VECTRA
SECURITY THAT THINKS®

SOLUTION BRIEF

Recommendations when evaluating Network Detection and Response (NDR) for infrastructure-as-a-service deployments

Introduction

Digital transformation is driving enterprises to rapidly enter the next chapter of the cloud. With nearly half of current infrastructure-as-a-service (IaaS) users running production applications on a public cloud infrastructure, organizations will increasingly look to capture the favorable business models, dynamic scaling, availability, and streamlined management that public clouds deliver.

This move to the cloud does not absolve enterprises of all responsibility. In Gartner's research report, Staying Secure in the Cloud Is a Shared Responsibility published Sept. 7, 2018, Senior Director Analyst Steve Riley, notes that "Security in the cloud is a shared responsibility."

Gartner goes on to state that, "Figure 1 illustrates the security handoff points for infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS) and software-as-a-service (SaaS) cloud models.

> "Security in the cloud is a shared responsibility." **Steve Riley** *Senior Director Analyst*

"The handoff point moves up the stack across the models. IaaS offers the most control, with the commensurate security responsibility left to customers. SaaS offers the least control, with the CSP taking on most of the security responsibility. 'People' in the diagram refers to customer-authorized users of applications and data, not to cloud provider employees."

IaaS	PaaS	SaaS
People	People	People
Data	Data	Data
Applications	Applications	Applications
Runtime	Runtime	Runtime
Middleware	Middleware	Middleware
Operating System	Operating System	Operating System
Virtual Network	Virtual Network	Virtual Network
Hypervisor	Hypervisor	Hypervisor
Servers	Servers	Servers
Storage	Storage	Storage
Physical Network	Physical Network	Physical Network

CSP Responsibility | Customer Responsibility

Figure 1: Gartner security handoff points for IaaS, PaaS and SaaS

One of the key findings of Gartner's report is that "the cloud reduces the scope of required traditional security work but doesn't eliminate it. Moving workloads to the cloud doesn't automatically make them 'more secure.'"

Vectra agrees and is of the opinion that it merely shifts the scope required for security operations. In order for security teams to have comprehensive visibility of threats to your digital business, the scope must be expanded beyond the network to include the cloud.

Cloud workloads are not automatically more secure

It is important that organizations detect and respond to traditional network threats, as well as attempts to steal data hosted by the cloud service provider through compromised administrator credentials and privileged access abuse.

Vectra believes security leaders are looking to maintain the same level of visibility and threat detection in the public cloud that they largely enjoy in their own environments today. This document lays out the six foundational tenets when evaluating NDR requirements for cloud deployments.

The cloud does not eliminate security work

1. Consider all identifying behaviors

Attackers often follow the path of least resistance by exploiting human behavior or longstanding infrastructure vulnerabilities. Long before attackers reach a virtual workload, they will have already compromised an end-user device or stolen administrative credentials.

As a result, cloud infrastructures often encounter cyberthreats in the more advanced phases of the attack lifecycle such as internal reconnaissance, lateral movement and data exfiltration.

So rather than focusing on the initial exploit, it is important to detect attackers who have compromised the perimeter and are already inside the infrastructure.

2. Visibility without the use of agents

Native integrations through recent features like AWS VPC traffic mirroring and Azure virtual network TAP eliminate the complexity created by agents. In addtion, further telemetry can be gained by natively integrating with the CSPs API, gaining access to things like control plane events.

By integrating with native IaaS features, most solutions have access to all activity between cloud workloads without the management overhead. Consider NDR solutions that do not rely on agents for visibility.

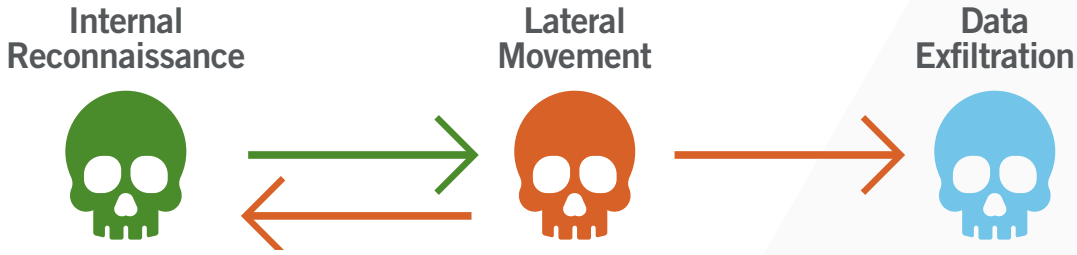

Figure 2: Cloud attacks commonly occur in these three phases of the attack lifecycle

3. Correlated visibility across multicloud environments

While initial multicloud use cases were often a result of disparate teams selecting various cloud providers for their individual goals, the approach today is more deliberate. Organizations have realized that they do not want to become overly dependent on a single cloud provider.

There are also varying degrees of efficiency that can be achieved by using multiple cloud vendors, and multicloud environments offer flexibility in shifting workloads based on business needs.

From a security perspective, this means that NDR solutions must be able to correlate events across multiple cloud environments. Solutions with single-cloud visibility will result in gaps in threat detection.

This also results in an onerous, manual task to correlate behaviors across multiple clouds, making it nearly impossible to connect the dots for attacks that have moved across various public and private networks.

An NDR solution should have native integrations across several IaaS providers and be able to correlate events and incidents across these providers. Ideally, it should also leverage advanced analytics that can surface security incidents rather than a stream of disconnected alerts.

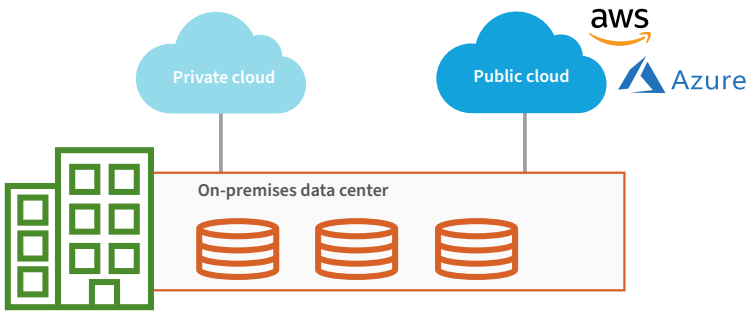

Figure 3: Most enterprises use a combination of on-premises and multicloud approaches

4. Automated correlation between on-premises and cloud environments

Initially, security teams have deployed lift-and-shift approaches to the cloud. Now, as companies' cloud strategies mature, there are true hybrid cloud deployments that span data centers, private clouds, and one or more public cloud service providers.

As part of this hybrid paradigm, on-premises environments still play a crucial role. Reasons to keep both cloud and on-premises environments vary but often include:

- A need to keep data on-premises or in a private cloud to alleviate data security concerns while using the power and agility of the public cloud to execute transactions
- Support for legacy applications that are costly or unable to be virtualized as well as cloud-friendly modern applications
- A desire for a distributed hybrid cloud architecture to prevent a single point of failure and build business resilience

History of course teaches us that threat actors continue to innovate, resulting in attacks that cross cloud and enterprise boundaries. An attacker can initially compromise an on-premises host, eventually gain access to credentials for a cloud resource, and move laterally to access it.

In this environment, an NDR solution must support native deployment across both public IaaS and on-premises environments and correlate events and incidents between the two.

5. Continuously monitor privileged access

A traditional, access-based approach to zero trust relies on one-time gating decisions that use a predefined list of privileged identities. This approach is fundamentally flawed when cyberattackers have already obtained credentials or have escalated privileges.

In an environment that inherently lacks traditional security boundaries, like the cloud, the need for continuous, real-time assessment of user, host and service privilege levels is especially pronounced.

In addition, the complexity of access management makes it prone to misconfigurations. Continuous monitoring and alerting for unusual privileged access are a must for modern NDR solutions.

6. Efficiency matters

The need for full-stack visibility through the entire attack lifecycle across cloud and on-premises data sources will generate vast amounts of behavioral data. The scaling and storage capabilities of typical cloud deployments also adds to the volume of data.

The sheer volume, velocity and variety of data inhibits the ability to detect and respond effectively. Security analysts are already overwhelmed with events and alerts, most of which are false positives or low risk.

An NDR solution that relies on security-enriched network metadata and selective file capture delivers the best investigative value. It is easier and faster to find things — at a much lower computational and storage cost.

Further, a solution that presents findings as a single incident — including chains of related activities rather than isolated alerts that must be manually pieced together — saves valuable time and maximizes security resources. In addition, a solution leveraging Threat Intel will be able to strengthen these detections with attribution to speed up investigations.

Consider NDR solutions that can efficiently detect incidents across vast data sources and do not place an additional burden on your security team.

Conclusion

The NDR market has seen high levels of innovation and disruption. New approaches are proving its value to customers while disrupting this long-established market. Support for the public cloud is a strong example of new requirements that have evolved from an everchanging network.

NDR solutions must keep up with these evolving challenges. Yet, at its core, NDR solutions must continue to fulfill the fundamental need to detect and respond to threats quickly and efficiently.

Email info@vectra.ai vectra.ai

For more information please contact a service representative at sales-inquiries@vectra.ai.