HADRIAN

Hadrian Nova vs Traditional Penetration Testing

THE CASE FOR RETHINKING PENETRATION TESTING

Penetration testing is one of the most important tools in a security team's arsenal. It's also one of the least adapted to the way modern organizations operate. Attack surfaces change daily. New assets come online with every deployment. Acquisitions, cloud migrations, and third-party integrations expand the perimeter faster than any scheduled engagement can cover. The traditional pentest model was designed for a slower world. That's not a knock on the testers. It's a structural critique of the delivery model itself.

FREQUENCY MISMATCH.

Most organizations test once or twice a year. Their attack surface changes daily. The gap between tests is the gap in which exposures go unvalidated.

SCOPE RIGIDITY.

Traditional engagements require pre-negotiated scope, rules of engagement, and scheduling weeks in advance. The attack surface doesn't wait for a statement of work.

INCONSISTENT RESULTS.

Two testers given the same scope will find different things. Findings depend on individual skill, time pressure, and what the tester decides to prioritize. There is no reproducibility guarantee.

SLOW FEEDBACK LOOPS.

From kickoff to final report typically takes two to four weeks. By the time findings are triaged and tickets are created, the environment has already changed.

MANUAL HANDOFF FRICTION.

Results arrive as a PDF. Findings get re-entered into ticketing systems, validated by internal teams, and tracked through remediation manually. Retesting requires a new engagement.

AGENTIC PENTESTING: A DIFFERENT MODEL

Agentic pentesting uses autonomous AI agents to execute genuine penetration testing, not vulnerability scanning, against an organization's external attack surface. Specialized agents chain techniques together, exploit real vulnerabilities, and demonstrate actual impact, the same way a human tester would, but across a broader scope and on a faster timeline.

Hadrian Nova is an agentic pentesting engine built on Hadrian's external exposure management platform. Nova's Orchestrator coordinates a fleet of specialized AI agents, each expert in a distinct attack class, adapting in real time to concentrate effort on the most promising attack paths. Hadrian's offensive security specialists steer the investigation, validate every finding, and sign off every report. Zero false positives. Because Nova is built on the same platform as Hadrian's external exposure management engine, every test starts with what Hadrian already knows about your attack surface. That context makes every test smarter.

No software to install. Deploy in under five minutes. Results the same day.

HADRIAN NOVA VS TRADITIONAL PENTESTING

DIMENSION	TRADITIONAL PENTESTING	HADRIAN NOVA
TESTING FREQUENCY	1-2 times per year, scheduled months in advance	On demand. Test before releases, audits, or whenever the attack surface changes
TIME TO FIRST FINDING	Days to weeks after engagement begins	Hours
SCOPE	Fixed and pre-negotiated. Changes require a new SOW	Flexible. Adjust in real time to match the current attack surface
COST STRUCTURE	$20,000-$80,000+ per engagement	Consumption-based pricing per test. Predictable and scalable
CONSISTENCY	Varies by tester. No two engagements are identical	Deterministic and reproducible
RETESTING	Requires a new paid engagement	Built in at no additional cost
REMEDIATION WORKFLOW	PDF report, manual ticket creation	Findings integrated into security platforms, auto-triaged
FALSE POSITIVE RATE	Generally low but varies by tester	Zero. Every finding validated by Hadrian's offensive security team
COVERAGE BREADTH	Limited by tester time and engagement window	Full defined scope tested without time pressure
COMPLIANCE	Point-in-time attestation	Complements mandated tests. Pre-validate before audit windows

WHEN TO USE WHICH

Agentic pentesting dramatically increases the scope and frequency of offensive security programs, but is not a wholesale replacement for traditional engagements. The most effective security programs use both.

USE HADRIAN NOVA WHEN

you need to validate your exposure between annual engagements, test on demand before a release or audit, rapidly assess newly acquired assets, or retest remediated issues without waiting for a new engagement cycle.

USE TRADITIONAL PENTESTING WHEN

a compliance framework requires a named, certified tester and formal attestation, or when the testing objective involves deep business logic review in complex applications where human creativity adds the most value.

USE BOTH WHEN

preparing for an audit. Run Nova first to find and fix issues, then use the traditional engagement to validate and produce the attestation. Fewer surprises, faster remediation, cleaner report.

ABOUT HADRIAN

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 organization's most critical cyber risks. Trained by elite hackers with top offensive knowledge, Hadrian adapts the organization's unique environment to continuously probe, discover and validate the risks that attackers can actually exploit.

TO LEARN MORE: HADRIAN.IO

REQUEST A DEMO