Target: demo.example-business.com

Generated: May 11, 2026
Report ID: A976289BA3C7

EXPOSURE ASSESSMENT SUMMARY

42 MEDIUM

AI Exposure Score: 42 · Confidence: 82%

SERVICES OBSERVED **4**

ISSUES SURFACED **3**

Score 42/100 — Moderate exposure. Improvements recommended. Completing the actions below is projected to reduce your exposure score.

4 open ports; remote-admin surface present; no database surface; web: HTTP(80), HTTPS(443), HTTP-alt(8080).

ADJUSTED RISK (IDENTITY-WEIGHTED): 52 MEDIUM · Adjusted for identity exposure. AI exposure score unchanged for monitoring.
Primary Risk Driver: Identity exposure (breached credentials detected)

LIKELIHOOD OF COMPROMISE

MEDIUM

Based on:

- Exposed internet-facing services
- Identity breach signals detected

What this means: An attacker could realistically attempt access using known credentials and exposed services.

CHANGE SINCE LAST SCAN

RISK DELTA	PORTS OPENED	PORTS CLOSED	PREVIOUS SCAN
+12 (worse)	1	0	May 4, 2026

RDP port appeared since last scan — risk increased.

1 port opened · risk delta +12 (worse)

TOP RISKS CONTRIBUTING TO ACCESS

LIKELY ATTACK PATH

1. Attacker obtains breached credentials from public datasets
2. Identifies exposed internet-facing service (e.g. web, DNS)
3. Attempts access using credential reuse or brute force
4. Gains foothold if authentication controls are weak

This is the most common real-world compromise path when identity exposure is detected.

Primary context: compromised credentials increase likelihood of exploitation.

HIGH 3389/tcp

Remote desktop is publicly accessible

WHY RDP exposed to the internet is one of the most common ransomware entry points. Attackers actively scan for port 3389 and attempt credential brute force.

FIX *Restrict RDP to VPN or trusted IP ranges only. Disable if not actively used.*

Owner: Firewall / network admin

MEDIUM 80/tcp, 8080/tcp

HTTP traffic is not redirected to HTTPS

WHY Unencrypted HTTP allows credential interception and session hijacking on any non-TLS connection.

FIX *Configure a 301 redirect from HTTP to HTTPS on all web services.*

Owner: Web server / IT admin

MEDIUM 8080/tcp

Alternate HTTP port (8080) is exposed

WHY Publicly reachable staging or alternate web services increase attack surface unnecessarily.

FIX *Close port 8080 if not serving active traffic. Apply HTTPS redirect if retained.*

Owner: Web server / IT admin

OPEN PORTS — FULL INVENTORY

PORT	PROTO	SERVICE	CONTEXT	STATUS
80	tcp	http	HTTP Web Service	Review
443	tcp	https	HTTPS Web Service (TLS)	Expected
3389	tcp	rdp	RDP Remote Desktop	Review
8080	tcp	http-alt	HTTP Alternate	Review

IMMEDIATE NEXT ACTIONS

1	**Redirect HTTP to HTTPS (ports 80, 8080)** *Est. ~5 min*	Ensure your web server returns a 301 redirect for all plain-HTTP traffic. Close port 8080 / 8880 if they serve no active purpose. Enforce TLS 1.2+ with strong cipher suites on any remaining HTTPS endpoints.
2	**Restrict remote-access ports (3389)** *Est. ~15 min*	Remote access ports publicly reachable are a top attack vector. If required: enforce VPN or IP allow-list plus strong MFA. If not required: block at the firewall immediately.
3	**Re-scan to confirm improvement** *Est. ~1 min*	After applying fixes, run a new snapshot from your VigilantAI dashboard. Your score will update and a new compliance evidence entry will be created automatically.

REMEDIATION & VERIFICATION

Apply each action below, then re-run a snapshot from your VigilantAI dashboard to generate updated verification evidence.

HIGH **Close RDP (port 3389)**

1. Block port 3389 inbound on your firewall.
2. Use a VPN for remote access instead of direct RDP.
3. Enable Network Level Authentication if RDP must remain open.

COMPLIANCE & INSURANCE MAPPING

Use your Evidence Trail to generate time-stamped documentation for auditors and cyber insurance underwriters.

FRAMEWORK	CONTROL	HOW VIGILANTAI SATISFIES IT
HIPAA Security Rule	§164.308(a)(1)	Satisfies the external network risk analysis requirement for covered entities and BAs.
HIPAA Security Rule	§164.312(e)(1)	TLS posture analysis evidences transmission security controls for ePHI in transit.
PCI-DSS	Req. 1	Documents network security controls and perimeter exposure for cardholder data environment.
PCI-DSS	Req. 11	Point-in-time external scan satisfies security testing and vulnerability management requirements.
SOC 2 (CC6)	CC6.1	Logical access control evidence: external attack surface inventory maintained and monitored.

FRAMEWORK	CONTROL	HOW VIGILANTAI SATISFIES IT
Cyber Insurance	Underwriter Q	Demonstrates continuous external monitoring — satisfies Coalition, Cowbell, and Chubb SMB policy requirements.

WEB SECURITY POSTURE

NEEDS REVIEW

TLS Certificate
INVALID

HTTPS / HSTS
HTTP to HTTPS: NO
HSTS: NO

Security Headers
CSP: NO
X-Frame: NO
Configured: —

Email Security
SPF: NO
DMARC: NO

What this does NOT include:

- Authenticated application testing or login-protected pages
- Internal network exposure or endpoint vulnerability assessment
- Third-party services and shadow IT connected to your domain

This assessment reflects external surface only. Generate the full report for complete security analysis.

IDENTITY BREACH EXPOSURE

MEDIUM RISK

1 of 4 tested business email addresses appears in known public breach datasets. Credential reuse against the exposed RDP service represents a realistic attack path.

Likelihood of compromise: MEDIUM

POTENTIAL ATTACK PATH

Common email patterns exposed

-> Potential credential reuse attempts

-> Increased unauthorized access risk

Confidence: MEDIUM

Why this matters: Exposed credentials are commonly reused across systems, increasing the likelihood of account takeover.

Generate the full report to see complete breach details and remediation steps.

SCOPE & LIMITATIONS

This report reflects a point-in-time external snapshot of internet-reachable services. It does not include authenticated testing, internal network visibility, or a guarantee that all exposures were discovered. Absence of findings does not imply absence of risk. References may include NVD and CISA KEV data. Support: getvigilantai.com/contact