Competitive Analysis:
Cynet vs. SentinelOne

Last update: March 2023

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 SentinelOne, especially for companies with lean security teams that can't afford the time required to leverage multiple focused solutions that cater to very large corporations. SentinelOne's solution is designed to be used by a large team of expert users that are looking for copious data and flexible search tools. This approach, however, is overwhelming for leaner security teams that do not have the bandwidth to appropriately support the tool. Reams of alert data, no alert prioritization, command-line forensic search, and manual machine-by-machine response are just the start.

Top reasons to choose Cynet over SentinelOne

cynet		SentinelOne
Designed for lean security teams		**Designed for large teams**
Cynet 360 reduces the burden on security teams by streamlining security operations and automating investigation and remediation processes.	VS	SentinelOne Singularity provides copious data and command-line tools, best suited for large teams of expert users, not teams with limited bandwidth.
Robust security features, out of the box		**Additional features sold separately**
Cynet 360 provides features like customizable remediation playbooks along with network and user deception files.	VS	Separate SentinelOne licenses are required to add customizable remediation, network deception and user deception.
Highly rated, highly affordable		**Priced at a premium**
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	SentinelOne achieves above average user ratings but that comes at a premium price, according to AWS Marketplace.

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.

VS

They're Narrow

The comparable SentinelOne package offers firewall management but limited visibility into network-based threats. Wider network coverage and deception technology both require additional licenses.

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.

VS

They're a Component

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

Nonstop Alerting Is Not the Answer

Most companies simply don't have the bandwidth to appropriately analyze every alert. Security tools musthelp their clients by reducing alert noise and clutter.

We Provide Clarity

If you have a lean security team that wants to focus on what's important, Cynet XDR leverages multiple streams of telemetry to accurately assess and prioritize threats.

VS

They Provide Clutter

SentinelOne provides an endless torrent of discreet endpoint alerts with no prioritization and little context – if you have the resources and time to figure it all out.

We Prioritize

Cynet alerts provide risk scores, rich context and accurate prioritization making it easy to focus on what's really important.

VS

They Flag

SentinelOne alerts provide simplistic malicious/ suspicious indicators, no scores and no prioritization –less clarity means more work for you.

Streamline Operations and Improve Security with Automation

Not every company has a large bench of security experts. Automated cybersecurity solutions allow your team to focus on important strategic initiatives.

We Reduce Burden

Cynet provides automated response workflows to relieve your overworked security team that may not have the bandwidth or expertise to fully investigate and respond to every alert.

VS

They Add Burden

If you want copious data and command-line tools so that your large team of experts can continuously investigate and prioritize alerts, SentinelOne is your ticket.

We're Automated

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.

VS

They're Manual

Many remediation actions require a considerable manual effort and customizable remediation is only available with SentinelOne's higher priced package.

We Provide the Whole Story

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

VS

They Provide a Snippet

SentinelOne's "Storyline" provides some telemetry correlation for a security analyst to then manually investigate and reconstruct an attack.

Cynet's Incident Engine automatically launches an investigation following certain high-risk alerts.

- First it traces back to understand how the discovered activity was generated to uncover the root cause of the attack.
- Then it searches to see if the same underlying malicious presence exists anywhere across your environment to uncover the full impact of the attack.
- Finally, it can automatically remove all components of the attack across your environment using built in remediation workflows or custom remediation playbooks.

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.

Their MDR is a Profit Center

At a list price of $66 per endpoint per year (according to AWS Marketplace), even a modestly sized MDR deployment is a windfall for SentinelOne and a very steep cost to pay for their clients.

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 to acquire multiple solutions such as SentinelOne that provide reams of raw data and require highly customized integration and configuration.

Business Differentiators

Capability	Explanation	cynet	SentinelOne
Autonomous Protection and Response	Automating the manual process of protecting against and remediating threats	✓ Simple, light, intuitive platform build for lean security teams	✓ Basic platform 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 poor corellation, no risk score for alert prioritization, cluttered UI
Consolidation	Multi-layered security that delivers protection across endpoints, networks and users	✓ Natively consolidated endpoint security, user behavior and network analytics, plus user and network deception technology	✗ Robust endpoint security and user behavior analytics but limited network analytics. Network and user deception available as add-ons.

Feature Differentiators

Threat Prevention and Detection

Capability	Explanation	cynet	SentinelOne
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
Compromised User Account Detection	Detect anomalous user behaviors that may be indicative of account takeover or a malicious insider threat.	✓ Full set of features	✗ Available as an add-on
Malicious Network Activity Detection	Detect malicious network behaviors such as reconaissance scanning, DNS and ICMP tunneling, lateral movement and responder attacks.	✓ Full set of features	✗ Lateral movement detection only
Deception technology	Lure attackers to reveal their presence using multiple types of decoys, including fake files, hosts, users and networks.	✓ Full set of features	✗ Available as an 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
Cloud Security Posture Management / SaaS Security Posture Management	CSPM and SSPM reduce the risk of cloud and SaaS configuration errors and oversights.	✓ Full set of features	✗ Not available
Centralized Log Management	CLM automatically collects the highest priority log data needed to quickly and accurately uncover threats across your environment	✓ Full set of features	✗ Available as an add-on

Investigation and Response

Capability	Explanation	cynet	SentinelOne
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	✗ "Storybook" provides some alert correlation which can be used for manual investigation
Customizable Remediation Playbooks	Automatically implement a predefined or customized sequence of remediation actions across the environment in response specific threats.	✓ Comprehensive set of pre-built playbooks and an intuitive playbook builder to create custom playbooks	✗ Customizable remediation is sold as an add-on feature
Forensics	Forensic dashboard for investigation, threat hunting and integrated threat intelligence.	✓ Powerful entity-based forensics to reveal rich information and activities associated with events.	✗ Basic searchable log forensics to create a global flat log of events.
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 packages	✗ Additional cost with tiered pricing for different MDR service levels

Architecture

Capability	cynet	SentinelOne
Supported Operating Systems	✓ Windows, Mac, Linux	✓ Windows, Mac, Linux
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	✗ Heavy agent with high/erratic memory consumption and high disk utilization
Mutli-tenancy	✓ Full muti-tenant architecture	✓ Full muti-tenant architecture
Console UX	✓ Attractive and highly functional	✓ Attractive, but needs extensive customization to be functional
RBAC Support	✓ Full RBAC	✓ Full RBAC
Agent Protection	✓ Agent Self-Protection/Anti Tamper	✓ Agent Self-Protection/Anti Tamper

* Comparison of Cynet 360 Ultimate vs. the closest matching package, SentinelOne Singularity Control.

Cynet enables any organization to put its cybersecurity on autopilotstreamlining 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 prevention and detection

Cynet provides attack prevention, detection 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.

Deception Security Built-in

Cynet is the only XDR vendor to include deception technology to lure attackers into revealing their presence.

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 efforts.