eSENTIRE

ATLAS PLATFORM

Atlas Sensor [FORMERLY ATLAS AGENT]

Extends Atlas across your environment. Included in every Atlas package.

Atlas Sensor runs alongside the EDR/EPP you already have. It collects forensic-level telemetry and logs, and gives the eSentire SOC host and identity response.

WHAT ATLAS SENSOR ENABLES

7 EDR/EPP platforms supported

3 OS families supported

- Syslog collection
- Active Directory identity response
- Patch Management
- IOC threat hunts
- Incident response (IR)
- Windows Event Log collection
- Pen testing
- Atlas AIDR
- TRU detections
- Telemetry collection

What Atlas Sensor Delivers

PREEMPT

Probes your defenses like an attacker would

- Identifies each host to Atlas and inventories its OS, installed software, network connections and signed-in users
- Maps installed software versions to known CVEs
- Endpoint presence for offensive security testing, available today
- Third-party application patching with Atlas Patch Management

  Windows 10 and later, or Windows Server 2025

DETECT

Watches every signal surface for threats

- Forensic-level telemetry from the endpoint
- Windows event logs, local log files and syslog
- Monitors files and targeted registry keys
- EDR bypass detections, eSentire detections and IOC threat detection on top of your EDR
- Atlas AIDR deployed with one toggle, with install and run status reported

RESPOND

Shuts them down and reduces future exposure

- Response actions on the host by Atlas and the eSentire SOC
- Revokes compromised identities as a response action
- Connects to on-prem Active Directory on Domain Controllers

How It Works

1. **Deploy**

   New customers deploy it alongside their EDR/EPP at onboarding.

2. **Connect**

   The sensor identifies each host to Atlas and runs alongside your supported EDR/EPP.

3. **Turn On Modules**

   Log collection, on-prem Active Directory, Patch Management and Atlas AIDR, on or off as you need them.

Works With Your EDR/EPP

Your EDR/EPP stays in place for front-line protection such as AV blocking. Atlas Sensor runs alongside it, and Atlas shows which EDR/EPPs are supported directly in the Atlas UI.

Supported EDR/EPP*

- Microsoft Defender (full and AV)
- SentinelOne
- CrowdStrike
- Cortex by Palo Alto Networks
- ThreatDown
- Sophos
- ESET

* A supported EDR/EPP must be in place. Atlas Sensor runs on Windows, macOS and Linux endpoints and servers. Windows 7 and Windows Server 2008 R2 are no longer supported.

> *"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

Thousands of organizations in **90+** countries | **25** years of SOC expertise | **2M+** endpoints protected | **Leader**, IDC Marketscape for MDR

Extend Atlas Across Your Environment.

Included in every Atlas package.

LET'S TALK SECURITY →

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

eSentire is a leader in Controlled Autonomy SecOps, protecting thousands of organizations in 90+ countries across 35+ industries. 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**.