increases Risk of Access Misuse

Without the ability to continuously monitor privileges assigned to accounts across cloud environments and the activity in these accounts, security teams are unable to detect malicious insider activity, account for compromise, and access misuse in a timely manner. The widespread use of automation in deployment exacerbates the impact of compromised accounts.

A Porous Human Perimeter Is Resulting in Data Loss from Cloud Stores

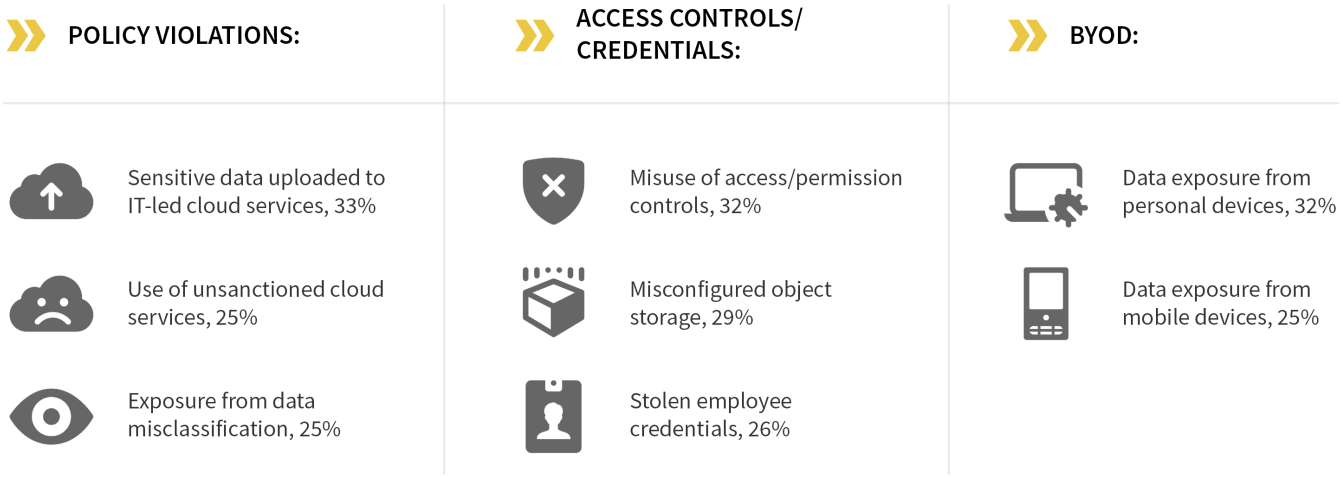
How common is data loss from cloud stores? Research conducted by ESG reveals that 50% of organizations who store data in a cloud have lost cloud-resident data.[9] Participating organizations report data loss from SaaS apps, IaaS services, and platform-as-a-service (PaaS) environments, indicating that there is not one type of cloud service with which data loss is exclusively associated.

Thematically, the cause of such widespread data loss from cloud stores is due to a porous human perimeter with policy violations, credential abuse, and insecure personal devices (see Figure 5).

[8] ibid

[9] Source: ESG Master Survey Results, *Trends in Cloud Data Security*, January 2019.

Figure 5. Top Contributors to Cloud-based Data Loss



Source: Enterprise Strategy Group

The root cause across these issues is a lack of visibility into what cloud-resident data is sensitive, who has access with what level of privileges, and the security posture of the devices from which cloud-based data is being accessed.

The Extensive Set of SaaS Applications Is Creating Identity Governance Challenges

The widespread use of enterprise file sync and share (EFSS) services for storing and sharing content along with productivity and collaboration tools has created identity governance challenges. Absent the use of an identity provider (IDP) for single sign-on (SSO) functionality as a means to federate access to cloud apps and more, the roles and privileges of identity may be in the silos of each cloud application, not only challenging basic identity and access administration, but also creating a likelihood of overprivileged accounts. Traditional role-based access controls are a poor fit in dynamic cloud environments because they assign a fixed set of privileges to a user or role, even when most of the privileges are no longer needed.

New Workflows Are Expanding Third-party Risk

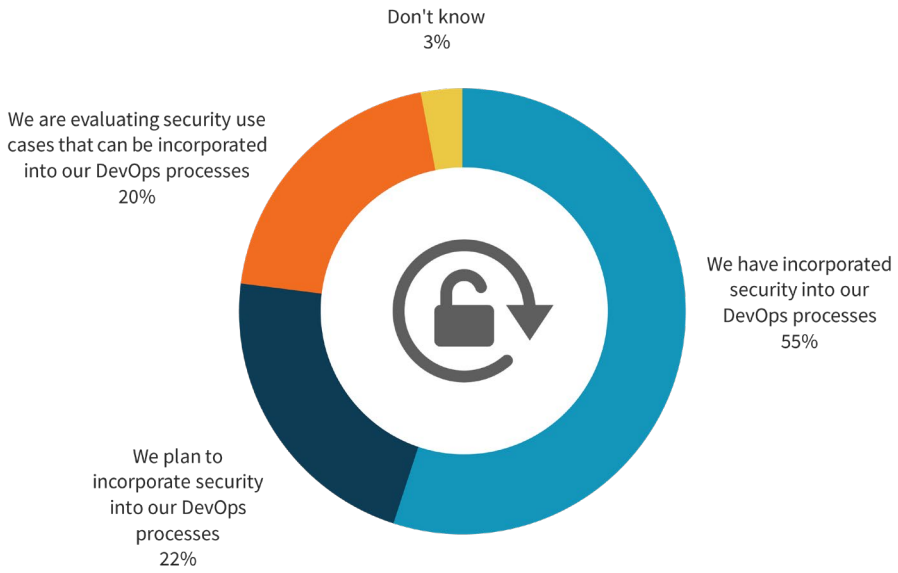
Another dynamic born out of the use of cloud apps such as EFSS services and productivity and collaboration tools is how they have enabled collaborative workflows not only among employees but also with a range of third parties. The fact that so many different types of individuals have access to cloud-resident data has increased third-party risk. In fact, 40% of ESG research respondents stated that business partners have access to their organization's cloud-resident sensitive data.[10]

Leverage Secure DevOps and Proven Best Practices to Keep Pace at Scale

Fortunately, there are a range of solutions for these issues, which collectively are offered as a set of best practices for updating a cybersecurity program for the cloud era, some of which are new, and others the reapplications of proven approaches. At the center of retooling programs is treating security as an immutable DevOps use case with an initial focus on people and process. Fortunately, many organizations that participated in ESG's research that are down their own cloud-native paths are actively employing secure DevOps or "DevSecOps" practices (see Figure 6).

[10] Source: ESG Master Survey Results, *Trends in Cloud Data Security*, January 2019.

Figure 6. Integration of Security into DevOps Processes



Source: Enterprise Strategy Group

The 55% of respondents indicating they have incorporated security into their DevOps processes is a marked increase from 34% of participants who said the same in a 2017 ESG research study.[11] Where in the software development lifecycle (SDLC) did respondents start? Initial DevSecOps use cases included those implemented in both the pre-deployment and runtime stages such as hardening workload configurations during integration and automating the application of runtime controls at build time.

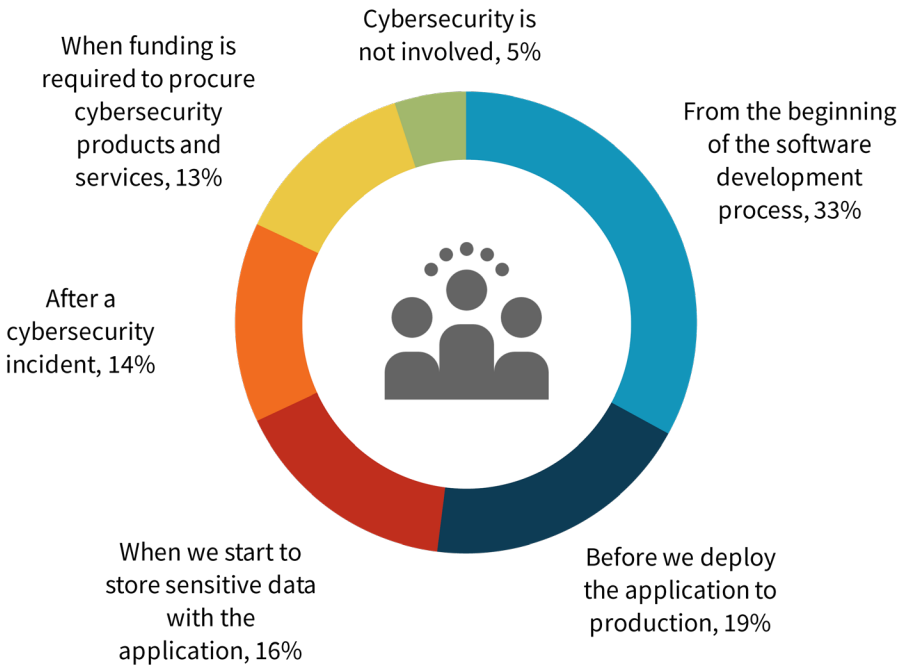
Of note are the percentages of businesses currently doing so selectively, planning to do so, or evaluating DevSecOps use cases, indicative of a need for specifics for how to get started or expand their secure DevOps program.

Get Started with Organizational Alignment

In the spirit of "first things first," a secure DevOps program must be treated as a team sport. Just as DevOps has been about a cultural shift away from virtual boundaries between development and operations teams, this is also how security should be brought into the fold. That is, securing cloud-native applications must be treated as a shared responsibility among cross-functional project team members, which raises the question: when does security get involved in the process of securing cloud-native applications? While some organizations in ESG's study involve the cybersecurity team from the beginning of the software development process, per the 33% who said they do so, too many wait to treat security as a priority and a first-class DevOps citizen (see Figure 7).

[11] Source: ESG Master Survey Results, *Trends in Hybrid Cloud Security*, November 2017.

Figure 7. The Involvement of Cybersecurity in the Cloud-native Application Development Process



Source: Enterprise Strategy Group

A dose of pragmatism is in order for those who have not yet embarked on a secure DevOps program: start small and establish repeatable processes via automated security checks and balances that lead to the corollary of infrastructure-as-code, and security-as-code.

Secure the Cloud-native Application Lifecycle

The current set of DevSecOps use cases cited by ESG research respondents reflects an intent to secure the entire cloud-native application lifecycle.

ESG's research further highlights that securing *both* the pre-deployment and runtime stages are important, with a relatively equal number of respondents citing each stage as more important than the other and only 22% sharing that they view the importance of securing the pre-deployment and runtime phases as equal. Much of the discussion around secure DevOps use cases has been framed by a call to "shift-left" to build security into the development and integration stages via use cases such as code scanning and vulnerability remediation. Writing secure code and shipping hardened images to production is a big part of the DevSecOps equation, but equally important are automatically applying runtime controls vis-à-vis integration with the CI/CD orchestration tooling used to push apps to production. The current set of DevSecOps use cases cited by ESG research respondents reflects an intent to secure the entire cloud-native application lifecycle (see Figure 8).

Figure 8. Secure DevOps Use Cases by Stage

Pre-deployment:

- **26%** Software vulnerability scanning of registry-resident container images
- **25%** API vulnerability management (in both)
- **23%** Software vulnerability scanning in the build pipeline
- **20%** Discovery, inventory, and auditing of APIs in mobile and cloud native apps (in both since discovery and runtime is pre and auditing is runtime)

Runtime:

32% Malware detection and prevention

30% Software vulnerability scanning of production containers and server workloads

26% System activity recording for incident response

26% Network segmentation and monitoring of inter-container and workload communication

25% API vulnerability management (in both)

23% Exploit detection and prevention

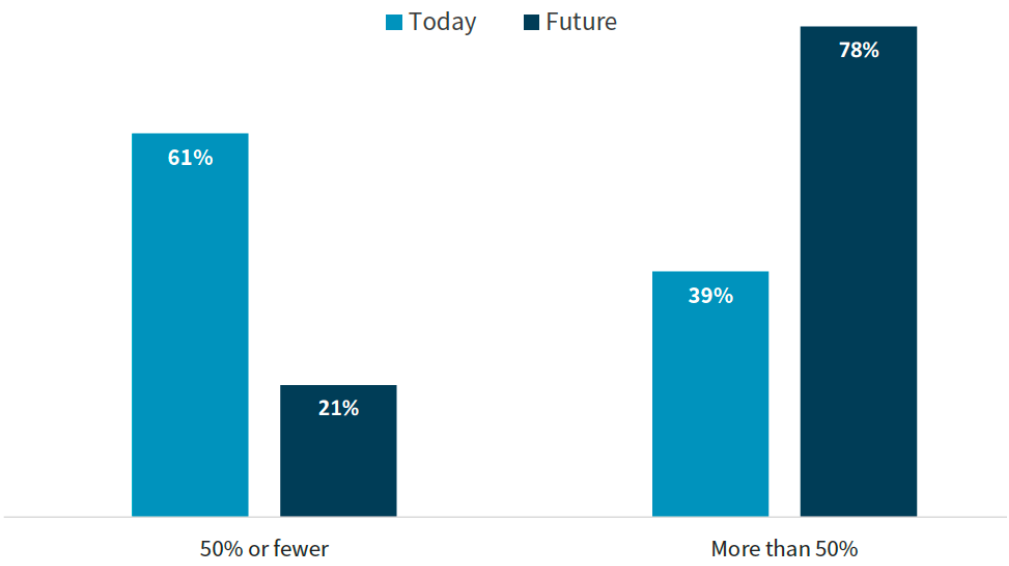
20% Discovery, inventory, and auditing of APIs in mobile and cloud native apps

20% Access controls and auditing of management actions

Source: Enterprise Strategy Group

Where does implementing these use cases along the build-ship-run continuum lead us? As noted above, a critical success factor in implementing a secure DevOps program is repeatability, achieved by implementing security-as-code that can be replicated across multiple projects. As such, there is good news: an expanded set of use cases and more involvement of the cybersecurity team will increase the number of cloud-native apps secured via DevSecOps over time (see Figure 9).

Figure 9. Percentage of Cloud-native Apps Secured via the Involvement of the Cybersecurity Team



Source: Enterprise Strategy Group

Secure Fleets of Web Apps via Defense in Depth

The web-tiers of modern applications are often deployed in public cloud platforms for two obvious reasons: auto-scaling of the back-end to meet periods of high demand and access to content delivery networks (CDNs) for local edge-based access to scale the front-end. To achieve these performance and quality-of-service (QoS) objectives, web apps are being refactored or built from scratch on cloud-native architectures. Because exploits against known vulnerabilities and zero-day threats are of concern, a defense-in-depth approach is required to protect these fleets of web apps from compromise.

In addition to employing traditional rules-based solutions to mitigate cross-site scripting (XSS) attacks and SQL injection attacks, DevOps teams also need newer, effective methods to protect against new attack methods in production cloud environments. To do so, behavioral-based approaches that provide advanced context around web requests should be viewed as highly appropriate for apps deployed in auto-scaling groups as there should be no deviations from baselines or normal system activity. Additionally, effective software and security teams have established their baseline of expected web request traffic patterns. Doing so allows them to more readily identify anomalous or unexpected traffic patterns, which together with other request context such as IP address reputation or unexpected HTTP request header values are indicative of an attack.

Next-gen web application firewalls (WAF) and runtime application self-protection (RASP) solutions provide a proactive means to monitor web request traffic and instrument and observe web requests before the payloads reach the application origin. Additionally, comparing next-gen WAF and RASP runtime analysis against known good behavior of a system in question allows for sharing possible malicious request indicators, thus preventing the same attack pattern from adversely impacting other subscribers to the same services. Leveraging anonymized, but highly relevant, peer-level data sourced from production traffic yields a higher level of fidelity in the detection and prevention of attacks while reducing false positives. A next-gen WAF approach also allows DevOps teams to use automated web defense with high precision in production, unlike legacy WAF vendors that rely on regular expression pattern matching rules and signatures.

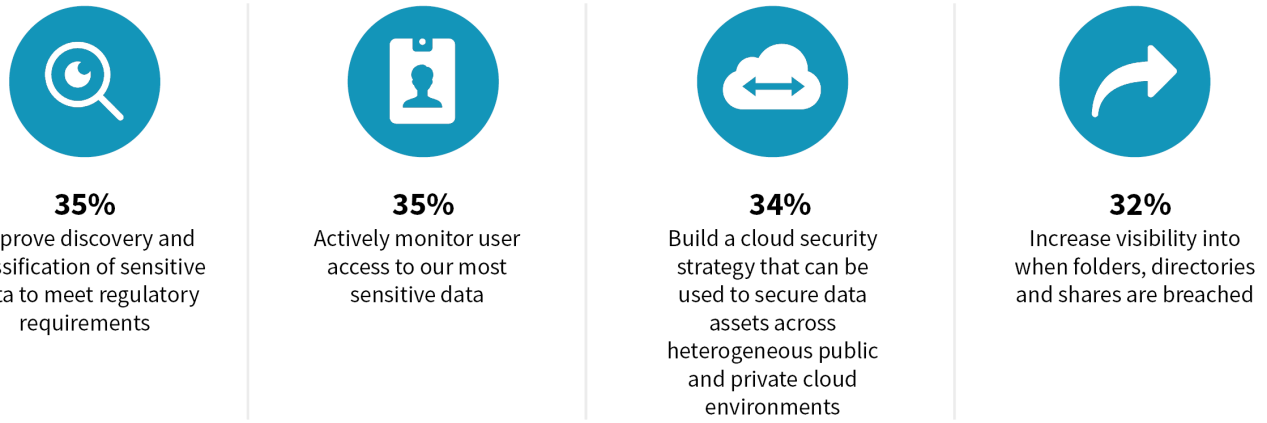
Leveraging anonymized, but highly relevant, peer-level data sourced from production traffic yields a higher level of fidelity in the detection and prevention of attacks while reducing false positives.

Employ Least Privilege to Protect the Identity Perimeter

The cloud security readiness gap is highlighted by the 81% of research participants who shared that their on-premises data security practices are more mature than those for securing cloud-resident data. Core to closing this gap is an identity perimeter-based approach to protecting cloud assets and data in cloud stores. To secure the identity perimeter, organizations need to enforce the principle of least privilege and continuously monitor access and privileges to detect misuse and compromise. They need visibility into the who, what, when, where, and how of access to and use of cloud-resident data to establish context to protect the integrity of these data assets. The best practices to do so are highlighted as the top cloud data security priorities shared by participants in research conducted by ESG (see Figure 10).[12]

[12] Source: ESG Master Survey Results, *Trends in Cloud Data Security*, January 2019.

Figure 10. Top Cloud Data Security Priorities



Source: Enterprise Strategy Group

A pragmatic approach is rooted in first gaining visibility into the who, what, where, and how dimensions of data access and usage to inform privilege management policy.

In addition to discovering and classifying data and actively monitoring user access to an organization's most sensitive data, other priorities include building a strategy that secures data across disparate environments and gaining greater visibility into when cloud-stores are breached. At the core of taking action against the priorities is a focus on privilege management via a zero-trust implementation of least privileged access. Zero-trust in this context is rooted in first gaining visibility into the who, what, where, and how dimensions of data access and usage to inform privilege management policy.

The Bigger Truth

The research findings analyzed in this report are intended to help inform not only corporate cybersecurity and DevOps teams, but also line-of-business leaders on the cybersecurity implications of cloud-first initiatives including:

- **Increased heterogeneity**. The disparate mix of technologies used in cloud-native apps along with the use of a wide variety of SaaS applications has resulted in a heterogenous mix of cloud services making the centralized implementation of policies and processes challenging.
- **Visibility gaps**. The need to gain greater visibility into cloud usage includes identifying and remediating both software and configuration vulnerabilities, locking down the use of privileged and service accounts, and discovering not only what cloud services are storing sensitive data, but also which users have access to those assets.
- **An expanded perimeter**. The amorphous perimeter of the cloud era necessitates a broader definition of the perimeter inclusive of network, data, and user, making identity a critical cloud security control.

However, where there are challenges, there are opportunities, with perhaps the biggest opportunity being shifting the organizational view of cybersecurity as a tax on innovation to an immutable requirement for all cloud-related projects. High-level best practices for securing cloud-native applications and the expanded perimeter include:

- **Employ an application lifecycle approach**. A secure DevOps program will employ DevOps-friendly cybersecurity controls that integrate natively with the CI/CD tool chain to secure the development, integration, test, build, delivery, and runtime stages of an application's lifecycle.

- Secure the identity perimeter. Treating the usage patterns and the privileges with which users access cloud-resident data collectively as an identity perimeter starts with the discovery of sensitive data and extends to continuous monitoring to detect policy violations and anomalous activity that puts data assets at risk.

The gap between the degree to which cloud services and cloud-native technologies have and will continue to be consumed and organizational readiness to secure that usage requires a retooling of cybersecurity programs to keep pace with the speed of the cloud era.

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides actionable insight and intelligence to the global IT community.