







# FINDING EVIL IN YOUR CLOUD THAT OTHER VENDORS MISS

## Current Teams and Tools Aren't Equipped For Cloud Attacks

Every organization where Permiso has detected an incident had a mature vulnerability management program in place. The vast majority of them had a Cloud Security Posture Management system to ensure resources are deployed and configured properly. But CSPMs and other tools haven't approached the cloud with the security fundamentals of detection and response. Consequently, security teams haven't been able to keep up with the tactics of modern threat actors. Organizations struggle to develop runtime visibility in their cloud infrastructure environments and respond to an incident in a timely manner and their tools and tricks that worked on-premise simply don't translate in the cloud.

Today, cloud security is largely predicated on demonstrating compliance and maintaining visibility into environments, securing the resources within them, and understanding the vulnerabilities associated with each. History is indeed repeating itself and what we witnessed in the journey to securing data centers twenty year ago is now happening again in the cloud. Enterprises start with compliance before developing more advanced detection and response capabilities. Permiso is focused on that next phase of cloud security - finding evil in the cloud.

## What We're Doing

| FEATURES AND BUGS   | CSPM | SIEM | PERMISO |
|---|------|------|---------|
|  Alert Fatigue                        | ✓    | ✓    |         |
|  High False Positives                 | ✓    | ✓    |         |
|  False Negatives (\$%#@#!)            | ✓    | ✓    |         |
|  Identity Threat Detection & Response |      |      | ✓       |
|  TTP-Based Detections                 |      |      | ✓       |
|  Cloud Threat Detection Badasses      |      |      | ✓       |

## Why Cloud Detection and Response Needs To Secure Every Layer of the Cloud

Managing identities and analyzing their corresponding behavior across cloud environments presents one of the single biggest challenges for cloud detection and response. The fragmented authentication boundaries across cloud environments makes it hard to tie a user in Okta to that same user in GitHub or AWS. Okta, as an identity provider, isn't privy to the activity on the other side of the 'wall' in AWS, Azure, Github and other Saas, IaaS, or PaaS vendors. Similarly, AWS's purview is limited to the identities and behaviors within that AWS environment. These silos make cloud threat detection and effective Incident Response daunting or impossible for most security teams. Teams are left to use poorly designed legacy tools to dig through logs in order to find a small picture of the overall activity that occurred without any other context.

This problem is compounded by the fact that these users assume shared roles and credentials and the corresponding activity within the environment is associated back to the role as opposed to the individual that assumed that role. Because many attacks are orchestrated across multiple services in the cloud, being able to replay those attacks across those cloud applications by trying to dig through logs and make sense of the data proves to be a very arduous and time consuming task - unless you use Permiso!



"The power of Permiso and the p0 labs team provides our team with visibility and detection into our public cloud environment that isn't covered by our CSPM and SIEM today."

**Sebastian Goodwin, Former CISO**



**16** days is the median number of days an attacker is present in a target's environment before being detected

[M-Trends 2023 Report]

**75** percent of IT and security teams agree that their cloud-specific knowledge is limited and needs to grow

[GCAT Cloud Detection & Response Survey Report]

### WHO

Permiso identifies which identities, credentials, roles, secrets, and users are in your environment.

### HOW

Permiso creates an immutable ledger of attributed activity for identities across SaaS, IaaS, and PaaS boundaries.

### WHAT

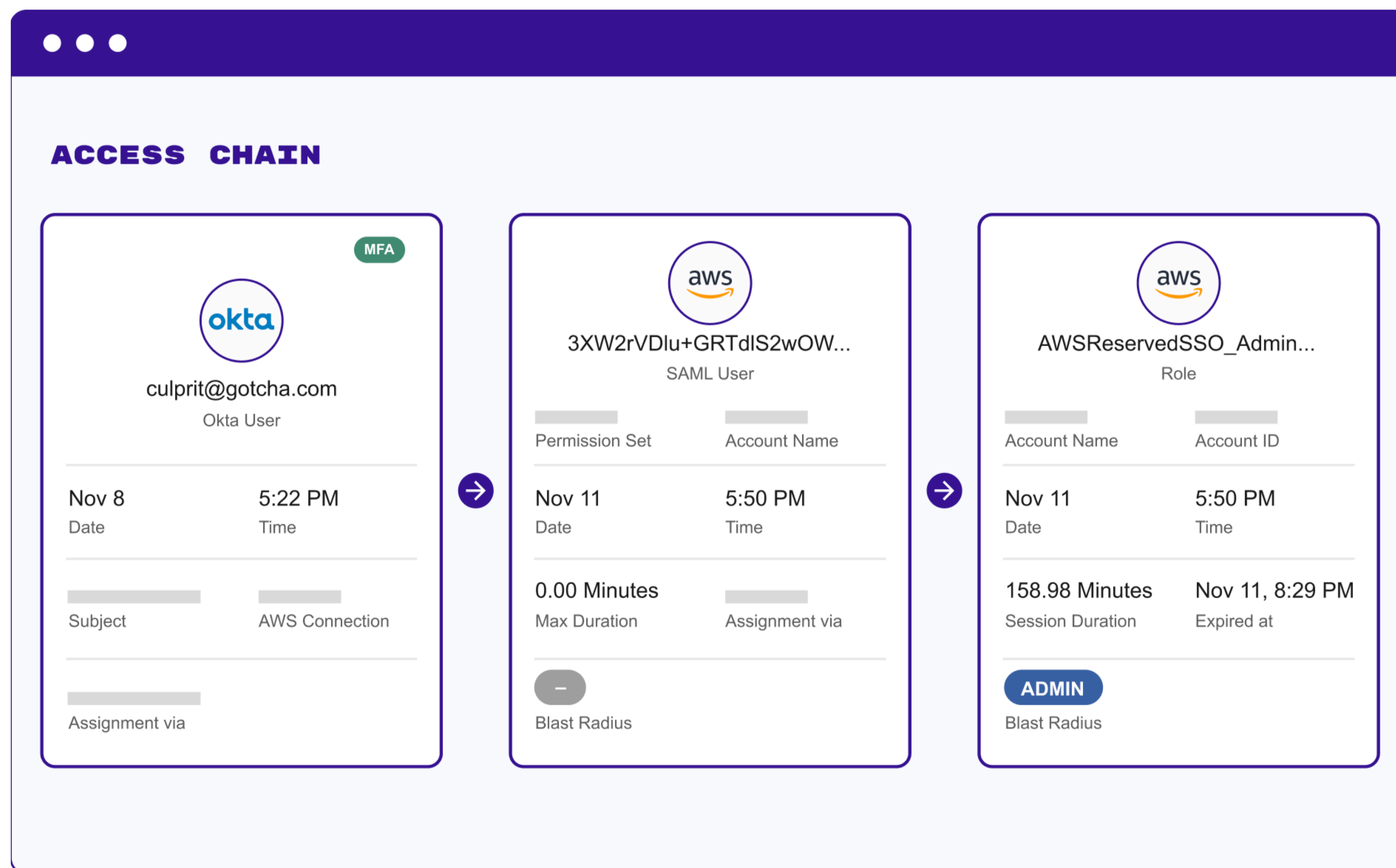
Permiso uses access, behavior, and multi-nodal classifiers to analyze the activity ledger for suspicious, malicious, or known bad patterns.

## Tackling CDR

- Provide complete visibility into the identities across your cloud SaaS environments, what changes are being made, and who is making them
- Detect access anomalies coupled with significant changes in your environment to discover malicious threat actors
- Identify policy violations at runtime such as console access, bypassing identity federation, bypassing MFA or use of root access, as well as overprivileged accounts
- Monitor credentials and secrets that are being used by your Identities

## Synthesize Identity and Activity Across The Cloud

Permiso creates session constructs for the identities across cloud and SaaS applications to break down visibility boundaries and understand user behavior and intent across your environment. Session constructs are developed by stitching together activity across cloud applications, services, and providers to create an immutable ledger of activity in an environment. Permiso creates a unified identity across authentication boundaries and presents this as a forensically sound access chain. By tying all activity back to a singular identity, Permiso is able to detect access anomalies, behavioral anomalies, or specific activities associated with compromised credentials. Permiso is also able to detect activities that may place your environment at undue risk.



## Powered By Cloud Security Experts

Permiso focuses on building cloud detection and response solutions to help customers detect and disrupt cloud security incidents. The company's research team focuses on three areas: evaluating the security and operating controls of public cloud and SaaS vendors, collaborating with the cloud security community to understand global observations, and actively investigating cloud breaches and attacker tooling. The ultimate goal of this research is to develop powerful Tactics, Techniques, and Procedures (TTP)-based detections that are powered by real-world incidents or methods that we expect to see adversaries use.

**Eric Tan, CIO & SVP Technology**

### Common Use Cases

- **Prevent Data Theft** - Detect suspicious activity in your account such as database snapshots, email exporting, EC2 and EBS snapshots and private S3 bucket cloning
- **Thwart Crypto Mining Attacks** - Monitor real-time access anomalies, publicly exposed API credentials, detect compute credential hijacking attacks and usage of long-lived or unused keys or tokens
- **Detect Insider Threat** - Monitor the ongoing activity of overprivileged and high risk identities
- **Uncover Runtime Policy Violations** - Detect use of root, console access without MFA, and federated vs. non-federated access
- **Monitor Change Attribution** - Track all sources of DevOps changes from GitHub, Terraform, and cloud environments to attribute all changes back to a specific user (human, machine, or vendor)

Combining this research with the unique and patent-pending multi-flow activity and identity attribution engines in our product allows us to deliver first-of-their-kind TTP-based detections with a near-zero false positive rate. The flywheel of feedback, between what our research teams discover daily and what our product teams build, will continue to allow us to stay one step ahead of the adversary.