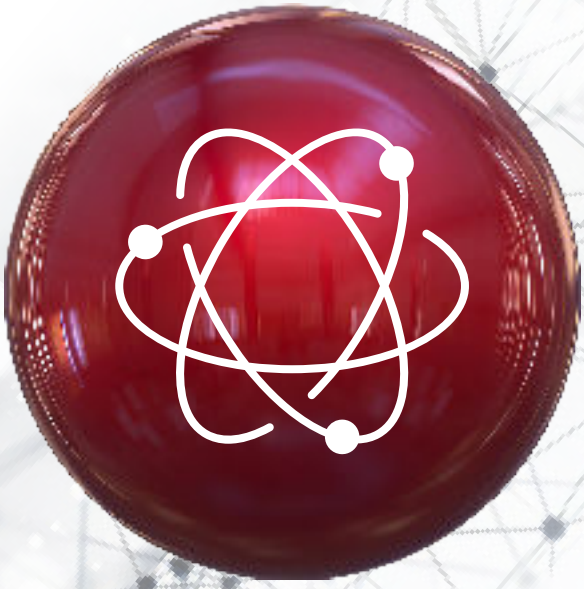
edgescan

AUTONOMOUS PENETRATION TESTING

Edgescan ATOMIC

Start with context.
Rapidly test autonomously.
Stay in control.



Atomic is not an autonomous hacker dropped onto an unfamiliar target.

It is an autonomous offensive capability operating on top of an existing continuous security program.

Applications evolve. Infrastructure changes. APIs expand. AI threats evolve. Cloud environments grow. Every change has the potential to introduce new security risks.

Traditional penetration testing provides invaluable assurance, delivering the depth and expertise organizations rely on. However, it happens on a schedule. Edgescan Atomic gives you the power to launch autonomous penetration testing whenever you need it, putting more control, greater flexibility, and faster security validation directly in your hands.

Edgescan Atomic's Agentic AI operates within the Edgescan platform, reasoning through the objectives you define, while leveraging the rich context already gathered about the asset being tested. The result is faster, deeper and more efficient security assessments.

Data-first, what does your AI know before it starts?
Context is king, rather than starting from a blank canvas, Edgescan Atomic leverages the battle-hardened Edgescan platform, which is used by hundreds of enterprises globally. This includes code, application state, APIs, authentication workflows, previous asset context findings and 20M+ triaged vulnerabilities, giving Atomic the context it needs to reason, test and deliver smarter, more informed and efficient autonomous testing.

Autonomy with enforced control: Autonomous, but never uncontrolled. The Edgescan Harness uses deterministic security engines to enforce operational boundaries. Every action initiated by Atomic passes through the harness where scope, permissions, approvals, and policies are verified before execution. Architecturally separate from the Atomic AI model, Atomic gives AI the freedom to think like an attacker, while the Edgescan Harness determines what it is allowed to do.

The advantage isn't just autonomous testing. It's what Atomic knows before it starts.

EDGESCAN **ATOMIC**

With Edgescan Intelligence Atomic Starts Ahead

Atomic can start from zero, but it becomes significantly more effective when powered by Edgescan Intelligence. Edgescan Atomic begins with validated security intelligence, then independently explores the target to discover new vulnerabilities, attack paths and chained exposures.

Atomic starts informed, not blind, meaning;

- Faster time to meaningful findings
- More focused testing
- Less wasted AI/token activity
- Better prioritization of attack paths
- Stronger continuity between continuous scanning and autonomous pentesting
- Better governance because the target and known state are already defined

AI with purpose

Key Features

Atomic is designed to increase testing frequency, depth, validation, accelerate change, and give your team the confidence to act. Atomic is built on a data-first foundation, drawing on 20M+ triaged vulnerabilities and years of real-world testing by CREST and OSCP-certified experts. Atomic combines proven security intelligence with Agentic AI and the Edgescan Harness to orchestrate controlled autonomous testing. *The Harness turns autonomous offensive testing into a controlled, auditable and policy-enforced security process.*

Agentic AI Attack Exploration: Unlike signature-based scanners, Agentic AI plans, adapts and pursues attack hypotheses as evidence emerges, enabling Atomic to investigate paths beyond predetermined scanner logic

Data-First Testing: Starts with 20M+ triaged vulnerabilities, scan history, asset context and validated findings.

Autonomous Offensive Testing: Launch directly from Edgescan using ready-made or customized prompts to focus testing where you need it.

Real-World Attack Coverage: Atomic autonomously hunts the access-control and business logic flaws scanners miss including BOLA, IDOR, broken access control, and everyday business logic.

AI Validation & Evidence: Proves discovered vulnerabilities through validation and supporting evidence, and clearly identifies AI-generated findings.

Controlled Execution: The Edgescan Harness provides deterministic controls for scope, permissions, approvals, policies and execution.

Expert Oversight & Escalation: Atomic runs autonomously within the Edgescan Platform, with complex findings available for an expert-led test when deeper human assessment is required.

Bounded Testing & Cost: A defined assessment budget and hard ceiling provide predictable cost per test.

Platform-Native Results: Comprehensive findings, evidence and insights are delivered directly into the Edgescan Platform.

Benefits

Atomic's advantage isn't AI alone. It's AI with a head start. Autonomous penetration testing with context, control and validation built in.

Have More Control

Rapidly launch autonomous testing on demand with strong guardrails.

Move Faster

Immediately launch testing directly from the platform using existing context for fast, efficient and accurate coverage

Explore Differently

Atomic uses goal-driven autonomous attack exploration to reason through and investigate attack paths beyond traditional automation, adapting as new opportunities are discovered.

Reduce Triage Load

Validated findings and supporting evidence reduce analyst investigation and unnecessary noise.

Predictable Cost

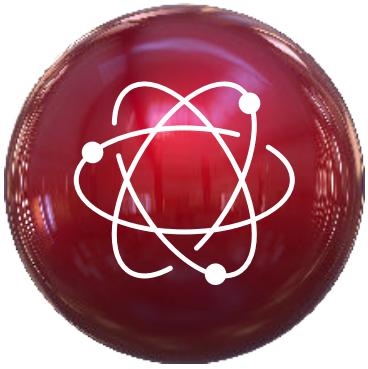
One attack credit provides one autonomous assessment, with a defined per-test cost and hard ceiling.

Extend, Don't Replace

Consolidate on a platform you already run, more offensive coverage with no net-new console, data model or integration debt to stand up.

How *ATOMIC* works

Atomic combines AI with the intelligence already collected by the Edgescan platform, allowing organizations to perform autonomous penetration testing with greater speed, context, focus and confidence.



Continuous attack surface intelligence

The Edgescan Platform continuously builds intelligence around your attack surface. Continuous does not mean continuously burning through AI cycles, it means continuously understanding your environment and applying autonomous testing when you decide that changes, exposures or risk justify deeper investigation.

Context matters, start with existing intelligence

Atomic starts with what Edgescan already knows. It can use existing knowledge of the application and attack surface rather than starting from scratch. Edgescan context can include code, application state, APIs, authentication flows, known applications, endpoints, technologies and patterns, previous findings and 20M+ triaged vulnerabilities within the Edgescan vulnerability intelligence.

Reduce repeated work

Existing context reduces the reconnaissance and repeated work agents need to carry out. Instead of rediscovering what Edgescan already knows, Atomic can focus its reasoning on what has changed, what remains unknown and where deeper testing is worthwhile. The same context can be reused for regression testing, allowing Atomic to focus on meaningful changes and new attack paths.

More time for actual testing

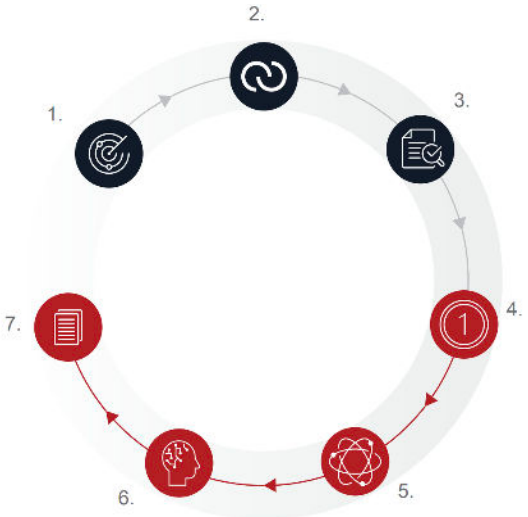
Less time spent rediscovering known functionality and rebuilding context means more testing effort spent investigating meaningful attacks. Time, compute and tokens can be focused on actual testing, with Atomic exploring and adapting within the defined operational boundaries of the Edgescan Harness

Continuous Intelligence, Selective Autonomy.

Each Atomic attack credit provides an autonomous penetration test, allowing organizations to perform additional security validation whenever required.

Start with intelligence, not a blank canvas

Machine discovery → AI reasoning → exploit validation → human escalation



1. Automated Exposure Management

Automation and offensive technology continuously scans, maps, and tests the web applications, APIs and infrastructure to discover vulnerabilities using Edgescan technology.

2. Site Maps and Vulnerabilities Saved within the Edgescan Platform

Sitemaps, discovered vulnerabilities, authentication workflows, and API manifest files are saved to the platform, alongside Edgescan's wider vulnerability intelligence, including 20M+ triaged vulnerabilities.

3. Vulnerabilities Validated

Vulnerabilities are validated by Edgescan's expert validation engine and team of certified security experts.

- Exploitation Verified
- False Positive Eliminated
- Risk Confirmed
- Evidence Captured

4. User Applies an Attack Credit

A user invokes an AI-powered autonomous assessment by applying an Attack Credit.

5. Edgescan Atomic Consumes Edgescan Intelligence

The AI harness - running the same toolset human testers use - consumes platform history to target where automation is blind: auth layers and business logic.

6. Autonomous Execution

Atomic uses the intelligence to reason and build an adaptive attack strategy and orchestrate AI-powered penetration testing within defined guardrails, exploring additional exposures and weaknesses beyond automated scans.

7. Results Reported to the User

Comprehensive results and insights are delivered to the user in Edgescan.

EDGESCAN **ATOMIC**

The Edgescan Harness

AI drives the testing,
the Harness controls execution.

The Edgescan Harness uses deterministic security engines to enforce operational boundaries

- Scope, permissions and policies enforced
- Approved tools, techniques and actions only
- Approval gates for controlled actions
- Bounded resource usage and rate limits
- Credential-controlled and access restricted
- Non-destructive testing by design
- Third-party endpoints handled within defined boundaries
- Every action logged, auditable and blocked if it violates policy

Frequently asked questions

Does Atomic replace penetration testing?

Atomic extends expert-led testing by providing autonomous offensive validation between scheduled assessments. Complex business logic, creative abuse cases and high-judgement scenarios can still be escalated to Edgescan experts.

Why not simply book another penetration test?

Because not every release, API change or infrastructure change warrants a new multi-day human engagement. Atomic provides rapid offensive validation when additional assurance is needed, while preserving expert-led testing for scenarios where human judgement creates the greatest value.

When should I use Atomic?

Whenever additional confidence or rapid response is required

- Rapid deep testing is required
- After major releases
- Following infrastructure changes
- During or after cloud migration
- When introducing new APIs
- Before production deployment

Are the findings just AI output?

No. Atomic validates discovered vulnerabilities, providing supporting evidence alongside findings to improve confidence and reduce unnecessary investigation.

How is Atomic different from scanners?

Scanners detect known patterns and vulnerabilities. Atomic performs autonomous offensive security testing, using Agentic AI to reason, adapt and explore attack paths, then validate what it finds in ways scanners can't.

How is licensing managed?

Each Atomic attack credit provides one autonomous penetration test. Apply the credit within the Edgescan platform whenever you want to launch a new assessment.

What about larger or complex environments?

Atomic is designed to deliver and complete assessments within defined platform limits. If limits are reached, Atomic wraps up gracefully and returns all validated findings and evidence captured during the assessment.

Security moves fast.
Your testing should, too.

Edgescan provides expert-led, continuous security validation. Atomic extends the capability by giving organizations the freedom to launch autonomous penetration testing whenever their environment changes.

Together they provide more control, greater flexibility and faster security validation, combining the speed of AI with the expertise of Edgescan.

Ready to see Atomic in action?

Talk to your Edgescan representative today and see how Atomic can accelerate your security outcomes.

sales@edgescan.com

edgescan

IRELAND | Unit 701 Northwest Business Park, Ballycoolin, Dublin 15, D15 CH26
UNITED STATES | 445 Park Avenue, 9th Floor, New York, NY 10022