KEYPOINT INTELLIGENCE

MANAGED DETECTION AND RESPONSE AS A SERVICE

People, Process, and Technology for an Effective Security Program

KEYPOINT INTELLIGENCE
80 Little Falls Road
Fairfield, NJ 07004
TEL: +1 973 797 2100
keypointintelligence.com

MANAGED DETECTION AND RESPONSE AS A SERVICE

PEOPLE, PROCESS, AND TECHNOLOGY FOR AN EFFECTIVE SECURITY PROGRAM

Everyone can be hacked. The difference is in the response.

6 HOURS

Average industry time between notification about critical incident and reaction.

36 HOURS

Average time for IT/ Security team to take a response action and remediate the threat.

50 DAYS

Attackers will stay undetected in your network, impacting your key assets, IP, code, brand, pricing.

WHAT IS MDR AS A SERVICE?

1. Acquire industry leading expertise to help drive detection and response. The level of competency and experience gained from investigating a range of incidents across different client environments results in a world- class MDR expert team. For a typical enterprise, finding, developing, and retaining this talent is not impossible, but it's often not affordable.

2. Become proactive rather than becoming the attacker's victim waiting to react. Being proactive means to always be vigilant. Detection and response teams fail because they can't escape the constant deluge of activities to which they have to react and respond. MDR as a Service is the way out for shifting in the direction of a proactive security approach.

3. Sharing responsibility with your internal security team. Even when an organization has a detection and response team in place, deciding what to prioritize is a challenge. For example, the internal team may focus on external threats but hand off insider threat incidents to an outside firm performing MDR.

Keypoint Intelligence takes your existing tools, tunes them to maximum, and automates response to minimize reaction time and better protect your business.

ACS
agile cybersecurity solutions

Keypoint Intelligence Partner Team

Examples of Customer Tools

splunk> elastic Azure Sentinel LogRhythm CROWDSTRIKE chronicle Radar ACCEDIAN SentinelOne

Managed Detection and Response

The Most cost-effective service

WHY MANAGED DETECTION AND RESPONSE AS A SERVICE?

When business-critical assets are at risk in today's digital economy, protecting those assets must be of the utmost priority. Increasingly, compliance and regulatory entities require logging and security monitoring be in place.

It's no secret that there is a scarcity of skilled cybersecurity professionals, approximately a half a million according to the FBI, which has generated a significant challenge for CIOs and CISOs to identify, hire, and retain top talent to protect their digital landscape.

To build internal Security Monitoring today, business owners need to make large CAPEX investments and most CFO and CEOs prefer predictable Operational expenses. In-house SOCs are typically very expensive and overloaded, engineers are burning out from boring routine, and 24x7 coverage is a struggle to gain full visibility of attacks and policy violation inside the network.

Keypoint Intelligence MDR as a Service

Keypoint Intelligence provides a tailor-made approach to predict, prevent, detect, and respond to malicious activity. MDR as a Service is a perfect choice for proactive companies who want to strengthen their security postures and remain a step ahead of the cybercriminals.

- Recapture value from your cybersecurity tool investments
- Help make your tools work more effectively
- Automated response allows you to react to incidents in minutes, not hours
- Your environment is monitored 24x7 and you will receive notifications about confirmed threats and anomalies

THREE LEVELS TO CHOOSE FROM

	STANDARD	ENHANCED	PROFESSIONAL
Detection Only Endpoint Protection Solution - SentinelOne Control	X	X	X
24x7 Monitoring, Notifications & Response to Endpoint Incidents	X	X	X
Self-provisioned deployment in hours, not days	X	X	X
Handle multi-step investigations: trace activities associated with compromised systems	X	X	X
24x7 Alert triage performed by analysts and apply the MITRE & Kill-chain methodology to see the attack lifecycle	X	X	X
Direct Chat with our analysts in 24x7 mode	X	X	X
Detailed Remediation Guidance	X	X	X
Scheduled Automated Reports	X	X	X
Multi-channel Alerting (e.g. via SMS, Calls, Slack or Email)	X	X	X
Activity reporting and data retention	X	X	X
Office 365 / Google Workspace Email Threats		X	X
Proactive Threat Hunting		X	X
Advanced Metrics, Reporting and Summaries for Compliance		X	X
Dedicated Customer Engagement Manager		X	X
Vulnerability Scanners Logs Integration (e.g. Nessus)		X	X
Containment and Remediation		X	X
Resilience Recommendations		X	X
Employees and domain passwords leaks monitoring in Darknet		X	X
Co-Managing your SIEM			X
(Splunk, Elastic, Azure, Sumo Logic, LogRythm, IBM QRadar, ArcSight, etc.)			X
Top 20 Pre-Defined Reports for PCI, HIPAA and CIS			X
Keypoint Intelligence library with 1500+ detection rules			X
Cloud Security Monitoring: AWS/Azure/GCP Log Trail & API Integration			X
Tuning your security tools to improve visibility			X
Malware Analysis			X
Custom Reporting			X
Customer portal access via War Room			X
Manual Remote response with customer IT (40 hours/year)			X
Automated Response Integration with Customer Tools			X
SOAR as a Service to decrease time to Respond and Automate IR			X
Integration with Ticket/Incident Management systems (ConnectWise, ServiceNow, Jira)			X


KEYPOINT
INTELLIGENCE
keypointintelligence.com