Competitive Analysis:

Cynet 360 AutoXDR™ vs. Trend Micro Vision One + Apex One

Top reasons to choose Cynet over Trend Micro

cynet		TREND MICRO
Designed for lean security teams Cynet 360 reduces the burden on security teams by streamlining security operations and automating investigation and remediation processes.	VS	**Designed for large teams...and large budgets** Full protection from Trend Micro Vision One requires multiple products and licenses, increasing complexity and overall TCO.
Visibility across multiple layers Cynet provides intuitive visibility across endpoints, user, cloud and network-based threats.	VS	**You can't protect what you can't see** Trend Micro does not provide visibility into user-based threats, while visibility into network-based threats requires a separate license.
Optimized and automated Fully automated remediation for infected hosts, compromised user accounts, and attacker-controlled network traffic.	VS	**Minimal automation** Limited automation to a subset of host and file threats.

Cynet 360 AutoXDR™ Difference

Detailed Explanation

Attack Detection & Prevention

Trend Micro Vision One + Apex One provides on-prem, virtual and cloud workloads with advanced endpoint prevention and detection of file/process based attacks (malware, exploits, etc.). However, Trend Micro Deep Security lacks the ability to identify and block attacks that manifests 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 continuously collects and analyzes endpoint, user and network activities within the protected environment, powering the ability to identify and block both file/process-based attacks, as well network and user based ones, rendering complete coverage beyond the capabilities of Trend Micro Vision One + Apex One. Cynet AutoXDR can be deployed on all workloads, regardless if they are physical or virtual, on-prem or in the cloud.

Moreover, by fusing together all the environment activity signals, Cynet AutoXDR is able to form 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 Trend Micro Vision One + Apex One does. In that way, Cynet would successfully block the execution of processes that Trend Micro Vision One + Apex One would allow to run.

Response

Coverage

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

Unlike Trend Micro Vision One + Apex One that has a limited number of endpoints/file remediations (isolate, kill process and delete/quarantine file), Cynet AutoXDR provides a complete set of remediation tools for infected endpoints, malicious files/processes, compromised user accounts and attacker-controlled traffic. Moreover, Cynet 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 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 AutoXDR without need of human intervention.

Monitoring & Control

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

Cynet AutoXDR automates 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 360 AutoXDR vs. Trend Micro Vision One + Apex One Comparison

	cynet	TREND MICRO
Detection & Prevention		
Multilayered Malware Protection		
Signature Based	✓	✓
ML Based Static Analysis	✓	✓
Dynamic Analysis (Sandbox)	✓	Sold separately
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)	✓	Sold separately
Deception		
Decoys: Data Files, Credentials, Network Shares, URL, RDP	✓	✗

	cynet	TREND MICRO
Response		
Remediation		
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	Full MDR included with Cynet Elite and Ultimate	Sold separately
Monitoring & Control		
Vulnerability Management	✓	✓
Inventory Reports	✓	✗
File Integrity Monitoring	✓	✓