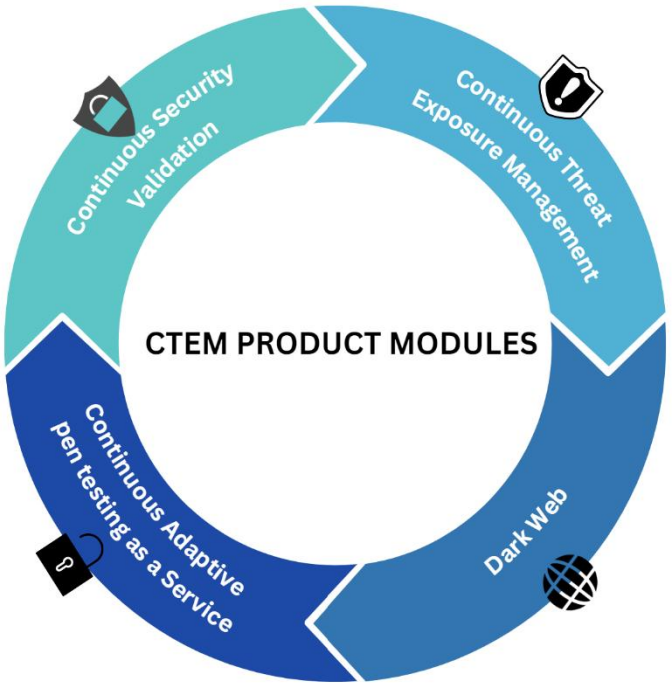
ATTACKLENS – An AI Based Continuous Threat Exposure Management (CTEM) Solution

Evidence-driven security for a faster, safer world.

EXTERNAL CTEM PRODUCT FEATURES



AI-Powered Seedless Discovery Engine

AttackLens.ai transforms how organizations discover their entire digital footprint. Instead of requiring manual scope definition or agent deployment, our platform uses advanced reconnaissance techniques to automatically map every internet-facing asset known and unknown.

The "Attacker's Perspective" Engine

Most tools scan for vulnerabilities; AttackLens.ai scans for **exploitability**. It simulates the reconnaissance phase of a real cyberattack to see which "doors" are not only unlocked but are also being actively scouted by threat actors.

Black-Box Reconnaissance of Exposed & Forgotten

In today's decentralized enterprise, development teams, business units, and acquired companies spin up cloud resources S3 buckets, Azure Blobs, Kubernetes clusters, RDS databases, Lambda functions, APIs often without central IT awareness or governance. From an external attacker's perspective, these resources are discoverable through public reconnaissance and frequently exploitable. AttackLens.ai performs the exact same external black-box discovery techniques that threat actors use to map your internet-facing infrastructure

Web & Application Layer Exposure Detection

Subdomain Enumeration, Web Application Fingerprinting & Vulnerability Surface Beyond infrastructure, every web application, web service, and API exposed to the internet represents attack surface. Most organizations lose track of web properties, subdomains, and applications.

Vendor Risk & External Dependency Mapping Cloud Infrastructure

Organizations don't exist in isolation. They depend on vendors, partners, integrations, and supply chain partners each introducing external attack surface that's often invisible to the primary organization.

Credential & Secret Exposure Monitoring

Automated Detection of Leaked API Keys, Passwords & Sensitive Data. One exposed API key, database password, or private credential can compromise an entire organization. Yet credentials leak constantly to public repositories, pastebin, dark web, and accidental exposure.

The Problem: The Visibility Gap

Modern enterprises are losing the battle of visibility. As infrastructure migrates to multi-cloud and remote environments, the attack surface has become elastic and unmanageable.

- **Asset Blindness:** 33% of security teams see less than 75% of their attack surface (HackerOne). 64% of breaches involve assets organizations didn't know existed (Verizon DBIR).
- **Shadow IT & AI:** Unsanctioned cloud buckets, S3 storage, RDS databases, and Shadow AI instances create entry points unknown to IT. 80% of organizations have shadow IT they don't track (Gartner).
- **Alert Fatigue:** Security teams are overwhelmed by thousands of low-context alerts from fragmented tools. Average organization receives 10,000+ alerts daily with 80% false positives (Gartner).
- **Speed of Exploitation:** Vulnerabilities are often exploited within hours of disclosure (43% within 24 hours), while manual patching takes 36+ days (Gartner). Attackers scan the internet continuously; organizations run periodic scans.
- **Credential Exposure:** 3.5 million secrets exposed annually on GitHub alone. Exposed credentials are weaponized within 5 minutes (GitGuardian).
- **Compliance Risk:** Unknown assets create regulatory violations. 43% of organizations fail audits due to asset discovery gaps (Forrester).

The Solution: Continuous Threat Exposure Management

AttackLens.ai replaces periodic "snapshots" with a Continuous Exposure Management (CEM) framework. Our value proposition lies in shifting security from a reactive (waiting for a breach) to a proactive (preventing the breach) stance.

- **Real-Time Digital Twin:** We create a live, agentless inventory of every internet-facing asset across your entire digital footprint.
- **Reduction in MTTR (Mean Time to Repair):** By delivering prioritized, high-context alerts correlated with actual threat intelligence and exploitability, we reduce the time spent on manual discovery, alert triage, and false positive investigation by 90%.
- **Compliance Assurance:** We provide the "continuous monitoring" evidence required by modern regulations. Automated compliance alignment with India's DPDP Act, ISMS, PCI-DSS, SOC 2, GDPR, HIPAA, and other regulatory frameworks.
- **Autonomous Discovery:** Passive and active crawling across global IPv4 space, DNS hierarchies, certificate databases, cloud provider metadata, and git repositories to discover domains, IPs, APIs, cloud buckets, and shadow infrastructure.
- **Live Risk Telemetry:** 24/7 continuous monitoring of configuration changes, certificate expirations, credential exposure, threat actor activity, and vulnerability disclosures. Instant alerts when new exposures appear or existing ones change state.
- **Attacker's Perspective Engine:** Instead of asking "what's vulnerable?" we ask "what can attackers actually exploit?" Correlation with threat intelligence, exploit availability, and active threat actor targeting ensures prioritization aligns with real-world risk, not CVSS scores alone.
- **Credential & Secret Monitoring:** Continuous scanning of public sources (GitHub, Pastebin, dark web, container registries) for exposed API keys, database passwords, SSH keys, and credentials
- **Cloud & Shadow IT Mapping:** Black-box reconnaissance of cloud infrastructure across AWS, Azure, GCP discovering S3 buckets, RDS databases, EC2 instances, Lambda functions, managed services, and all shadow deployments without requiring cloud account access.
- **Supply Chain & Third-Party Risk:** Automated discovery of vendor infrastructure, partner integrations, and API dependencies. Understand which external systems pose risk and what data flows to third parties.
- **Remediation Automation & Validation:** Integrated workflow automation that creates tickets, routes to responsible teams, tracks remediation progress, and automatically re-scans to validate fixes. Proof of remediation for audits and compliance.

What makes AttackLens.ai a "Moat-Driven" Product?

1. **AI-Powered Asset Attribution:** Uses proprietary ML models to accurately fingerprint and claim assets belonging to a parent company, even when they lack clear naming conventions.
2. **Shadow AI Discovery:** Specifically tracks the use of unsanctioned AI models and API keys within the organization's ecosystem. AttackLens.ai is among the first to address Shadow AI as distinct attack surface. Monitors LLM usage, discovers exposed credentials on GitHub/Pastebin/dark web, maps data flow to external AI providers, validates model sources, identifies GDPR/HIPAA/PCI-DSS violations. No competitive alternative exists. Takes 18-24 months for competitors to replicate.
3. **Zero-Configuration Setup:** Requires only a company name or primary domain to begin mapping the entire global footprint in minutes. Proprietary "seedless" discovery engine built on years of R&D. No manual scope definition, no API configuration, no agent deployment, no network access required.

Focused Industries

We focus on sectors where digital trust is non-negotiable and regulatory pressure is high:

BFSI (Banking & Finance)
The largest segment, accounting for ~24% of the market due to high breach costs ($6M+ average).

Healthcare
Rapidly adopting telemedicine and interconnected medical IoT devices.

Enterprise IT & eCommerce
Organizations with massive, high-velocity digital footprints.

MSSPs
Partners who use our platform to manage the attack surfaces of hundreds of smaller clients simultaneously.

EXTERNAL CTEMS PRODUCT FLOW

Six stages. One loop that never stops.

Discover
Continuous internal discovery with no prior knowledge and no manual input. Every asset is identified, registered, and time-stamped the moment it comes online.

Enumerate
Every discovered asset is assessed in real time across two dimensions simultaneously. Packages are matched against live CVE databases and configurations are tested against CIS benchmarks

Map
A live model of the entire environment. Asset connections, trust zones, network paths, and credential relationships are constructed and updated continuously

Prioritise
Every signal is combined into one ranked remediation backlog. Severity, asset criticality, network position, attack path proximity, exploit availability, and compliance status are all factored in

Act
Three resolution modes for operational reality. Mitigate, Remediate, and accept Risk.

Track
Every finding carries an immutable lifecycle, time-stamped and owner-attributed at every transition.

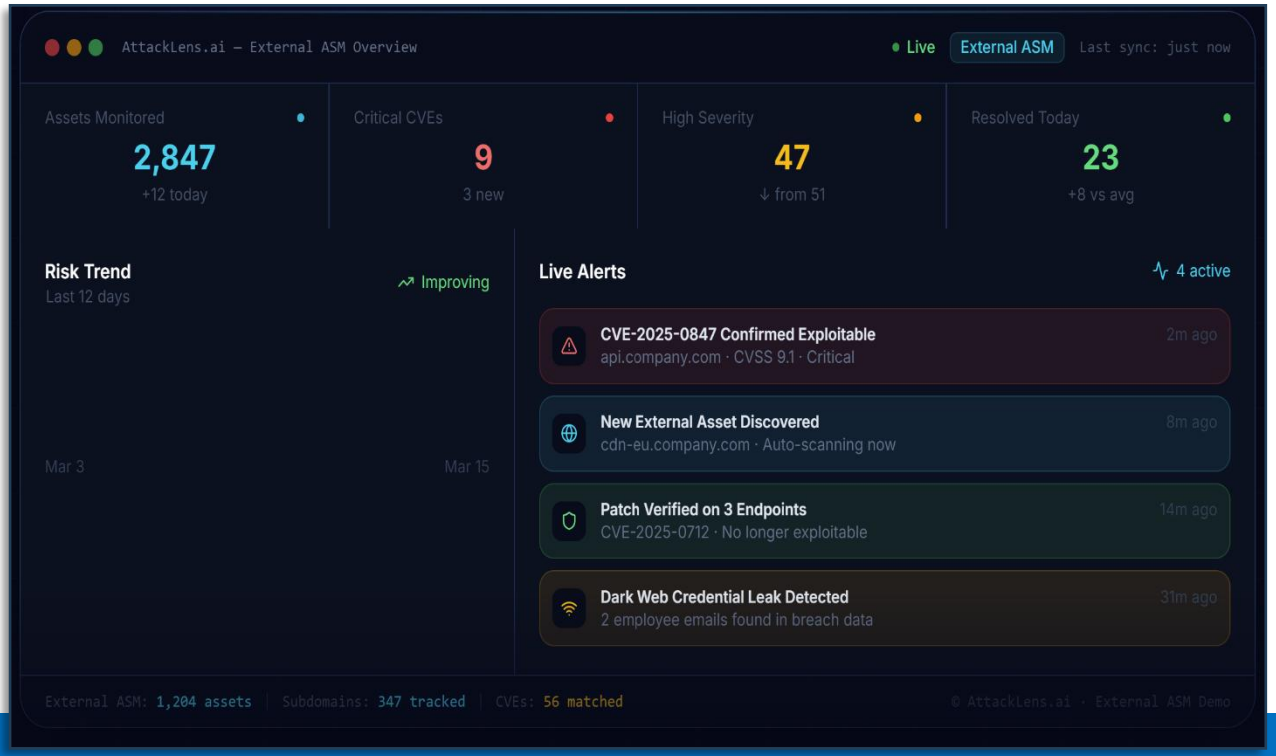
REPORTING

One data source. Five views. Every stakeholder sees what they need to act. Zero manual assembly. Zero reconciliation

Executive Summary

Board, CEO, CFO, C-suite

- Single risk score (0 to 100) with 12 month trend line
- Top three risks in business outcomes, CVE identifiers
- Remediation velocity segmented by severity
- Compliance posture with trajectory
- Resource and environment context that supports investment conversations



Vulnerability Intelligence

Security engineers, SOC, security ops

- Newly discovered CVEs with exploitability scoring
- Prioritised remediation queue with ownership and SLA state
- Findings approaching or breaching SLA surfaced at the top
- Regressed and re-opened findings isolated and flagged

Asset Inventory

IT ops, infrastructure, asset owners

- Full estate inventory maintained continuously, not quarterly
- Per asset security posture with open vulns and benchmark score
- New, changed, and decommissioned assets tracked on discovery
- Software and versions flagged for EOL and known exposure

Risk Assessment

GRC, risk managers, CRO, CFO

- Highest consequence attack paths mapped end to end
- Governed risk acceptance list, risk mitigation and remediation
- Residual risk projection based on current remediation pipeline
- Risk introduction rate versus resolution rate over time

CIS Compliance

Auditors, compliance managers, regulators

- Per control pass/fail with expected versus actual values
- Aggregate score by benchmark version and profile level
- Remediation steps mapped to every failing control
- Suppressed controls governed with approver, rationale, and expiry

USECASES

1 From Services to Product Innovation

For years, our team operated in cybersecurity services — identifying critical threats but constrained by reliance on third-party tools. We knew what needed to be done, but lacked control over how it was executed. This limitation sparked a shift: we began collecting real-world use cases and transforming them into a unified product platform.

2 The Hidden Risk: Unknown Digital Assets

During multiple vulnerability assessments, we consistently discovered undocumented assets, forgotten subdomains, and shadow IT infrastructure. In many cases, customers were completely unaware of these exposures. This revealed a fundamental truth: you cannot secure what you don't know exists.

3 The Wake-Up Call: Unknown Attack Incidents

In a critical incident, a client received a vulnerability report from an unidentified external party concerning previously unknown assets. These assets were outside the defined scope of our services. If visibility is incomplete, can security ever be complete? This became a defining moment — highlighting the urgent need for continuous and complete asset

4 The Industry-Wide Reality: Limited Visibility

With over 6 years in the cybersecurity market, we've observed a consistent pattern: no organization has 100% visibility of its digital assets. This isn't a tooling issue — it's a systemic gap in how security is approached.

5 The Efficiency Problem

Traditional VAPT processes are time-consuming, manual-heavy, and difficult to scale. Our engineers were spending excessive time on exploitation, proof-of-concept creation, and reporting. This led to a key innovation: AI-driven PTaaS (Penetration Testing as a Service) to deliver faster, scalable, and continuous security validation.

6 The Silent Threat: Third-Party Breaches

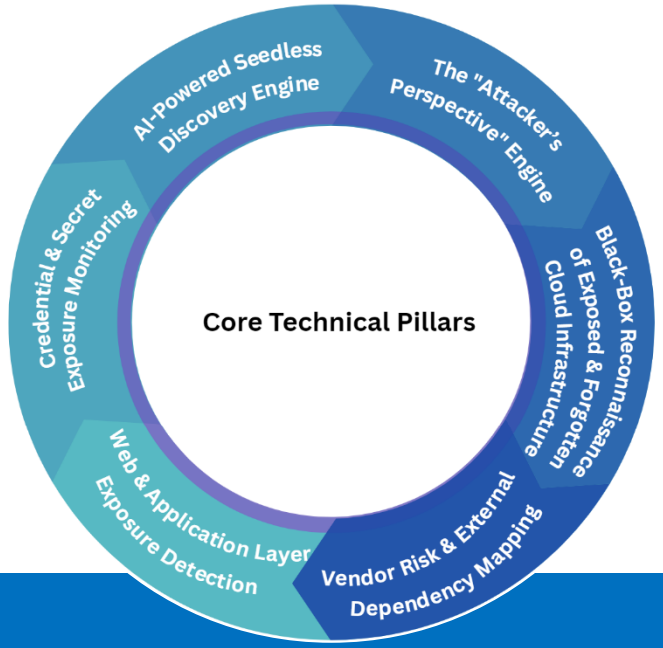
We encountered a case where an employee used official credentials on a third-party platform that was breached. Credentials were leaked on the dark web and attackers gained access to internal enterprise tools. Your security is only as strong as your weakest external dependency.

7 Regulatory Push: Compliance Driving Adoption

Regulators like the Reserve Bank of India have mandated stronger cybersecurity frameworks. Attack Surface Management is becoming mandatory, especially in banking. Compliance is no longer optional — it's a business necessity.

8 Rise in Global Cyber Threats & Digital Growth

Cybercrime is evolving rapidly with more sophisticated attacks, increasing frequency, and expanding attack surfaces. Global digital adoption is accelerating — creating both opportunity and exponentially larger attack surfaces. Organizations now need multi-layered, continuous threat protection, not periodic assessments.



BORNSEC BORN TO SECURE | Attacklens Continuous Threat Exposure Management