AEGIS EIGHT
aegiseight.com

ASD Essentials assessment

Automated Google Workspace posture review, aligned to the ASD Essentials maturity model.

Achieved maturity

ML0

FREE TRIAL — one report per Google Workspace tenant. Subscribe to enable continuous monitoring and change-triggered alerts.

Organisation	Acme Workspace Pty Ltd
Contact	security@acme-workspace.com.au
Tenant ID	C03sample
Scan ID	sample-google-scan-001
Generated	27 June 2026 at 3:10 pm
Target maturity	ML2
Achieved maturity	ML0
Assessor	Aegis Eight automated assessment
Report version	1.0

Executive snapshot

Acme Workspace Pty Ltd · scan 2026-06-27 · remediation roadmap · full evidence in section 4.

OVERALL MATURITY

Achieved **ML0** against a target of **ML2** · **Target not met**

Essentials uses a weakest-link rule: your overall level is set by the lowest-scoring strategy, not the average.

ASSESSMENT LIMITATIONS & EVIDENCE GAPS

This report is an automated Google Admin APIs posture review at the ASD **Fair** evidence tier — configuration reviewed via API responses, not interactive device testing. It is suitable for prioritising remediation but is not a substitute for a formal on-site or IRAP assessment.

Tier	What this means for you
Fair	Automated scan — live tenant configuration via Google Admin APIs. This report operates here.
Good	Applied-state verification, sign-in analysis, or RSoP exports — available via attestation or upcoming collectors (see "Stronger evidence (Good tier)" notes in section 4).
Excellent	Simulated control testing (live sentinel sign-in tests) — Microsoft 365 only today; not automated for Google Workspace.

This scan has **7 no-visibility findings** and **11 poor-evidence findings**. Scope exclusions and next steps are listed in section 2.

- Evidence is collected from Admin SDK, Reports API, and Chrome Management API responses (Fair tier per ASD process guide) — devices and policies were not interactively tested.
- ChromeOS and Chrome browser policy signals are automated. Windows and macOS endpoints managed outside Chrome require third-party MDM or manual evidence.
- Full scope and limitations in section 2.

Top risks

Business email compromise risk (3) · CRITICAL · BLOCKS ML1
Weak MFA coverage is the leading cause of account takeover and is a baseline requirement for most cyber-insurance policies.

Unpatched device exposure (8) · CRITICAL · BLOCKS ML1
Unpatched operating systems are a primary ransomware entry point and can affect cyber-insurance eligibility.

Phishing-vulnerable authentication · HIGH
Weak MFA coverage is the leading cause of account takeover and is a baseline requirement for most cyber-insurance policies.

Privileged-account takeover risk · INFO · BLOCKS ML1
Excess or unmonitored admin access widens the blast radius of any breach and is a common audit and insurer finding.

Incomplete posture assessment (2) · INFO · BLOCKS ML1
Without application control, untrusted executables can run — a key ransomware vector and a frequent insurer question.

REMEDIATION ROADMAP

Path from ML0 to ML2: **0 of 9 completed · 8 in Immediate blockers to ML1 · baseline scan**. Future scans will show progress as actions are completed. Full checklist.

Remediation roadmap

> **0 of 9 completed · 8 in Immediate blockers to ML1 · baseline scan** · Mark actions complete in your runbook; the next scan will track progress.

A single prioritised path from ML0 to ML2. Complete ML-tier blockers first. Effort colours: **Quick fix** · **Multi-step** · **Day's work** · **Project**. Detailed recommendations are in section 4.

Immediate blockers to ML1

8 actions · Scale: Half day to one day

- [ ] **Register MFA for 1 user · Blocks ML1**
  Quick fix
- [ ] **Remediate 1 non-compliant device · Blocks ML1**
  Multi-step
- [ ] **Block privileged sign-ins from untrusted networks · Blocks ML1**
  Day's work
- [ ] **Macro-borne malware risk · Blocks ML1**
  Day's work
- [ ] **Protect missing Google Workspace workloads · Blocks ML1**
  Multi-step
- [ ] **Provide vulnerability scanning evidence · Blocks ML1**
  Day's work
- [ ] **Register MFA for affected users · Blocks ML1**
  Quick fix
- [ ] **Restore scan permissions and re-run assessment · Blocks ML1**
  Multi-step

Additional steps to ML2

1 action · Scale: Half day to one day

- [ ] **Forward security logs to a central SIEM**
  Day's work

Cyber risk register

Unique risks grouped by theme (max 20 shown). Effort matches the roadmap legend above. Per-control evidence is in section 4.

Severity	Priority	Risk	Why it matters	Effort	ML	Cnt	Status
Critical	Immediate	**Business email compromise risk**	One user can sign in to Google Workspace with only a password, increasing the likelihood of account takeover, email fraud, and access to Gmail and Drive data.	Quick fix	**ML1**	1	Open
Critical	Immediate	**Unpatched device exposure**	One managed device reports non-compliant and may be missing required security updates or configuration — confirm patch state with vulnerability management evidence.	Multi-step	**ML1**	1	Open
Critical	Immediate	**Unpatched device exposure**	One managed device reports non-compliant and may be missing required security updates or configuration — confirm patch state with vulnerability management evidence.	Multi-step	**ML1**	1	Open
Critical	30 days	**Business email compromise risk**	One user can sign in to Google Workspace with only a password, increasing the likelihood of account takeover, email fraud, and access to Gmail and Drive data.	Quick fix	—	1	Open
Critical	30 days	**Unpatched device exposure**	One managed device reports non-compliant and may be missing required security updates or configuration — confirm patch state with vulnerability management evidence.	Multi-step	—	1	Open
Critical	30 days	**Unpatched device exposure**		Multi-step	—	1	Open

			One managed device reports non-compliant and may be missing required security updates or configuration — confirm patch state with vulnerability management evidence.				
Critical	30 days	**Unpatched device exposure**	One managed device reports non-compliant and may be missing required security updates or configuration — confirm patch state with vulnerability management evidence.	Multi-step	—	1	Open
Critical	30 days	**Unpatched device exposure**	One managed device reports non-compliant and may be missing required security updates or configuration — confirm patch state with vulnerability management evidence.	Multi-step	—	1	Open
High	30 days	**Phishing-vulnerable authentication**	SMS, voice, or email OTP defaults are easier to intercept than authenticator apps, FIDO2 keys, or Windows Hello — weakening protection against targeted phishing.	Day's work	—	1	Open
Info	Monitor	**Business email compromise risk**	Can sign in to Google Workspace with only a password, increasing the likelihood of account takeover, email fraud, and access to Gmail and Drive data.	Quick fix	**ML1**	1	Open
Info	Monitor	**Privileged-account takeover risk**	Privileged accounts may be able to sign in from untrusted locations — the same paths attackers use for initial access.	Day's work	**ML1**	1	Open
Info	Monitor	**Delayed breach detection risk**	Without confirmed central logging of sign-in and privileged-access events, an attacker may operate inside Gmail, Drive, and admin tools longer before detection — weakening incident response and insurance evidence.	Day's work	—	1	Open
Info	Monitor	**Unpatched device exposure**	Chrome Management compliance is a proxy for patch state, not direct proof of missing updates or CVEs. Provide vulnerability scanning or MDM evidence to demonstrate patch cadence against ASD windows.	Day's work	**ML1**	1	Open
Info	Monitor	**Unpatched device exposure**	Chrome Management compliance is a proxy for patch state, not direct proof of missing updates or CVEs. Provide vulnerability scanning or MDM evidence to demonstrate patch cadence against ASD windows.	Day's work	**ML1**	1	Open
Info	Monitor	**Data loss and recovery risk**	One or more critical workloads (Gmail, Drive) lack demonstrated backup coverage — increasing recovery time after ransomware or accidental deletion.	Multi-step	**ML1**	1	Open
Info	Monitor	**Incomplete posture assessment**	This control could not be assessed because required Google API data was not collected — the report may understate risk until permissions are restored and the scan re-run.	Multi-step	**ML1**	1	Open
Info	Monitor	**Macro-borne malware risk**	Office macros from untrusted sources are a common ransomware and phishing delivery path.	Day's work	**ML1**	1	Open
Info	Monitor	**Macro-borne malware risk**	Office macros from untrusted sources are a common ransomware and phishing delivery path.	Day's work	—	1	Open
Info	Monitor	**Macro-borne malware risk**	Office macros from untrusted sources are a common ransomware and phishing delivery path.	Day's work	—	1	Open
Info	Monitor	**Incomplete posture assessment**	This control could not be assessed because required Google API data was not collected — the report may understate risk until permissions are restored and the scan re-run.	Multi-step	**ML1**	1	Open

20 open findings total · 20 unique risk groups.

Executive dashboard

Achieved **ML0** to target **ML2** · **Target not met**

Progress toward ML2

Multi-factor authentication	50% effective · achieved ML0	3/6
Restrict administrative privileges	60% effective · achieved ML0	3/5
Patch operating systems	0% effective · achieved ML0	0/3
Patch applications	0% effective · achieved ML0	0/3
Regular backups	0% effective · achieved ML0	0/1
Application control	0% effective · achieved ML0	0/1
Configure Microsoft Office macros	0% effective · achieved ML0	0/2
User application hardening	0% effective · achieved ML0	0/1

ASSESSMENT EVIDENCE

4 Google API sources queried · 16 of 27 findings backed by live tenant data · Assessment performed 20 June 2026, 12:00 am (UTC). Full audit trail available on request via the auditor PDF.

1. Executive summary

Aegis Eight conducted an automated review of Acme Workspace Pty Ltd's Google Workspace tenant against the ASD Essentials maturity model. The overall achieved maturity level is **ML0** against a target of **ML2**. The tenant does not currently meet the target maturity level based on automated signals.

> **WHY YOUR OVERALL MATURITY IS ML0**
>
> Essentials maturity follows the **weakest-link rule**: your overall level is set by the lowest-scoring mitigation strategy, not the average. Findings rated Effective elsewhere do not raise the overall number until every strategy reaches the next maturity level together.
>
> **Blocking ML1:** all eight mitigation strategies are currently at ML0. Address the worst-performing controls first.

Mitigation strategy summary

Mitigation strategy	Achieved	Worst outcome
Multi-factor authentication	ML0	Ineffective
Restrict administrative privileges	ML0	No visibility
Patch operating systems	ML0	Ineffective
Patch applications	ML0	Ineffective
Regular backups	ML0	Not assessed
Application control	ML0	No visibility
Configure Microsoft Office macros	ML0	Not applicable
User application hardening	ML0	No visibility

Findings by outcome

Outcome	Findings
Effective	7
Alternate control	0
Ineffective	9
No visibility	7
Not implemented	0
Not applicable	3
Not assessed	1

2. Scope

Automated Essentials posture review of a Google Workspace tenant via read-only Admin SDK, Reports, and Chrome Management APIs under domain-wide delegation.

In scope

• Google Workspace directory users, 2-Step Verification enrollment, and Super Admin role assignments via Admin SDK.
• Sign-in audit reports (login activity metadata only) via the Reports API.
• ChromeOS device inventory and compliance via Chrome Management.
• Chrome browser policies (extension install, Safe Browsing, auto-update) via Chrome Management.
• Google Vault retention policies when Vault is licensed.

Out of scope (this automated pass)

• Gmail, Drive, Chat, Meet, and Calendar content — only directory and audit metadata.
• Windows and macOS patch posture unless managed through Chrome browser policies.
• Microsoft Office macro configuration — not applicable to native Google Docs.
• Third-party backup tooling, immutability/off-tenant copies, and signed-off DR exercise records — provide attestation to elevate evidence quality.
• Vulnerability scanner cadence, patch timeframes against ASD windows, and event log forwarding/retention.

Assessment limitations

• Evidence is collected from Admin SDK, Reports API, and Chrome Management API responses (Fair tier per ASD process guide) — devices and policies were not interactively tested.
• ChromeOS and Chrome browser policy signals are automated. Windows and macOS endpoints managed outside Chrome require third-party MDM or manual evidence.
• Configure Office macros does not apply to native Google Workspace tenants — findings are marked Not applicable.
• Google Vault backup posture is assessed when Vault is licensed; otherwise backup findings show no visibility or require attestation.
• Application control is assessed via Chrome extension install policies — not equivalent to AppLocker/WDAC on Windows.
• The scan is point-in-time. Continuous monitoring requires a subscription plan.

> **PERMISSIONS USED & DATA HANDLING**
>
> Aegis Eight accessed your Google Workspace tenant under **read-only Google Admin APIs permissions** granted via domain-wide delegation by your Super Administrator. No write, create, update, or delete permissions were requested or granted.
>
> • **Scopes used:** admin.directory.user.readonly, admin.directory.user.security, admin.directory.rolemanagement.readonly, admin.reports.audit.readonly, chrome.management.policy.readonly, chrome.management.reports.readonly (plus optional Vault scopes when licensed).
>
> • **Tenant isolation:** access is scoped to your tenant only. Multi-tenancy means Aegis Eight is deployed into many tenants, not that it reads across them.
>
> • **Retention:** scan signals and raw API responses are retained for 90 days (full payload), then reduced to hashes and summary metadata. Per-tenant shorter-retention overrides are available on request.
>
> • **Revocation:** Admin Console ’ Security ’ API controls ’ Domain-wide delegation ’ remove Aegis Eight Client ID. On request after revocation, all tenant scan data is purged within 30 days.
>
> Full details: aegiseight.com/security.

3. Methodology

This assessment follows the four-stage process described in the ASD Essentials assessment process guide (October 2024). Stages 1 (planning) and 2 (scope determination) are condensed into the automated tenant connection. Stage 3 (control assessment) is performed by querying Google Admin APIs for configuration evidence. Stage 4 (report development) is this document.

Evidence quality

The ASD process guide defines four evidence quality tiers. Automated Google Admin APIs collection operates at the "Fair" tier — reviewing system configuration through API responses rather than running scripts on individual devices. Every Fair-tier sub-control finding in this report carries the live API endpoint and the UTC timestamp at which it was queried, so the evidence chain is reproducible by an IRAP assessor without re-running the scan. Section 6 lists every query and maps each finding to its provenance. Where a finding can be uplifted to the Good tier by an additional collector, a "Stronger evidence (Good tier)" note is shown beneath the observation.

Tier	Description
Excellent	Testing a control with a simulated activity (e.g. attempting to run a test application to check application control rulesets).
Good	Reviewing the configuration of a system through the system's interface.
Fair	Reviewing a copy of a system's configuration (e.g. API responses, reports, screenshots). Aegis Eight's automated scan operates at this tier.
Poor	A policy or verbal statement of intent.

Assessment outcomes

Per the ASD guide, each control receives one of seven standardised outcomes. Aegis Eight applies these to each sub-control finding within a mitigation strategy. A mitigation strategy is only claimed at a maturity level when every sub-control at that level is rated "Effective" or "Alternate control".

4. Mitigation strategies

The eight ASD mitigation strategies are presented below. Each strategy includes sub-control findings with their assessment outcome, evidence quality, and observation. Affected account and device lists are in the appendix.

4.1 Multi-factor authentication

Achieved: **ML0** · Evidence: Good · 3/7 controls effective.

ML	Control	Outcome	Evidence	Observation
ML1	Multi-factor authentication is used to authenticate privileged users of important data repositories and online services.	Effective	Fair	All 2 privileged user(s) have MFA registered. Live query: https:/ / admin. googleapis. com-/ admin/ directory/ v1/ users at 2026-06-20 00:00:30Z Stronger evidence (Good tier): Sign-in log analysis (proves MFA was actually requested on real sign-ins)
ML1	Multi-factor authentication is used to authenticate the organisation's users of online	Ineffective	Fair	16/18 users (88.9%) have MFA registered against the Google Workspace tenant.

	services that process, store or communicate sensitive data.			*What this means: One user can sign in to Google Workspace with only a password, increasing the likelihood of account takeover, email fraud, and access to Gmail and Drive data.* Live query: https:/ / admin. googleapis. com-/ admin/ directory/ v1/ users at 2026-06-20 00:00:30Z Stronger evidence (Good tier): Sign-in log analysis (proves MFA was actually requested on real sign-ins)
ML1	Multi-factor authentication is used to authenticate users of online customer services that process, store or communicate sensitive customer data.	No visibility	Poor	Customer-facing services and any non-M365 identity providers are outside the visibility of this automated scan. *What this means: Can sign in to Google Workspace with only a password, increasing the likelihood of account takeover, email fraud, and access to Gmail and Drive data.*
ML2	Multi-factor authentication is used to authenticate unprivileged users of important data repositories and internal systems.	Ineffective	Fair	Registration: 88.9%, capability coverage: 94.4%. *What this means: One user can sign in to Google Workspace with only a password, increasing the likelihood of account takeover, email fraud, and access to Gmail and Drive data.* Live query: https:/ / admin. googleapis. com-/ admin/ directory/ v1/ users at 2026-06-20 00:00:30Z Stronger evidence (Good tier): Sign-in log analysis (proves MFA was actually requested on real sign-ins)
ML2	Successful and unsuccessful multi-factor authentication events are centrally logged.	Effective	Good	62 sign-in event(s) retrieved from Google Workspace over the last 7 day(s) (58 successful, 41 required MFA). Live query: https:/ / admin. googleapis. com/ admin/ reports-/ v1/ activity/ users/ all/ applications/ login at 2026-06-20 00:00:30Z
ML3	Multi-factor authentication is phishing-resistant.	Ineffective	Fair	0.0% of users have a phishing-resistant default method (authenticator, FIDO2, Windows Hello, passkey). *What this means: SMS, voice, or email OTP defaults are easier to intercept than authenticator apps, FIDO2 keys, or Windows Hello — weakening protection against targeted phishing.* Live query: https:/ / admin. googleapis. com-/ admin/ directory/ v1/ users at 2026-06-20 00:00:30Z Stronger evidence (Good tier): Sign-in log analysis (proves MFA was actually requested on real sign-ins)
ML1	Privileged users are actually challenged for MFA on real sign-ins (not just registered for MFA).	Effective	Good	8/8 privileged sign-ins required MFA over the last 7 day(s); no successful privileged sign-ins bypassed MFA. Live query: https:/ / admin. googleapis. com/ admin/ reports-/ v1/ activity/ users/ all/ applications/ login at 2026-06-20 00:00:30Z

Affected accounts and devices

• [ML1] Multi-factor authentication is used to authenticate the organisation's users of online services that process, store or communicate sensitive data. — 1 affected

• [ML2] Multi-factor authentication is used to authenticate unprivileged users of important data repositories and internal systems. — 1 affected

• [ML3] Multi-factor authentication is phishing-resistant. — 17 affected

Full lists are in the appendix at the end of this report.

Recommendations

• **[ML1]** Drive MFA registration above 95% — 2 user(s) still unregistered.

• **[ML1]** Provide evidence of MFA enforcement on any customer-facing application that handles sensitive data.

• **[ML2]** Push registration to at least 99% and ensure all users are MFA-capable.

• **[ML2]** Confirm Google Workspace sign-in logs are forwarded to a centralised log store (e.g. Sentinel, Splunk) with retention meeting ASD ML2 requirements.

• **[ML3]** Migrate users from SMS/voice/email defaults to authenticator app, FIDO2 security keys, or Windows Hello for Business.

4.2 Restrict administrative privileges

Achieved: **ML0** · Evidence: Fair · 4/6 controls effective.

ML	Control	Outcome	Evidence	Observation
ML1	Privileged accounts are strictly limited to only those required to administer the system.	Effective	Fair	2 effective Global Administrator(s) (2 direct user assignment(s), 0 group-based privileged assignment(s)); 4 total privileged role assignment(s) in Google Workspace. Live query: https:/ / admin. googleapis. com-/ admin/ directory/ v1/ roleAssignments at 2026-06-20 00:00:30Z Stronger evidence (Good tier): PIM activation history (distinguishes standing vs JIT-activated privilege) Requires PIM scopes and a tenant licensed for PIM
ML1	Privileged accounts are prevented from accessing the internet, email and web services.	No visibility	Poor	Network segmentation, conditional access, and policy enforcement for privileged accounts are not directly observable from the data collected. *What this means: Privileged accounts may be able to sign in from untrusted locations — the same paths attackers use for initial access.* Stronger evidence (Excellent tier): Live synthetic test (opt-in sentinel framework) Requires synthetic testing enabled in the dashboard or trial setup wizard
ML2	Privileged access is limited to that required for personnel to undertake their duties (ML2).	Effective	Fair	2 effective Global Administrator(s) (2 direct); ML2 expects no more than 3. Live query: https:/ / admin. googleapis. com-/ admin/ directory/ v1/ roleAssignments at 2026-06-20 00:00:30Z Stronger evidence (Good tier): PIM activation history (distinguishes standing vs JIT-activated privilege) Requires PIM scopes and a tenant licensed for PIM
ML2	Privileged user activities are centrally logged.	No visibility	Poor	Audit log forwarding and retention are not measured by this scan. *What this means: Without confirmed central logging of sign-in and privileged-access events, an attacker may operate inside Gmail, Drive, and admin tools longer before detection — weakening incident response and insurance evidence.*
ML3	Just-in-time administration is used for administering systems, applications and data repositories.	Effective	Fair	Effective Global Admin count (2, 2 direct) is within the ML3 expectation of no more than 2; verify PIM/just-in-time elevation is in use.

				Live query: https:/ / admin. googleapis. com- / admin/ directory/ v1/ roleAssignments at 2026-06-20 00:00:30Z Stronger evidence (Good tier): PIM activation history (distinguishes standing vs JIT-activated privilege) Requires PIM scopes and a tenant licensed for PIM
ML1	Inactive privileged accounts are identified and removed or disabled.	Effective	Fair	No Global Administrators were inactive (no sign-in 90+ days) in the user hygiene sample. Live query: https:/ / admin. googleapis. com- / admin/ directory/ v1/ users at 2026-06-20 00:00:30Z

Recommendations

• **[ML1]** Provide conditional access policy exports showing privileged accounts are blocked from non-admin workloads.

• **[ML2]** Confirm Google Workspace audit logs are shipped to a SIEM with adequate retention.

• **[ML3]** Confirm Google Workspace privileged access management is configured for time-bound, approval-based elevation.

4.3 Patch operating systems

Achieved: **ML0** · Evidence: Fair · 0/4 controls effective.

ML	Control	Outcome	Evidence	Observation
ML1	Missing-patch risk is tracked with vulnerability scanning (not inferred from Intune compliance alone).	No visibility	Poor	This scan does not collect CVE/KB age or scanner cadence — Intune compliance is a separate proxy finding below. *What this means: Chrome Management compliance is a proxy for patch state, not direct proof of missing updates or CVEs. Provide vulnerability scanning or MDM evidence to demonstrate patch cadence against ASD windows.* Stronger evidence (Good tier): Defender Vulnerability Management (KB / CVE / ASD patch-window age) Requires ThreatHunting. Read. All and Defender for Endpoint
ML1	Operating systems patch timeliness is assessed via Intune compliance as a proxy (not direct CVE/KB age).	Ineffective	Fair	Intune compliance used as a proxy for ASD patch timeframes — 5/6 devices (83.3%) report compliant against Intune policy; 1 non-compliant. *What this means: One managed device reports non-compliant and may be missing required security updates or configuration — confirm patch state with vulnerability management evidence.* Live query: https:/ / chromemanagement. googleapis. com- / v1/ customers/ my_customer/ devices- / chromeDevices at 2026-06-20 00:00:30Z Stronger evidence (Good tier): Intune deviceCompliancePolicyStates (per-device RSoP) Requires DeviceManagementManagedDevices. Read. All per-device RSoP query
ML2	ML2 patch timeframes are assessed via Intune compliance proxy (not direct vulnerability age).	Ineffective	Fair	5/6 devices (83.3%) report compliant against Intune policy; 1 non-compliant. *What this means: One managed device reports non-compliant and may be missing required security updates or configuration*

				— confirm patch state with vulnerability management evidence. Live query: https:/ / chromemanagement. googleapis. com- / v1/ customers/ my_customer/ devices- / chromeDevices at 2026-06-20 00:00:30Z Stronger evidence (Good tier): Intune deviceCompliancePolicyStates (per-device RSoP) Requires DeviceManagementManagedDevices. Read. All per-device RSoP query
ML3	ML3 patch timeframes are assessed via Intune compliance proxy (not direct vulnerability age).	Ineffective	Fair	5/6 devices (83.3%) report compliant against Intune policy; 1 non-compliant. *What this means: One managed device reports non-compliant and may be missing required security updates or configuration — confirm patch state with vulnerability management evidence.* Live query: https:/ / chromemanagement. googleapis. com- / v1/ customers/ my_customer/ devices- / chromeDevices at 2026-06-20 00:00:30Z Stronger evidence (Good tier): Intune deviceCompliancePolicyStates (per-device RSoP) Requires DeviceManagementManagedDevices. Read. All per-device RSoP query

Affected accounts and devices

• [ML1] Operating systems patch timeliness is assessed via Intune compliance as a proxy (not direct CVE/KB age). — 1 affected

• [ML2] ML2 patch timeframes are assessed via Intune compliance proxy (not direct vulnerability age). — 1 affected

• [ML3] ML3 patch timeframes are assessed via Intune compliance proxy (not direct vulnerability age). — 1 affected

Full lists are in the appendix at the end of this report.

Recommendations

• **[ML1]** Grant ThreatHunting.Read.All and enable Defender TVM, or provide third-party vulnerability evidence.

• **[ML1]** Investigate 1 non-compliant device(s); compliance gaps are a proxy signal, not proof of missing patches.

• **[ML2]** Raise device compliance to at least 95% for ML2.

• **[ML3]** Raise device compliance to at least 99% for ML3.

4.4 Patch applications

Achieved: **ML0** · Evidence: Fair · 0/4 controls effective.

ML	Control	Outcome	Evidence	Observation
ML1	Missing-patch risk is tracked with vulnerability scanning (not inferred from Intune compliance alone).	No visibility	Poor	This scan does not collect CVE/KB age or scanner cadence — Intune compliance is a separate proxy finding below. *What this means: Chrome Management compliance is a proxy for patch state, not direct proof of missing updates or CVEs. Provide vulnerability scanning or MDM evidence to demonstrate patch cadence against ASD windows.* Stronger evidence (Good tier): Defender Vulnerability Management (KB / CVE / ASD patch-window age)

	Requires ThreatHunting. Read. All and Defender for Endpoint			
ML1	Applications patch timeliness is assessed via Intune compliance as a proxy (not direct CVE/KB age).	Ineffective	Fair	Intune compliance used as a proxy for ASD patch timeframes — 5/6 devices (83.3%) report compliant against Intune policy; 1 non-compliant. *What this means: One managed device reports non-compliant and may be missing required security updates or configuration — confirm patch state with vulnerability management evidence.* Live query: https:/ / chromemanagement. googleapis. com- / v1/ customers/ my_customer/ devices- / chromeDevices at 2026-06-20 00:00:30Z Stronger evidence (Good tier): Intune deviceCompliancePolicyStates (per-device RSoP) Requires DeviceManagementManagedDevices. Read. All per-device RSoP query
ML2	ML2 patch timeframes are assessed via Intune compliance proxy (not direct vulnerability age).	Ineffective	Fair	5/6 devices (83.3%) report compliant against Intune policy; 1 non-compliant. *What this means: One managed device reports non-compliant and may be missing required security updates or configuration — confirm patch state with vulnerability management evidence.* Live query: https:/ / chromemanagement. googleapis. com- / v1/ customers/ my_customer/ devices- / chromeDevices at 2026-06-20 00:00:30Z Stronger evidence (Good tier): Intune deviceCompliancePolicyStates (per-device RSoP) Requires DeviceManagementManagedDevices. Read. All per-device RSoP query
ML3	ML3 patch timeframes are assessed via Intune compliance proxy (not direct vulnerability age).	Ineffective	Fair	5/6 devices (83.3%) report compliant against Intune policy; 1 non-compliant. *What this means: One managed device reports non-compliant and may be missing required security updates or configuration — confirm patch state with vulnerability management evidence.* Live query: https:/ / chromemanagement. googleapis. com- / v1/ customers/ my_customer/ devices- / chromeDevices at 2026-06-20 00:00:30Z Stronger evidence (Good tier): Intune deviceCompliancePolicyStates (per-device RSoP) Requires DeviceManagementManagedDevices. Read. All per-device RSoP query

Affected accounts and devices

• [ML1] Applications patch timeliness is assessed via Intune compliance as a proxy (not direct CVE/KB age). — 1 affected

• [ML2] ML2 patch timeframes are assessed via Intune compliance proxy (not direct vulnerability age). — 1 affected

• [ML3] ML3 patch timeframes are assessed via Intune compliance proxy (not direct vulnerability age). — 1 affected

Full lists are in the appendix at the end of this report.

Recommendations

• **[ML1]** Grant ThreatHunting.Read.All and enable Defender TVM, or provide third-party vulnerability evidence.

• **[ML1]** Investigate 1 non-compliant device(s); compliance gaps are a proxy signal, not proof of missing patches.

• **[ML2]** Raise device compliance to at least 95% for ML2.

• **[ML3]** Raise device compliance to at least 99% for ML3.

4.5 Regular backups

Achieved: **ML0** · Evidence: **Poor** · 0/1 controls effective.

ML	Control	Outcome	Evidence	Observation
ML1	Regular backups are performed, tested, and access-controlled per ASD maturity model.	Not assessed	Poor	Google Vault is not licensed or not enabled for this domain — Admin SDK returned no Vault coverage. *What this means: One or more critical workloads (Gmail, Drive) lack demonstrated backup coverage — increasing recovery time after ransomware or accidental deletion.*

Recommendations

• **[ML1]** If you use Google Vault, confirm it is enabled for Mail, Drive, and Groups. If you use a third-party backup product, provide the backup policy, retention schedule, last restore-test record, and backup administrator access list.

4.6 Application control

Achieved: **ML0** · Evidence: **Poor** · application control: insufficient Intune visibility.

ML	Control	Outcome	Evidence	Observation
ML1	Application control is implemented on workstations and servers per ASD maturity model.	No visibility	Poor	Intune device configuration profiles were not collected during this scan. *What this means: This control could not be assessed because required Google API data was not collected — the report may understate risk until permissions are restored and the scan re-run.*

Recommendations

• **[ML1]** Grant DeviceManagementConfiguration.Read.All and confirm Intune is licensed for the tenant.

4.7 Configure Microsoft Office macros

Achieved: **ML0** · Evidence: **Poor** · 0/3 controls effective.

ML	Control	Outcome	Evidence	Observation
ML1	Microsoft Office macros are configured per ASD maturity model (disabled or strictly controlled).	Not applicable	Poor	Office macro controls do not apply to a Google Workspace tenant using native Google Docs. *What this means: Office macros from untrusted sources are a common ransomware and phishing delivery path.*
ML2	Macros from the internet are blocked; only macros from trusted locations may run.	Not applicable	Poor	Office macro controls do not apply to a Google Workspace tenant using native Google Docs. *What this means: Office macros from untrusted sources are a common ransomware and phishing delivery path.*

ML3	Macro settings are centrally managed and verified across all Office applications.	Not applicable	Poor	Office macro controls do not apply to a Google Workspace tenant using native Google Docs. *What this means: Office macros from untrusted sources are a common ransomware and phishing delivery path.*

4.8 User application hardening

Achieved: **ML0** · Evidence: Poor · user application hardening: insufficient Intune visibility.

ML	Control	Outcome	Evidence	Observation
ML1	User applications (browser, PDF, Office, .NET, PowerShell) are hardened per ASD maturity model.	No visibility	Poor	Intune device configuration profiles were not collected during this scan. *What this means: This control could not be assessed because required Google API data was not collected — the report may understate risk until permissions are restored and the scan re-run.*

Recommendations

• **[ML1]** Grant DeviceManagementConfiguration.Read.All and confirm Intune is licensed for the tenant.

Appendix — affected accounts and devices

25 affected accounts or devices across 9 findings. Summary by control:

- Multi-factor authentication — 19 affected
- Patch applications — 3 affected
- Patch operating systems — 3 affected

Detail — highest-volume findings

MULTI-FACTOR AUTHENTICATION · [ML3] MULTI-FACTOR AUTHENTICATION IS PHISHING-RESISTANT. — 17 AFFECTED

• user0@acme-workspace.com.au
• user10@acme-workspace.com.au
• user11@acme-workspace.com.au
• user12@acme-workspace.com.au
• user13@acme-workspace.com.au
• user14@acme-workspace.com.au
• user15@acme-workspace.com.au
• user16@acme-workspace.com.au
• user17@acme-workspace.com.au
• user1@acme-workspace.com.au
• user2@acme-workspace.com.au
• user3@acme-workspace.com.au
• user4@acme-workspace.com.au
• user5@acme-workspace.com.au
• user6@acme-workspace.com.au
• user8@acme-workspace.com.au
• user9@acme-workspace.com.au

MULTI-FACTOR AUTHENTICATION · [ML1] MULTI-FACTOR AUTHENTICATION IS USED TO AUTHENTICATE THE ORGANISATION'S USERS OF ONLINE SERVICES THAT PROCESS, STORE OR COMMUNICATE SENSITIVE DATA. — 1 AFFECTED

• user7@acme-workspace.com.au

MULTI-FACTOR AUTHENTICATION · [ML2] MULTI-FACTOR AUTHENTICATION IS USED TO AUTHENTICATE UNPRIVILEGED USERS OF IMPORTANT DATA REPOSITORIES AND INTERNAL SYSTEMS. — 1 AFFECTED

• user7@acme-workspace.com.au

PATCH OPERATING SYSTEMS · [ML1] OPERATING SYSTEMS PATCH TIMELINESS IS ASSESSED VIA INTUNE COMPLIANCE AS A PROXY (NOT DIRECT CVE/KB AGE). — 1 AFFECTED

• CHROMEBOOK-0 · ChromeOS 131.0.6778.264 · user0@acme-workspace.com.au [noncompliant]

PATCH OPERATING SYSTEMS · [ML2] ML2 PATCH TIMEFRAMES ARE ASSESSED VIA INTUNE COMPLIANCE PROXY (NOT DIRECT VULNERABILITY AGE). — 1 AFFECTED

• CHROMEBOOK-0 · ChromeOS 131.0.6778.264 · user0@acme-workspace.com.au [noncompliant]

Other affected findings (counts only)

- [ML3] ML3 patch timeframes are assessed via Intune compliance proxy (not direct vulnerability age). — 1 affected
- [ML1] Applications patch timeliness is assessed via Intune compliance as a proxy (not direct CVE/KB age). — 1 affected
- [ML2] ML2 patch timeframes are assessed via Intune compliance proxy (not direct vulnerability age). — 1 affected
- [ML3] ML3 patch timeframes are assessed via Intune compliance proxy (not direct vulnerability age). — 1 affected

6. Evidence chain appendix

This appendix lists every Google Admin APIs endpoint queried during scan **sample-google-scan-001** at 2026-06-20 00:00:30Z, and maps each sub-control finding to the live query that sourced it. Findings without API provenance (No visibility, Not assessed, Not applicable, or manual placeholders) are omitted from the per-finding register.

Live Google API queries (deduplicated)

Endpoint	Queried (UTC)	Response hash	Snapshot ref
https:/ / admin. googleapis. com/ admin/ directory-/ v1/ roleAssignments	2026-06-20 00:00:30Z	6383736fa17a…	sample-snapshot-google-001
https:/ / admin. googleapis. com/ admin/ directory-/ v1/ users	2026-06-20 00:00:30Z	cd8ca3298d25…	sample-snapshot-google-001
https:/ / admin. googleapis. com/ admin/ reports/ v1-/ activity/ users/ all/ applications/ login	2026-06-20 00:00:30Z	b6da9bcda98f…	sample-snapshot-google-001
https:/ / chromemanagement. googleapis. com/ v1-/ customers/ my_customer/ devices-/ chromeDevices	2026-06-20 00:00:30Z	84daf678879a…	sample-snapshot-google-001

Per-finding provenance register

16 of 27 sub-control findings carry a live-query provenance record (16 with a SHA-256 response hash). Hashes bind API-derived findings to the canonical JSON payload Aegis Eight used when scoring — not every finding has a hash (blind spots and manual placeholders do not).

Finding	ML	Tier	Live query	Queried (UTC)
mfa.ml1.privileged_users Multi-factor authentication Also: / reports/ authenticationMethods/ userRegistrationDetails	**ML1**	Fair	https:/ / admin. googleapis. com/ admin/ directory-/ v1/ users	2026-06-20 00:00:30Z
mfa.ml1.organisation_users Multi-factor authentication Also: / reports/ authenticationMethods/ userRegistrationDetails	**ML1**	Fair	https:/ / admin. googleapis. com/ admin/ directory-/ v1/ users	2026-06-20 00:00:30Z

mfa.ml2.unprivileged_users Multi-factor authentication Also: / reports/ authenticationMethods/ userRegistrationDetails	**ML2**	Fair	https:/ / admin. googleapis. com/ admin/ directory-/ v1/ users	2026-06-20 00:00:30Z
mfa.ml2.event_logging Multi-factor authentication Also: / auditLogs/ signIns	**ML2**	Good	https:/ / admin. googleapis. com/ admin/ reports/ v1-/ activity/ users/ all/ applications/ login	2026-06-20 00:00:30Z
mfa.ml3.phishing_resistant Multi-factor authentication Also: / reports/ authenticationMethods/ userRegistrationDetails	**ML3**	Fair	https:/ / admin. googleapis. com/ admin/ directory-/ v1/ users	2026-06-20 00:00:30Z
mfa.ml1.privileged_enforcement Multi-factor authentication Also: / auditLogs/ signIns	**ML1**	Good	https:/ / admin. googleapis. com/ admin/ reports/ v1-/ activity/ users/ all/ applications/ login	2026-06-20 00:00:30Z
admin.ml1.privileged_count_bounded Restrict administrative privileges Also: / directoryRoles, / directoryRoles/ {id}/ members	**ML1**	Fair	https:/ / admin. googleapis. com/ admin/ directory-/ v1/ roleAssignments	2026-06-20 00:00:30Z
admin.ml2.privileged_count_reduced Restrict administrative privileges	**ML2**	Fair	https:/ / admin. googleapis. com/ admin/ directory-/ v1/ roleAssignments	2026-06-20 00:00:30Z
admin.ml3.just_in_time Restrict administrative privileges	**ML3**	Fair	https:/ / admin. googleapis. com/ admin/ directory-/ v1/ roleAssignments	2026-06-20 00:00:30Z
admin.ml1.inactive_privileged Restrict administrative privileges Also: / users	**ML1**	Fair	https:/ / admin. googleapis. com/ admin/ directory-/ v1/ users	2026-06-20 00:00:30Z
patch_operating_systems.ml1. - patch_timeframes Patch operating systems Also: / deviceManagement/ managedDevices	**ML1**	Fair	https:/ / chromemanagement. googleapis. com/ v1-/ customers/ my_customer/ devices-/ chromeDevices	2026-06-20 00:00:30Z
patch_operating_systems.ml2. - tighter_compliance Patch operating systems	**ML2**	Fair	https:/ / chromemanagement. googleapis. com/ v1-/ customers/ my_customer/ devices-/ chromeDevices	2026-06-20 00:00:30Z
patch_operating_systems.ml3. - fleet_compliance Patch operating systems	**ML3**	Fair	https:/ / chromemanagement. googleapis. com/ v1-/ customers/ my_customer/ devices-/ chromeDevices	2026-06-20 00:00:30Z
patch_applications.ml1.patch_timeframes Patch applications Also: / deviceManagement/ managedDevices	**ML1**	Fair	https:/ / chromemanagement. googleapis. com/ v1-/ customers/ my_customer/ devices-/ chromeDevices	2026-06-20 00:00:30Z
patch_applications.ml2.tighter_compliance Patch applications	**ML2**	Fair	https:/ / chromemanagement. googleapis. com/ v1-/ customers/ my_customer/ devices-/ chromeDevices	2026-06-20 00:00:30Z
patch_applications.ml3.fleet_compliance Patch applications	**ML3**	Fair	https:/ / chromemanagement. googleapis. com/ v1-/ customers/ my_customer/ devices-/ chromeDevices	2026-06-20 00:00:30Z

11 finding(s) omitted — no Google API provenance (No visibility, Not assessed, Not applicable, or manual evidence only).

How to access the evidence pack

Subscription customers can download a deterministic evidence pack (persisted scan snapshot + scored assessment + per-finding manifest, typically 50–500 KB JSON) from the dashboard at **/dashboard/scans/-sample-google-scan-001**. The pack is built from the stored snapshot at download time — no live Google Admin APIs calls are made — and can be forwarded to an IRAP assessor, cyber insurer, or internal compliance reviewer as-is.

Where a finding carries a **responseHash**, an assessor verifies it by re-querying the recorded endpoint within Google's documented retention windows, hashing the canonical JSON payload the same way, and comparing to the manifest entry. Raw API response bodies are not bundled in the pack — only aggregated signals, scores, and hashes.

Trial report: evidence-pack download is part of the paid subscription. Endpoints, timestamps, and hashes in this appendix let you (or an assessor) evaluate the evidence chain before subscribing; the JSON export unlocks on subscription.

7. Conclusion and next steps

This automated assessment is intended to accelerate — not replace — a formal ASD Essentials assessment. Outcomes marked "No visibility" or "Not assessed" require manual evidence collection per the ASD process guide.

> **THIS IS YOUR BASELINE SCAN — WHAT UNLOCKS NEXT**
>
> Continuous-monitoring subscribers receive:
>
> • **Change-triggered alerts** whenever an assessed control regresses — new admin without MFA, a device falling out of compliance, a backup policy disabled — so posture drift surfaces in days, not at the next quarterly audit.
>
> • **Trend reporting** across re-scans, so future versions of this report show progress (or regression) over time rather than a single point-in-time snapshot.
>
> • **Path 2 collectors** as they ship (sign-in audit analysis, Chrome device applied-state, expanded Vault signals) — each one lifts the findings marked "Stronger evidence (Good tier)" above from Fair to Good evidence quality, which materially strengthens IRAP-QAF and cyber-insurance evidence trails.
>
> • **Evidence-chain retention** for the full subscription window (vs. 90 days on the free trial), with hash-addressed raw Google API responses available on demand for assessors.
>
> Subscribe at aegiseight.com to enable.

What Aegis Eight provides

Posture visibility · Automated assessment support · Evidence collection · Remediation guidance.

What Aegis Eight does not provide

Formal ASD certification · Guaranteed compliance · Legal sign-off. This report should be used in conjunction with a qualified assessor for any compliance attestation.

References

• ASD Essentials assessment process guide (October 2024)
• ASD Essentials maturity model (November 2023)