ExtraHop

Rise Above the Noise.

NETWORK DETECTION & RESPONSE:

Cloud Security's Missing Link

How virtual taps' arrival to the cloud is revolutionizing enterprise security

EXECUTIVE SUMMARY

Cloud security teams traditionally rely on perimeter-focused security tools or logs that can miss critical threats. As breaches become more common, enterprises are recognizing the need for visibility in east-west corridor traffic, but until recently gaining access to network data has been difficult. With the introduction of Amazon VPC Traffic Mirroring, security teams can now access the missing link in cloud security without the need to deploy agents. Network detection and response provides observed ground truth with context, that can't be turned off or evaded by savvy attackers. This report shows why cloud-native NDR is the best approach for detecting, investigating, and responding to threats in AWS environments.

TABLE OF CONTENTS

The missing link in cloud security 2

What's the east-west corridor and why is it important to enterprise security? 3

How do traffic mirroring capabilities empower enterprises? 4

What's the future of NDR in the cloud—and how can you capitalize on it? 5

Conclusion 6

THE MISSING LINK IN CLOUD SECURITY

It's the holy trinity of enterprise security: Gartner's SOC Visibility Triad.

If you're not familiar with the triad, here's a bit of backstory: It comes from the Cold War-era idea of a "Nuclear Triad"—strategic bombers, intercontinental ballistic missiles, and submarines—that significantly reduced the risk of an enemy destroying all of one nation's nuclear forces in one strike.

In short, the Nuclear Triad was a cohesive mechanism that essentially prevented first strikes altogether. In much the same way, modern enterprises can deploy a triad of security measures to significantly reduce the risk of attackers operating on a network long enough to achieve their goals.

THE SOC VISIBILITY TRIAD INCLUDES:	
ENDPOINT DETECTION & RESPONSE (EDR)	• Records system activities and events taking place on endpoints (e.g. desktops, servers, IoT devices) • Provides security teams with the visibility they need to uncover incidents on the perimeter (North-South)
SECURITY INFORMATION & EVENT MANAGEMENT (SIEM)	• Collects and analyzes logs generated by the IT infrastructure, applications, and other security tools • Provides event correlation, threat monitoring, and incident response
NETWORK DETECTION & RESPONSE (NDR)	• Analyzes network traffic in real time to provide ground truth • Detects and contextualizes threats inside the perimeter (East-West) • Enables rapid response to suspicious network activity, minimizing the potential impact

of cloud misconfigurations go unreported

TOP BARRIERS TO FASTER CLOUD ADOPTION:

Data security

General security risks

Each category serves a different purpose, but it can be distilled down to this: EDR and SIEM protect your perimeter, monitoring outside threats and (ideally) warning you if someone breaks in. NDR works off of the assumption that no matter how advanced your perimeter protection, those outside security measures will eventually fail. And whether it's malicious outside attackers or an insider threat, knowing what happens in your environment is just as essential as keeping unwanted visitors out.

When enterprises started migrating to the cloud en masse, EDR and SIEM solutions quickly followed, ensuring hybrid enterprises had plenty of opportunities to fend off outside attackers. But NDR—an emerging category even on-prem—has had a slower journey to the cloud, leaving a dangerous gap in cloud security. When Security

Operations teams have little to no visibility inside their organization, they can't protect it. Currently, attackers can dwell an average of three or more months inside an enterprise before detection, which obviously opens the door for catastrophic consequences. For example, misconfigurations are a top threat in the cloud—yet 99% percent go unreported, which can lead to massive data breaches.

But finally, the public cloud is maturing. With this maturation, cloud-first enterprises are getting the opportunity to restore the missing link in the SOC Visibility Triad and ensure that, if and when perimeter security fails, they're able to analyze suspicious behavior and respond to threats as soon as they appear.

What's the east-west corridor and why is it important to enterprise security?

Think of all network traffic like a compass, with different types of traffic running perpendicular from one another. The north-south corridor encompasses traffic between servers and outside users, also known as the interaction between your enterprise and the outside world. That's covered by EDR and SIEM.

The east-west traffic corridor is the route that all server-to-server traffic takes. Everything that happens inside of your enterprise. If it's not being monitored, you've got a huge security blind spot.

Traditional, on-premises enterprises handled this in the past by implementing traffic mirroring tools that created an exact replica of network traffic by physically splitting the fiber optic beam. Over time, network vendors like Cisco began implementing tap functionality like the switched port analyzer (SPAN) to mimic the same effect through software.

Obviously, neither of those approaches are an option in the cloud. And without that data, NDR in the cloud just isn't fully possible. For cloud-first hybrid enterprises, this has caused a bit of a headache in recent years. When surveyed, 66% of businesses listed security as the biggest barrier to cloud migration. Because of security and visibility gaps in the cloud, many of these organizations were either stalling or postponing their migrations altogether. In extreme cases, organizations that had already started a migration to the cloud have been known to send cloud resources back to on-premises solutions.

Hybrid companies concerned with protecting the east-west corridor have attempted workarounds, but they remain extraordinarily complicated for Security Operations teams to manage and, even worse, are largely ineffective. However, two main strategies have prevailed:

1. Routing traffic through an in-line virtual appliance, which has an impact on performance and bandwidth.

2. Placing packet-forwarding agents on cloud instances, which provides the traffic information, but is highly fallible and requires a Herculean effort from Security Operations teams.

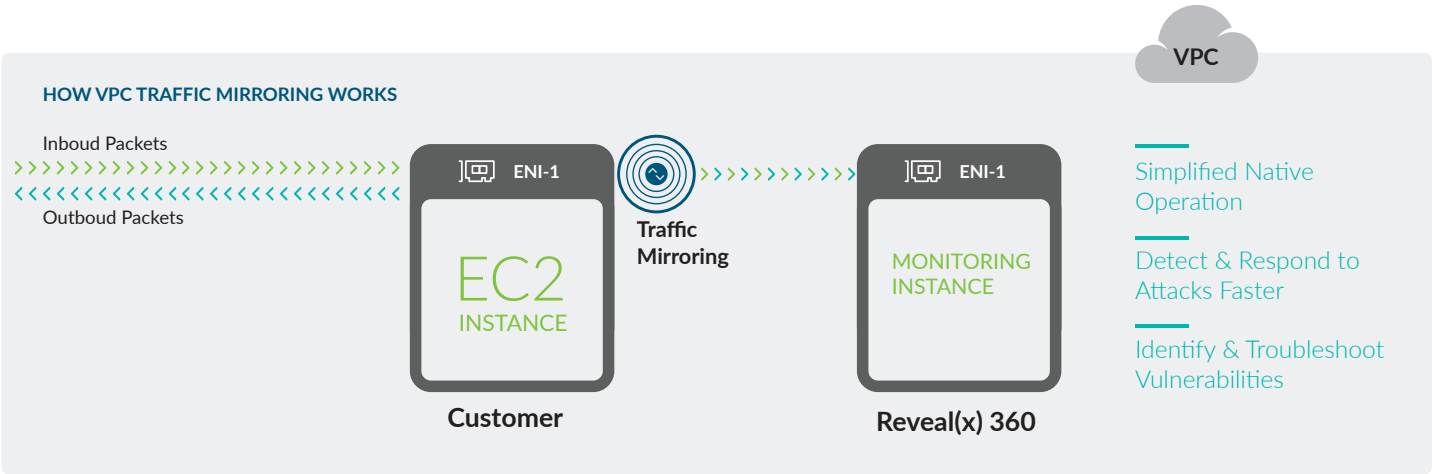
Yet even these expensive workarounds cannot cover the entire east-west attack surface and are no replacement for real NDR.

How do traffic mirroring capabilities empower enterprises?

When AWS announced Amazon VPC Traffic Mirroring, they opened up a world of possibilities for enterprises using or planning to migrate to AWS. Like on-premises traffic mirroring, Amazon VPC Traffic Mirroring provides copies of all network traffic within the perimeter for analytics and troubleshooting.

Why is that helpful? Simply put, it's an attacker's worst nightmare: undetectable and unable to be turned off. Traffic mirroring is designed to ensure enterprises can be 100% confident they know what's happening inside of their organization in real time—and unlike endpoint and log data, data from network traffic cannot be altered or exploited.

AWS is doing the heavy lifting, laying the groundwork natively so enterprises no longer have to build workarounds. With the click of a button, users can now route traffic from specific instances or entire VPCs directly to analytical tools. That east-west visibility gap? It has effectively been eliminated in AWS.



What's the future of NDR in the cloud – and how can you capitalize on it?

Now that Amazon Web Services has made NDR in AWS environments possible, tools and solutions are flooding the market. This provides a key opportunity for enterprises on multiple levels.

First, it enables you to equip Security Operations and IT Operations teams with the tools they need to achieve cross-functional success and reach their full potential. Instead of being bombarded with alerts all day and struggling to make sense of what's going on in their organization, they'll have the tools they need to isolate serious threats and prioritize essential activities.

They'll also be able to apply the scalable computing resources of the cloud to the task of performing machine learning on network data. Machine learning can surface high-fidelity information about asset behaviors and trends, correlate alerts and data, build predictive models, and make sense of observed activities across sensors in customer deployments.

At the end of the day, enterprises will thrive on higher-quality insights and fewer false positives, saving time and preventing alert fatigue. With deep insights and rich data, ops teams can answer critical questions, like whether company logins have been compromised or sensitive files have been accessed across the entire hybrid environment. Decisions can be made in real time and in context, based off of the most powerful, objective, complete source of data: the network.

The benefits of cloud-native NDR go beyond security—it also provides new opportunities for cross-team collaboration and increased productivity, and delivers a way to amplify your other enterprise solutions. But to achieve this functionality and success, it's essential to select the right tool.

BENEFITS & SOLUTIONS

Cloud-first enterprises should look for an NDR solution that:

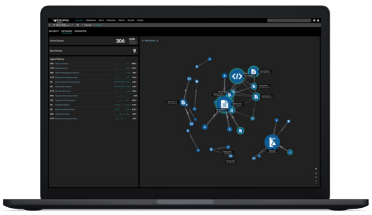
- **Scales to the enterprise level:** Make sure your entire attack surface is secure, from your data center, across your cloud workloads, to your remote sites.
- **Provides high-fidelity insights, based off of machine learning:** Put the vast compute resources of the cloud to work for sophisticated analysis of network data.
- **Goes way beyond alerts:** Index and store metrics for streamlined investigation and provide continuous packet capture for deeper forensic investigation.
- **Puts insights in context for your organization and delivers information intuitively:** Understand the big picture of what's happening across every tier of the environment, from users to web to database to storage to network.
- **Creates a strong foundation for critical business initiatives:** Enterprises on the fence about undertaking cloud adoption or other innovative strategies should be able to rest easy, knowing NDR is the fail safe that will protect their organization at any time, in any scenario.

NEXT STEPS FOR ENTERPRISES

In a day and age where data breaches regularly make the front page, it's impossible to overstate the value cloud-native NDR can deliver to enterprises. You may not be able to stop breaches, but you can make sure they're limited to minimal damage.

Now that traffic mirroring is available in the cloud, the missing link of the SOC Visibility Triad has been restored. Cloud-first enterprises can embrace NDR and full enterprise protection.

ExtraHop Reveal(x) 360 is the first and only SaaS-based NDR solution for hybrid environments. Reveal(x) 360 leverages Amazon VPC Traffic Mirroring to provide agentless visibility, real-time detection, and intelligent response in AWS environments.



FREE TRIAL

Try Reveal(x) 360 for Free.

See how ExtraHop Reveal(x) 360 analyzes every transaction in the cloud, detects threats in real time, and helps you intelligently respond to attacks. Request your free trial at at **extrahop.com/freetrial/**.

ABOUT EXTRAHOP

ExtraHop provides cloud-native network detection and response for the hybrid enterprise. Whether you're investigating threats, ensuring the availability of critical applications, or securing your cloud investment, ExtraHop's breakthrough approach helps you rise above the noise so you can protect and accelerate your business. To experience the power of ExtraHop, explore our interactive online demo or connect with us on LinkedIn and Twitter.

ExtraHop

info@extrahop.com
www.extrahop.com