

Competitive Analysis: Cynet vs. CrowdStrike

Last update: February 2023

Companies today are turning to Cynet and newer Extended Detection and Response (XDR) solutions that provide expanded visibility across your 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 CrowdStrike Falcon, 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. CrowdStrike Falcon EDR 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, limited remediation capabilities along with easily bypassed endpoint agents are just some of the issues with CrowdStrike.

Top reasons to choose Cynet over CrowdStrike



Designed for lean security teams

Cynet 360 reduces the burden on security teams by streamlining security operations and automating investigation and remediation processes.



Robust security features, out of the box

Cynet 360 provides features like customizable remediation playbooks along with network and user deception files.



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.



Designed for large teams

CrowdStrike Falcon provides copious data and command-line tools, best suited for large teams of expert users, not teams with limited bandwidth.

Limited features, sold separately

A separate license with a ticketing tool is required to add customizable remediation; network deception and user deception are not available.

Priced at a premium

CrowdStrike achieves above average user ratings but that comes at a premium price.

Visibility is Key to Threat Protection

You can't protect what you can't see. Effective protection requires visibility beyond the endpoint.

We're Expansive

Cynet delivers visibility into endpoint, user and network-based threats. And we leverage deception technology.



They're Narrow

The comparable CrowdStrike package covers endpoint and user-based threats, but limited visibility into network-based threats.

We're A Solution

If you want a solution that provides defense in depth out of the box, protecting against endpoint, user and network-based threats along with deception technology, Cynet's best of suite platform is for you.



They're a Component

If you can afford all the additional tools required for a full threat protection stack, you can use CrowdStrike Falcon as one of your stack components.

Simplicity Is Complexity Resolved

Many security tools require a steep learning curve and significant ongoing support. Tools that are "overly configurable" often mire users in unnecessary, yet time consuming details. Security tools should be easy to learn, intuitive to set up and operate, and accessible by anyone on the security team.

We're Intuitive

If you have a lean security team that wants to focus on what's important, Cynet XDR requires a very short learning curve to learn, configure and operate. You'll be up and going in days.



They're Confusing

CrowdStrike requires a high level of expertise to learn and operate - if you have the resources and time to figure it all out. Tuning all the settings in CrowdStrike Falcon can take months.

We Leverage Rules and ML

Configuring Cynet is easy. You start with best practice settings and can leverage our included MDR service for any questions or advice to tune the platform for your unique environment.



They're Strictly ML

CrowdStrike requires lots of trial and error to hone in on configuration settings that aren't too strict or too lenient. Too strict and everything gets blocked. Too lenient and you open yourself up to risk.

Automation Streamlines Operations and Improves Security

Not every company has a large bench of security experts. To be effective, cybersecurity solutions must be useable, intuitive and preferably automated.

We Eliminate Threats

Cynet provides a wide array of automated remediation actions across files, hosts, users and networks, including pre-built and customizable remediation playbooks to fully resolve attacks without the need of human intervention.



They Leave Malicious Files

CrowdStrike has scanless security which identifies and blocks malicious files – but automatic, multi-action remediation requires an add-on. These unattended threats are at risk to execute under certain circumstances.

We Provide the Whole Story

Cynet's Incident Engine provides automated attack investigation and reconstruction including root cause analysis and attack scope determination.



They Provide a Snippet

CrowdStrike provides some telemetry correlation for a security analyst to then manually investigate and reconstruct an attack. Automated attack investigation is available as an add-on.

A Security Tool Must Protect Itself

The easiest way for attackers to bypass security controls is to simply disable them. It's critical that security tools have strong self-protection capabilities to avoid.

We Persist

Cynet actively and fully protects its agent from being terminated or manipulated. Alarms are useless if criminals can just turn them off.



They Perish

The CrowdStrike endpoint sensor is far too easy to disable - leaving the endpoint and your entire environment vulnerable to attackers.

Independent Testing Is More Trustworthy Than Vendor Claims

The MITRE ATT&CK evaluation provides open, unbiased testing of leading EDR solutions against simulated attack scenarios. Results can be used to understand vendors' capabilities.

We Detect More and Better

For the second year in a row, Cynet XDR detected more attack techniques than CrowdStrike, 98.2% vs. 94.4% in the 2022 evaluation.

vs

Their Detection Was Subpar

CrowdStrike also scored lower than Cynet in preventing attacks before any further infiltration (sub-steps) could take place in the test environment (84% vs. Cynet's 88%).

We Detected 100% of Linux Attacks

In the 2021 Evaluation, Cynet achieved a 100% detection rate for the threat techniques attempted on Linux machines, prevented every attack presented, and provided full information on every technique attempted.

vs

They Provided 16.7% Coverage for Linux

CrowdStrike's missed most Linux attack steps, only detecting 16.7%, meaning you should think twice if you have Linux machines in your environment.

We Are Leaders in Visibility

Cynet leveraged 15 different data sources for detecting threats, the highest number achieved in the 2021 MITRE ATT&CK evaluation. The more data sources, the broader the visibility and the more accurate the detection.

vs

Their Visibility was Middle of the Pack

CrowdStrike leveraged 50% less data sources than Cynet (10 vs. 15), meaning less visibility when detecting common attack vectors and less context to help analysts investigate alerts.

No Nickel and Diming

Many security platform providers offer a highly complex pricing structure that aims to reap revenue from a variety of platform and service configurations and add-ons. Most clients, understandably, prefer simplicity and openness.

Our MDR is a Help Center

Cynet Elite and Ultimate packages include a full 24x7 MDR service that continuously monitors all client environments, providing best-of-breed detection and response services – *at no extra cost*.



Their MDR is a Profit Center

CrowdStrike provides an optional MDR service (called Falcon Complete) at a very steep premium, putting it well out of reach for most mid-sized enterprises.

We Have One Solution for One Price

As a Cynet Elite or Ultimate client, you get everything we offer, including a full MDR service, at one price. Simple.



They Profit from Required Add-Ons

In addition to Falcon Premium, you need to add in Falcon X, Falcon Device Control, Falcon Overwatch and CrowdStrike Services and you still won't get all the capabilities Cynet provides out of the box. Way more complexity and way more cost.

We Focus on Companies Outside of the Fortune 500



Most companies prefer solutions like Cynet that are intuitive, easy to use and highly automated to reduce the burden on the company's limited resources at an affordable price point.



They Focus on Very Large Enterprises



Very large enterprises can afford the cost to acquire and the time to operate multiple, expensive solutions such as CrowdStrike that provide reams of raw data and require highly customized integration and configuration.

Business Differentiators



Capability	Explanation	 cynet	 CROWDSTRIKE
Autonomous Protection and Response	Automating the manual process of protecting against and remediating threats	✓ Simple, light, intuitive platform build for lean security teams	✗ Intuitive platform with extensive settings meant to be customized and leveraged by expert security teams
Alerts and Context	Accurate alerting that helps identify true threats while mitigating against alert fatigue	✓ Accurate alerts with strong correlation, risk scores for alert prioritization, clean UI	✓ Accurate alerts with strong correlation, risk scores for alert prioritization, clean UI
Automation	Automated capabilities that reduce the burden on lean security teams	✓ Broad set of automated capabilities to minimize manual intervention	✗ Commmands to support manual intervention

Feature Differentiators



Threat Prevention and Detection

Capability	Explanation	 cynet	 CROWDSTRIKE
Endpoint Prevention and Detection	Multilayer malware protection and detection, including static and behavioral AI to detect exploits, malicious scripts and fileless attacks	✓ Full set of features	✗ Full set of features - however malicious files are left on infected host
Compromised User Account Detection	Detect anomalous user behaviors that may be indicative of account takeover or a malicious insider threat	✓ Full set of features	✗ Not available
Malicious Network Activity Detection	Detect malicious network behaviors such as reconnaissance scanning, DNS and ICMP tunneling, lateral movement and responder attacks	✓ Full set of features	✗ Not available
Deception technology	Lure attackers to reveal their presence using multiple types of decoys, including fake files, hosts, users and networks	✓ Full set of features	✗ Not available
Device Control	Protect against data loss and the introduction of malware by allowing only trusted removable devices	✓ Full set of features	✗ Available as add-on
Threat Hunting	Proactively search for threats across the organization	✓ Full set of features	✗ Available as add on
Security Policy Features	Define and enforce security policies around device control, network control, blacklists, exclusions, etc.	✓ Full set of features	✓ Full set of features

Investigation and Response

Capability	Explanation	 cynet	 CROWDSTRIKE
Incident Engine	Automatically determine root cause and scope of an attack across the environment and apply all necessary remediation actions	✓ Cynet's Incident Engine provides automated attack investigation and reconstruction including root cause analysis and attack scop determination	✗ Automated attack investigation
Remediation Playbooks	Automatically implement a predefined sequence of remediation actions across the environment in response specific threats	✓ Comprehensive set of pre-build playbooks and an intuitive playbook builder to create custom playbooks	✓ Pre-built and customized playbooks
Forensics	Forensic dashboard for investigation, threat hunting and integrated threat intelligence	✓ Intuitive interfac with prebuilt queries, visualization and advanced searchcapabilities	✓ Intuitive interface with prebuilt queries, visualization and advanced search capabilities.
Managed Detection and Response (MDR) Service	24x7 monitoring, investigation, on-demand analysis, incident response and threat hunting	✓ Full MDR included with Cynet Elite and Ultimate	✗ Additional cost with tiered pricing for service diferent MDR service levels

Architecture

Capability	 cynet	 CROWDSTRIKE
Supported Operating Systems	✓ Windows, Mac, Linux	✓ Windows, Mac, Linux
Deployment	✓ Cloud, On Prem, Hybrid	✗ Cloud
Agent	✓ Automatic self-distributing agent, auto deployment on new endpoints	✗ Manual download or create scripts for third-party deployment tools for automated installation
Agent resources	✓ Lightweight agent with minimal performance overhead	✓ Lightweight agent with minimal performance overhead
Mutli-tenancy	✓ Full muti-tenant architecture	✓ Full muti-tenant architecture
Console UX	✓ Attractive and highly functional	✓ Attractive and functional
Agent Protection	✓ Agent Self-Protection/Anti Tamper	✗ Poor. Very easy to disable
RBAC Support	✓ Full RBAC	✓ Full RBAC

* Comparison of Cynet 360 Ultimate vs. the closest matching package, CrowdStrike Falcon Elite.

Cynet enables any organization to put its cybersecurity on autopilot, streamlining and automating their entire security operations while providing enhanced levels of visibility and protection, regardless of the security team's size, skill or resources and without the need for a multi-product security stack.

It does so by:

- Natively consolidating the essential security technologies (including EPP, EDR, Deception, Network Analytics and more) needed to provide organizations with comprehensive threat protection into a single easy-to-use XDR platform.
- Automating the manual process of investigation and remediation across the environment.
- Providing a 24-7 proactive MDR service - monitoring, investigation, on-demand analysis, incident response and threat hunting - at an affordable price.

Cynet Key Differentiators

XDR - 360 attack detection and prevention

Cynet provides attack detection, prevention and remediation against endpoint, network, and user-based attacks.

Response Automation

Automated investigation to unveil an attack's root cause and impact, coupled by automated remediation to eradicate all malicious presence and activity.

24x7 MDR services included

Cynet 360 Elite and Ultimate packages include access to a top skilled analyst team that provides alert monitoring, threat hunting, attack investigation and assistance with incident response.

Network Analytics and Deception Built-in

Cynet includes network analytics and deception technology to extend threat detection across your environment.

Lightspeed deployment and immediate value

Seamless distribution of thousands of agents within a single hour with immediate security benefits.

Operational simplicity

Single lightweight agent delivers all prevention, detection, and response automation capabilities, thereby reducing operational costs and effort.