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

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

**Additional features sold separately**
Separate SentinelOne licenses are required to add customizable remediation, network deception and user deception.

**Priced at a premium**
SentinelOne achieves above average user ratings but that comes at a premium price, according to AWS Marketplace.
Nonstop Alerting Is Not the Answer

Most companies simply don’t have the bandwidth to appropriately analyze every alert. Security tools must help 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.

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.

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

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.

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.

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.

They Provide a Snippet
SentinelOne’s “Storyline” provides some telemetry correlation for a security analyst to then manually investigate and reconstruct an attack.

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 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.

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.

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’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.

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.

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

#### Threat Prevention and Detection

<table>
<thead>
<tr>
<th>Capability</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Endpoint Prevention and Detection</td>
<td>Multi-layer, multi-tier approach to prevent and detect threats, including anti-malware, anti-virus, anti-ransomware, anti-phishing, anti-malware.</td>
</tr>
<tr>
<td>Comprehensive User Account Management</td>
<td>Detect anomalous user behavior, including login attempts, failed logins, and remote logins.</td>
</tr>
<tr>
<td>Malicious Network Activity Detection</td>
<td>Detect malicious network activity, such as DNS requests, network reconnaissance, and ICMP tunneling, lateral movement, and reconnaissance scanning.</td>
</tr>
<tr>
<td>Forensics</td>
<td>The most detailed forensics and investigative environment, including real-time, incident investigation tools.</td>
</tr>
</tbody>
</table>

#### Investigation and Response

<table>
<thead>
<tr>
<th>Capability</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incident Engine</td>
<td>Real-time detection and threat hunting, including security events and incident investigation actions.</td>
</tr>
<tr>
<td>Customizable Prevention Playbooks</td>
<td>Automatically implement a playbook that is based on the threat and the environment, with or without an incident response.</td>
</tr>
<tr>
<td>Forensics</td>
<td>Time-based forensics tool, including real-time, incident investigation, and real-time logs.</td>
</tr>
</tbody>
</table>

#### Architecture

<table>
<thead>
<tr>
<th>Capability</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supporting Operating Systems</td>
<td>Windows, Mac, Linux</td>
</tr>
<tr>
<td>Agent</td>
<td>Automatic self-deployment, auto-deployment of new endpoints</td>
</tr>
<tr>
<td>Agent Resources</td>
<td>Light-weighted agent with minimal performance overhead</td>
</tr>
<tr>
<td>Multitenancy</td>
<td>Full multi-tenant architecture</td>
</tr>
<tr>
<td>Continuous (U)</td>
<td>Accessible and highly functional</td>
</tr>
<tr>
<td>RBAC Support</td>
<td>Role-based access control</td>
</tr>
<tr>
<td>Agent Protection</td>
<td>Agent Self-Protection/Host Sanitizer</td>
</tr>
</tbody>
</table>

* Comparison of Cynet 360 Ultimate vs. the closest matching package, SentinelOne Singularity Control.
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 prevention and detection**
Cynet provides attack prevention, detection and remediation against endpoint, network, and user-based attacks.

**Response Automation**
Automated investigation to unravel 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.