Raven Security -- Securing the web, one system at a time.

Fixed-scope security reviews for websites, web applications, and AI features. We test your predefined domains using our own modified open-weight security models--with zero training on client data--prove every finding, and re-scan for free after you fix.

HOW OUR MODELS WORK (ZERO TRAINING ON YOUR DATA)

- Modified open-weight models: We modify the weights of open security models directly and edit our testing logic and system prompts by hand from real human security findings.
- Zero training datasets: We do not maintain a training corpus, and we never train or fine-tune models on client traffic, source responses, credentials, or findings.
- Predefined scope & production safety: Our outbound scope filter restricts testing to the exact domains you authorize in writing. Linked outside systems (like ERPs or third-party vendors) are never probed -- they are listed under 'Observed, Not Tested'.

HOW AN ENGAGEMENT RUNS (4 STEPS)

01. Authorize the scope: You list the exact domains, applications, and test login roles in a short written scope. We never touch a host that isn't on that signed list.

02. Models + reviewers test: Our modified open-weight models and human reviewers test your predefined scope from the outside and inside each login role, inside strict rate and safety guardrails.

03. Get the report & proof: You receive an OWASP-mapped report ordered by what to fix first: what is wrong, why it matters, the attached proof, and what to change--plus any outside URLs observed.

04. Fix, re-scan & attest: Your team makes the fixes. Within 45 days (60 on Infrastructure), we re-scan the scope for free and issue your 1-page Letter of Attestation.

PUBLISHED FIXED PRICING (USD -- NO SUBSCRIPTION)

SITE -- $1,800 (Small business)

Your public website and perimeter, tested from the outside the way an automated or AI attacker sees it.

- Up to 3 internet-facing hosts you name
- Public pages, forms, plugins, and exposed files
- Check of any public-facing AI chat widget
- 1 complimentary re-scan within 45 days + Letter of Attestation

APPLICATION -- $4,500 (Small to mid-size | Most Popular)

One web application and its APIs, tested from the outside and from inside every login role you give us.

- 1 web application + public site (up to 4 hosts)
- Up to 3 user roles/logins tested for permission drift
- APIs, multi-step workflows, and in-app AI features
- 1 complimentary re-scan within 45 days + Letter of Attestation

INFRASTRUCTURE -- $9,500 (Mid-size organization)

Up to ten of your internet-facing hosts, applications, and AI workflows, tested together the way attackers chain them.

- Up to 10 predefined hosts & 2 applications (up to 6 logins)
- Full AI & Agent Deep-Dive (RAG, tool-calling, prompt injection) included
- Live walkthrough call + OWASP-mapped report
- 1 complimentary re-scan within 60 days + Executive Attestation

MODULAR ADD-ONS & NORTH AMERICAN OFFICES

- AI & Agent Feature Deep-Dive (+$1,500): For companies shipping a customer chatbot, RAG search over company documents, automated intake forms, or tool-calling AI agents.
- Extra Logins or Hosts Pack (+$750): Straightforward math when your application has more permission tiers (such as regional managers, dealers, or read-only auditors) or a few extra subdomains.
- Annual or Post-Launch Re-Verification (25% off plan rate): We don't sell subscriptions. If

Sample Report: Northline Fasteners Inc. (Invented illustration)

Application + AI & Agent Deep-Dive | Wholesale industrial distribution | 42 employees | Initial review: Oct 12-15, 2026 | Complimentary re-scan: Oct 28, 2026

PREDEFINED DOMAINS IN SCOPE & TEST LOGINS

- Scope host: www.northline.example (Public marketing site & catalog)
- Scope host: portal.northline.example (Contractor ordering & invoice portal)
- Scope host: api.northline.example (Portal REST & AI order-assistant API)
- Scope host: files.northline.example (Spec sheets & compliance document host)
- Test login: Contractor A (acct_1042 -- standard customer role)
- Test login: Contractor B (acct_2089 -- second customer role for cross-account checks)
- Test login: Warehouse Staff (staff_04 -- internal fulfillment role)

PRIORITIZED FINDINGS (ITEMS RS-01 AND RS-02)

RS-01 | [FIX FIRST] | portal.northline.example | OWASP API1:2023 | Broken Object Level Authorization | Re-scan: CLOSED

1. What we found: A signed-in contractor can open any other contractor's order history and negotiated unit pricing.

2. Why it matters: Any customer with a valid login can read competitors' custom discount tiers, shipping addresses, and past invoices by changing the order number in the address bar.

3. Proof attached: Signed in as Contractor A (acct_1042), requested an order belonging to Contractor B (acct_2089) and received the full invoice record.

```
Session: acct_1042 (Contractor A) -> GET https://portal.northline.example/api/orders/88412 -> HTTP
200 OK (returned account_id: acct_2089, net_tier: 'Distributor-18%', total: $14,820.00)
```

4. What to change: In the order-detail handler, scope the database query by the signed-in session's account_id (WHERE id = $1 AND account_id = $2) instead of checking only that a user is logged in.

Re-scan verification: Verified Oct 28: requesting /api/orders/88412 as acct_1042 now returns HTTP 404 Not Found.

RS-02 | [FIX FIRST] | api.northline.example | OWASP LLM06:2025 | Sensitive Information Disclosure (RAG) | Re-scan: CLOSE

1. What we found: The portal's AI order assistant answers questions using quote PDFs belonging to other customer accounts.

2. Why it matters: All uploaded custom quote PDFs are indexed in a shared vector collection without tenant filtering. A contractor asking the assistant to 'summarize recent stainless anchor quotes' receives pricing quoted to other companies.

3. Proof attached: Prompted '/api/assistant/chat' as Contractor A; the response cited and quoted a custom PDF uploaded under Contractor B's account.

```
Session: acct_1042 -> POST /api/assistant/chat -> Response cited source_doc:
'quote_acct_2089_oct.pdf' (belonging to Contractor B)
```

4. What to change: Attach 'account_id' metadata to every document chunk at indexing time, and enforce a mandatory server-side metadata filter ('account_id == session.accountId') on every vector search query.

Re-scan verification: Verified Oct 28: vector retrieval now filters by session account_id; cross-account prompts return zero chunks.

PRIORITIZED FINDINGS (ITEMS RS-03 AND RS-04)

RS-03 | [HIGH] | files.northline.example | OWASP A05:2021 | Security Misconfiguration | Re-scan: CLOSED

1. What we found: Last year's internal IT audit report and a customer CSV export are publicly downloadable without a login.

2. Why it matters: Documents uploaded to a temporary folder for an external auditor were never removed and have already been indexed by search crawlers.

3. Proof attached: Fetched the directory listing and file headers from an unauthenticated browser session with no cookies.

```
Unauthenticated -> GET https://files.northline.example/shared/2025-audit-summary.pdf -> HTTP 200 OK (application/pdf, 1.4 MB, Last-Modified: 2025-11-04)
```

4. What to change: Remove the '/shared/' public directory, disable directory listing on the file host, and require a signed, expiring download URL from the portal.

Re-scan verification: Verified Oct 28: '/shared/' returns HTTP 404 and directory listing is disabled.

RS-04 | [MEDIUM] | www.northline.example | OWASP A06:2021 | Vulnerable and Outdated Components | Re-scan: STILL OPE

1. What we found: A product gallery plugin installed for a 2022 trade show is four years out of date and still active.

2. Why it matters: The installed version carries two public unauthenticated file-upload advisories that automated bots routinely scan for across the web.

3. Proof attached: The public asset manifest on 'www.northline.example' serves the plugin's scripts and version header ('v2.1.4', released 2022).

```
Unauthenticated -> GET https://www.northline.example/wp-content/plugins/pro-gallery-lite/readme.txt -> Stable tag: 2.1.4
```

4. What to change: Uninstall the unused 'pro-gallery-lite' plugin completely, or update it to the current patched release ('v4.8+').

Re-scan verification: Observed Oct 28: plugin was deactivated in the CMS menu, but the plugin folder is still reachable on disk. Delete the directory to finish closing.

PART 3: OBSERVED OUTSIDE OF SCOPE (NOT TESTED)

Our models never push on or probe domains outside your signed written scope. When outgoing links or script references to external hosts are observed during testing, we record them below for your awareness:

Host: erp.northline-internal.example

- Where seen: Linked from staff footer menu on portal.northline.example
- Role: Internal ERP web login exposed to the public internet (not on signed scope list)
- Action taken: Observed link only. Zero requests sent. Flagged for client to put behind VPN or add to a future scope.

Host: legacy-2023.northline.example

- Where seen: Referenced in an old JavaScript bundle on www.northline.example
- Role: Forgotten staging subdomain from a 2023 redesign
- Action taken: Observed DNS reference only. Not probed because it was outside the 4 named hosts.

Host: checkout.stripe.com / calendly.com

- Where seen: Embedded on www.northline.example/request-account
- Role: Third-party payment and scheduling providers
- Action taken: Blocked automatically by our outbound scope filter. We never test third-party vendor infrastructure.

Letter of Security Assessment & Remediation Attestation

Ref: RS-2026-1048-ATT | Issued by: Raven Security Inc. (Toronto, ON) / Raven Security LLC (New York, NY)

1. ASSESSMENT SUMMARY

This letter confirms that Raven Security performed an independent, fixed-scope security assessment of the internet-facing systems named below for Northline Fasteners Inc. between October 12 and October 15, 2026, followed by a verification re-scan on October 28, 2026.

2. PREDEFINED SCOPE & ROLES VERIFIED

- www.northline.example (Public marketing site & catalog)
- portal.northline.example (Contractor ordering & invoice portal)
- api.northline.example (Portal REST & AI order-assistant API)
- files.northline.example (Spec sheets & compliance document host)

3. TESTING STANDARDS & METHODOLOGY

Testing combined modified open-weight security models and human verification mapped against the OWASP Web Security Testing Guide (WSTG v4.2), OWASP API Security Top 10 (2023), OWASP Top 10 for LLM Applications (2025), and the Penetration Testing Execution Standard (PTES).

4. REMEDIATION & RE-SCAN VERIFICATION OUTCOME

All Critical ('Fix first') and High-severity findings identified during the initial review--including cross-account authorization and AI retrieval isolation--were remediated by Northline Fasteners Inc. and independently verified as Closed during the October 28, 2026 re-scan. One Medium-severity hygiene item remains scheduled for removal.

5. INDEPENDENCE & SIGN-OFF

Raven Security is an independent security assessment practice. We do not sell remediation software or development hours for the systems we review. Client credentials and evidence were handled in encrypted storage with zero model training on client data.

Signed: Alessandro Ravelli (OSCP, GWAPT, CISSP) -- Principal Reviewer & Founder

Raven Security LLC (New York, NY) | Raven Security Inc. (Toronto, ON)