Intercept X Advanced with EDR

Intelligente Endpoint Detection and Response

Sophos Intercept X Advanced with EDR kombiniert intelligente Endpoint Detection and Response (EDR) mit branchenweit erstklassiger Malware-Erkennung, leistungsstarkem Exploit-Schutz und anderen einmaligen Endpoint Protection Features.

EDR beginnt mit dem stärksten Schutz

Um Datenpannen zuverlässig zu verhindern, ist eine gute Prävention unerlässlich. Intercept X vereint einmaligen Schutz und Endpoint Detection and Response in einer einzigen Lösung. So werden die meisten Bedrohungen gestoppt, bevor sie überhaupt Schaden anrichten können. Dazu bietet Intercept X Advanced with EDR weiterführende 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. Je mehr Bedrohungen abgewehrt werden, desto weniger Vorfälle müssen von den IT-Mitarbeitern untersucht werden. So können sich IT-Abteilungen auf die Optimierung ihrer Hauptressourcen und auf ihre IT-Aufgaben konzentrieren statt False Positive-Meldungen und einer Flut von Benachrichtigungen nachzugehen.

Mehr Know-how – ohne zusätzliches Personal

Intercept X Advanced with EDR übernimmt die Arbeit von geschultem Fachpersonal – Unternehmen bekommen so mehr Know-how, ohne weitere Mitarbeiter einstellen zu müssen. Im Gegensatz zu anderen EDR-Lösungen, die eine Unterstützung durch hochqualifiziertes Fachpersonal benötigen, nutzt Intercept X Advanced with EDR leistungsstarkes Machine Learning und aktuelle Bedrohungsdaten aus den SophosLabs.

Sicherheits-Know-how: Mit Intercept X Advanced with EDR überträgt sich das Sicherheits-Know-how auf die IT – potenzielle Bedrohungen werden automatisch erkannt und priorisiert. Dank Machine Learning werden verdächtige Ereignisse erkannt und entsprechend ihrer Dringlichkeit priorisiert. So können Analysten schnell feststellen, worauf sie sich konzentrieren sollten und welche Systeme betroffen sein könnten.

Malware-Know-how: In den meisten Fällen verlassen sich Unternehmen auf MalwareExperten, die verdächtige Dateien per Reverse-Engineering analysieren. Diese Vorgehensweise ist zeitraubend und kompliziert, und viele Unternehmen verfügen auch nicht über das notwendige Fachpersonal. Die bessere Alternative: Intercept X Advanced with EDR mit Deep Learning-Malware-Analyse. Diese Funktion analysiert mit sehr hoher Genauigkeit automatisch Malware, indem sie Dateiattribute und Code aufschlüsselt und mit Millionen anderer Dateien vergleicht. So können Analysten schnell feststellen, welche Attribute und Code-Segmente Ähnlichkeit zu "als unschädlich bekannten" oder "als schädlich bekannten" Dateien aufweisen und können entscheiden, ob eine Datei blockiert oder erlaubt werden soll.

Bedrohungsdaten-Know-how: Wenn Intercept X Advanced with EDR eine potenziell verdächtige Datei anzeigt, können IT-Administratoren aktuelle Bedrohungsdaten aus den Sophos-Labs abrufen, um nähere Informationen zu erhalten. In unseren Sophos-Labs gehen täglich etwa 400.000 bislang unbekannte Malware-Samples ein und werden untersucht. Diese und weitere Bedrohungsdaten werden gesammelt und kategorisiert, um die Analyse so einfach wie möglich zu gestalten. Auf diese Weise können auch IT-Abteilungen, die nicht durch hochqualifiziertes

Lösung

Security & Identity

Produkt

Intercept X

Highlights

- EDR in Kombination mit dem stärksten Endpoint-Schutz
- Deep Learning-Malware-Analyse
- Jederzeit abrufbare Bedrohungsdaten aus den SophosLabs
- Machine Learning zur Erkennung und Priorisierung verdächtiger Ereignisse
- Schnell erreichbare leistungsstarle EDR dank geführter Analyse
- Reaktion auf Vorfälle mit einem einzigen Klick

Geführte Reaktion auf Vorfälle

Fachpersonal unterstützt werden oder kostspieligen Zugang zu komplexen Bedrohungsdaten haben, von weltweit führender Spitzenforschung in der Cybersecurity profitieren.

Dank Intercept X Advanced with EDR können Administratoren kritische Fragen zu Sicherheitsvorfällen klären, da sie einen detaillierten Einblick erhalten: Wo hatte der Angriff seinen Ursprung, welche Bereiche sind betroffen und welche Maßnahmen sollten ergriffen werden? Auf diese Weise erhalten auch weniger spezialisierte IT-Abteilungen schnell einen Überblick über ihren Sicherheitsstatus, denn geführte Analysen enthalten Empfehlungen für nächste Schritte, eine verständliche visuelle Darstellung des Angriffs sowie integriertes Know-how.

Nach Abschluss einer Analyse können IT-Mitarbeiter mit nur einem Klick schnell reagieren und z.B. Endpoints isolieren, um sie sofort zu bereinigen, Dateien entfernen/blockieren oder einen forensischen Snapshot erzeugen.

Anwendungsfälle für intelligente DER

Intelligente Endpoint Detection and Response bedeutet: IT-Abteilungen haben ausreichend Einblick und das notwendige Know-how, damit sie die Fragen beantworten können, die aufkommen, wenn auf einen Sicherheitsvorfall reagiert werden muss.

Mit intelligenter EDR können IT-Abteilungen:

- Ausmaß und Folgen von Sicherheitsvorfällen verstehen
- Angriffe aufspüren, die eventuell noch nicht bemerkt wurden
- Im Netzwerk nach Indikatoren für eine Kompromittierung suchen
- Ereignisse für die weitere Analyse priorisieren
- Dateien analysieren und bestimmen, ob es sich um Bedrohungen oder potenziell unerwünschte Anwendungen handelt
- Jederzeit den aktuellen Sicherheitsstatus ihres Unternehmens melden

Zur Abwehr der vielfältigen Bedrohungen nutzt Intercept X Advanced with EDR ein umfassendes, hochentwickeltes Konzept zum Endpoint-Schutz und verlässt sich nicht auf einen einzelnen Sicherheitsansatz. Das bezeichnen wir als „Power of the Plus" – eine Kombination führender traditioneller und moderner Techniken. Intercept X Advanced with EDR kombiniert branchenweit erstklassige Malware-Erkennung, leistungsstarken Exploit-Schutz und intelligente Endpoint Detection and Response (EDR).

Zu den modernen Techniken gehören Deep Learning Malware-Erkennung, Exploit-Abwehr und spezielle Funktionen für Ransomware-Schutz. Zu den traditionellen Techniken gehören Virenschutz, Verhaltensanalysen, Erkennung von schädlichem Datenverkehr, Data Loss Prevention und mehr.

Intercept X Advanced with EDR kombiniert Endpoint Detection and Response-Funktionen mit den modernen Techniken von Intercept X und den traditionellen Techniken von Sophos Central Endpoint Protection. Und dies alles bieten wir in einer zentralen Lösung, in einem zentralen Agenten.

INTERCEPT X

Lösung

Security & Identity

Produkt

Intercept X

Highlights

- EDR in Kombination mit dem stärksten Endpoint-Schutz
- Deep Learning-Malware-Analyse
- Jederzeit abrufbare Bedrohungsdaten aus den SophosLabs
- Machine Learning zur Erkennung und Priorisierung verdächtiger Ereignisse
- Schnell erreichbare leistungsstarke EDR dank geführter Analyse
- Reaktion auf Vorfälle mit einem einzigen Klick

SOPHOS