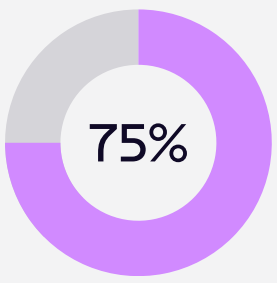
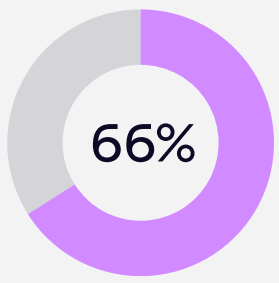
HADRIAN

The ROI Guide to Offensive Security

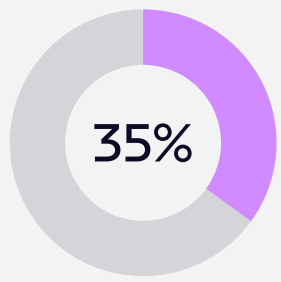
Offensive security complements and validates existing cybersecurity investments by identifying gaps in existing controls. Analysis shows that security leaders are increasingly investing in offensive security to proactively identify and remediate risks.



75.2% of organizations to increase their offensive security practices because of unknown risk[1]



Remote access and internet facing applications account for **39%** and **27%** of initial access vectors in the first half of 2023[2]



Following a breach **35%** of organizations invest in offensive security, the 4th most common investment[3]

Traditional offensive security methods, such as manual penetration testing, vulnerability scanning and attack surface management, can allow risks to go undetected and unresolved. Figure 1 indicates the top concerns that surveyed security professional had when considering their external threat exposure.

Figure 1 - Top threat exposure concerns[1]

Main challenges that traditional offensive security methods face:

Leaves blindspots

Legacy tools, such as ASM or vulnerability scanners, only test for a fraction of the potential risks. In-depth human testing can not scale to cover the breadth of modern attack surfaces.

Unactionable results

Remediation efficiency is decreased by tools and reports that contain unvalidated risks and false-positives. Contextless prioritization results in poor focus and slow resolution.

Resource intensive

Manual processes are required to coordinate testing or configure tools. Additional research is required to understand the risks and identify the optimal remediation steps.

Case Studies

Leaves blindspots

A Netherlands-based manufacturing company suffered a significant data breach due to unnoticed security vulnerabilities. The attackers used compromised credentials to access an RDP server, exploiting security misconfigurations and inadequate authentication measures.

This breach impacted over 100 devices, causing major operational disruptions and financial losses. The attack halted production, and the deletion of backup data extended the downtime, taking over two months to recover.

Unactionable results

A Belelux-based retailer, which experienced a severe data exfiltration incident due to weak authentication and exposed assets. Attackers exploited an open RDP channel to infiltrate the network, targeting domain controllers and stealing sensitive data, which was then sold on the dark web.

This incident resulted in substantial reputational damage and loss of customer trust due to the exposure of sensitive information.

Resource intensive

A German banking and financial service, which conducted annual third-party penetration tests, which were costly and infrequent, resulting in gaps in visibility and protection.

These tests required significant manual effort for coordination, execution, and follow-up, diverting resources from other crucial security tasks

Assumptions

One the next page we provide a sample calculation for calculating the value of an automated offensive security solution. The assumptions utilized in the calculation are listed below and explained in greater detail at the back of the report.

Alert overload Percentage of false positives: 30% Hourly rate of analyst: $60 Savings with Hadrian: 50%	**Manual asset inventory** Time spent per asset: 10min Hourly rate of analyst: $80 Savings with Hadrian: 60%
Third-party testing Daily rate for testing: $1000 - $3000 per day Savings with Hadrian: 20%	**Cyber insurance costs** Premium: $1.5k per $1million in liabilities Savings with Hadrian: 1%
Legacy licences Vulnerability scanner licences: $20,000 Savings with Hadrian: 20%	**Lost revenue** Likelihood of an exploit per asset: 0.002% Unique vulnerabilities found by Hadrian: 50%

Sample Calculations

The sample calculations below can be used to estimate the value of Hadrian's offensive solution. To utilize the calculations, simply fill in the missing fields and follow the provided instructions. The assumptions are based on composite estimates by Forrester Consulting.

Alert overload			
A1	Time spent triaging alerts	Hours	
B1	Percentage of false positives	30%	
C1	Hourly rate of analyst	$60	
D1	Savings with Hadrian	50%	
T1	Total (A1 x B1 x C1 x D1)		

Third-party testing		
A2	Days of testing conducted	Days
B2	Daily rate for testing (blended)	$2,000
C2	Savings with Hadrian	20%
T2	Total (A2 x B2 x C2)	

Legacy licences		
A3	Number of vulnerability scanners utilized	
B3	Average licence cost	$20,000
C3	Savings with Hadrian	20%
T3	Total (A3 x B3 x C3)	

Manual asset inventory		
A4	Number of assets	
B4	Time spent inventorying assets	0.16 hour
C4	Hourly rate of analyst	$80
D4	Savings with Hadrian	60%
T4	Total (A4 x B4 x C4 x D4)	

Cyber insurance costs		
A5	Business liability ($million)	Days
B5	Premium	$1,500
C5	Savings with Hadrian	1%
T5	Total (A5 x B5 x C5)	

Lost revenue		
A6	Number of assets	
B6	Likelihood of an exploit per asset	0.002%
C6	Unique vulnerabilities found by Hadrian	50%
D6	Cost of a breach per asset	
T6	Total (A6 x B6 x C6 x D6)	

Total value of Hadrian = T1 + T2 + T3 + T4 + T5 + T6

HADRIAN

Quantifiable Benefits

Challenge	Solution
Alert overload Cybersecurity teams face a barrage of alerts, diverting resources and attention from strategic security tasks. Investigating security alerts is resource-intensive, with 30% of all alerts estimated to be false positives that need manually remove. Third-party tools, such as security rating services and attack surface management, have exacerbated this situation by misclassifying the severity of vulnerabilities. This strained resources and hindered the focus on crucial security endeavors.	**Intelligence-driven prioritization** Hadrian's proprietary risk-scoring algorithms cut through the noise and allow security teams to focus on the most important risks. The Security Operations Centre (SOC) can focus on important incidents, vulnerability management processes can better prioritize patching, and DevSecOps teams can concentrate on critical issues. Prioritization is performed by Hadrian's Orchestrator AI which considers a range of factors including the likelihood of exploitation, and potential business impact. The proprietary scoring algorithms learn from user feedback to become more accurate.
Expensive third-party tests Third-party penetration tests are expensive and often conducted on an annual basis. The periodic nature of the testing means that organizations lack visibility between assessments. Additionally, these tests have limited scope, meaning only a subset of exposed assets are assessed. The typical daily rate for manual penetration testing can range from $1000 to $3000 per day.	**Automated penetration testing** Hadrian's automated penetration testing emulates the behavior of real-world attackers at the faction of a cost. Human readable reporting enables remediation to be actioned immediately and automatic follow-up scans verify whether resolution was successful. Hadrian's platform conducts threat assessments continuously, there is no need to wait for the next manual test. The automated penetration testing examines security flaws 24 hours a day, all year round.
Legacy security licences Ineffective or isolated security tools result in limited insights. Additionally, point solutions such as vulnerability scanners or security rating services often serve very limited use cases. Many organizations face challenges in understanding the effectiveness of their existing security tools and identifying areas for refinement.	**Next-generation AI solution** Hadrian's comprehensive offensive security capabilities enable existing tools to be fully or partially replaced, saving tens of thousands per year. Hadrian can also identify infrastructure and edge devices that can be decommissioned, further reducing costs. The platform's built-in reporting enables the organization to quantifiably measure security posture improvements that are made over time.

Challenge	Solution
Manual asset inventory Organizations depend on time-consuming manual processes, involving spreadsheets and manual scripts, to inventory their digital assets. Teams spend time maintaining the scripts and deduplicating the results they produce. It is estimated that 10 minutes of engineer time per asset is needed to manually inventory assets. This workload and limited data accuracy hinder monitoring of the attack surface due to the lack of automation and infrequent updates.	**Continuous automated discovery** Hadrian's platform finds and catalogs assets around the clock to build an accurate and always up-to-date inventory. The results can be easily reviewed in several table-based and graphic formats, or exported for external analysis. The asset-finding algorithms used by Hadrian employ best practices and propriety techniques. The in-house development team continuously updates the technology to identify new asset classes and improve automation.
High cyber insurance costs When negotiating premium adjustments with an organization, cybersecurity insurance providers consider numerous factors. However, organizations lack insight into the security posture of their peers or themselves. Without access to credible evidence about the strength of the organization's security posture or industry benchmarks cyberinsurance premiums is estimated to be $1,500 per year per $1 million in damages.	**Automated penetration testing** Hadrian enables organizations to realize savings due to preferred terms and conditions for their cyber insurance. By providing measurable evidence of reduced risk of a breach organizations are equipped to negotiate with insurance providers. The platform also enables organizations to benchmark their security against their peers, enabling them to understand their relative security posture and responsiveness to threats.
Lost revenue and damages A breach or service disruption can have a material impact on an organization's bottom line. The subsequent costs downstream encompass remediation, downtime, lost productivity, legal fines, and brand damage. Regulatory fines, such as GDPR penalties, can be severe, potentially imposing significant financial burdens on organizations. Additionally, organizations may also face increased scrutiny from regulators.	**Increased resilience** Hadrian enables organizations to reduce risk exposure with clear, actionable steps. This not only reduces the likelihood of a breach it also reduces the potential impact that one could have. According to IBM's Cost of a Data Breach report, 35% of organizations invest in offensive security testing following a breach. By investing early, organizations can get ahead and reduce the likelihood significantly.

Unquantifiable Benefits

Challenge	Solution
Slow security processes Essential components of exposure management including the process of planning and conducting tests, validating results, and researching remediation. Security teams follow this process to comprehend attack paths and offer guidance to remediation teams. However, when conducted manually these processes are extremely time-consuming. This means that security resources are spread thin and can not effectively investigate issues fully.	**Continuous risk mitigation** Hadrian completely automates discovery, validation, prioritization and remediation processes. The platform continuously verifies security posture and enables security teams to proactively address exploitable vulnerabilities. Orchestrator AI simplifies remediation by providing pertinent business units with clear, step-by-step resolution instructions. Additionally, the platform automatically performs regression testing to confirm the effectiveness of remediation.
M&A and partner assessments During Mergers and Acquisitions (M&A), understanding and managing the attack surface of newly integrated entities if often a struggle, resulting in unknown assets and risks associated with the IT departments of acquired subsidiaries that were not fully integrated with the parent organization's IT department. Without insight into security posture, organizations are unable to take steps to mitigate their risk exposure. Some organizations engage 3rd parties to assist, which can cost $250,000 per acquisition.	**Automated risk insights** Hadrian eliminates the need for special projects to obtain an inventory of all subsidiaries and business partners attack surface and exposed risks. Hadrian's platform efficiently identifies unknown assets, offering organizations complete visibility and reducing the workload for internal teams. Real-time risk assessments provide insights across the entire footprint of the acquired company. Orchestrator AI utilizes its neural network graph of the internet to discover all external-facing assets, and comprehensively tests them to discover risks.
Compliance expenses Conducting penetration tests is a common component of compliance standards including ISO 27001, SOC2, NIS2, DORA, HIPAA and PCI-DSS. For organizations that must comply with the regulation, conducting these assessments can be an expensive additional cost. Furthermore, organizations can spend weeks compiling reports to demonstrate to demonstrate compliance. When conducted on a quarterly basis this can become a full time function.	**On-demand reporting** Hadrian helps organizations meet penetration testing, vulnerability and risk management requirements. The platform continuously performs assessments reducing the supplementary testing that needs to be coordinated. Hadrian’s dashboard allows security teams to monitor and demonstrate the effectiveness of their processes. Reports can be generated on demand and easily shared with internal and external stakeholders.

Challenge	Solution
Siloed security teams Slow security testing practices are not fit for purpose in today's fast paced development cycles. Penetration tests can take a month to plan, 2 months to perform and then several weeks for the report to be compiled. This is incompatible with development teams that work in 2 week sprint. Existing tools to perform security assessments are complex. Not only are they difficult to configure and use, the results often contain false positives and are difficult for non-security personnel to understand and act upon.	**Collaborative & streamlined workflows** Hadrian streamlines the attack surface management process, enabling security operations to maintain a secure cyber environment. The platform's automated penetration testing capabilities identify exploitable risks in real-time, providing development teams with near-instant feedback. Orchestrator AI is built to simplify offensive security workflows by autonomously validating results to remove false-positives. Hadrian also provides step-by-step instructions to enable remediating teams to immediately take action.
Third-party and forgotten applications Discovering vulnerabilities in third-party software becomes challenging for organizations without an updated and accurate inventory list. The absence of visibility into external attack surfaces and security gaps. The lack of visibility poses a significant issue. For instance, a preproduction environment may have been created to test the functionality for a new feature but was not decommissioned. Such overlooked applications often fail to meet security standards.	**Supply chain visibility** Hadrian's probes are capable of identifying over 10,000 SaaS applications and thousands of software packages and versions, ensuring comprehensive application identification. Continuously scanning the internet, Hadrian's platform examines technology, versions, and configurations to identify potential security threats. This process allows Hadrian to unveil your organization's posture and assess the impact of a compromise in third-party software.
Brand abuse and phishing The extensive number of subdomains and the dynamic nature of DNS infrastructure pose challenges in monitoring. Subdomains can easily go unnoticed, making them susceptible to takeover attempts and infrastructure compromise. Unclaimed or poorly managed subdomains can serve as an entry point for threat actors, leading to potential brand damage, loss of customer trust, and data breaches. For instance, attackers may exploit a subdomain to steal authentication cookies.	**Build a trusted brand** Hadrian prevents brand damage by monitoring subdomain vulnerabilities susceptible to takeovers. The platform continuously scans DNS infrastructure to identify emerging risks. The platform instantly alerts security teams, enabling proactive remediation and preventing subdomains from being taken over for use in a phishing campaign. Swift remediation eliminates the risk of customers, employees, and partners encountering malicious phishing sites.

About Hadrian

Defensive security should be validated by offensive security. Hadrian provides the hacker perspective, revealing the targets and methods that could be used in a real-world data breach. Hadrian's continuous and comprehensive testing discovers and validates risks completely autonomously.

Our solution

Hadrian's platform combines attack surface discovery, automated penetration testing, and threat exposure management technologies in a cloud-based and agentless platform. The platform is powered by Orchestrator AI, which emulates the techniques and behaviors of a real-world threat actor, to provide continuous 24x7 detection of internet-facing threats and autonomously remove false positives.

Orchestrator AI uses its knowledge of your environment to test for exploitable OWASP Top Ten risks, known and zero-day vulnerabilities, and exposed and misconfigured services. Scans are chained together to simulate complex multidimensional attacks. The cutting-edge technology is constantly updated and improved by Hadrian's in-house hacker team.

+200	+1.2m	40%
businesses protected	assets secured	faster MTTR

Trusted by

ABN·AMRO · SHV ENERGY · macmillan education · WeatherTech · LEROY MERLIN · LOTTOMatica · RITUALS... · BIOLANDES · nedap

> ‘What’s exciting about what Hadrian is doing is they solved a seemingly impossible puzzle: finding weaknesses in a complex network with human-like detail, at scale, from the outside and continuously. What usually takes a dedicated team of security engineers a few weeks to figure out for one system, they can do in minutes for thousands of systems.”
>
> **Tiago Teles, Security Lead - ABN AMRO**

1 - SANS (2023) ‘Building a Resilient Offensive Security Strategy’
2 - RAPID9 (2023) ‘2023 Mid-Year Threat Review’
3 - IBM Security (2023) ‘Cost of a Data Breach Report 2023’

Book a demo at hadrian.io/demo

HADRIAN

Contact us at info@hadrian.io