



DOMAIN SECURITY ASSESSMENT

October 4, 2026 at 4:28 AM CT

Public internet-facing posture

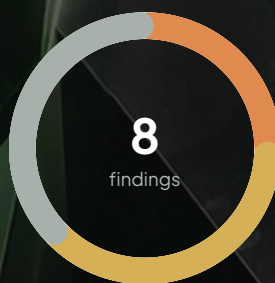
platterivermarketing.com

SEVERITY MIX



CRITICAL

Scanner grade F



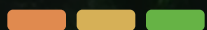
- 0 CRITICAL
- 2 HIGH
- 3 MEDIUM
- 3 LOW

3 passed

POSTURE

Each block is one check from this scan

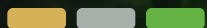
Email



No DMARC record found

HIGH

Website



Content-Security-Policy header missing

MEDIUM

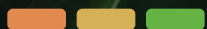
DNS



DNSSEC is not enabled

LOW

TLS



HTTP does not redirect to HTTPS

HIGH

saintcybersecurity.com

(531) 625-2111

[Book a free security review](#)

SAINT Technology Services

Page 1 of 10

OVERVIEW

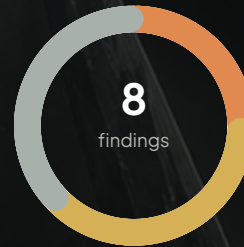
Executive summary

SCORE



CRITICAL
Scanner grade F

SEVERITY MIX



0 CRITICAL
2 HIGH
3 MEDIUM
3 LOW

3 passed

POSTURE Each block is one check from this scan

Email

No DMARC record found

HIGH

Website

Content-Security-Policy header missing

MEDIUM

DNS

DNSSEC is not enabled

LOW

TLS

HTTP does not redirect to HTTPS

HIGH

platterivermarketing.com scored 59 out of 100. The risk label for that score is CRITICAL.

The scan recorded 8 findings: 0 critical, 2 high, 3 medium, and 3 low.

Across email, website, DNS, and TLS, Email is HIGH, Website is MEDIUM, DNS is LOW, and TLS is HIGH.

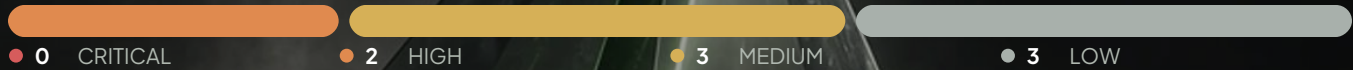
The priority plan lists critical and high findings as immediate, medium findings as next, and low or informational findings as hardening.

Mail provider: Microsoft 365

FINDINGS

What needs attention

Each card is one result from this scan. The severity label is the scanner's label.



Email Security

HIGH

No DMARC record found

WHY IT MATTERS

DMARC is what actually tells the world's mail servers to reject spoofed mail from this domain – and it's what gives you visibility into who is sending as you. Without it, SPF and DKIM have no enforcement.

OBSERVED

No TXT record at `_dmarc.platterivermarketing.com`

REMEDIATION

1. Publish a TXT record at `_dmarc.<domain>` starting with `v=DMARC1;p=none; rua=mailto:you@domain` to begin monitoring.
2. Review aggregate reports for 2–4 weeks to identify all legitimate senders.
3. Move policy to `p=quarantine`, then `p=reject`.

HOW SAINT CAN HELP

SAINT runs the full DMARC rollout – monitoring, sender identification, and staged enforcement to `p=reject` – as part of our managed email security service.

Email Security

MEDIUM

No DKIM keys found at common selectors

WHY IT MATTERS

DKIM cryptographically signs outbound mail. Without it, DMARC alignment depends entirely on SPF, and forwarded mail from this domain will often fail authentication. (Note: this check probes common selectors; a custom selector may exist.)

OBSERVED

Probed selectors: selector1, selector2, google, default, dkim, k1, s1, s2, mail, zoho

REMEDATION

1. Enable DKIM signing in your mail platform (built into Microsoft 365 and Google Workspace).
2. Publish the platform-provided CNAME/TXT selector records in DNS.
3. Rotate keys at least annually; use 2048-bit keys.

HOW SAINT CAN HELP

SAINT enables and verifies DKIM across every platform that sends as your domain, including third-party tools like invoicing and marketing systems.

Website Security

HIGH

HTTP does not redirect to HTTPS

WHY IT MATTERS

Visitors who type the bare domain get an unencrypted connection an attacker on the same network can intercept.

OBSERVED

http://platterivermarketing.com returned 530

REMEDATION

1. Add a permanent 301 redirect from http:// to https:// at the web server or CDN.

HOW SAINT CAN HELP

One-line fix in most stacks - SAINT includes this in the web hardening pass.

Website Security

MEDIUM

Strict-Transport-Security (HSTS) header missing

WHY IT MATTERS

Without HSTS, browsers will still attempt insecure HTTP on first visit, enabling SSL-stripping attacks.

OBSERVED

Header absent on <https://platterivermarketing.com>

REMEDIATION

1. Send Strict-Transport-Security: max-age=31536000; includeSubDomains once all subdomains serve HTTPS.
2. Consider HSTS preload once stable.

HOW SAINT CAN HELP

SAINT deploys HSTS carefully - with subdomain inventory first, so nothing breaks.

MEDIUM

Content-Security-Policy header missing

WHY IT MATTERS

CSP is the primary browser-side defense against cross-site scripting and injected malicious scripts (the mechanism behind card-skimming attacks like Magecart).

OBSERVED

Header absent

REMEDIATION

1. Deploy CSP in Report-Only mode to inventory legitimate script sources.
2. Enforce a policy restricting script-src to known origins.

HOW SAINT CAN HELP

SAINT builds and tunes CSP for your actual site so it blocks injections without breaking functionality.

Website Security

LOW

X-Content-Type-Options header missing

WHY IT MATTERS

Browsers may MIME-sniff responses, which can turn uploaded files into executable script.

OBSERVED

Header absent

REMEDIATION

1. Send X-Content-Type-Options: nosniff on all responses.

HOW SAINT CAN HELP

Included in SAINT's standard security-header deployment.

DNS & Domain

LOW

DNSSEC is not enabled

WHY IT MATTERS

Without DNSSEC, resolvers cannot verify DNS answers for this domain are authentic, leaving room for cache-poisoning and redirection attacks.

OBSERVED

AD flag not set on validating resolver

REMEDIATION

1. Enable DNSSEC at your DNS host (one-click in Cloudflare) and publish the DS record at your registrar.

HOW SAINT CAN HELP

SAINT handles the registrar/DNS-host coordination and validates the chain end to end.

DNS & Domain

LOW

No CAA record – any certificate authority can issue certs for this domain

WHY IT MATTERS

CAA restricts which CAs may issue TLS certificates for the domain, shrinking the attack surface for fraudulent certificate issuance.

OBSERVED

No CAA records

REMEDIATION

1. Publish a CAA record authorizing only the CA(s) you actually use, e.g. 0 issue "letsencrypt.org".

HOW SAINT CAN HELP

SAINT sets CAA as part of our DNS hardening baseline.

SEQUENCE

Priority action plan

Items stay in the severity the scanner assigned.

Immediate	2	
Next	3	
Hardening	3	

Immediate

Critical and high findings.

HIGH**No DMARC record found**

Publish a TXT record at `_dmarc.<domain>` starting with `v=DMARC1; p=none; rua=mailto:you@domain` to begin monitoring.

HIGH**HTTP does not redirect to HTTPS**

Add a permanent 301 redirect from `http://` to `https://` at the web server or CDN.

Next

Medium findings.

MEDIUM**No DKIM keys found at common selectors**

Enable DKIM signing in your mail platform (built into Microsoft 365 and Google Workspace).

MEDIUM**Strict-Transport-Security (HSTS) header missing**

Send Strict-Transport-Security: `max-age=31536000; includeSubDomains` once all subdomains serve HTTPS.

MEDIUM**Content-Security-Policy header missing**

Deploy CSP in Report-Only mode to inventory legitimate script sources.

Hardening

Low and informational findings.

LOW**X-Content-Type-Options header missing**

Send X-Content-Type-Options: `nosniff` on all responses.

LOW**DNSSEC is not enabled**

Enable DNSSEC at your DNS host (one-click in Cloudflare) and publish the DS record at your registrar.

LOW**No CAA record – any certificate authority can issue certs for this domain**

Publish a CAA record authorizing only the CA(s) you actually use, e.g. 0 issue "letsencrypt.org".

PASSED CHECKS

What's already protected

These checks passed at scan time. A pass is not a certification.

Email Security

SECURE SPF published with hard-fail (-all)

Website Security

SECURE Site served over HTTPS with a valid certificate

SECURE Clickjacking protection in place



Let's secure what's next.

Book a free security review and walk through these results with SAINT Technology Services.

saintcybersecurity.com

(531) 625-2111

Book a free security review

<https://saintsecured.com/book>



© 2026 SAINT Technology Services · Lincoln, Nebraska · Veteran-owned. Scan results are based on publicly observable records at scan time and are informational, not a penetration test, certification, or vulnerability assessment.