HADRIAN

ATLAS

DISCOVER EVERYTHING. VALIDATE WHAT'S REAL. ACT ON WHAT MATTERS.

A NEW BREED OF AGENTIC EXTERNAL EXPOSURE MANAGEMENT

Hadrian Atlas is a continuous external exposure management platform that discovers your entire external attack surface and validates which exposures are actually exploitable. A fleet of purpose-built AI agents, each specialized for a specific attack class, chains techniques the way a human attacker would across thousands of assets simultaneously. Every finding is independently validated before your team is notified. No false positives. No wasted triage time.

CHALLENGE

External attack surfaces are expanding faster than security teams can track them. New subdomains, APIs, cloud instances, and third-party integrations appear with every deployment, acquisition, and configuration change. Traditional approaches rely on periodic scanning, asset inventories that go stale between cycles, and alert volumes that overwhelm teams with unverified noise. By the time a real exposure is identified, triaged, and prioritized, the attacker has already moved.

SOLUTION

Atlas discovers assets the way an attacker would, starting with no scope rather than working from a pre-defined inventory. Its event-driven architecture detects changes in real time, triggering new tests the moment your attack surface shifts. There are no scan windows and no scheduled cycles.

A fleet of bespoke AI agents validates every exposure. Each agent is purpose-built for a specific attack class, equipped with its own toolset and exploitation logic, trained by Hadrian's offensive security team. Agents chain vulnerabilities together and exploit real application behavior, not just version-matching CVEs against a list of assets. Testing depth is adaptive and concentrates where attacker progress is actually possible, not spread thinly across every asset.

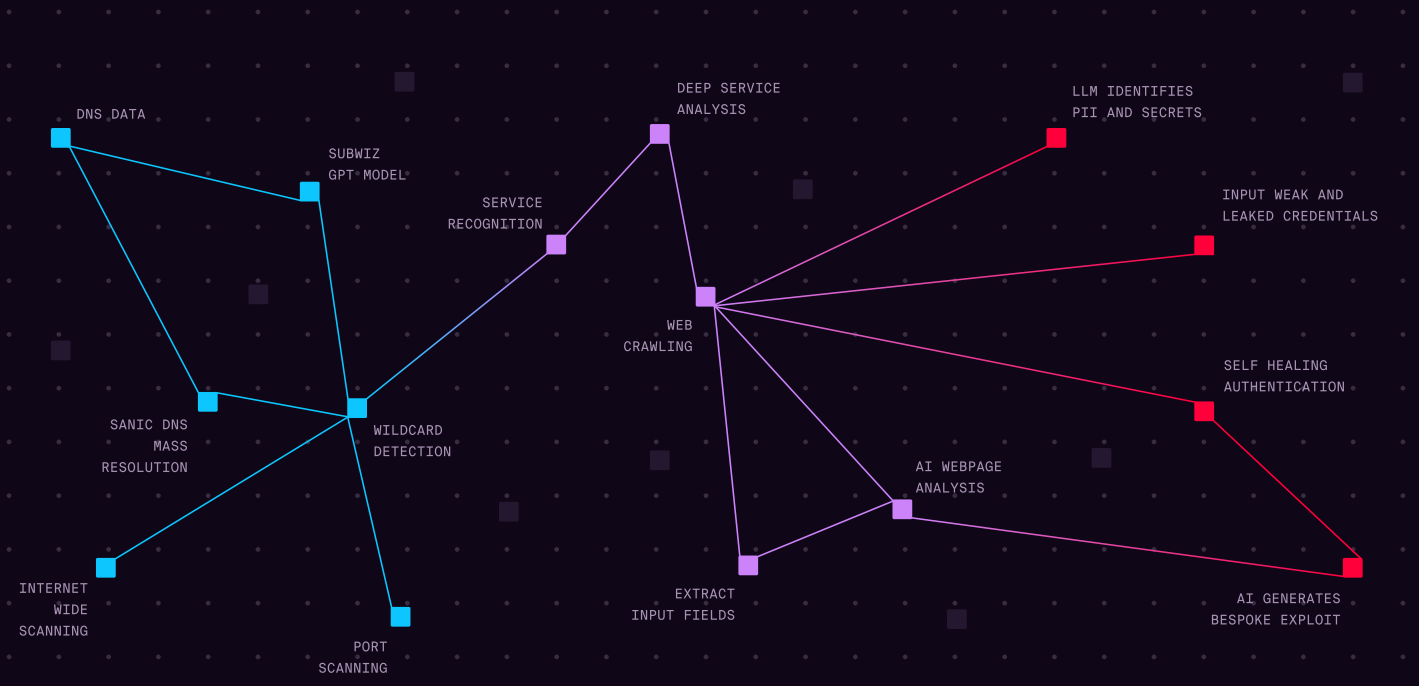
Findings are prioritized by real-world exploitability and business context, not just CVSS scores. Every exposure is independently validated before a notification is sent, so your team only acts on what is confirmed and exploitable.

BENEFITS

- **ZERO FALSE POSITIVES**
  Every finding is independently validated before your team is notified.
- **10X VISIBILITY OF CRITICAL VULNERABILITIES.**
  Discover shadow IT, forgotten assets, and new infrastructure across your entire external perimeter.
- **ATTACKER-ALIGNED TESTING.**
  Atlas goes deep where attackers can actually progress, not uniformly across every asset.
- **80% REDUCTION IN MEAN TIME TO REMEDIATE.**
  Findings include proof of exploit, reproduction steps, and remediation guidance.
- **88% FASTER ALERT INVESTIGATION.**
  Cut average investigation time from 25 minutes to 3 minutes with validated, contextualized findings.
- **8 HOURS SAVED PER SOC ANALYST PER WEEK.**
  Eliminate time spent chasing unverified alerts. Every notification from Atlas is validated and exploitable.
- **DEPLOYS IN UNDER 5 MINUTES.**
  No software to install, no agents, no credentials required. Cloud-deployed and operational immediately.

INTRODUCING ATLAS: VALIDATE EXTERNAL EXPOSURE

Atlas runs a continuous loop across your external attack surface. Discovery agents map every reachable asset maintaining a live inventory that updates hourly. The event-driven architecture launches specialized vulnerability agents to test it immediately. Each agent is purpose-built for a specific attack class, trained by Hadrian's offensive security team, and equipped with its own exploitation toolset. Every finding is validated independently before reaching your team, and prioritized by business context.



KEY CAPABILITIES

- **CONTINUOUS ASSET DISCOVERY.**

Hourly scans map every subdomain, API, cloud instance, certificate, and service endpoint automatically.

- **EVENT-DRIVEN ARCHITECTURE.**

Configuration changes trigger immediate retesting. No scan windows, no gaps.

- **AI-NATIVE EXPLOITATION.**

Agents chain vulnerabilities and exploit real application behavior, not just pattern-matching CVEs.

- **ADAPTIVE TESTING DEPTH.**

Testing concentrates where attacker progress is actually possible, not applied uniformly across every asset.

- **BUSINESS CONTEXT PRIORITIZATION.**

Findings ranked by exploitability and business impact, not generic CVSS scores.

- **INTEGRATIONS.**

Out of the box automations are built for popular SIEM and ticketing systems, with REST API for custom integrations.

RECOGNISED BY LEADING ANALYSTS

Gartner Peer Insights 4.9/5 ★

GIGAOM RADAR REPORT 2025

FROST & SULLIVAN BEST PRACTICES AWARDS

COMPLIANT WITH

AICPA SOC

ISO 27001

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 an 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, VISIT: HADRIAN.IO

REQUEST A DEMO