HADRIAN

EXPOSURE MANAGEMENT FOR THE FINANCIAL SERVICES SECTOR

Financial services organizations are among the most targeted sectors globally, operating complex multi-partner ecosystems under the most demanding regulatory frameworks in any industry. Open banking APIs, payment integrations, wealth management portals, and correspondent banking relationships create external attack surfaces that change daily. Legacy systems coexist with rapid cloud adoption, and regulations including DORA, PCI DSS, SOX, and GDPR make preemptive cybersecurity action essential.

KEY CHALLENGES

- **Third-party and partner exposure**

  Open banking APIs, payment processors, and fintech partnerships multiply exposed assets. Each connection introduces DNS records, subdomains, and cloud instances security teams may not know exist.

- **Regulatory complexity**

  DORA, PCI DSS 4.0, SOX, GDPR, and NIS2 require evidence of continuous security validation, not periodic assessments. Meeting these overlapping mandates demands real-time posture visibility.

- **Alert overload and the verification gap**

  Hadrian's 2026 Benchmark Report found 95% of security leaders dissatisfied with their ability to prioritize remediation based on real-world risk. 60% cite too many unverified findings as their top frustration.

- **Credential theft and infostealer exposure**

  Financial institutions are primary targets for infostealer malware. Leaked credentials from employees and partners create authenticated access paths into core systems and customer applications.

- **Shadow AI and undocumented endpoints**

  Hadrian's Benchmark Report found 97% of organizations run AI-generated code in production while 81% lack visibility into AI tool usage. These undocumented endpoints are unmonitored entry points into regulated environments.

SOLUTION REQUIREMENTS

- **Complete asset inventory**

  Detection of all exposed assets, including subsidiaries and acquired entities.

- **Real-time discovery**

  Tracking attack surface changes as soon as they occur.

- **Event-Driven Testing**

  Testing that is triggered automatically by infrastructure changes, not just by a calendar schedule.

- **Evidence-Based Validation**

  Autonomous exploitation that proves risk reality and eliminates alert fatigue.

- **Context enrichment**

  Prioritizing risks with information on the asset, its function, and its connection to other assets.

- **Native threat intelligence**

  Prioritization informed by the likelihood of exploitation by real-world threat actors.

- **Reporting capabilities**

  Quick assessment and reporting on the organization's security posture and specific risks.

- **Detailed asset inventory**

  Visibility into shadow IT, third-party infrastructure, and assets inherited through M&A

HADRIAN FOR FINANCIAL SERVICES

Hadrian's agentic AI platform is the engine of your Continuous Threat Exposure Management (CTEM) program. Our unified approach maps your external attack surface, autonomously validates exposures, and prioritizes remediation based on real-world risk.

"Hadrian's centralized asset inventory is a game changer for us, it saves my team dozens of hours every week conducting manual asset discover and immediately alerts us to any shadow IT that might occur"

Group Cybersecurity Team, Crédit Agricole Personal Finance & Mobility

Continuous Attack Surface Discovery

Get complete, real-time visibility. Hadrian continuously maps your external perimeter, detecting new cloud instances, shadow IT, and configuration changes the moment they appear. Our event-based architecture ensures there are no visibility gaps between scans.

Adversarial Exposure Validation

Hadrian's agentic AI autonomously emulates the TTPs of sophisticated threat actors. Unlike standard scanners, it validates exploitability by safely executing complex attack chains, ensuring your team focuses only on verified risks.

Validated Remediation

Fix what matters. By confirming exploitability, Hadrian allows security teams to prioritize the <1% of vulnerabilities that actually threaten the business. We provide clear, evidence-based remediation steps to drastically reduce Mean Time to Remediate (MTTR).

Hadrian autonomously and continuously identifies exposures across external attack surfaces, producing easy-to-understand results that include reproduction and remediation instructions. The platform seamlessly complements existing workflows with integrations into more than 100 SIEM, SOAR, and ITSM systems.

Hadrian is the only vendor recognized as both a Leader and an Outperformer in the GigaOm Radar 2024 report on Attack Surface Management.

ABOUT HADRIAN

Hadrian is an agentic AI offensive security platform that helps modern security teams prevent breaches by continuously assessing the external attack surface, validating real-world threats, and prioritizing exploitable exposures. Agentic AI powers 10x visibility into your critical risks, cuts through false positives, and provides step-by-step remediation guidance. Organizations reduce time to resolution by 80%, reclaim 10+ hours weekly, and act before attackers can. With Hadrian, you don't just keep up, you leave your adversaries in the dust.

REQUEST A DEMO