SOPHOS SYNCHROWORKS CONSULTING

Top 5 Reasons You Need EDR

Endpoint detection and response (EDR) tools are built to supplement endpoint security with increased detection, investigation, and response capabilities. However, the hype surrounding EDR tools can make it difficult to understand how exactly they can be used and why they are needed. Making matters worse, today's EDR solutions often struggle to provide value for many organizations as they can be difficult to use, lack sufficient protection capabilities, and are resource intensive.

Sophos Intercept X with EDR integrates intelligent EDR with the industry's top-rated endpoint and server protection in a single solution, making it the easiest way for organizations to answer the tough questions about security incidents. Here are some additional reasons to consider an EDR solution.

Maintain IT security operations hygiene and hunt down stealthy threats

Depending on the organization IT operations and IT security staff can either be part of the same team, operate independently or even be the same person. Whatever the setup, the two areas require different use cases from an EDR tool, so that tool should be capable of performing both sets of tasks and remain accessible without compromising on power.

For the IT operations admin keeping their organization's estate in good health is critical. For example, finding machines with performance issues such as low disk space or high memory usage. Locating devices that have vulnerable programs that require patching. Tracking down endpoints and servers that have RDP enabled unnecessarily or still have guest counts enabled. Sophos EDR gives admins the tools to ask all of these questions and many more, as well as the ability to remotely access the devices to fix security holes by investigating performance issues, installing patches, and disabling RDP and guest accounts.

Cybersecurity specialists need to be able to hunt down subtle, evasive threats that aren't automatically convicted by their endpoint protection. Their EDR tool needs to be efficient at tracking down indicators of compromise (IoCs) such as: identifying processes attempting to connect on non-standard ports, processes that have edited files or registry keys, processes disguising themselves as something else, and tracking down which employees clicked a link in a phishing email. Sophos EDR makes it easy to quickly perform these types of investigation across an organization's entire estate. Then, it's just as easy to remotely access a device of interest to dig deeper, deploy forensic tools and terminate suspicious processes.

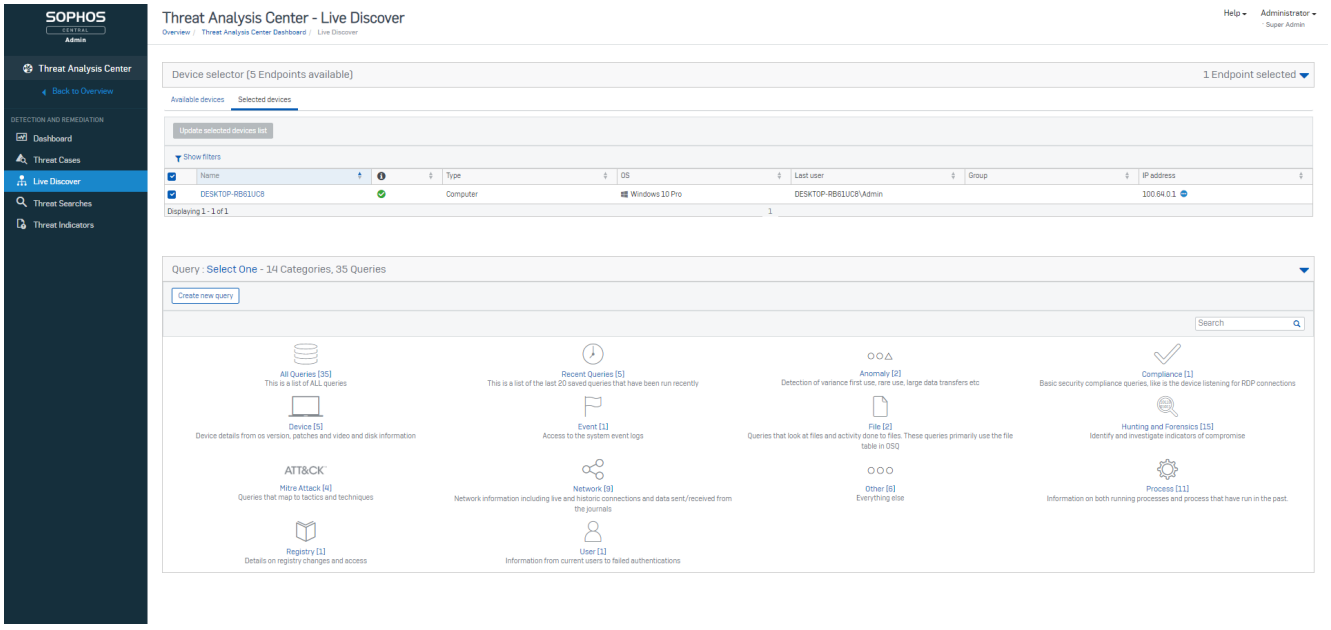


Figure 1: Sophos Intercept X with EDR lets users ask detailed questions across their entire estate

Detect attacks that have gone unnoticed

When it comes to cybersecurity, even the most advanced tools can be defeated given enough time and resources, making it difficult to truly understand when attacks are happening. Organizations often rely solely on prevention to stay protected, and while prevention is critical, EDR offers another layer of detection capabilities to potentially find incidents that have gone unnoticed.

Organizations can leverage EDR to detect attacks by searching for indicators of compromise (IOCs). This is a quick and straightforward way to hunt for attacks that may have been missed. Threat searches are frequently kicked off after a notification from third-party threat intelligence: for example, a government agency (such as US-CERT, CERT-UK, or CERT Australia) might inform an organization that there is suspicious activity in their network. The notification may be accompanied by a list of IOCs, which can be used as a starting point to determine what is happening.

The Threat Indicators feature in Intercept X provides a list of the top suspicious events, so analysts know exactly what they should be investigating. By leveraging SophosLabs machine learning capabilities, a list of the top suspicious events is presented, ranked by their threat score. This makes it easy for analysts to prioritize their workloads and focus on the most important events.

Knowing where to start the analyst can then track down all instances of that suspicious item across their entire estate and quickly take action to clean up. In addition, they can leverage powerful SQL queries to track down other indicators of compromise such as processes editing registry keys and processes attempting to connect on non-standard ports.

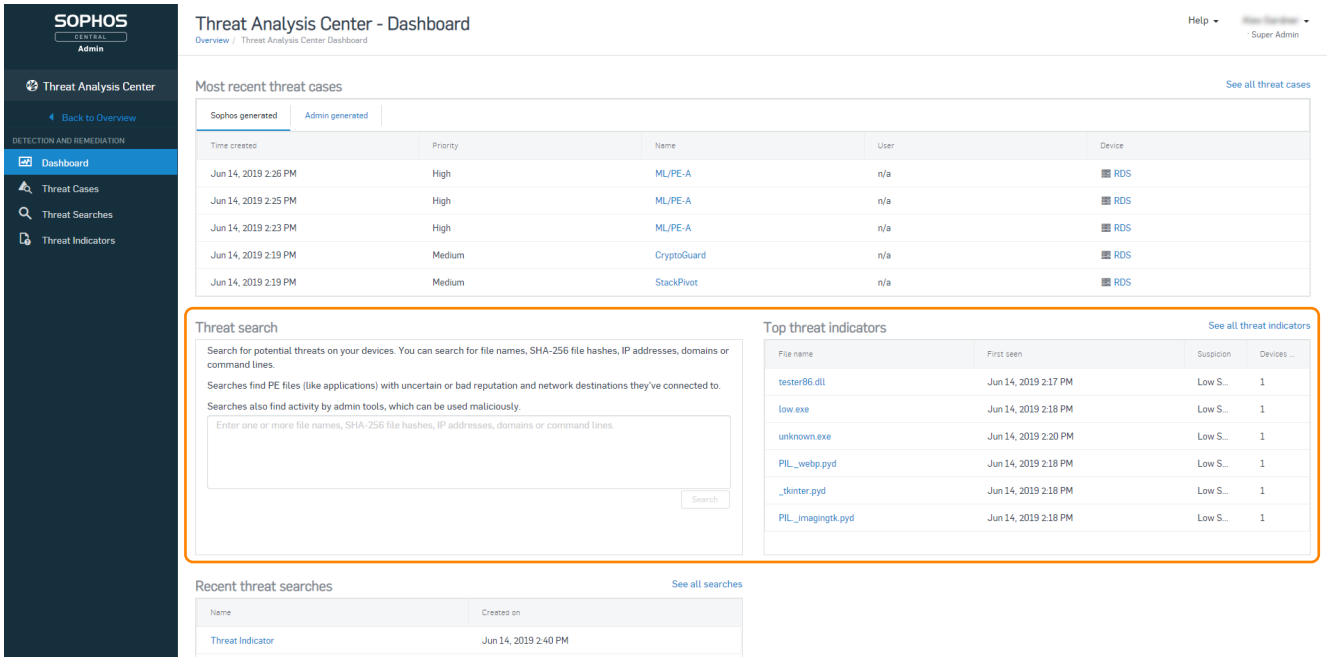


Figure 2: Sophos Intercept X with EDR offers the ability to search for indicators of compromise across the network. It also leverages machine learning to determine the top suspicious events that should be investigated

Combining the ability to ask detailed questions with guidance on where to start, as well as curated threat intelligence gives admins the best of all worlds and makes Sophos EDR straightforward to use without sacrificing any power or granularity.

Respond faster to potential incidents

Once incidents are detected, IT and security teams usually scramble to remediate them as fast as possible to reduce the risk of attacks spreading and to limit any potential damage. Naturally, the most pertinent question to ask is how to get rid of each respective threat. On average, security and IT teams spend more than three hours trying to remediate each incident. EDR can speed this up significantly.

The first step an analyst might take during the incident response process would be to stop an attack from spreading. Intercept X with EDR isolates endpoints and servers on demand, which is a key step to stop a threat from spreading throughout the environment. Analysts will often do this before investigating, buying time while they determine the best course of action.

The investigation process can be a slow and painful one. This of course assumes an investigation occurs at all. Incident response traditionally relies heavily on highly-skilled human analysts. Most EDR tools also rely heavily on analysts to know which questions to ask and how to interpret the answers. However, with Intercept X with EDR, security teams of all skill levels can quickly respond to security incidents thanks to guided investigations that offer suggested next steps, clear visual attack representations, and built-in expertise.

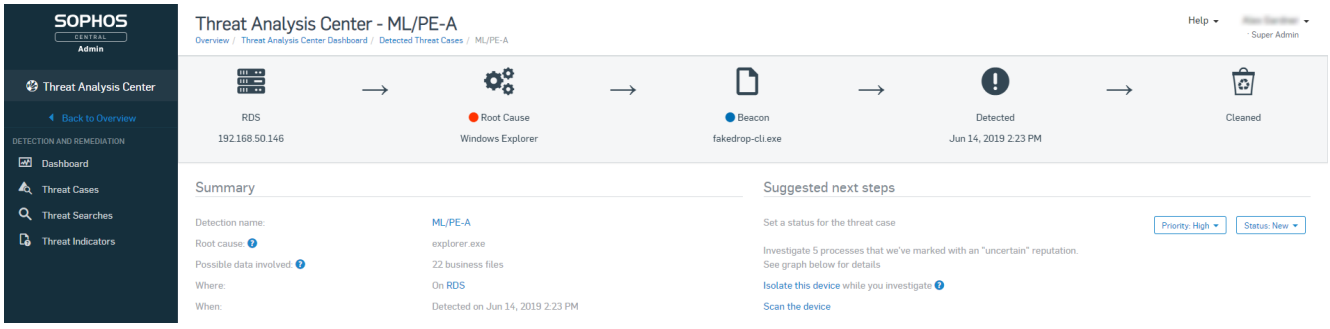
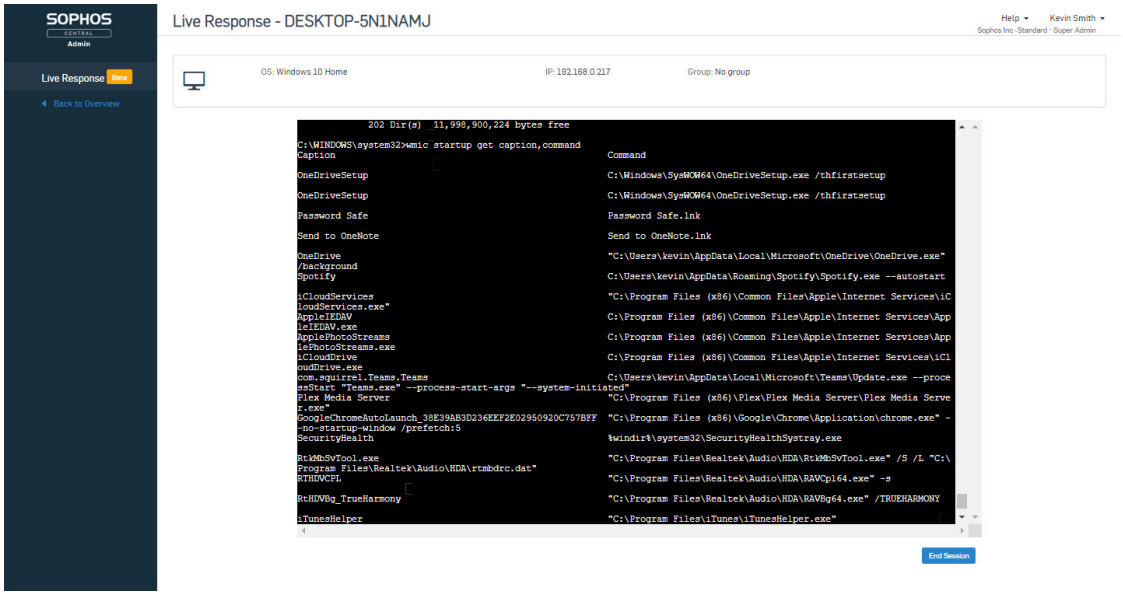


Figure 3: Guided incident response offers suggested next steps and on-demand endpoint isolation to quickly and safely resolve incidents.

Sophos EDR also includes the ability to remotely access devices via a command line interface. It's ideal for rapid response, even when the employee is not office-based. Upon accessing the device admins can perform further investigation by deploying forensic tools, install/uninstall software, terminate processes and reboot the device.



Figures 4: Action buttons are located throughout Intercept X with EDR that offer multiple remediation options, with "clean and block" being the most common.

Add expertise without adding headcount

By a large margin, organizations looking to add endpoint detection and response capabilities cite "staff knowledge" as the top impediment to EDR adoption. This shouldn't come as a great surprise, as the talent gap for finding qualified cybersecurity professionals has been widely discussed for several years. This barrier is especially pronounced with smaller organizations.

Top reasons why organizations have not implemented EDR

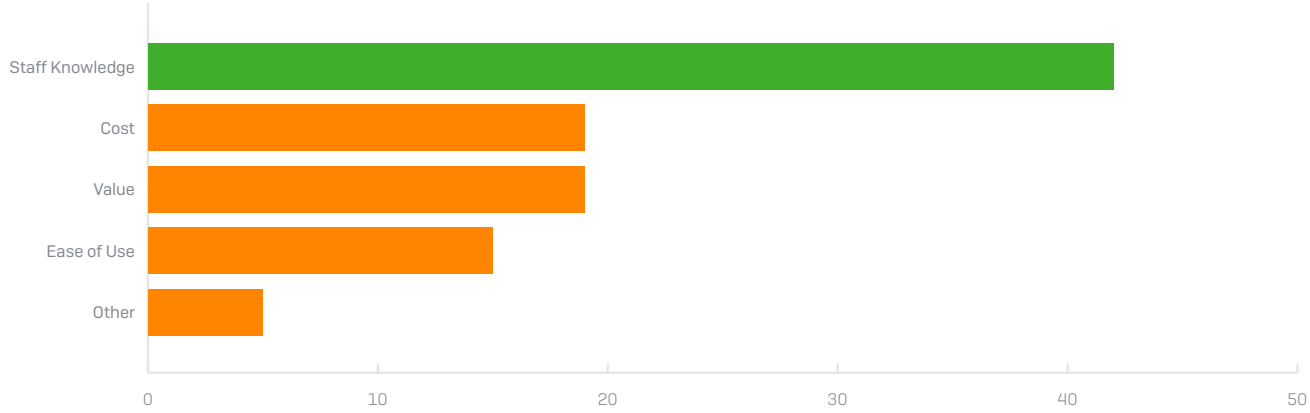


Figure 5: Staff knowledge was cited as the top reason why organizations have not adopted an endpoint detection and response (EDR) solution (Source: Sapio study in conjunction with Sophos, October 2018)

To combat the staff knowledge gap, Intercept X with EDR replicates the capabilities associated with hard-to-find analysts. It leverages machine learning to integrate deep security insight and is enhanced with curated SophosLabs threat intelligence, so you can add expertise without having to add staff. The intelligent EDR capabilities help fill the gaps caused by a lack of staff knowledge, reproducing the functions of several types of analysts:

- Security analysts: These are the front-line analysts tasked with triaging incidents and determining which alerts need to be immediately addressed. Ideally, they're also able to proactively hunt to detect any attacks that may have gone unnoticed. Intercept X with EDR automatically detects and prioritizes potential threats. Using machine learning, suspicious events are identified and given a threat score. The events with the highest scores are the most immediately important. Analysts can quickly see where to focus their attention and start investigating.
- Malware analysts: Organizations may rely on malware experts that specialize in reverse engineering suspicious files in order to analyze them. Not only is this approach time consuming and difficult to achieve, but it assumes a level of cybersecurity sophistication most organizations do not possess. Malware analysts are needed to decide if a file that was not blocked is actually malicious. They also may look at files that were convicted but may actually be false positives. Intercept X with EDR offers a better approach to malware analysis by leveraging machine learning. Using the industry's best endpoint malware detection engine, malware is automatically analyzed in extreme detail, breaking down file attributes and code components and comparing them to millions of other files. Analysts can easily see which attributes and code segments are similar to "known-good" and "known-bad" files so they can determine if a file should be blocked or allowed.

- **Threat intelligence analysts**: Investigations may rely on third-party threat intelligence (often at an additional cost) to add insight and context into threats. Analysts are needed to interpret and integrate this data to ensure it adds value. Threat intelligence can be used as a starting point to investigations, as a means for asking the security community what it thinks of a suspicious file, or to determine if an attack is targeting the organization. Intercept X with EDR provides IT and security administrators the ability to gather more information by accessing on-demand threat intelligence curated by SophosLabs. To maintain full visibility into the threat landscape, SophosLabs tracks, deconstructs, and analyzes 400,000 unique and previously unseen malware attacks each day in a constant search for the latest and greatest attack techniques. This threat intelligence is collected, aggregated, and summarized for easy analysis so teams that do not have dedicated threat intelligence analysts or access to expensive and hard to understand threat feeds can benefit from one of the top cybersecurity research and data science teams in the world.

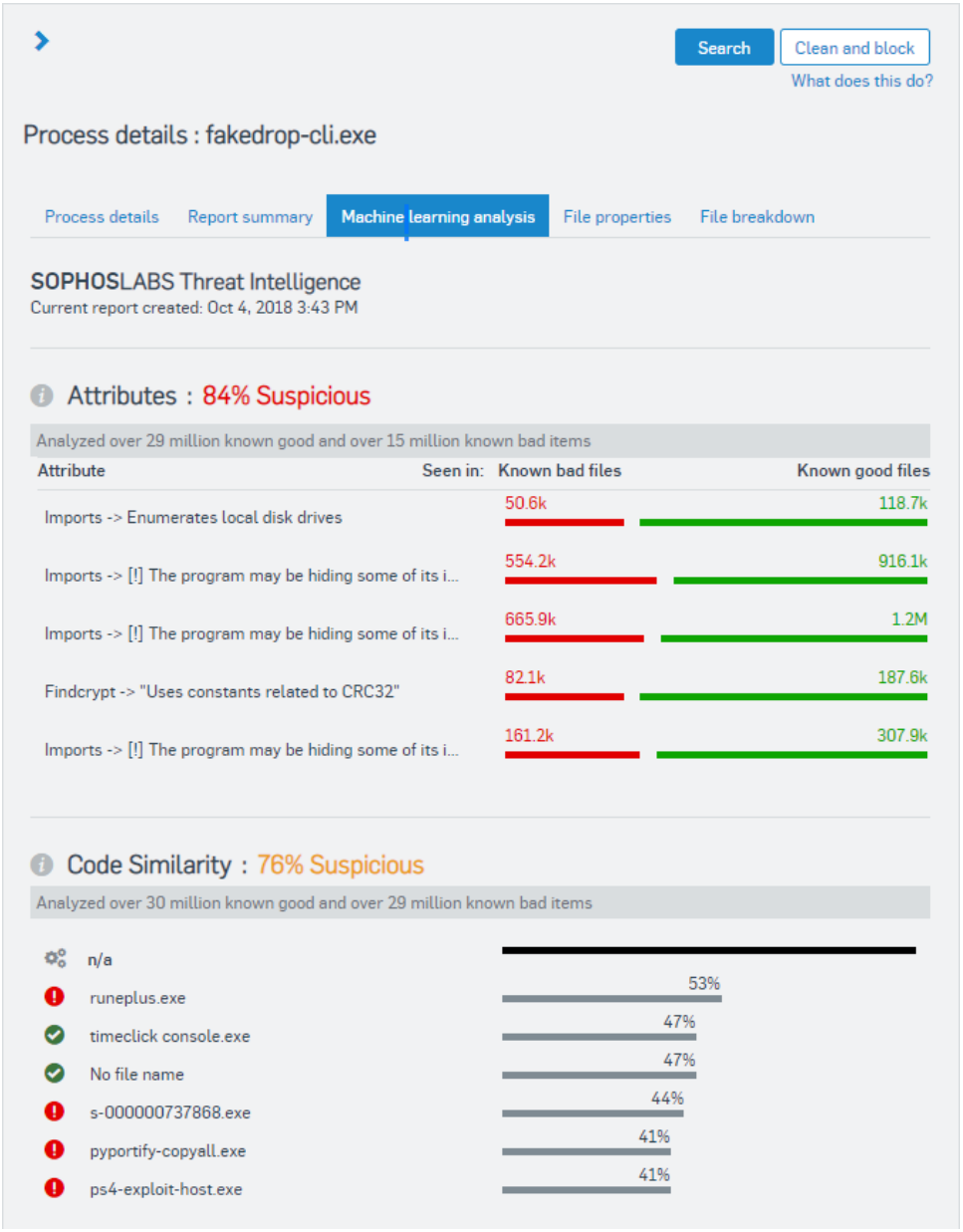


Figure 6: Machine learning analysis displays the attributes, code similarity, and file path analysis for powerful yet simple analysis.

Managed Threat Response (MTR)

Looking for help managing EDR? Sophos' MTR service fuses technology and expert analysis for improved threat hunting and detection, deeper investigation of alerts, and targeted actions to respond to threats.

Understand how an attack happened and how to stop it from happening again

Security analysts have recurring nightmares where they have suffered an attack: an executive screams, "How did this happen?!" and all they can do is shrug their shoulders. Identifying and removing malicious files solves the immediate problem, but it doesn't shed light upon how it got there in the first place or what the attacker did before the attack was shut down.

Threat cases, included with Intercept X with EDR, spotlight all the events that led up to a detection, making it easy to understand which files, processes, and registry keys were touched by the malware to determine the impact of an attack. It provides a visual representation of the entire attack chain, ensuring confident reporting about how the attack started and where the attacker went. More importantly, by understanding the root cause of an attack, the IT team will be much more likely to prevent it from ever happening again.

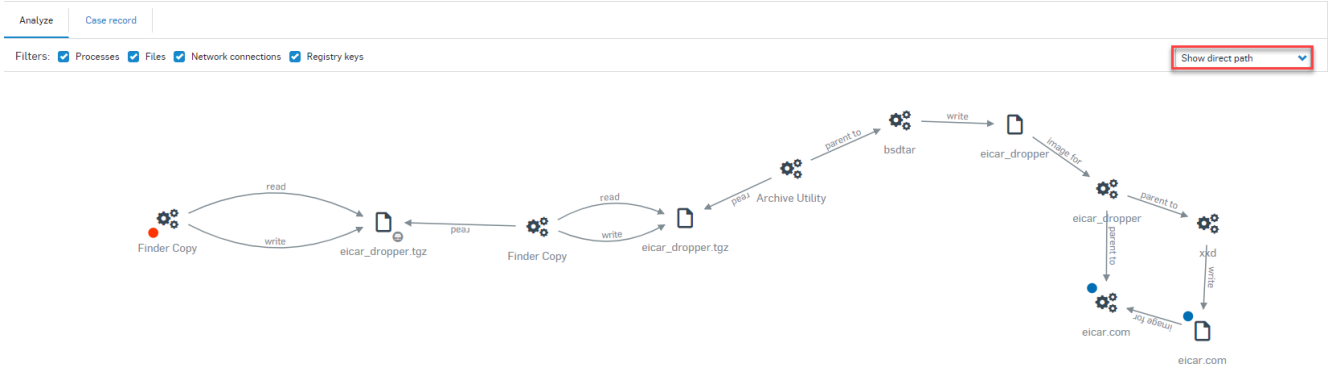


Figure 7: Threat cases provide a visual and interactive representation of the attack chain.

Cross-estate visibility for your endpoints and servers

Sophos offers EDR for Intercept X and Intercept X for Server, giving you unparalleled visibility across your entire estate. That's on top of industry-leading protection that stops the latest threats such as ransomware, blocks exploit techniques and shuts hackers down.

Find out more and start your free trial at sophos.com/interceptx

Try it now for free

Register for a free 30-day evaluation at sophos.com/interceptx

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

2020-05-27 (MP)

SYNCHROWORKS CONSULTING SOPHOS