Competitive Analysis:

Cynet 360 AutoXDR™ VS Cylance

Cynet 360 AutoXDR™ Difference

Detailed Explanation

Attack Prevention & Detection

Malicious activity manifests itself in one of three ways: file/process execution, network traffic and user behavior. Cylance is oriented on file/process-based threats and typically gain good results on that field. Cylance relies solely on AI-based static analysis capabilities to detect and prevent attacks. While this approach is efficient against malicious files, it offers little protection against fileless, Macros and LOLbin threats. Moreover, researchers have demonstrated that AI-based analysis approaches can be bypassed by identifying the biases inherent in the detection algorithms toward certain benign files to trick the product into accepting malicious files (see here).

Users of AI-based static analysis report that it is prone to false positives and often blocks legitimate software as malicious. To overcome the false positives, IT and security teams must invest heavily in whitelisting and exclusion of organizational software and other legitimate apps.

Cylance also lacks the ability to identify and block attacks that manifest only in anomalous network traffic (lateral movement, data exfiltration and network-based credential theft) or user behavior (anomalous login of compromised user account).

Cynet 360 AutoXDR™ uses Cynet Sensor Fusion™ technology to continuously collect and analyze endpoint, user and network activities within the protected environment, powering the ability to identify and block file/process-based attacks, as well network and user-based attacks, rendering complete coverage beyond the capabilities of Cylance. Cynet 360 AutoXDR™ also provides deception technologies to help expose threats across your environment.

Moreover, by fusing together all the environment activity signals, Cynet 360 AutoXDR™ is able to uncover the true context of each process execution, network traffic and user behavior to unveil and block threats that are undetectable by monitoring just file/processes as Cylance does. Cynet 360 AutoXDR™ successfully blocks the execution of processes that Cylance allows to run.

Response

Coverage

Advanced cyberattacks leave their mark across all parts of the targeted environment: endpoints, files, process, user accounts and network traffic.

Cylance has a limited number of endpoint/file remediations (isolate, kill process and delete/quarantine file), limited host remediations and no network or user remediation capabilities. Cynet provides a complete set of remediation tools for infected endpoints, malicious files/ processes, compromised user accounts and attacker-controlled traffic. Moreover, Cynet 360 AutoXDR™ can act as a response orchestration interface that communicates with core components such as Firewalls and Active Directory to expand the response process across the entire environment.

Automation

Cynet 360 AutoXDR™ supports the use of preset and user-created created remediation playbooks that automate response for detected threats by chaining together several discreet remediation actions (for example, isolate the endpoint + disable user account in Active Directory as an automated response user account compromise detection). These playbooks both scale the security team alert-handling capacity by automating repetitive tasks and radically increase the share of attacks that are autonomously addressed and resolved by Cynet 360 AutoXDR™ without need of human intervention.

Monitoring & Control

Continuous monitoring of all entities and activities in the environment enables users to discover exposed attack surfaces and address them (vulnerable systems and apps, unchanged user passwords, etc.), thereby eliminating the risk of up to 60% of common attack vectors.

Cynet 360 AutoXDR™ uses Cynet Sensor Fusion™ technology to automate the collection and correlation of executed file/processes, user account activities, file access and network traffic, introducing unmatched speed and ease to all monitoring and control workflows.

Cynet includes 24x7 Managed Detection and Response (MDR) services to all clients that continuously monitor clients' environments, providing best-of-breed detection and response services. Cylance offers MDR services, CylanceGUARD, but as an optional, fee-based service.

Cynet 360 AutoXDR™ VS Cylance Comparison Table

Prevention & Detection

Multilayered Malware Protection

Behavioral Analysis	✓	✗
Dynamic Analysis (Sandbox)	✓	✗

Compromised User Account Detection

Anomalous User Logins	✓	✗
Preset User Activity Rules	✓	✗
Malicious Insider	✓	✗

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

Remediation

Host Remediation	Isolate, Restart, Change IP, Delete\ Disable Service, Delete\Disable Scheduled Task, Run Command, Run Script	Isolate, Run Command, Run Script
User Remediation		
Network Remediation		

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