



Monthly executive summary | Prepared: 24 October 2026 | Overall risk: Moderate

Key Metrics

Devices Monitored

24

Active sample endpoints

Threats Detected

12

Blocked / resolved detections

Quarantine Items

18

Messages held for review

Policy Violations

3

Configuration exceptions

Secure Score

84%
CURRENT

Previous month
72%
+12 pp
month-on-month

Sample Microsoft Secure Score. A posture indicator, not a guarantee against an incident.

Risk Overview

ELEVATED 1

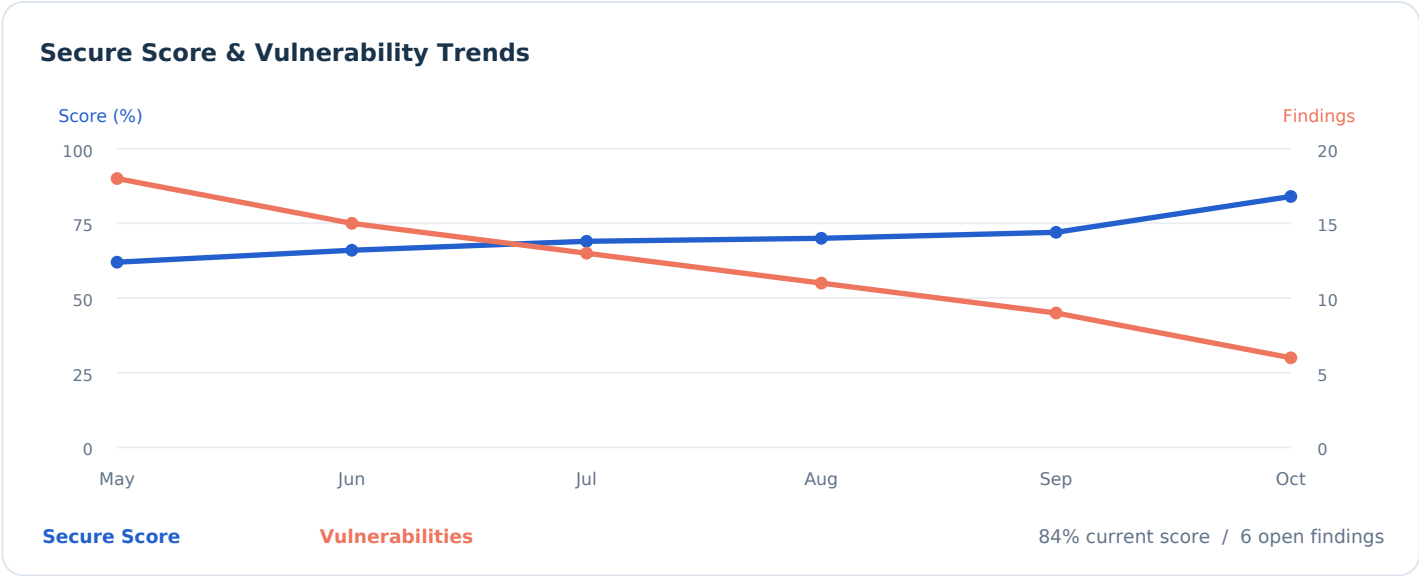
MODERATE 2

LOW 3

INCIDENTS THIS MONTH: 2
Both closed | 1 fewer than September

OPEN VULNERABILITY FINDINGS: 6
3 fewer than September | 1 elevated

Monthly Trend Analysis



All values are invented for demonstration. Detection, email, incident and vulnerability counts describe different record types and should not be added together.



Monthly Intake Summary

Example Advisory Group | October 2026

SAMPLE / FICTIONAL DATA

A stronger baseline. A practical next step.

The fictional organisation operates 24 monitored endpoints. Security posture improved from 72% to 84% after seven configuration improvements. Six vulnerability findings remain open, with the gateway finding requiring the earliest action.

Changes Made

- 01 Strengthened sign-in requirements for privileged accounts.
- 02 Reviewed conditional access coverage and documented exceptions.
- 03 Enabled a consistent endpoint firewall configuration.
- 04 Applied an agreed attack surface reduction baseline.
- 05 Tightened external sharing and guest-access defaults.
- 06 Reviewed email protection and outbound notification settings.
- 07 Validated device inventory and assigned owners to follow-up actions.

Accepted Risks

One legacy meeting-room device remains on a restricted network while replacement is arranged. The fictional client accepted this temporary position until 15 November 2026.

Deferred Actions

The legacy VPN gateway update requires a coordinated maintenance window. External administration is to be restricted immediately, with the update targeted for 31 October 2026.

Next Month Steps

- Verify completion of the gateway remediation and repeat the exposure check.
- Close the endpoint update gaps and recheck the six open findings.
- Review guest access with the business owner and confirm device replacement.

Fictional approval record and dates. This sample demonstrates reporting structure; it is not evidence of work performed for a real client.



Risk Heatmap

MODERATE

Secure Score 84%. Change +12 percentage points from the previous month.

ELEVATED	Prioritise and validate remediation	1
MODERATE	Schedule within the agreed patch cycle	2
LOW	Track and resolve with routine hardening	3

CVSS / EPSS Distribution

Six fictional vulnerability records. Values are sample estimates, not live feed data.

	Low	Medium	High	Critical
EPSS probability				
10-100%	0	0	1	0
1-<10%	0	1	0	0
0.1-<1%	1	1	0	0
<0.1%	2	0	0	0

CVSS technical severity bands

Top Vulnerabilities (CVSS Ranked)

Observed sample range: 2.8-8.1. No critical findings in this example.



Posture Summary

Overall posture is Moderate: 1 elevated, 2 moderate and 3 low findings remain. The legacy remote-access gateway is the first priority. Endpoint application updates follow, with the lower-severity items assigned to routine hardening. A stronger Secure Score does not remove the need to resolve exposed vulnerabilities.

CVSS describes technical severity. EPSS estimates exploitation likelihood for applicable published vulnerabilities. These fictional IDs and probabilities illustrate the layout only; they are not real CVEs or EPSS predictions.



Top Vulnerabilities & Remediation Roadmap

Six fictional findings, ranked by technical severity. Due dates and ownership are example planning data. Record IDs are internal sample references, not published CVE identifiers.

F-01 Legacy remote-access gateway CVSS 8.1 EPSS 12.00% 1 gateway Restrict administration and apply the validated vendor update.	ELEVATED TARGET 31 Oct
F-02 Browser update gap CVSS 6.5 EPSS 2.40% 3 endpoints Apply current browser updates; verify restart and version.	MODERATE TARGET 28 Oct
F-03 Document reader update gap CVSS 5.3 EPSS 0.80% 2 endpoints Deploy the approved reader update and repeat the check.	MODERATE TARGET 07 Nov
F-04 Unused local service CVSS 3.7 EPSS 0.10% 1 endpoint Remove the unused service after owner validation.	LOW TARGET 15 Nov
F-05 Legacy TLS configuration CVSS 3.1 EPSS 0.05% 1 gateway Retire the legacy setting after compatibility checks.	LOW TARGET 15 Nov
F-06 Wireless firmware baseline CVSS 2.8 EPSS 0.02% 1 access point Stage the agreed firmware baseline in a change window.	LOW TARGET 20 Nov

Owner for sample remediation: IT service team. Business owner approves downtime. Verify completion with a fresh check; do not close a finding solely because a change was scheduled.



Environmental Risk Signals

An illustrative view of internet, identity, application, email, endpoint and credential exposure.

NE

Internet Exposure
2 reachable services
One sample administration service needs restriction.

ID

Identity Exposure
Privileged MFA enabled
Review guest access and the recorded exceptions.

AP

Application Exposure
6 open findings
1 elevated, 2 moderate and 3 low severity.

MA

Email Exposure
18 messages quarantined
12 related detections blocked or resolved.

EN

Endpoint Exposure
24 of 24 reporting
3 endpoints require browser-update follow-up.

CR

Credential Exposure
No sample match found
Limited demonstration dataset; continue monitoring.

External Exposure Assessment

External IP	203.0.113.42 (documentation-only address)
Sample host	gateway.example.test
Open ports	443/tcp - HTTPS 8443/tcp - administration
Review priority	Elevated - restrict administration exposure
Illustrative scan	24 October 2026, 10:00 AEST

Summary: the public HTTPS service is expected in this fictional environment. The administration service requires an agreed access restriction and the gateway update referenced in F-01. Retest after the change and record the result.

No systems were scanned to create this sample. The IP address is from a documentation range and the .test hostname is reserved for examples.



Supporting Artefacts

Synthetic evidence examples linked to the sample findings. These are generated illustrations, not screenshots or exports from a real client environment.

E-01 / Endpoint Update Review

Example asset	Observation	Reference
EXAMPLE - LAPTOP-02	Browser update pending	F-02
EXAMPLE - LAPTOP-07	Browser update pending	F-02
EXAMPLE - DESKTOP-03	Restart validation required	F-02

E-02 / External Exposure Snapshot

EXAMPLE DATA - NO NETWORK SCAN PERFORMED

Host: gateway.example.test | IP: 203.0.113.42

443/tcp open https expected public service

8443/tcp open admin restrict access [F-01]

Observed: 24 Oct 2026 10:00 AEST (fictional)

E-03 / Posture & Configuration Record

Current sample Secure Score: 84% | Previous: 72%

Privileged accounts: MFA control recorded as enabled

Exceptions awaiting review: 3 | Owner: example IT team

Reference: monthly intake summary and next-month plan

Evidence Handling in an Actual Engagement

Client evidence should be scoped, timestamped and linked to a specific observation. Access and retention are agreed for the engagement. Completion is supported by validation evidence, rather than an unverified status change.

SAMPLE REPORT. Every name, device, address, count, score, finding, approval and evidence record in this document is fictional. It is a format example, not an assurance or compliance certification.