



The League of Lazy Sysadmins

Cloudflare Executive Report Synthetic Data (I'm not saying it's aliens, but...)

100% organic, cage-free, gluten-free portfolio data

Prepared for: **The BOFH (Bastard Operator From Hell)**

Date: **15/Apr/2026**

Period: **2026-04-01 to 2026-04-14 (UTC)**

Permission Denied (you shouldn't be reading this)

Notes:

- Generated with generate_cf_output_data. Proudly assembled by monkeys with typewriters. Warranty void in 52 countries.

Multi-Zone Security Summary

2026-04-01 to 2026-04-14 (UTC)

Zones (sorted by score asc (worst first), tie-break zone name (a-z))

Zone	Score	Grade	Critical Risks	Warnings
hogsmeade.io	0	F	4	6
nautilus.net	47	D+	1	3
rivendell.dev	47	D+	1	3
trantor.org	47	D+	1	3
wayne-enterprises.io	100	A+	0	0

Common risks (count of zones affected)

Risk	Zones
Apex record not proxied - origin IP exposed to attackers (APEX-001)	4 zones
Certificate expires in {days} days - renew immediately (CERT-001)	4 zones
DNSSEC disabled - domain spoofing risk (DNS-001)	4 zones
TLS/SSL mode Full without CA-validated origin certificate - upgrade to Full (Strict). (TLS-003)	3 zones
Browser Integrity Check is off - consider enabling to reduce automated abuse. (SEC-006)	1 zone
DDoS protection disabled - availability at risk (SEC-001)	1 zone
Minimum TLS version is {version} at edge - raise to at least 1.2 immediately. (TLS-004)	1 zone
Cloudflare Security Level is off or essentially off - known threats are barely challenged. (SEC-002)	1 zone
TLS/SSL mode Off - enable HTTPS immediately. (TLS-001)	1 zone
TLS 1.3 is not enabled at edge - enable for stronger defaults. (TLS-005)	1 zone

Grade distribution

Band	Zones
A+ (>=95)	1 zones
A (85-94)	0 zones
B (75-84)	0 zones
C+ (65-74)	0 zones
C (55-64)	0 zones
D+ (45-54)	3 zones
D (35-44)	0 zones
F (<35)	1 zones

Executive summary

wayne-enterprises.io · 2026-04-01 to 2026-04-14 (UTC) - Last 14 Days

Verdict HEALTHY	Score 100 / A+	Zone status active	TLS/SSL Mode strict	Always HTTPS on
Requests 2.5M ▲7.5%	Encrypted requests 2.4M ▲8.7%	Cache hit ratio 84.7% ▲3	Blocked/Challenged 39K Δ+5K	Mitigation rate 2.1% ▲1.5
4xx rate 0.4%	5xx rate 0.1%	Edge p50/p95 76/292 ms	Origin response 180 ms	
DNS queries 1.6M ▲5.3%	Avg DNS QPS 1.3	DNS records 92	Proxied 74 ▲1	DNS-only 18 ▼1
Audit events 12	Cert packs 4	Expiring ≤30d 0	Cert expires -	Apex protection proxied

Takeaways

[i] [CMP-001] Comparing to: 2026-03-18 to 2026-03-31

Executive summary

hogsmeade.io · 2026-04-01 to 2026-04-14 (UTC) - Last 14 Days

Verdict HEALTHY	Score 0 / F	Zone status active	TLS/SSL Mode off	Always HTTPS off
Requests 2.3M ▲7.5%	Encrypted requests 1.6M ▲8.7%	Cache hit ratio 18.3% ▲3	Blocked/Challenged 312K ▲+37K	Mitigation rate 17.7% ▲1.5
4xx rate 3.6%	5xx rate 1.3%	Edge p50/p95 332/1280 ms	Origin response 790 ms	
DNS queries 1.8M ▲5.3%	Avg DNS QPS 1.5	DNS records 88	Proxied 19 ▲1	DNS-only 69 ▼1
Audit events 163	Cert packs 4	Expiring ≤30d 2	Cert expires -	Apex protection exposed

Takeaways

- (!) [APEX-001] Apex record not proxied - origin IP exposed to attackers
- ✗ [TLS-001] TLS/SSL mode Off - enable HTTPS immediately.
- ✗ [TLS-004] Minimum TLS version is 1.0 at edge - raise to at least 1.2 immediately.
- (!) [TLS-005] TLS 1.3 is not enabled at edge - enable for stronger defaults.
- (!) [SEC-006] Browser Integrity Check is off - consider enabling to reduce automated abuse.
- (!) [DNS-001] DNSSEC disabled - domain spoofing risk
- ✗ [SEC-002] Cloudflare Security Level is off or essentially off - known threats are barely challenged.
- (!) [WAF-001] Web Application Firewall disabled - no attack protection

Actions

- [>] [SEC-002] Enable Cloudflare automatic Security Level (Security app) - avoid off or essentially off.
- [>] [TLS-007] Enable Always Use HTTPS - redirects HTTP to HTTPS for all traffic.
- [>] [DNS-001] Enable DNSSEC - prevents DNS spoofing and domain hijacking.
- [>] [TLS-001] Change SSL/TLS mode to Full (Strict) for end-to-end encryption with certificate validation.
- [>] [WAF-001] Review Web Application Firewall (WAF) and rate-limiting baseline.
- [>] [APEX-001] Enable proxy on apex A/AAAA record - hides origin IP.
- [>] [CERT-002] Renew TLS certificate before expiry - prevents outages.
- [>] [COR-005] Review audit log - check for unauthorized changes.

Executive summary

rivendell.dev · 2026-04-01 to 2026-04-14 (UTC) - Last 14 Days

Verdict HEALTHY	Score 47 / D+	Zone status active	TLS/SSL Mode full	Always HTTPS on
Requests 2.2M ▲7.5%	Encrypted requests 2.1M ▲8.7%	Cache hit ratio 53.8% ▲3	Blocked/Challenged 142K Δ+17K	Mitigation rate 8.7% ▲1.5
4xx rate 1.2%	5xx rate 0.3%	Edge p50/p95 143/551 ms	Origin response 340 ms	
DNS queries 1.5M ▲5.3%	Avg DNS QPS 1.3	DNS records 90	Proxied 48 ▲1	DNS-only 42 ▼1
Audit events 41	Cert packs 4	Expiring ≤30d 1	Cert expires -	Apex protection exposed

Takeaways

- (!) [APEX-001] Apex record not proxied - origin IP exposed to attackers
- (!) [TLS-003] TLS/SSL mode Full without CA-validated origin certificate - upgrade to Full (Strict).
- (!) [DNS-001] DNSSEC disabled - domain spoofing risk
- ✖ [CERT-001] Certificate expires in 1 days - renew immediately
- [i] [TLS-004] Minimum TLS version is 1.2. Evaluate TLS 1.3 adoption when client compatibility allows.
- [i] [TLS-006] HSTS enabled but configuration is suboptimal: max-age is 15552000s (set at least 31536000 for one year); Include Subdomains is off.
- [i] [SEC-007] Email obfuscation is off. Enable to reduce email address harvesting.
- [i] [TLS-009] Opportunistic Encryption is off - optional edge HTTPS hint for HTTP clients.

Actions

- [>] [DNS-001] Enable DNSSEC - prevents DNS spoofing and domain hijacking.
- [>] [TLS-003] Upgrade TLS/SSL mode from Full to Full (Strict) - enables CA certificate validation.
- [>] [APEX-001] Enable proxy on apex A/AAAA record - hides origin IP.
- [>] [CERT-002] Renew TLS certificate before expiry - prevents outages.

Executive summary

trantor.org · 2026-04-01 to 2026-04-14 (UTC) - Last 14 Days

Verdict HEALTHY	Score 47 / D+	Zone status active	TLS/SSL Mode full	Always HTTPS on
Requests 2.2M ▲7.5%	Encrypted requests 2.1M ▲8.7%	Cache hit ratio 53.8% ▲3	Blocked/Challenged 142K Δ+17K	Mitigation rate 8.7% ▲1.5
4xx rate 1.2%	5xx rate 0.3%	Edge p50/p95 143/551 ms	Origin response 340 ms	
DNS queries 1.5M ▲5.3%	Avg DNS QPS 1.3	DNS records 90	Proxied 48 ▲1	DNS-only 42 ▼1
Audit events 41	Cert packs 4	Expiring ≤30d 1	Cert expires -	Apex protection exposed

Takeaways

- (!)[APEX-001] Apex record not proxied - origin IP exposed to attackers
- (!)[TLS-003] TLS/SSL mode Full without CA-validated origin certificate - upgrade to Full (Strict).
- (!)[DNS-001] DNSSEC disabled - domain spoofing risk
- ✖[CERT-001] Certificate expires in 1 days - renew immediately
- [i][TLS-004] Minimum TLS version is 1.2. Evaluate TLS 1.3 adoption when client compatibility allows.
- [i][TLS-006] HSTS enabled but configuration is suboptimal: max-age is 15552000s (set at least 31536000 for one year); Include Subdomains is off.
- [i][SEC-007] Email obfuscation is off. Enable to reduce email address harvesting.
- [i][TLS-009] Opportunistic Encryption is off - optional edge HTTPS hint for HTTP clients.

Actions

- [>][DNS-001] Enable DNSSEC - prevents DNS spoofing and domain hijacking.
- [>][TLS-003] Upgrade TLS/SSL mode from Full to Full (Strict) - enables CA certificate validation.
- [>][APEX-001] Enable proxy on apex A/AAAA record - hides origin IP.
- [>][CERT-002] Renew TLS certificate before expiry - prevents outages.

Executive summary

nautilus.net · 2026-04-01 to 2026-04-14 (UTC) - Last 14 Days

Verdict HEALTHY	Score 47 / D+	Zone status active	TLS/SSL Mode full	Always HTTPS on
Requests 2.2M ▲7.5%	Encrypted requests 2.1M ▲8.7%	Cache hit ratio 53.8% ▲3	Blocked/Challenged 142K Δ+17K	Mitigation rate 8.7% ▲1.5
4xx rate 1.2%	5xx rate 0.3%	Edge p50/p95 143/551 ms	Origin response 340 ms	
DNS queries 1.5M ▲5.3%	Avg DNS QPS 1.3	DNS records 90	Proxied 48 ▲1	DNS-only 42 ▼1
Audit events 41	Cert packs 4	Expiring ≤30d 1	Cert expires -	Apex protection exposed

Takeaways

- (!)[APEX-001] Apex record not proxied - origin IP exposed to attackers
- (!)[TLS-003] TLS/SSL mode Full without CA-validated origin certificate - upgrade to Full (Strict).
- (!)[DNS-001] DNSSEC disabled - domain spoofing risk
- ✖[CERT-001] Certificate expires in 1 days - renew immediately
- [i][TLS-004] Minimum TLS version is 1.2. Evaluate TLS 1.3 adoption when client compatibility allows.
- [i][TLS-006] HSTS enabled but configuration is suboptimal: max-age is 15552000s (set at least 31536000 for one year); Include Subdomains is off.
- [i][SEC-007] Email obfuscation is off. Enable to reduce email address harvesting.
- [i][TLS-009] Opportunistic Encryption is off - optional edge HTTPS hint for HTTP clients.

Actions

- [>][DNS-001] Enable DNSSEC - prevents DNS spoofing and domain hijacking.
- [>][TLS-003] Upgrade TLS/SSL mode from Full to Full (Strict) - enables CA certificate validation.
- [>][APEX-001] Enable proxy on apex A/AAAA record - hides origin IP.
- [>][CERT-002] Renew TLS certificate before expiry - prevents outages.

Appendix

Metric notes

- Average DNS QPS is period-level average throughput and should be interpreted with query totals and peak intervals together.
- Cache hit ratio depends on workload profile (static vs dynamic/API) and should be compared as a trend for the same zone.
- Mitigation metrics reflect sampled events and configured actions; trend direction is more reliable than single-day absolute counts.
- Unique visitors are deduplicated for the selected period; daily totals may not match dashboard windows that include partial current-day traffic.

Security Controls Reference (NIST 800-53)

[AU-2] Audit Events (COR-005)

[CM-6] Configuration Settings (SEC-002, SEC-003)

[SC-12] Cryptographic Key Establishment and Management (CERT-001, CERT-002)

[SC-13] Cryptographic Protection (CERT-001, CERT-002, TLS-001, TLS-003, TLS-004, TLS-005, TLS-006)

[SC-18] Mobile Code (SEC-007)

[SC-20] Secure Name / Address Resolution Service (APEX-001, DNS-001)

[SC-7] Boundary Protection (APEX-001, COR-003, SEC-001)

[SC-8] Transmission Confidentiality and Integrity (TLS-001, TLS-003, TLS-004, TLS-005, TLS-006, TLS-007, TLS-009)

[SI-3] Malicious Code Protection (SEC-006, WAF-001)

[SI-4] Information System Monitoring (CMP-001, COR-001, COR-003, COR-004, COR-005, SEC-001, SEC-002, SEC-003, SEC-006, WAF-001)