SOLUTION BRIEF

Cloud Threat Investigation 101: Hunting with MITRE ATT&CK

Enterprise security teams have extensive experience investigating threats to their endpoints and networks—but cloud-native threats are a new paradigm.

In many cases, the cloud environment is externally managed by the cloud service provider, as in the case of Microsoft 365. There are no agents, no network security infrastructure, or any other ways of detecting events that the security team owns and operates. Cloud-native attacks are typically not even malware-based. Instead, they rely on compromised accounts and features of the cloud services themselves to land and expand an attack.

Connect With Us

That doesn't mean the consequences are not real. Data exfiltration is still the primary goal of cloud-native attacks. So how are security teams dealing with these today?

For many it is a manual effort to sort through incidents provided by their cloud access security broker (CASB). Most feed those events to a SIEM for further analysis, but the numbers can be in the millions, making cloud threat investigation a labor-intensive security practice.

There has not been an efficient way to gain visibility into cloud attacks and establish a repeatable risk mitigation process.

Parsing Through the Haystack

A CASB, when implemented properly, provides a multimode connection to cloud services that covers all entry and exit points for a cloud-native threat.

- **Application programming interface (API):** Connection to services like Amazon Web Services (AWS) or Microsoft 365 via API allows for full visibility into data, activity, and configuration of the cloud environment.
- **Forward proxy:** Connection via forward proxy, such as a next-generation secure web gateway provides visibility and control over services that do not publish a public API for deep inspection. Instead, inspection is provided inline by the proxy.
- **Reverse proxy:** Connection via reverse proxy gives deep contextual information about the user accessing the cloud service, coupled with identity and access management (IAM) tools to detect unmanaged devices and anomalous access events.

Together, this multimode approach feeds millions of events into a machine learning-based analytics function, which, in turn, generates thousands of anomalies and often just dozens of actual threats. This function, known as user and entity behavior analytics (UEBA), removes the tedious work of event correlation from security analysts so they can focus on what's important to their investigation: anomalous events and actual attack behavior.

Translation to a Common Language with MITRE ATT&CK

This is only part of the process. Every security operations center (SOC) investigates threats from multiple environments. The only way to understand the full scope of an attack is to speak the same language across each environment—and that language is MITRE ATT&CK®.

By mapping cloud anomalies and threats to the MITRE ATT&CK Matrix for Cloud, McAfee® MVISION Cloud: CASB brings cloud threat investigation into the security operations center (SOC) with unprecedented effectiveness, opening the door to a new paradigm of full-scope threat defense, from endpoints, to networks, and now in the cloud.

Make Cloud Investigation Part of Your Workflow

To effectively mitigate risk in cloud environments, security teams need a tool set that not only speaks the MITRE language, but fits into the workflow of multiple teams seamlessly.

For SOC teams, a new, rich set of cloud anomaly and threat events, along with incidents from DLP, Configuration Audit, and Vulnerability Scanning, are now mapped and tagged with the familiar MITRE ATT&CK tactics and techniques they use today in their investigation process. They can feed these directly into their SIEM or SOAR platform in multiple ways, including APIs, providing a constant feed of pre-filtered incidents.

SOC analysts can also view the MITRE ATT&CK framework directly in MVISION Cloud for quick analysis of threats and their impact on specific users, data, and cloud services. From MVISION Cloud, analysts have multiple views.

- **Retrospective**, showing all the cloud attacks that have fully executed in their environment

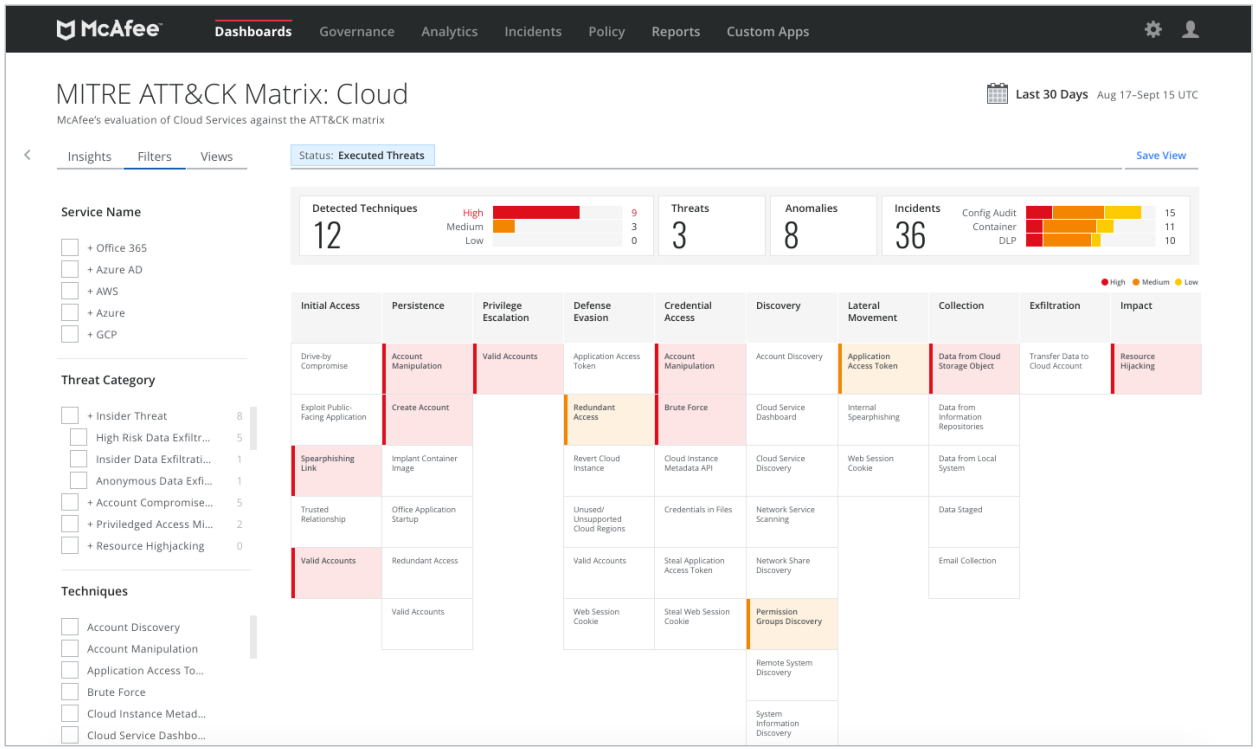

Figure 1. View threats that have already executed in your multi-cloud environment from MVISION Cloud.

- **Proactive**, showing attacks in progress so they can be stopped
- **A full kill-chain view of an attack**, combining incidents, anomalies, threats, and vulnerabilities into a holistic string of infractions

Security teams responsible for protecting their critical assets in cloud environments like Microsoft 365, Microsoft Teams, AWS, Azure, and others can identify gaps in protection and make policy and configuration changes directly from the MITRE ATT&CK view of an ongoing threat.

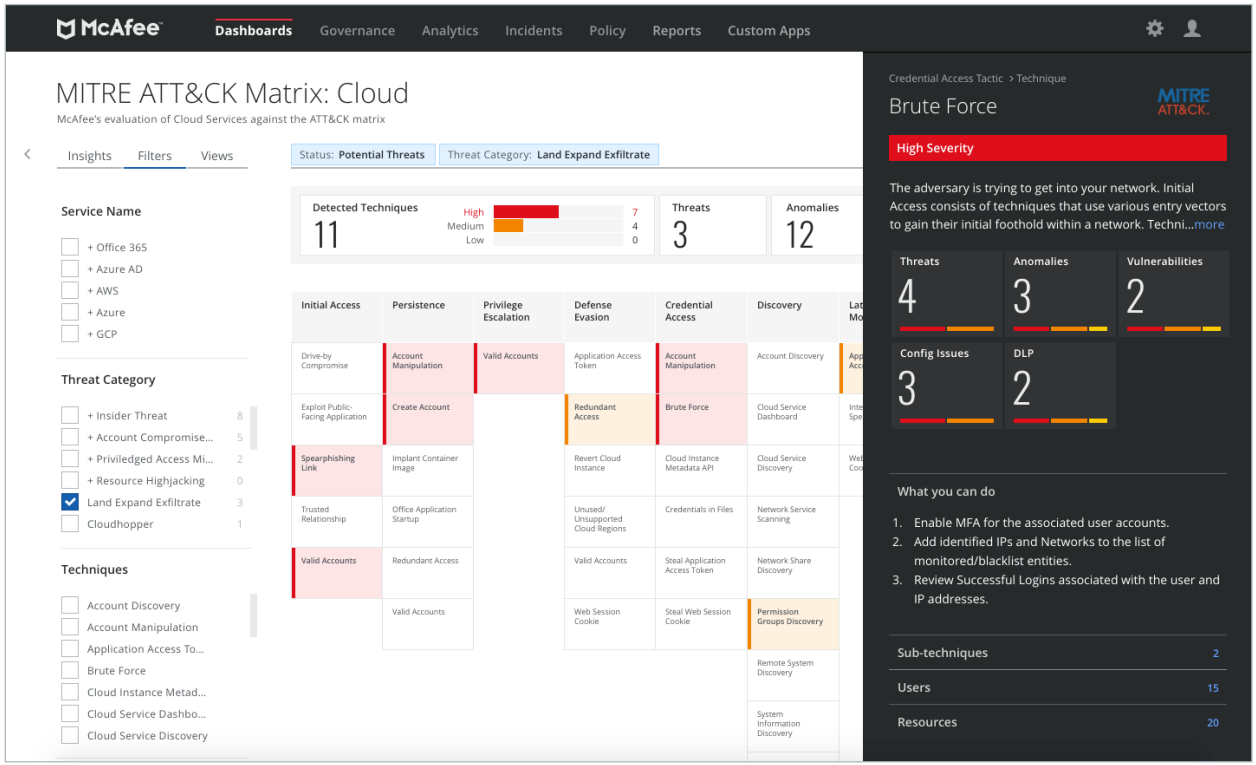

Figure 2. View attacks that are in progress, shown here, highlighting a drill-down into a brute-force adversary technique.

By visualizing attacks across the ATT&CK Matrix, effective policy decisions can be made at the right stage to stop the adversary before they are successful in achieving their goal.

MVISION Cloud: A Single Platform for Multi-Cloud Security

The world's leading security teams use MITRE ATT&CK. With MVISION Cloud, McAfee is bringing cloud security incidents into the mainstream SOC. This is a critical paradigm shift for threat investigation. Now, not only can enterprises defend themselves against malware-based breach attempts, they can also stop data breaches from cloud-native attacks.

Only with MVISION Cloud can security teams:

- Bring pre-filtered cloud security incidents into their SOC, mapped to the MITRE ATT&CK framework
- Visualize both executed and potential attacks to their cloud environments, across multiple SaaS, PaaS, and IaaS services
- Stop ongoing and future attacks by implementing recommended policy and cloud service configuration changes directly associated to MITRE ATT&CK techniques

With McAfee, threat investigation isn't just for one environment—it is for all of your environments, from cloud to endpoint to your analytics platforms. With McAfee MVISION Cloud, MVISION EDR, and MVISION Insights, your enterprise has an extended detection and response (XDR) platform for the heterogenous attacks you face today.

Get Started with Cloud Threat Investigation

To get started with cloud threat investigation using MITRE ATT&CK, contact us now. Click here to request a demo.

McAfee

2821 Mission College Blvd.
Santa Clara, CA 95054
888.847.8766
www.mcafee.com