

The Hacker Perspective

Agentic hacking identifies, validates, and prioritizes exposures before adversaries strike. With Hadrian, agentic AI can proactively find and mitigate OWASP Top Ten issues, zero-day and known vulnerabilities, and misconfigurations across your entire external attack surface.

Preempt your adversaries and prevent breaches before they can launch an attack. Hadrian helps you move from a reactive to a proactive cybersecurity approach by automating attack surface management, adversarial exposure validation, and threat exposure management.

Hadrian continuously monitors your entire digital infrastructure, scaling to identify vulnerabilities across both on-prem and cloud environments, while providing real-time, actionable security insights. AI agents trained by experienced hackers ensure that security teams can focus on the highest-priority risks, preventing potential breaches and strengthening your security posture across the entire attack surface.

What makes Hadrian different

Always On

Hadrian tests 24/7 at scale across the entire attack surface, ensuring real-time visibility and protection against emerging threats.

High Accuracy

Hadrian eliminates noise by validating exposures with agentic AI adversarial testing tailored to specific business context via brand fingerprinting.

Instant Deployment

Hadrian requires no setup or maintenance, providing instant attack surface insights for the latest threats without adding operational burden.

Key benefits



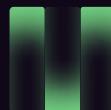
Discover Assets

Gain real-time asset insights with automated reconnaissance and contextualization. Hadrian's asset inventory saves customers an average of 10+ hours per week.



Reveal Exposures

10x visibility of critical risks with in-depth assessments. Hadrian's agentic threat assessment architecture replicates real-world hacker techniques and behaviors, eliminating false positives..



Resolve Issues

Reduce MTTR by 80% with streamlined workflows and integrations. Use step-by-step remediation guidance and collaborate to accelerate resolution.

Hadrian Offensive Security Platform

The dashboard provides a high-level overview of the platform's performance and threat landscape. Key metrics include:

- ASSETS:** 224
- DOMAINS:** 108
- IPS:** 086
- CERTIFICATES:** 074

Security level: 17F

Severity	Count
CRITICAL	002
HIGH	002
MEDIUM	005

Mean time to remediate: (Hadrian vs. Industry Benchmark)

Time	Hadrian	Industry Benchmark
100+ DAYS	0	100+
75+ DAYS	0	75+
50+ DAYS	0	50+
25+ DAYS	1	25+
0+ DAYS	100	0+

Unresolved risks: All risks

New domains: All domains

Outside-In Perspective

Hadrian continuously scans your external attack surface, identifying exposures just as an adversary would.

Event-Based Architecture

Hadrian responds to changes in your environment in real time, ensuring threats are detected as they emerge.

Zero-Touch Deployment

Hadrian requires no installation or agent setup, providing instant visibility into your attack surface.

Agentic AI Validation

Automated AI active testing emulates real-world attack techniques to uncover vulnerabilities with precision.

Context-Based Prioritization

Intelligent risk scoring helps teams focus on the most critical vulnerabilities based on real-world exploitability.

Seamless Integration

Easily integrates with existing security workflows, enhancing your defenses without adding complexity.

Best in class

Hadrian's offensive security reveals how real-world attacks could compromise applications and infrastructure. Our agentic platform continuously tests to comprehensively assess internet-facing assets. The cloud-based, agentless technology is constantly updated and improved by Hadrian's ethical hacker team.



Gartner
4.9/5 ★
Peer Insights™

