Lösungsbeschreibung

Sophos Endpoint

Verhindern Sie Sicherheitsverstöße, Ransomware-Angriffe und Datenverluste

Sophos Intercept X ist die branchenweit führende Endpoint-Security-Lösung und sorgt mit mehreren Schutzschichten für einzigartigen Schutz vor komplexen Bedrohungen. Mit umfassenden Abwehrmaßnahmen werden die meisten Bedrohungen bereits gestoppt, bevor sie Systeme beeinträchtigen. Starke EDR/XDR-Tools ermöglichen IT- und Sicherheitsteams, Bedrohungen zu suchen, zu analysieren und darauf zu reagieren.

Anwendungsfälle

1 | PRÄVENTIVE CYBERSECURITY

Gewünschtes Ergebnis: Mehr Bedrohungen bereits im Vorfeld stoppen, um Risiken zu minimieren und den Arbeitsaufwand für Analysen und Reaktionsmaßnahmen zu reduzieren.

Lösung: Intercept X nutzt einen umfassenden Ansatz zum Schutz aller Endpoints und verlässt sich nicht auf eine einzelne Sicherheitstechnologie. Web, Anwendungs- und Peripherie-Kontrollen reduzieren die Angriffsfläche und blockieren gängige Angriffsvektoren. KI, Verhaltensanalysen, Anti-Ransomware, Anti-Exploit und weitere hochmoderne Technologien stoppen Bedrohungen schnell, bevor diese sich ausweiten.

2 | EINFACHE VERWALTUNG

Gewünschtes Ergebnis: Die Verwaltung vereinfachen, damit mehr Zeit bleibt für die Bedrohungsprävention, -erkennung und -reaktion.

Lösung: Bei uns erhalten sie mit Sophos Central eine cloudbasierte Management-Konsole, über die Sie alle Sophos-Produkte zentral verwalten sowie Bedrohungen suchen und analysieren können. Starke Standard-Richtlinieneinstellungen stellen sicher, dass Sie ohne zusätzliche Schulungen und Feinabstimmungen sofort über die empfohlenen Schutzeinstellungen verfügen. Mit dem integrierten Account Health Check können Sie Sicherheitsprobleme einfach erkennen und beheben.

3 | KONTEXTSENSITIVE ABWEHR

Gewünschtes Ergebnis: Abwehrmechanismen, die sich automatisch an die Entwicklung eines Angriffs anpassen.

Lösung: Wenn Intercept X einen manuellen Angriff erkennt, werden auf dem Endpoint automatisch zusätzliche Abwehrmaßnahmen aktiviert, um ein Fortschreiten des Angriff zu verhindern. Adaptive Attack Protection blockiert verdächtige Aktivitäten wie das Herunterladen von Remote-Admin-Tools und gibt Ihrem Team wertvolle Zeit, um zu reagieren.

4 | DETECTION AND RESPONSE

Gewünschtes Ergebnis: Bedrohungen erkennen und beseitigen, die nicht allein durch Schutzmaßnahmen bekämpft werden können.

Lösung: Unsere leistungsstarken EDR/XDR-Funktionen können mit Sicherheitstools von Sophos und anderen Herstellern genutzt werden. Sie ermöglichen Ihnen, verdächtige Aktivitäten zu suchen, zu analysieren und darauf zu reagieren – z. B. eine Datenexfiltration oder stille Angreifer, die keinen Schadcode verwenden. Wenn Sie nicht ausreichend interne Ressourcen haben, um sich selbst um Ihre Cybersicherheit zu kümmern, können Sie unseren MDR-Service in Anspruch nehmen, bei dem ein Expertenteam 24/7 für Ihre Sicherheit sorgt.

Gartner

Zum vierzehnten Mal in Folge ein Leader im Gartner Magic Quadrant for Endpoint Protection Platforms

SE Labs

Branchenführende Schutzergebnisse in unabhängigen Produkttests

THE CHANNEL CO. CRN TECH INNOVATORS 2023

Beste Endpoint Security in den CRN Tech Innovators Awards (Juli 2023)

Mehr erfahren und Sophos Intercept X testen:
sophos.de/endpoint

2024-01-15 SB-DE (PC)

SOPHOS