

M365 × Azure Security Scan

MICROSOFT CLOUD SECURITY POSTURE

Know your exposure.
Prioritize what to fix next.

Turn Microsoft 365 and Azure security evidence into prioritized findings, practical recommendations and verifiable follow-up. Give security and platform teams a shared view of posture, coverage and remediation progress.



Assess connected Microsoft services

Review configuration and supported security evidence with read-only collection.



Connect findings to action

See severity, affected resources, recommendations and verification steps.



Show progress with evidence

Compare assessments and export detailed PDF, CSV and JSON reports.

CAPABILITIES

A connected view of Microsoft risk.

Bring identity, collaboration, device and Azure configuration evidence into one assessment workspace. Review the finding, the affected object and the action needed to improve posture.

CAPABILITY	WHAT IT ENABLES
Entra ID	Review authentication configuration, MFA registration, privileged roles, application consent and credential expiry. Identify identity configuration issues and access risks to investigate.
Exchange Online	Assess forwarding, audit and delegation settings through supported read-only collection. Review mail configuration that can expose information or weaken oversight.
Teams & sharing	Assess Teams policies and SharePoint or OneDrive sharing configuration. Bring collaboration controls and external sharing into the security review.
Intune	Review available device and compliance evidence from the connected tenant. Understand which managed-device observations need follow-up.
Azure	Assess connected subscriptions and supported resource configuration, including Storage, Key Vault and AKS checks. Prioritize cloud configuration findings against identified resources.
Microsoft Defender	Collect enabled recommendations, alerts and vulnerability assessment evidence, including CVEs and provider fixes. Connect provider-reported vulnerabilities to resources and next actions.

✓ Coverage is part of the result

Dataset access depends on approved permissions, connected subscriptions and active Microsoft service plans. Missing or incomplete evidence is shown as not assessed, with reasons and steps to complete coverage.

IN PRACTICE

From a finding to a verified result.

Prioritize the work, document the decision and use a later assessment to verify improvement.

- 01

Connect and assess
Choose the tenant and authorized Azure subscriptions. Run manually or schedule recurring assessments.
- 02

Investigate in context
Filter findings and inventory, search CVEs and inspect affected identities, applications, devices and resources.
- 03

Review the remediation
Use recommendations and verification steps. Route proposals to a different approving actor; your team applies the change.
- 04

Rescan and report
Compare runs to separate verified improvements, regressions, new observations and lost coverage. Export the evidence.

WHERE IT HELPS

Security leadership	Platform owners	Risk & assurance
Review posture, priority actions and the coverage behind the assessment.	Work from affected objects, recommendations and verification steps.	Use scoped reports and comparisons to track evidence of improvement.

Add identity context to the investigation

When connected to Protect Identity IGA, selected Entra identities can be linked through immutable identifiers to accessible role, organization and owner context. Access certification remains in IGA; privileged asset access remains in GovPAM.

Configuration assessment is read-only. Vulnerability evidence comes from enabled Microsoft Defender assessments; the product does not launch an active host or network penetration test.

YOUR NEXT STEP

Turn your tenant into an action plan.

Review the product against your Microsoft environment, assessment priorities and evidence requirements.

01 Set the assessment scope

Choose Microsoft services, authorized Azure subscriptions and the read access to review.

02 Follow a priority finding

Explore severity, evidence, affected resources, recommendations and verification.

03 Review the report

See the executive summary, detailed observations, coverage gaps and remediation progress.

Add security assessment on your terms.

Install M365 x Azure Security Scan as a separate subscribed product or alongside IGA and GovPAM. Keep assessment evidence in its dedicated customer deployment and database.

Each customer installation has its own service configuration, state, databases and keys. Choose one, two or all three products, with separate subscriptions.

LET'S PLAN YOUR DEMONSTRATION

Book a security scan demonstration

Make posture visible. Make remediation measurable.

sales@protectidentity.co.za

Collection requires tenant administrator consent and relevant Microsoft entitlements. Azure scope and service permissions are explicitly selected; Microsoft policy changes are performed by your team.