Sophos Managed Detection and Response

Upptäcker och hanterar hot dygnet runt

Sophos MDR är en komplett dygnet runt-tjänst som levereras av experter och upptäcker och hanterar cyberattacker som riktar in sig på dina datorer, servrar, nätverk, arbetslaster i molnmiljöer, e-postkonton och mer.

Tjänster för förebyggande av ransomware-incidenter och dataintrång

Säkerhetsåtgärder har blivit ett absolut måste för företag. De moderna driftmiljöernas komplexitet och cyberhotens hastighet gör det dock allt svårare för de flesta organisationer att själva upptäcka och bekämpa dessa hot.

Med Sophos MDR stoppar våra experter avancerade hackerattacker. Vi vidtar åtgärder för att neutralisera hot innan de kan störa din affärsverksamhet eller äventyra dina känsliga data. Sophos MDR kan anpassas med olika servicenivåer och levereras via vår patentskyddade teknik eller med hjälp av dina befintliga investeringar i cybersäkerhetsteknik.

Cybersäkerhet som en tjänst

Sophos MDR:s utökade egenskaper för att upptäcka och hantera (XDR) dataintrång ger en komplett säkerhetstäckning oavsett var du lagrar dina data. Dessutom kan Sophos MDR:

- **Upptäcka fler cyberhot än säkerhetsverktyg kan identifiera på egen hand**
  Våra verktyg blockerar automatiskt 99,98 % av alla hot, vilket gör att våra analytiker kan fokusera på att spåra upp de mest sofistikerade hackarna, som bara kan upptäckas och stoppas av en expert.
- **Vidta åtgärder för att stoppa hot från att störa din affärsverksamhet**
  Våra analytiker upptäcker, undersöker och hanterar hot på några få minuter – oavsett om du behöver ett fullskaligt svar på incidenter eller hjälp med att fatta rätt beslut.
- **Identifiera hotets bakomliggande orsak för att förhindra framtida incidenter**
  Vi vidtar proaktivt åtgärder och ger rekommendationer som minskar risken för din organisation. Färre incidenter betyder färre störningar för din IT- och säkerhetspersonal, dina medarbetare och dina kunder.

Kompatibelt med dina befintliga cybersäkerhetsverktyg

Vi kan tillhandahålla tekniken du behöver med hjälp av våra prisbelönta produkter, eller så kan våra analytiker använda sig av din befintliga cybersäkerhetsteknik för att upptäcka och hantera hot.

Sophos MDR är kompatibelt med säkerhetstelemetri från leverantörer som Microsoft, CrowdStrike, Palo Alto Networks, Fortinet, Check Point, Rapid7, Amazon Web Services (AWS), Google, Okta, Darktrace och många fler. Tjänsterna konsolideras, korreleras och prioriteras automatiskt med insikter från Sophos Adaptive Cybersecurity Ecosystem (ACE) och underrättelseenheten Sophos X-Ops.

Höjdpunkter

- Stoppa ransomware-attacker och andra avancerade hackerattacker med ett expertteam som är tillgängligt dygnet runt för hantering av hot
- Maximera ROI på dina befintliga cybersäkerhetstekniker
- Låt Sophos MDR utföra en fullskalig incidenthantering, arbeta med dig för att hantera säkerhetsincidenter, leverera detaljerade meddelanden om hot och ge vägledning
- Förbättra cyberförsäkringens omfattning med dygnet runt-övervakning och kapacitet för EDR (Endpoint Detection and Response)
- Se till att dina interna IT- och säkerhetsmedarbetare kan fokusera på affärsmöjligheter

SOPHOS

MDR anpassad efter dina behov

Sophos MDR kan anpassas med olika servicenivåer och alternativ för att hantera hot. Låt Sophos MDR-team utföra en fullskalig incidenthantering, arbeta med dig för att hantera cyberhot eller informera ditt interna säkerhetsteam så fort ett hot upptäcks. Vårt team lär sig snabbt vem, vad, när och hur i fråga om en attack. Vi kan hantera hot på några få minuter.

Viktiga funktioner

Upptäcker och hanterar hot dygnet runt

Vi upptäcker och hanterar hot innan de kan äventyra dina data eller orsaka driftstopp. Med hjälp av sex globala säkerhetscentraler (SOC) erbjuder Sophos MDR skydd dygnet runt.

Kompatibelt med säkerhetsverktyg från andra leverantörer än Sophos

Sophos MDR kan integrera telemetri från tredje parts klient-, brandväggs-, identitets- och e-posttekniker samt andra säkerhetstekniker som del av Sophos ACE.

Fullskalig incidenthantering

När ett aktivt hot har identifierats kan Sophos MDR-team utföra en omfattande uppsättning motåtgärder för att störa, hålla tillbaka och eliminera hackaren.

Vecko- eller månadsrapportering

Sophos Central är den enda instrumentpanel du behöver för varningar, rapportering och styrning i realtid. Vecko- och månadsrapporter ger insikt i säkerhetsundersökningar, cyberhot och ditt säkerhetsläge.

Sophos Adaptive Cybersecurity Ecosystem

Sophos ACE förhindrar automatiskt kriminell aktivitet och gör det möjligt för oss att söka efter svaga signaler om hot som det krävs att en person upptäcker, undersöker och eliminerar.

Expertledd hotspårning

Proaktiv hotspårning utförd av expertanalytiker avslöjar och eliminerar snabbt fler hot än säkerhetsprodukter kan upptäcka på egen hand. Sophos MDR-teamet kan även använda telemetri från tredjepartsleverantör för att spåra hot och identifiera hackarbeteenden som har undsluppit upptäckt av använda verktygsuppsättningar.

Direkt telefonsupport

Dina medarbetare kan ringa vår säkerhetscentral (SOC) direkt för att granska potentiella hot och aktiva incidenter. Sophos MDR-team är tillgängligt dygnet runt och stöds av supportteam på 26 platser världen över.

Dedikerad incidenthanteringsansvarig

Vi ger dig en dedikerad incidenthanteringsansvarig som samarbetar med ditt interna team och externa partner så fort vi identifierar en incident och arbetar med dig tills incidenten är hanterad.

Analys av grundorsak

Förutom att ge dig proaktiva rekommendationer för att förbättra ditt säkerhetsläge utför vi även en analys av grundorsaken för att identifiera de underliggande problemen som ledde till en incident. Vi vägleder dig i att ta itu med säkerhetsbrister så att de inte kan utnyttjas i framtiden.

Hälsokontroll av Sophos-konto

Vi granskar kontinuerligt inställningar och konfigurationer för klienter som hanteras av Sophos XDR och säkerställer att de körs på toppnivå.

Begränsning av hot

För organisationer som väljer att Sophos MDR inte ska utföra fullskalig incidenthantering kan Sophos MDR-teamet utföra begränsande åtgärder som stör hotet och förhindrar spridning. Detta minskar arbetsbelastningen för interna säkerhetsteam och gör att de snabbt kan vidta hjälpåtgärder.

Informationsbriefing: ”Sophos MDR ThreatCast”

”Sophos MDR ThreatCast” levereras av Sophos MDR-team och är en månatlig briefing som är tillgänglig exklusivt för Sophos MDR-kunder. Den ger insikt i den senaste hotinformationen och bästa säkerhetspraxis.

Breach Protection Warranty

Garantin ingår i Sophos MDR Complete, Årsavtal (1-5 år) samt månads licenser och täcker upp till 1 miljon USD i svarsutgifter. Det finns inga garantinivåer, minimiavtalsvillkor eller ytterligare köpkrav.

Sophos servicenivåer

	Sophos hotrådgivare	Sophos MDR	Sophos MDR Complete
Expertledd hotspårning och hothantering	✓	✓	✓
Kompatibelt med säkerhetsverktyg från andra leverantörer än Sophos	✓	✓	✓
Vecko- eller månadsrapportering	✓	✓	✓
Månatlig informationsbriefing: "Sophos MDR ThreatCast"	✓	✓	✓
Hälsokontroll av Sophos-konto		✓	✓
Expertledd hotspårning		✓	✓
Begränsning av hot: attacker störs, förhindrar spridning Använder komplett Sophos XDR-verktygsset (skydd, upptäckt och hantering) eller Sophos XDR Sensor (upptäckt och hantering)		✓	✓
Direkt telefonsupport vid aktiva incidenter		✓	✓
Fullskalig incidenthantering: hot elimineras Kräver komplett Sophos XDR-verktygsuppsättning (skydd, upptäckt och hantering)			✓
Analys av grundorsak			✓
Dedikerad ansvarig för incidenthantering			✓
Breach Protection Warranty Täcker upp till 1 miljon USD i svarsutgifter			✓

Inkluderade Sophos MDR-integrationer

Säkerhetsdata från följande källor kan integreras för användning av Sophos MDR-teamet utan extra kostnad. Telemetrikällor används för att öka synligheten tvärs över din miljö, generera nya hotupptäckter och förbättra exaktheten på befintliga tjänster för hotupptäckt, utföra hotspårning och möjliggöra ytterligare egenskaper för hantering av hot.

Sophos XDR

Den enda XDR-plattformen som kombinerar klient-, server-, brandväggs-, moln-, e-post-, mobil- och Microsoft-integrationer

Ingår i priset för Sophos MDR och Sophos MDR Complete

Sophos Firewall

Övervaka och filtrera inkommande och utgående nätverkstrafik för att stoppa avancerade hot innan de kan orsaka skada

Produkten säljs separat, integreras utan extra kostnad

Microsoft Graph Security

- Microsoft Defender for Endpoint
- Microsoft Defender for Cloud
- Microsoft Defender for Cloud Apps
- Microsoft Defender for Identity
- Identity Protection (Azure AD)
- Microsoft Azure Sentinel
- Office 365 Security and Compliance Center
- Azure Information Protection

Sophos Endpoint

Blockera avancerade hot och upptäck kriminella beteenden – inklusive hackare som imiterar legitima användare

Ingår i priset för Sophos MDR och Sophos MDR Complete

Sophos Email

Skydda din inkorg mot skadliga program och dra nytta av avancerad AI som stoppar målinriktade imitations- och nätfiskeattacker

Produkten säljs separat, integreras utan extra kostnad

Office 365 Management Activity

Ger information om användare, administratörer, system och policyhändelser från loggar i Office 365 och Azure Active Directory

Sophos Cloud

Stoppa intrång i molnet och få synlighet tvärs över dina kritiska molntjänster, inklusive AWS, Azure och Google Cloud Platform

Produkten säljs separat, integreras utan extra kostnad

90 dagars datalagring

Lagrar data från alla Sophos-produkter och eventuella produkter från tredje part (ej Sophos) i Sophos Data Lake

Klientskydd från tredje part

Kompatibelt med ...

- Microsoft
- CrowdStrike
- SentinelOne
- Trend Micro
- Trellix
- BlackBerry (Cylance)
- Symantec (Broadcom)
- Malwarebytes

Tilläggsintegrationer

Säkerhetsdata från följande tredjepartskällor kan integreras för användning av Sophos MDR-teamet via köp av integrationspaket. Telemetrikällor används för att öka synligheten tvärs över din miljö, generera nya hotupptäckter och förbättra exaktheten på befintliga tjänster för hotupptäckt, utföra hotspårning och möjliggöra ytterligare egenskaper för hantering av hot.

Sophos Network Detection and Response

Övervaka kontinuerligt aktivitet inuti ditt nätverk för att upptäcka misstänkta handlingar som sker mellan enheter som annars är osedda

Kompatibelt med valfritt nätverk via SPAN-portspegling

Brandvägg

Kompatibelt med ...

- Palo Alto Networks
- Fortinet
- Check Point
- Cisco
- SonicWall

Identity

Kompatibelt med ...

- Okta
- Duo
- ManageEngine

Public Cloud

Kompatibelt med ...

- AWS Security Hub
- AWS CloudTrail
- Orca Security
- Google Cloud Platform Security

E-post

Kompatibelt med ...

- Proofpoint
- Mimecast

Network

Kompatibelt med ...

- Darktrace
- Tinkst Canary
- Skyhigh Security

1-Year Data Retention

Vägledd Sophos MDR-onboarding

Som komplement är vägledd Sophos MDR-onboarding tillgänglig för fjärrassistans vid onboarding. Tjänsten erbjuder praktisk support för en smidig och effektiv användning, säkerställer konfigurationer för bästa praxis och levererar träning för att maximera värdet av din MDR-investering. Du tilldelas en dedikerad kontakt i Sophos Professional Services-organisation som är med dig under de första 90 dagarna för att säkerställa att din implementering lyckas. Vägledd Sophos MDR-onboarding inkluderar:

Dag 1 – implementering

- Projektkickoff
- Konfiguration av Sophos Central och granskning av funktioner
- Bygg och test av implementeringsprocesser
- Konfiguration av MDR-integrationer
- Konfiguration av Sophos NDR-sensorer
- Företagsomfattande implementering

Dag 30 – XDR-träning

- Lär dig att tänka och agera som en säkerhetscentral
- Förstå hur du spårar kompromissindikatorer
- Få en förståelse för hur du använder vår XDR-plattform för administrativa uppgifter
- Lär dig att konstruera förfrågningar för framtida undersökningar

Dag 90 – bedömning av säkerhetsläge

- Granska befintliga policyer för rekommendationer om bästa praxis
- Diskutera oanvända funktioner som skulle kunna ge ytterligare skydd
- Säkerhetsbedömning enligt NIST-ramverk
- Motta sammanfattande rapport med rekommendationer från vår granskning

För mer information, gå till

sophos.com/mdr

Sverige Sälj
Telefon: +46 858 400 600
E-post: sweden.sales@sophos.com

23-01-24 DS-SE (PC)

SOPHOS