FAZ AUSTRALIA

faz8

PROFESSIONAL ASSESSMENT · COMMERCIAL IN CONFIDENCE

Website and AI Security Assessment

How exposed your business is to automated attacks, malicious bots, AI agents, data harvesting and digital impersonation, and what to fix first.

Prepared for	**Sample Client**
Website	example.com.au
Assessed	27 November 2026, 00:44 AEDT
Protection score	**86 / 100**
Document	FAZ8-FULL-20261127-SAMPLE01 · Version 1.0

Faz Australia Pty Ltd · ABN 67 608 122 514 · Level 2, 7 Neptune St, Phillip ACT 2606 info@fazaustralia.com · www.fazaustralia.com

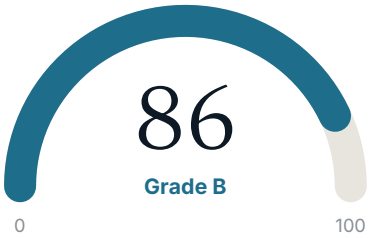
CONTENTS

What is in *this report*

01	Executive summary	03
02	What this means for your business	04
03	Priority action plan	05
04	Methodology	06
05	Site profile and threat model	07
06	AI discoverability and readiness	07
07	Findings register	08
08	Findings · Medium	09
09	Findings · Low	11
10	AI crawler and agent policy	13
11	Defence matrix	14
12	Framework alignment	15
13	Scope, method and safeguards	17
14	Your next step	18

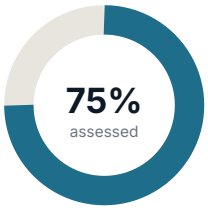
Findings *overview*

PROTECTION SCORE



Covers the 75% of weighted controls assessed.

ASSESSMENT COVERAGE AND CONFIDENCE



75% of control weight assessed

25% not scored (form and lead integrity)

Confidence: **Moderate**

High needs 90% or more coverage

CYBER EXPOSURE

Moderate

Highest finding is Medium

BUSINESS IMPACT

Moderate

Highest gap in forms, exposure or email

AI READINESS

Limited

Discoverability score 0, provisional

CHECKS PASSED

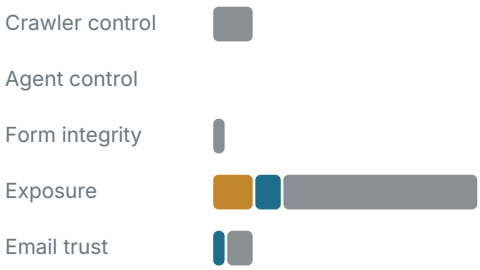
44 of 50

Website scan and bot checks in this run

CATEGORY SCORES

Crawler and scraper control	100
Agent and headless control	100
Form and lead integrity	NOT SCORED
Exposure and hardening	62
Abuse throttling	100
Email and domain trust	95

FINDINGS BY CATEGORY AND SEVERITY



Medium 3 **Low 3** **Info 20**

No Critical or High findings.

EXECUTIVE SUMMARY

example.com.au has a protection score of 86/100 (grade B). The website security scan scored 70/100 and the bot assessment was 100/100 for resilience to bots, AI agents and API abuse. Together they found 6 gaps; the most important is: Missing HSTS Header. 44 of 50 checks passed. The pages that follow describe every gap, how to close it and how to check the fix.

Sources: faz8 assessment run sample01, 27 November 2026, 00:44 AEDT

44 of 50 checks passed. *Missing HSTS Header.*

3	0	44 / 50	3 hrs
Medium findings to fix this month	Critical or High findings	Checks that passed	Estimated developer time to close every priority action

WHAT COULD HAPPEN

MEDIUM · PRIVACY

Missing HSTS header

Without an HSTS header, customers' connections may not always be secure, increasing the risk of data interception.

MEDIUM · TRUST

Missing Content-Security-Policy

The lack of a CSP encourages potential cross-site scripting attacks, compromising customer safety and trust.

MEDIUM · PRIVACY

Missing X-Frame-Options

The absence of this header allows clickjacking attacks, which can exploit customer interactions on the site.

WORKING WELL

- Some pages challenge automated visitors
- Bot / WAF protection detected: Vercel Firewall
- Scripted clients are blocked or challenged
- Some AI/scraper user agents are blocked
- Home page is rate limited

IF YOU DO NOTHING

- Ignoring these issues may lead to data breaches.
- Customer trust could diminish due to security concerns.
- The organisation may face legal liabilities if a breach occurs.

STATED PLAINLY this is an external, non destructive assessment of how your website and its automated traffic handling look from outside. It is not a penetration test, an API security test or a certification.

Sources: faz8 run sample01; scan example.com.au

03 · PRIORITY ACTION PLAN

Two actions, about three hours, *3 of 6 findings closed*

01 HARDEN THE SITE

Close exposed files, headers and components

#	Action	Level	Closes	Effort	Owner	Gain
1	**Implement security headers for better protection.** Add HSTS, Content Security Policy, and X-Frame-Options headers in the web server configuration.	MEDIUM	FIND-01 FIND-02 FIND-03	2 hrs	Developer	**+9**
2	**Establish a robots.txt file for clearer bot management.** Create and configure a ruleset in the root directory to manage automated access.	INFO	-	1 hr	Developer	-

+9

Protection points from all actions, recalculated by the engine

3 of 6

Findings closed by the plan

28 Dec

Free retest date, 2026

STATED PLAINLY gains are calculated by scoring again with the listed findings fixed and apply to the 75% of controls assessed. Form and lead integrity could not be measured and is checked at retest.

Sources: faz8 remediation guidance; faz8 scoring model v1.0

How a finding becomes *a score you can defend*

01 DISCOVER
Map pages, forms, endpoints and policies

02 PROBE
12 client identities, real browsers, AI agents and the website scan

03 SCORE
Each finding deducts points from its category

04 VERIFY
Every finding has a retest check

SEVERITY LEVELS

Critical · fix in 48 hours	**-40**
High · fix in 2 weeks	**-25**
Medium · fix in 30 days	**-12**
Low · next release	**-5**
Informational · awareness	**0**

A finding removes these points from its category, taken from what is left, so many small gaps cannot push a category below zero. Not scored categories are excluded and shown, never counted as passes.

PROTECTION SCORE

Category	Weight	Score
Crawler and scraper control	10	**100**
Agent and headless control	10	**100**
Form and lead integrity	25	N/S
Exposure and hardening	25	**62**
Abuse throttling	10	**100**
Email and domain trust	20	**95**

`(10×100 + 10×100 + 25×62 + 10×100 + 20×95) ÷ 75 = 86`

INDICATOR DEFINITIONS

Indicator	Low	Moderate	High	Critical
Cyber exposure	No finding above Low	**Highest finding Medium**	Any High finding	Any Critical finding
Business impact	No gap in forms, exposure or email	**Medium gap**	High gap	Critical gap
Confidence	Under 70% coverage	**70 to 89%**	90% or more	

AI readiness	Limited	Developing	Good	Advanced
Score band	**0 to 39**	40 to 64	65 to 84	85 to 100

STATED PLAINLY

grades run A 90+, B 80 to 89, C 65 to 79, D 50 to 64, F below 50. A grade is provisional when more than 25% of weight is unscored, and cannot support the faz8 Assessed badge. The current result for Sample Client is shown in bold.

Sources: faz8 scoring model v1.0; OWASP Automated Threats to Web Applications

05 · SITE PROFILE AND THREAT MODEL

A site scored for the threats *that fit it*

PLATFORM

WordPress

Bot management detected: Vercel Firewall.

WHAT ATTACKERS WANT

Backend data

Automated tools go for backend data, published content.

WHAT YOU WANT

Be found and trusted

Search engines and AI assistants send you customers; visitors trust your domain.

Threat	OWASP code	Weighting	Why
Spamming	OAT-017	DOWN	No forms found on the pages assessed; form defences were not scored
Content scraping	OAT-011	NEUTRAL	1 public page(s) crawled; published content can be copied
Account attacks	OAT-007, 008	DOWN	No login or account features found
Direct API abuse	API4	UP	4 backend endpoint(s) found

06 · AI DISCOVERABILITY AND READINESS

0 of 100, provisional. *Readable, but not deliberately.*

Signal	Points
Deliberate AI crawler policy in robots.txt	0 / 25
AI crawlers and search engines can reach the site	0 / 25
Clean page titles	N/S
Valid sitemap	0 / 5
llms.txt (emerging, low weight)	0 / 5
Structured business data (schema.org)	N/S

HOW IT IS CALCULATED

0 of the 60 points assessed = 0. Signals nothing measured are shown as N/S and left out.

STATED PLAINLY

this measures whether AI services can read your site accurately. It does not guarantee that an assistant will recommend or cite you. AI readiness never deducts Protection points.

Sources: faz8 run sample01; OpenAI, Anthropic and Perplexity crawler documentation

07 · FINDINGS REGISTER

6 findings to fix, *plus 20 observations to note*

ID	Finding	Level	Category	Action
FIND-01	Missing HSTS Header	MEDIUM	Exposure and hardening	1
FIND-02	Missing Content-Security-Policy	MEDIUM	Exposure and hardening	1
FIND-03	Missing X-Frame-Options	MEDIUM	Exposure and hardening	1
FIND-04	Missing X-Content-Type-Options	LOW	Exposure and hardening	None
FIND-05	Missing Permissions-Policy	LOW	Exposure and hardening	None
FIND-06	No MTA-STS policy	LOW	Email and domain trust	None
FIND-07	Missing Referrer-Policy	INFO	Exposure and hardening	None
FIND-08	Missing Cross-Origin-Opener-Policy	INFO	Exposure and hardening	None
FIND-09	Missing Cross-Origin-Embedder-Policy	INFO	Exposure and hardening	None
FIND-10	Missing Cross-Origin-Resource-Policy	INFO	Exposure and hardening	None
FIND-11	Integrity-Policy enforcement header missing	INFO	Exposure and hardening	None
FIND-12	Origin-Agent-Cluster not enabled	INFO	Exposure and hardening	None
FIND-13	Reporting-Endpoints header missing	INFO	Exposure and hardening	None
FIND-14	Integrity-Policy-Report-Only header missing	INFO	Exposure and hardening	None
FIND-15	security.txt not found	INFO	Exposure and hardening	None
FIND-16	Dependency scan skipped: no lockfile available	INFO	Exposure and hardening	None
FIND-17	No SMTP TLS reporting (TLS-RPT)	INFO	Email and domain trust	None
FIND-18	No CAA record	INFO	Email and domain trust	None

8 more informational item(s) are in the JSON report.

Sources: faz8 run sample01; OpenAI, Anthropic and Perplexity crawler documentation

Real gaps, *worth fixing this month*

MEDIUM FIND-01 · EXPOSURE AND HARDENING

Missing HSTS Header

Browsers may not enforce HTTPS.

The absence of the HTTP Strict Transport Security (HSTS) header potentially exposes example.com.au to man-in-the-middle attacks. This header is crucial for enforcing secure connections and preventing downgrade attacks.

Recommended fix MEDIUM

Implement the HSTS header by adding 'Strict-Transport-Security: max-age=31536000; includeSubDomains' to your server responses. Consider using 'preload' only if all subdomains support HTTPS.

WHY IT MATTERS

Without HSTS, users may inadvertently connect via unsecured HTTP. This finding relates to OWASP A04 and ASD ISM cryptography guidelines, as it undermines the security of data in transit.

Retest: Check the headers returned by example.com.au in a web browser's developer tools or use an external security scanner to confirm the presence of the HSTS header.

OWASP A04 | ASD ISM Cryptography | SOC 2 CC6.7

MEDIUM FIND-02 · EXPOSURE AND HARDENING

Missing Content-Security-Policy

No CSP header found. The site is more vulnerable to XSS.

The Content-Security-Policy (CSP) is missing, which helps control resources the user agent is allowed to load, reducing risks like Cross-Site Scripting (XSS).

Recommended fix MEDIUM

Implement a CSP starting in report-only mode: 'Content-Security-Policy-Report-Only: default-src 'self';'. Include necessary third-party hosts and enforce once confident.

WHY IT MATTERS

The absence of a CSP can lead to increased vulnerability to malicious script injection, relating to OWASP A05.

Retest: Check the website's HTTP response headers for the presence of a Content-Security-Policy directive to ensure proper implementation.

OWASP A05 | ASD ISM Software Development | SOC 2 CC6.6

Sources: faz8 run sample01; OpenAI, Anthropic and Perplexity crawler documentation

MEDIUM

FIND-03 · EXPOSURE AND HARDENING

Missing X-Frame-Options

Site may be vulnerable to clickjacking.

The website is missing the X-Frame-Options header, potentially allowing clickjacking attacks where users can be tricked into clicking on malicious content.

Recommended fix MEDIUM

To mitigate this risk, configure the server to include the X-Frame-Options header with a value of 'DENY' or 'SAMEORIGIN'.

WHY IT MATTERS

This issue poses a security risk relating to OWASP A02 and ASD ISM Software Development, as it could lead to unauthorised actions taken on behalf of the user.

Retest: After applying the remediation, use a web security tool to confirm that the X-Frame-Options header is present in the response headers.

OWASP A02 | ASD ISM Software Development | SOC 2 CC6.6

Sources: faz8 run sample01; OpenAI, Anthropic and Perplexity crawler documentation

Smaller gaps today, *bigger ones if the site grows*

LOW

FIND-04 · EXPOSURE AND HARDENING

Missing X-Content-Type-Options

MIME-type sniffing is not prevented.

The site example.com.au is missing the X-Content-Type-Options header, which helps prevent browsers from interpreting files as a different MIME type.

Recommended fix LOW

To enhance security, configure the server to include 'X-Content-Type-Options: nosniff' in HTTP response headers.

WHY IT MATTERS

This could allow for content type sniffing, potentially leading to cross-site scripting (XSS) exploits. Related to OWASP A02.

Retest: Check the HTTP response headers using browser developer tools or online header checkers to confirm the header is present.

OWASP A02 | ASD ISM Software Development | SOC 2 CC6.6

LOW

FIND-05 · EXPOSURE AND HARDENING

Missing Permissions-Policy

Browser features (camera, geolocation...) are not restricted.

The site does not implement a Permissions-Policy header, which governs the use of specific browser features like geolocation or camera access. This header can mitigate the risk of unwanted access.

Recommended fix LOW

Implement the Permissions-Policy header by adding 'Permissions-Policy: geolocation=(), microphone=(), camera=()' to your HTTP response headers.

WHY IT MATTERS

Without this policy, example.com.au may inadvertently allow access to sensitive device capabilities, which relates to ASD ISM software development practices.

Retest: Check the HTTP response headers for the presence of the Permissions-Policy header to ensure it is configured correctly.

OWASP A02 | ASD ISM Software Development | SOC 2 CC6.6

Sources: faz8 run sample01; OpenAI, Anthropic and Perplexity crawler documentation

LOW

FIND-06 · EMAIL AND DOMAIN TRUST

No MTA-STS policy

Attackers on-path can strip STARTTLS and read mail in transit.

The absence of a Mail Transfer AgentStrict Transport Security (MTA-STS) policy can expose email communications to interception and downgrade attacks, making it easier for malicious actors to tamper with emails sent to and from example.com.au.

Recommended fix LOW

To mitigate this risk, configure and publish an MTA-STS policy by creating a TXT record for _mta-sts.example.com.au and providing the necessary .well-known/mta-sts.txt file at the suggested URL.

WHY IT MATTERS

This finding relates to ASD ISM email security guidelines. Without MTA-STS, the site is more vulnerable to email spoofing and phishing attacks, compromising both user trust and data integrity.

Retest: Confirm the MTA-STS policy is correctly published by checking the DNS records for the TXT entry and accessing the specified URL to ensure that the policy file is accessible and correctly formatted.

OWASP A04 | ASD ISM Email | SOC 2 CC6.7

NOT SCORED

NOT SCORED **Landing page served a bot-protection challenge.** HTTP 429. Results will be incomplete and can vary between runs.

NOT SCORED **Could not verify: Dependency manifest (package.json / lockfiles).** /package.json -> HTTP 429: bot protection / rate limiting answered instead of the real page. Allowlist your IP in the WAF, or re-run with --delay 0.5 --threads 1.

NOT SCORED **Could not verify: WordPress installer.** /wp-admin/install.php -> HTTP 429: bot protection / rate limiting answered instead of the real page. Allowlist your IP in the WAF, or re-run with --delay 0.5 --threads 1.

NOT SCORED **Could not verify: phpMyAdmin interface.** /phpmyadmin/ -> HTTP 429: bot protection / rate limiting answered instead of the real page. Allowlist your IP in the WAF, or re-run with --delay 0.5 --threads 1.

NOT SCORED **Could not verify: WordPress XML-RPC endpoint.** /xmlrpc.php -> HTTP 429: bot protection / rate limiting answered instead of the real page. Allowlist your IP in the WAF, or re-run with --delay 0.5 --threads 1.

NOT SCORED **Could not verify: GeoServer web console.** /geoserver/web/ -> HTTP 429: bot protection / rate limiting answered instead of the real page. Allowlist your IP in the WAF, or re-run with --delay 0.5 --threads 1.

Sources: faz8 run sample01 action log; website scan example.com.au

AI services visit for three reasons. *Treat each on its merits.*

SEARCH

Appear in AI search results

OAI-SearchBot, PerplexityBot, Claude-SearchBot, Googlebot, Bingbot

Recommendation: Allow; verify search engines by IP

USER INITIATED

A person asks an assistant to open your page

ChatGPT-User, Claude-User, Perplexity-User

Recommendation: Allow

TRAINING

Content used to train models

GPTBot, ClaudeBot, Google-Extended, CCBot, Bytespider

Recommendation: your choice; default Disallow

ROBOTS.TXT, PASTE READY

```
# Search and user initiated access
User-agent: OAI-SearchBot
User-agent: ChatGPT-User
User-agent: PerplexityBot
User-agent: Perplexity-User
User-agent: Claude-SearchBot
User-agent: Claude-User
Allow: /

# Model training (business choice)
User-agent: GPTBot
User-agent: ClaudeBot
User-agent: Google-Extended
User-agent: CCBot
User-agent: Bytespider
Disallow: /

User-agent: *
Allow: /
# No valid sitemap was found. Publish one, then add:
# Sitemap: https://example.com.au/sitemap.xml
```

STRUCTURED BUSINESS DATA, STARTER

```
{ "@context": "https://schema.org",
  "@type": "Organization",
  "name": "Sample Client",
  "url": "https://example.com.au",
  "telephone": "REPLACE-ME",
  "address": { "@type": "PostalAddress",
    "streetAddress": "REPLACE-ME",
    "addressLocality": "REPLACE-ME",
    "postalCode": "REPLACE-ME",
    "addressCountry": "AU" } }
```

Replace every REPLACE-ME value before publishing. llms.txt is optional: an emerging convention with limited adoption, so it carries low weight.

STATED PLAINLY robots.txt is a request, not a lock. Edge bot protection enforces it for crawlers that ignore it, and allowing a crawler does not guarantee citation.

Sources: OpenAI, Anthropic, Perplexity and Google crawler documentation; schema.org

20 controls tested, *20 held*

HELD defence worked · GAP defence missing · POLICY business choice · NOT SCORED inconclusive

CRAWLER IDENTITY TEST, 12 CLIENTS

Client	Result	HTTP	Note
Python requests library	HELD	429	
curl command-line client	HELD	429	
Go HTTP client	HELD	429	
Scrapy scraping framework	HELD	429	
No User-Agent header	HELD	429	
HeadlessChrome user agent	HELD	429	
OpenAI GPTBot	HELD	429	
Anthropic ClaudeBot	HELD	429	
Common Crawl CCBot	HELD	429	
PerplexityBot	HELD	429	
ByteDance Bytespider	HELD	429	
Googlebot (spoofed, from a non-Google address)	HELD	429	

COMMON API PATH EXPOSURE

Backend endpoint	Result
https://example.com.au/api/ HTTP 429	HELD
https://example.com.au/wp-json/ HTTP 429	HELD
https://example.com.au/graphql HTTP 429	HELD
https://example.com.au/api/v1/ HTTP 429	HELD

BROWSER, FORM AND EXPOSURE TESTS

Check	Result
Unmodified headless Chromium	HELD
Headless Chromium with ordinary browser settings	HELD
Rate limit, home page	HELD
Rate limit, api endpoint	HELD

STATED PLAINLY the API checks are discovery only. Authentication, authorisation, object level access and API abuse testing are not part of this assessment.

Sources: faz8 run sample01 action log

Evidence your auditors recognise, *without claiming certification*

SOURCE HIERARCHY FOR THIS REPORT

1 Australian law: Privacy Act 1988 (APP 11), Spam Act 2003

2 Government guidance: ASD Information Security Manual, ACSC

3 Standards: ISO/IEC 27001:2022, NIST CSF 2.0

4 Threat taxonomies: OWASP Automated Threats, API Top 10

Framework	Bots	AI agents	Forms	Data exposure	Email trust	APIs
OWASP Automated Threats	●	●	◐	●	○	○
ASD Information Security Manual	●	●	◐	●	●	○
ISO/IEC 27001:2022 Annex A	●	●	◐	●	●	○
NIST CSF 2.0	●	●	◐	●	●	○
Privacy Act 1988, APP 11	○	○	◐	●	○	○
OWASP API Security Top 10	○	○	○	○	○	◐

● evidence in this run ◐ partial: not measured in this run, or needs a separate API assessment ○ outside the scope of that framework

Finding	OWASP	ISO/IEC 27001, NIST CSF	ASD ISM	Other
FIND-01	A04		Cryptography	SOC 2 CC6.7
FIND-02	A05		Software Development	SOC 2 CC6.6
FIND-03	A02		Software Development	SOC 2 CC6.6
FIND-04	A02		Software Development	SOC 2 CC6.6
FIND-05	A02		Software Development	SOC 2 CC6.6
FIND-06	A04		Email	SOC 2 CC6.7

Website scan references	Indicative status (external view only)
OWASP Top 10	**Gaps identified**
ASD Information Security Manual (ISM)	**Gaps identified**
SOC 2 Trust Services Criteria	**Gaps identified**

Sources: faz8 run sample01 action log

STATED PLAINLY statuses are a gap indication from an external assessment, not a formal compliance assessment or certification. The ASD Essential Eight covers endpoint and system controls that an external assessment cannot observe.

Sources: OWASP; ASD ISM; ISO/IEC 27001:2022; NIST CSF 2.0; OAIC Australian Privacy Principles

Read only, in scope, *and fully reproducible*

51	0	33s	75
Requests of a 600 budget	Form submissions made	Bot run time	Actions logged as evidence

AUTHORISATION

Status	UNVERIFIED
Method	Not verified for this run
Authorised by	Account holder confirmed ownership or written permission
Recorded	27 November 2026, 00:42 AEDT, run sample01

SAFEGUARDS

Scope	example.com.au only
Pace	2 per second, 8 per second bursts
Methods	GET and OPTIONS only
Permitted submissions	None
Never done	CAPTCHA solving, payments, deletions

TEST COVERAGE

Test	Status
Reconnaissance	COMPLETE
Crawler & scraper personas	COMPLETE
Rate-limit probe	COMPLETE
Headless browser detection	COMPLETE
Form defence audit	INCONCLUSIVE
Backend API probe	COMPLETE
Autonomous AI agent	COMPLETE
Security headers, TLS and exposed files	COMPLETE
SPF, DKIM, DMARC	COMPLETE
Dependencies (OSV.dev) no lockfile available	SKIPPED

EVIDENCE PACK

The full action log for run sample01 (every request, click and decision) is kept and available from Faz Australia Pty Ltd on request. Evidence fingerprint (SHA-256 of the website scan and bot run records):

`[withheld in sample report]` . Website scanner version 1.0.

LIMITATION, STATED PLAINLY this assessment reflects the externally observable behaviour of example.com.au at the time stated. It is not a penetration test, API security test, code review or certification, and does not assess internal systems or Essential Eight maturity. Faz Australia Pty Ltd accepts no liability for decisions made solely on this report. Commercial in confidence; prepared for Sample Client only.

Sources: faz8 run record sample01

14 · YOUR NEXT STEP

Fix it yourself, or let us. *Either way, your retest is booked.*

OPTION 1 · SELF FIX

Fix it yourself

Each finding above has a recommended fix and a retest check.

Free retest on 28 December 2026

OPTION 2 · RECOMMENDED

Faz fixes it

All 2 actions, about 3 hours

Fixed price, quoted in 1 business day

OPTION 3 · ONGOING

Stay protected

Monthly rescan and trend

Alerts on significant change

IMPLEMENTATION ESTIMATE

Work package	Effort
Implement security headers for better protection.	2 hrs
Establish a robots.txt file for clearer bot management.	1 hr
Total	**3 hrs**

Faz fixed price is calculated from these hours on your rate card. Hours are estimates from each action's effort rating.

WHAT FAZ8 MONITORING INCLUDES

Feature	Status
Monthly rescan with score trend	INCLUDED
Alerts when pages, endpoints or defences change	INCLUDED
AI crawler policy drift	INCLUDED
SPF, DKIM and DMARC monitoring	INCLUDED
Monthly remediation recommendations	INCLUDED
API security testing	ROADMAP
AI citation tracking	ROADMAP

Production rule: included only when live in the engine.

Talk to Our Support Team

At Faz Australia

+61 2 6110 2002 · info@fazaustralia.com · www.fazaustralia.com

GLOSSARY

Bot protection: scores visitors on behaviour and challenges automated ones. **Headless browser:** a browser run by software with no screen. **Turnstile:** Cloudflare's free, mostly invisible human check. **SPF, DKIM, DMARC:** email settings that stop others sending as your domain. **Structured data:** machine readable business details for search and AI services.

Sources: faz8 run record sample01