

AI-Driven Offensive Security

Dynamic asset discovery,
Continuous penetration testing,
AI-driven threat prioritization.

Proactively mitigate threats by embracing the hacker's perspective. Hadrian reveals exploitable vulnerabilities by continuously assessing threats across your entire business with the precision of a world-class team of penetration testers. Embrace offensive security and remediate your critical exposures with less effort.

■ DISCOVER EVERYTHING

10x visibility of critical risks

Gain real-time visibility of every asset and exposure in your digital attack surface. Hadrian's 24x7x365 analysis keeps you fully aware at all times, minimizing the window of vulnerability.

■ AUTOMATE TRIAGE

10 hours saved per week (avg)

Focus on exploitable risks and remove false positives with in-depth penetration testing. Hadrian's fully automated assessments are unobtrusive and enriched with threat intel.

■ RESOLVE FASTER

80% reduction in MTTR

Accelerate response time and create a step change in security posture. Hadrian triggers and orchestrates workflows to streamline remediation and prevent threat actors from attacking.

The Hadrian Advantage

At the heart of the platform is Orchestrator AI, the industry's most advanced threat discovery engine, replicating a team of hackers to identify risks around the clock.



Discovery

Built in the cloud, Hadrian is deployed in minutes and immediately makes an inventory of all of your digital assets using its neural network graph of the internet. Cloud assets are seamlessly imported and cataloged via agentless cloud connectors.



Contextualization

Hadrian's platform contextualizes your assets to understand what they are and how they are interconnected to reveal how an adversary could conduct an attack. Machine learning algorithms build a picture of your topology and potential threats.



Validation

Orchestrator AI actively tests assets to find exploitable OWASP risks, known and zero-day vulnerabilities, and exposed and misconfigured services. The non-intrusive tests are chained together to simulate complex multidimensional attacks.



Prioritization

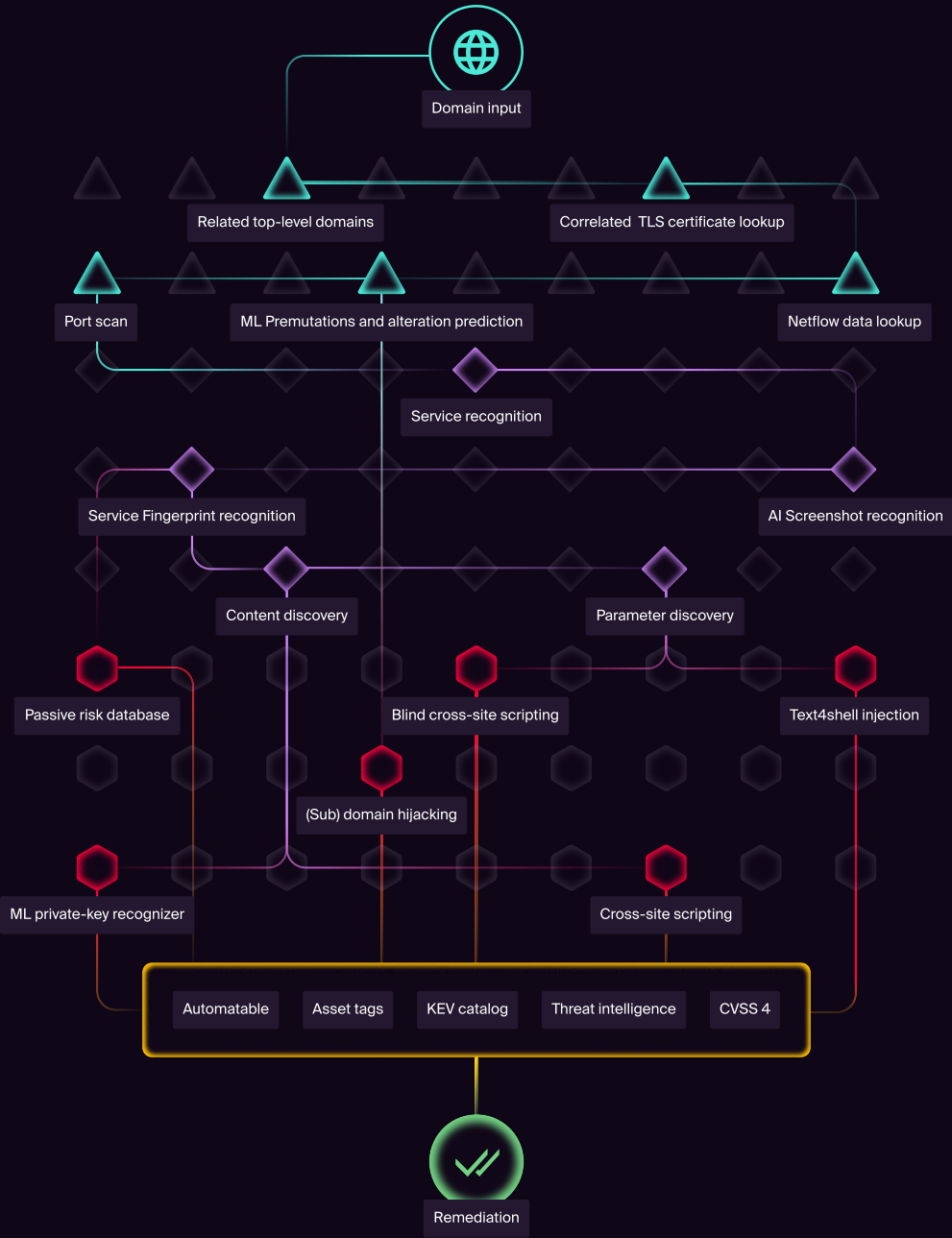
Findings are filtered into true positives and potential exposures, enriched with threat intel, business and asset context, and technical factors to prioritize the highest risk. Proprietary scoring algorithms learn and become more accurate over time.



Remediation

Hadrian's smart workflows and role-based access ensure that the correct teams respond quickly. The platform is built API-first and integrates into any ecosystem with our expansive range of integrations into the most common security and IT tools.


Hadrian's Orchestrator AI




The hacker perspective

Thinking like a hacker reveals how real-world attacks could compromise applications and infrastructure. To uncover the threats our autonomous platform tests continuously to comprehensively assess internet-facing assets. The cutting-edge technology is cloud-based, completely agentless and constantly updated and improved by Hadrian's ethical hacker team.


Key use cases




Automated penetration testing
Comprehensively test every asset for exploitable vulnerabilities.




Third-party risk management
Centralize visibility of the supply chain and subsidiaries, and attribute assets.




Continuous attack surface management
Monitor your digital assets in real time for changes and new risks.




Cloud exposure visibility and control
Continuous visibility of assets and risks across multi-cloud environments.




Risk-based vulnerability management
Focus your remediation efforts on the risks that matter most.



Compliance assurance and reporting
Proactively identify and fix compliance risks and improve reporting.



Threat exposure reduction
Improve security posture with continuous remediation processes.



DNS monitoring and exposure
Detect vulnerable and misconfigured DNS infrastructure.

Trusted by market leaders