SOPHOS INTERCEPT X ADVANCED WITH EDR

Open Ended Questions

- How do you know if your business is under attack / have a security incident?
- When you have a potential security incident or find something that wasn't blocked by your endpoint protection, what is your process for investigating and responding? Is that been an effective process? What tools are you relying on?
- What process and tools do you have in place to understand the scope and impact of an attack?
- What level of visibility do you have into your endpoints to report on your security or compliance posture?
- EAP specific: What compelled you to join the EAP program for EDR? How has your experience been?

Conversation Starters

- The EDR Early Access Program was the most successful in Sophos history. 500+ customers and 20,000+ endpoints enrolled. The feedback has been overwhelmingly positive with participants commending guided investigations, deep learning malware analysis, SophosLabs intelligence, and easy search capabilities.
- In a recent study (Source: Sapio study in conjunction with Sophos, October 2018), "Staff knowledge" was cited as the top barrier to EDR adoption. Sophos addresses this with built-in expertise.
- It takes organizations on average over 3 hours to respond to potential security incidents. That process, including investigation and remediation, can be sped up significantly with EDR functionality.

Top EDR Use Cases

- Confidently report on your security posture at any given moment
- Detect attacks that have gone unnoticed
- Investigate attacks that are tagged as suspicious (but are not definitely malicious)
- Understand the scope and impact of an incident
- Conduct analysis by replicating capabilities associated with hard to find analysts
- Respond faster to potential incidents

SOPHOS INTERCEPT X ADVANCED WITH EDR

Intercept X Advanced with EDR Strengths

- EDR starts with the Strongest Protection
  - Sophos consistently rates at or near the top in 3rd party endpoint protection tests
  - EDR and the best protection combined into a single agent and product.
  - Reduce noise and lighter EDR workload
- Sophos allows you to add expertise, without adding headcount
  - Replicates the capabilities associated with hard to find analysts
  - Leverages Sophos' machine learning expertise, such as the Deep Learning Malware Analysis feature
  - On-demand curated threat intelligence from SophosLabs by leveraging machine learning and SophosLabs intelligence.
- Guided incident response
  - Helps you answer the tough questions as part of an investigation
  - Approachable yet powerful EDR is a good fit for teams of all skill levels
  - Respond to incidents with a single click

Top EDR Use Cases

- Intercept X Advanced with EDR datasheet
- Intercept X Advanced with EDR presentation

- Top 5 reasons you need EDR solution brief
- Demo video (available on sophos.com/endpoint)
- Sophos.com/ProveIt

SOPHOS INTERCEPT X ADVANCED WITH EDR

Objection Handling

I am already using Intercept X, I thought I was protected, why do I need EDR too?	• The prevention is the same in Intercept X and Intercept X Advanced with EDR. The EDR version gives you the ability to detect the rare threat that evades Intercept X protection or investigate events that are suspicious but need confirmation before being blocked. • Intercept X gives organizations the ability to answer the tough questions about a suspicious incident. • Upgrade to EDR version for richer threat intelligence, additional context, and faster incident response
I am looking into another EDR tool that offers some functionality that Sophos is missing	• While other EDR tools may contain features not included in Intercept X, those features will likely go unused. This is because most EDR tools are difficult to use, resource intensive, and difficult to get value out of. Unlike competitors, Sophos allows you to add EDR expertise without adding headcount. • Many features in Intercept X, such as Deep Learning Malware Analysis, guided investigations, and SophosLabs threat intelligence are Sophos unique strengths. Also, EDR starts with the strongest protection, and Intercept X Advanced with EDR is built with the industry's best protection. This means that the EDR will have a lighter workload because the protection filters out much of the noise
I don't have a sophisticated enough team / don't have the ability to hire more analysts to run EDR	• With Intercept X Advanced with EDR expertise is built into the product so you do not need to hire additional headcount. You can use the product today with the team you have. • Intercept X Advanced with EDR replicates the tasks normally performed by skilled analysts. Unlike other EDR solutions which rely on highly skilled human analysts to ask questions and interpret data, Intercept X Advanced with EDR is powered by machine learning and enhanced with curated SophosLabs threat intelligence. • Intercept X Advanced with EDR will save you time and energy if there is any suspicious activity in your environment. Quickly and confidently answer the tough questions about an incident.
I am using another vendor(s) why should I switch to Sophos?	• EDR starts with the strongest protection, and Intercept X has the best protection built in. This means a lower EDR workload and a reduction in time consuming noise. • Unlike other EDR solutions which rely on highly skilled human analysts to ask questions and interpret data, Intercept X Advanced with EDR is powered by machine learning and enhanced with curated SophosLabs threat intelligence. • Sophos in intuitive to use and easy to understand, leveraging guided investigations, built-in expertise, and rapid response options.