

Is medicaredentalinsurance.com a scam? TrustSniffer's high-risk assessment: 0/100

medicaredentalinsurance.com

Verdict

0

OUT OF 100

CRITICAL RISK

medicaredentalinsurance.com shows high-risk / scam indicators.

This assessment found strong scam indicators. Do not pay, sign in, or share personal details with this site.

Sensitive Interaction Risk

Governance Risk

Assessed 2026-08-19 by automated analysis. Classification confidence 55%.

What this site appears to be

A marketing/informational page for ServerAvatar describing server management features: deployment, SSL/security, monitoring, and documentation. No forms or direct transaction prompts are present in the captured content.

Evidence status and limitations

- Evidence completeness: UNKNOWN
- The real-world operator identity was not independently verified.
 - Module-level completeness metadata is unavailable for this legacy report.

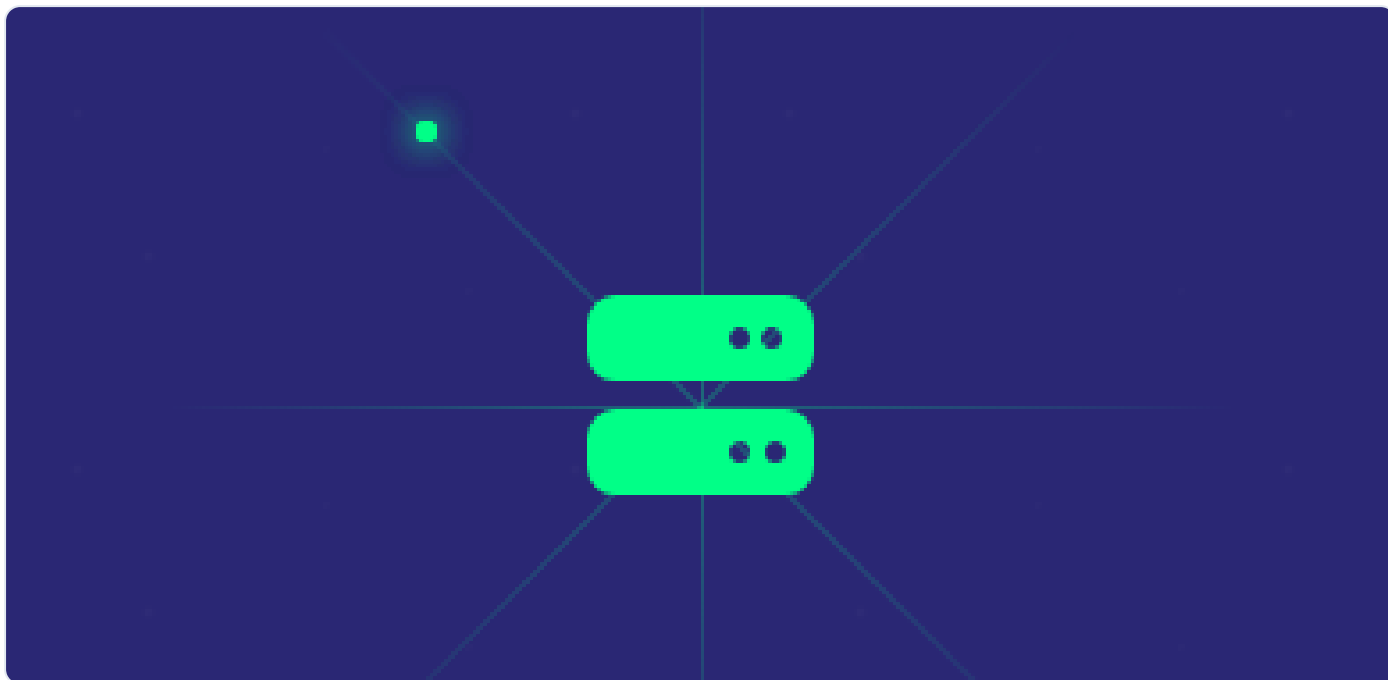
At a glance

The checks that decide most of this verdict.

Malware engines	12 flagged it VirusTotal	RISK
Google Safe Browsing	Not listed Google	CLEAR
Abuse reports on the host	0 reports AbuseIPDB; shared hosting inflates this count	NOTED
Domain age	7.0 years old Registered history	CLEAR
Web archive	Archived since 2010 Public history exists	CLEAR
Certificate	Encrypted connection Issued by WE1	NOTED

The page as captured

<https://medicaresdentalinsurance.com/>



What medicaredentalinsurance.com served when TrustSniffer captured it on 2026-08-19. The page may look different now.

Key findings

- Automated classification: Sensitive Interaction Risk.
- Domain age: 3 to 10 years (registration continuity).
- Public web-archive history exists since 2010.
- At least one reputation service TrustSniffer consulted had flagged this domain at assessment time.

Full analysis

Security Alert

Fortinet, Kaspersky, Sophos flagged this site in external intelligence checks, indicating elevated compromise/scam exposure that requires immediate caution.

The website at medicaredentalinsurance.com presents itself as a ServerAvatar-branded server-management platform, describing application deployment, SSL and security functions, performance monitoring, and documentation for developers, agencies, and businesses. Its apparent model is informational SaaS promotion or managed-service provision, although the ServerAvatar presentation does not align clearly with the domain name.

Scam/Impersonation Risk

The site carries a material scam and impersonation concern because external security intelligence recorded malicious detections and confirmed blacklist listings, including detections from Fortinet, Kaspersky, and Sophos. This conflicts with the otherwise benign captured homepage, which contains no login form, payment prompt, hidden form, or direct transaction mechanism. The domain-to-brand mismatch is an additional identity-context anomaly: a domain named for dental insurance presents ServerAvatar server-management content. No separate conflicting legal-entity names, confirmed brand impersonation, or phishing form were observed in the

supplied page evidence. The presence of a valid certificate or stable page behavior does not offset the confirmed external reputation concern.

EVIDENCE

- External reputation telemetry recorded 12 malicious detections from 17 evaluated results; Fortinet, Kaspersky, and Sophos were among the flagged vendors, and blacklist status was confirmed by two sources.
- The homepage title is “Proudly Managed By ServerAvatar,” while the assessed domain is medicaredentalinsurance.com.
- The homepage contains 0 forms, no sensitive form, no login form, and no hidden forms; its captured status was HTTP 200.

Regulatory Verification Notes

The captured content describes a server-management SaaS offering rather than an insurance, investment, or other regulated financial service. It does not state a license, registration number, or regulated authorization, so regulatory status is not established from the page and should be treated as a disclosure gap rather than independent evidence of fraud. Identity verification remains unconfirmed; the ServerAvatar branding is an on-page presentation, not proof of affiliation with the real-world operator. The domain has a multi-year registration history through NameSilo, LLC, but that administrative fact does not resolve the external security contradiction or establish the operator’s identity.

EVIDENCE

- WHOIS records show registration on 2019-09-03 and an age of 6.96 years; the registrar is NameSilo, LLC.
- Archive telemetry records 23 snapshots spanning 2010–2025, with 16 years tracked.
- The site is served on AS13335 by CLOUDFLARENET - Cloudflare, Inc., US.
- TLS uses issuer WE1 with DV validation and is valid to 2026-11-09T18:31:28+00:00.

What to Verify Next

Before any sensitive interaction, an organization should independently confirm that the ServerAvatar branding and the assessed domain are connected through an official, separately established corporate channel. If the site is intended to provide insurance or another regulated service, the claimed operator and authorization should be checked directly against the relevant jurisdictional registry. Security teams should also obtain an independent reputation review and preserve the current page capture before permitting the domain in enterprise workflows. Any contact or support channel should be confirmed through an independently sourced official channel rather than relying solely on the assessed site.

EVIDENCE

- The homepage identifies ServerAvatar but provides no captured corporate identity, license number, or regulatory authorization.
- The page presents informational product content and documentation links rather than a formal legal, licensing, or service-terms disclosure.
- Behavioral analysis recorded 2 successful runs, with 0 wallet-connect runs, 0 password-external forms, and 0 cloaking detections.

Summary Verdict

The overall posture is **critical trust risk**, with sensitive interactions not supportable on the available evidence. The cleanly presented SaaS content is outweighed by confirmed external malicious and blacklist signals, while the real-world operator remains unverified.

Infrastructure Integrity

Cloudflare CDN/WAF protection and Cloudflare edge hosting provide a mitigating layer against direct origin exposure, but all observed addresses were CDN edges and the origin was not independently visible. This infrastructure can reduce routine network exposure; it is not evidence that the website or its operator is legitimate.

Closing Assessment

Enterprise controls should restrict the domain from login, credential, payment, and other sensitive workflows until independent identity, authorization, and security validation are completed.

Written analysis generated 2026-08-19 by the TrustSniffer Analysis Engine from the evidence in this report.

What the analysis found

2 findings contributed to this verdict, raised by registration and ownership, analysis engine, behaviour in a sandbox, external reputation.

01 Governance Risk

- The registration record withholds contact details for the operator.
Registration and ownership rule:KF_WHOIS_HIDDEN
- Registration details are held behind a privacy service, so no operator is named publicly. This is common and legal, and it also means there is nobody to check.

Registration and ownership rule:KF_WHOIS_PRIVATE

02 Sensitive Interaction Risk

- The analysis matched a pattern TrustSniffer treats as a direct threat to a visitor.
Analysis engine signal:direct_threat
- Most of what the page loaded came from other domains rather than from this one.
Behaviour in a sandbox rule:BEHAV_EXTERNAL_RATIO_HIGH
- An external threat feed lists this domain: either Google Safe Browsing marked it malicious, or a significant number of malware engines flagged it.
External reputation rule:EXT_BLACKLIST_CRITICAL

Identity verification

Status	UNVERIFIED
Identity score	30/100
Identity verification confidence	25%

- No on-site identity signals detected

Identity verification measures whether the site can be independently connected to a real-world brand or person. It is separate from the classification confidence.

What TrustSniffer observed

First-party facts recorded during the assessment of medicaredentalinsurance.com.

- The request stayed on medicaredentalinsurance.com. It was not redirected to another domain. CLEAR
- Registration is published under NameSilo, LLC. CLEAR
- DNS for this domain is served by cloudflare.com, across 2 name servers. NOTED
- The registration is paid up to 2026-09-03. NOTED
- The earliest public archive of this site is from 2010-09-13. CLEAR
- It is hosted on CLOUDFLARENET, from a server in US. NOTED

Domain intelligence

Registrar	NameSilo, LLC
Hosting	CLOUDFLARENET - Cloudflare, Inc., US
Country	US
Server IP	2606:4700:3031::6815:39c
Name servers	CRUZ.NS.CLOUDFLARE.COM, NILE.NS.CLOUDFLARE.COM
SSL issuer	WE1
SSL expiry	2026-11-09
Domain age	6.96 years (continuous registration)
Domain expiry	2026-09-03

Archive first seen	2010-09-13
Archive snapshots	Not counted (archive lookup incomplete)
Reputation	VirusTotal: 12 flagged AbuseIPDB: 0 reports Google Safe Browsing: 0 matches

About this assessment

A trust score summarises the evidence TrustSniffer could collect about medicaredentalinsurance.com at assessment time. It is a starting point for your own judgement, not a guarantee: a high score means the signals were consistent with a legitimately operated site, a low or critical score means several risk patterns were present.

TrustSniffer assesses a website from the evidence it can collect at a point in time: domain registration and age, hosting and certificate, the content the site served, and third-party reputation feeds. A score is a summary of that evidence, not a guarantee and not a legal finding. There is no human rating and no user review in it. A site can change after it is assessed.

This report online: <https://trustsniffer.com/report/medicaredentalinsurance.com> · assessed 2026-08-19