Companies today are turning to Cynet and newer Extended Detection and Response (XDR) solutions that provide expanded visibility across your environment, preventing and detecting 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 Sophos, especially for companies with lean security teams that can’t afford the time required to leverage a large set of focused solutions. Sophos Intercept X Advanced with EDR is designed to be used by a large team of expert users that are looking for a large volume of granular settings, options and capabilities which require many layers of configuration. This approach, however, is overwhelming for leaner security teams that do not have the bandwidth to appropriately support the tool. Poor threat investigation dashboards, substandard EDR remediation capabilities and requiring users to navigate through multiple alert dashboards are just the start.

Top reasons to choose Cynet over Sophos

**Designed for efficiency**
Cynet 360 automatically collects and correlates alerts and related data to identify suspicious or problematic activity, all presented on a streamlined dashboard.

**Robust security features, out of the box**
Cynet 360 delivers 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 screen switching**
Users must navigate separate dashboards for each alert category, with little context connecting them together, leading to a poor understanding of the current environment status.

**Out of scope**
Sophos does not offer customizable remediation playbooks or deception technology.

**Multiple tools, higher TCO**
Sophos achieves average user ratings, while bundling together all the components needed for full protection drives up your overall cost.
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
As an XDR, we have visibility into endpoint, user and network-based threats. And we leverage deception technology.

They’re Narrow
Sophos Intercept X Advanced only sees endpoint threats, and lacks any deception capabilities to expose attackers’ intentions.

We’re A Solution
If you want a solution that provides defense in depth out of the box, 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, or the expensive optional upgrades, Sophos Intercept X can be used as one component of your security stack.

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 with a clear, easy to use interface.

They Provide Clutter
Sophos provides a separate dashboard for each alert category, with each dashboard showing the last 5 events for the category and little context leading to a poor understanding of the current environment status.
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 Fully Automated
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.

We Eliminate Manual Tasks
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.

We Provide the Whole Story
Cynet’s Incident Engine provides automated attack investigation and reconstruction including root cause analysis and attack scope determination.

They Barely Support Manual Response
Anything but basic host remediation actions (delete/quarantine/kill) require a considerable manual effort using a command line interface on the Sophos platform.

They Are Manual Task Oriented
Default remediation actions on protected endpoints are almost nonexistent with Sophos. Admins can only choose to update the device, perform a full scan or isolate the device.

They Only Provide Sound Bites
Sophos claims root cause analysis capabilities but results are spotty. Admins must manually navigate through multiple forensic dashboards, each with a different look and feel.

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 add-ons. Most companies, understandably, prefer simplicity and openness.

Cynet Elite and Ultimate customers benefit from a full 24x7 MDR service that continuously monitors all client environments, providing best-of-breed detection and response services. Sophos baseline MDR is priced at a premium, so even a modestly sized deployment is a windfall for Sophos and a very steep cost to pay for their clients. And you’d need the more expensive MDR Complete to come close to Cynet’s included MDR services!

Our MDR is a Help Center

We’re Clear and Intuitive

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.

VS

Their MDR is a Profit Center

They Add Complexity and Overhead

Sophos requires significant administrative overhead due to its highly granular configuration requirements and lack of a single, centralized dashboard to view the entire environment.
## Independent Testing Is More Trustworthy Than Vendor Claims

The MITRE ATT&CK evaluation provides open, unbiased testing of leading XDR solutions against simulated attack scenarios. Results can be used to get a sense of vendors’ capabilities.

### We Detect More and Better
For the second year in a row, Cynet XDR detected more attack techniques than Sophos 98.2% vs. 80.7% in the 2022 evaluation.

### Their Detection Was Subpar
Sophos also allowed six times as many sub-steps to execute at each attack stage as Cynet before detecting threats. The faster threats are detected, the less likely they are to cause damage.

### We Stop Attacks Early
Cynet prevented 88% of attacks before any further infiltration (sub-steps) could take place in the test environment during the 2022 MITRE evaluation.

### They Are Slow to Recognize Attacks
Sophos prevented a mere 44.95% of attacks before any further infiltration (sub-steps) could take place. The more attack steps allowed, the more likely an attack will be successful.

### 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.

### Their Visibility was Bottom of the Pack
Sophos leveraged less than half the data sources as Cynet (7 vs. 15), meaning less visibility when detecting common attack vectors and less context to help analysts investigate alerts.
### Business Differentiators

<table>
<thead>
<tr>
<th>Capability</th>
<th>Cynet</th>
<th>Sophos</th>
</tr>
</thead>
<tbody>
<tr>
<td>Autonomous Protection and Response</td>
<td>Automating the manual process of protecting against, and remediating threats</td>
<td>Basic platform insert to be customized and other agility expert services</td>
</tr>
<tr>
<td>Alerts and Context</td>
<td>Accurate alerting that helps identify false negatives while mitigating against false positives</td>
<td>Accurate alerts with more granularity, risk scores for alert prioritization, issue chain</td>
</tr>
<tr>
<td>Automation</td>
<td>Automated capabilities that reduce the burden on lean security teams</td>
<td>Release trained to reduce the burden on lean security teams</td>
</tr>
<tr>
<td>Visibility</td>
<td>Ability to zoom in across multiple layers</td>
<td>Full 180° coverage requires multiple location tools</td>
</tr>
</tbody>
</table>

### Feature Differentiators

#### Threat Prevention and Detection

<table>
<thead>
<tr>
<th>Capability</th>
<th>Cynet</th>
<th>Sophos</th>
</tr>
</thead>
<tbody>
<tr>
<td>Endpoint Prevention and Detection</td>
<td>Multiple layers: malware detection, including static and dynamic detection, detect exploits, malicious scripts and fileless attacks.</td>
<td>Full set of features</td>
</tr>
<tr>
<td>Compromised User Account Detection</td>
<td>Detect anomalous user behaviors that may indicate a potential threat</td>
<td>Not available</td>
</tr>
<tr>
<td>Malicious Network Activity Detection</td>
<td>Detect malicious network activity behaviors, such as reconnaissance scanning, C&amp;I (C2 and IoC) scanning, lateral movement and required indicators.</td>
<td>Full set of features</td>
</tr>
<tr>
<td>Deception Technology</td>
<td>Lure attackers to misdirect attention by using deception tactics, including fake files, hosts, users, and networks.</td>
<td>Full set of features</td>
</tr>
<tr>
<td>Security Policy Features</td>
<td>Define and enforce security policies around device control, network control, blacklists, exclusions, etc.</td>
<td>Full set of features</td>
</tr>
<tr>
<td>Deception</td>
<td>Lure attackers to misdirect attention by using deception tactics, including fake files, hosts, users, and networks.</td>
<td>Full set of features</td>
</tr>
</tbody>
</table>

#### Investigation and Response

<table>
<thead>
<tr>
<th>Capability</th>
<th>Cynet</th>
<th>Sophos</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remediation Playbooks</td>
<td>Automatically implement a predefined sequence of remediation actions across the environment in response to specific threats.</td>
<td>Not available.</td>
</tr>
<tr>
<td>Forensics</td>
<td>Forensic dashboard for investigation, threat hunting and integrated threat intelligence</td>
<td>Not available.</td>
</tr>
<tr>
<td>Managed Detection and Response (MDR) Service</td>
<td>24/7 monitoring, investigating, incident analysis, and threat response capabilities</td>
<td>Full MDR included with Cynet Elite and Ultimate</td>
</tr>
</tbody>
</table>

### Architecture

<table>
<thead>
<tr>
<th>Capability</th>
<th>Cynet</th>
<th>Sophos</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported Operating Systems</td>
<td>Windows, Mac, Linux</td>
<td>Windows, Mac, Linux</td>
</tr>
<tr>
<td>Deployment</td>
<td>Cloud, Hybrid</td>
<td>Cloud, On Prem, Hybrid</td>
</tr>
<tr>
<td>Agent</td>
<td>Automatic self-deploying agent, autodeployment on new endpoints</td>
<td>Automatic self-deploying agent, autodeployment on new endpoints</td>
</tr>
<tr>
<td>Agent resources</td>
<td>Lightweight agent with minimal performance overhead</td>
<td>Deployment to Windows OS (up to 8 minutes, large agent footprint for On Prem deployment only)</td>
</tr>
<tr>
<td>Multi-tenancy</td>
<td>Full multi-tenant architecture</td>
<td>Full multi-tenant architecture</td>
</tr>
<tr>
<td>Console UI</td>
<td>Attractive and highly functional</td>
<td>Gated, complex interface with authentication of subaccounts, significant administrative overhead for initial configuration</td>
</tr>
<tr>
<td>Agent Detection</td>
<td>Agent Self-Protects/Skip Tamper</td>
<td>Agent Self-Protects/Skip Tamper</td>
</tr>
<tr>
<td>IRRAC Support</td>
<td>Full IRRAC</td>
<td>Full IRRAC</td>
</tr>
</tbody>
</table>
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.

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 includes deception technology to lure attackers into revealing their presence.

Lightspeed deployment and immediate value
Seamless distribution across 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.