corelight

THE CASE FOR NETWORK DETECTION & RESPONSE IN THE CLOUD

5 considerations for effective multi-cloud threat detection

THE CASE FOR
NETWORK DETECTION & RESPONSE IN THE CLOUD

Multi-cloud environments present significant security challenges. Expanding attack surfaces, constantly evolving cyber threats, and ephemeral network topology demand:

- A unified security approach with advanced analytical capabilities to manage the complexities of multi-cloud security.
- Consistent triage workflow across different cloud providers for timely, effective incident response.
- Data protection strategies include encryption and access control across your entire multi-cloud infrastructure.

With Network Detection and Response (NDR), you can link network telemetry with host data enrichment for a complete view and gain the ability to identify all services and activities in your multi-cloud environments.

CLOUD SECURITY **CHALLENGES**

Shallow threat detection

Detections using flow log analysis are limited, e.g. flow logs can only detect C2 communication with known command and control servers.

Attackers evade EDR

APTs find ways to bypass EDR and CNAPP solutions by using LOTL techniques—such as PowerShell scripts or WMI tools—that mimic legitimate system activities.

Inconsistent telemetry

Cloud logs are not exhaustive, often have inconsistent schemas, and may not be designed for security use cases, which increases downstream analytics and automation costs.

More tools, more required learning

Multi-cloud deployments mean more SOC training on a sprawling toolset (e.g., AWS Guard Duty, GCP Security Command Center), which negatively impacts incident response and automation.

CLOUD SECURITY **LANDSCAPE**

As enterprises adopt cloud services and utilize hybrid cloud/on-premises environments, adversaries continually expand their targeting strategies. Open NDR gives you a holistic view that spans across hybrid and multi-cloud environments for consistent and uniform visibility.

47% of executives worry about cyber threats on and through the cloud. [1]

CLOUD BREACHES

44% of organizations have experienced a cloud data breach with 14% having had one in the past year.[2]

CLOUD WORKLOAD INCREASE

52% of North American organizations expect at least 41% of their workloads to operate on the cloud in the next two years.[3]

+41%

CLOUD INTRUSIONS

Cloud environment intrusions increased 75% YoY. [4]

CLOUD VISIBILITY

Businesses need full cloud visibility, including into applications and APIs, to eliminate misconfigurations, vulnerabilities and other security threats.[5]

CLOUD INFRASTRUCTURE PROVIDERS

98% of enterprises surveyed are using or plan to use at least two cloud infrastructure providers, and 31% are using at least four providers.[6]

SECURITY PROGRAM RECOMMENDATIONS

Organizations should focus on building a comprehensive security program that spans the entire enterprise, from cloud and on-premises, to IT/OT, and all assets.[4]

1 PwC 2024 Global Digital Trust Insights
2 Thales 2024 Cloud Security Study
3 CrowdStrike Falcon Cloud Security on AWSeBook 2023
4 Mandiant M-TRENDS 2024 Special Report
5 CrowdStrike 2024 Global Threat Report
6 451 Research Report

5 CONSIDERATIONS FOR THREAT DETECTION IN **MULTI-CLOUD ENVIRONMENTS**

1

The need for unified security architecture

Across the cloud providers, AWS VPC Flow Logs must be enabled for each of the VPCs, GCP Flow Logs must be enabled for each VPC subnet, whereas Azure NSG Flow Logs must be enabled for every network security group.

A fragmented approach to security coupled with a variation in formats can lead to blind spots. A holistic view that spans across hybrid and multi-cloud environments is needed for consistent and uniform visibility.

2

Cloud-native detection tool limitations

While tools offered by AWS, GCP, and Azure clouds incorporate threat intelligence and can analyze vast amounts of data, they often rely on VPC flow logs that may have inherent limitations—flow logs can only detect command and control communication with a known C2 server. It is crucial to understand where these tools excel and where additional measures may be required to cover the gaps.

3

Detections tailored to your multi-cloud footprint

Effective threat detection is not a one-size-fits-all solution; it requires careful tuning to the specific services and environments in use. This means setting up detections for cloud-specific attacks such as service enumeration, C2 traffic, and potential data exfiltration attempts.

4 Integrated threat intelligence

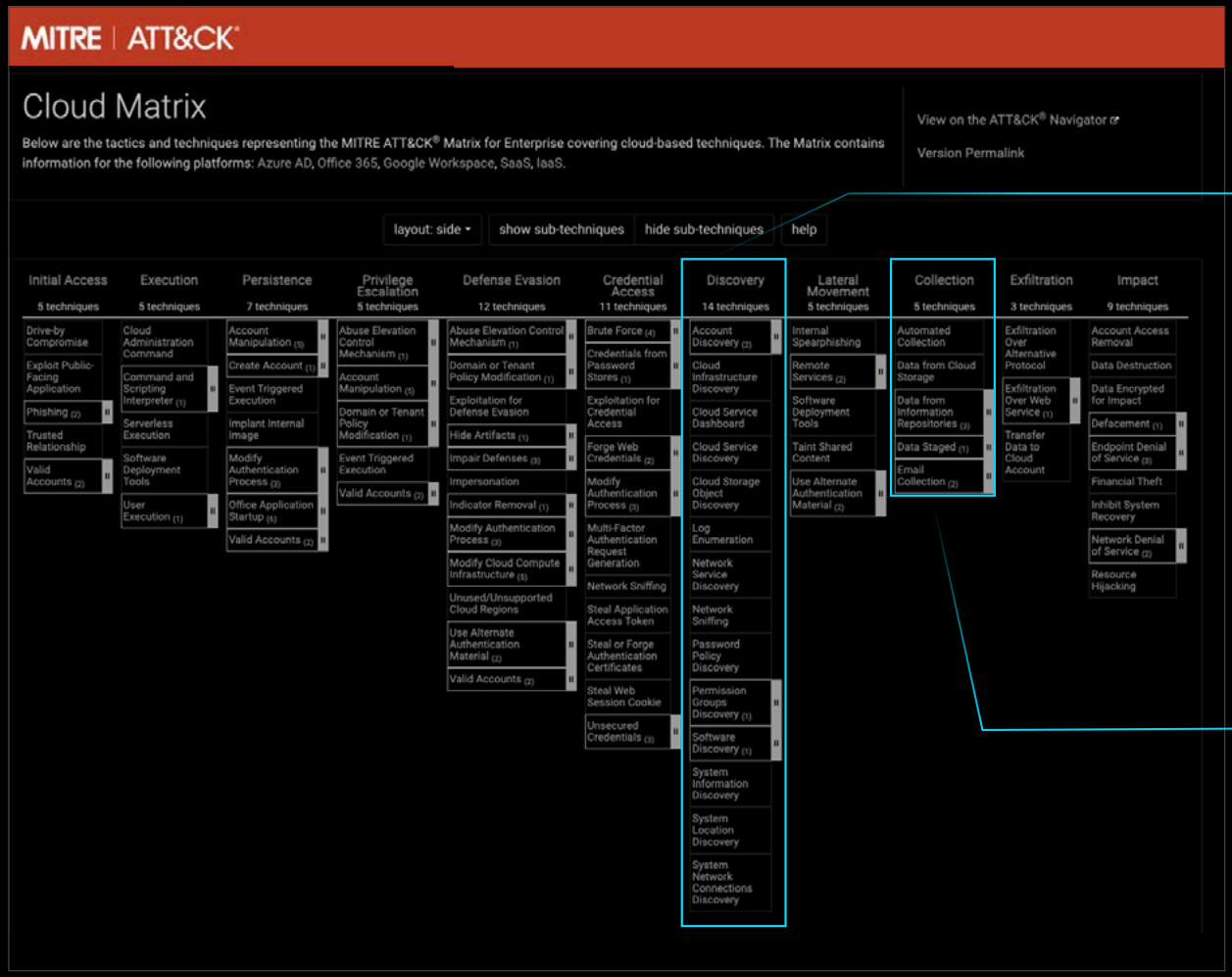
In the cloud, adversaries often employ different tactics than they do in traditional IT environments. Rather than deploying malware, they may exploit IAM credentials to siphon data stealthily. Access to comprehensive threat intelligence feeds and analysis enhances the ability to anticipate and counter these tactics.

5 Detection team training

Tools across various cloud service providers like GuardDuty in AWS, Security Command Center in GCP and Defender in Azure, necessitate specialized knowledge and skills. Ensuring team profiency with these tools and understanding the nuances of each cloud environment is crucial. Consistent telemetry and detection methodologies across multi-cloud platforms alleviate the need for extensive training and enable a more streamlined approach.

MITRE ATT&CK® TTPs

Cloud- and identity-focused activities categorized by the MITRE ATT&CK® enterprise tactics.

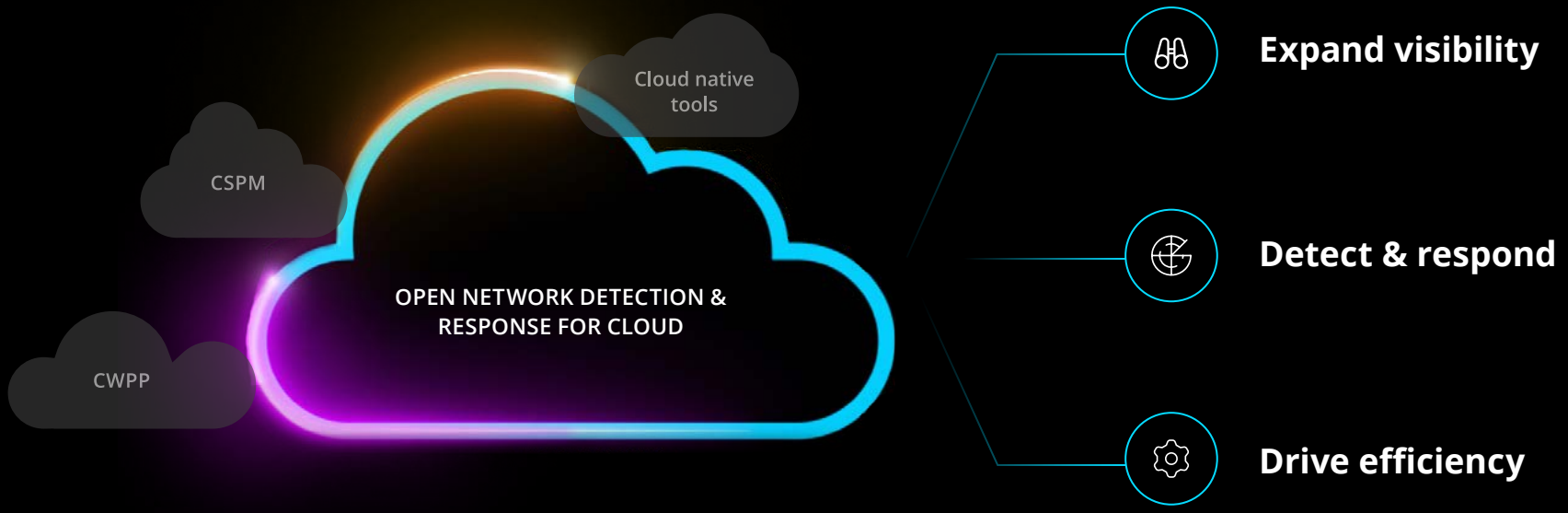


Correctly identify host using service enumeration for reconnaissance purpose, which is often an indicator of a compromised host.

- Network service discovery
- T1046, used widely
- Cloud service discovery
- T1580, used in Pacu and Scattered spider
- System network connections discovery
- T1049 used widely

Detection of network-level collection techniques is immutable and a powerful way to **stop data exfiltration before it occurs.**

- Data collection
- T1530, many examples including scattered spider
- Data staging
- T1074, many examples including Shark, QUIETCANARY
- Data exfiltration techniques



CLOSE CLOUD VISIBILITY GAPS **WITH NDR**

In multi-cloud environments, achieving comprehensive visibility and rapid threat detection is essential. NDR is a key solution for effective threat detection in these environments.

NDR enriches network telemetry with host data context to give you a complete view and the ability to identify all services and activities within your cloud environments.

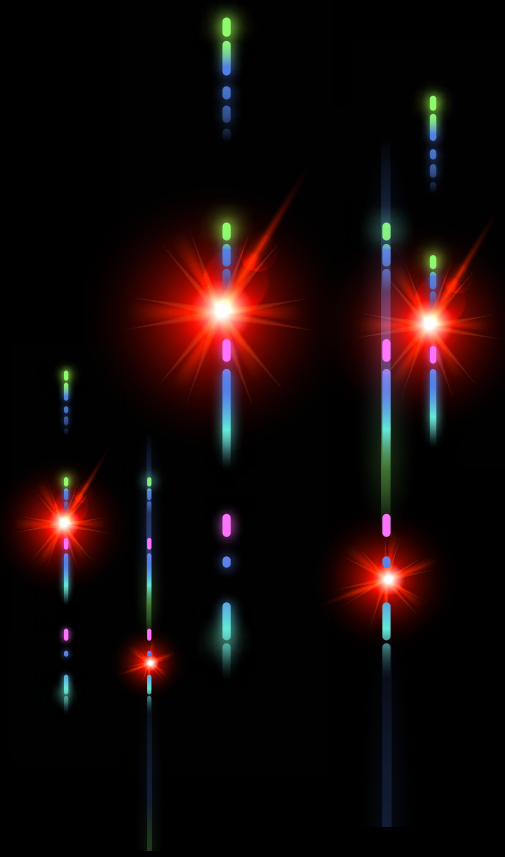
MULTI-CLOUD STRATEGY **WITH NDR**

One of the significant advantages of NDR in a multi-cloud strategy is its capacity to detect and disrupt cloud-specific threats. Such threats often involve sophisticated tactics like the use of command and control (C2) channels, which can be tunneled through various protocols or to unknown servers. NDR equips security teams with the necessary intelligence to identify these unconventional communication patterns, allowing for timely intervention.

Behavioral anomalies within a cloud environment can be subtle and easily overlooked. NDR can detect when a host is reaching out to multiple services to determine which ones it can access—a potential indicator of compromise. SOCs can then investigate these early warning signs and gain the ability to contain threats before they escalate.

NDR can also drive more value from existing security tools. It helps fill coverage gaps and transforms cloud traffic into detailed logs, files, and insights that enable faster triage. By consolidating datasets and tools such as network security monitoring (NSM), intrusion detection systems (IDS), and packet capture (PCAP), NDR streamlines analyst workflows and reduces security tool sprawl.

NDR shortens the learning curve—it does not require extensive upskilling or retraining. Using NDR, SOCs can extend their capabilities to the cloud with familiar resources and workflows to enable seamless transitions and integrations into any existing security posture.



LEARN ABOUT THE OPEN NDR PLATFORM ›

TRUSTED BY

CROWDSTRIKE Mandiant Microsoft splunk>

"Corelight helps you to find bad things happening like sneaky viruses or hackers trying to get in."

—G2.com validated review

Gartner Peer Insights™

corelight

info@corelight.com | 888-547-9497