Solution Brief

eSENTIRE

eSentire Controlled Autonomy SecOps for Manufacturing Organizations

Preempt, Detect, and Respond Across IT, OT, Cloud, and Identity Before Production Is at Risk.

Most manufacturing organizations today are battling AI-enabled cyber threats that move faster than traditional security programs were built to handle. For security leaders, the gap is coverage: the ability to detect a threat moving across IT and OT boundaries, correlate it in real time, and act on it before it reaches production systems. Three converging conditions make this structurally difficult:

1. *The heightened use of valid credentials means attackers can operate as authorized users, generating few to no traditional alerts, allowing them to embed deeply within your environment.*

   Use of valid credentials has led to an **85%** intrusion ratio.

2. *The interconnected nature of IT/OT means that compromised credentials can move from your network to production system in minutes.*

   It takes an average time of **14 minutes** for attackers to move from credential theft to active exploitation.

3. *Third-party remote access is one of the most exploited, and least monitored, entry points in manufacturing.*

   Attacks against manufacturing organizations have grown by **81.6%** year-over-year.

Source: eSentire Threat Response Unit (TRU)

Controlled Autonomy SecOps, Built for Manufacturing Environments

eSentire's Atlas Platform continuously exposes, detects, and disrupts cyberattacks across any vendor stack, with every autonomous action explainable, reversible, and policy-bounded. Rather than waiting for an alert to escalate, Atlas AI Operatives apply an attacker's lens to your environment continuously across IT, OT, cloud, and identity simultaneously and act at machine speed within the authority boundaries your team defines.

This is not bolt-on AI. eSentire's Atlas Platform was built from the ground up as an agentic platform with offense sharpening defense, defense informing offense, and an operating model in a continuous closed loop:

PREEMPT

Continuously probes your environment from the attacker's perspective. Maps your attack surface across IT, OT, cloud, and identity, and validate exposures before adversaries take advantage.

DETECT

24/7 managed detection across any signal source. Ingests from your existing EDR, network, SIEM, cloud, and identity. Atlas AI engages every signal in under 30 seconds; no delay.

RESPOND

Machine-speed containment within customer-defined authority envelopes. High-consequence actions like isolating a production system are staged for human review before execution. Every action is explainable and reversible.

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

Fully autonomous security creates a new accountability problem: when an AI system makes a consequential decision about a production asset, who is responsible? Controlled Autonomy SecOps is the architecture designed to answer that question.

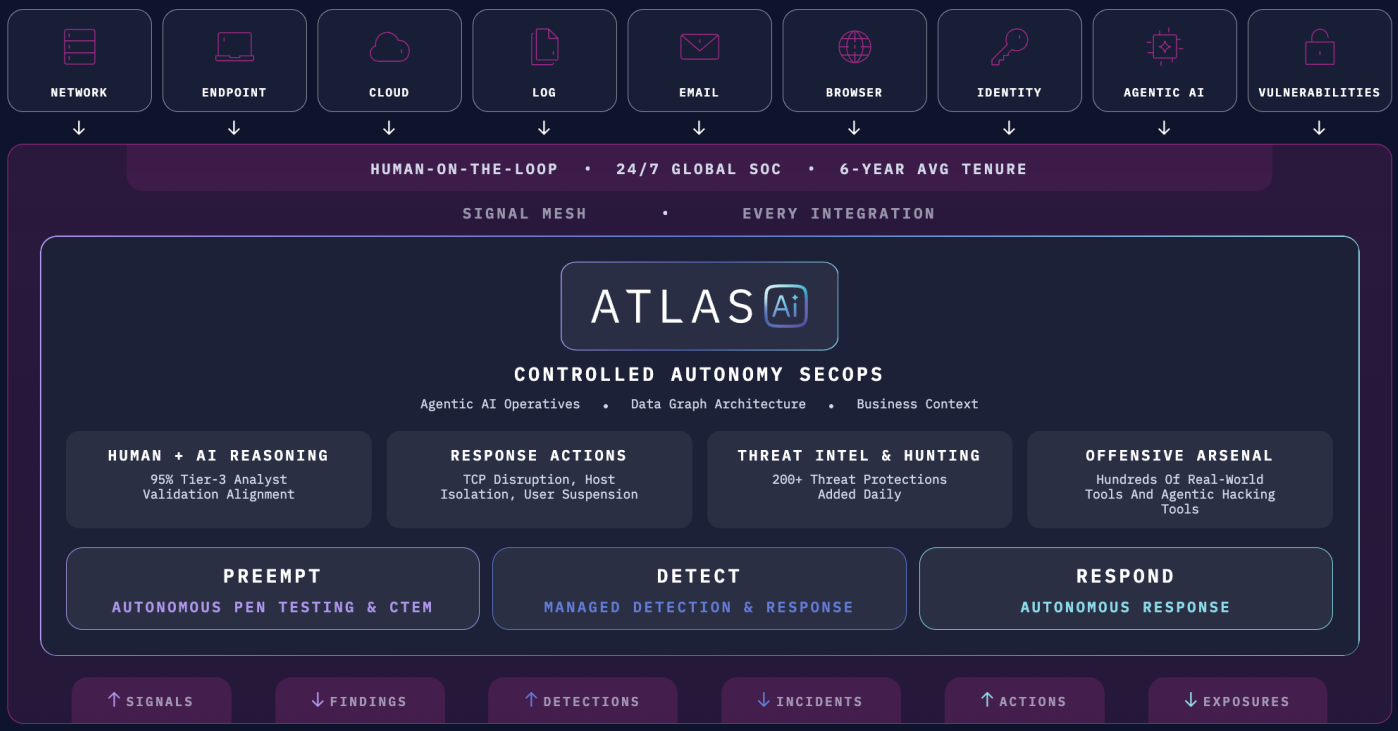
For manufacturing, this means your team retains operational control. Atlas moves at machine speed inside the boundaries you set. The decision to stop the line stays with the people who understand production consequences.

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



Closing the Gap: Manufacturing-Specific Capabilities

The challenge/solution table below maps the specific exposures manufacturing security leaders face to how the Atlas Platform addresses them across any stack and any vendor, from day one.

Manufacturing Security Challenge	How eSentire Addresses It
IT/OT boundaries create detection blind spots	Atlas ingests signal across IT, OT, cloud, and identity simultaneously. Threats moving across boundaries are correlated in real time, not discovered after the fact.
Vendor remote access is an unmonitored entry point	Every third-party connection is treated as a potential attack path. Atlas monitors remote access sessions with the same depth applied to internal network traffic.
Ransomware moves faster than analyst queues	Atlas AI Operatives engage every alert in under 30 seconds. Investigation, enrichment, and, where policy allows, containment, happen before a human picks up the ticket.
Legacy security tools weren't built for converged environments	Atlas layers across your existing stack on day one. No rip-and-replace. Every tool you already run works harder with bidirectional enrichment from Atlas.
Production decisions can't wait on incomplete data	Every Atlas action is explainable and reversible. When a threat crosses an OT boundary, your team has the context to decide – stop the line or keep running – with confidence.

CASE STUDY

Rawlings Sporting Goods

Rawlings Sporting Goods outsourced 24/7 SOC-as-a-Service to eSentire, resulting in 24/7 threat detection and response capabilities, seamless integration with their existing tech stack, and a centralized view of their environment for complete attack surface visibility.

VIEW CASE STUDY →

"The great thing about working with the SOC with eSentire has been not only the responsiveness but really them becoming an extension of our team. It's been fantastic to have somebody that not only understands our business, but also our environment and allows us to continue to grow as a company because they're growing with us along the way."

- MARK HAUBEIN, VP Information Technology, Rawlings

Ready to Get Started?

Connect with an eSentire Security Specialist to see Managed Detection & Response working across your Microsoft environment.

LET'S TALK SECURITY →

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

eSentire is a leader in Controlled Autonomy SecOps, protecting 2,000+ organizations across 35+ industries around the world. Founded in 2001, the company's Controlled Autonomy SecOps operating model pairs agentic AI operatives with engineered human-judgment controls, delivering expert-depth security outcomes at machine speed without ceding accountability to opaque automation. Powered by the unified agentic AI Atlas Platform, eSentire's Atlas AI + 24/7 expert human SOC coverage delivers offensive capabilities that preempt exposures before attackers do, detect, and respond to stop threats in real time. For more information, visit **www.esentire.com** and follow **@eSentire**.