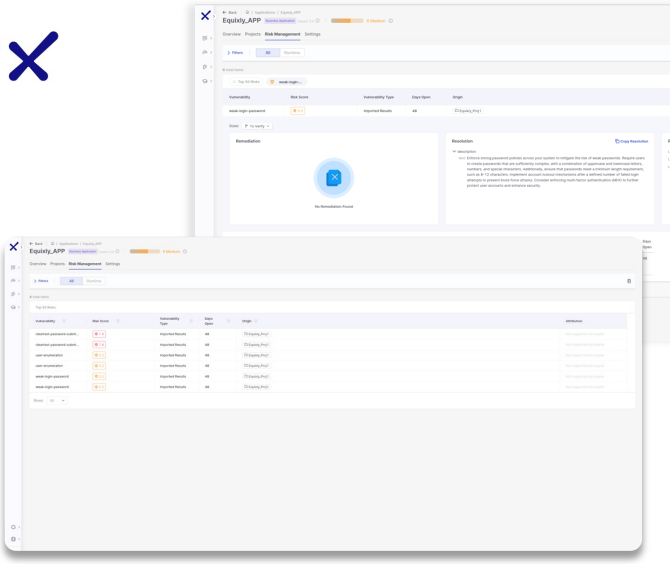
equixly | Checkmarx



Equixly + Checkmarx

Extend Checkmarx One with continuous, agentic offensive testing to uncover business logic and authorization risks traditional tools cannot see.

Attack Web Applications with an Agentic AI Hacker

Traditional DAST tools remain effective for identifying runtime vulnerabilities in web applications, but they were not designed to address the unique risks of modern APIs. APIs expose core business logic, data relationships, and authorization models that DAST cannot fully understand, leaving critical gaps around access control, logic abuse, and unmanaged or unknown endpoints.

By combining Checkmarx with Equixly, customers gain comprehensive application protection. This integrated approach provides full visibility across web and API surfaces, continuously identifies business-logic and authorization risks, and aligns security coverage with how modern applications are built, deployed, and attacked, significantly reducing real-world breach risk.

From Detection to Proof

Checkmarx finds vulnerabilities. Equixly proves which ones attackers can exploit.

Business Logic Under Pressure

Not just code flaws but real-world abuse of workflows, authorization, and API interactions.

Continuous, Not Periodic

Security validation that keeps pace with app releases, not annual snapshots.

Exploit-Driven Prioritisation

Focus remediation on risks validated in runtime conditions, not theoretical severity.

One Workflow, Stronger Outcomes

Exploit-validated findings delivered inside Checkmarx without new silos, or tool sprawl.

API-Native Offensive Testing

Built for modern API architectures, that truly understands how to test them.

Combined Impact

Stronger Application Risk Prioritization

- Security teams move from vulnerability volume to exploit-proven risk, improving focus within the Checkmarx workflow.

Reduced Application Breach Exposure

- Continuous offensive validation helps identify high-impact API and business logic vulnerabilities before they are exploited.

Improved ROI on Checkmarx Investment

- The integration maximizes the value of existing AppSec tooling by validating findings in real-world runtime conditions.

Shorter Time to Remediation

- Exploit context reduces debate and accelerates engineering response, shrinking exposure windows across applications.

Continuous Assurance Between Releases

- As applications evolve, validation keeps pace, eliminating the structural gap between development velocity and security testing.

Greater Confidence at Leadership Level

- Security leaders gain demonstrable evidence that applications are not just scanned but actively tested against modern attack techniques.

Align Your Application Security with Modern Attack Reality

Book a demo to see how Equixly extends Checkmarx with continuous, exploit-driven API penetration testing.

BOOK A DEMO

Checkmarx

About Checkmarx

Checkmarx is the leader in agentic application security, delivering enterprise-grade protection while lowering engineering costs and accelerating development velocity. The Checkmarx One platform scans trillions of lines of code each year for companies, cutting vulnerability density by more than half. Its autonomous security agents detect and counter AI-driven threats across the SDLC, providing prevention-first protection for legacy, modern, and AI-generated code at enterprise scale.

equixly

About Equixly

Equixly is a deep-tech cybersecurity company that automates API security testing through agentic AI. Its autonomous testing platform identifies complex business-logic vulnerabilities, enabling enterprises to scale security with software development. Equixly is backed by 33N Ventures, 360 Capital, Alpha Intelligence Capital, and JME Ventures, and recognized by Gartner, UniCredit and BCG for its pioneering work in agentic AI security testing.