

Sophos XDR

Abwehr gegen aktive Angreifer mit EDR und XDR



Angreifer entwickeln ihre Techniken ständig weiter, um Schwachstellen auszunutzen und ihre Angriffe noch schneller und effizienter auszuführen. Noch nie war es so wichtig, Angreifer schnellstmöglich zu erkennen und Reaktionsmaßnahmen einzuleiten. Mit der zentralen XDR-Plattform (Extended Detection and Response) von Sophos erkennen, analysieren und bekämpfen Sie mehrphasige Bedrohungen und aktive Angreifer in Ihrem gesamten Security-Ökosystem jetzt noch schneller.

Anwendungsfälle

1 | STARKE ABWEHR ALS GRUNDLAGE FÜR EFFEKTIVEN SCHUTZ

Gewünschtes Ergebnis: Mehr Bedrohungen im Vorfeld stoppen, um Ihren Workload zu reduzieren.

Lösung: Konzentrieren Sie sich auf fokussierte Analysen, indem Sie Sicherheitsverstöße schon im Vorfeld verhindern. Sophos XDR bietet einzigartigen Schutz, der komplexe Bedrohungen schnell stoppt, bevor sie sich ausweiten. Schützen Sie Endpoints und Server mit modernsten Technologien wie KI, Verhaltensanalyse, Anti-Ransomware und Anti-Exploit-Technologie.

2 | SCHNELLERE REAKTION AUF BEDROHUNGEN

Gewünschtes Ergebnis: Bedrohungen schnell erkennen, analysieren und auf diese reagieren.

Lösung: KI-priorisierte Erkennungen, die auf Threat Intelligence von Sophos X-Ops basieren, ermöglichen ein schnelles und einfaches Erkennen verdächtiger Ereignisse, die sofortige Aufmerksamkeit erfordern. Führen Sie Threat Hunts durch und reagieren Sie blitzschnell – mit optimierten Analyse-Workflows, leistungsstarken Suchfunktionen, kollaborativer Fallmanagement-Software und automatischen Reaktionsmaßnahmen.

3 | TRANSPARENZ ÜBER ANGRIFFSFLÄCHEN

Gewünschtes Ergebnis: Für alle wichtigen Angriffsflächen vollständige Transparenz über evasive Bedrohungen erhalten.

Lösung: Nutzen Sie die vollständig integrierten und XDR-fähigen Lösungen von Sophos, um über die Endpoint-Ebene hinaus Einsicht in alle Vorgänge zu erhalten, oder greifen Sie auf bereits vorhandene Technologien zurück. Erstellen Sie mit unserer zentralen XDR-Plattform ein eng vernetztes Ökosystem aus Endpoint-, Firewall-, Netzwerk-, E-Mail-, Identity- und Cloud-Sicherheitslösungen, über das Sie Bedrohungen schnell erkennen und Reaktionsmaßnahmen einleiten können.

4 | MEHR EFFIZIENZ FÜR INTERNE SOCS UND IT-ADMINISTRATOREN

Gewünschtes Ergebnis: Sicherheitsanalysten und IT-Generalisten können einfach Analysen durchführen und Reaktionsmaßnahmen ergreifen.

Lösung: Sophos XDR sorgt für mehr Effizienz und eignet sich sowohl für dedizierte interne SOC-Teams als auch für Administratoren, die Sicherheits- und andere IT-Aufgaben übernehmen. Vollständige Transparenz und konkrete Anweisungen helfen Ihnen, schnell und effektiv auf Bedrohungen zu reagieren.

Gartner

Im Gartner Market Guide für XDR 2023 ausgezeichnet

**MITRE
ATT&CK**

Herausragende Ergebnisse bei den MITRE Engenuity ATT&CK Evaluations 2023

G2 Leader

Von G2-Benutzern als die Nr. 1 unter den XDR-Lösungen eingestuft (Frühjahr 2023)

Mehr erfahren und Sophos XDR testen:
sophos.de/xdr