

Competitive Analysis:

Cynet 360 AutoXDR™ vs. Cybereason

Companies today are turning to Cynet 360 and newer Extended Detection and Response (XDR) solutions that provide expanded visibility across the environment, detecting and preventing endpoint, network, user and cloud-based threats on a single platform. Cynet also provides extended automated response capabilities to greatly reduce the burden on your security team and ensure threats are quickly and properly addressed before damage can be done.

Cynet has many advantages over Cybereason, especially for companies that prefer broad XDR capabilities such as user behavior analytics, network detection and response, deception, CSPM, SSPM, and centralized log management. Cybereason performs well as an EDR but comes with a premium pricetag.

Top reasons to choose Cynet over Cybereason



Visibility across endpoints, users, network and cloud

Cynet 360 gathers and analyzes threat data from multiple layers, providing a fuller picture of potential security incidents.



Visibility across...endpoints

Cybereason Ultimate provides adequate visibility into file/process-based threats, such as malware, exploits, etc. However, there's no view into network or user-based threats.

Robust security controls

Cynet 360 amplifies your security with capabilities that include user behavior analytics, deception technology and CSPM.



The usual features

Cybereason Ultimate provides security capabilities that are typical for EDR tools.

Highly rated, highly affordable


Cynet is consistently ranked by small to medium enterprises as [one of the best XDR solutions](#) and comes at an affordable price point, reducing your security TCO.



Mediocre user ratings, higher pricing

Cybereason Ultimate customers pay a premium price for an [average](#) solution.

Cynet 360 AutoXDR vs. Cybereason Comparison Table

		
Detection & Prevention		
Multilayered malware protection		
Signature based	✓	✓
ML based static analysis	✓	✓
Dynamic analysis (sandbox)	✓	✓
Compromised user account detection		
Anomalous user logins	✓	✗
Preset user activity rules	✓	✗
Malicious Network traffic		
Tunneling based data exfiltration	✓	✗
Credential theft (LLNMR\NBT-NS attacks)	✓	✗
Lateral movement (pass the hash etc.)	✓	✗
Reconnaissance (scanning attacks)	✓	✗
Deception		
Decoys: Data Files, Credentials, Network Shares, URL, RDP	✓	✗

Response		
Host Remediation	Isolate, Restart, Change IP, Delete/Disable Service, Delete/Disable Scheduled Task, Run Command, Run Script	Isolate, Run Command, RunScript.
User Remediation	Disable/Enable, Reset Password	✗
Network Remediation	Block Traffic, Clear DNS Cache	✗
Orchestration		
Expand Remediation Across the Environment Infrastructure: Firewall, Proxy, AD, etc.	✓	✗
Automation		
Chain Discreet Remediation Actions to a Single Flow that Runs Automatically when a Predefined Alert is Triggered	✓	✗

Managed Detection & Response Services

Full MDR Integrated in the Product Offering



Monitoring & Control

Vulnerability Management



Inventory Management



Risk Reporting



File Integrity Monitoring

