Competitive Analysis:

Cynet vs. Sophos

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, 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

cynet		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.	VS	**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.
Robust security features, out of the box Cynet 360 delivers features like customizable remediation playbooks along with network and user deception files.	VS	**Out of scope** Sophos does not offer customizable remediation playbooks or deception technology.
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	**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.

VS

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.

VS

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.

VS

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.

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.

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.

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.

We Provide the Whole Story

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

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.

Our MDR is a Help Center

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.

VS

Their MDR is a Profit Center

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!

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

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

Capability	Explanation	cynet	SOPHOS
Autonomous Protection and Response	Automating the manual process of protecting against, and remediating threats	✓ Simple, light, intuitive platform built for lean security teams	✗ Basic platform meant to be customized and lever aged 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	✗ Missed detections when offline that are generally detected when back online, no risk score or alert prioritization
Automation	Automated capabilities that reduce the burden on lean security teams.	✓ Broad set of automated capabilities to minimize manual intervention	✗ Archaic command line ac- cess for manual intervention
Visibility	Ability to see threats across multiple layers	✓ Broad XDR coverage	✗ Full XDR coverage requires multiple Sophos tools

Feature Differentiators

Threat Prevention and Detection

Capability	Explanation	cynet	SOPHOS
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	✗ 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	✗ Sold separately
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
Security Policy Features	Define and enforce security policies around device control, network control, blacklists, exclusions, etc.	✓ Full set of features	✓ Full set of features
SaaS Security Posture Management	SSPM reduces the risk associated with SaaS configuration errors and oversights.	✓ Full set of features	✗ Sold separately

Investigation and Response

Capability	Explanation	cynet	SOPHOS
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	✗ Not available. Only offers basic traditional AV actions (delete/quarantine /kill) and manual command line interface to host
Forensics	Forensic dashboard for investigation, threat hunting and integrated threat intelligence	✓ Intuitive interface with prebuilt queries, visualization and advanced search capabilities.	✗ EDR forensics limited to Host/Endpoint, lacks User & Network layers
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

Architecture

Capability	cynet	SOPHOS
Supported Operating Systems	✓ Windows, Mac, Linux	✓ Windows, Mac, Linux
Deployment	✓ Cloud, On Prem, Hybrid	✓ Cloud, On Prem, Hybrid
Agent	✓ Automatic self-distributing agent, auto-deployment on new endpoints	✗ Automatic self-distributing agent, auto-deployment on new endpoints for On Prem deployment only
Agent resources	✓ Lightweight agent with minimal performance overhead	✗ Deployment on Windows OS up to 10 minutes, large agent footprint with 12+ subproceses running
Mutli-tenancy	✓ Full muti-tenant architecture	✓ Full muti-tenant architecture
Console UX	✓ Attractive and highly functional	✗ Dated, complex interface with abundance of sub-menus, significant adminstrative overhead for initial configuration
Agent Protection	✓ Agent Self-Protection/Anti Tamper	✓ Agent Self-Protection/Anti Tamper
RBAC support	✓ Full RBAC	✓ Full RBAC

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 includeaccess 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.