ENTERPRISE SECURITY VALIDATION BROCHURE

RefineSec

Validate Your Defenses in Real-Time

Validate, measure, remediate, and improve.

The only Agentic AI CTEM platform bridging the gap: Automated remediation from Breach/Attack Simulation across EDR, XDR, and DLP.

RefineSec continuously maps your attack surface and simulates real-world breach paths to validate the live efficacy of your EDR, XDR, AV, and DLP controls - turning uncertainty into measurable resilience.

Validate Live Defenses

Continuously test whether your controls work in practice - not just on paper.

Measure True Risk

Cut through alert noise to quantify actual exploitability and exposure.

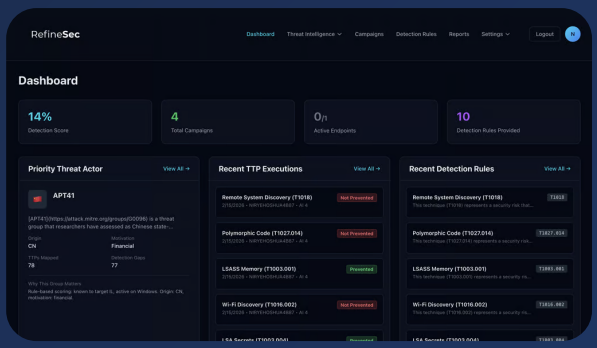
Remediate Fast

Push ready-to-deploy prevention logic and policy updates directly to your stack.

Improve Continuously

Re-test remediated gaps and track hardening progress over time.

- AI-driven breach simulation
- Ready-to-deploy remediation
- Board-ready reporting
- Sovereign deployment options



Operational clarity across simulated attacks, missed techniques, remediation outcomes, and resilience progress - built for security teams and executive stakeholders.

THE MARKET PROBLEM

The EDR / XDR Reality Check: Exposing the Gaps in Your Defense

Heavy investment in EDR and XDR often creates false confidence. Vendor promises suggest broad protection, but empirical validation shows many environments remain vulnerable to sophisticated, mutated, AI real-world attack paths.

V
Volatility

Polymorphic AI attacks mutate continuously, creating evasive behaviors that bypass static detections.

U
Uncertainty

93% of malicious actions concentrate around a small set of MITRE ATT&CK techniques many teams still under-validate.

C
Complexity

Standard EDR/XDR deployments often achieve only 20-30% effective coverage against mutated threat variants.

A
Ambiguity

With 450k+ new malware samples every day, manual rules engineering cannot keep pace with attacker iteration.

Why reactive validation is not enough

70-80%
of sophisticated mutated attacks may evade default configurations.

10
core MITRE techniques account for most observed malicious actions.

450k+
daily malware samples overwhelm manual content creation.

1 truth
Only live simulation shows what your controls actually stop.

RefineSec replaces "wait and see" security with empirical, proactive validation - exposing exploitable gaps before an adversary does.

MITRE ATT&CK aligned validation

MITRE | ATT&CK™

Not more alerts. Teams need proof of control efficacy, precise exposure measurement, and a path from simulation to action.

Not generic assurance. Teams need validation against real breach methods and AI-mutated variants that target production environments.

Not isolated testing. Teams need a full-stack view across EDR, XDR, AV, and DLP working together.

Strategic value: move from vendor promises to measured security performance and actionable tuning.

ATTACKERS adopt AI; DEFENDERS have yet to catch up

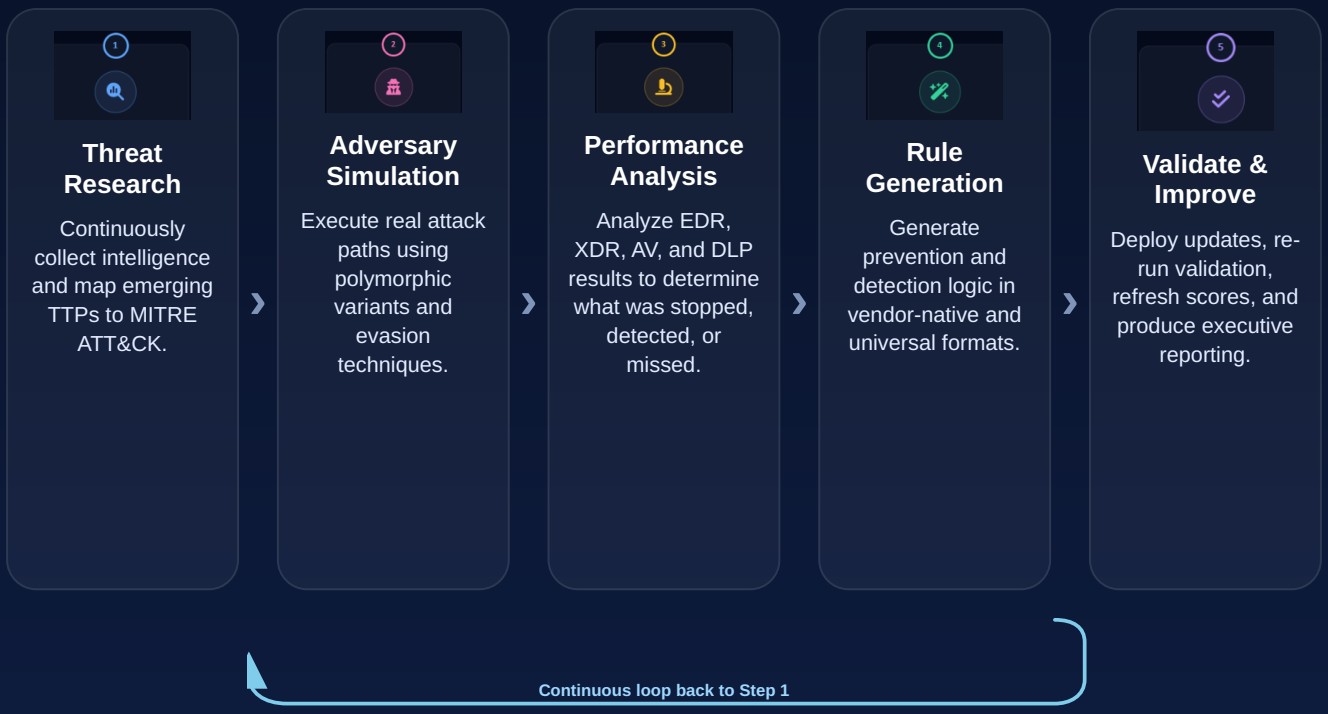
HOW IT WORKS

The Continuous Resilience Platform

RefineSec delivers an Agentic AI-powered CTEM solution that shifts organizations from reactive detection to continuous prevention through a closed-loop operating model.

How It Works: 5 Steps to Continuous Prevention

A continuous, automated cycle that validates controls, generates remediation, and restarts to prove resilience over time.



Isolated Environment | No Production Risk | Same-Day Results | < 1 Hour Deployment

The loop restarts continuously - daily, weekly, or monthly - to verify hardening and sustain resilience.

Zero-risk validation

Every test runs in isolated sandboxes or VMs to ensure zero production impact and zero business disruption.

Full-stack coverage

Validate the complete control plane across EDR, XDR, AV, and DLP - not point solutions in isolation.

REMEDIATION AT SCALE

BEYOND VISIBILITY: ACTIVE REMEDIATION

Stop Pointing at Gaps. Start Closing Them. Traditional BAS platforms leave teams with a long to-do list of vulnerabilities. RefineSec bridges the final mile - turning simulation insights into active, automated defenses before an adversary can even strike.

How remediation becomes operational

Autonomous hardening

For every technique that bypasses your controls, RefineSec generates prevention rules prioritized by business impact - reducing the gap between detection, tuning, and enforcement.

Expose
Simulate a production-relevant attack path and isolate the exact failure point.

→

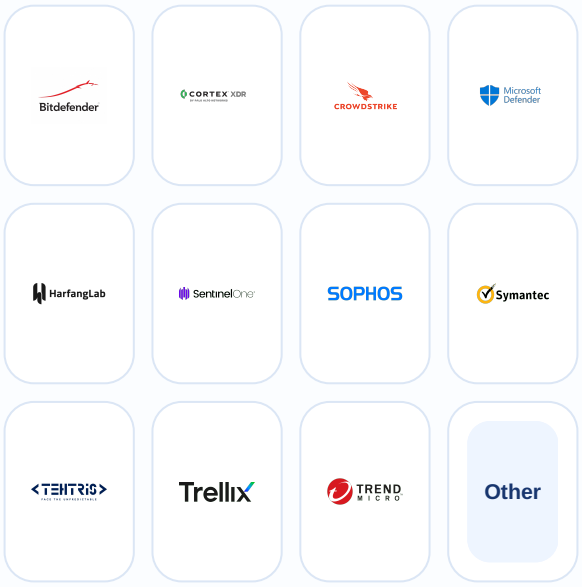
Generate
Create rule logic and policy updates matched to the missed technique.

→

Enforce
Deliver ready-to-deploy prevention content back into the security stack.

Vendor-native prevention delivery

Endpoint and detection ecosystems sorted alphabetically for easier scanning, with additional partner logos integrated into the page 4 delivery view.



Universal defensive standards

Instant remediation
Move from finding exposure to deploying controls without long manual cycles.

Lower engineering effort
Reduce the burden on SOC and detection teams by automating content creation.

Preemptive protection
Continuously close the window between simulation insight and defensive action.

Supports vendor-native delivery plus universal content formats such as Sigma, Sysmon, and YARA.

DEPLOYMENT FLEXIBILITY

Your Environment. Your Sovereignty.

Whether you operate fully in the cloud, require local EU data sovereignty, or run entirely disconnected, air-gapped infrastructure - RefineSec seamlessly adapts to your architectural requirements with zero operational friction.

OPTION 1

Audit Service

A low-friction service model where RefineSec experts execute the simulation cycle and deliver prioritized remediation outputs with minimal internal overhead.

- Fast start for lean security teams
- No heavy operational lift
- Actionable results and implementation guidance

OPTION 2

Sovereign SaaS

France-hosted deployment designed for organizations that need managed speed while preserving EU data sovereignty and operational assurance.

- Supports strict residency expectations
- Accelerates rollout and onboarding
- Ideal for regulated enterprise environments

OPTION 3

Air-Gapped

A full on-premise deployment model for disconnected or classified infrastructures that require total control of validation logic, data, and operations.

- Designed for critical infrastructure and government
- Keeps validation intelligence local
- Supports absolute operational security

Operational confidence across every hosting model

Rapid adaptation
RefineSec adapts to your environment quickly to deliver same-day time to value.

Zero production disruption
Validation occurs in isolated execution layers, not on live production systems.

SATAWAH-ready
Secure Any Time, Any Where, Any Hosting with one continuous resilience logic.

EXECUTIVE VALUE

BUSINESS VALUE AND PROOF POINTS

Proven Resilience Against Real-World Adversaries. RefineSec turns complex security metrics into a data-driven bridge for board-level oversight. By continuously validating your controls against top MITRE ATT&CK techniques, the platform proves where protection succeeds and where automated tuning is required.

Board-ready security performance

Measure control efficacy, track remediation outcomes, and show how resilience improves across repeated validation cycles - without depending on assumptions or vendor defaults.

Validation speed — **Same day**

Production safety — **Zero risk**

Coverage improvement loop — **Continuous**

Leadership clarity — **Board-ready**

Neutralizing high-prevalence techniques

Legacy tools test generic signatures. RefineSec validates live readiness against the exact MITRE ATT&CK methods favored by modern attackers - including AI-mutated variants designed to slip past standard EDR and AV configurations.

- Higher confidence in existing EDR/XDR investments
- Faster translation from exposure finding to deployable control
- Clear evidence trail for technical and executive audiences
- Continuous retesting to confirm the gap is truly closed

TECHNIQUE	MITRE	HOW REFINESEC PROVES AND IMPROVES RESILIENCE
Process Injection	T1055	Simulates advanced injection variants to surface missed detections and generate deployable prevention logic for memory manipulation and process abuse.
Credential Theft	T1555	Runs realistic theft scenarios to validate exposure and harden controls with rules mapped to observed attack behavior.
Impair Defenses	T1562	Tests tampering and self-deactivation techniques, then closes the gap with prioritized defensive content and re-validation.

Transform Your Security Posture Today

Validate, measure, remediate, and improve resilience against real-world adversaries with an Agentic AI CTEM platform built for operational security teams and executive accountability.

RefineSec LLC
Agentic AI CTEM Platform
contact@refinesec.com
www.refinesec.com