Cyber Solutions Products

First Watch Technologies Managed Detection and Response* (MDR) Service, provides 24/7 threat detection, monitoring, alerting, threat hunting, and remediation. Our service is powered by SentinelOne® a cloud-based platform, we prioritize threats over false positives. First Watch incident responders have uniquely crafted proprietary behavior-based detections to elevate your security posture.

WHAT'S INCLUDED?	MxDR	MDR Pro	MDR
Next Generation Anti-virus (EPP) • Built-in Static AI and Behavioral AI Analysis, Firewall: with location awareness and network connectivity controls • Device Control for USB and Bluethooth Devices	✓	✓	✓
Managed Threat Detection and Response • Customized configuration and setup EPP unique to the environment • Review all detections to determine if false positive or an actual threat • Manage EPP to include remediation, malware analysis of threats and adding exclusions	✓	✓	✓
24x7 Threat Monitoring Detections & Response • Every console threat is reviewed, acted upon, and documented • Full response capabilities • Automated threat response including remediation	✓	✓	✓
Rapid Response & Remediation • Ransomware Rollback • Leverage AI to detect and respond to active threats • Detect threats across entire attack surface	✓	✓	✓
Active Threat Hunting • Active hunting & tracking of attacker techniques, global APT campaigns, and emerging cyber crimes • Alerting and remediation when threats are detected in your environment	✓	✓	✓
Proprietary Behavior Based Detections • Behavior based detections based on MITRE ATT&CK framework (Techniques, Tatics & Procedures) TTPs • Tuning of customer's enironment	✓	✓	✓
Unlimited Incident Response Investigations • Full Incident Response • Root Cause Analysis (RCA) to include Initial Infection Vector (IIV) and exfil/breach determination	✓	✓	✓
Slack Channel • Collaboration between customer and First Watch cyber analysts • Communication channel for customer and First Watch MDR team • Assigned customer advisor	✓	✓	
Squad Model • Dedicated team of experienced cyber analysts • Dedicated project manager • Quarterly threat landscape reviews	✓	✓	
Managed Extended Detection & Response (MxDR) • Cloud based SIEM (Devo) • Correlation of endpoint and network traffic • Log source ingestion: Email, Firewall and Proxy Logs	✓		

COWBELL RX PRICING FOR FIRST WATCH CYBER SOLUTIONS PRODUCTS

MxDR: $15.25 per log source per endpoint per month.	Billed Annually.	Requires the purchase of MDR Pro. Includes 1 log source. $3.00 per additional log source per endpoint per month. Services start as low as 10 endpoints.
MDR Pro: $12.25 per endpoint per month.	Billed Annually.	Services start as low as 10 endpoints.
MDR: $10.75 per endpoint per month.	Billed Annually.	Services start as low as 10 endpoints.

First Watch Technologies, Inc. uses Devo, a cloud based SIEM to deliver full MxDR capabilities.