24/7 SOC Response, With the EDR You Choose.

ArmorPoint MXDR pairs an XDR platform with a 24/7 U.S.-based SOC. We provide your EDR or connect the one you already use, and our analysts investigate suspicious activity either way. The difference is whether they act through the EDR or guide your team. Identity actions, such as disabling an account, run on your approval where an integration is in place.

ArmorPoint Provides the EDR.

EDR LICENSE INCLUDED

EDR + SOC Response

Automated protection backed by analysts who can act. The EDR enforces configured policies automatically, while ArmorPoint's 24/7 SOC investigates suspicious activity and initiates containment when needed.

DETECT	Provided EDR
INVESTIGATE	ArmorPoint SOC
RESPOND	**ArmorPoint SOC** Analyst-initiated

AVAILABLE EDR OPTIONS

- SentinelOne — COMPLETE
- CROWDSTRIKE — DEFEND
- cybereason — EDR

YOUR TEAM MANAGES

EDR deployment, policies, versions, and maintenance.

ARMORPOINT PROVIDES

Initial setup and Level 1 support: troubleshooting, guidance, and vendor liaison.

SOC-INITIATED CONTAINMENT

With standing authorization, ArmorPoint analysts can isolate endpoints, terminate malicious processes, and quarantine files without waiting for approval on each action.

Keep Your Existing EDR.

BIDIRECTIONAL API

Connected for Response

Extend your existing EDR with 24/7 SOC investigation and response. ArmorPoint analysts evaluate detections in the context of your broader security environment, determine when action is needed, and initiate endpoint response through the bidirectional API.

DETECT	Your EDR
INVESTIGATE	ArmorPoint SOC
RESPOND	**ArmorPoint SOC** Via EDR API

BIDIRECTIONAL EDR INTEGRATIONS

Microsoft Defender · FORTINET · SOPHOS · IRU (formerly Kandji) · CORTEX · TREND MICRO · SentinelOne · CROWDSTRIKE

YOUR TEAM MANAGES

EDR licensing, policies, configuration, and day-to-day administration.

REQUIRES

The Integration Marketplace add-on.

SOC RESPONSE VIA API

When your incident response plan authorizes it, ArmorPoint analysts act through your existing EDR. Otherwise, they give your team the steps to take.

DETECTION-EVENT API

Connected for Investigation

Make more informed response decisions without replacing your EDR. ArmorPoint analysts investigate your EDR's detection events alongside other connected security activity, helping your team understand what needs attention and why.

DETECT	Your EDR
INVESTIGATE	ArmorPoint SOC
RESPOND	**Your team** SOC-guided

WHAT YOUR TEAM RECEIVES

- **Detection details** — What triggered the investigation
- **Analyst findings** — What the SOC found and why it matters
- **Recommended actions** — Steps for your team to take in the EDR

YOUR TEAM MANAGES

EDR configuration, policy management, and ongoing maintenance.

GUIDED ENDPOINT RESPONSE

Your team carries out endpoint response in its EDR, informed by ArmorPoint's investigation findings and recommended actions.

See How Response Would Work in Your Environment.

Review your EDR setup with ArmorPoint to understand what you can retain, which endpoint actions the SOC can perform, and when your team would take the next step.

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