Competitive Analysis:

Cynet vs. VMware Carbon Black

Last update: February 2023

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

Cynet 360 AutoXDR has many advantages over VMware Carbon Black Endpoint, especially for companies with lean security teams that can't afford the time required to leverage many focused solutions that cater to very large corporations. VMware Carbon Black Endpoint is designed to be used by a large team of expert users that are looking for copious data and highly customizable configuration options. This approach, however, is overwhelming for leaner security teams that do not have the bandwidth to appropriately support the tool. A highly complex and time-consuming configuration, and minimal automatic remediation are just some of the issues with VMware Carbon Black Endpoint.

Top reasons to choose Cynet over VMware Carbon Black

cynet		vmware Carbon Black
Designed for efficiency Cynet 360 AutoXDR automatically collects and correlates alerts and related data to identify suspicious or problematic activity, all presented on a streamlined dashboard.	VS	**Designed for large teams** VMware Carbon Black is a complex product that requires significant fine-tuning, best suited for the large enterprises that use it.
Elite protection against today's threats Cynet detected 107 of the 109 MITRE ATT&CK techniques (98.5%), scoring the 3rd highest result across all vendors.	VS	**Average protection** VMware Carbon Black only detected 90 of the 109 MITRE ATT&CK techniques (82.5%), leaving customers significantly exposed.
Highly rated, highly affordable Cynet 360 is consistently ranked by users as one of the easiest to use XDRs and comes at an affordable price point, reducing your security TCO.	VS	**Premium pricing** VMware Carbon Black achieves average user ratings and comes with a premium price tag, driving up your security TCO.

Cynet 360 AutoXDR Difference

Detailed Explanation

Attack Detection & Prevention Detailed Explanation

VMware Carbon Black Endpoint is a traditional endpoint solution that focused on file/process-based threats: malware, exploits, fileless, macros etc., and typically achieves good results in that context. However, it 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 VMware Carbon Black.

Response

Coverage

Advanced cyberattacks target all parts of the environment: endpoints, files, process, user accounts and network traffic.

Unlike VMware Carbon Black Endpoint, which has a limited number of endpoints/file remediations (isolate, kill process and delete/quarantine file), 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 response automation with both provided and user created remediation playbooks that chain together discreet remediation actions to a single flow. These playbooks enable the security team to radically scale their capacity by automating repetitive tasks, increasing the share of attacks that are addressed and resolved by Cynet 360 AutoXDR without need of human intervention.

Managed Detection and Response (MDR)

Cynet's CyOps team operates a 24/7 SOC, providing Cynet Elite and Ultimate customers with full MDR services. CyOps continuously monitors, trains and optimizes Cynet 360 AutoXDR detection algorithms based on over 30 threat intelligence feeds and detected attacks.

CyOps provides customers with the additional services:

- Alert monitoring
- Attack investigation
- Threat hunting
- Remediation guidance
- Exclusions, whitelisting and system fine tuning

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 360 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. VMware Carbon Black Endpoint Comparison

	cynet	vmware
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)	✓	✓

	cynet	vmware
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	✓	✗

	cynet	vmware
Infrastructure		
Number of Agents	1	1
Agent impact on endpoint performance		
Clashes with existing software, manual exclusions, blue screens	Lightweight agent with minimal to zero impact	Three separately developed agents pieced together
Deployment model	Flexible: on-prem, SaaS or Hybrid	On-Prem, SaaS
Self-distributing agent		
Auto-deployment on newly joined endpoints without need of manual configuration