eSENTIRE

ATLAS PLATFORM

Controlled Autonomy SecOps

The Gaps in AI-Powered Security

AI-powered threats move at machine speed, and attackers now probe defenses faster than quarterly pen tests can keep up. SOC teams face an impossible choice: drown in alerts, trust AI blindly, or scale humans to match the tempo. eSentire's Atlas Platform resolves this with agentic AI operatives that run continuous offensive validation, autonomous pen testing, and machine-speed detection, investigation and response, all under engineered human-judgment controls.

-7 Days
Mean Time to Exploit
Mandiant M-Trends, 2026

1,900+
Attacks per week
SentinelOne, 2025

53%
of security leaders
Cite qualified candidates as a high-impact challenge
KPMG Cybersecurity Survey, 2026

10-20%
Utilization of existing security technology
Ernst & Young, 2025

Continuous Security Coverage

Most MDR providers only play defense after a breach begins. eSentire operates a continuous security lifecycle that unifies offensive validation, managed detection, and autonomous response, one compounding flywheel under Controlled Autonomy governance. Better MDR means offense sharpens detection; detection accelerates response, response stops the attacker, and every autonomous action is explainable, reversible, and policy bounded. On repeat.

PREEMPT
Autonomous Offensive Security & CTEM

- Recurring adversarial validation, not quarterly pen tests
- Vulnerability Scanning and ingestion through Qualys, Tenable, Rapid7, Wiz
- Attack simulation with adversary TTP's
- External attack surface management (EASM)
- Addresses the five-stage CTEM lifecycle

DETECT
Managed Detection & Response

- 24/7 SOC with unlimited threat hunting
- Multi-signal ingestion — any vendor, any stack
- Agentic AI investigation across every signal
- Automated containment in minutes
- Full audit trail for investigation process and actions

RESPOND
Controlled Autonomous Response

- AI operative teams — Investigator, Critic, Reporter
- Machine-speed containment, human-on-the-loop
- Policy-bounded action within customer authority envelopes
- Every decision explainable, reversible, auditable
- Tier-3 analyst validation on every outcome

ATLAS Benefits

99% less noise
Atla AI + Tier-3 Analyst Validation Alignment

99.99% initial host
Compromise Prevention

<30s to engage
Mean Time to Engage (MTTE) a Signal

<5min
From Signal to Full Threat Context

The Engine Behind Controlled Autonomy

Atlas leverages elite agentic AI operatives to work together in a continuous security lifecycle across offense, defense and response. Every cycle shrinks the attack surface. Every autonomous action is governed by four trust conditions.

The Four Trust Conditions

Atlas delivers because these trust conditions hold it in check. Each one is what allows Atlas to act at machine speed without forcing customers to choose between autonomy and accountability. The architecture that boards, regulators, and cyber insurers increasingly require.

1. **Explainability:** Every action produces a human-readable rationale — the feedback signal in plain language.
2. **Shadow Approval:** High-consequence actions are staged for human review with the investigation already complete. Human-on-the-loop scales because the analyst confirms a finished case.
3. **Reversibility:** Every action is architecturally reversible. Giving Atlas the ability to engage in under 30 seconds without ceding control on decisions.
4. **Policy-Bounded Authority:** The customer defines the authority envelope; Atlas executes inside it. Anything outside escalates instead of executing — autonomy delegated, not outsourced.

The Atlas Platform

Why 2,000+ Security Teams Run with eSentire

> *"We look at eSentire to be the experts. We trust them implicitly. They're with us through the thick and thin till the end."*

CISO, Financial Services
GARTNER PEER INSIGHTS

> *"eSentire has been an indispensable partner. Their proactive monitoring and strategic advice have contributed to a significant improvement in our cyber resilience."*

Security Leader, Six-year customer
GARTNER PEER INSIGHTS

2,000+ organizations in **80+** countries | **25** years of SOC expertise | **2M+** endpoints protected | MDR Leader, Forrester Wave™

Who controls the pace, you or the attacker?

See how Atlas delivers offense and defense in the same loop.

LET'S TALK SECURITY →

IF YOU'RE EXPERIENCING A SECURIT Y INCIDENT OR BREACH CONTACT US 1-866-579-2200

eSentire

eSentire, Inc., the Authority in Managed Detection and Response (MDR), protects the critical data and applications of 2000+ organizations in 80+ countries, across 35 industries from known and unknown cyber threats by providing Continuous Threat Exposure Management, Managed Detection and Response, and Incident Response services designed to build an organization's cyber resilience & prevent business disruption. Founded in 2001, eSentire protects the world's most targeted organizations with 65% of its global base recognized as critical infrastructure, vital to economic health and stability. By combining open XDR platform technology, 24/7 threat hunting, and proven security operations leadership, eSentire's award-winning MDR services and team of experts help organizations anticipate, withstand and recover from cyberattacks. For more information, visit **www.esentire.com** and follow **@eSentire**.