ArmorPoint.

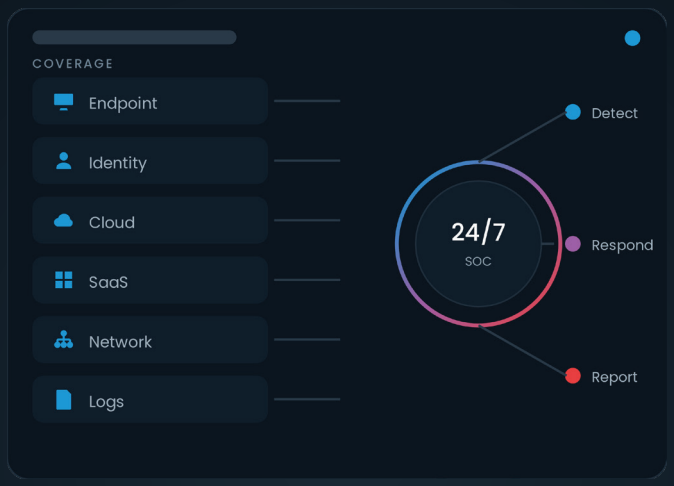
MXDR • SOLUTION BRIEF

MANAGED EXTENDED DETECTION AND RESPONSE

Full-Stack Managed Security Operations, Run by ArmorPoint.

Your team does not need more disconnected alerts. You need a security operation that can see, investigate, respond, and prove the work. ArmorPoint MXDR combines the ArmorPoint platform with a 24/7 U.S.-based SOC to run managed security operations across your environment.

BEST FOR Organizations that need broad security coverage without building a full SOC



THE PROBLEM MXDR SOLVES

Security teams are expected to cover endpoint, identity, cloud, SaaS, network, logs, vulnerabilities, and compliance evidence. Most do not have the staff, time, or operational model to run all of that around the clock. ArmorPoint MXDR runs detection, investigation, response, and reporting across the full platform, so coverage stops depending on headcount.

WHAT'S INCLUDED

- 24/7 U.S.-based SOC monitoring, investigation, and response
- The full ArmorPoint platform, including the ArmorPoint Agent
- Multi-source detection across endpoint, identity, cloud, SaaS, network, and logs
- Documented escalation, response workflow, and evidence trail
- Recurring reporting built for executives, auditors, and insurers

> "As an engineer, I like that they take *remediation accountability* rather than just dumping alerts on the customer."
>
> **AMMAR EKBOTE**
> Software Engineer at Pinterest and 2026 SC Awards Judge
>
> Pinterest

YOUR EDR, OR OURS

MXDR is built to work with an EDR solution. Bring the EDR you already run or include one through ArmorPoint. How much of the response ArmorPoint runs for you depends on which EDR you use.

Bidirectional integration — FULL RESPONSE

YOUR EDR ⟷ ARMORPOINT SOC

AVAILABLE ONLY WITH THE FOUR EDRs WE RUN

SentinelOne • CrowdStrike • Cybereason • Microsoft Defender

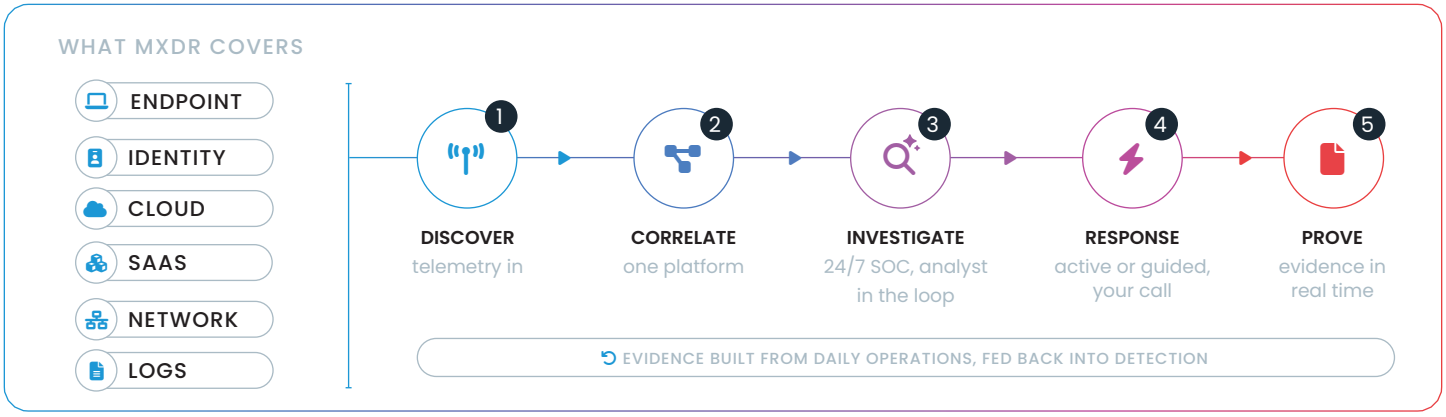
SOC-initiated isolation, quarantine, and containment, executed directly from the ArmorPoint platform under rules of engagement you approve in advance.

Ingest-only integration — GUIDED RESPONSE

YOUR EDR → ARMORPOINT SOC

Bring an EDR outside the core four and ArmorPoint ingests its telemetry for detection and investigation. Response executes through your own EDR console.

HOW MXDR WORKS



Plus vulnerability management, external attack surface visibility, threat intelligence, and compliance-ready reporting, all run on the same platform.

WHO OWNS WHAT

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

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

WHEN TO CHOOSE MXDR

- → Your internal team is lean and carrying response on top of everything else
- → You need ArmorPoint to run more of the operation, not hand you more alerts
- → Endpoint-only coverage is too narrow for your risk
- → Compliance pressure is rising, and evidence requests keep coming

WHY ARMORPOINT

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

Instead of stitching together tools, tickets, and multiple vendors, ArmorPoint runs detection, investigation, response, and reporting as a single, continuous workflow, with predictable per-device pricing and no unpredictable data-ingestion costs.

Request a SecOps Fit Review armorpoint.com/services/mxdr

SC Awards EXCELLENCE AWARD WINNER 2026

CYBERSECURITY STARS AWARDS WINNER 2026 The Hacker News

MES computing MES MIDMARKET 100 2026