BORNSEC
BORN TO SECURE

Attacklens
ATTACK SURFACE MANAGEMENT PLATFORM

ATTACKLENS CAPTAS AI

Continuous Adaptive Penetration Testing Powered by Autonomous AI Agents

What You Get with Attacklens CAPTAS AI?

40–60%
Faster vulnerability discovery

30–50%
Reduction in false positives

2-3X
Increase in attack path visibility

30–60%
Reduction in remediation time

Info@attacklens.ai | +918040273737

Attacklens CAPTAS AI provides on-demand penetration testing powered by LLM-driven autonomous agents.

- It intelligently simulates real-world attack scenarios across web, API, mobile, infrastructure, and thick client environments.
- The system dynamically adapts to new assets and exposures, enabling faster discovery of unknown vulnerabilities.
- Designed for safe and controlled execution, it delivers continuous, high-impact security insights.

What is Attacklens CAPTAS?

Continuous Adaptive Penetration Testing (CAPT) is a service that:

- Continuously scans and tests your attack surface
- Adapts testing based on new threats, changes in infrastructure, and discovered vulnerabilities
- Uses AI to prioritize, simulate, and evolve attack scenarios

Key Components

1 AI-Driven Risk Prioritization

- Uses ML models to:
  - Rank vulnerabilities by exploitability (not just CVSS)
  - Correlate threats with real-world attack patterns
  - Reduce false positives

2 Adaptive Attack Simulation

- Mimics real attackers using:
  - Automated exploitation
  - Attack chaining (multi-step attacks)
  - MITRE ATT&CK mapping

3 Continuous Validation

- Re-tests vulnerabilities after fixes
- Validates whether patches actually worked

4 Context-Aware Testing

- Adapts based on:
  - Industry (BFSI, healthcare, edtech, etc.)
  - Tech stack (cloud, APIs, SaaS apps)
  - Threat intelligence feeds

Info@attacklens.ai | +918040273737

Traditional Pentesting	Advanced PenTest CAPTAS
Once or twice a year	Continuous (24/7)
Manual-heavy	AI + automation
Static scope	Dynamic scope
Point-in-time report	Real-time dashboard
Limited attack paths	Adaptive multi-stage attacks

Value Addition

- Early breach detection
- Reduced attack surface
- Continuous compliance (DPDP, ISO 27001, SOC 2)
- Lower cost vs repeated pentests
- Better visibility for CISOs

Key Features

- Autonomous pentesting agents
- Real-time attack surface visualization
- Exploit validation (not just detection)
- Attack path mapping
- API & cloud security testing
- Continuous compliance reporting
- Developer-friendly remediation guidance

BORNSEC
BORN TO SECURE

Attacklens
ATTACK SURFACE MANAGEMENT PLATFORM

Info@attacklens.ai | +918040273737