HADRIAN

NOVA

THE AI THAT HACKS YOU
SHOULD BE ON YOUR SIDE.

Hadrian Nova is an agentic pentesting engine that continuously identifies external attack vectors that could be exploited today. Its fleet of AI hacker agents runs offensive tests against your external attack surface on demand, identifies what's actually exploitable, and delivers validated findings within hours before real-world threat actors discover them. No scheduling. No vendor dependency. No out-of-date reports.

THE WAY OFFENSIVE SECURITY WAS MEANT TO BE.

YOUR SCHEDULE. YOUR SCOPE.

You define what gets tested, adjust scope on your terms, and get repeatable coverage without renegotiating an SOW or waiting on procurement.

NO DAYS OFF. NO OFF DAYS.

Pentesting that's available 24/7. Validated findings within hours, at the same depth and quality every time. Run it before an audit, after a release, or ahead of a board meeting.

HACKER-TRAINED. BATTLE-TESTED.

Nova's AI is trained by elite offensive security professionals. It learns your environment, maps your stack, and chains vulnerabilities the way a skilled attacker would.

WHY HADRIAN

Most tools discover assets or test them. Only Hadrian does both.

BREADTH.

Hadrian's event-driven architecture discovers every subdomain, API, and cloud instance automatically. Configuration changes trigger real-time discovery.

DEPTH.

On-demand, compliance-ready pentests with human-in-the-loop validation. You control the scope. No procurement cycles, no quarterly windows, no waiting.

ADAPTIVE.

Nova learns each organization's environment and evolves with attacker tactics, techniques, and procedures. Coverage deepens over time, not just repeats.

99.5%
False positives eliminated

80%
Faster time to resolution

10x
Visibility of critical vulns

The Hadrian advantage

	MANUAL PENTEST	HADRIAN NOVA
SCHEDULING	Weeks of coordination	On demand, start today
SCOPING	Negotiation with vendor	You define it, you control it
TURNAROUND	Weeks to months	Hours
CONSISTENCY	Depends on the tester	Same quality every time
COVERAGE	Same playbooks each time	Evolves with attacker tradecraft
VALIDATION	Varies by engagement	Human-reviewed, zero false positives

HOW IT WORKS

1. DEFINE SCOPE

Select targets and testing parameters on your terms. No vendor negotiation.

2. CLICK LAUNCH

Kick off the pentest on demand. No scheduling delays, no lead time.

3. AI-DRIVEN TESTING

Agentic AI executes real attacker techniques, chaining vulnerabilities like a skilled pentester.

4. HUMAN REVIEW

Expert offensive security practitioners validate novel and high-impact findings.

5. REPORT DELIVERY

Validated findings with reproduction steps and execution evidence delivered within hours.

No software to install. No complex setup. Deploy in under 5 minutes. Same day results.

KEY CAPABILITIES

- **DEEP ATTACK PATH EXPLORATION**

  Simulate how attackers chain vulnerabilities and escalate access within real asset context.

- **CONTEXT-RICH ASSET ANALYSIS**

  Builds and retains knowledge about systems, and configurations for more precise testing.

- **EXPERT-LEVEL OFFENSIVE REASONING**

  Replicate how skilled hackers prioritize, pivot, and adapt without human capacity limits.

- **CONTROLLED SCOPING AND REPEATABILITY**

  Define what gets tested and re-run deep assessments as environments evolve.

- **VALIDATED FINDINGS WITH TRANSPARENCY**

  Full visibility into attack paths and exploitation steps, with human-reviewed results for accuracy and safety.

- **HUMAN AND AI COLLABORATION**

  Combine machine-scale testing with the expertise of elite hackers, enabling deeper validation, faster iteration, and more reliable results.

TAKE THE FIRST STEP IN THE SHOES OF YOUR ADVERSARY

Hadrian is an external exposure management provider that pioneered the AI attacker's perspective approach. Its agentic engine offers frictionless, always-on discovery, validation, and mobilization of an organization's most critical cyber risks. Trained by elite hackers with top offensive knowledge, Hadrian adapts to the organization's unique environment to continuously probe, discover, and validate the risks that attackers can actually exploit.

LEARN MORE: HADRIAN.IO

FROST & SULLIVAN BEST PRACTICES AWARDS

GIGAOM RADAR REPORT 2025

Gartner Peer Insights™ 4.9/5 ★

AICPA SOC

ISO 27001