

Executive report

Synthetic example - no observations

Executive report generated Sep 24, 2026, 12:00 UTC

Planning report, not an invoice. Azure values are preview estimates. Prices are USD scenarios, excluding tax and discounts.

Executive summary

Unique identities	Sources included	Sources skipped
0	0 / 0	0

Azure identity records: 0

Collection at a glance

Dataset: Source coverage

Collected: 0 included; 0 skipped

Interpretation: Included means some data was accessible, not that every dataset succeeded.

Dataset: Repository inventory

Collected: 0

Interpretation: 0 with complete default-branch activity. Visible scope only.

Dataset: Provider billing datasets

Collected: Not recorded

Interpretation: Each product/period has separate status; unavailable is not zero. See coverage details.

Dataset: Daily usage detail

Collected: 0

Interpretation: Raw usage rows, not seats. Summarized separately below; do not add to monthly aggregates.

Dataset: Enablement estimates

Collected: Legacy identity-only estimate

Interpretation: Potential usage if enabled, not current charges. Two product rows can describe the same person.

Collected rows are evidence records, not licensed users. Usage subtotals keep source, scope, period, product and unit separate. Complete monthly usage summaries take precedence over overlapping daily detail; premium/AI breakdowns remain in the evidence appendix. Never add organizations to a parent enterprise or treat these amounts as invoices. Empty results and inaccessible datasets do not establish zero liability.

Source status

Collection warnings

Report-wide warning: SYNTHETIC DEMO: all organizations, people, repositories and billing amounts are fictional. Not customer evidence or an invoice.

Usage and security evidence

Current settings do not prove recent scans or payment. Reported billing usage is not an invoice. Missing data is not zero. Daily activity uses GitHub authored dates (excluding two automation accounts) and Azure committer dates (including automation).

Repository inventory

No rows collected. See collection evidence for availability.

Security settings

No rows collected. See collection evidence for availability.

Daily activity

No rows collected. See collection evidence for availability.

Reported billing usage

No rows collected. See collection evidence for availability.

Collection evidence

No rows collected. See collection evidence for availability.

Repository links

Recommended next steps

CIO decision brief

CIO decision summary

Readiness: No evidence

Summary: Azure DevOps: no evidence. There is insufficient collected evidence to assess this provider. Prioritize evidence validation and ownership before committing spend. No defensible savings estimate or overall security-health rating can be derived from this snapshot.

Methodology: Local rule-based analysis, not AI-generated advice. Based on the full collected provider scope, not screen filters. Priorities are suggested review order, not vulnerability severity. No savings, compliance conclusion or purchasing approval is established. Human review is required.

CIO evidence

Fact ID	Evidence
F1	Source coverage: 0 included, 0 skipped; 0 observed provider identities, not licensed seats.
F2	Inventory: 0 distinct repositories observed; 0 with unavailable activity and 0 with unknown or missing security-setting evidence. Inventory completeness is not independently verified.
F3	Security review: 0 active repositories have at least one explicitly disabled collected setting. A disabled default setup does not rule out a custom pipeline; enablement is not scanning success.
F4	Activity review: 0 repositories have zero observed default-branch commits in their complete collected windows. Windows can differ; inactivity is not proof a repository or license is unnecessary.
F5	Financial evidence: 0 modeled pricing rows, 0 provider-count enablement estimates, 0 readable billing datasets of 0 requested, and 0 daily usage rows. Datasets and detail overlap; row counts are not seats. Modeled costs are not actual charges; billing usage is not an invoice or proof of payment.
F6	Collection evidence: 0 partial, unavailable or not-requested dataset checks. Uncollected data is unknown, not zero.

CIO recommendations

Priority: P1

Recommendation: Close evidence gaps before a purchasing decision

Owner: Platform owner and reporting owner

Horizon: Next 7 days

Fact IDs: F1, F2, F6

Action: Confirm intended source coverage and review unavailable datasets. Request an authorized read-only export where access is missing; do not grant broader privileges merely to complete this report.

Priority: P1

Recommendation: Reconcile modeled costs with entitlements and billing

Owner: FinOps and procurement

Horizon: Before renewal or purchase

Fact IDs: F1, F5

Action: Obtain per-product billable usage, Basic/Test Plans entitlements, included benefits, billing scope and contract prices. Validate organization-level identity deduplication before treating preview estimates as a purchase quantity.

Priority: P2

Recommendation: Measure security outcomes, not only enablement

Owner: Security engineering

Horizon: Next 30 days

Fact IDs: F2, F3

Action: Collect last successful scans, severity and age of open findings, remediation times and branch-policy coverage. Agree targets by repository criticality; current settings alone cannot establish effectiveness or compliance.

Priority: P2

Recommendation: Establish a repeatable baseline

Owner: Platform owner and FinOps

Horizon: Next reporting cycle

Fact IDs: F1, F4, F5

Action: Repeat the same source scope and date window after gaps are resolved. Compare authorized retained snapshots for usage, cost and remediation trends; this single snapshot does not establish improvement or savings.

Recommended collection

Dataset: Basic/Test Plans entitlements, included benefits and official billable committers

Decision supported: Establish actual purchase quantities and potential duplicate entitlements.

Access and limits: Review the collected billing snapshots and their coverage first. Seat entitlements and unresolved billing populations require an authorized owner export; this report does not establish complete license coverage.

Dataset: Invoices, billing scope, contract prices and discounts

Decision supported: Reconcile scenarios to actual spend; quantify savings only after eligibility and contractual review.

Access and limits: Billing-owner-approved export. Do not include payment details or credentials. Not collected by this feature.

Dataset: Last successful scans, finding severity/age and remediation times

Decision supported: Assess security effectiveness and prioritize remediation by business impact.

Access and limits: Existing security-report read access; collect aggregates, not source code or secret values. Not collected by this feature.

Dataset: Repository owners, business criticality and branch protection/policies

Decision supported: Assign accountability and distinguish justified exceptions from control gaps.

Access and limits: Existing repository metadata read access and owner confirmation. Not collected by this feature.

Dataset: Pipelines, Artifacts and parallel-job usage with entitlements

Decision supported: Assess non-security spend and utilization; keep compute/storage/AI usage separate from security licenses.

Access and limits: Existing usage-report access or authorized exports. Organization billing rows may cover some meters, but utilization and entitlement coverage are not established.

Resolve skipped sources, review identity matches, and verify official membership, product enablement and billable usage before making purchasing decisions. Costs are scenarios; overlapping counts are not an invoice total.

Cross-provider identities are not automatically merged. Skipped sources are excluded from totals.

Export notes

Unsupported PDF font characters appear as ?. CSV and HTML retain full Unicode text.

Executive report

Synthetic example - no observations

Executive report generated Sep 24, 2026, 12:00 UTC

Planning report, not an invoice. Observed GitHub activity is not licensed-seat inventory or confirmed billable usage. Prices are USD scenarios, excluding tax and discounts.

Executive summary

Unique identities	Sources included	Sources skipped
0	0 / 0	0

GitHub identity records: 0

Collection at a glance

Dataset: Source coverage

Collected: 0 included; 0 skipped

Interpretation: Included means some data was accessible, not that every dataset succeeded.

Dataset: Repository inventory

Collected: 0

Interpretation: 0 with complete default-branch activity. Visible scope only.

Dataset: Provider billing datasets

Collected: Not recorded

Interpretation: Each product/period has separate status; unavailable is not zero. See coverage details.

Dataset: Daily usage detail

Collected: 0

Interpretation: Raw usage rows, not seats. Summarized separately below; do not add to monthly aggregates.

Collected rows are evidence records, not licensed users. Usage subtotals keep source, scope, period, product and unit separate. Complete monthly usage summaries take precedence over overlapping daily detail; premium/AI breakdowns remain in the evidence appendix. Never add organizations to a parent enterprise or treat these amounts as invoices. Empty results and inaccessible datasets do not establish zero liability.

Source status

Collection warnings

Report-wide warning: SYNTHETIC DEMO: all organizations, people, repositories and billing amounts are fictional. Not customer evidence or an invoice.

Usage and security evidence

Current settings do not prove recent scans or payment. Reported billing usage is not an invoice. Missing data is not zero. Daily activity uses GitHub authored dates (excluding two automation accounts) and Azure committer dates (including automation).

Repository inventory

No rows collected. See collection evidence for availability.

Security settings

No rows collected. See collection evidence for availability.

Daily activity

No rows collected. See collection evidence for availability.

Reported billing usage

No rows collected. See collection evidence for availability.

Collection evidence

No rows collected. See collection evidence for availability.

Repository links

Recommended next steps

CIO decision brief

CIO decision summary

Readiness: No evidence

Summary: GitHub Enterprise: no evidence. There is insufficient collected evidence to assess this provider. Prioritize evidence validation and ownership before committing spend. No defensible savings estimate or overall security-health rating can be derived from this snapshot.

Methodology: Local rule-based analysis, not AI-generated advice. Based on the full collected provider scope, not screen filters. Priorities are suggested review order, not vulnerability severity. No savings, compliance conclusion or purchasing approval is established. Human review is required.

CIO evidence

Fact ID	Evidence
F1	Source coverage: 0 included, 0 skipped; 0 observed provider identities, not licensed seats.
F2	Inventory: 0 distinct repositories observed; 0 with unavailable activity and 0 with unknown or missing security-setting evidence. Inventory completeness is not independently verified.
F3	Security review: 0 active repositories have at least one explicitly disabled collected setting. A disabled default setup does not rule out a custom pipeline; enablement is not scanning success.
F4	Activity review: 0 repositories have zero observed default-branch commits in their complete collected windows. Windows can differ; inactivity is not proof a repository or license is unnecessary.
F5	Financial evidence: 0 modeled pricing rows, 0 provider-count enablement estimates, 0 readable billing datasets of 0 requested, and 0 daily usage rows. Datasets and detail overlap; row counts are not seats. Modeled costs are not actual charges; billing usage is not an invoice or proof of payment.
F6	Collection evidence: 0 partial, unavailable or not-requested dataset checks. Uncollected data is unknown, not zero.

CIO recommendations

Priority: P1

Recommendation: Close evidence gaps before a purchasing decision

Owner: Platform owner and reporting owner

Horizon: Next 7 days

Fact IDs: F1, F2, F6

Action: Confirm intended source coverage and review unavailable datasets. Request an authorized read-only export where access is missing; do not grant broader privileges merely to complete this report.

Priority: P1

Recommendation: Reconcile modeled costs with entitlements and billing

Owner: FinOps and procurement

Horizon: Before renewal or purchase

Fact IDs: F1, F5

Action: Obtain Enterprise seat assignments, official product-billable committer counts, billing scope and contract prices. Separate Enterprise seats, Code Security and Secret Protection; observed authors are not a billing population.

Priority: P2

Recommendation: Measure security outcomes, not only enablement

Owner: Security engineering

Horizon: Next 30 days

Fact IDs: F2, F3

Action: Collect last successful scans, severity and age of open findings, remediation times and branch-policy coverage. Agree targets by repository criticality; current settings alone cannot establish effectiveness or compliance.

Priority: P2

Recommendation: Establish a repeatable baseline

Owner: Platform owner and FinOps

Horizon: Next reporting cycle

Fact IDs: F1, F4, F5

Action: Repeat the same source scope and date window after gaps are resolved. Compare authorized retained snapshots for usage, cost and remediation trends; this single snapshot does not establish improvement or savings.

Recommended collection

Dataset: Enterprise seats, outside collaborators and official billable committers

Decision supported: Establish actual purchase quantities and potential duplicate entitlements.

Access and limits: Review the collected billing snapshots and their coverage first. Seat entitlements and unresolved billing populations require an authorized owner export; this report does not establish complete license coverage.

Dataset: Invoices, billing scope, contract prices and discounts

Decision supported: Reconcile scenarios to actual spend; quantify savings only after eligibility and contractual review.

Access and limits: Billing-owner-approved export. Do not include payment details or credentials. Not collected by this feature.

Dataset: Last successful scans, finding severity/age and remediation times

Decision supported: Assess security effectiveness and prioritize remediation by business impact.

Access and limits: Existing security-report read access; collect aggregates, not source code or secret values. Not collected by this feature.

Dataset: Repository owners, business criticality and branch protection/policies

Decision supported: Assign accountability and distinguish justified exceptions from control gaps.

Access and limits: Existing repository metadata read access and owner confirmation. Not collected by this feature.

Dataset: Actions, Packages and Copilot usage with entitlements

Decision supported: Assess non-security spend and utilization; keep compute/storage/AI usage separate from security licenses.

Access and limits: Existing usage-report access or authorized exports. Organization billing rows may cover some meters, but utilization and entitlement coverage are not established.

Resolve skipped sources, review identity matches, and verify official membership, product enablement and billable usage before making purchasing decisions. Costs are scenarios; overlapping counts are not an invoice total.

Cross-provider identities are not automatically merged. Skipped sources are excluded from totals.

Export notes

Unsupported PDF font characters appear as ?. CSV and HTML retain full Unicode text.