PERMISO

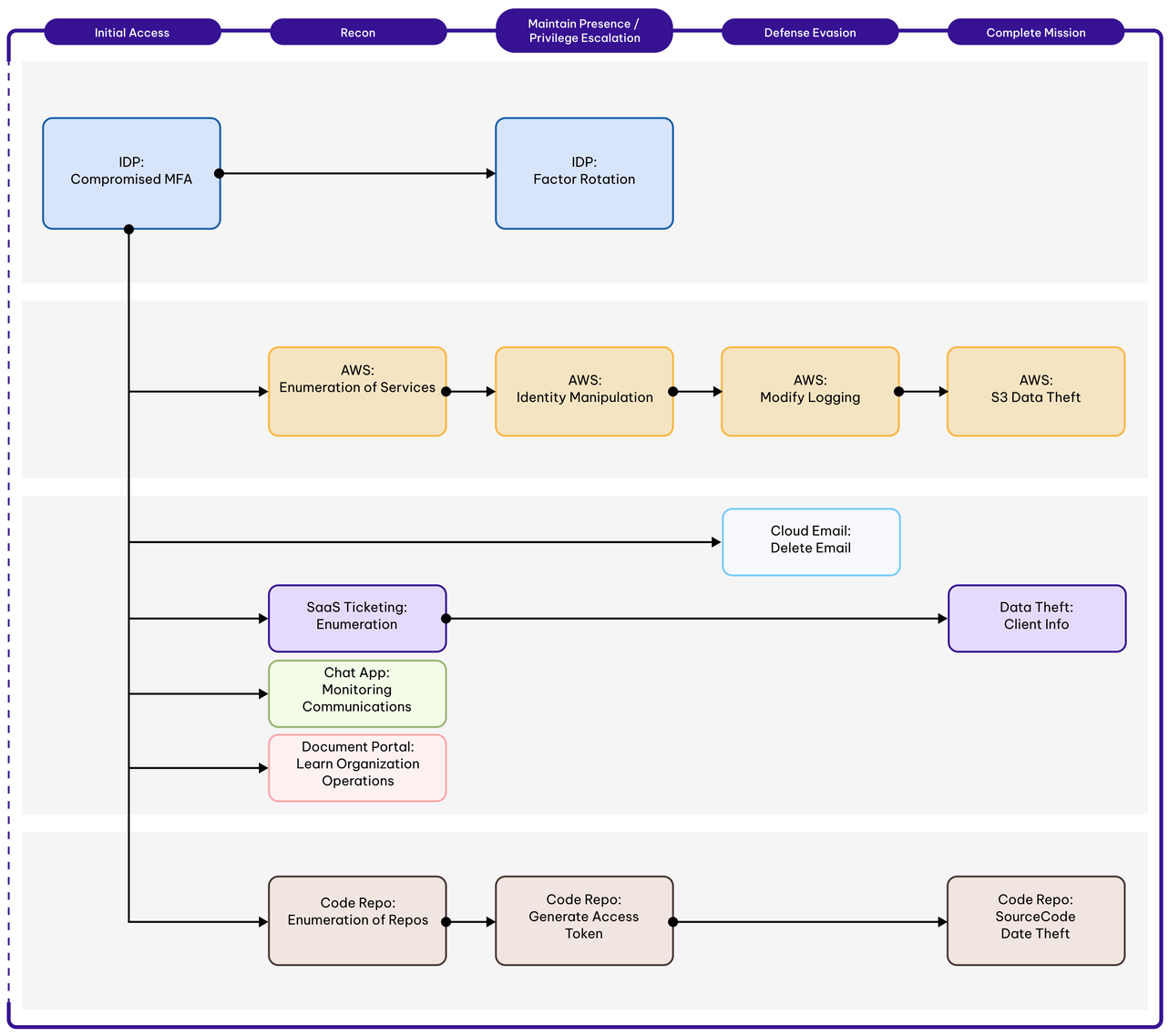
CLOUDSEC HEALTH CHECK
A CHECKUP FOR YOUR CLOUD

Answer the Question “How Am I Doing With Cloud Security?”

In every organization where Permiso detected an incident in a cloud environment, a mature vulnerability management program was in place. The vast majority of those incidents we detected had a Cloud Security Posture Management system to ensure resources were deployed and configured properly.

Runtime visibility in the cloud continues to evade security professionals. The complexity of trying to sequence all activity in a cloud environment across authentication boundaries like Okta, AWS and GitHub, for instance, is an arduous task. Synthesizing that activity with their corresponding identities, which are ultimately using shared credentials, is nearly impossible. Permiso’s CloudSec Health Check is a way for companies to understand how they’re doing with respect to cloud security, and how they’re doing relative to their peers. There’s a lot more to cloud than posture and configuration, and security teams shouldn’t have to spend hours querying logs to try to replay activity in their environment.

EXPANDED CDR ATTACK



Finding Evil In The Cloud Isn’t Easy

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. But modern threat actors are moving across these authentication boundaries over the course of their attack.

This problem is compounded when users assume shared roles and credentials since the corresponding activity within the environment is associated back to the role as opposed to the individual assuming the role. Because many attacks are orchestrated across multiple services in the cloud, replaying those attacks across each cloud application is an important capability. However, trying to manually dig through logs and make sense of the data across these applications proves to be a very arduous and time-consuming task - unless you use Permiso!

What Our Report Tells You

- Gain 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, use of root access, and overprivileged accounts
- Monitor credentials and secrets being used by your identities

What We’re Looking For

WHO

Permiso identifies the identities, credentials, roles, secrets and users 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.

---

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

[M-Trends 2023 Report]

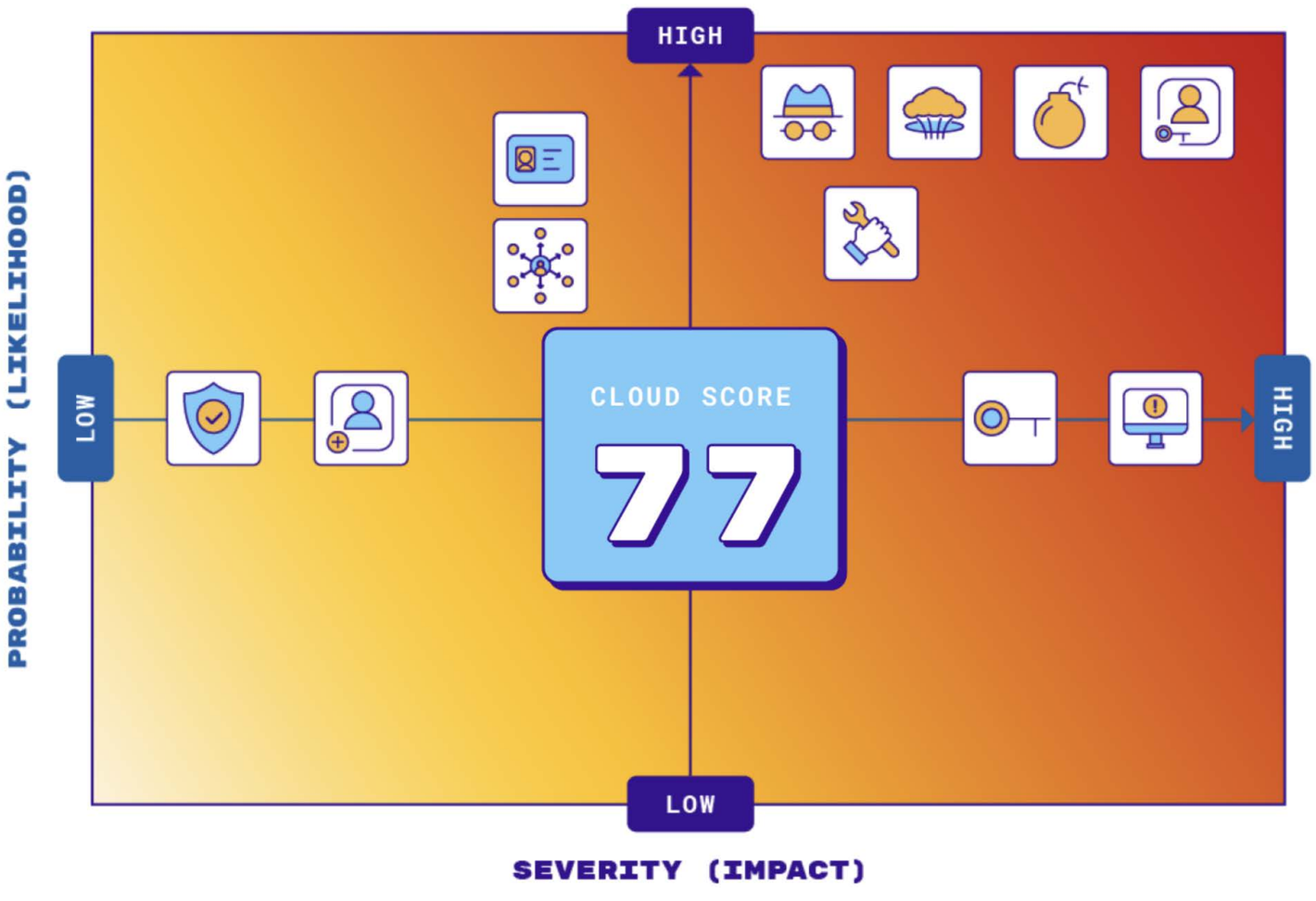
75 percent of IT and security teams agree that their cloud-specific knowledge is limited and needs to grow

[GCAT Cloud Detection & Response Survey Report]

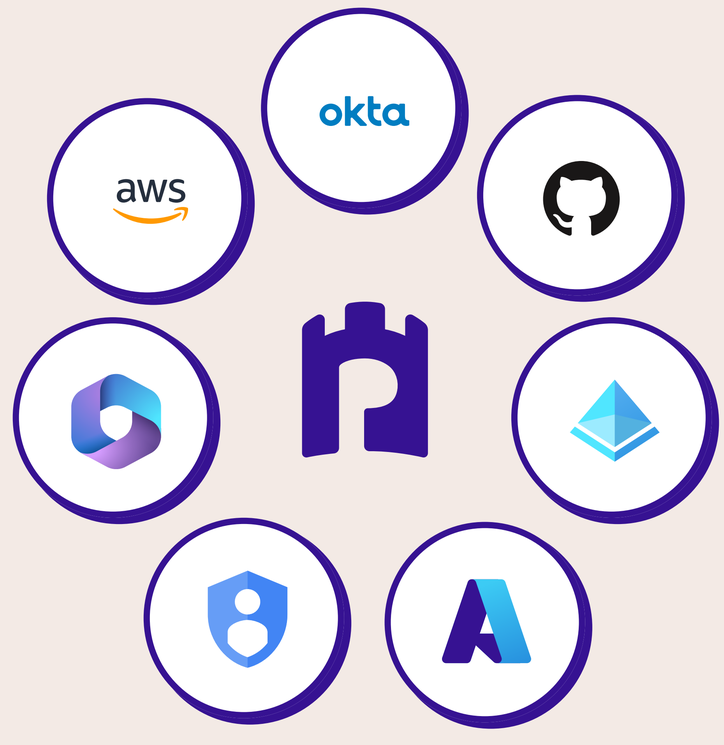
PERMISO

Synthesize Identity and Activity Across The Cloud

Permiso's CloudSec Health Check creates session constructs for the identities across cloud, IaaS, PaaS, SaaS and CI/CD 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 and specific activities associated with compromised credentials. Permiso is also able to detect activities that may place your organization at undue risk.



Full Diagnostic Check Up



Powered By Cloud Security Experts

The Permiso team is comprised of security veterans -- from the former Head of Advanced Practices at Mandiant, to seasoned product executives at FireEye. 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 threat actor activity, and actively investigating cloud breaches and attacker tradecraft. 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.

VULNERABILITY	SEVERITY (IMPACT)	PROBABILITY (LIKELIHOOD)	IMPACT
Public EC2 with IMDSv1	Critical	Critical	-4
AWS Console Access without MFA	Critical	Critical	-4
Unused Long-Lived Access Keys	High	Critical	-3
Overprivileged Users and Roles	Critical	High	-3
Azure AD Password Spraying	Critical	High	-3
Rhino Privilege Escalation	High	High	-2
Old Long-Lived Access Keys	Medium	Critical	-2
Unused Roles	High	Medium	-1
Unused Identities	High	Medium	-1

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.