Network Detection and Response in the Cloud Comes of Age

An ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) White Paper

Prepared for ExtraHop

By Paula Musich

July 2019

EMA™
IT AND DATA MANAGEMENT
RESEARCH | INDUSTRY ANALYSIS | CONSULTING

INTRODUCTION

IT security practitioners are learning the hard way that taking legacy network security tools and applying them to cloud-based workloads doesn't really work all that well, but few cloud-native options exist to provide the visibility and control needed to secure traffic traversing to and from, as well as between, those workloads. This is because the shared security responsibility model used by public cloud providers, such as Amazon Web Services (AWS) and others, prohibits access to physical network hardware. While agent and log-based approaches have been applied as stopgap measures to bring at least some visibility, they come with their own baggage. They can create traffic bottlenecks, increase complexity, and introduce their own vulnerabilities. Recognizing the barrier that this complexity and lack of visibility are creating for broader cloud adoption, IaaS providers are beginning to address these issues. Microsoft led the charge in 2018 at its Ignite conference when it became the first public cloud provider to offer a virtual network tap to enable out-of-band monitoring for Azure network traffic. Microsoft's much larger rival in the IaaS market, Amazon Web Services, followed suit in late June 2019, when Amazon launched its first traffic mirroring capability for customers using its Virtual Private Cloud (VPC) service.

The Azure virtual network tap and Amazon's new VPC Traffic Mirroring opened the doors for network performance and network security monitoring partners to bring a comprehensive view of network activity to the task of managing and securing traffic generated by public cloud workloads. At least 15 partners joined AWS in its VPC Traffic Mirroring launch. Notable among them was ExtraHop Networks, which used the occasion to launch the first SaaS-based network detection and response for AWS workloads.

BRINGING NDR AS A SERVICE TO THE MASSES?

IT security practitioners have been stymied in their efforts to secure the growing amount of East/West network traffic in cloud environments because existing packet capture appliances are not allowed to access span ports on the cloud providers' networks. The alternatives available to date have been either more limited log collection from the cloud provider or agent-based collection. Neither provides continuous visibility and both can miss more sophisticated, multi-staged attacks. At the same time, the alternatives require the acquisition of separate tools that don't integrate well into existing, on-premises security tools and workflows.

The introduction of VPC Traffic Mirroring enables AWS customers to capture traffic from any workload in an AWS Virtual Private Cloud and route it to the detection tools they are already using. That's great for organizations that have the wherewithal to acquire, deploy, and scale the use of network traffic analysis tools in their SOC, but the cost and expertise required to do that exclude companies with more limited budgets and staff.

VPC Traffic Mirroring enables AWS customers to capture traffic from any workload in an AWS Virtual Private Cloud and route it to the detection tools they are already using.

ExtraHop's new Reveal(x) Cloud SaaS offering for AWS takes the deployment burden away from AWS customers, enabling fast service provisioning and instant asset discovery, and providing threat detection, investigation, and response. It works across multiple AWS VPCs used by a single customer, leveraging a secure VPC tunnel to ensure the safe transmission of customer data between AWS VPCs. Along with continual asset discovery, the service classifies assets in order to prioritize investigation of suspicious activities according to risk levels, and that activity can be performed at up to 25 Gbps per VPC. The service also provides application-level decoding across Amazon Elastic Compute (EC2), Amazon Simple Storage Service (S3), and Amazon Elastic Load Balancing services to detect unusual behavior that could represent lateral attacker movement or other malicious activity. To provide visibility into encrypted cloud traffic, the service performs SSL/TLS decryption at scale. The same machine learning technology used in its on-premise Reveal(x) product is used to detect command and control (or exfiltration) activity. The service operates across a hybrid attack surface, providing a unified view of both cloud and on-premises network activity in a common user interface. At the same time, the service is built around widely used security management frameworks, such as CIS Top 20 Security Controls, the NIST Cybersecurity Framework, and others, which allows for common security management and effectiveness measurement across cloud and on-premise assets. It also integrates with popular security orchestration and automation platforms to automate response workflows.

EMA PERSPECTIVE

The advent of virtual network taps or traffic mirroring of customers' AWS VPC goes a long way toward improving visibility of cloud traffic, enabling much faster detection and mitigation of attacks aimed at cloud-resident applications and data. It also paves the way to more easily achieve compliance with regulatory mandates that require monitoring activity around specific datasets. However, not every AWS customer has the wherewithal to acquire, deploy, operate, and maintain their own network detection and response capability. With its new Reveal(x) Cloud NDR service, ExtraHop offloads the need to acquire and provision network traffic analysis, perform firmware upgrades, establish high-availability configurations, and monitor system health telemetry from the AWS customer's security team. That team still retains control over who can actually access and view their own VPC traffic because the service is designed to be multitenant and uses a private link to turn on VPC mirroring. Multitenancy is supported via commercially available identity management technology. By eliminating the need to deploy and maintain packet capture and monitoring infrastructure and by pricing the service correctly, ExtraHop can bring a greater level of visibility and control over AWS workload traffic to a much broader audience. If ExtraHop can find a way to federate identity across its own service operators, customers, and managed security services channel partners, it can seriously increase the number of available outlets for the service, extending the reach of it even further.

With its new Reveal(X) Cloud NDR service, ExtraHop offloads the need to acquire and provision network traffic analysis.

Because of the cost and complexity involved in performing network detection and response, that activity has been limited to larger, more sophisticated SOCs that have a deep bench of security expertise. Alternatively, they are available as part of a broader managed detection and response service, staffed by expensive professionals. Such services have been extended to customers looking to protect applications and data in both IaaS and SaaS environments. With its new Reveal(x) Cloud SaaS offering, ExtraHop occupies a middle ground that could bring NDR down to Earth for smaller security teams looking to protect hybrid cloud workloads.

ABOUT EXTRAHOP

ExtraHop provides enterprise cyber analytics that deliver security and performance from the inside out. Its approach analyzes all network interactions in real time and applies advanced machine learning to help investigate threats, ensure the delivery of critical applications, and protect cloud investments. Leading global customers, such as Credit Suisse, Hasbro, Caesars Entertainment, and Liberty Global, use its technology to gain full visibility, real-time detection, and guided investigation. For more information, go to ExtraHop's interactive online demo or connect with it on LinkedIn and Twitter.

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help EMA's clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals, and IT vendors at www.enterprisemanagement.com or blog.enterprisemanagement.com. You can also follow EMA on Twitter, Facebook, or LinkedIn.

Corporate Headquarters:
1995 North 57th Court, Suite 120
Boulder, CO 80301
Phone: +1 303.543.9500
Fax: +1 303.543.7687
www.enterprisemanagement.com

3863.071519