Cloud Security is Much More than Prevention and Compliance

Pathfinder

April 2021

Commissioned by

ExtraHop

451 Research

S&P Global
Market Intelligence

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.

Executive Summary

While discussions about cloud security often quickly diverge into specific tooling, it is imperative for organizations to understand the broader context of cloud adoption so they can address the root causes of potential issues. Data from our research reveals several trends: a significant proportion of modern DevOps is distributed inside the organization, but the reality of cloud transformation is that many security teams will be asked to address hybrid and/or multicloud use cases. As they do so, teams are rushing to address a perceived gap in cloud skills.

As they look to address tooling gaps, organizations will find they require a combination of cloud-specific security tooling and enterprise security capabilities. Cloud-specific tooling includes cloud security posture management, cloud workload protection platform and some specific services from cloud providers.

Using cloud-specific tooling is a positive step but likely not enough. Cloud security should fit into the organization's broader security management practice. This means deploying and integrating tooling such as security information and event management and network detection and response, which can address coverage for both existing on-premises scenarios and cloud-native ones. Ultimately, addressing cloud security requires a combination of cloud-specific security tooling with existing enterprise security capabilities. The prudent mindset is to start with prevention and compliance but then quickly incorporate cloud threat detection and response.

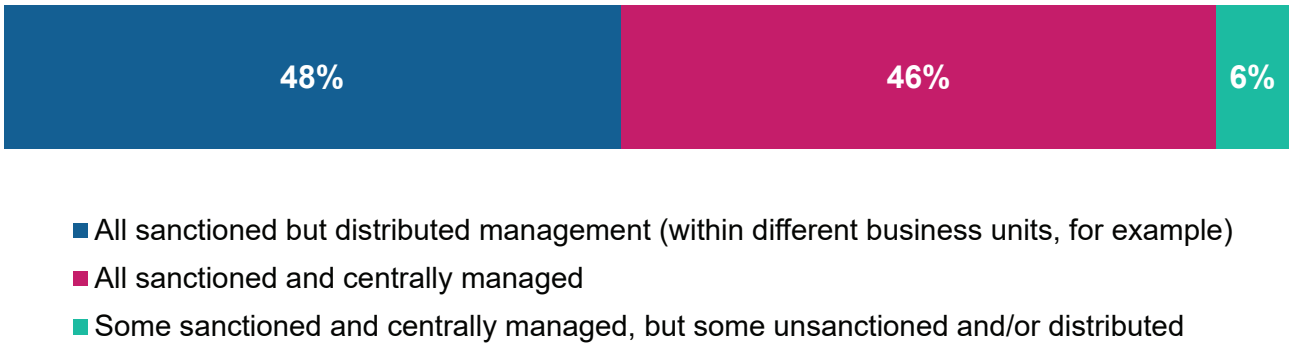
Introduction

As an industry, we're way past the point of highlighting that cloud security is an important topic. It is now imperative to understand just how to go about implementing a robust cloud security approach that can cover threat mitigation, monitoring, detection and response. Rather than jump into deploying a specific product category to protect their cloud workloads, we believe it is important for practitioners to understand key industry trends so that they can orient themselves and their organization and develop the right approach to addressing cloud security. For many organizations, this means addressing both human and technological aspects.

Organizational Challenges

Jumping into security tooling conversations without understanding the context – including what is driving cloud implementations – can lead to adverse effects such as unnecessary friction and, worse, possible security gaps. The two data points in Figures 1 and 2 below illustrate trends we see as particularly relevant to cloud security. There's a good correlation between DevOps practices and cloud adoption, so the comparisons are applicable. The first key point is that nearly half of all DevOps work is managed within business units, which means security functionality must necessarily address a large, distributed set of stakeholders.

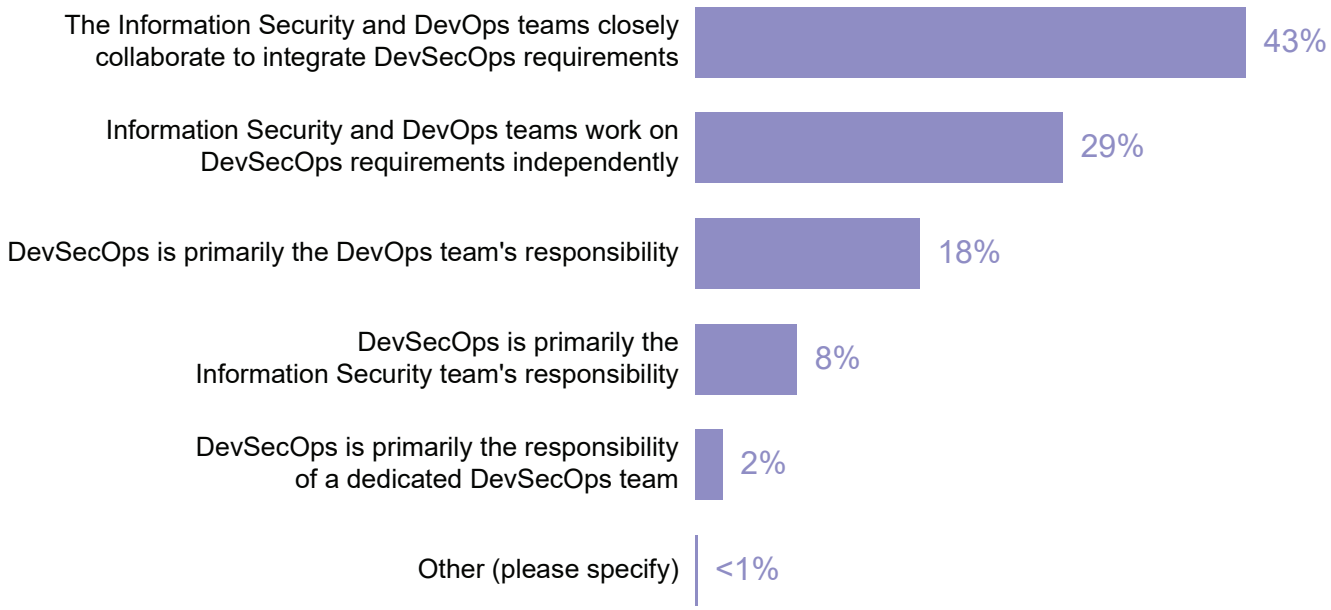
Figure 1: DevOps Management



Q: What best describes your DevOps management?
Base: All respondents, abbreviated fielding (n=337)
Source: 451 Research's Voice of the Enterprise: DevOps, Organizational Dynamics 2020

The second finding is that the integration of security practices with DevOps is, in most cases, a work in progress. Understanding this may help security teams craft an effective approach that enhances collaboration.

Figure 2: DevSecOps Collaboration



Q: For DevSecOps (i.e., the integration of security elements into DevOps), which of the following most closely describes the level of team collaboration in your organization?

Base: All respondents (n=551)

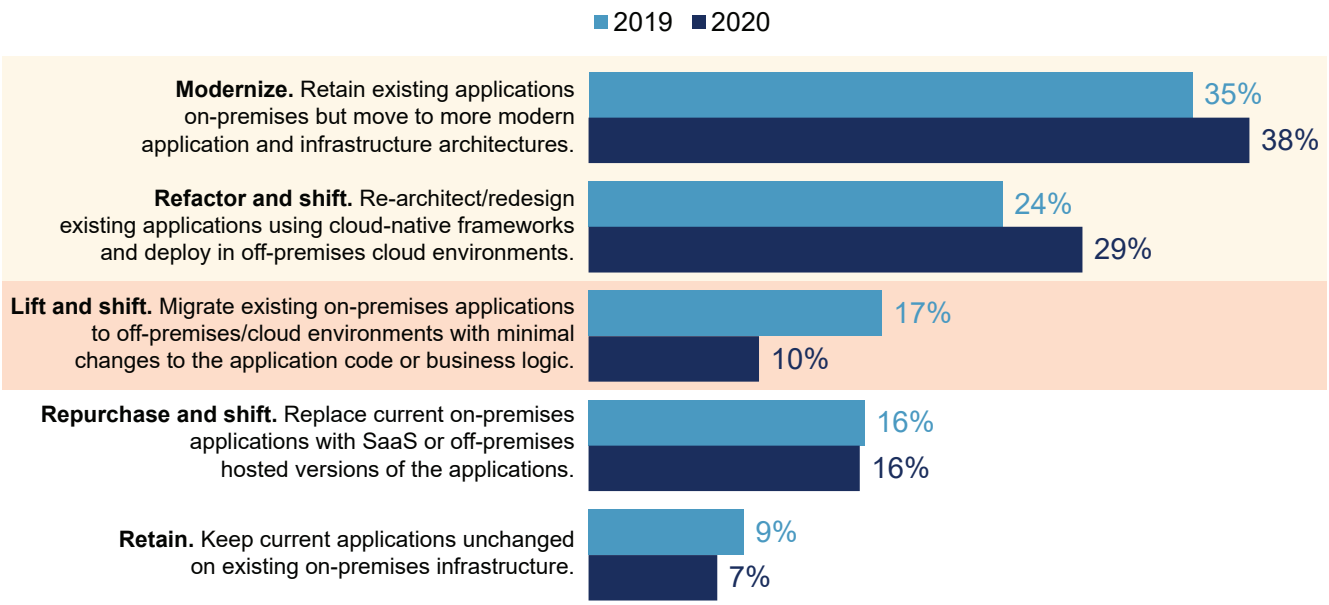
Source: 451 Research's Voice of the Enterprise: DevOps, Organizational Dynamics 2020

Multicloud and Hybrid Are a Reality

Beyond the need for collaboration across teams, our research points to usage patterns for cloud platforms that clearly indicate that, at the organizational level, 'cloud' adoption will mean supporting both traditional on-premises deployments and cloud-based environments. Security tooling needs to be able to address diverse environments.

Two key findings emerged from recent 451 survey data regarding IT application modernization. First, traditional 'lift and shift' is a small and diminishing proportion of responses (see Figure 3). Second, there's a broad equivalence between those choosing on-premises modernization (which may include cloud-native technologies) with those choosing cloud-based options.

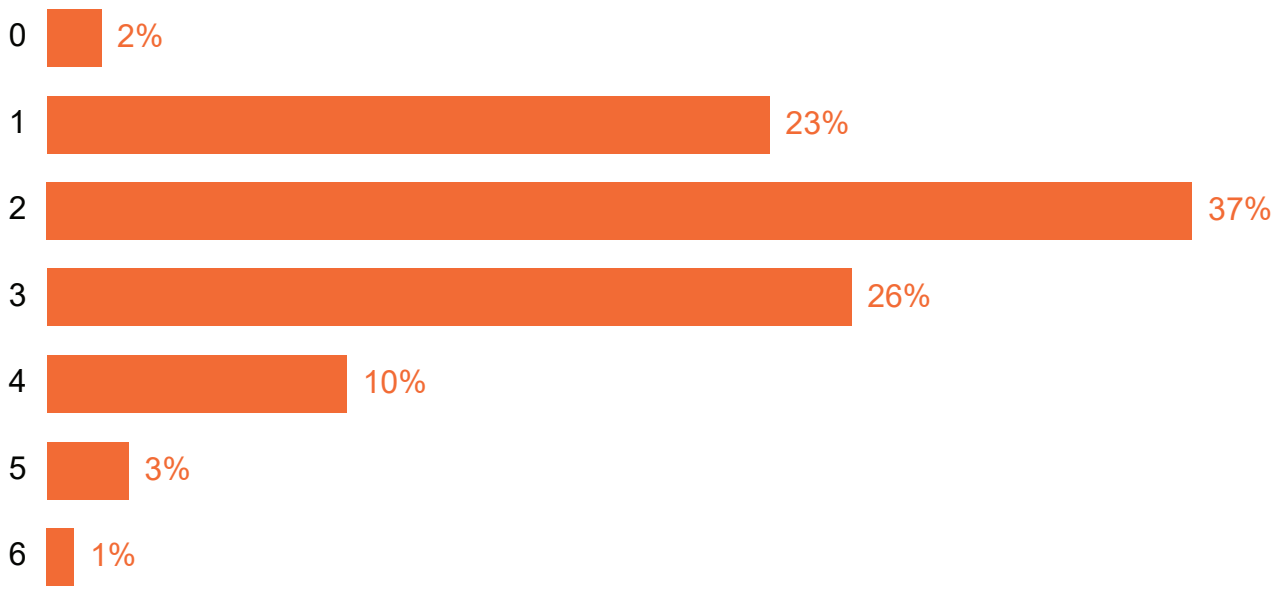
Figure 3: Nuanced View of Destinations



Q: Which of the following best describes your organization's approach to mission-critical legacy applications and workloads going forward?
Base: All respondents (n=496)
Source: 451 Research's Voice of the Enterprise: Digital Pulse, Workloads & Key Projects 2020

Another key finding is that most respondents said that they use two or more cloud providers. The impact on cloud security is that customers will need to consider tooling that works well across multiple environments.

Figure 4: Cloud IaaS/PaaS Usage

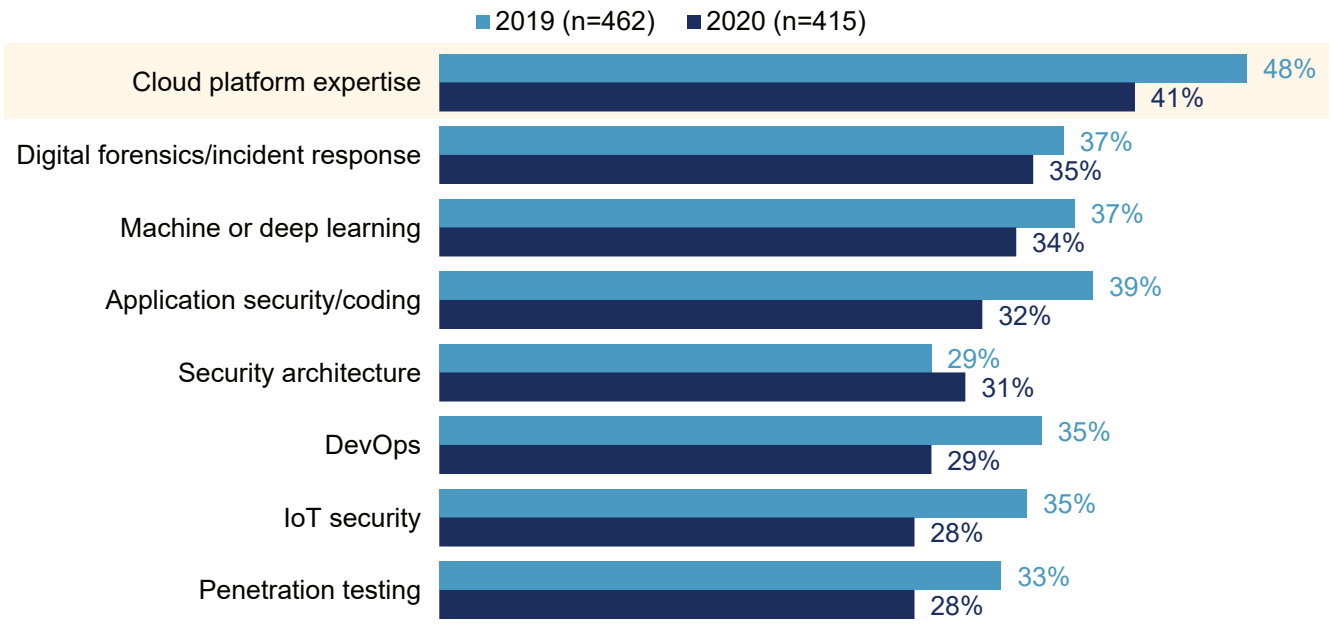


Q: How many cloud providers does your organization use?
Base: Organizations that use IaaS/PaaS/public cloud (n=230)
Source: 451 Research's Voice of the Enterprise: Cloud, Hosting & Managed Services, Vendor Evaluations 2020

Security Teams Ramping up on Cloud Skills

Security teams are recognizing they need to equip themselves to tackle these new cloud security challenges. The data below illustrates this: for two years in a row, security respondents have indicated that cloud technologies is the top skill that their organization does not adequately address, although the latest numbers are lower, which could indicate a positive trend. This is a key topic to address so that practitioners can make informed decisions about how to secure cloud environments.

Figure 5: Cloud Skills Are a Key Gap



Q: Which skillsets are inadequately addressed at your organization today? Please select all that apply.

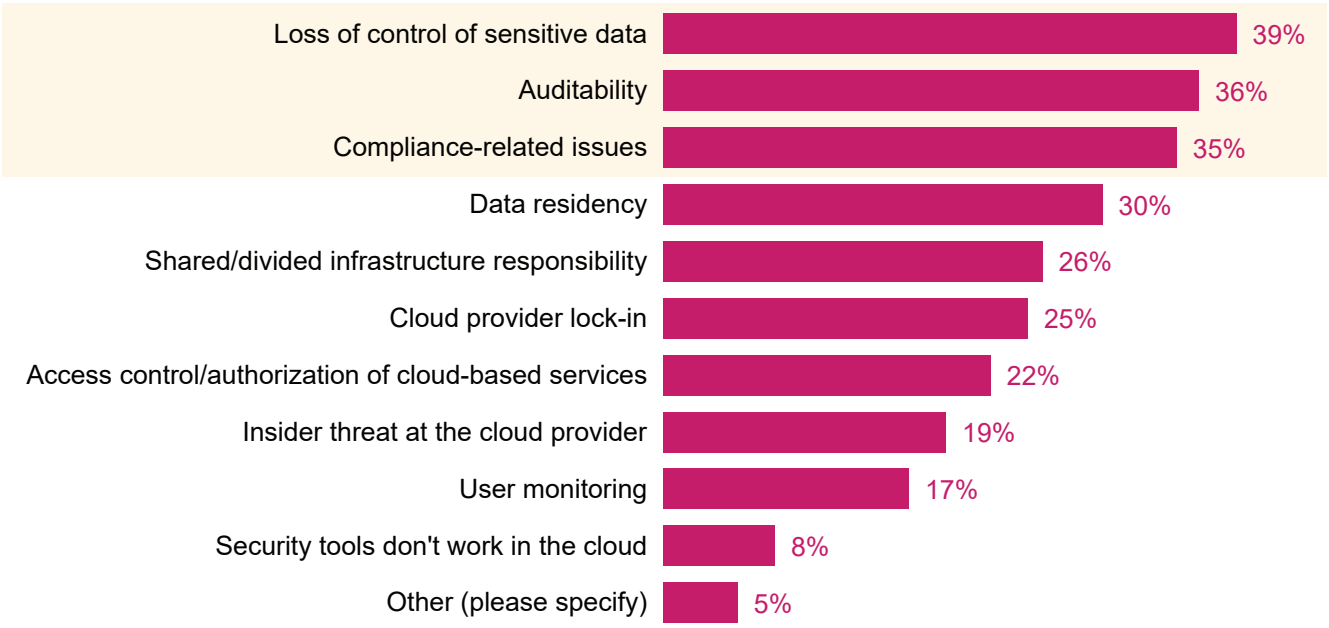
Base: All respondents

Source: 451 Research's Voice of the Enterprise: Information Security, Organizational Dynamics 2019 and 2020

Security Challenges Reflect Broad Cloud Usage

As they tackle cloud security demands, security practitioners' main concerns have to do with the broad, uncontrolled use of cloud. Security professional respondents to a recent 451 survey identified their top cloud security concerns as uncontrolled use of sensitive data, possibly in uncontrolled locations; whether cloud environments are properly configured; and how to report on the state of cloud security compliance to key stakeholders.

Figure 6: Cloud Security Concerns



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

Base: All respondents (n=199)

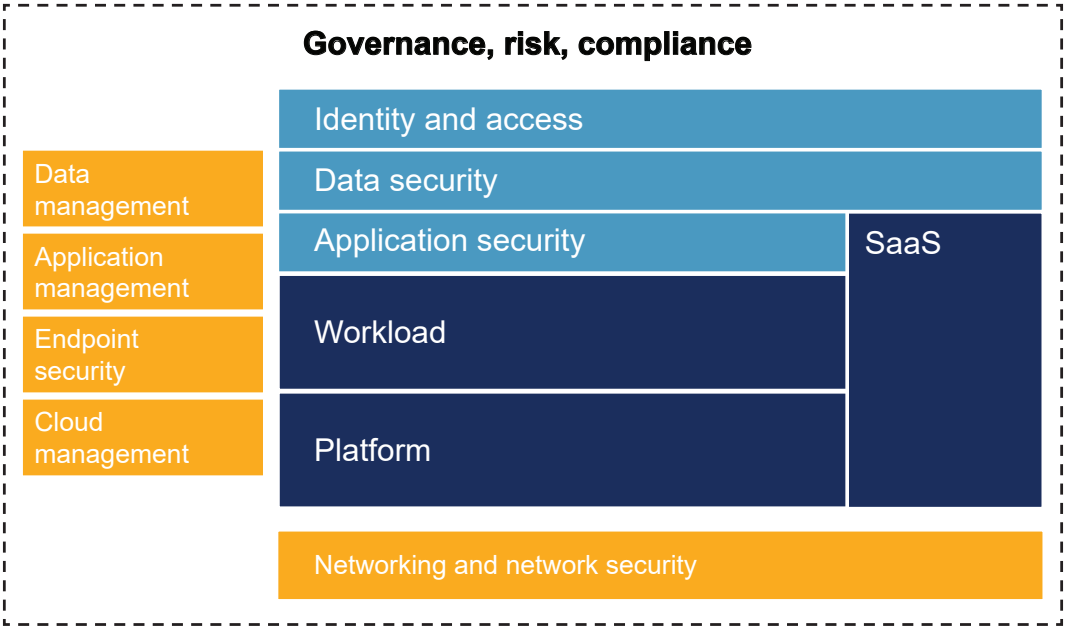
Source: 451 Research's Voice of the Enterprise: Information Security, Budgets & Outlook 2020

Cloud Security in Context

As we consider tooling, we use the model in Figure 7 below to understand key influences in cloud security. The explicit targets for cloud security are usually the 'platform' and 'workload' layers for IaaS and PaaS environments. 'Platform' refers to basic constructs that organizations use to create cloud-native environments, such as cloud accounts, virtual machines, instantiation instructions, networking constructs and storage buckets. 'Workload' refers to the actual virtual machines, containers, serverless functions, PaaS services, etc., that are instantiated on top of the cloud platform. We note that security concerns targeting application security, data security, and identity and access management also increasingly influence these areas.

As cloud environments become more prevalent, additional areas (in yellow) increasingly add native support for cloud security use cases. Finally, there's an increased movement to better fit cloud security concerns in broader governance, risk and compliance models that organizations use for IT management. We're long past the point of cloud 'science projects'; organizations are now deploying cloud initiatives across the board, covering public, private and hybrid cloud deployments. These deployments require both cloud-specific tooling and enterprise-wide security capabilities.

Figure 7: Framing Cloud-Native Security



Source: 451 Research

Cloud-Specific Security Tooling

While the market is in a continuous state of innovation, the two key types of cloud-specific tools are targeted at the cloud environments and the hosts running cloud 'workloads.'

Cloud Security Posture Management

Cloud security posture management (CSPM) refers to the general class of tools offered by cloud providers and third-party vendors to inspect current or proposed configurations of cloud assets. These tools usually tackle the 'platform' components in the model above. In most cases, these assets refer to the basic building blocks of cloud presence – networking, compute, storage, etc. Recently, CSPM vendors have started offering increased support for containers and container management platforms such as Kubernetes.

CSPM tools generally scan cloud configurations on a periodic basis using the provider's own management APIs, or they integrate themselves into the development process – usually via a continuous integration system – for analyzing configurations specified via infrastructure-as-code practices. Some CSPM tools incorporate the processing of activity logs from cloud providers to detect potential changes. Most CSPM offerings compare configurations and current state against a predefined set of criteria tied to customer-defined targets, provider- or industry-recommended practices, or standards such as CIS controls and PCI-DSS.

CSPM tools are generally effective at identifying potential configuration issues within the base cloud platforms. Offerings from the cloud providers are limited to their own environments, while third-party tools usually offer multicloud support.

By their very nature, CSPM tools focus on configurations and not on runtime state or runtime activity, such as application activity and network traffic. Other key challenges for CSPM tools include proper coverage for the plethora of services offered by cloud providers and having the necessary policy management constructs to support the many separate cloud initiatives within larger organizations.

Cloud Workload Protection

Cloud workload protection platforms (CWPPs) are generally host-centric security tooling for hosts running in public, private or hybrid clouds and address the components in the 'workload' section of our model. CWPPs initially focused on virtual machines but have increasingly expanded to other forms of compute such as cloud-provided bare-metal server and container workloads, often in conjunction with Kubernetes-based orchestration.

Importantly, CWPP offerings are mostly agent-based, meaning they require an agent to be installed on the host itself or the supporting environment. For environments that have achieved streamlined automation of host-based workloads, it typically means inserting the agent on base images, but this still requires considerations such as compatibility with OS or container runtime and agent maintenance, etc.

CWPP offerings are aimed at providing a consolidated view of security use cases centered on a host, which makes it possible to segment concerns about the host from concerns about the cloud environment itself. While the exact feature set applied will vary by product and type of workload being secured, the typical use cases for CWPP include:

- Host and application configuration management and reporting, which is useful for systems hardening and compliance reporting
- Vulnerability management
- File integrity monitoring
- Anti-malware protection, including memory protection
- Application control ('allow lists' and 'deny lists' for processes and binaries)
- Endpoint detection and response support for cloud assets, including behavior monitoring and investigation support

In some cases, CWPP can also assist with network-centric configurations, such as policy management for cloud firewalls, and setting up micro-segmentation for workloads.

CWPPs have been a popular component for cloud security architecture because they typically align well with existing workflows for security teams, treating the cloud-based hosts in a comparable manner to traditional server endpoints. CWPPs are better suited for this than traditional, non-cloud security tools since they can provide the necessary runtime information about workloads while interacting better with the elastic and dynamic nature of cloud workloads and cloud service provider APIs.

Some of the obstacles related to CWPPs include the overhead of managing the agents, as mentioned above, and the focus on a host-centric view that makes it more difficult for security teams to consider broader impacts of security events. Understanding the broader role that a workload has on the environment is a key concern for those involved in cloud threat detection and response, particularly as attack patterns now typically include distinct stages such as reconnaissance, compromise, lateral movement and exfiltration.

Cloud Provider Security Services

In addition to third-party CSPM and CWPP tooling as described above, customers can pick some security functionality from the cloud providers themselves: all major providers have put together services aimed at addressing some elements of cloud security. These services cover areas such as data loss prevention, aggregating security alerts from multiple sources, cloud-specific threat detection and traffic protection via application firewalls.

It is possible for customers to use these services in conjunction with CSPM and CWPP for enhanced security coverage. A key benefit of cloud provider security services is that they're relatively easy to enable/consume, usually just a few clicks or API calls away.

That said, there are also a few potential downsides to these services: first, they're invariably limited in scope to the provider itself, and any provider's implementation is generally different enough from the others. Given the multicloud nature of deployments, this places the onus of managing these differences on customers themselves. There may also be consistency issues – all services may not exist in all provider regions – and, in some cases, cost may become an issue as well.

Enterprise Security tooling

As organizations deploy cloud environments, they quickly realize it is important to tie these deployments to the broader efforts around security. With that in mind, we believe it is important to call out two types of technology aimed at supporting cloud-native deployments in public and private environments.

Security Information and Event Management

Security information and event management (SIEM) systems have been a key tool for many security operations teams. SIEM systems can be on-premises or cloud-based offerings, and they typically perform log aggregation and management from multiple sources. SIEMs then deploy different analytics capabilities to the data, including rules and anomaly detection, followed by visualizations, reporting and alerting. Many SIEM systems will interoperate with more sophisticated orchestration and automation systems.

In the context of cloud security, SIEM systems are often a collection point for security telemetry from both on-premises sources and cloud environments. It is quite possible that security insights from the other tooling mentioned here will find its way into a customer's SIEM system.

A key challenge that SIEMs need to overcome is balancing generic collection from multiple sources while performing more sophisticated analytics that depend on the nuances of each environment. SIEMs also usually require specific expertise for tuning and creating meaningful rules.

Network Detection and Response

Network detection and response (NDR) refers to technology for monitoring, analyzing and responding to security use cases within network traffic at scale. NDR typically covers both 'north-south' (in and out of datacenters and security zones) and 'east-west' ('between' servers or endpoints within the same security zone) traffic flows. As traffic is observed, NDR tools typically parse the packets or flows being analyzed and are then able to perform more advanced analysis for numerous security use cases. NDR offerings typically go beyond more traditional network traffic analysis tooling by providing capabilities for deeper searches into existing data, threat analytics and integrated responses with other components in an organization's security architecture.

The type of analysis that is done varies, but it normally includes using machine-learning-based models for anomaly detection, use of historical patterns, use of traffic metadata for matching against security insights such as threat intelligence, and use of frameworks such as MITRE's ATT&CK.

In the context of cloud security, NDR is relevant on two important fronts: first, several NDR tools can be deployed to cloud environments using the increasingly common traffic-mirroring capabilities made available by the cloud providers precisely for this purpose; second, as shown before, many cloud deployments will coexist with hybrid or on-premises deployments, and security teams are likely to consider NDR as it is meant to support both cloud and on-premises scenarios.

Using network-based analytics such as NDR may be suitable to get a broader perspective of activity within an environment, particularly when the participant endpoints may not have security agents installed. This is quite common in scenarios such as supporting IoT-type devices that may not be able to install agents and dealing with unmanaged endpoints or, in some cases, endpoints that had their agents disabled by the attackers.

NDR tooling may also be effective in observing attempts at lateral movement by attackers, particularly if the analytics process was able to derive an accurate baseline of expected traffic.

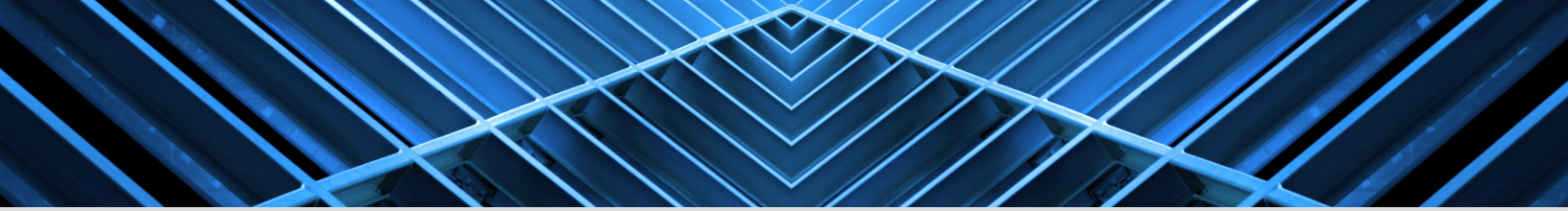
When considering NDR, customers should be aware of a couple of challenges: first, the placement of sensors or collectors for traffic capture is key because NDR tooling bases its analysis on the traffic it is able to capture; second, there's an industry-wide shift to using increasingly strong encryption support for data in transit for most modern applications. This means NDR tooling must either somehow obtain the necessary keys for decryption (which may require additional configuration or deployment of specialized endpoint agents) or settle for performing traffic analysis without looking at application payloads.

Conclusions

The research indicates that as organizations increase their cloud deployments, they're likely to do so in a manner that spans multiple environments, technologies and teams. Failing to account for this when considering security architecture may lead to incomplete or inefficient coverage.

While security teams are actively ramping up on their cloud capabilities and identifying key areas of concern, they should maintain a broader view of cloud security and be able to support deployments on public providers as well as on private cloud or on-premises infrastructure. From a technology perspective, cloud security should likely include a combination of tooling to address the key use cases for platform and workload, but also the broader integration with the rest of the organization's security architecture, particularly as teams look to defend resources that may be interconnected across environments.

Because organizations have their unique requirements, we expect their choices for security architecture will be different in the particulars, but all will likely follow a common path – one that starts with collaboration across teams and a good focus on prevention and compliance, but that quickly builds on creating solid practices for threat monitoring, detection and response.



content provided by: ExtraHop

Cloud workloads are deployed into highly dynamic environments, often utilizing and coexisting with a wide variety of cloud providers and third-party platforms and services. The workloads themselves range from legacy applications that have been migrated from traditional on-premises data centers, to applications that have been built specifically to run on cloud platforms, to entirely serverless applications. Some may receive weekly or daily updates while others may exist for only a few seconds, creating a serious challenge for SecOps and SOC teams tasked with maintaining continuous visibility and security of cloud-based workloads.

There are many ways to monitor and protect cloud workloads, from agent-based third-party solutions, to cloud provider monitoring and logging, to perimeter-based firewalls and WAFs. All technologies have certain advantages and drawbacks, so organizations often deploy a variety of cloud workload security solutions depending on their regulatory environment, desired security profile, and tolerance for risk. Over the past several years, network detection and response (NDR) has seen widespread deployment in traditional data center environments, primarily to inspect east-west traffic flowing between workloads for threats and anomalies. Now its benefits are being realized by organizations running workloads in cloud environments.

NDR is a unique security technology in that it provides what SecOps practitioners consider the 'ground source of truth'. NDR taps into network traffic flows via strategically placed sensors or cloud-native packet mirroring services to analyze an exact copy of network packets. Users, devices, network protocols, and key metrics are identified, and machine learning is then applied to identify and report any threats and anomalies in real-time. Since NDR is agentless and out-of-band, attackers cannot detect or avoid it, providing SecOps with an unassailable observation perch from which they can monitor all network activity and rapidly identify threats and attacks. And since NDR is agentless, there are no agents to integrate during development, and no updates to install after deployment, making NDR entirely frictionless from a DevOps perspective.

ExtraHop Reveal(x) 360, a SaaS-based NDR security solution, helps to erase visibility gaps and protect workloads across hybrid and cloud environments including AWS, Azure, and Google Cloud. By integrating with cloud-native packet mirroring services, Reveal(x) 360 provides real-time visibility into network traffic flowing to and from workloads, even when that traffic is encrypted. Reveal(x) 360 applies advanced machine learning and behavioral analysis to network metadata to accurately identify anomalous behavior associated with attacks, breach attempts, and malware. Once threats are discovered, Reveal(x) 360 can alert your security team for remediation, or integrate with SOAR solutions for auto-remediation. The result is stronger security posture and minimized risk for both hybrid and cloud-first organizations.

Whether you're improving visibility into your cloud workloads, investigating threats, or securing your investment in cloud, ExtraHop helps you protect and accelerate your business.

To try ExtraHop Reveal(x) 360 for yourself, visit our interactive online demo at www.extrahop.com/demo or learn more at www.extrahop.com/products/cloud.

CONTACTS

The Americas
+1 877 863 1306
market.intelligence@spglobal.com

Europe, Middle East & Africa
+44 20 7176 1234
market.intelligence@spglobal.com

Asia-Pacific
+852 2533 3565
market.intelligence@spglobal.com

www.spglobal.com/marketintelligence