FINETIC TRUST CENTRE

INTERNET-FACING SECURITY ASSESSMENT

The public boundary, tested from the outside.

A redacted account of owner-authorised black-box testing against Young Studio and Finetic services without source, repository or credential access.

EVIDENCE-BACKED RESULT

No critical unauthenticated compromise was demonstrated.

ASSESSMENT

YS-BBX-2026-07

PUBLISHED

28 July 2026

SCOPE

Unauthenticated public Internet boundary

EVIDENCE CLASS

Owner-authorised first-party assessment

Executive result

> **First-party assessment.**
> This is not independent certification, a formal compliance audit or a guarantee that the service is vulnerability-free. A zero-match scanner result applies only to the signatures and conditions tested.

The assessment did not authenticate as a Finetic administrator, bypass protected Finetic APIs, retrieve a protected media library or active session, find a publicly exposed repository or environment file, extract an application secret, demonstrate a confirmed injection or remote-code-execution result, or leave a sustained outage or persistent configuration change.

Coverage

AREA	EVIDENCE COLLECTED
Network exposure	All 65,535 TCP ports on the primary public address, with external verification to distinguish NAT-loopback effects.
DNS and names	Public DNS, certificate-transparency records, 20,000 DNS candidates and 20,000 virtual-host candidates.
Public content	156,650 public content candidates per Finetic host.
Known signatures	6,318 Nuclei medium/high/critical templates issuing 96,955 requests.
HTTP parsing	12 CL.TE and TE.CL request-smuggling probes.
Published images	Public OCI tag metadata and representative historical-image secret scanning.

Confirmed improvements

- Excessive public licence and customer metadata was removed from the main Finetic deployment.
- Previously actionable `tar`, `undici` and `brace-expansion` dependencies were removed or upgraded.
- External TCP/5222 exposure was no longer reachable from four independent regions on retest.
- Plaintext chat error responses and explicit APISIX patch disclosure were removed from the previously observed route.
- Finetic v0.1.92 suppresses the Express framework-identification response header.

Open and unverified items

- DMARC remains absent and the current SPF record uses soft-fail.
- CAA, DNSSEC, MTA-STS and TLS-RPT were not present at the time of testing.
- A separate, non-Finetic household media service remained externally reachable and should be assessed or restricted separately.

- The intentionally stopped reviewer deployment and retired chat hostnames did not complete TLS on retest. Application-level remediation is not claimed as verified while those services are offline.
- Source review, authenticated production testing, destructive restore testing and independent certification were outside this assessment.

How this relates to the release assessment

The external black-box assessment tested the Internet-facing boundary without credentials or source access. The separate Finetic v0.1.92 application assessment tested a disposable restricted container through anonymous, administrator and standard-user flows. Neither assessment replaces the other.

Safe publication statement

This public edition deliberately excludes credentials, access tokens, private keys, internal addresses, private media paths, personal viewing records and details that would materially increase attackability. The underlying owner-authorised work remains private.

Finetic Trust Centre · YS-BBX-2026-07 · Public evidence at youngstudio.uk/trust/