Sabiki | AIRM
AGENTIC IDENTITY RISK MANAGEMENT

SAMPLE REPORT
DATA ANONYMISED

NON-HUMAN IDENTITY RISK REPORT · TECHNICAL PROFILE

Every identity, *measured*.

The complete technical profile of all 1,782 non-human identities in this tenant — blast radius, ownership, credential age, and exactly how each severity is calculated.

1,782	96	501	27
IDENTITIES PROFILED	CRITICAL BLAST RADIUS	WITHOUT AN ACCOUNTABLE OWNER	EXPIRED OR AGEING CREDENTIALS

02 August 2026 · Scan via Microsoft Graph API
Agentless · Read-only

This report is a snapshot — the live dashboard is not.
portal.sabikisecurity.com

METHODOLOGY

How every severity is *calculated*

Every identity is scored the same way in every tenant — three weighted components, assessed from read-only Graph API evidence. Nothing is hand-tuned per client.

30%

STATIC

What the identity **holds**: permission scope, consent breadth, publisher trust, credential hygiene. Changes only when grants change.

40%

BEHAVIOURAL

What the identity **does**: authentication patterns, resources reached, volume and timing — assessed against six behavioural signals.

30%

ANOMALY

How the identity **changes**: scan-over-scan deviation from its own established pattern, flagged by the Anomaly Intelligence Engine.

Blast-radius bands — what each level means

BAND	CRITERIA (PERMISSION REACH)	THIS TENANT
● CRITICAL	Tenant-wide read/write on mail, files or directory; can modify other applications' access; or privileged role held.	96 · 5%
● MEDIUM	Broad read on one workload, or write access scoped to specific sites, mailboxes or groups.	71 · 4%
● LOW	Narrow, scoped grants — a single calendar, profile read, sign-in only, or no standing consent.	1,615 · 91%

⚠ **The priority class is quiet-critical:** full capability, zero anomaly. It never trips a traditional alert, and it is devastating if its credentials are compromised. All six priority findings in this tenant are of this class.

EVIDENCE BASIS

Microsoft Graph API, agentless, read-only. Nothing is installed and nothing is changed. Copilot activity is read from the tenant's own audit log over a rolling 30-day window.

THE POPULATION

1,782 identities, *classified*

Every automated login in the tenant, grouped by what it is, what it can reach, and how it got its access.

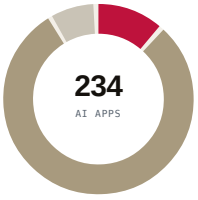
Blast radius

ALL 1,782 IDENTITIES

Critical	96	5%
Medium	71	4%
Low	1,615	91%

AI apps by origin

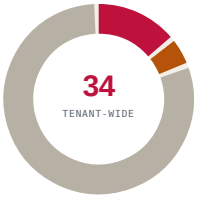
ALL 234 AI APPLICATIONS



Third-party consented	28	12%
Copilot Studio (internal)	187	80%
Microsoft first-party	19	8%

Consent scope

GRANT SCOPE · ALL 234 AI APPS



Tenant-wide (all users)	34	15%
Single user	12	5%
No standing consent	188	80%

What the 96 critical-blast-radius identities are

CATEGORY	EXAMPLES IN THIS TENANT	REVIEW POSTURE
External AI apps	Perplexity (×2), ChatGPT, Claude for Office, Quill AI Prod	Priority findings — decide now
Backup & migration tools	Veeam, Spanning, CodeTwo	Legitimate broad access — same review, lower urgency
IT-admin utilities	PnP PowerShell App, PDF utilities	Rotate credentials; confirm ownership
Security tooling	ShieldPoint Identity Protection, MFA Push Notification	Confirm admin consent was intentional
Microsoft first-party	Exchange, SharePoint service principals	Broad by design — excluded from findings

The critical tail is mostly not AI. Backup, migration and admin tools legitimately need broad access — but they carry the same risk profile as an unreviewed AI app and belong in the same ownership, credential and review regime. The full 1,782-row inventory export accompanies this report.

FINDINGS DETAIL

The critical tail, *item by item*

Six priority findings, three admin-consent validations, and the credential-hygiene queue — everything below reconciles with the Executive Summary. Reach counts are illustrative pending portal fields (214 staff assumed).

#	IDENTITY	CONSENT	FIRST SEEN	BLAST RADIUS — COUNTED	SEVERITY
1	**SalesIntel Sync — "Directory Login"**	Tenant-wide	—	1,782 identities · 214 contact lists · watchlist match	CRITICAL
2	**Perplexity**	Tenant-wide	17 Jun 2026	214 mbx r/w+send · ~38.4k files · 234 apps	CRITICAL
3	**ChatGPT**	Tenant-wide	17 Jun 2026	214 mbx r/w+send · ~38.4k files · 234 apps	CRITICAL
4	**Claude for Office**	Admin, tenant-wide	17 Jun 2026	214 mbx read · ~38.4k files · 234 apps	CRITICAL
5	**Quill AI Prod**	Tenant-wide	17 Jun 2026	~38.4k files r/w · 234 apps · unrecognised	CRITICAL
6	**Perplexity (Teams)**	Tenant-wide	—	214 mbx read · ~38.4k files read · duplicate	CRITICAL

Admin consents to validate

3

Claude for Office — privileged authentication administrator (auth.admin@client.example) · **ShieldPoint Identity Protection** — global administrator (global.admin-1@client.example) · **MFA Push Notification** — global administrator (global.admin-2@client.example).

What to do. Confirm each was intentional; require a second approver for future tenant-wide consent.

Credential hygiene queue

27

27 identities run on expired or unrotated credentials. At least one — **PnP PowerShell App** — pairs an expired credential with **critical** blast radius: the highest-priority rotation in the tenant.

What to do. Rotate critical-access credentials first; set a standing rotation policy.

Ownership & governance counts

COUNT OF IDENTITIES · THIS SCAN

APPENDIX

Definitions & *reconciliation*

Every term used in this suite, defined once — so the numbers reconcile across all five reports, because they are the same numbers.

TERM	DEFINITION
Non-human identity	Any login that is not a person: service accounts, app registrations, OAuth-connected apps, connectors, AI agents and Copilots.
Blast radius	The damage an identity could do if compromised, measured from the permissions it holds — independent of behaviour.
Quiet-critical	Critical blast radius with no anomalous behaviour. Invisible to activity-based alerting; the priority review class.
Tenant-wide consent	A grant approved for every user in the organisation — one approval, everyone's data.
Unowned identity	No accountable person recorded — the creator has left or was never captured.
Watchlist match	The application is flagged by name on Sabiki's threat-intelligence register of apps associated with data-harvesting, over-permissioning or abuse.
Labelled-sensitive	A file carrying a Microsoft sensitivity label. "Zero labelled reads" means Copilot touched no such file in the audit window.
Behavioural signals	Six monitored patterns: Dormant Identity Activated · Auth Method Change · New Resource Access · Off-Hours Auth · Auth Volume Spike · Impersonation Spike.

RECONCILIATION

1,782 total = 234 AI applications + 1,548 other non-human identities. 96 critical = 6 priority findings + security/backup/admin tooling + Microsoft first-party (excluded from findings by design). 501 unowned includes 61 critical. All five reports in this suite draw from this single scan.

COMPANION REPORTS

Executive Summary (board edition, 4pp) · Executive Security Summary (full, 11pp) · Weekly Operations Summary (3pp) · Compliance Framework Report (EU AI Act sample, 4pp) · Identity Inventory Export (CSV, 1,782 rows).

CONTINUOUS MONITORING IS RUNNING

Every number in this report is re-measured on every scan. The next edition shows *movement* — what appeared, what was resolved, what drifted.