MITRE

# Cybersecurity Network Monitoring Challenge in Commercial Service Provider Clouds

**Sponsor:** DoD
**Dept. No.:** N454
**Contract No.:** W15P7T-13-C-A802
**Project No.:** 0721N0MZ



**Approved for Public Release; Distribution Unlimited. Public Release Case Number 21-0358**



**Annapolis Junction, MD**

**Author:**
**Kerry S Long**

**February 2021**

# Executive Summary

This paper explores the challenges in performing traditional cybersecurity network monitoring inside a commercial Cloud Service Provider (CSP). The intent of this paper is not to encourage or discourage traditional network monitoring within a commercial cloud, but rather to explore the issues that need to be considered when deciding on such a course. The paper focuses on Microsoft's Azure and Amazon's Amazon Web Services (AWS). The challenges and recommendations in this paper may also be relevant to additional Cloud Service Providers (e.g., Google, IBM, and Oracle).

**Figure 1** depicts the traditional network monitoring approach in a customer's legacy (non-CSP) environment. As customers move into modern clouds, they may seek to duplicate these monitoring capabilities within a CSP's infrastructure.

For this paper, network monitoring is defined as a capability that encompasses full network packet capture (pcap) of all network ports and protocols, network session summarization (netflow), and real-time intrusion detection systems (IDS) at consolidated network traffic aggregation ("choke point") locations within a cloud environment. Commercial CSPs do not provide network monitoring capabilities to their customers in the same manner nor to the same extent as is available in traditional network monitoring environments. CSPs do heavily monitor their own internal network infrastructures, but that information is not shared with the customer. CSPs and their third-party cloud appliance partners do offer limited options for real-time IDS and netflow collection at cloud networking choke points within Infrastructure as a Service (IaaS) at virtual network/virtual cloud boundaries. Some of these 3rd party appliances can also perform limited packet capture based-on specific SSL decrypted sessions if the firewall is configured to intercept and decrypt passing SSL sessions. CSPs do not currently support full packet capture at consolidated boundaries, however. There is essentially no traditional network monitoring capabilities for Function as a Service (FaaS), or Software as a Service (SaaS). PaaS (Platform as a Service) network monitoring in available only in very specific circumstances.

As an alternative to capturing all inbound and outbound network packets at consolidated choke points, CSPs offer packet capture at individual virtual machine (VM) endpoints, cloud native logs, and cloud integrated Endpoint Detection and Response (EDR) products. **Figure 2** depicts this alternative approach. This endpoint-based network monitoring approach has more integrity concerns compared to a centralized one, since the evidence capture /analysis processes reside in the same memory space as targeted processes. This approach also has greater storage and processing costs. EDR solutions assume a full functioning operating system and networking stack accessible to the customer. Endpoints in the cloud will increasingly represent a wide range of devices: PaaS applications, third-party appliances, Internet of Things, etc. As such, many endpoints may not be able to implement an EDR capability.

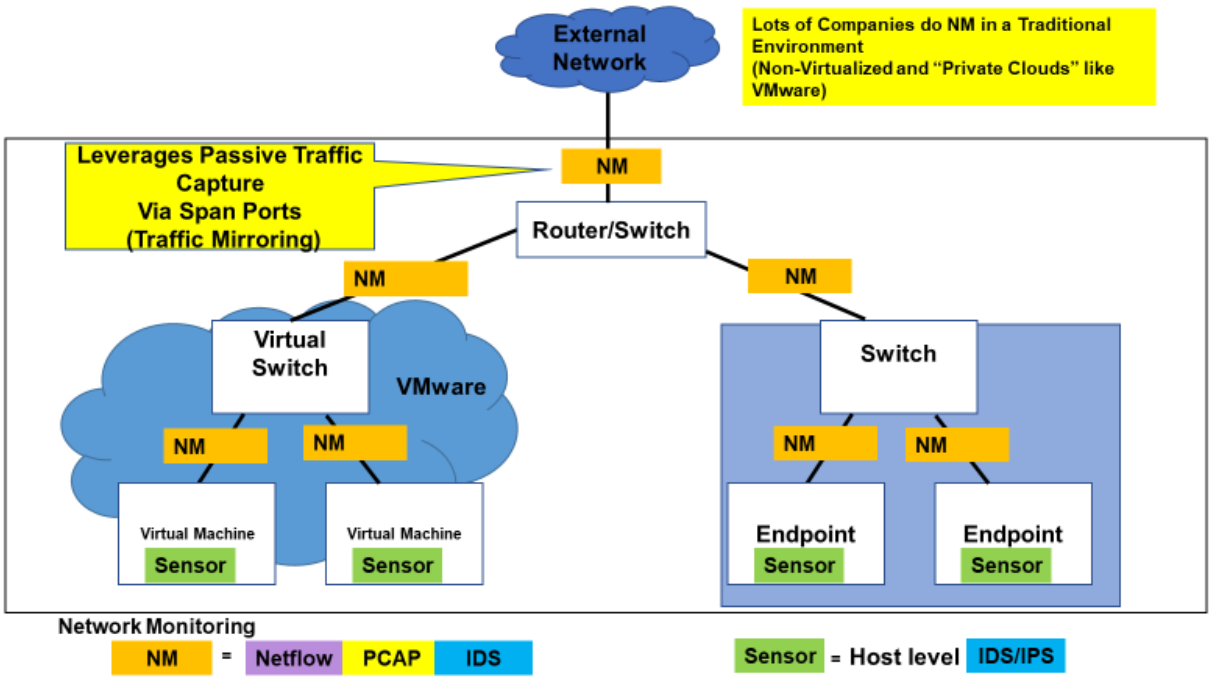


**Figure 1. Traditional Cybersecurity Network Monitoring at Key Network Points**

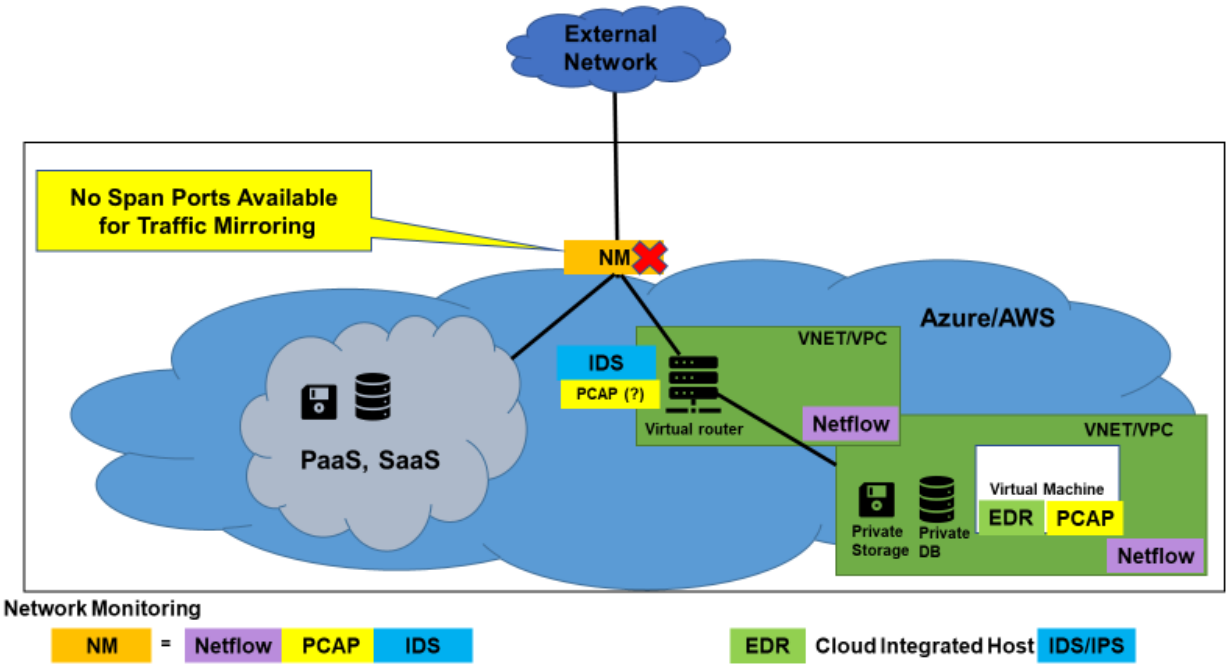


**Figure 2. CSP Advocated Network Monitoring Approaches via Endpoints and Limited Network Information**

## Summary of Analysis

If a customer desires to perform full packet capture at consolidated locations within a commercial cloud, it will require engineering effort and experimentation to build and validate customized virtual capture appliances in target environments. In the case of AWS IaaS, a capture appliance could be built leveraging AWS host packet mirroring capabilities on a virtual routing appliance such as the Palo Alto VM series. For Azure IaaS packet capture at Virtual Network boundaries, the customer would have to build a virtual routing/capture appliance with network packet capturing software running on the host operating system. Although such appliances could feasibly be built as a proof of concepts by the customer, deploying operational appliances that could confidently monitor and deliver production traffic would be risky.

For AWS and Azure FaaS/SaaS services, the options for traditional network monitoring such as netflow records, IDS, and packet capture are currently not available. Certain PaaS services may eventually be capable of limited network monitoring. The situation is likely similar in all commercial CSP offerings, whether individually or in more complex multi-cloud configurations.

## Near Term Recommendations (within the next 18 months)

- Customers should develop a high-level network monitoring strategy, logical architecture, and concept of operations that consider the challenges of CSP network monitoring described in this paper as well as the security analytics different types of network monitoring data will enable.
- Customers should leverage all native logging capabilities and services CSPs offer to protect their cloud assets.
- CSPs and their commercial partners offer options for netflow record collection, limited network packet collection and real-time signature-based IDS at strategic network consolidation points. Customers should take advantage of these offerings.
- Customers should decide whether they wish to perform packet capture in the cloud and how it should be performed. Packet capture still offers advantages within the IaaS cloud for security operators; however, its disadvantages are also more pronounced in the cloud.
- If customers do engineer their own virtual appliances for packet collection, significant testing needs to be performed under varying load conditions to ensure choke point capture solutions do not adversely impact the delivery of production traffic.
- Customers should selectively activate host-based packet captures on their most critical assets and forgo the expense and management challenges of collecting packets on every IaaS endpoint.
- A well-crafted EDR platform might significantly reduce the impact of reduced packet capture within the cloud. More study is needed to determine if a suitable EDR product exists or could be altered to collect and store sufficient security-relevant artifacts for forensic and hunting purposes. As part of this investigation, the generation of “what is suitable EDR” criteria should be developed as a living document and shared with the community.

- Customers should continually scan the CSP and third-party vendor space for new solutions and technologies that can address current network monitoring shortcomings. Commercial clouds innovate and implement new solutions at an extremely rapid rate.

# Table of Contents

# List of Figures



# List of Tables

# 1 Introduction

This paper explores the challenges for performing traditional cybersecurity network monitoring inside a commercial Cloud Service Provider (CSP) as of the first quarter, 2021. The intent of this paper is not to encourage or discourage traditional network monitoring within a commercial cloud, but rather to explore the issues that need to be considered when deciding on such a course.

Cloud technologies and capabilities change rapidly, therefore it is very possible that additional monitoring capabilities will be available within the next several months. For this paper, traditional network monitoring is defined as a capability that encompasses full network packet capture (pcap) of all network ports and protocols, network session summarization (netflow), and real-time intrusion detection systems (IDS) at consolidated network traffic aggregation ("choke point") locations within a cloud environment. The paper focuses on Microsoft's Azure and Amazon's Amazon Web Services (AWS). The challenges and recommendations in this paper may also be relevant to additional Cloud Service Providers (e.g., Google, IBM, and Oracle).

# 2 Traditional Cybersecurity Network Monitoring via Consolidated Choke Points Background

Traditional security network monitoring often occurs at locations on the network where multiple network segments come together into consolidated aggregators or "choke points." Such locations allow one monitoring device to monitor and record network traffic bound to multiple network hosts. Within commercial clouds an analog to traditional network choke points might be the boundaries of AWS Virtual Private Clouds (VPCs) or Azure Virtual Networks (VNETs).

Security network monitoring typically entails performing three actions at these consolidated network locations:

1. Recording network sessions (netflow) for quick determinations of network activity
2. Performing real-time intrusion detection (IDS) that alerts and/or acts immediately on suspicious behavior.
3. Capturing all packets (pcap) for forensics and retrospective intrusion detection analysis

**Figure 3** depicts traditional cybersecurity network monitoring. Monitoring networks at strategic consolidation choke points allows a customer to understand the nature of traffic leaving its trusted boundary without having to parse through all the network traffic that occurs within a trusted boundary between endpoints—a significant reduction in traffic. Choke point monitoring also ensures the integrity of the monitoring process by isolating the monitor from the likely exploitation target—endpoint machines. Capturing network packets in capture files (pcap) provides a universally accepted, data-rich forensic artifact. Most existing Cybersecurity Operation Center functions, training, and tooling depend on these pcap files being available.

In the past, organizations enabled choke point monitoring by configuring physical/virtual appliances in the network path to mirror all inbound and outbound network traffic they were

receiving to a dedicated interface called a mirror port or, in Cisco parlance, a Switched Port Analyzer (SPAN) port. Organizations would attach analysis machines to these mirrored ports and perform all aspects of network monitoring required.

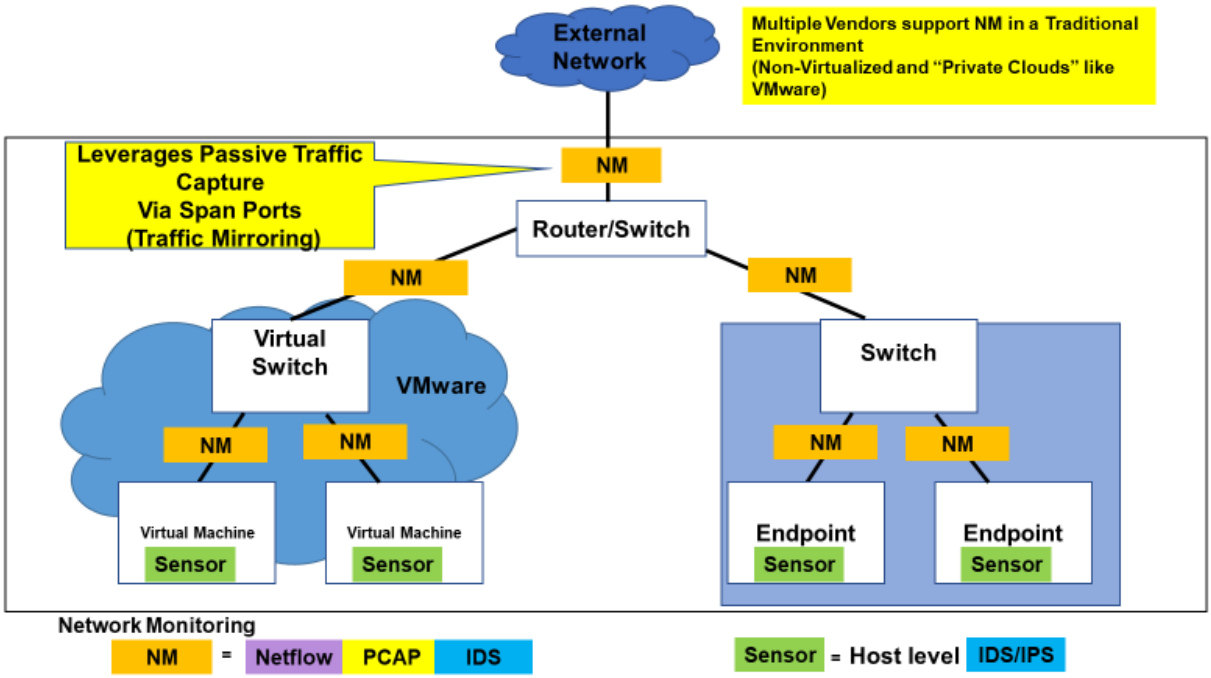


**Figure 3. Traditional Monitoring at Key Consolidated Network Choke Points**

# 3 Cybersecurity Network Monitoring Challenges in a Cloud

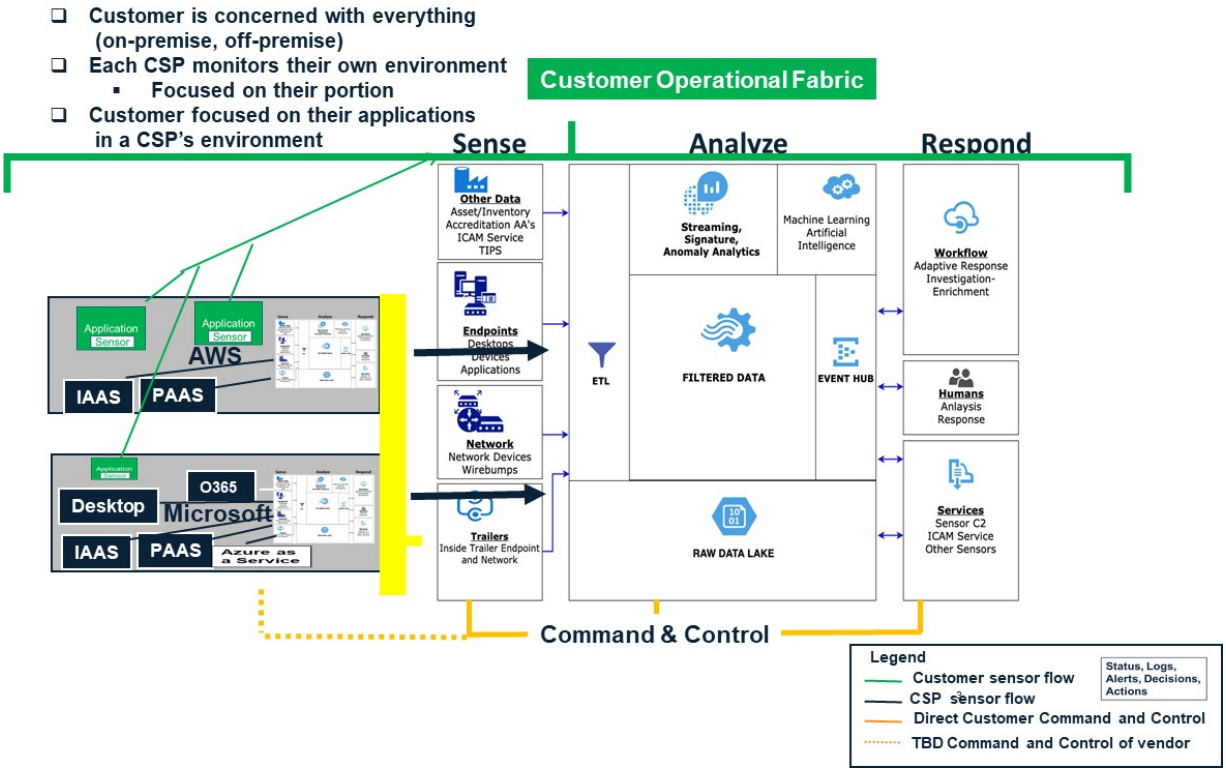


Figure 4 depicts a notional customer processing environment, which includes multi-vendor, multi-cloud environments all requiring instrumentation to sense, analyze, and respond to network, host, and cloud events. This environment is significantly different from previous customer processing environments. In this new processing environment, customers will have to cede significant operational control to CSP's and third-party vendors for many operational aspects including security aspects.

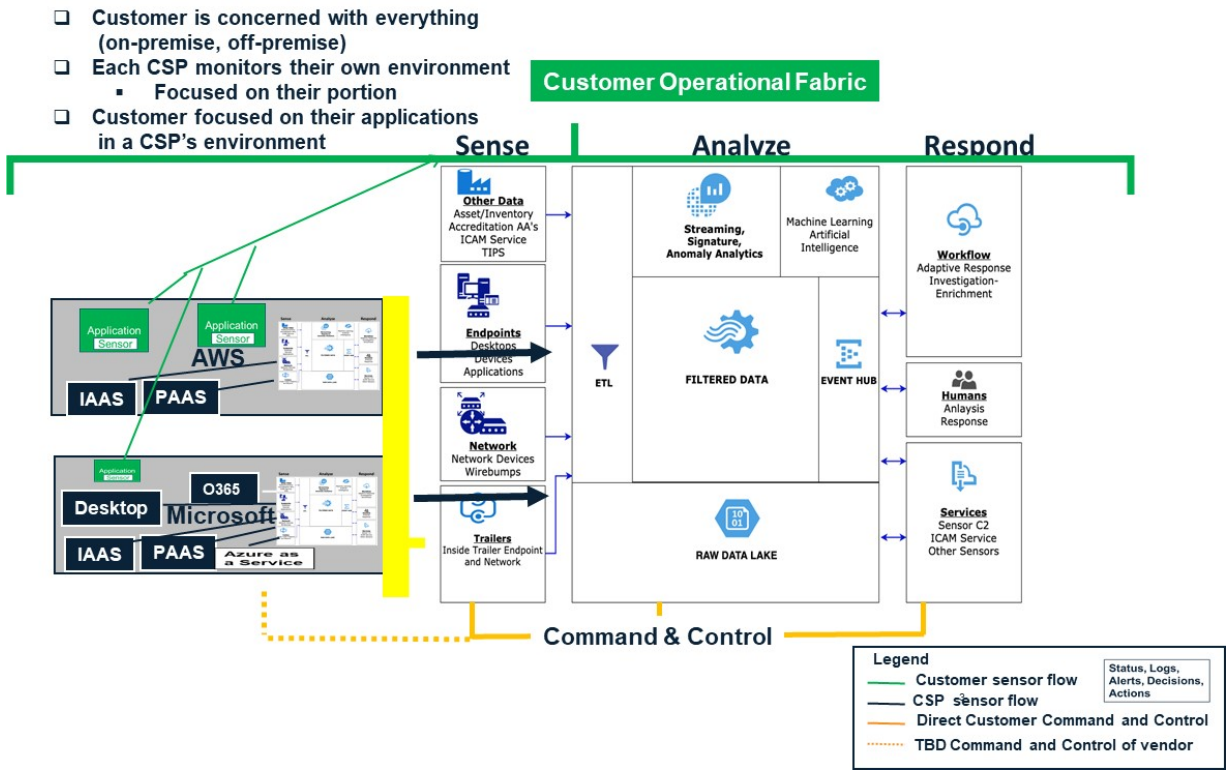


**Figure 4. Strategic End-to-End Cybersecurity Sense, Analyze, and Respond Concept Includes Use of Commercial Cloud Service Providers**

Commercial clouds offer numerous services that all leverage an underlying software defined networking (SDN) construct. This SDN is largely invisible to the cloud customer and provides only limited opportunities for them to influence and monitor its operations. CSPs do heavily control and monitor their own internal network infrastructures, but this capability is not shared with the customer. For example, a customer has no ability to configure or even observe the virtual and physical switches and routers responsible for delivering its traffic. Commercial clouds do not offer traffic mirroring/SPAN port capabilities on their switches and routers to customers. **Figure 5** depicts the CSP advocated network monitoring approach based on endpoint detection and select network logging. Both Azure and AWS offer native netflow session recording capabilities to inventory traffic entering and leaving Azure VNETs and AWS VPCs. However, netflow records do not offer the forensic fidelity of packet capture, for example instance application layer data, required for network forensics and hunting activities.

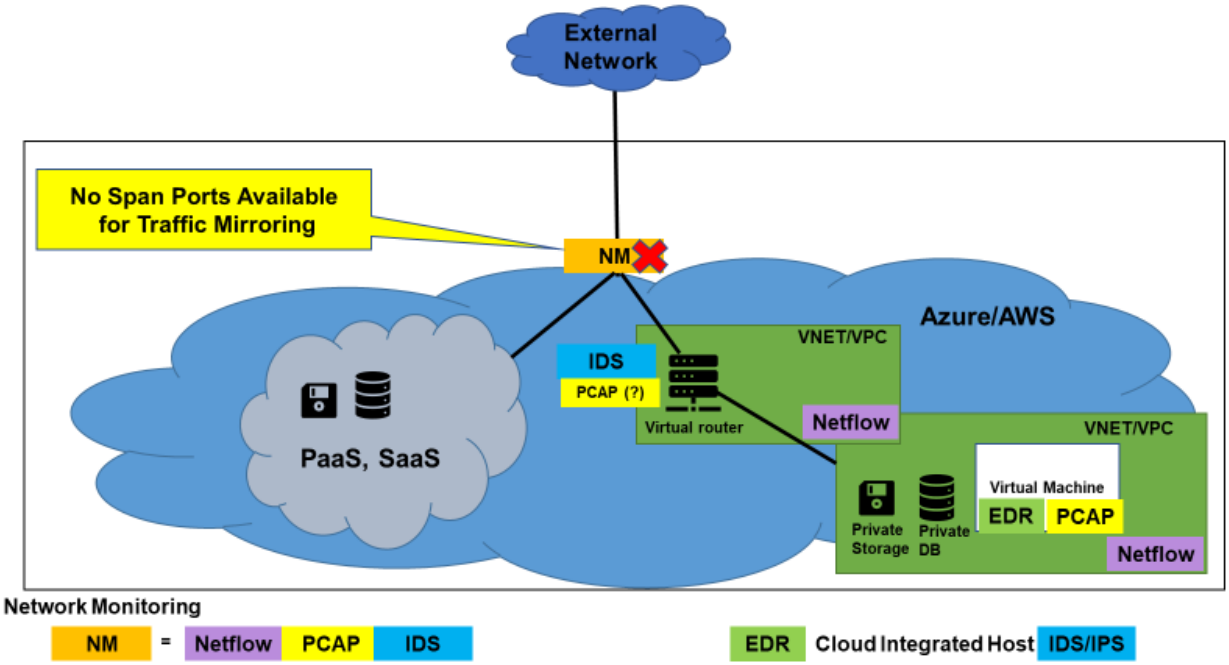


**Figure 5. CSP Advocated Network Monitoring Approaches via Endpoint and Select Network Information**

CSP Infrastructure as a Service (IaaS) offerings and certain private Platform as a Service (PaaS) offerings do permit the configuring of customized routes in VNET/VPCs, called user-defined routes, which can force traffic through virtual appliances usually located in their own dedicated VNET/VPC or subnet. **Figure 6** depicts an Azure approach allowing customers to leverage third-party firewall and routing appliances. In Azure this only applies to outgoing customer traffic from a VNET. Traffic inbound to Azure services from either a customer's home or an on-premise network is not affected by user-defined routes and cannot be directed through a customer's virtual network appliance. AWS offers a similar capability but additionally allows customers to configure an inbound route for traffic originating from a virtual private gateway/internet gateway to force incoming traffic bound for a VPC through a virtual appliance.[1]

With user-defined routes, it is theoretically possible to insert a network monitoring appliance into the routing path to perform choke point network monitoring. Unfortunately, because these monitoring appliances are now in the routing path, they must perform production routing functions and meet performance and uptime guarantees. Firewall and routing appliances are designed to assume production routing responsibilities - network monitoring appliances are not. None of the CSP or third-party firewalls or routing appliances currently available in commercial clouds offer the ability to perform the full packet capture functions of traditional network monitoring. Network monitoring appliances that could provide full packet capture capabilities do

[1] https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Route_Tables.html. Accessed December 11, 2020.

not perform routing. Unfortunately, there is no known hybrid virtual appliance on the market that can perform both routing and full packet capture effectively.

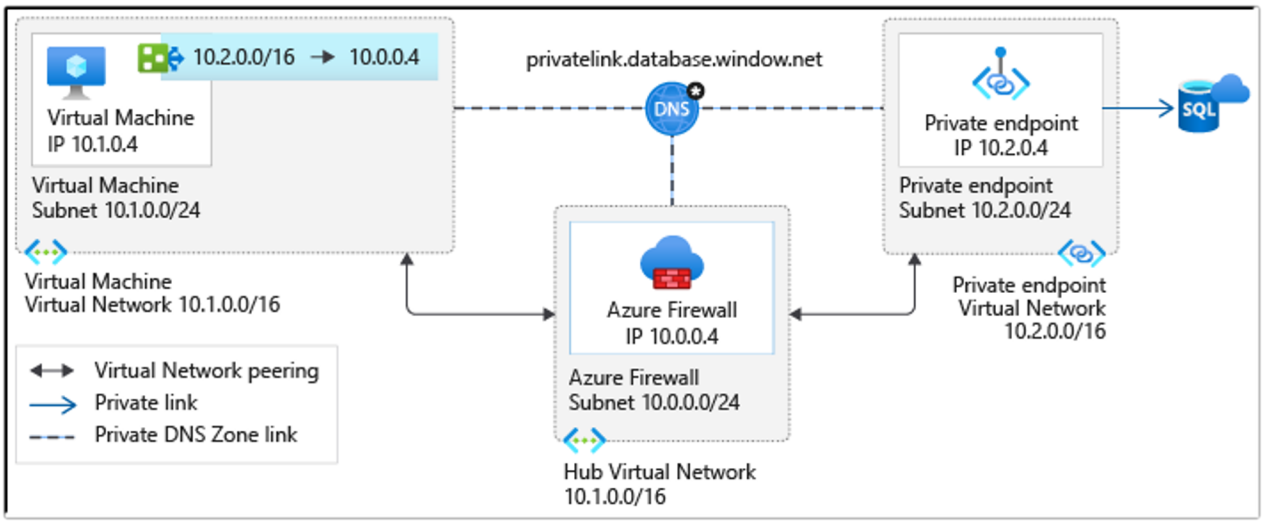


**Figure 6. Azure Firewall Appliance Inserted into Routing Path for Security (Not Monitoring) - Courtesy of Microsoft Corporation[2]**

In summary, performing traditional network monitoring in the cloud is challenging due to lack of visibility/control of the underlying cloud infrastructure and due to a lack of existing CSP or third-party products that adequately address this new reality.

# 4 Analysis

This section contains the following topics:

- CSP network monitoring options and alternatives
- Potential solutions for packet capture at choke points within a CSP
- PaaS network monitoring options

## 4.1 CSP Network Monitoring Options and Alternatives

Cloud Service Providers offer multiple logging options in varying formats that contain security-relevant information about cloud use for their customers. These logs often focus more on user interactions with the cloud application programming interface (API) and endpoint performance statistics rather than on collecting security-relevant forensic data about endpoints or their network interactions. As such, these CSP logs are more of a complement to network traffic monitoring than they are a substitute.

[2] https://docs.microsoft.com/en-us/azure/private-link/inspect-traffic-with-azure-firewall. Accessed December 7, 2020.

CSPs are now offering security monitoring services for an extra fee that could in theory replace traditional network monitoring functions by a customer. AWS Guard Duty, for example, uses both cloud API interactions and virtual network access records to detect unusual and hostile behavior. Unfortunately, the detection methods they use are often not shared with the customer and these services cannot really be customized to meet specific customer needs. As such, these services enhance rather than replace the functionality of network monitoring.

A possible substitute for network monitoring in the cloud might be a well-coordinated endpoint forensic collection operation using host-based agents. Endpoint forensic artifacts, such as memory maps and system logs, could prove superior to network monitoring in terms of detection and hunting value in the longer term, especially as network traffic encryption becomes ubiquitous.

However, in practice collecting endpoint forensic artifacts has some major drawbacks:

- Currently there is no industry-wide consensus on what forensic artifacts should be collected from endpoints and in what format they should be captured. Until this changes, it is difficult to integrate tools and operations around them. Endpoint artifacts can differ widely for Linux, Mac, and Windows endpoints and between commercial products within an operating system.
- Forensic artifacts on a host can be more easily compromised than on an independent, consolidated observation point.
- Vendor Endpoint Detection and Response (EDR) solutions are often the vehicle used to collect endpoint artifacts in the cloud. However, these products often do not collect and forward very much forensic data; instead, they forward alerts and synopses. This is not sufficient for long-term forensics, independent analytic development, or hunting operations. Newer EDR products such as Windows Defender Endpoint have partially addressed this concern. Defender collects significant forensic data and stores it centrally, but only if it is associated with a Defender triggered alert.[3]

Despite the promise of native cloud logs and host-based forensic collection, customers in commercial clouds may still wish to perform traditional network security monitoring at strategic choke points. Perhaps in a tacit nod to the importance of this, AWS and Azure now provide two of the three major components of traditional network monitoring as options: network session summarizations and real-time IDS. Full packet capture is not currently available at strategic choke points within CSPs; however, some limited packet capture capabilities are.

Azure allows customers to collect network traffic summaries (netflows) at virtual subnet boundaries. AWS offers consolidated network session records from each endpoint within a VPC. Azure and AWS, through third-party firewall products like Palo Alto and Cisco, provides basic real-time Snort IDS capabilities for VNET traffic routed through it. AWS offers a similar capability through its newly announced Firewall service.[4] Third party firewall appliances like the

[3] https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/data-storage-privacy. Accessed December 8, 2020.

[4] https://aws.amazon.com/network-firewall/features/. Accessed November 30, 2020.

Palo Alto can perform limited packet capture through a capability called SSL break and inspect. With break and inspect, the firewall serves as a man in the middle to encrypted SSL sessions entering and leaving one or more VNET/VPCs. The Palo Alto firewall has the capability to decrypt these SSL sessions and forward the network packets to an analysis host for analysis and storage. Palo Alto recommends customers use this capability selectively to reduce processing overhead. This packet capture capability only pertains to the SSL protocol. Unfortunately, there is still no supported solution from either the CSPs or third parties to address full packet capture at virtual network boundaries (see **Table 1**).

**Table 1. Network Monitoring (Full PCAP, Netflow, Real-Time IDS) Functions Available via Azure and AWS (**Red indicates capability not currently available**)**

| | Azure | | | AWS | | |
|---|---|---|---|---|---|---|
| **Network Monitoring Capabilities** | **IAAS** | **Private PAAS** | **Public PaaS/SAAS** | **IAAS/Private PaaS** | **Private PAAS** | **Public PaaS/SAAS** |
| Full Packet Capture (PCAP) | VM endpoints<br>Agent-based | | | VM endpoints<br>Hypervisor-based | | |
| Network Flow | Provided for Subnets | Leveraging Azure private endpoints | | Provided by VPC flow logs | Provided by VPC flow logs | |
| Real-Time IDS | Third-party provided appliances (Palo Alto/Cisco) | Leveraging private endpoints, user-defined routes, third-party appliances | | Provided by AWS Firewall & third-party appliances | Leveraging user-defined routes & third-party appliances | |

Instead of full packet capture at VPCs/VNETs, CSPs offer the capability to collect traffic at each IaaS endpoint individually. Azure provides an operating system (OS) agent that monitors traffic entering the OS networking stack and forwards packets to an Azure Storage Container. AWS has created an application specific integrated circuit (ASIC)-based capture capability called "Traffic Mirroring" that copies all traffic from a virtual machine's (VM's) virtual network interface card (NIC) and forwards it to another AWS VM for analysis. AWS has inadvertently introduced some confusion into the marketplace recently by advertising a "new" capability titled "VPC Traffic Mirroring." Despite what the name seems to connote, this offering is not a consolidated packet capture capability for traffic entering and leaving a VPC. Rather it is just a convenient frontend for turning on and managing packet collection on AWS virtual machines within a VPC.

The task of collecting packets at numerous endpoints within every single VNET/VPC can get complex and expensive, as storage and processing costs increase linearly with the amount of packets captured. To address complexity issues, CSPs have partnered with companies like

Gigamon and Ixia to provide packet broker platforms that will collect and organize packet traffic from multiple endpoints and distribute them to multiple IDS tools.[5]

If a customer wishes to capture network traffic at strategic choke points, there are no native cloud services or virtual cloud appliances that provide network-based full packet capture. Some third-party virtual firewall providers like Cisco and Palo Alto are now providing limited packet capture capabilities for troubleshooting and secure socket layer (SSL) decryption scenarios in very specific, narrowly focused use cases. This limited capture capability is not satisfactory for network monitoring.

## 4.2 Potential Solutions for Packet Capture at Choke Points Within a CSP

If capturing packets at strategic network boundaries within a cloud is desired, it will require the customer to create and support its own solution. The most likely possibility is to leverage user-defined routing rules provided by CSPs and customer-engineered virtual appliances. VPCs and VNETS can be cleverly arranged with user-defined routes to ensure that all inbound and outbound traffic passes through a virtual appliance. A virtual appliance can be created that both captures and routes all network traffic it receives. This might be possible in Azure, by constructing a simple Linux router with a network sniffing package installed and replacing the firewall appliance pictured in **Figure 6** with it. In AWS, a virtual routing appliance like Palo Alto's VM-Series could in theory be altered by enabling AWS native traffic mirroring on its underlying VM. Both AWS and Azure potential solutions are a significant departure from what CSPs currently support or recommend. The customer will be responsible for significant development and testing of these solutions to ensure they can endure expected and unexpected traffic conditions. It would be desirable therefore to have a vendor or CSP-tested and supported capability. Unfortunately, no such capability is currently known to exist.

**Table 2** summarizes the pros and cons of adopting one or more options with regard to cloud packet collection.

**Table 2. Full Network Packet Capture (PCAP) Options in the Cloud**

| Option | Advantages | Disadvantages |
|---|---|---|
| **Endpoint-Based PCAP**<br>• Collect packets at endpoints only | • Fully supported by CSP and vendors for IaaS<br>• Can see east-west traffic within VNETs/VPCs<br>• Can leverage existing customer IDS tools and artifact retention architecture | • More packets to process and store<br>• Harder to manage multiple collection sensors<br>• No possibility to monitor private PaaS traffic<br>• Collection not isolated from compromised assets in the case of Azure; AWS uses hypervisor to isolate |

[5] https://blog.gigamon.com/2018/09/24/why-microsofts-new-vtap-service-works-even-better-with-gigasecure-for-azure/. Accessed December 10, 2020.

| Option | Advantages | Disadvantages |
|---|---|---|
| | | • Requires expensive third-party packet brokers<br>• Endpoint collection agent could impact endpoint operations in Azure |
| **Strategic PCAP**<br>• Adopt strategic consolidated packet capture at network choke points<br>• Use endpoint packet collection sparingly | • Can leverage existing customer IDS tools and artifact retention architecture<br>• Integrates most easily with current security operation center (SOC) operations<br>• Less costly option to capture PCAP<br>• Collection independent of possible compromised hosts<br>• Possibility of monitoring network traffic bound to certain private PaaS services | • No current vendor or cloud provider supports options for choke point collection<br>• Will require custom development, engineering, and support<br>• Misses east-west traffic |
| **Alternatives to PCAP**<br>• Forgo packet capture altogether and rely on native cloud logs<br>• Rely on netflow records collected at VNET/VPC boundaries, and alerts from EDR agents | • No PCAP greatly reduces cost of information storage and processing<br>• Cloud logs and partner EDR solutions are well integrated into cloud portal and other cloud products | • Reduced forensics capabilities due to lack of universally accepted data artifact<br>• Reduced hunting capabilities using traditional methods<br>• Tied to a commercial EDR product for analytics development and hunting |

## 4.3 PaaS Network Monitoring Options

The preceding discussion focused solely on monitoring network traffic destined to IaaS assets within the cloud. PaaS network monitoring is even less supported in commercial clouds such as AWS and Azure, and Software as a Service (SaaS) services are completely obscured from the customer. Theoretically certain PaaS services (private PaaS) that can be isolated in private customer subnets could be compelled to route traffic through network monitoring virtual appliances providing the same network monitoring options available for IaaS assets. In general, CSPs recommend using native logs to monitor access to PaaS services. The context provided by these logs is superior in many ways to what might be gained through network monitoring, as it is enriched from multiple cloud provider data sources. Still there may be cases where customers wish to analyze "ground truth" to ascertain the nature of access to their applications hosted on PaaS assets or wish to have a unified security picture for all their web and database services, whether they are running on premises, on IaaS servers, or within multiple cloud providers' PaaS. Currently only network monitoring can offer this unified capability.

## 4.4 Summary of Analysis

A summary of the analysis follows:

- The results of analysis indicate there are some limited options to perform network-based monitoring within commercial clouds.
- Real-time intrusion detection at consolidated choke point locations can be achieved with third-party virtual appliances.
- CSPs offer the capability to collect netflow records for traffic passing through VPC/VNET boundaries.
- CSPs do not support network packet capture at VPC/VNET boundaries.
- CSP-provided packet capturing options rely on collection at individual workload endpoints.
- Analysis and/or collection at endpoints is more vulnerable to tampering or disruption than consolidated collection and is more expensive to obtain.
- Customers could engineer and prototype a consolidated network capture appliance using existing components found within CSPs. It is not clear how well these prototypes will perform in production environments.

# 5 Recommendations to Move Forward

This section provides near-term (within the next 18 months) and long-term recommendations if a customer decides to adopt consolidated network security monitoring in a commercial cloud environment. These recommendations seek to emulate a capability customer already possess and depend on within their traditional enterprise networks.

## 5.1 Near-Term Recommendations

The near-term recommendations focus on current available capabilities a customer can leverage immediately from CSPs and their third-party partners.

- Customers should develop a high-level network monitoring strategy, logical architecture, and concept of operations that consider the challenges of CSP network monitoring described in this paper as well as the security analytics different types of network monitoring data will enable.
- Customers should leverage all native logging capabilities and services CSPs offer to protect their cloud assets.
- CSPs and their commercial partners offer options for netflow record collection, limited network packet collection and real-time signature-based IDS at strategic network consolidation points. Customers should take advantage of these offerings.

- Customers should decide whether to perform full network packet capture and how it should be performed. Packet capture still offers compelling advantages within the IaaS cloud for security operators; however, its disadvantages are also more pronounced in the cloud.
- Customers should selectively activate host-based packet captures on their most critical assets and forgo the expense and management headache of collecting packets on every IaaS endpoint.
- A well-crafted EDR platform might significantly reduce the impact of reduced packet capture within the cloud. More study is needed to determine if a suitable EDR product exists or could be altered to collect and store sufficient security-relevant artifacts for forensic and hunting purposes. As part of this investigation, the generation of "what is suitable EDR" criteria should be developed as a living document and shared with the community.
- Customers should continually scan the CSP and third-party vendor space for new solutions and technologies that can address current network monitoring shortcomings. Commercial clouds innovate and implement new solutions at an extremely rapid rate.
- If customers do engineer their own virtual appliances for packet collection, significant testing needs to be performed under varying load conditions to ensure choke point capture solutions do not adversely impact the delivery of production traffic.

## 5.2 Long-Term Recommendations

The longer-term recommendations focus on technical concepts and capabilities that need investigation, development, and productization by CSPs and their third-party partners in consultation with customers, MITRE, and academia. By their nature, the longer-term recommendations may or may not develop quickly enough to satisfy near-term customer challenges.

- The customer community should develop guidance on the acceptable mixture of EDR capabilities and strategic network monitoring capabilities required to secure their commercial cloud environments. This guidance should be informed by, but not constrained by, what CSPs and their third-party partners currently offer.
- The customer community should directly engage with CSPs to discuss possible ways forward in creating a CSP supported and tested solution for strategic network-based packet capture.
- The customer community should directly engage with defensive cyber and network monitoring vendors to encourage evolution of their capabilities to support strategic network monitoring capabilities in commercial clouds, such as full packet capture, IDS, and netflow record creation.

- The CSPs and Defensive Cyber and Network monitoring vendors should ensure data consistency and functional interoperability to support customers that leverage multi-vendor, multi-cloud environments.