ArmorPoint.

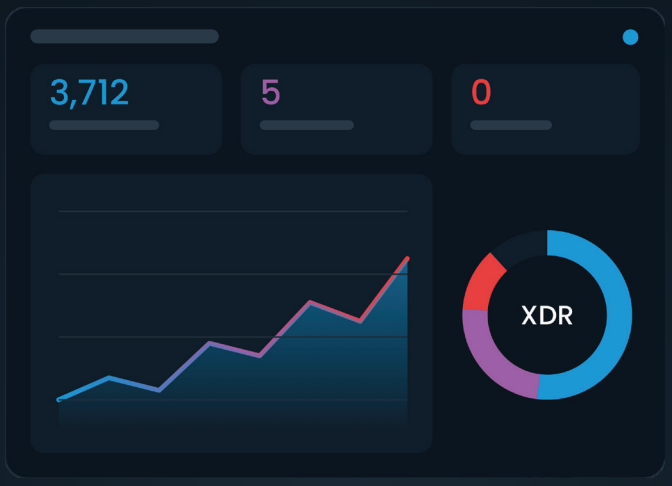
XDR • SOLUTION BRIEF

EXTENDED DETECTION AND RESPONSE

The ArmorPoint XDR Platform, Run by Your Team.

ArmorPoint XDR is the unified security operations platform behind ArmorPoint's managed MDR and MXDR services. It brings endpoint, identity, cloud, SaaS, network, and log data into one platform so your analysts can detect, investigate, respond, and prove the work.

BEST FOR Security teams with in-house analysts that want one platform, not a managed service



THE PROBLEM ARMORPOINT XDR SOLVES

Your analysts are stretched across consoles that don't talk to each other, so tracing a single attack means switching between tools while the clock runs. The point tools bought to close that gap usually cost more than they return once you count licensing, upkeep, and the seams between them. Teams don't want another managed service. They want to run their own security operation on a platform built for it.

WHAT'S INCLUDED

- Unified XDR platform operated by your team
- AI-assisted alert correlation and prioritization
- Endpoint, identity, cloud, SaaS, network, and log visibility
- Built-in reporting and MITRE ATT&CK-mapped incident reports
- Access Integration Marketplace, APIs, and webhooks
- Optional advisory and implementation services

ONE PLATFORM, FIVE OPERATIONAL HUBS

Visualize

Dashboards, scheduled reports, and a live data canvas on one source of truth, so the CISO, the auditor, and the analyst all see the same numbers.

Operations

AI-accelerated triage surfaces the signal that matters, so your analysts spend their time on incidents instead of the queue.

Governance

One control set mapped across CMMC, SOC 2, PCI, HIPAA, NIST CSF, and custom, every control linked to live evidence, not screenshots gathered the week before an audit.

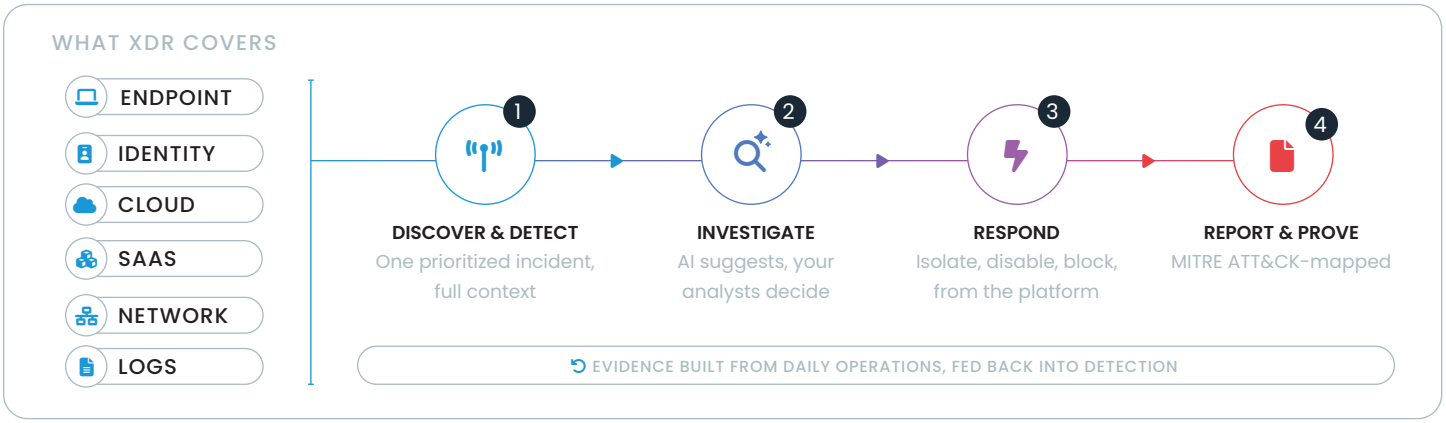
Environment

Every asset, identity, and app across endpoints, cloud, and SaaS in one inventory. If it produces a log, ArmorPoint can ingest it, so nothing has to run in the dark.

Response Center

Curated feeds, CVE enrichment, and your external attack surface, all checked against your real inventory, so you spend time on the threats that actually reach you.

HOW XDR WORKS



THE OPERATING MODEL

RESPONSIBILITY	YOUR TEAM	ARMORPOINT
Daily monitoring, investigation, and response	Primary	Provides platform
Detection tuning and workflow design	Primary	Tooling/Guidance
Platform operations, pipelines, and updates	Visibility	Primary
Support and optional services	Choose what to layer	Delivers

EDR INTEGRATIONS

SentinelOne · CROWDSTRIKE · cybereason · Microsoft Defender for Endpoint

WHEN TO CHOOSE XDR

- → You have in-house analysts and want detection, investigation, and response to stay on your team
- → Your team is switching between consoles to trace a single attack
- → Point tools cost more than they return once you count licensing and upkeep
- → You want the platform now, with the option to add MDR or MXDR later

WHY ARMORPOINT

One platform, one workflow, and one security operation under your control.

Your team stays in control while ArmorPoint provides the technology trusted by our own 24/7 SOC. As your needs evolve, you can add MDR or MXDR on the same platform, without replatforming.

Talk to a Security Engineer armorpoint.com/services/xdr

SC Awards EXCELLENCE AWARD WINNER 2026 · CYBERSECURITY STARS AWARDS WINNER 2026 The Hacker News · MES computing MES MIDMARKET 100 2026