

You Shouldn't Have to Choose Between Speed and Depth

Detection is fast.
Investigation isn't. That's where incidents escalate.

SECTION 01 – THE REALITY

SOC TOOLS

- Fast detection
- Alert-driven workflows
- Limited endpoint visibility
- No full-text search

Fast, but shallow

FORENSIC TOOLS (Magnet, EnCase)

- Full-text search
- Deep artifact analysis
- Complete visibility

But:

- Slow acquisition
- Offline workflows
- Specialist-led

Deep, but slow

SECTION 02 – CORE INSIGHT

Your investigation model doesn't scale

You're not lacking tools.
You're stuck between two systems that don't work together.

TRADITIONAL DFIR

A "large case" =

10–20

systems

VS

WITH MAGELLAN

A "large investigation" =

10–20,000

systems

Attacks don't stay contained to a handful of endpoints.

SECTION 03 – WHAT ACTUALLY HAPPENS



SECTION 04 – THE TRADEOFF

Speed (SOC tools)

✗ No depth

Depth (Forensic tools)

✗ No speed

*"You don't need more alerts.
You need forensic answers — at the moment the alert fires."*

AIR + Magellan: Forensic Capability at SOC Scale

Automated collection meets real-time investigation — inside the SOC.

SECTION 06 — HOW IT WORKS



SECTION 07 — WHAT'S DIFFERENT

- Full-text search across all endpoints
- Automated evidence collection
- SOC-native workflows
- Deep artifact-level visibility
- Near real-time investigation
- Scalable across every alert

SECTION 08 — COMPARISON

CAPABILITY	Magnet / EnCase	AIR + Magellan
Full-text search	Yes (offline)	Yes (near real-time)
Investigation speed	Hours–days	Minutes
Workflow	Case-based	Continuous
Users	Specialists	SOC analysts
Investigation timing	After escalation	At alert stage
Scale	10–20 systems	10–20,000 systems

SECTION 09 — STRONG STATEMENT

Most investigations shouldn't require forensic workflows

Forensic tools remain critical for deep cases.
But they shouldn't be the default for everyday investigation.

SECTION 10 — WHAT CHANGES

BEFORE	WITH AIR + MAGELLAN
Alert → Triage → Escalate → Investigate (<i>Magnet / EnCase</i>)	Alert → Investigate immediately → Respond

SECTION 11 — OUTCOMES

- Replace most traditional DFIR workflows
- Reduce reliance on Magnet & EnCase
- Investigate every alert — not just escalated cases
- Get to root cause faster
- Scale investigations across thousands of systems

FINAL POSITIONING

Forensic answers — at SOC speed and scale

Stop escalating. Start investigating.

▶ See Magellan in Action

Book a Demo →