SOPHOS
Cybersecurity evolved.

Intercept X Advanced with EDR

Speziell für Threat Hunting und IT Operations entwickelte Endpoint Detection and Response

Sophos Intercept X Advanced with EDR kombiniert leistungsstarke Endpoint Detection and Response (EDR) mit einzigartiger Endpoint Protection. Nutzen Sie die Funktionen entweder zum Threat Hunting, um aktive Angreifer zu erkennen, oder aber in IT Operations, um sicherzustellen, dass Sicherheitsvorgaben durchgesetzt werden. Wenn ein Problem gefunden wird, haben Sie per Remote-Zugriff die Möglichkeit, gezielte Maßnahmen zu ergreifen.

Highlights

- EDR in Kombination mit dem stärksten Endpoint-Schutz
- Entwickelt für Sicherheitsanalysten und IT-Administratoren
- Proaktiv sicherstellen, dass Sicherheitsvorgaben durchgesetzt werden, und Bedrohungssuche, bevor Schäden entstehen
- Sofort einsatzbereite, individuell anpassbare SQL-Abfragen
- Bis zu 90 Tage schneller Zugriff auf aktuelle und Verlaufsdaten auf der Festplatte
- Gezielte Maßnahmen per Remote-Zugriff über die Befehlszeile
- Erkennen, Analysieren und Priorisieren von Vorfällen mittels Machine Learning
- Beschleunigung von Analysen und Reduzierung der Verweilzeit von Angriffen
- Verfügbar für Windows, MacOS* und Linux

** In Kürze erhältlich*

EDR beginnt mit dem stärksten Schutz

Um Datenpannen zuverlässig zu verhindern, ist eine gute Prävention unerlässlich. Intercept X vereint einzigartige Endpoint Protection mit EDR in einer einzigen Lösung. So werden die meisten Bedrohungen bereits gestoppt, bevor sie Schaden anrichten können. Intercept X Advanced with EDR bietet zusätzliche Cybersecurity zur Erkennung, Analyse und Reaktion auf potenzielle Sicherheitsbedrohungen.

Die Integration von EDR in eine erstklassige Endpoint Protection Suite ermöglicht es Intercept X, den EDR-Workload deutlich zu verringern. Da mehr Bedrohungen bereits im Vorfeld ausgeschaltet werden, vergeuden Analysten weniger Zeit mit der Verfolgung von False Positives und werden nicht mit einer Flut von Warnmeldungen überfordert.

Mehr Know-how – ohne zusätzliches Personal

Erkennen, priorisieren und analysieren Sie Bedrohungen automatisch mittels künstlicher Intelligenz: Dank Machine Learning erkennt und priorisiert Intercept X Advanced with EDR potenzielle Bedrohungen automatisch. Wenn eine potenziell schädliche Datei entdeckt wird, können Benutzer per Deep Learning-Malware-Analyse mit extremer Genauigkeit automatisch Malware analysieren, indem sie Dateiattribute und Code aufschlüsseln und mit Millionen anderer Dateien vergleichen.

Sofort einsatzbereite Abfragen: Mit vorformulierte, nach Anwendungsfall kategorisierten SQL-Abfragen können Sicherheitsanalysten und IT-Administratoren Sophos EDR sofort nutzen. Die Abfragen können für benutzerdefinierte Suchen einfach abgewandelt, komplett neu formuliert oder aus der Community bezogen werden.

Finden Sie die Antworten auf schwierige Fragen, indem Sie in die Rolle hochqualifizierter Analysten schlüpfen: Intercept X Advanced with EDR übernimmt die Arbeit von geschultem Fachpersonal – Unternehmen bekommen so mehr Know-how, ohne weitere Mitarbeiter einstellen zu müssen.

Threat Hunting und Optimierung von IT Operations

Sophos Intercept X Advanced ist die erste EDR-Lösung, die speziell für IT-Administratoren und Sicherheitsanalysten entwickelt wurde. Mit Sophos Intercept X Advanced können Sie beliebige Abfragen dazu erstellen, was in der Vergangenheit passiert ist und was momentan auf Ihren Endpoints passiert. Diese Abfragen können Sie entweder zum Threat Hunting nutzen, um aktive Angreifer zu erkennen, oder aber in IT Operations, um sicherzustellen, dass Sicherheitsvorgaben durchgesetzt werden. Wenn ein Problem gefunden wird, können Sie per Remote-Zugriff gezielte Maßnahmen ergreifen. Ermöglicht wird dies durch die leistungsstarken Funktionen „Live Discover“ und „Live Response“.

Live Discover – Beliebige Fragen stellen, um immer einen Schritt voraus zu bleiben: Mit Live Discover können Sicherheitsanalysten und IT-Administratoren praktisch jede Frage über ihre Endpoints und Server stellen und beantworten. Decken Sie schnell und einfach Probleme in IT Operations auf, um sicherzustellen, dass Sicherheitsvorgaben durchgesetzt werden, und stellen Sie detaillierte Fragen, um verdächtigen Aktivitäten auf den Grund zu gehen. Live Discover nutzt leistungsstarke, sofort einsatzbereite, individuell anpassbare SQL-Abfragen, mit denen bis zu 90 Tage aktuelle und Verlaufsdaten auf der Festplatte durchsucht werden können. Hier einige Anwendungsbeispiele:

IT Operations

- Warum läuft ein System langsam? Steht ein Neustart aus?
- Welche Geräte verfügen über bekannte Schwachstellen, unbekannte Dienste oder nicht autorisierte Browser-Erweiterungen?
- Werden Programme ausgeführt, die entfernt werden sollten?
- Ist Remote Sharing aktiviert? Befinden sich unverschlüsselte SSH-Schlüssel auf dem Gerät? Sind Gastkonten aktiviert?
- Verfügt das Gerät über die Kopie einer bestimmten Datei?

Threat Hunting

- Welche Prozesse versuchen, eine Netzwerkverbindung über Nicht-Standardports herzustellen?
- Erkannte Kompromittierungs-Indikatoren mit Zuordnungen zum MITRE ATT&CK Framework auflisten
- Prozesse anzeigen, die kürzlich Dateien oder Registry-Schlüssel geändert haben
- Details über PowerShell-Ausführungen suchen
- Prozesse identifizieren, die als services.exe getarnt sind

Live Response – Per Remote-Zugriff gezielte Maßnahmen ergreifen: Wenn Probleme erkannt werden, erhalten Benutzer per Live Response über die Befehlszeile Zugriff auf Endpoints und Server in ihrer gesamten Unternehmensumgebung. Per Remote-Zugriff können auf Geräten weitere Analysen vorgenommen und Probleme behoben werden. Administratoren können u. a. Geräte neu starten, aktive Prozesse beenden, Skripts ausführen, Konfigurationsdateien bearbeiten, Software installieren/deinstallieren und forensische Tools ausführen.

Managed Detection and Response

Unser Fully-Managed-Service Sophos Managed Threat Response (MTR) bietet 24/7 Managed Detection and Response mit aktiver Bekämpfung von Bedrohungen durch ein Sophos-Expertenteam. Andere Managed Detection and Response (MDR) Services informieren Sie lediglich über Angriffe und verdächtige Ereignisse. Mit Sophos MTR erhält Ihr Unternehmen ein Expertenteam, das für Sie gezielte Maßnahmen ergreift, um selbst hochkomplexe Bedrohungen unschädlich zu machen. Kunden, die sich für Sophos MTR entscheiden, erhalten auch Intercept X Advanced with EDR.

	Sophos Intercept X Advanced with EDR	Sophos Intercept X Advanced	Sophos Endpoint Protection
Traditionelle Techniken	✓	✓	✓
Deep Learning	✓	✓	
Anti-Exploit	✓	✓	
CryptoGuard Anti-Ransomware	✓	✓	
Endpoint Detection and Response (EDR)	✓		

Jetzt kostenfrei testen

Kostenlose 30-Tage-Testversion unter www.sophos.de/intercept-x

Sales DACH (Deutschland, Österreich, Schweiz)
Tel.: +49 611 5858 0 | +49 721 255 16 0
E-Mail: sales@sophos.de

20-05-12 DS-DE (MP)

SOPHOS