deepwatch™

Next-Generation Managed Endpoint Detection and Response (NG-MEDR)

Deepwatch holistic security operations and the advanced CrowdStrike Falcon Platform offer next-generation endpoint protection and effective security operations.

KEY CHALLENGES ADDRESSED BY NG-MEDR

Comprehensive Visibility: Organizations need more visibility into their endpoint information and NG-MEDR provides detailed insights and monitoring capabilities to ensure no endpoint is left exposed.

Advanced Malware and Ransomware Protection: Insufficientprotection against sophisticated malware and ransomware attacks is a common issue. NG-MEDR integrates cutting-edge threat intelligence to defend against these threats.

Extensive Telemetry Data Collection: Detecting attacks requires extensive telemetry data collection, which NG-MEDR captures and analyzes vast amounts of data to identify and mitigate these advancing threats.

Effective Attack Response: Enterprises often face difficulties in analyzing, isolating, remediating, and responding to attacks on endpoints, servers, and virtual machines (VMs). NG-MEDR streamlines these processes, ensuring rapid and effective responses.

Efficient Endpoint Protection Management: Managing the planning, deployment, operations, tuning, automation, and updates of endpoint protection platforms (EPP) and agents across diverse environments can be challenging. NG-MEDR simplifies and automates these tasks, enhancing operational efficiency.

Cybersecurity Skills Gap: A shortage of cybersecurity expertise is a critical issue for many organizations. NG-MEDR offers expert event triage and leverages Deepwatch Experts' extensive experience to bridge this gap.

ENDPOINT PROTECTION FOR CYBER RESILIENCE

Enhanced Endpoint Insights: NG-MEDR provides deep insights through extensive log gathering via SIEM systems for comprehensive visibility and analysis.

Higher Fidelity Signals: Using XDR principles, NG-MEDR ensures precise threat detection with high-fidelity EDR signals from endpoints.

Augmented Data Telemetry: We enhance EDR data with additional log telemetry from firewalls, IDS/IPS, IPAM, and other sources for a more complete security picture.

Contextual Enrichment: NG-MEDR enriches detections with log data, reducing triage time, false positives, and accelerating MTTR for faster response.

Key Benefits

NG-MEDR delivers exceptional value through its proactive and responsive capabilities:

Rapid Threat Prevention and Analysis:

- ✓ **Prevention:** Action within <1 minute
- ✓ **Analysis:** Analysis within <60 minutes

Swift Response Times:

- ✓ **Initial Response:** Response within <10 minutes for critical alerts
- ✓ **Full Analysis:** Complete analysis within <60 minutes for critical alerts

Integrated Platform:

- ✓ Enhances enrichment, correlation, intelligence, and hyperautomation
- ✓ Ensures a coordinated response with clear roles and responsibilities

Continuous Optimization:

- ✓ Regular health and tuning recommendations

MEDR	NG-MEDR
Stand-alone Solution - MEDR Only	Holistic Solution - MDR + MEDR
Limited Scope to Endpoints alerts and telemetry	Holistic visibility to multiple telemetry and event sources
Response actions based only on endpoint data	Response actions from a range of trusted sources
Limited conditions for response actions	Flexible response actions based on expert guidance and environment conditions
Response actions API-based only	Matured endpoint program that knows automation and API connections work
	Certified human experts can verify and extend response actions