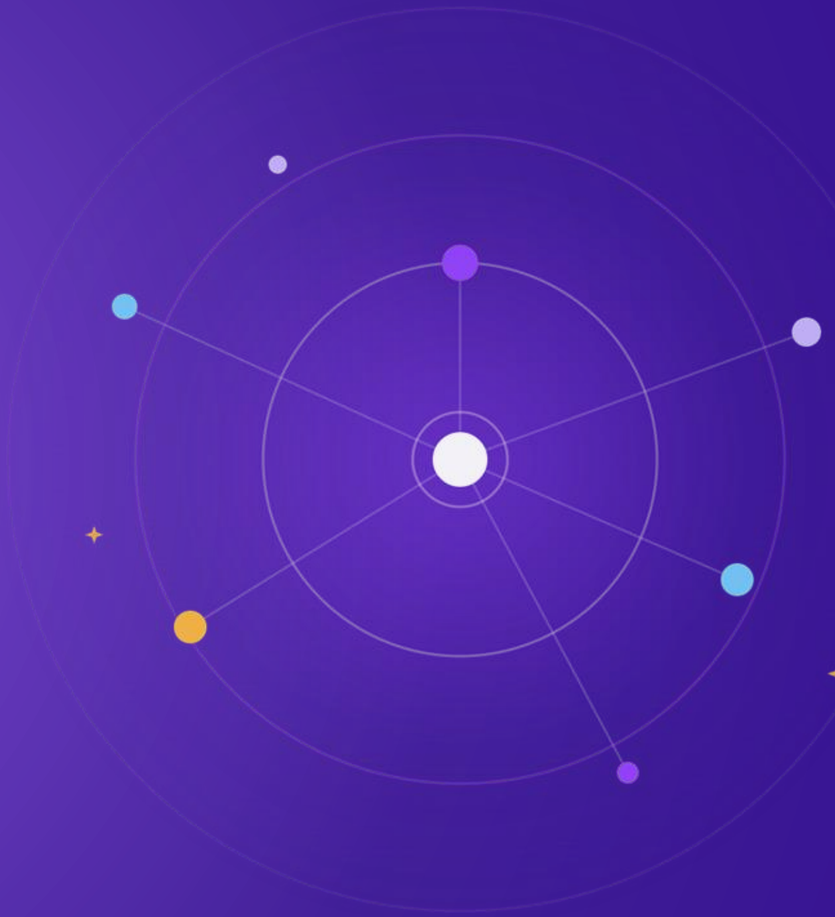
PERMISO

CONFIDENTIAL

IDENTITY SECURITY · PROOF OF VALUE

Identity Risk Assessment



A prioritized snapshot of identity risk across **ACME, Inc.** 's cloud, SaaS, and AI environments — environments — captured at the first PoV checkpoint.

PREPARED BY
Permiso Security

DATA CURRENT AS OF
May 19, 2026

STAGE
First PoV Checkpoint

Current State at a Glance

TOTAL IDENTITIES

14,085

Across Azure AD, Okta, Atlassian, Snowflake, Dynatrace & JFrog

1.66K
HUMAN IDENTITIES

6.05K
MACHINE IDENTITIES

335
AGENT IDENTITIES

494 TOTAL ALERTS — 90-DAY WINDOW

- **20** Critical
- **124** High
- **162** Medium
- **188** Low

827 TOTAL EXPOSURES — BY SEVERITY

- **59** Critical
- **343** High
- **248** Medium
- **177** Low

KEY TAKEAWAY

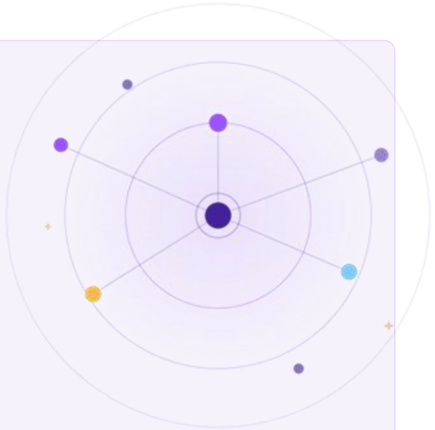
ACME's most material risk is **standing or weakly governed identity privilege** — especially among service principals and administrative workflows — not alert volume.

THEME 01 · FINDINGS

Privileged Role Activity

Routine PIM elevation to Global Admin — even when approved and time-bound — exposes the full tenant to compromise during each activation window. The core issue is reliance on the broadest possible privilege when **scoped roles exist for nearly every operational task.**

Global Admin Role Added Highest-severity campaign · likely known admin activity	127 ALERTS	• CRITICAL
Azure Owner Assignment Subscription-level ownership granted	53 ALERTS	• MEDIUM
Azure Contributor Assignment 104 alerts across 7 identities	104 ALERTS	• LOW



PRIVILEGED ACCESS

127

PIM-related alerts — the highest-severity activation campaign observed in observed in the window.

CONTEXT

PIM justifications observed included "Check permission," "Daily Task," "Azure Policy Check." Activity traced to a known admin naming convention (`james.hartley@acme-inc.com`) and excluded from findings.

PERMISO

Privileged Role Activation

Global Admin activation should not be a standard operational workflow — nearly every operational task has a purpose-built Entra role.
Entra role.

01

Close the Role-Mapping Gap

If scoped role coverage for routine tasks isn't established, establish it first. If a scoped role already exists, the Global Admin activation should be denied.

PRIMARY

02

Require Meaningful Justification

Tie every activation to a specific, audited business justification for a task that cannot be cannot be completed with a scoped role.

03

Enforce Strict Activation Windows

Maximum 2-hour activation windows, with no self-renewal permitted.

04

Require Peer Approval

Global Admin and subscription Owner activations must be approved by a second named party. Self-approval is not permitted.

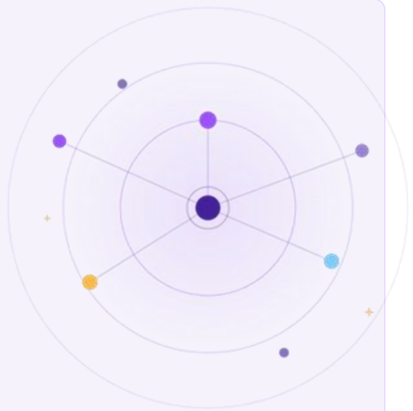
05

Alert on Every Activation — Without Exception

Treat every activation as requiring review. Review eligible assignments quarterly toward a ceiling of 4–5 accounts.

Non-Human Identity Exposure

Service principals with durable credentials and broad permissions — especially when **orphaned, dormant, or ownerless** — are durable attack paths, harder to detect than human account misuse.



NON-HUMAN IDENTITIES

Durable credentials, broad scope, and no owner combine into an attack path that outlives the workflows that created it — and rarely produces a user-facing signal.

HIGHEST-RISK IDENTITIES

LogAnalytics Reader SP Security Watchlists · No Owner	• CRITICAL
AZ-INFRA-DEPLOY-SYS-PD / NP Inactive · admin blast-radius	• CRITICAL
ComplianceTrack CCR Mail Retrieval Overly permissive scope	• HIGH
CloudBackupForMicrosoft365 High blast-radius · No Owner	• HIGH
DataMigrate Pro / LinkBridge Connector High blast-radius · No Owner	• HIGH

THEME 02 · CONCENTRATION

NHI Concentration Risk

Risk concentrates in a small number of non-human identities — making it both measurable and fast to remediate.

29

Broad Data Access Permissions

Identities holding excessive data access scope across the environment.

11

Directory-Level Admin Roles

NHIs assigned Global Admin or Privileged Role Admin Admin directory roles.

8

Dormant Admin Blast-Radius SPs

5 dormant + 3 dormant orphaned service principals carrying admin blast radius.

HIGHEST-VALUE REMEDIATION

Assign owners, rotate or remove credentials, and reduce permissions on these identities — **faster to fix than human workflow changes** , with outsized posture impact.

THEME 03 · FINDINGS

Sensitive Data Shared Externally

Permiso identified sensitive file movement to third-party and AI-enabled platforms. While these destinations align with commonly used business platforms, continued monitoring is recommended — **data theft is a top priority for known threat-actor groups.**

487
DATA-SHARING EVENTS

128
PUBLIC-SHARING EXPOSURES

TOP SENDERS – ALL ROUTING TO AI PLATFORMS

Jennifer.Caldwell
Michael.Patterson
Rachel.Simmons
David.Thornton

AI DESTINATIONS – HIGHEST CONCERN

app.rogo.ai — HIGH CONCERN
73 FILES
9 SENDERS

search.hebbia.ai — MONITOR
18 FILES
1 SENDER

RECOMMENDATION

Destinations broadly align with sanctioned business platforms, so most activity may be policy-compliant — but Permiso recommends **continued monitoring of sensitive-data sharing to AI data sharing to AI platforms** , where exfiltration risk concentrates.

THEME 03 · DETAIL

PERMISO

Single-Use Destinations — Full Detail

All 13 destinations below had exactly one file transferred, sorted by risk profile. Personal/consumer platforms and external regulatory portals are flagged for priority review.
for priority review.

DESTINATION	USER IDENTITY	FILE	FLAG
web.whatsapp.com	Mustafa.Kanchwala	Support_Tickets_Q2.pdf	REVIEW
wings.sfc.hk	John.Washco	abm877_04_2026.xlsx	REVIEW
sandbox-4.reactblade…azure.net	Scott.Whitfield	ACME CLO 2019-1 Nightly Compliance Report.pdf	REVIEW
client.schwab.com	Karen.Delgado	Schwab Financial Planning Fact Finder.pdf	REVIEW
get.activedisclosure.com	Paul.Stanton	ACME Skyline Lending LP 03.31.26 - AD workbook.xlsx	
acme.lightning.force.com	Lisa.Carmichael	ACME Specialty Lending LLC RFI_vF.docx	
acme.seismic.com	Megan.Foster	Copy of FLXR Webinar blast Contacts.csv	
forms.monday.com	Amy.Gallagher	WhyActiveETFsMatterMorein2026_Mar2026.pdf	
portal.azure.com	Chris.Vandenberg	tabularShell - 2026-05-07T084018.csv	
make.powerautomate.com	Jason.Merritt	citiSplitPdfResult_002.pdf	
plutus.pd.acme.com	Diane.Prescott	SFM_2026_1.xlsx	
www.clientaxcess.com	Robert.Ashford	Fund VIII Conversion Tax Notice_5.15.26.pdf	
ironcladapp.com	Greg.Lawson	Cornerstone - ACME Renewal Order Form.pdf	

THEME 04 DISCOVER

PERMISO

AI Agent Inventory

14 AI Agents Discovered

9 Observed at Runtime

3 Shadow / Unsanctioned

COPILOT STUDIO · 5

Registered in Azure, confirmed calling foundational models at models at runtime.

LAMBDA-EMBEDDED · 6

Inferred via runtime model endpoint calls; source code not inspected.

SHADOW AGENTS · 3

ChatGPT Enterprise API, Rogo AI & Hebbia — not registered in any identity store.

WHY IT MATTERS

Static registration alone is insufficient — **9 of 14 agents surfaced only via runtime telemetry** and would not appear in a traditional asset scan. Shadow agents route company data to unvetted external AI platforms with no sanctioned identity attached.

THEME 04 PROTECT

AI Agent Access Risk

OVER-PERMISSIONED AGENT IDENTITIES

7 **agents hold permissions they have never exercised** at runtime — standing scope with no with no observed use.

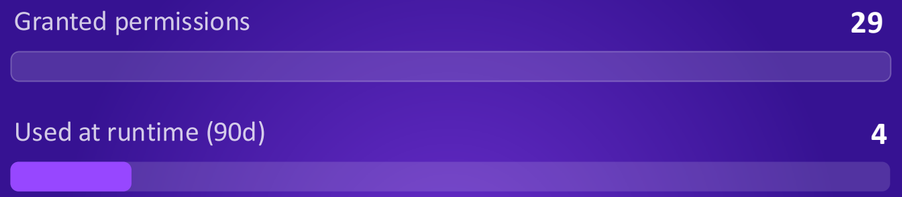
3 agents run on **hard-coded credentials or OAuth delegations** with no expiry policy.

4 agents have **no assigned owner** and no record in the NHI inventory.

- MCP and CLI tool grants are not tracked to the underlying role — **Permiso traces past the tool layer** to the **tool layer** to the actual credential assumed.

GRANTED VS. USED

ACME-DataSync-Agent



86%

of granted permissions unused in 90 days

RECOMMENDATION

Provable least privilege for agents requires **runtime data, not just configuration reviews.** Permiso traces each agent past the MCP and CLI layer to the actual infrastructure role it assumes — making unused scope visible and actionable.

THEME 04 DEFEND

PERMISO

Agent Runtime Monitoring

2,847	34	6	7 min
SESSIONS RECORDED · 90D	CLASSIFIERS FIRED	OFF-BASELINE ANOMALIES	AVG. SESSION DURATION

FLAGGED BEHAVIORS

ACME-DataSync-Agent

MEDIUM

Called a sub-agent outside its registered scope; **exfiltration classifier fired.** Session recorded and recorded and preserved.

Copilot-HRAssist

REVIEW

Off-baseline spike: **3× normal tool-call volume** in a single session. No exfiltration confirmed; requires review.

- 1 agent invoked another agent dynamically — **agent-spawning-agent pattern** recorded in the recorded in the Universal Identity Graph.

- **Agent kill-switch** available for sanctioned managed agents — containment the moment moment anomalous behavior is confirmed.

BEHAVIORAL TRUTH

Config scanning tells you what an agent may do. Permiso's runtime engine tells you what it **actually did** — every tool call and sub-agent invocation, tied back to the initiating identity. initiating identity.

ADDITIONAL FINDINGS

MFA-Related Findings

• HIGH

CLEAREST ACTIONABLE OUTLIER

Sandra.Mitchell@acme-inc.com

Authenticating with **SMS-based MFA** — the weakest available factor and a known phishing / SIM-swap target.
target.

• MEDIUM

Kevin.Harrington@acme-inc.com

Okta MFA Multiple Verification Deny — repeated denied prompts consistent with possible MFA-fatigue activity.
fatigue activity.

RECOMMENDATION

Ensure **Sandra.Mitchell** moves to strong, phishing-resistant MFA resistant MFA factors such as **Okta Verify FastPass** or **FIDO2 / FIDO2 / WebAuthn.**

Highest-Impact Remediation Plan

PRIORITY 1

Clean up high-blast-radius service principals principals

- Assign owners; disable dormant SPs
- Remove over-privileged Graph permissions
- Rotate credentials

PRIORITY 2

Tighten privileged access governance

- Require approval for Global Admin / Owner activation activation
- Standardize justifications
- Enforce least privilege

PRIORITY 3

Control sensitive data to SaaS / AI

- Confirm sanctioned destinations
- Apply DLP allow-listing
- Block uploads to unsanctioned AI platforms

EXPECTED IMPACT

Remediating a small number of high-blast-radius identities delivers the **greatest posture improvement with the least operational effort.**

FINAL ASSESSMENT

PRIVILEGED ACCESS

Frequent but mostly attributable to known admin identities — **governance controls needed.**

NON-HUMAN IDENTITIES

Most urgent posture issue — ownerless / / dormant service principals with admin blast blast radius.

SENSITIVE DATA SHARING

128 public-sharing exposures with notable AI notable AI / SaaS destinations.

The fastest path to measurable risk reduction: **remediate a small set of privileged service principals** and enforce stronger stronger governance around privileged activation and sensitive-data movement.