outsec

EXTERNAL FOOTPRINT REPORT

outsec trace

[Business Name Pty Ltd]

Engagement	Assessment run	Catalogue version
Sample OutSec Trace report	06 October 2026	1.0.0

Report generated
05 October 2026 at 09:00

Summary NEEDS ATTENTION: 2 HIGH FINDINGS

CONFIDENTIAL. Prepared exclusively for [Business Name Pty Ltd] and Outliers Collective / OutSec.
Non-intrusive external checks only. No credentials, no exploitation, no access to your systems.

Executive summary

This report covers what is visible about **[Business Name Pty Ltd]** from the public internet, gathered without access to your systems. 2 findings need prompt attention -- see the findings below for each one. The rest are lower-priority improvements or context. Each check is explained in plain language at https://dev.outsec.au/trace/understanding.

2	0	13	14	8
HIGH	MEDIUM	LOW	INFORMATIONAL	NOT DETERMINED

Coverage

63 of 63 catalogue checks (v1.0.0) produced a result this run. Every catalogue check ran.

EMAIL SECURITY — Result: pass · finding (high, medium or low) · observation · not determined

RESULT	CHECK	DETAIL	ASSET
HIGH	Does the domain publish a DMARC record at all?	no DMARC record found	[business].com.au
LOW	Does the domain publish an MTA-STS policy (_mta-sts.<domain> TXT record)?	no v=STSv1 TXT record at _mta-sts.[business].com.au	[business].com.au
LOW	Does the domain publish a TLS-RPT reporting address (_smtp._tls.<domain> TXT record)?	no v=TLSRPTv1 TXT record at _smtp._tls.[business].com.au	[business].com.au
PASS	Does the domain publish an SPF record at all?	SPF TXT record present	[business].com.au
PASS	Does the SPF record's trailing mechanism reject or merely flag unlisted senders?	ends in -all (hardfail): mail from senders not listed should be rejected	[business].com.au
PASS	Does the SPF record's evaluation chain exceed RFC 7208's 10-DNS-lookup limit?	10 or fewer DNS lookups required to evaluate the record	[business].com.au

RESULT	CHECK	DETAIL	ASSET
PASS	Does the domain publish more than one SPF-shaped TXT record?	Exactly one SPF record found	[business].com.au
PASS	Does mail sent from this domain carry a DKIM signature, checked against common selectors?	At least one common selector resolves with a valid-shaped DKIM TXT record	[business].com.au
PASS	Does the domain's mail server(s) support opportunistic transport encryption (STARTTLS)?	STARTTLS advertised and negotiation succeeds	[business].com.au
NOT DETERMINED	Does the DMARC policy actually instruct receivers to act on failures?	no DMARC record exists to grade (see email.dmarc.present)	[business].com.au
NOT DETERMINED	Is DMARC aggregate reporting (rua=) configured at all?	no DMARC record exists to check for a reporting address (see email.dmarc.present)	[business].com.au
NOT DETERMINED	Is the DMARC record structurally valid enough to evaluate reliably?	no DMARC record exists to validate (see email.dmarc.present)	[business].com.au
NOT DETERMINED	If the DMARC rua= destination is on an external domain, does that domain publish the required authorization record?	no DMARC record exists to check rua= authorization against (see email.dmarc.present)	[business].com.au

WHOIS / REGISTRATION

Result: pass · finding (high, medium or low) · observation · not determined

RESULT	CHECK	DETAIL	ASSET
NOT DETERMINED	How close is this domain to its registration expiry date?	no expiry date field found in WHOIS response	[business].com.au

RESULT	CHECK	DETAIL	ASSET
NOT DETERMINED	Does the domain have a registrar transfer lock (clientTransferProhibited or equivalent) set?	auDA (.au) has no registrant-controllable transfer-lock status -- only serverTransferProhibited exists, which the registry sets itself (typically for an active dispute/hold), not something a registrant/ registrar can enable as a protective measure. This check's pass/fail semantics don't apply to .au.	[business].com.au

SUBDOMAIN TAKEOVER

Result: pass · finding (high, medium or low) · observation · not determined

RESULT	CHECK	DETAIL	ASSET
PASS	Does any MX host still resolve, or is mail routed to a dangling hostname a third party could reclaim?	MX host resolves (or there are no MX hosts at all)	[business]-com-au.mail.protection.outlook.com
PASS	Does any discovered hostname's CNAME point to a third-party service resource that appears to have been deprovisioned or left unclaimed, which a third party could potentially claim and use to serve content on the client's own subdomain?	No CNAME matches a known vulnerable-service fingerprint pattern, or the matched service's resource is still claimed	[business].com.au

LOOKALIKE DOMAIN MONITORING

Result: pass · finding (high, medium or low) · observation · not determined

[business].com.au: 1 registered lookalike(s) with live mail -- see per-domain findings below

RESULT	CHECK	DETAIL	ASSET
HIGH	Are any typosquat/homoglyph permutations of the domain registered with an active mail exchange?	live MX (mailforward.[registrar].com) points at unrelated infrastructure	[8usiness].com.au
PASS	Does any registered lookalike domain's live web page visually match the real site's homepage?	No registered lookalike's screenshot is a close visual match to the real homepage	[business].com.au

DNS HYGIENE

Result: pass · finding (high, medium or low) · observation · not determined

RESULT	CHECK	DETAIL	ASSET
LOW	Does a CAA record restrict which Certificate Authorities may issue TLS certificates for this domain?	no CAA record found	[business].com.au
OBSERVATION	Is the domain's DNS cryptographically signed and validating?	not signed at all -- still an opt-in minority practice	[business].com.au
OBSERVATION	Does the reverse-DNS (PTR) record for a hostname's IP relate back to that hostname?	PTR is generic cloud-provider reverse DNS -- expected on shared infrastructure	[business].com.au
OBSERVATION	Does the reverse-DNS (PTR) record for a hostname's IP relate back to that hostname?	PTR is generic cloud-provider reverse DNS -- expected on shared infrastructure	docs.[business].com.au
OBSERVATION	Does the reverse-DNS (PTR) record for a hostname's IP relate back to that hostname?	PTR is generic cloud-provider reverse DNS -- expected on shared infrastructure	portal.[business].com.au
OBSERVATION	Does the reverse-DNS (PTR) record for a hostname's IP relate back to that hostname?	PTR is generic cloud-provider reverse DNS -- expected on shared infrastructure	www.[business].com.au

RESULT	CHECK	DETAIL	ASSET
PASS	Does any of the domain's own authoritative nameservers also answer recursive queries (i.e. behave as an open resolver), rather than being locked down to authoritative-only?	No authoritative nameserver sets the RA (recursion available) flag	[business].com.au
PASS	Do any of the domain's authoritative nameservers permit unauthenticated DNS zone transfer (AXFR)?	Every authoritative nameserver refuses the zone transfer	[business].com.au
PASS	Do all of the domain's authoritative nameservers agree on the domain's own NS record set?	Every authoritative nameserver returns the same NS record set	[business].com.au

EXPOSURE

Result: pass · finding (high, medium or low) · observation · not determined

RESULT	CHECK	DETAIL	ASSET
PASS	Are well-known sensitive paths (.git, .env, backup files, credential files) exposed?	None of the probed paths return real content	[business].com.au
PASS	Do cloud storage buckets/ containers matching common naming conventions for this organisation exist, and are they publicly listable?	No matching bucket/ container found on any provider	[business].com.au
PASS	Does the site's own published JavaScript contain hardcoded API keys or secrets?	No key-shaped strings found in crawled JS	[business].com.au
PASS	Does the site publish JavaScript source map (.map) files?	No .map files found in the crawled asset list	[business].com.au

RESULT	CHECK	DETAIL	ASSET
PASS	Are debug/management interfaces (Spring Actuator, metrics, phpinfo) exposed?	None of the probed debug/management paths return real content	[business].com.au

WEB HARDENING

Result: pass · finding (high, medium or low) · observation · not determined

RESULT	CHECK	DETAIL	ASSET
LOW	Does the site send a Content-Security-Policy header, and if so, is it permissive?	no Content-Security-Policy header present	[business].com.au
LOW	Does the site send an X-Frame-Options header (or equivalent CSP frame-ancestors)?	no X-Frame-Options header present	[business].com.au
LOW	Does the site send X-Content-Type-Options: nosniff?	no X-Content-Type-Options header present	[business].com.au
LOW	Does the site send a Permissions-Policy header restricting browser feature access (camera/mic/geolocation/etc.)?	no Permissions-Policy header: the site doesn't restrict which browser features (such as camera, microphone or geolocation) its pages and embedded content can request	[business].com.au
LOW	Do cookies set by the site carry Secure, HttpOnly, and SameSite attributes?	missing Secure/HttpOnly: GAESA	[business].com.au
LOW	Does the site send a Content-Security-Policy header, and if so, is it permissive?	no Content-Security-Policy header present	www.[business].com.au
LOW	Does the site send an X-Frame-Options header (or equivalent CSP frame-ancestors)?	no X-Frame-Options header present	www.[business].com.au
LOW	Does the site send X-Content-Type-Options: nosniff?	no X-Content-Type-Options header present	www.[business].com.au

RESULT	CHECK	DETAIL	ASSET
LOW	Does the site send a Permissions-Policy header restricting browser feature access (camera/mic/geolocation/etc.)?	no Permissions-Policy header: the site doesn't restrict which browser features (such as camera, microphone or geolocation) its pages and embedded content can request	www.[business].com.au
LOW	Do cookies set by the site carry Secure, HttpOnly, and SameSite attributes?	missing Secure/HttpOnly: GAESA	www.[business].com.au
OBSERVATION	Does the site publish a security.txt file (RFC 9116) for responsible-disclosure contact?	security.txt published (RFC 9116) -- positive finding	[business].com.au
OBSERVATION	Does the site disclose its backend framework via X-Powered-By or similar?	X-Powered-By: Express -- discloses technology stack	[business].com.au
OBSERVATION	Does the site disclose its web server software via the Server header?	Server: Google Frontend -- discloses technology stack	[business].com.au
OBSERVATION	Is the domain on the browser HSTS preload list?	not on the HSTS preload list (never submitted)	[business].com.au
OBSERVATION	Does the site disclose its backend framework via X-Powered-By or similar?	X-Powered-By: Express -- discloses technology stack	www.[business].com.au
OBSERVATION	Does the site disclose its web server software via the Server header?	Server: Google Frontend -- discloses technology stack	www.[business].com.au
OBSERVATION	Is the domain on the browser HSTS preload list?	not on the HSTS preload list (never submitted)	www.[business].com.au
PASS	Does the site send a Strict-Transport-Security header, and how resilient is it?	present, >= 1 year (preload-eligible threshold)	[business].com.au

RESULT	CHECK	DETAIL	ASSET
PASS	Does the site send a Referrer-Policy header, and if so, does it avoid leaking full URLs to other origins?	Header absent (modern browsers already default to strict-origin-when-cross-origin), or present with a safe value	[business].com.au
PASS	Does plain HTTP redirect to HTTPS, and stay on HTTPS for the rest of the redirect chain?	HTTP responds with a 3xx redirect to an https:// location, and every subsequent hop in the chain (if any) also stays on https://	[business].com.au
PASS	Does the server accept obviously weak/deprecated TLS ciphers (RC4, single/triple-DES, export-grade, NULL encryption, MD5 MAC)?	Server refuses a TLS 1.2 handshake offering only known-broken cipher families	[business].com.au
PASS	Does the server accept a TLS 1.0 or TLS 1.1 handshake (both deprecated by RFC 8996)?	Server refuses both TLS 1.0 and TLS 1.1 handshakes	[business].com.au
PASS	Does the server reflect an arbitrary Origin header unconditionally in Access-Control-Allow-Origin, or return an unrestricted wildcard?	No CORS header present, or Access-Control-Allow-Origin is a fixed value that does NOT match the deliberately unusual probe Origin sent -- a real allowlist, not blind reflection	[business].com.au
PASS	Does the site send a Strict-Transport-Security header, and how resilient is it?	present, >= 1 year (preload-eligible threshold)	www. [business].com.au
PASS	Does the site send a Referrer-Policy header, and if so, does it avoid leaking full URLs to other origins?	Header absent (modern browsers already default to strict-origin-when-cross-origin), or present with a safe value	www. [business].com.au
PASS	Does plain HTTP redirect to HTTPS, and stay on HTTPS for the rest of the redirect chain?	HTTP responds with a 3xx redirect to an https:// location, and every subsequent hop in the chain (if any) also stays on https://	www. [business].com.au

RESULT	CHECK	DETAIL	ASSET
PASS	Does the server accept obviously weak/deprecated TLS ciphers (RC4, single/triple-DES, export-grade, NULL encryption, MD5 MAC)?	Server refuses a TLS 1.2 handshake offering only known-broken cipher families	www.[business].com.au
PASS	Does the server accept a TLS 1.0 or TLS 1.1 handshake (both deprecated by RFC 8996)?	Server refuses both TLS 1.0 and TLS 1.1 handshakes	www.[business].com.au
PASS	Does the server reflect an arbitrary Origin header unconditionally in Access-Control-Allow-Origin, or return an unrestricted wildcard?	No CORS header present, or Access-Control-Allow-Origin is a fixed value that does NOT match the deliberately unusual probe Origin sent -- a real allowlist, not blind reflection	www.[business].com.au

CERTIFICATES

Result: pass · finding (high, medium or low) · observation · not determined

RESULT	CHECK	DETAIL	ASSET
OBSERVATION	How many days remain until the certificate actually expires?	expires within 60 days (51 day(s) remaining)	[business].com.au
OBSERVATION	How many days remain until the certificate actually expires?	expires within 60 days (51 day(s) remaining)	www.[business].com.au
PASS	Does the TLS certificate served on a hostname actually cover that hostname (CN or SAN)?	Hostname present in certificate CN or SAN list	[business].com.au
PASS	Is the certificate's validity period within the current CA/Browser Forum maximum, and if not, how far out of date is the issuance policy it reflects?	compliant with current (post-Sept-2020) CA/Browser Forum maximum	[business].com.au
PASS	Does the served certificate chain actually validate against a standard trust store?	Chain validates against the default trust store	[business].com.au

RESULT	CHECK	DETAIL	ASSET
NOT DETERMINED	Does the TLS certificate served on a hostname actually cover that hostname (CN or SAN)?	could not connect over HTTPS: a secure (TLS) connection could not be established: the server closed or rejected the handshake	docs.[business].com.au
NOT DETERMINED	Does the TLS certificate served on a hostname actually cover that hostname (CN or SAN)?	could not connect over HTTPS: a secure (TLS) connection could not be established: the server closed or rejected the handshake	portal.[business].com.au
PASS	Does the TLS certificate served on a hostname actually cover that hostname (CN or SAN)?	Hostname present in certificate CN or SAN list	www.[business].com.au
PASS	Is the certificate's validity period within the current CA/Browser Forum maximum, and if not, how far out of date is the issuance policy it reflects?	compliant with current (post-Sept-2020) CA/Browser Forum maximum	www.[business].com.au
PASS	Does the served certificate chain actually validate against a standard trust store?	Chain validates against the default trust store	www.[business].com.au

What we could not determine

Per methodology: a check that couldn't be confirmed is reported explicitly, not silently omitted.

Risk checks with no result

RESULT	CHECK	ASSET	REASON
NOT DETERMINED	How close is this domain to its registration expiry date?	[business].com.au	no expiry date field found in WHOIS response

RESULT	CHECK	ASSET	REASON
NOT DETERMINED	Does the domain have a registrar transfer lock (clientTransferProhibited or equivalent) set?	[business].com.au	auDA (.au) has no registrant-controllable transfer-lock status -- only serverTransferProhibited exists, which the registry sets itself (typically for an active dispute/hold), not something a registrant/ registrar can enable as a protective measure. This check's pass/fail semantics don't apply to .au.
NOT DETERMINED	Does the DMARC policy actually instruct receivers to act on failures?	[business].com.au	no DMARC record exists to grade (see email.dmarc.present)
NOT DETERMINED	Is DMARC aggregate reporting (rua=) configured at all?	[business].com.au	no DMARC record exists to check for a reporting address (see email.dmarc.present)
NOT DETERMINED	Is the DMARC record structurally valid enough to evaluate reliably?	[business].com.au	no DMARC record exists to validate (see email.dmarc.present)
NOT DETERMINED	If the DMARC rua= destination is on an external domain, does that domain publish the required authorization record?	[business].com.au	no DMARC record exists to check rua= authorization against (see email.dmarc.present)
NOT DETERMINED	Does the TLS certificate served on a hostname actually cover that hostname (CN or SAN)?	docs. [business].com.au	could not connect over HTTPS: a secure (TLS) connection could not be established: the server closed or rejected the handshake
NOT DETERMINED	Does the TLS certificate served on a hostname actually cover that hostname (CN or SAN)?	portal. [business].com.au	could not connect over HTTPS: a secure (TLS) connection could not be established: the server closed or rejected the handshake

Evidence we couldn't gather

Informational only, no risk verdict attached either way -- this is supporting evidence (asset discovery, inventory data) that a lookup didn't return this run.

RESULT	CHECK	ASSET	REASON
NOT DETERMINED	What certificates has Certificate Transparency logged for this domain's hostnames?	[business].com.au	crt.sh query failed or returned no entries

METHODOLOGY & LIMITATIONS

This assessment used public records and data sources, plus direct requests to [Business Name Pty Ltd]'s internet-facing services of the kind a browser or mail server makes, and a small number of targeted checks, such as testing whether outdated encryption is still accepted. No port scanning, no login attempts, no exploitation. Findings are based on observed evidence and defined check criteria; where the evidence isn't enough, we report not determined rather than guess. A pass means a check's criteria were met when we observed it. It is not a statement that [Business Name Pty Ltd] is secure, and the absence of a finding does not prove that no vulnerability exists. Every report is reviewed by a person before it is issued.

This is a point-in-time snapshot. New findings can appear, and existing ones can be resolved, between assessments, so a quarterly cadence is recommended to track drift over time.

Check catalogue version 1.0.0, published and versioned. Every check in the catalogue is reported every run, pass or fail, per methodology.

Appendix: raw evidence

This section is deliberately raw: assets and evidence exactly as observed, with timestamps, no severity and no interpretation. It's provided for a technical reader (an IT team or MSP) to verify and act on directly. The same data, unabridged, is also available as JSON or CSV.

Domains (5)

ASSET	DISCOVERY SOURCE(S)	FIRST SEEN	LAST SEEN
[8usiness].com.au	dnstwist	06 Oct 2026	06 Oct 2026
[bisiness].com.au	dnstwist	06 Oct 2026	06 Oct 2026
[business].com.au	subfinder+assetfinder+crtsh+dnsx+bruteforce	06 Oct 2026	06 Oct 2026
[usiness].com.au	dnstwist	06 Oct 2026	06 Oct 2026
b.[usiness].com.au	dnstwist	06 Oct 2026	06 Oct 2026

Third-party infrastructure (MX/NS targets etc.) (5)

ASSET	DISCOVERY SOURCE(S)	FIRST SEEN	LAST SEEN
[business]-com-au.mail.protection.outlook.com	checkdmarc	06 Oct 2026	06 Oct 2026
ns1.[dns-host].com	dns	06 Oct 2026	06 Oct 2026
ns2.[dns-host].net	dns	06 Oct 2026	06 Oct 2026
ns3.[dns-host].io	dns	06 Oct 2026	06 Oct 2026
ns4.[dns-host].org	dns	06 Oct 2026	06 Oct 2026

IP addresses (1)

ASSET	DISCOVERY SOURCE(S)	FIRST SEEN	LAST SEEN
203.0.113.42	rdap	06 Oct 2026	06 Oct 2026

Subdomains (3)

ASSET	DISCOVERY SOURCE(S)	FIRST SEEN	LAST SEEN
docs.[business].com.au	dns	06 Oct 2026	06 Oct 2026
portal.[business].com.au	dns	06 Oct 2026	06 Oct 2026
www.[business].com.au	dns	06 Oct 2026	06 Oct 2026

How many candidate hostnames were discovered and how many resolve?

ASSET	DETAIL	OBSERVED
[business].com.au	278 candidate hostname(s) seen, 4 resolve	06 Oct 2026

Does the same organisation appear to own equivalent domains under other regional/ generic TLDs?

ASSET	DETAIL	OBSERVED
[business].com.au	3 candidate TLD(s) checked, none share the home domain's registrant org	06 Oct 2026

What ASN/organisation owns the IP space this domain resolves to?

ASSET	DETAIL	OBSERVED
203.0.113.42	AS64500 ([CLOUD-HOST-AS] - [Cloud hosting provider], US), US	06 Oct 2026

What certificates has Certificate Transparency logged for this domain's hostnames?

ASSET	DETAIL	OBSERVED
[business].com.au	crt.sh query failed or returned no entries	06 Oct 2026

What nameservers does this domain delegate to?

ASSET	DETAIL	OBSERVED
[business].com.au	4 nameserver(s): ns1.[dns-host].com, ns2.[dns-host].net, ns3.[dns-host].io, ns4.[dns-host].org	06 Oct 2026
ns1.[dns-host].com	nameserver for [business].com.au	06 Oct 2026

ASSET	DETAIL	OBSERVED
ns2.[dns-host].net	nameserver for [business].com.au	06 Oct 2026
ns3.[dns-host].io	nameserver for [business].com.au	06 Oct 2026
ns4.[dns-host].org	nameserver for [business].com.au	06 Oct 2026

What paths does the site's robots.txt declare disallowed?

ASSET	DETAIL	OBSERVED
[business].com.au	No robots.txt entries discovered during the crawl	06 Oct 2026

Which hostnames from a pinned common-infrastructure wordlist actually resolve, beyond what passive discovery already found?

ASSET	DETAIL	OBSERVED
[business].com.au	277 wordlist candidate(s) tried, 3 resolved: docs.[business].com.au, portal.[business].com.au, www.[business].com.au	06 Oct 2026

What mail servers does this domain route inbound mail to?

ASSET	DETAIL	OBSERVED
[business].com.au	1 MX host(s): [business]-com-au.mail.protection.outlook.com	06 Oct 2026
[business]-com-au.mail.protection.outlook.com	MX host for [business].com.au	06 Oct 2026

What email addresses does the site's own crawled content publish?

ASSET	DETAIL	OBSERVED
[business].com.au	None found	06 Oct 2026

What typosquat/homoglyph permutations of the domain are registered, regardless of whether they have live mail?

ASSET	DETAIL	OBSERVED
[bisiness].com.au	registered lookalike, no live mail exchange -- replacement permutation	06 Oct 2026
[business].com.au	4 registered lookalike(s) found, 3 with no live mail	06 Oct 2026
[usiness].com.au	registered lookalike, no live mail exchange -- omission permutation	06 Oct 2026
b.[usiness].com.au	registered lookalike, no live mail exchange -- subdomain permutation	06 Oct 2026

Is the registrant's WHOIS contact information hidden behind a privacy/proxy service?

ASSET	DETAIL	OBSERVED
[business].com.au	registrant details appear directly published (no privacy/proxy service detected)	06 Oct 2026

Was the WHOIS record updated recently?

ASSET	DETAIL	OBSERVED
[business].com.au	No update recorded in the last 30 days	06 Oct 2026

What country is the registrant contact listed in, per WHOIS?

ASSET	DETAIL	OBSERVED
[business].com.au	no registrant country field found (often redacted post-GDPR, with or without an active privacy service)	06 Oct 2026

Which registrar administers this domain, per WHOIS?

ASSET	DETAIL	OBSERVED
[business].com.au	registrar: [Registrar Pty Ltd]	06 Oct 2026