SLUŽBA / DATASHEET

SOPHOS

Bezpečnost v režii expertů výrobce.

Sophos MDR je plně spravovaná služba 24/7. Analytici výrobce odhalují, vyšetřují a zastavují útoky vedené lidmi dříve, než naruší Váš byznys - na koncových bodech, serverech, v sítích, cloudu i e-mailu.

99,98 %	24/7/365	6	$1 M
automaticky blokovaných hrozeb	nepřetržitý monitoring	globálních SOC center	Breach Warranty v MDR Complete

HROZBA

Ransomware a útoky vedené lidmi

Složitost moderních prostředí a rychlost útočníků ztěžují firmám vlastní detekci a reakci. Sophos MDR pomáhá zastavit pokročilé útoky dříve, než ohrozí data, provoz nebo obchodní kontinuitu.

PŘÍSTUP

Kybernetická bezpečnost jako služba

Díky XDR poskytuje širší viditelnost napříč prostředím. Sophos může jednat Vaším jménem v řádu minut, identifikovat hlavní příčinu incidentu a doporučit kroky pro snížení budoucího rizika.

KOMPATIBILITA

Pracuje s tím, co už máte

MDR lze dodat přes technologii Sophos nebo s využitím Vašich stávajících bezpečnostních nástrojů. Telemetrie je konsolidována, korelována a prioritizována v Sophos ACE a Sophos X-Ops.

KLÍČOVÉ VÝHODY

Co tím získáte

- Ochrana 24/7/365
- Obrana proti ransomware a hrozbám
- Reakce během minut
- Externí SOC bez zátěže interního týmu
- Přímý support, IR leader a RCA
- Breach Protection Warranty u MDComplete
- Redukce nákladů na školení interního týmu
- Celkové snížení nákladů na IT bezpečnost

PŘÍKLAD INTEGROVATELNÝCH TECHNOLOGIÍ

CrowdStrike	Rapid7	Check Point	AWS	Microsoft
Google	Palo Alto	Okta	Fortinet	Darktrace

SOPHOS

JAK TO FUNGUJE?

Reakce v řádu minut. Ne dnů.

Sophos MDR nabízí různé úrovně služby. Můžete delegovat plnou reakci na incidenty, spolupracovat na jejich řízení, nebo nechat upozornění směrovat do interního bezpečnostního týmu.

24/7	Monitoring a reakce Šest globálních SOC poskytuje nepřetržité pokrytí. Hrozby jsou detekovány a zastavovány dříve, než ohrozí data nebo způsobí výpadek.
XDR	Rozšířená detekce XDR rozšiřuje viditelnost napříč endpointy, servery, cloudem, sítí a e-mailem.
IR	Reakce na incident Při aktivní hrozbě může tým vzdáleně narušit aktivitu útočníka, zabránit dalšímu šíření a eliminovat jeho další akce.
HUNT	Threat hunting Vysoce vyškolení analytici proaktivně hledají signály hrozeb, které samotné bezpečnostní produkty nemusí odhalit.
RCA	Root Cause Analysis a doporučení Analýza příčin incidentu a proaktivní doporučení pomáhají snížit riziko opakování útoku.
SOC	Přímý support 24/7 Call-in přístup k Sophos SOC pro kontrolu potenciálních hrozeb a aktivních incidentů.
OWN	Dedikovaný incident leader Specialista funguje jako garant, průvodce a incident response leader až do úplného vyřešení incidentu.
REP	Reporting a Sophos Central Jeden dashboard pro alerty v reálném čase, reporting a management. Součástí jsou týdenní a měsíční přehledy.

SOPHOS

Sophos ekosystém bez zbytečné složitosti

- Sophos XDR, Sophos Firewall, Sophos Endpoint, Sophos Email a Sophos Cloud
- Microsoft Graph Security a MS Office 365 Management Activity
- Endpoint ochrana třetích stran: Trellix, Microsoft,
- CrowdStrike, SentinelOne, Symantec, Trend Micro a další
- 90denní retence dat v základním Sophos ekosystému

Rozšíření o 3rd party technologie

- Integrační balíčky: Network Detection and Response, Firewall, Identity, Public Cloud, Email a Network
- Roční retence dat podle zvolených integračních balíčků
- Telemetrie z endpointů, firewallů, identit, e-mailu, cloudu a dalších bezpečnostních technologií
- Automatická konsolidace, korelace a prioritizace dat v Sophos ACE a X-Ops

ÚROVEŇ SLUŽBY

Vyberte míru zapojení podle potřeb týmu.

Sophos MDR lze nastavit podle toho, zda chcete upozorňování a řízenou reakci, spolupráci s interním týmem, nebo plnou reakci na incidenty v režii odborníků výrobce.

Funkce služby	ESSENTIALS	COMPLETE
Nepřetržité sledování hrozeb a reakce pod vedením odborníků	✓	✓
Kompatibilita s bezpečnostními produkty jiných výrobců	✓	✓
Týdenní a měsíční reporting	✓	✓
Měsíční zpravodajský briefing Sophos MDR ThreatCast	✓	✓
Kontrola stavu účtu Sophos	✓	✓
Lov hrozeb vedený odborníky	✓	✓
Omezení hrozby - přerušení útoku a zabránění šíření	✓	✓
Přímá podpora po zavolání během aktivních incidentů	✓	✓
Úplná reakce na incident - kompletní eliminace hrozby	-	✓
Analýza kořenových příčin	-	✓
Vyhrazený pracovník pro reakci na incidenty	-	✓
Breach Protection Warranty až do výše 1 milionu USD	-	✓

* Upozornění: Funkce „Úplná reakce na incident“ (kompletní eliminace hrozby) vyžaduje nasazení plnohodnotného agenta Sophos XDR (ochrana, detekce a reakce).

SOPHOS

ÚROVEŇ SLUŽBY

Sophos MDR Essentials

- Detekce, vyšetřování a reakce
- Monitoring 24/7 a threat hunting
- Reakce na hrozby a omezení šíření
- Týdenní/měsíční reporting a ThreatCast

ÚROVEŇ SLUŽBY

Sophos MDR Complete

- Vše z Essentials + plná reakce na incident
- Root Cause Analysis
- Dedikovaný IR leader
- Breach Protection Warranty do $1 M

Breach Protection Warranty

Součást Sophos MDR Complete bez dalších nákladů. Krytí škod způsobených útočníkem až do $1 000 000; vztahuje se na endpointy, servery a další zařízení běžící pod Windows a macOS.

Máte zájem o bezprecedentní úroveň ochrany Sophos MDR?
Pro nezávaznou konzultaci, nacenění nebo technické detaily kontaktujte distributora: **SCENARIO S.R.O**

scenario

Tel.: +420 602 111 071
E-mail: strachota@scenario.cz
Web: www.it.scenario.cz