SOLUTION BRIEF

Endpoint Detection and Response.

Remediate Threats Before They Become Breaches.

ArmorPoint's Endpoint Threat Detection and Response solutions enable rapid threat detection and remediation by consolidating all relevant attack data into a user-friendly, interactive interface. Our platform displays the complete timeline of an attack, tracks the spread of malware across processes and users, and includes all associated communications, allowing for faster and more effective detection, response, and remediation of threats.

EDR can help reduce serious security incidents *by up to 50%*

CORE OUTCOMES

- Monitor endpoints continuously to detect suspicious activities and potential threats instantly
- Achieve complete visibility with integrated remediation tools
- Detect anomalous behavior and identify security breaches in real-time, moving away from reliance on periodic scans
- Reduce response times and limit the spread of threats within the network with automated response capabilities
- Rely on our team of experts to enhance your threat detection and response capabilities
- Build and Utilize detection rules across Windows, macOS, and Linux platforms
- Minimize downtime, data loss, and the financial impacts from security breaches

armorpoint.com sales@armorpoint.com

How it Works.

STEP 1	**SCOPING & PREPARATION**	→ Deploy the ArmorPoint EDR agent on endpoints such as desktops, laptops, servers. These agents analyze a wide range of data in real-time, including, running processes, active network connections, file and registry changes, user activities and behaviors, and system logs and events *Note: Any device without the EDR agent installed will not be protected.*
STEP 2	**BEHAVIORAL ANALYSIS AND THREAT DETECTION**	→ Utilizing advanced analytics, machine learning, and behavioral analysis, our EDR system sifts through vast amounts of data to identify patterns indicative of malicious activities. Our detection capabilities leverage anomaly detections, signature-based detections, and heuristic analysis to ensure comprehensive threat detection.
STEP 3	**ALERTING AND REPORTING**	→ Upon detection of a potential threat, our EDR generates immediate alerts and detailed reports. These alerts provide essential information, including the nature of the threat, affected endpoints, the timeline of detected activities, and recommended response actions, ensuring that your team can react promptly and effectively
STEP 4	**AUTOMATED RESPONSE**	→ Our EDR is equipped with automated response capabilities designed to contain and mitigate threats quickly. This includes isolating infected endpoints from the network, terminating malicious processes, and blocking or quarantining suspicious files, all while enforcing security policies and configurations to safeguard your network
STEP 5	**INVESTIGATION AND FORENSICS**	→ ArmorPoint's security analysts leverage our EDR platform to conduct thorough investigations. The platform provides powerful tools for root cause analysis, threat hunting, and event correlation, empowering our analysts to dive deep into security incidents and prevent future breaches

Alert Fatigue Ends Here. Start Remediating Threats Faster.

Transform raw endpoint data into actionable intelligence with ArmorPoint's EDR. Gain a comprehensive defense layer that includes advanced threat detection, swift response capabilities, and extensive monitoring. Enhance your organization's security posture to effectively protect, respond, and recover from cyber threats.

Ready to actively protect your endpoints? Schedule a consultation to talk to one of ArmorPoint's Solution Experts about how our Endpoint Threat Detection and Response can start enhancing your security operations today.

armorpoint.com sales@armorpoint.com