UNIFIED IDENTITY SECURITY

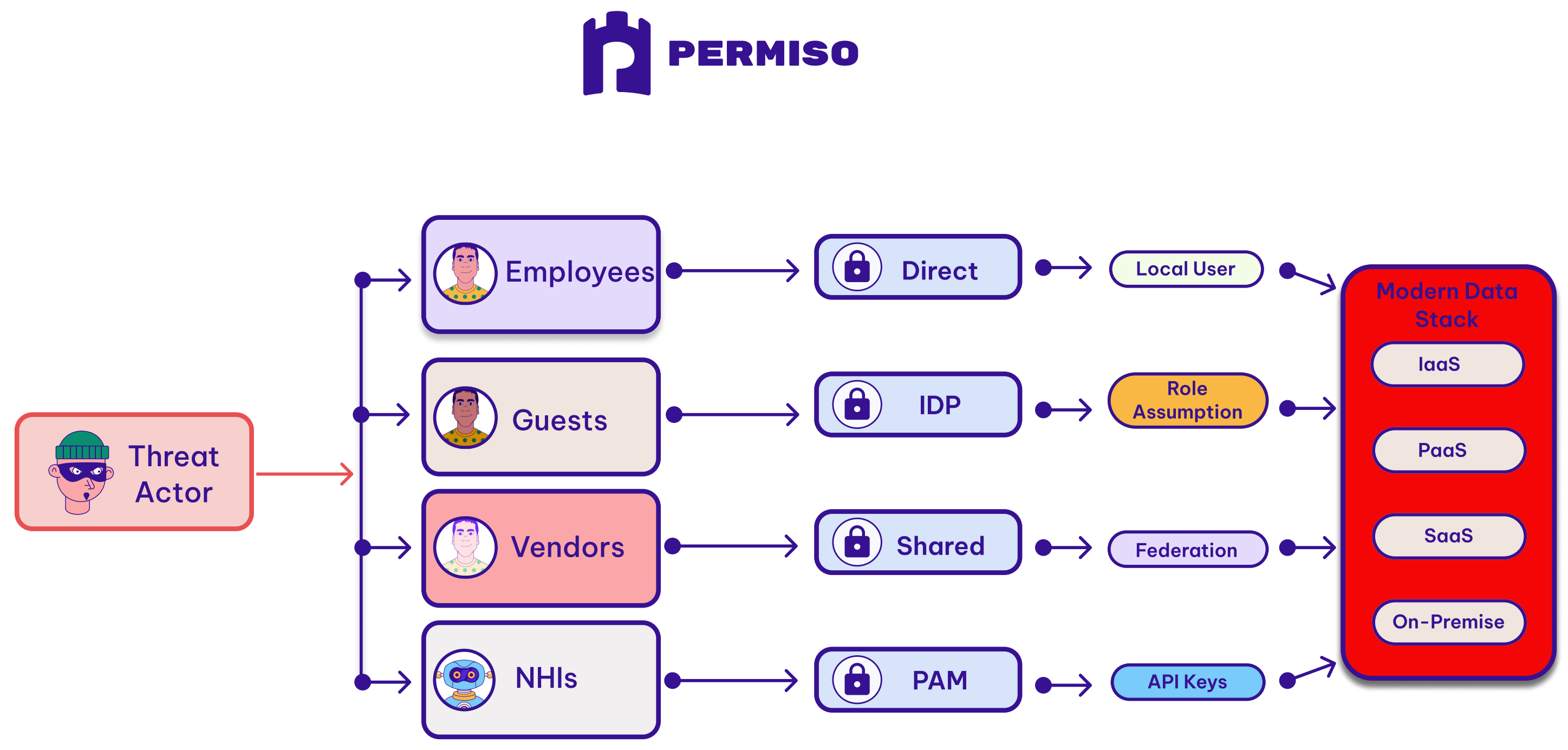
Your Identity Attack Surface is Bigger than You Realize

Protecting identities in a modern digital enterprise is complex, especially when they move across authentication boundaries, or access resources directly. The challenge is amplified when we consider the number and diversity of identities that exist in a typical environment. For example, non-human identities (API keys, tokens, service accounts) can easily outnumber human identities (employees, guests, contractors) by as much as 40:1.

Not only are there lots of identities that need to be managed, but also the multiple ways they are used in an environment and between environments. Shared credential usage is commonplace so too is provisioning non-human entities with excessive privileges, making the task of determining which identity performed a Create, Read, Update and Delete (CRUD) action across multiple environments extremely challenging.

The challenge is not helped by the siloed nature of existing cybersecurity solutions. Many existing solutions i.e. CSPM for IaaS or SSPM for SaaS, only provide partial visibility at the specific layer. These solutions also produce no shortage of alerts, and the problem with these alerts is that they lack actionable context. Most of the time these solutions are only of utility post-incident i.e. after a breach notification or during forensic investigations.

The lack of unified identity threat detection and response capability enables modern threat actors to move seamlessly across the authentication boundaries, going undetected for weeks or even months at a time. Attempting to piece together the full picture of a potential incident once identified usually takes days of digging through disparate logs from different security solutions and across different services layers. Being able to understand what resources threat actors accessed, how they gained access, and what CRUD actions they took in an environment is often difficult if not impossible to fully determine.



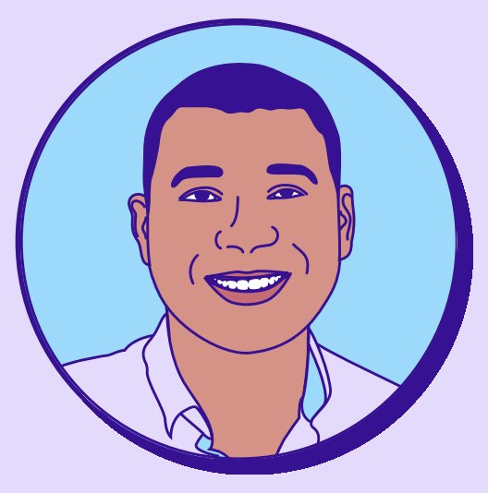
Universal Identity Graph

Permiso is the first unified identity security platform that has been battle tested against identity-based attacks in the cloud and on-prem, detecting threats even when threat actors attempt to mask their actions by leveraging assets available to them in any one environment.

Through the Universal Identity Graph, Permiso inventories every identity across IdPs, IaaS, PaaS and SaaS environments, including CI/CD platforms, and maps those identities to a human or non-human entity. Permiso then monitors and tracks their behavior to determine whether that activity is suspicious or malicious. By baselining 'normal' behavior and mapping activity against a deep library of TTPs from known threat actors, Permiso detect real threats in your environment, in real time, enabling SecOps teams to respond to those threats faster than ever.

Even through the use of shared credentials, Permiso attributes all of the corresponding activity back to the identity that performed them. This gives security teams a clear line of sight into who is in their environment and what they doing in order to more accurately and quickly detect evil. By living in the breach we also enable unparalleled identity attack surface management, specifically enabling you to answer the following questions:

- **Who are the riskiest identities in my environment?**
- **How and where is my current environment being accessed by human and non-human identities?**
- **How broadly is MFA enforced across the applications in my environments?**
- **Why is a particular identity performing certain CRUD actions? What permissions allow that identity to perform those actions?**
- **Can I detect attempts to compromise sensitive data such as code repos in real time?**



> *"Permiso has proven to be indispensable to the way we manage and secure identities across multiple cloud environments. "*
>
> ***Sebastian Goodwin, Chief Trust Officer***
>
> AUTODESK

292 days is the mean time it takes to identify and contain a breach involving stolen credentials

[IBM Cost of a Data Breach 2024 Report]

80 percent of all attacks involve identity and compromised credentials

[Crowdstrike Global Threat 2024 Report]

WHO

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

HOW

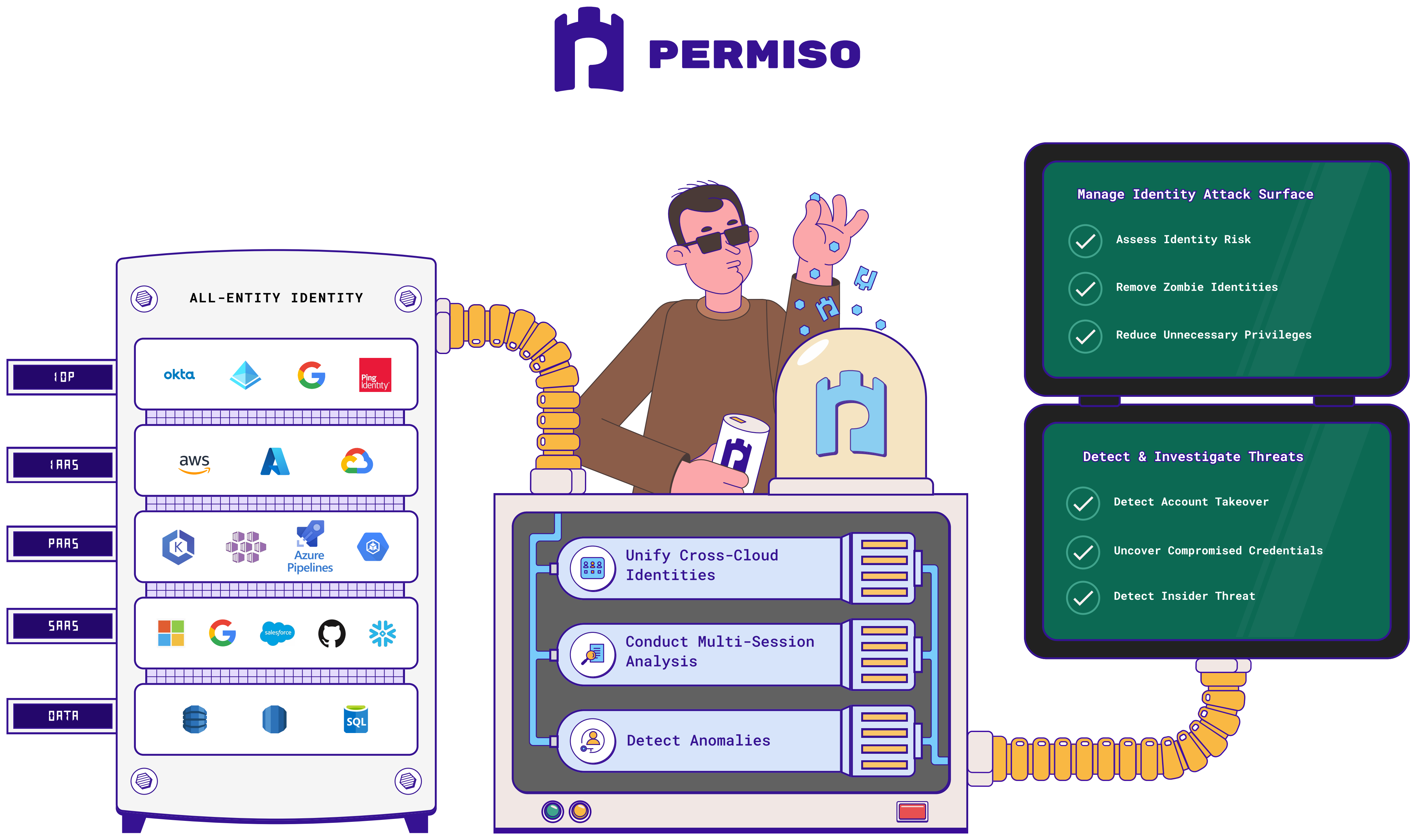
Permiso creates an immutable ledger of attributed activity for identities across the IdP, IaaS, PaaS and SaaS layers, including CI/CD platforms

WHAT

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

Tackling Identity Security

- Gain complete visibility into human and non-human identities across all environments, what CRUD actions are being taken, and who is making them
- Significantly improve Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR) to anomalous identity activity across all environments
- Monitor credentials and secrets that are being used by all identities across all environments
- Identify policy violations at runtime such as console access, enforcement of federation and MFA, use of root access, over-privileged accounts, and attempts to compromise sensitive data such as code repos



Manage Identity Attack Surface

- ✓ Assess Identity Risk
- ✓ Remove Zombie Identities
- ✓ Reduce Unnecessary Privileges

Detect & Investigate Threats

- ✓ Detect Account Takeover
- ✓ Uncover Compromised Credentials
- ✓ Detect Insider Threat

> *"Permiso's ability to track identities and their activities across IaaS, SaaS and identity providers at runtime is unlike any of our existing solutions."*
>
> ***Michael Hensley, Head of Cyber Security***
>
> MODERN HEALTH

Manage Identity Attack Surface

- **Assess Identity Risk** - Shine a light on all human and non-human identity risk, across all environments
- **Remove Zombie Identities** - Remove dormant identities and ghost accounts
- **Reduce Privileges** - Enforce privilege access management across all identities, remove unused and unnecessary privileges

Purpose Built to Detect Identity-Based Attacks

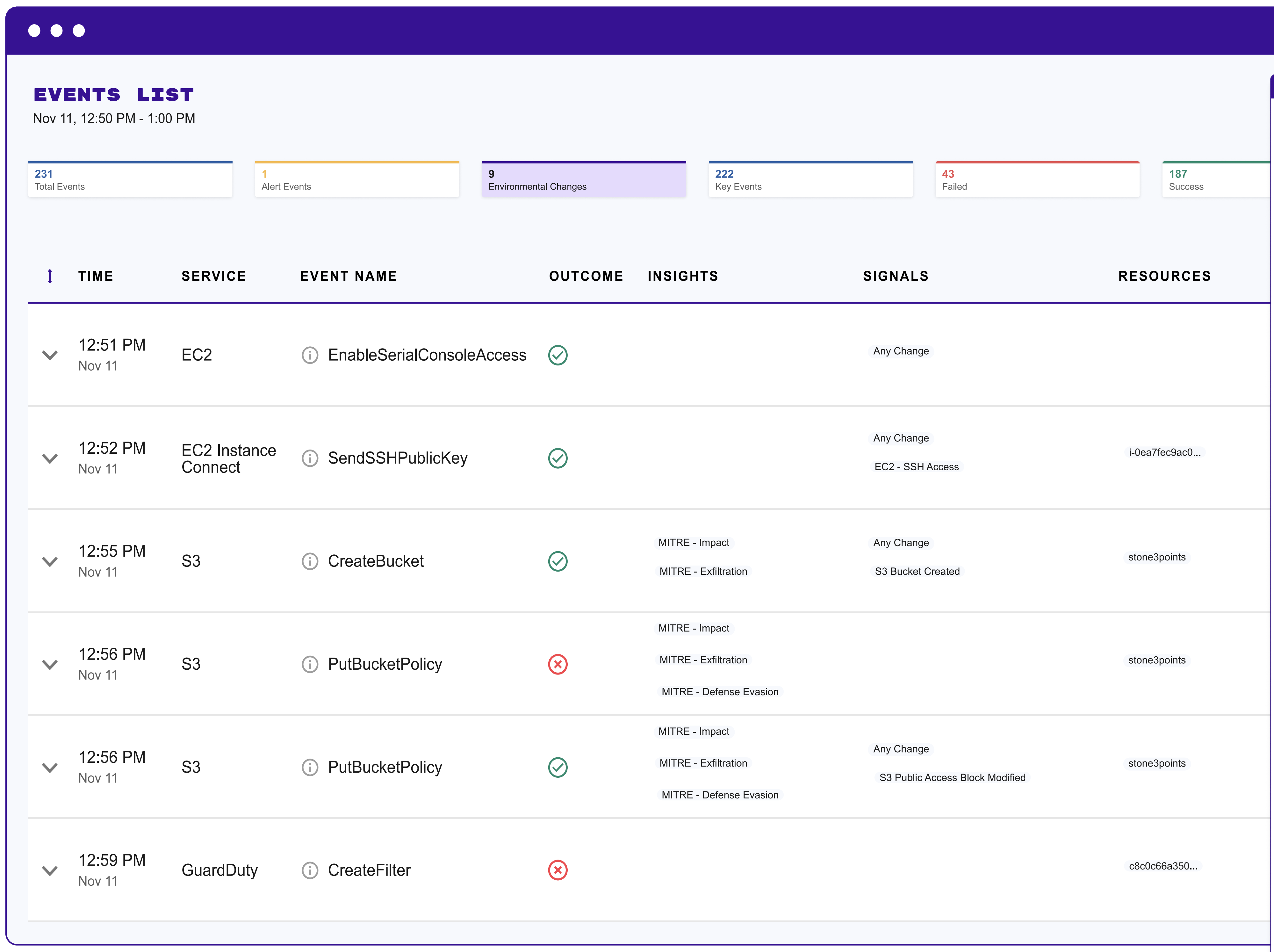
Permiso Security was founded to comprehensively detect identity risks and threats across a fragmented ecosystem, with the focus on addressing the greatest threat vector, compromised human and non-human identities. Through the Universal Identity Graph, Permiso is able to track all-entity identities (human and non-human) and their relationships to other identities, credentials and assets across other environments (IdP -> IaaS -> PaaS -> SaaS).

The Universal Identity Graph is powered by our proprietary, multi-environment runtime threat detection engine, combining 1k+ detection rules developed by our in-house P0 Labs experts with ML powered behavior-based detections. This capability enables organizations to identify at risk identities in real time through high fidelity alerting, while also illuminating likely attack paths. The end result is a dynamic, birds-eye view of your identity risk across all environments. Now organizations are able to detect threats such as account takeover, credential compromise and insider threat in real time, while at the same time reduce the identity attack surface through removing zombie identities and unnecessary privileges.

With Permiso's Universal Identity Graph you can at any time determine who your top 10 riskiest identities are and proactively manage access and permissions for any environment, not just your IaaS or SaaS services layer. Only with this unified approach can organizations shine a light on the siloes where threat actors such as LUCR-3 (aka Scattered Spider) hide in their bid to compromise high value data such as IP or source code.

Detect & Investigate Threats

- **Account Takeover** - Track all identities and all of their activities as well as their impact in any environment
- **Credential Compromise** - Tracks the entire lifecycle of credentials, their privileges and posture, as well as all of the sessions those credentials were used in and by what identity
- **Detect Insider Threat** - Monitor the ongoing activity of overprivileged and high risk identities

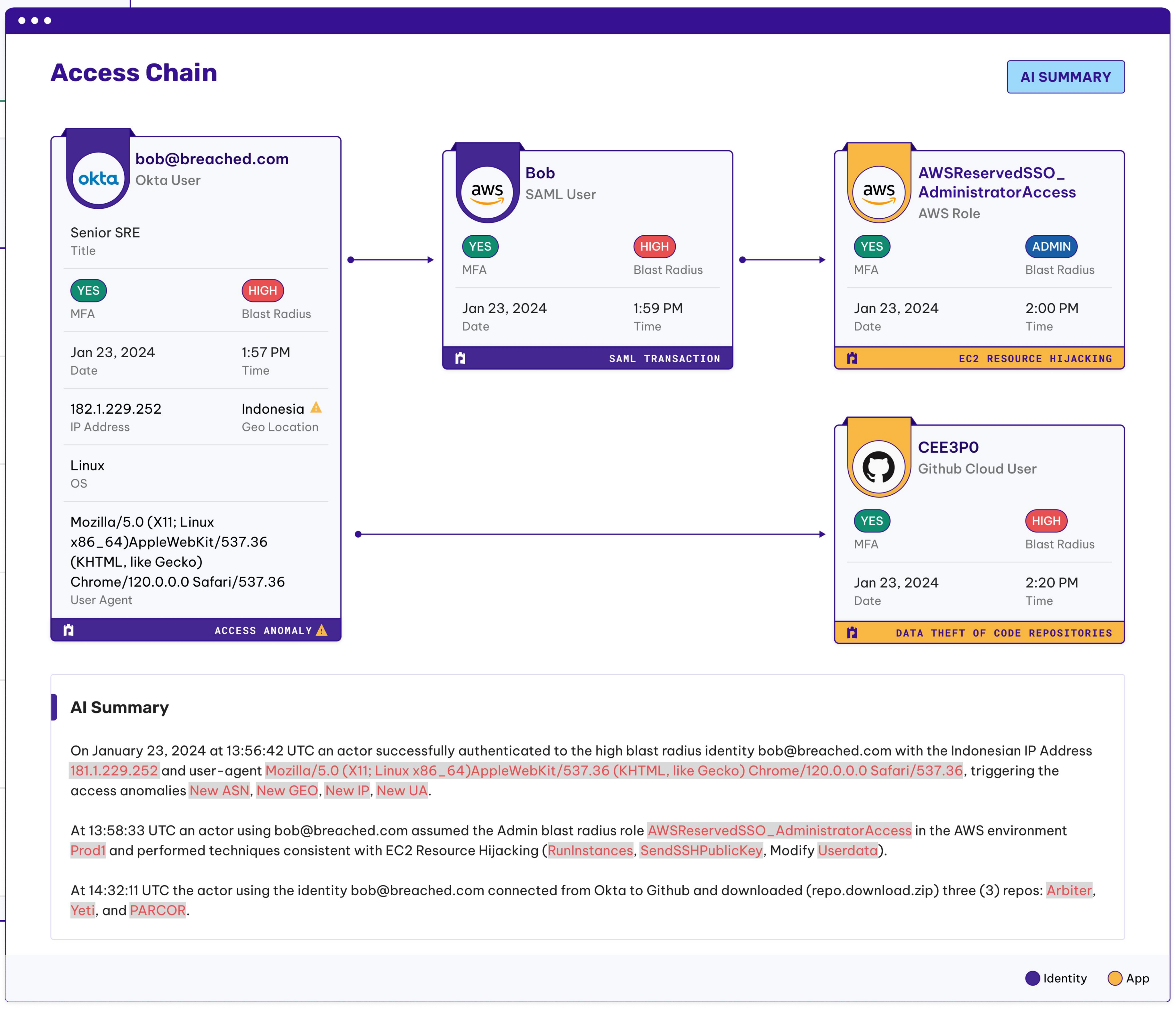


EVENTS LIST

Nov 11, 12:50 PM - 1:00 PM

231 Total Events | 1 Alert Events | 9 Environmental Changes | 222 Key Events | 43 Failed | 187 Success

TIME	SERVICE	EVENT NAME	OUTCOME	INSIGHTS	SIGNALS	RESOURCES
12:51 PM Nov 11	EC2	EnableSerialConsoleAccess	✓		Any Change	
12:52 PM Nov 11	EC2 Instance Connect	SendSSHPublicKey	✓		Any Change EC2 - SSH Access	i-0ea7fec9ac0...
12:55 PM Nov 11	S3	CreateBucket	✓	MITRE - Impact MITRE - Exfiltration	Any Change S3 Bucket Created	stone3points
12:56 PM Nov 11	S3	PutBucketPolicy	⊗	MITRE - Impact MITRE - Exfiltration MITRE - Defense Evasion		stone3points
12:56 PM Nov 11	S3	PutBucketPolicy	✓	MITRE - Impact MITRE - Exfiltration MITRE - Defense Evasion	Any Change S3 Public Access Block Modified	stone3points
12:59 PM Nov 11	GuardDuty	CreateFilter	⊗			c8c0c66a350...



Access Chain

AI SUMMARY

bob@breached.com
Okta User
Senior SRE — Title
YES — MFA | HIGH — Blast Radius
Jan 23, 2024 — Date | 1:57 PM — Time
182.1.229.252 — IP Address | Indonesia ⚠ — Geo Location
Linux — OS
Mozilla/5.0 (X11; Linux x86_64)AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36 — User Agent
ACCESS ANOMALY ⚠

Bob
SAML User
YES — MFA | HIGH — Blast Radius
Jan 23, 2024 — Date | 1:59 PM — Time
SAML TRANSACTION

AWSReservedSSO_AdministratorAccess
AWS Role
YES — MFA | ADMIN — Blast Radius
Jan 23, 2024 — Date | 2:00 PM — Time
EC2 RESOURCE HIJACKING

CEE3PO
Github Cloud User
YES — MFA | HIGH — Blast Radius
Jan 23, 2024 — Date | 2:20 PM — Time
DATA THEFT OF CODE REPOSITORIES

AI Summary

On January 23, 2024 at 13:56:42 UTC an actor successfully authenticated to the high blast radius identity bob@breached.com with the Indonesian IP Address 181.1.229.252 and user-agent Mozilla/5.0 (X11; Linux x86_64)AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36, triggering the access anomalies New ASN, New GEO, New IP, New UA.

At 13:58:33 UTC an actor using bob@breached.com assumed the Admin blast radius role AWSReservedSSO_AdministratorAccess in the AWS environment Prod1 and performed techniques consistent with EC2 Resource Hijacking (RunInstances, SendSSHPublicKey, Modify Userdata).

At 14:32:11 UTC the actor using the identity bob@breached.com connected from Okta to Github and downloaded (repo.download.zip) three (3) repos: Arbiter, Yeti, and PARCOR.

● Identity ● App