ArmorPoint.

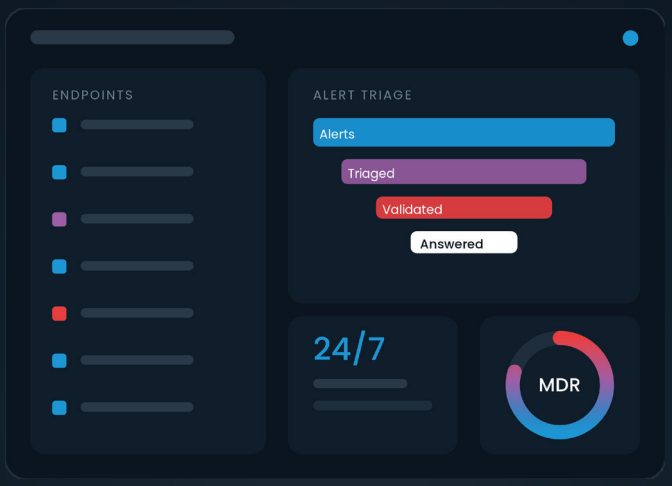
MDR • SOLUTION BRIEF

MANAGED DETECTION AND RESPONSE

From Endpoint Alerts to Answered Threats.

An EDR is very good at raising alarms and completely indifferent to who answers them. ArmorPoint MDR puts a 24/7 U.S.-based SOC behind your endpoints. Escalation-worthy alerts are triaged, investigated, and answered by an analyst, then documented so you can prove what happened.

BEST FOR Teams with endpoint risk and no 24/7 investigation and response behind their endpoints



THE PROBLEM MDR SOLVES

EDR tooling produces signals. Investigation, validation, response, and documentation still land on your team. Alert volume doesn't respect business hours, and most endpoint compromises won't either. Unvalidated alerts either burn analyst time or get ignored, and both carry a cost. When something is contained, someone has to record what happened, and why, for auditors and insurers.

> **ArmorPoint helps us answer three critical questions: How do we know we're secure? How do we know we're getting value? And is there anything we need to be concerned about?**
>
> **NATE SCHMITT**
> DIRECTOR OF CYBERSECURITY, CIT

WHAT'S INCLUDED

- 24/7 U.S.-based SOC monitoring across your covered endpoints
- EDR license and agent, provisioned through ArmorPoint
- Triage, investigation, and analyst validation of endpoint alerts
- Response and escalation under documented rules of engagement
- Case documentation and recurring reporting
- Endpoint-scope view of the ArmorPoint platform

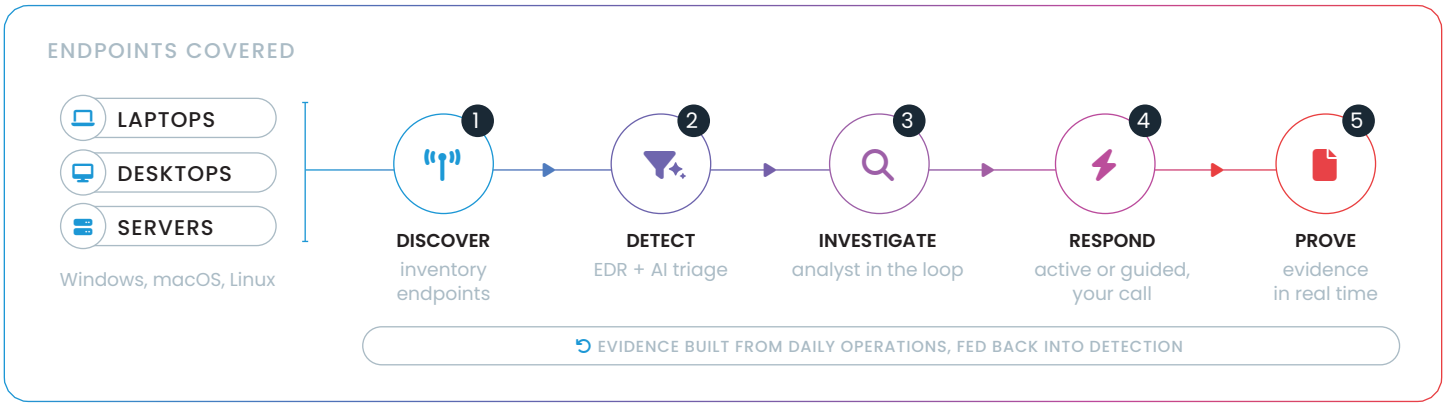
EDR, PROVISIONED THROUGH ARMORPOINT

MDR is built on EDR telemetry, so the EDR license and agent come provisioned through ArmorPoint as part of the service. That keeps detection, response actions, and the SOC workflow on one integration we run end to end, which lets an analyst execute an approved containment directly instead of opening a ticket between vendors.

SentinelOne · CROWDSTRIKE · cybereason

Already running an EDR you want to keep? That points you to MXDR, where bring-your-own EDR is supported. We map your options, including the transition path, during scoping.

HOW MDR WORKS



Vulnerability management, external attack surface visibility, threat intelligence, and compliance-ready reporting live on the same platform, visible from day one and included with MXDR.

WHO OWNS WHAT

RESPONSIBILITY	YOUR TEAM	ARMORPOINT
24/7 endpoint monitoring, investigation, and validation	Visibility	Primary
Containment and remediation	Approves	Recommends
Executing approved containment	Informed	Primary
Executing endpoint remediation and recovery	Approves and acts	Guides
Incident documentation and reporting	Visibility	Primary

You keep full platform visibility, and containment and remediation always run on your approval.

WHEN TO CHOOSE MDR

- → You want endpoint alerts investigated and contained under rules you approved in advance, not left to pile up
- → Endpoint alerts are being closed without investigation or not closed at all
- → A lean IT team is carrying security response on top of everything else
- → An auditor, insurer, or customer is asking how endpoint threats actually get handled

WHY ARMORPOINT

One platform, one SOC, and one accountable security operation.

ArmorPoint investigates, validates, responds, and documents endpoint threats as a single workflow, with predictable per-device pricing that scales with your business.

Scope Your MDR Fit armorpoint.com/services/mdr

SC Awards EXCELLENCE AWARD WINNER 2026

CYBERSECURITY STARS AWARDS WINNER 2026 The Hacker News

MES computing MES MIDMARKET 100 2026