ESG SHOWCASE

A Network-based Approach to Cloud Workload Security

Date: November 2021 **Author:** John Grady, Senior Analyst

ABSTRACT: Many of the tools organizations use to secure their cloud resources rely on logs and agents, have limited visibility into threats, or address only part of the environment. These limitations can result in increased complexity and reduced security effectiveness. Network-based tools that provide unified, threat-centric protection across an organization's entire environment, without impeding the speed of DevOps, can help alleviate these challenges and strengthen security. ExtraHop's Reveal(x) 360 platform provides cloud-native visibility, detection, and response for the hybrid enterprise.

The 'Cloud' Comes in Many Flavors, Leading to a Variety of Security Options

Migrating resources to the cloud has become a business imperative for many organizations, a trend only accelerated by the pandemic as organizations have sought to increase their resiliency and agility. Yet the cloud is not homogenous, and most organizations support a diverse set of cloud services such as infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), and software-as-a-service (SaaS). Specifically, ESG research has found that 78% of organizations use 2 or more IaaS providers.[1] Further, the architectures run in these cloud environments can vary from those closely mirroring traditional on-premises data centers (such as bare metal servers and virtual machines), to more cloud-native models (such as containers and serverless functions). This composition is in transition, with ESG research finding that, while most enterprise workloads (58%) are run on bare metal servers and virtual machines today, organizations anticipate that containers and serverless functions will comprise the majority of workloads (52%) 24 months from now.[2]

Obviously, protecting these resources is critical, so organizations are forced to select from a myriad of security tools with differing capabilities. While there are certainly important use cases these different tools can support, many also come with limitations that complicate the equation. Some examples include:

- Cloud workload protection (CWPP) and endpoint detection and response (EDR) solutions are deployed to prevent, detect, and respond to threats targeting enterprise workloads. These tools are agent-based, which can slow DevOps teams and cause organizational friction if not fully and seamlessly integrated into agile workflows and toolsets. Because of their focus on individual workloads, the telemetry these tools gather is limited to the workloads they are deployed upon. They are able to detect something malicious in the context of a particular workload but may not have broad enough visibility to piece together a comprehensive view of network activity to indicate something is anomalous. Further, bad actors often disable these controls early in the attack chain, leaving organizations blind to subsequent activity.

[1] Source: ESG Master Survey Results, *2021 Technology Spending Intentions Survey*, December 2020.
[2] Source: ESG Master Survey Results, *The Maturation of Cloud-native Security: Securing Modern Apps and Infrastructure*, June 2021.

- Cloud security posture management (CSPM) tools can help ensure compliance and alert when risk levels change. They do this by discovering cloud workloads and analyzing configurations against established compliance benchmarks. Yet while these capabilities are important, they do not provide visibility into threats, which prevents them from identifying or preventing actual attacks.

- Cloud service providers (CSPs) offer their own security tools, some of which include compliance and threat detection and prevention capabilities. These tools can be simple to deploy via native CSP management consoles but may not be applicable to other CSPs or on-premises environments. This siloed visibility and management introduces additional complexity and can reduce security effectiveness.

- Security information and event management (SIEM) can serve as the aggregation point to collect data from different control points covering different parts of the environment. However, logging everything in the cloud can become prohibitively expensive, as well as delay alerting when incidents do occur. Additionally, attackers can tamper with or disable log collection to make detecting their presence more difficult.

Many of these limitations align with the top challenges organizations report with regard to public cloud security (see Figure 1).[3] The threat landscape is cited most often, meaning that detecting malicious activity must be the priority. The increasing usage of IaaS and lack of staff and skills to properly secure these environments requires tools that are not only able to keep pace with the dynamic nature of IaaS adoption but are also familiar to security teams. Finally, with the complexity of attacks often making response more difficult, security teams must have consistent visibility across the entire environment and seamless response to address incidents when they do occur.

Figure 1. Top Public Cloud Infrastructure Security Challenges

Source: Enterprise Strategy Group

[3] Source: ESG Research Report, *Network Security for Cloud and Data Centers*, to be published.

Network Detection and Response Provides Threat-centric, Agentless Protection for Cloud Workloads

Network traffic analytics (NTA) tools are well established in many enterprise environments and have evolved toward network detection and response (NDR) to include integrated response capabilities. ESG research has found that 55% of organizations report using NTA/NDR tools in their on-premises environments.[4] Yet as resources have moved to the cloud, some organizations have shifted attention away from network-based security tools. However, while cloud environments are certainly different from on-premises networks, it remains critical to have comprehensive visibility into the traffic flows across all workloads, devices, and services, including IaaS, PaaS, and SaaS. Network detection and response solutions can provide this visibility and fill the gaps left by CWPP, EDR, CSPM, logs, and CSP-provided tools by providing three key differentiators:

While cloud environments are certainly different from on-premises networks, it remains critical to have comprehensive visibility into the traffic flows across all workloads, devices, and services.

1. Agentless architecture. Whether due to the scale of workloads or types of architectures, agents are not always practical. Because NDR does not require agents, security teams maintain full responsibility for deployment and management. This ensures that security and cloud operations teams can regain control to secure cloud environments, while DevOps teams can remain focused on their core responsibilities and work at their own pace without security operations adding friction and slowing the process down.

2. Threat-centric, out-of-band detection. Configuration hardening and other prevention strategies can block some attacks. But with the breadth of resources and tactics attackers now have, detecting attacks that will inevitably slip through the cracks must be a core pillar of any organization's security strategy. Detection tools should be invisible to attackers to prevent tampering or modification, and alert suspicious behavior early in the attack chain. More than ever, speed of detection is critical to ensure attackers are stopped before significant damage occurs. A good example of this is ransomware attacks, in which attackers spend significant time on the target network mapping and even exfiltrating data. In many cases, the victim is only alerted that they have been breached once the encryption process has begun, at which point it is too late.

3. Hybrid, multi-cloud visibility and response. Attackers clearly understand that most organizations have resources spread across multiple cloud providers and on-premises data centers and use this to their advantage as they move laterally, seeking to establish persistence and escalate privileges. The ability to correlate activity across different locations and resources and paint a comprehensive picture of the environment is critical to defend against these modern attacks. Further, response must be seamless so once malicious activity is detected, workloads can be quarantined to avoid further spread. Finally, this level of visibility enables organizations to proactively hunt threats in their environments and identify attacks much earlier in the attack chain.

Cloud-native NDR with ExtraHop Reveal(x) 360

ExtraHop Reveal(x) 360 is a cloud-native network detection and response platform, providing SaaS-based coverage across enterprise edge, core, and cloud deployments. This unified approach to hybrid and multi-cloud security eliminates visibility gaps and the friction of deploying and operating separate tools for each environment. Sensors deployed in on-premises data centers, clouds, or remote sites process network traffic into anonymized metadata and send it to Reveal(x) 360 for

[4] Source: ESG Research Report, *Network Security for Cloud and Data Centers*, to be published.

analysis. In the case of public cloud deployments, the solution uses CSP packet mirroring features, such as Amazon VPC Traffic Mirroring, to further simplify deployment. In addition to monitoring user traffic to SaaS applications such as Salesforce, Skype, and Slack, Reveal(x) 360 integrates with Microsoft 365 to monitor for suspicious or risky behaviors and correlate detections with broader network context. By unifying visibility across IaaS, PaaS, and SaaS services in a single console with visibility, the platform provides comprehensive network visibility.

Reveal(x) 360 analyzes all interactions across all workloads and more than 70 traffic protocols, including encrypted sessions. The platform uses cloud-scale machine learning algorithms, informed by the petabytes of anonymized threat intelligence collected by ExtraHop daily. These algorithms provide device identification, risk score, entity importance, and, ultimately, high-fidelity attack detection. The platform supports east/west traffic visibility, insider threat analysis, security hygiene violation detection, threat hunting, and rules-based critical CVE exploit detection to identify malicious activity.

The Bigger Truth

The self-service nature of the cloud has resulted in IT and security teams losing visibility and control over developer and line-of-business initiatives. As cybersecurity has become an executive and board-level concern, many organizations have put guardrails in place to ensure cloud usage remains within the confines of corporate policy. However, the business agility and flexibility provided by the cloud means that the genie will never be fully returned to the bottle, and security teams must adapt their tools and processes to fit this reality. Unfortunately, the breadth of disparate cloud resources available across IaaS, PaaS, and SaaS platforms has made this difficult.

Security teams must be able to maintain comprehensive visibility across the entire corporate environment, including the multitude of cloud services in use, to accurately detect threats before they impact the business and do so without adding unnecessary friction. Better integration of security into DevOps practices and tools can certainly help but is not a silver bullet. While the numerous cloud security tools that are available to organizations may help support some of these objectives, NDR can help security teams realize them all through a holistic approach to threat detection without impacting development teams. ExtraHop Reveal(x) 360 provides SaaS-based NDR coverage across enterprise edge, core, and cloud deployments to help organizations achieve these goals.

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

www.esg-global.com contact@esg-global.com 508.482.0188