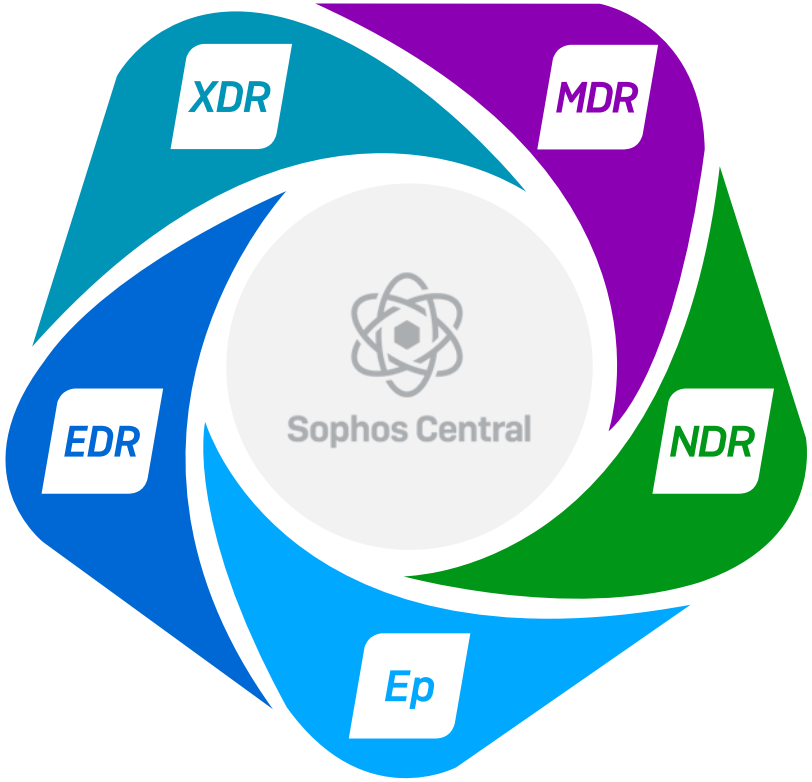
Sophos végpontvédelem

EDR, XDR, MDR és egyéb betűszavak…

Sophos Detection and Response megoldások

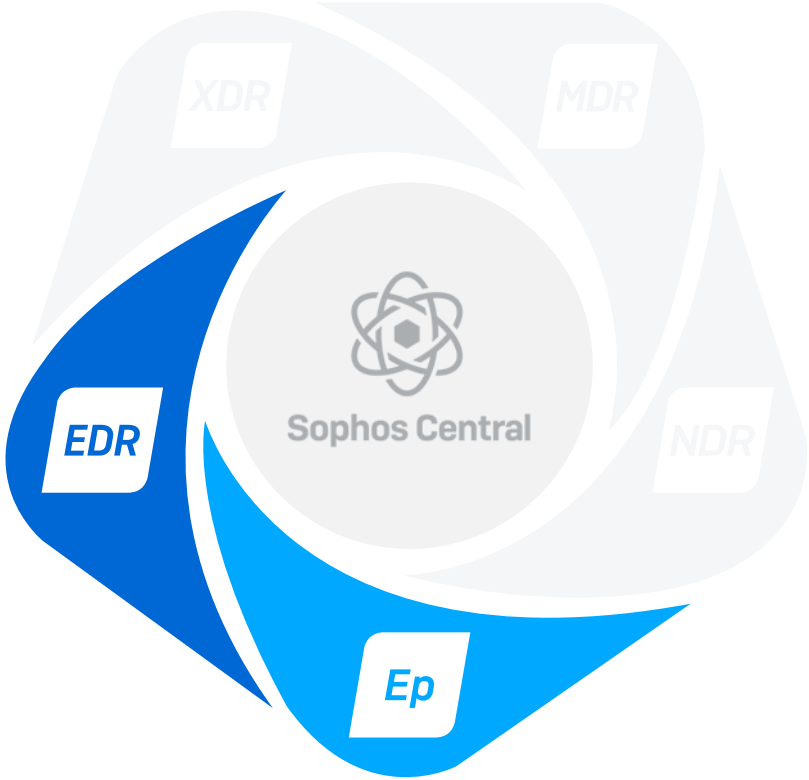


Sophos Detection and Response megoldások

Endpoint Protection

Sophos Detection and Response megoldások

Endpoint Detection and Response



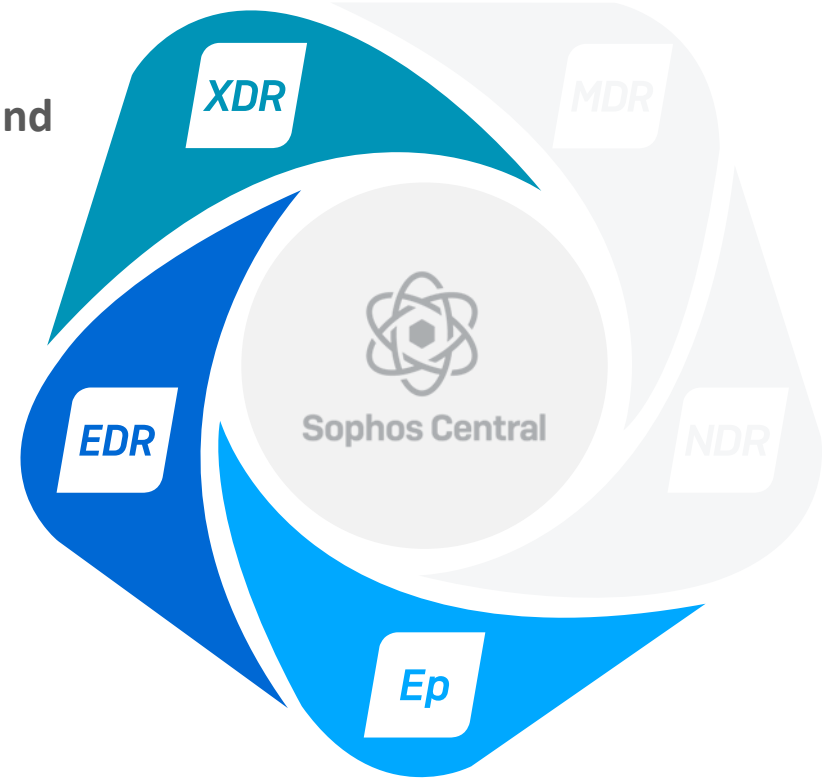
Endpoint Protection

SOPHOS

Sophos Detection and Response megoldások

Extended Detection and Response

Endpoint Detection and Response



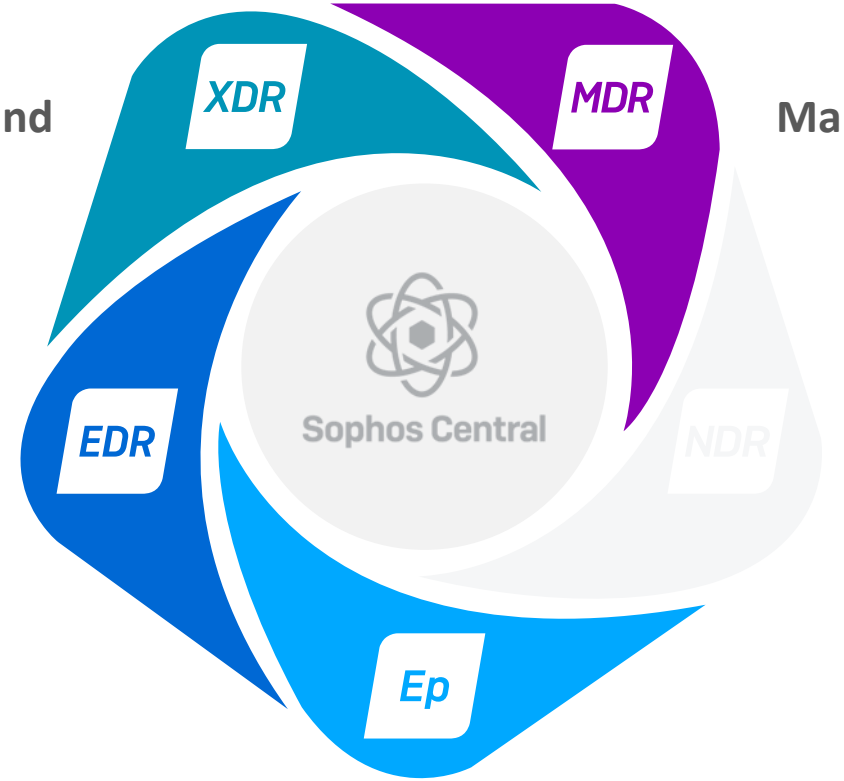
Endpoint Protection

SOPHOS

Sophos Detection and Response megoldások

Extended Detection and Response

Managed Detection and Response



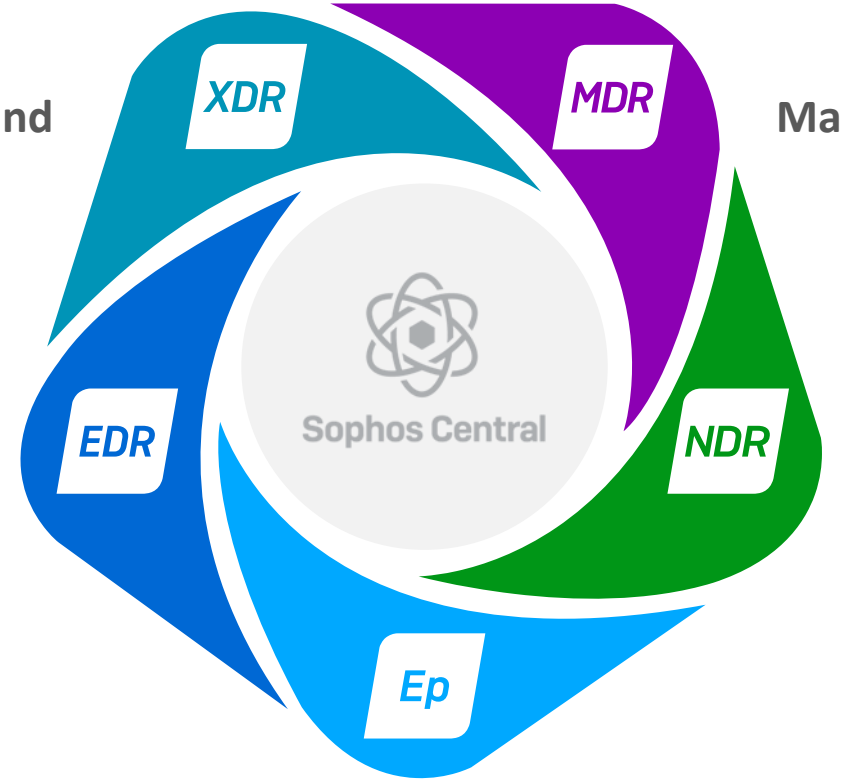
Endpoint Detection and Response

Endpoint Protection

Sophos Detection and Response megoldások

Extended Detection and Response

Managed Detection and Response



Endpoint Detection and Response

Network Detection and Response

Endpoint Protection

Sophos Detection and Response megoldások

MDR	Védelem az újszerű, kifinomult fenyegetésekkel és a fejlett aktív támadásokkal szemben. Magasan képzett szakemberek által nyújtott kiemelkedő minőségű 24/7 szolgáltatás.
XDR	Szakértői eszközök: lehetővé teszik az olyan összetett kártevők vizsgálatát és visszafejtését a teljes támadási felületen, amelyeket a műszaki megoldások maguktól nem képesek blokkolni.
EDR	Szakértői eszközök: lehetővé teszik az olyan összetett kártevők vizsgálatát és visszafejtését a munkaállomásokon és a szervereken, amelyeket a műszaki megoldások maguktól nem képesek blokkolni.
Ep	Az erős végpontvédelem alapkövetelmény. Minél több fenyegetést állít meg a rendszer automatikusan, annál kevesebb esetet kell kivizsgálnia és lereagálnia az IT biztonsági csapatnak.

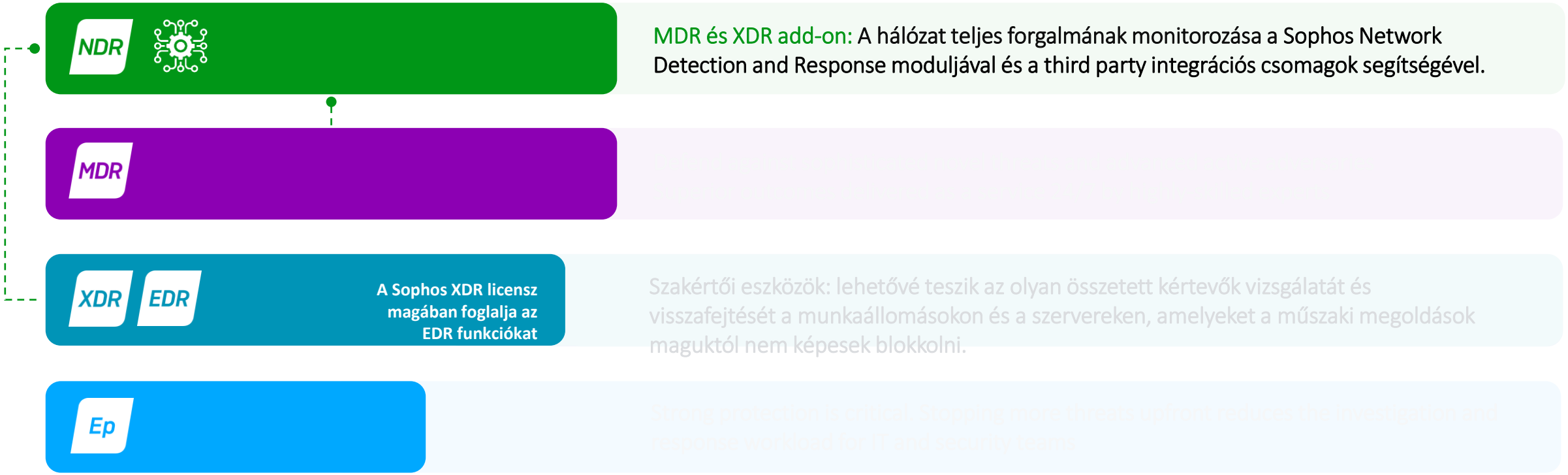
Sophos Detection and Response megoldások

Védelem az újszerű, kifinomult fenyegetésekkel és a fejlett aktív támadásokkal szemben. Magasan képzett szakemberek által nyújtott kiemelkedő minőségű 24/7 szolgáltatás.

Szakértői eszközök: lehetővé teszik az olyan összetett kártevők vizsgálatát és visszafejtését a teljes támadási felületen, amelyeket a műszaki megoldások maguktól nem képesek blokkolni.

Az erős végpontvédelem alapkövetelmény. Minél több fenyegetést állít meg a rendszer automatikusan, annál kevesebb esetet kell kivizsgálnia és lereagálnia az IT biztonsági csapatnak.

Sophos Detection and Response megoldások



Sophos végpontvédelem

A végpontvédelem amely önért és önnel dolgozik

A Sophos védelme adaptívan reagál a támadásokra

Sophos Endpoint

Az erős védelem létfontosságú. Minimalizálja a élő munkával vizsgálandó esetek számát.

A Sophos erőssége

Adaptív védelem
Pajzsokat fel: a védelem szintje automatikusan növekszik a támadásra utaló jelek esetén.

Univerzális Anti-ransomware
Hatékony védelem a helyi és távoli támadások ellen.

A legerősebb védelem már az alapbeállításokkal is
Telepítse és felejtse el – nincs szükség konfigurációra.

SE Labs
Consistent AAA Ratings

IDC
2024 MarketScape Leader

Gartner peerinsights
Customer's Choice

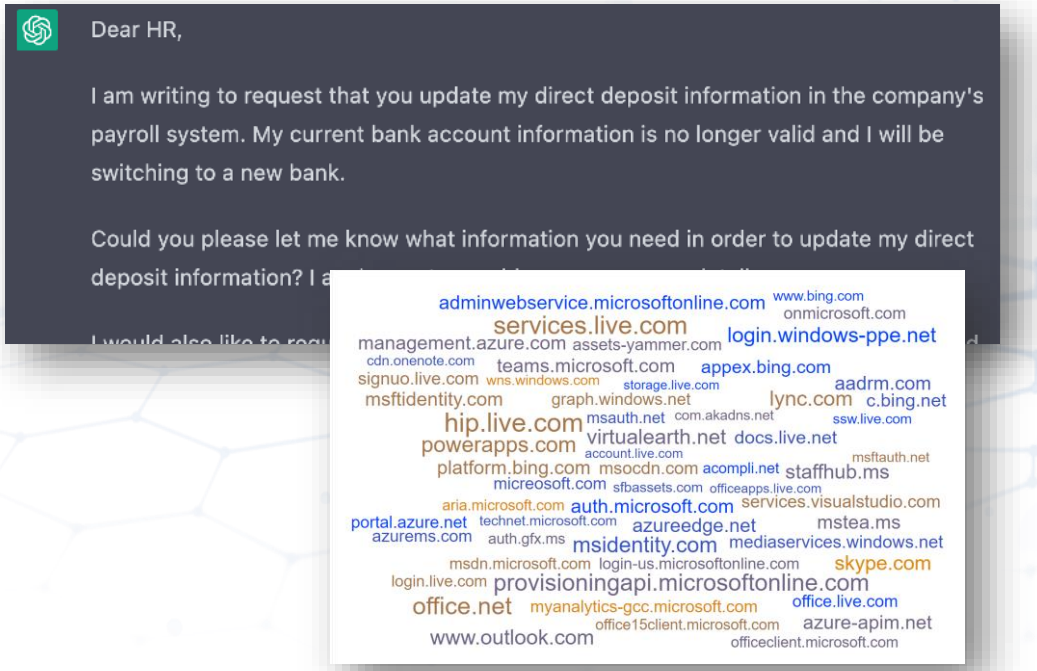
Gartner
EPP MQ Leader

Webes fenyegetések blokkolása

Állítsuk meg a kártevőket mielőtt azok célba érnének

Bajban a biztonsági tudatosságot célzó oktatások

A felhasználók számára egyre bonyolultabb a kártékony linkek és weboldalak észlelése.



Webszűrés

Phishing és más kártékony oldalak elérésének blokkolása

Állományok, weboldalak és IP címek elemzése

Folyamatos és gyakori frissítések

A Sophos Threat Intelligence támogatásával

SophosLabs: vírusszakértők globális csoportja

Real-time információk a Sophos Managed Detection & Response threat hunting specialistáitól

Felügyelet és kontroll

Webkontroll

A weboldalak látogatásának kategória alapú monitorozása vagy blokkolása, a rendszergazda által konfigurálhatóan.

Eszközfelügyelet

A perifériák és a hordozható meghajtók elérésének szabályozása.

Alkalmazáskontroll

A munkahelyi környezetben kéretlen alkalmazások észlelése és blokkolása.

Adatfelügyelet

Érzékeny információkat tartalmazó állományok másolásának monitorozása és tiltása.

SOPHOS

Viselkedési motor

Memóriavédelem

Futó processzek vizsgálata kártékony kódok után az állománymentes támadások ellen

További helyreállítási képességek

Alapos és szigorú tisztítási protokoll a támadások elhárítása után

SOPHOS

Anti-Exploitation technológia

Alkalmazásvédelem

Ember által kontrollált aktív támadás esetén megerősíti a processzek manipuláció elleni védelmét

Zero Trust Protection

Alapos és szigorú tisztítási protokoll a támadások elhárítása után

Független működés

Adatbázistól, gépi tanulástól vagy felhős erőforrásoktól függetlenül is működőképes

SOPHOS

Ransomware védelem

Szigorú ransomware védelem

A legmegbízhatóbb zero-touch végpontvédelem a zsarolóvírusok ellen

Zsarolóvírus technikák

A zsarolóvírusok sokféle formában érkezhetnek

- Felülíró titkosítás
- Időszakos titkosítás
- Távoli titkosítás
- Boot szintű titkosítás

Sophos Endpoint

A forrástól függetlenül blokkolja a ransomware támadásokat

Az állományok tartalmának elemzésével észleli a kártékony célú titkosítási kísérleteket

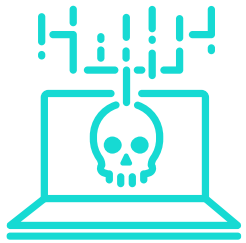
Blokkolja a helyi és a távoli titkosítóvírus támadást

Automatikusan visszaállítja az érintett állományokat méret és típus korlátozások nélkül

Automatikusan blokkolja a távoli meghajtókat

Megvédi a master boot recordot (MBR)

SOPHOS



Remote Ransomware Protection

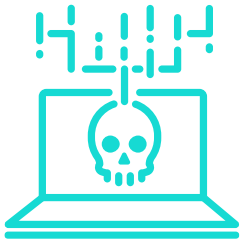
Egyedi anti-ransomware technológia, amely blokkolja ezt az új és népszerű kártékony titkosítási módszert.

A távoli titkosítás használata erőteljesen megnövekedett.

Az ember által végrehajtott zsarolóvírus-támadások átlagosan 60 százaléka használt távoli titkosítást - ez annak a jele, hogy a támadók a felderítés elkerülése érdekében továbbfejlesztették taktikájukat.

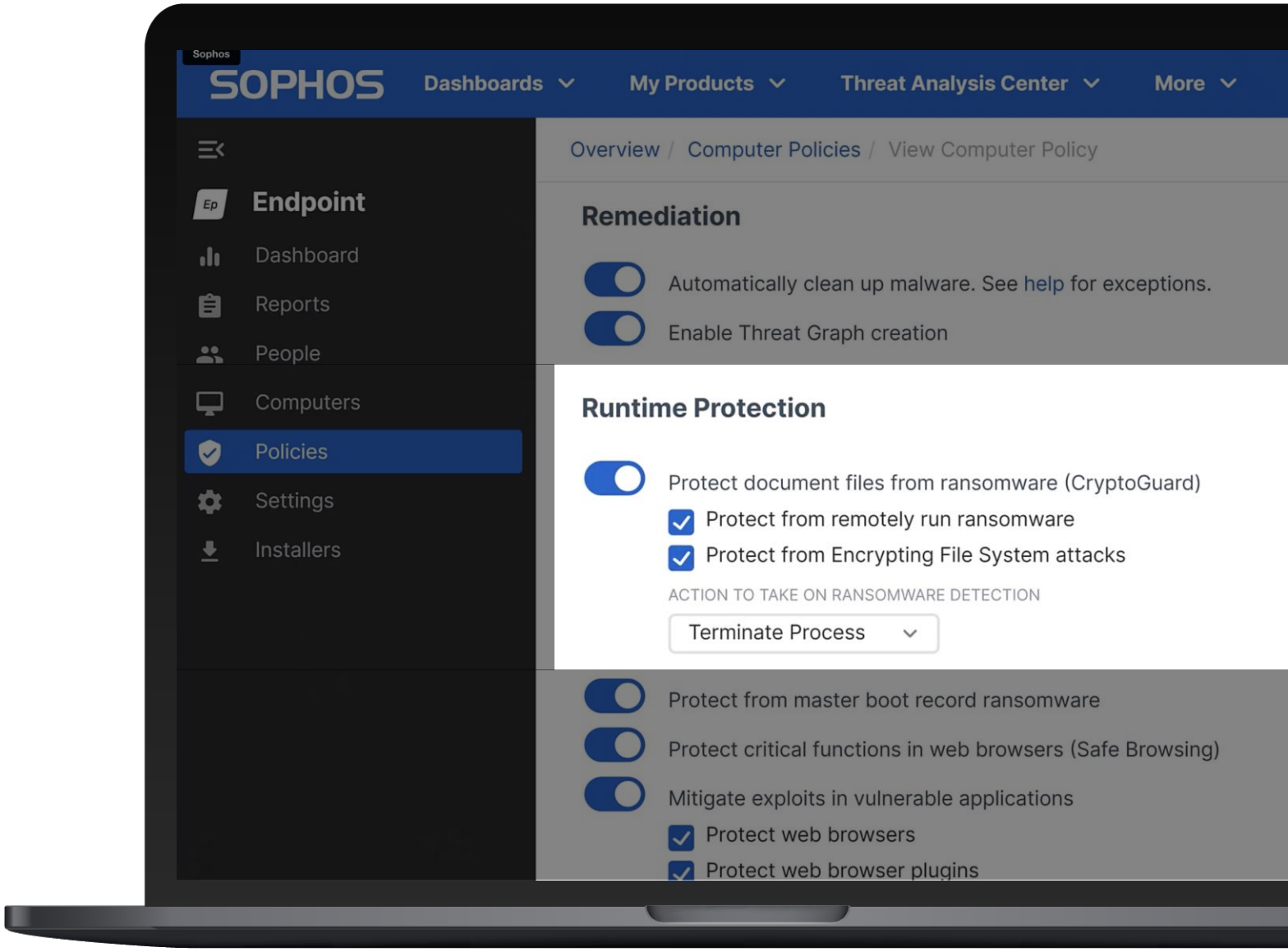
-Microsoft 2023 Digital Defense Report

SOPHOS



Remote Ransomware Protection

Egyedi anti-ransomware technológia, amely blokkolja ezt az új és népszerű kártékony titkosítási módszert.



Adaptive Attack Protection

Automatikusan növeli a védelem szintjét a végponton, amikor "hands-on-keyboard" támadást észlel

- Automatikusan aktiválódik, amikor a védelem egy „élő”, ember által végrehajtott támadást észlel.
- Növeli a védelem érzékenységét a károk elhárítása érdekében.
- Blokkolja a potenciálisan kártékony tevékenységeket.
- Automatikusan izolálni tudja az érintett eszközt, ezzel megakadályozva a továbbterjedést.

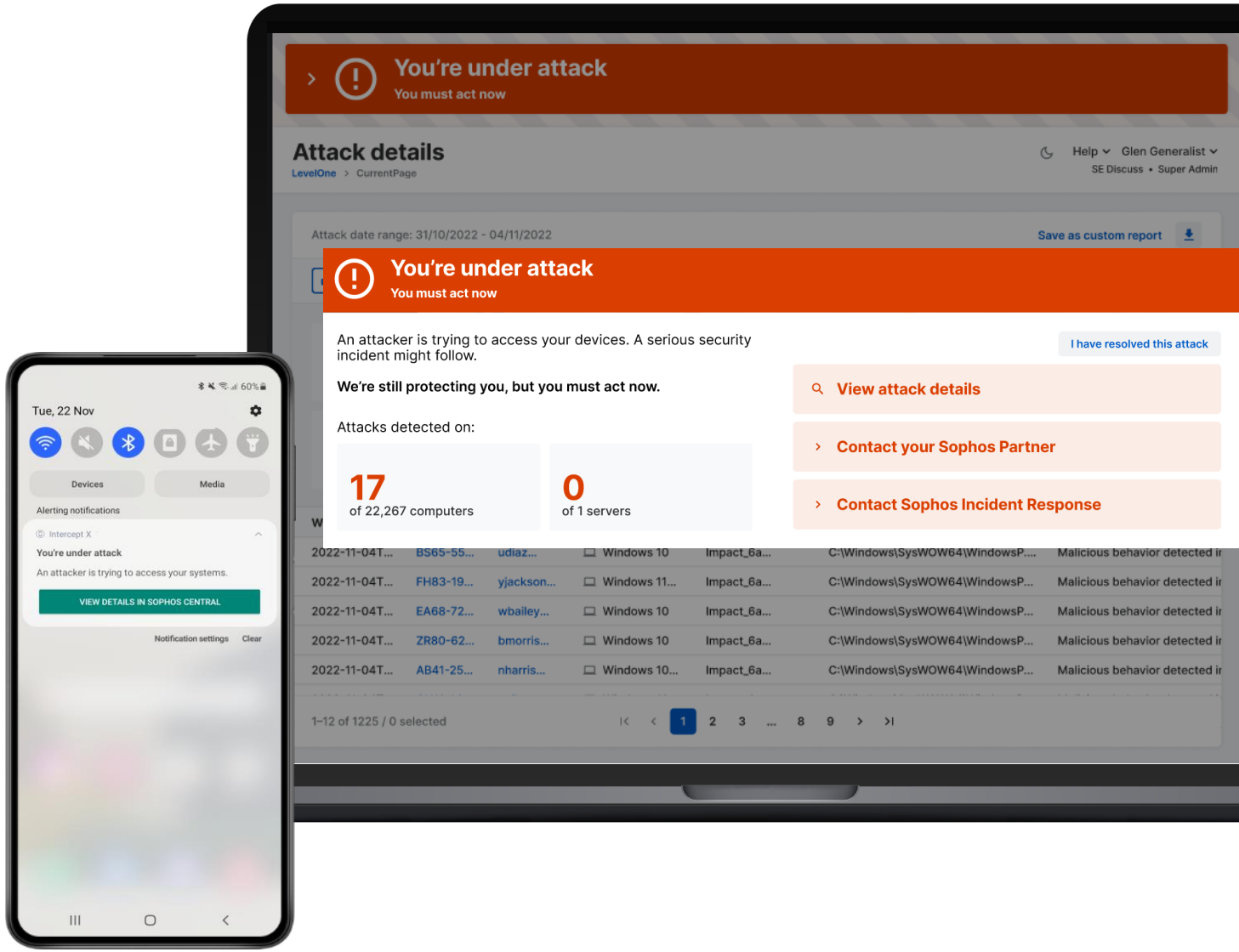
Safe Mode Protection

Megakadályozza, hogy a támadó a Windows Safe Mode-ját használva megkerülje a védelmi rendszer egyes elemeit

- Amikor a támadó nem tud áthatolni a védelmi rendszeren, akkor megpróbálja a gépet Safe Mode-ban újraindítani, ahol a biztonsági szoftver még nem, vagy csak részben indul el.
- A Sophos Adaptive Attack Protection szabályrendszer szinten akadályozza meg a védett gép Windows Safe Mode-ban történő újraindítását.
- Képes bizonyos Sophos végpontvédelmi funkciók (pl. CryptoGuard) futtatására Safe Mode-ban is.

Critical Attack Warning

Figyelmezteti az adminisztrátort, ha egy támadás folyamatban van, és azonnal javaslatokat ad az ellenlépésekre vonatkozóan.



Sophos Central

Biztonságcentrikus alapértelmezett házirendek

A szigorú alapbeállítások erős védelmet eredményeznek

Rugalmas házirendek

Felhasználó és eszköz alapú szabályok

Egyetlen kezelőfelület az összes Sophos termékhez

Az összes lényeges biztonsági információ egyetlen képernyőn

Account Health Check

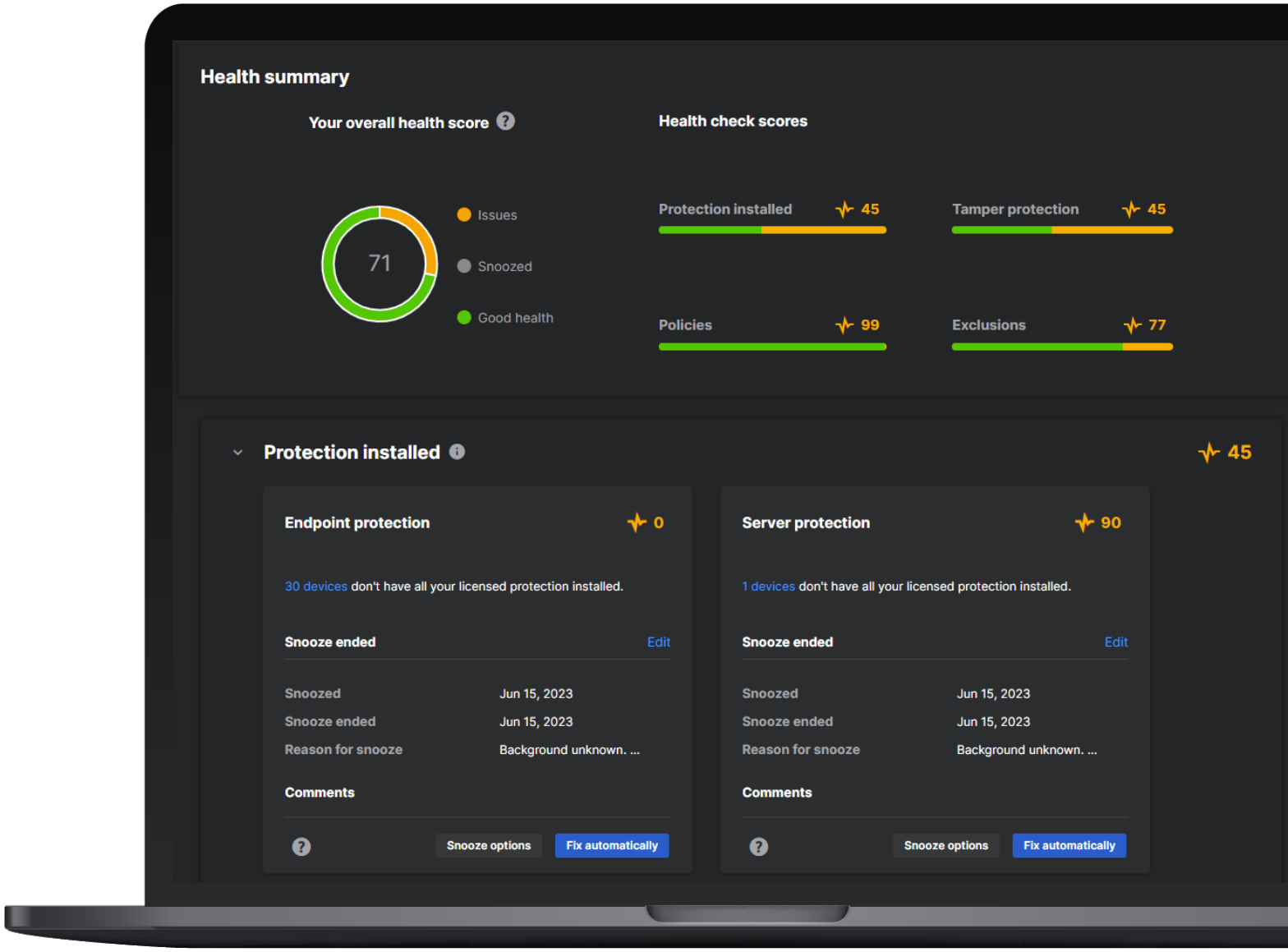
Könnyű módja annak, hogy az ügyfelek megértsék biztonsági státuszukat és összehasonlítsák magukat a többi végfelhasználóval.

A biztonsági eszközök hibás konfigurációja az első számú biztonsági fenyegetés az informatikai csapatok körében.

SOPHOS

Account Health Check

Könnyű módja annak, hogy az ügyfelek megértsék biztonsági státuszukat és összehasonlítsák magukat a többi végfelhasználóval.

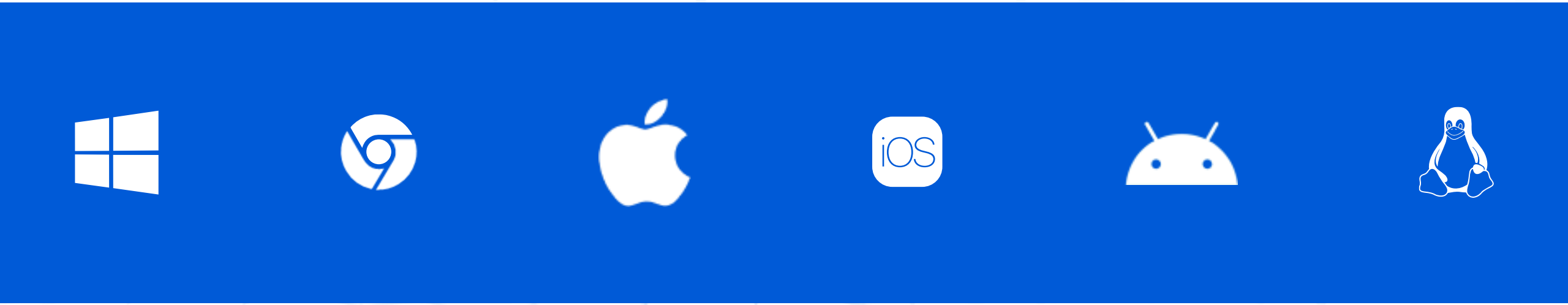


Account Health Check

Könnyű módja annak, hogy az ügyfelek megértsék biztonsági státuszukat és összehasonlítsák magukat a többi végfelhasználóval.

- Azonosítja azokat a félrekonfigurálásokat, amelyek kockázatot jelentenek a szervezet számára.
- Egyetlen gombnyomással javítja a problémákat.
- A szervezet pontszámát össze tudja vetni más, hasonló méretű végfelhasználó eredményével.
- A pontszám változása időben követhető.

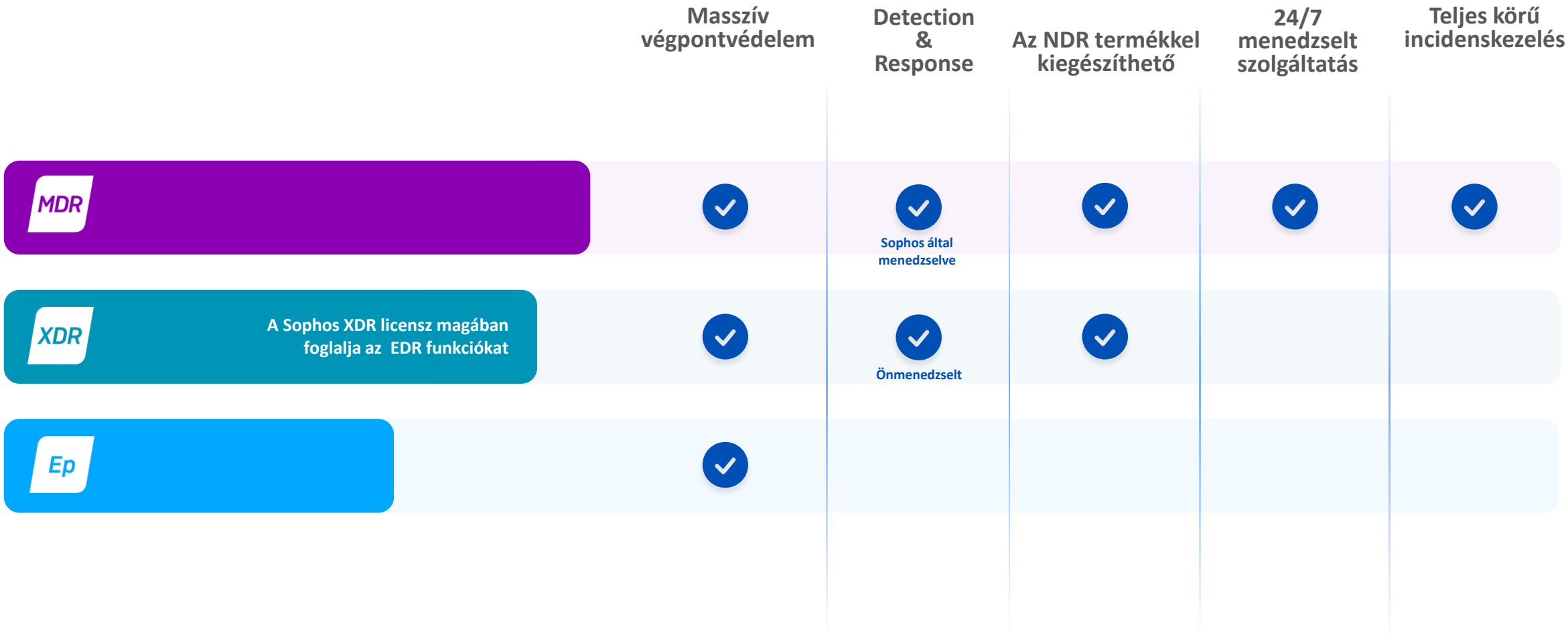
Védelem minden végponton – platformtól függetlenül



SOPHOS

Licenszelés és további termékek

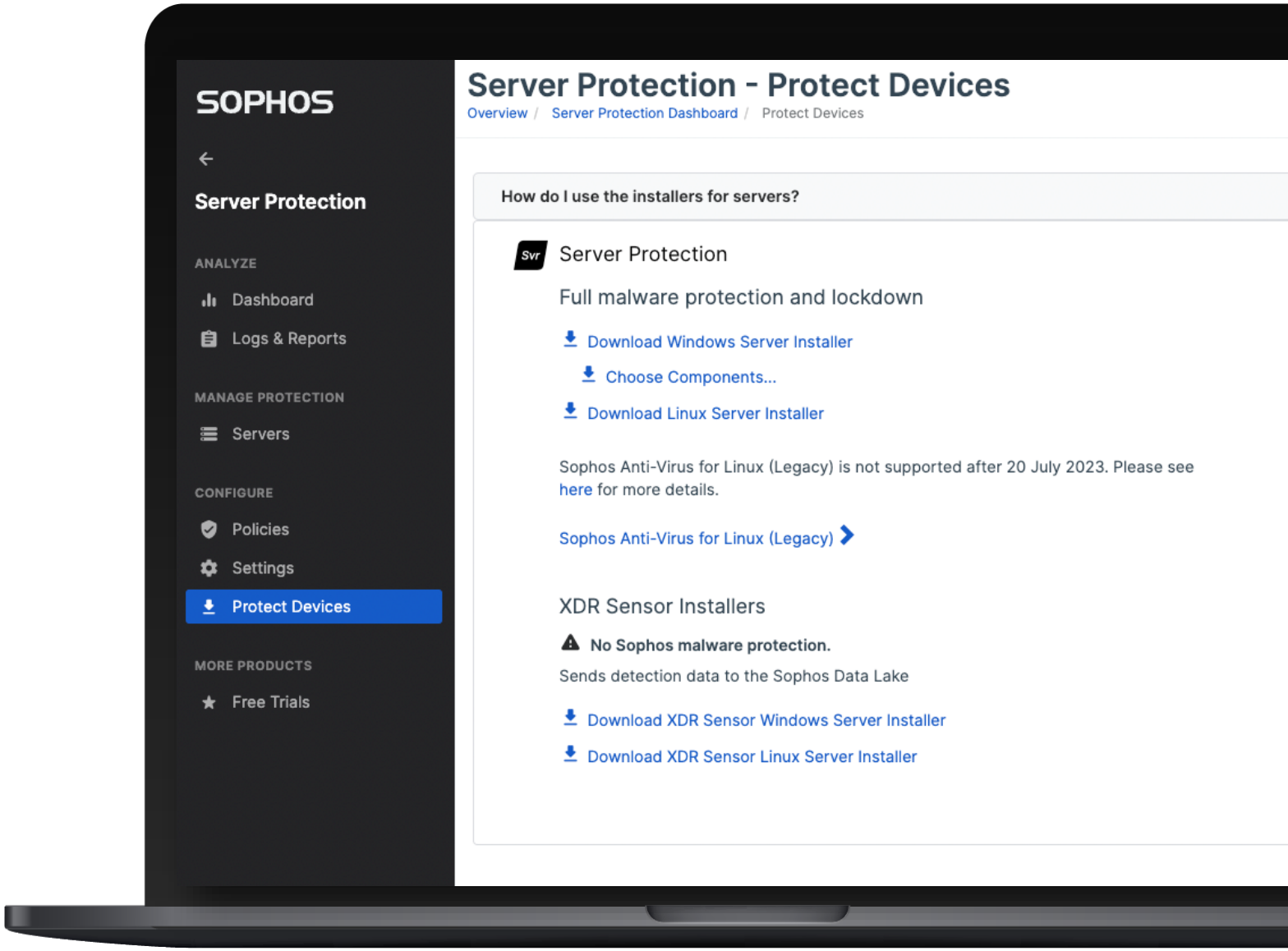
Sophos EP/XDR/MDR



SOPHOS

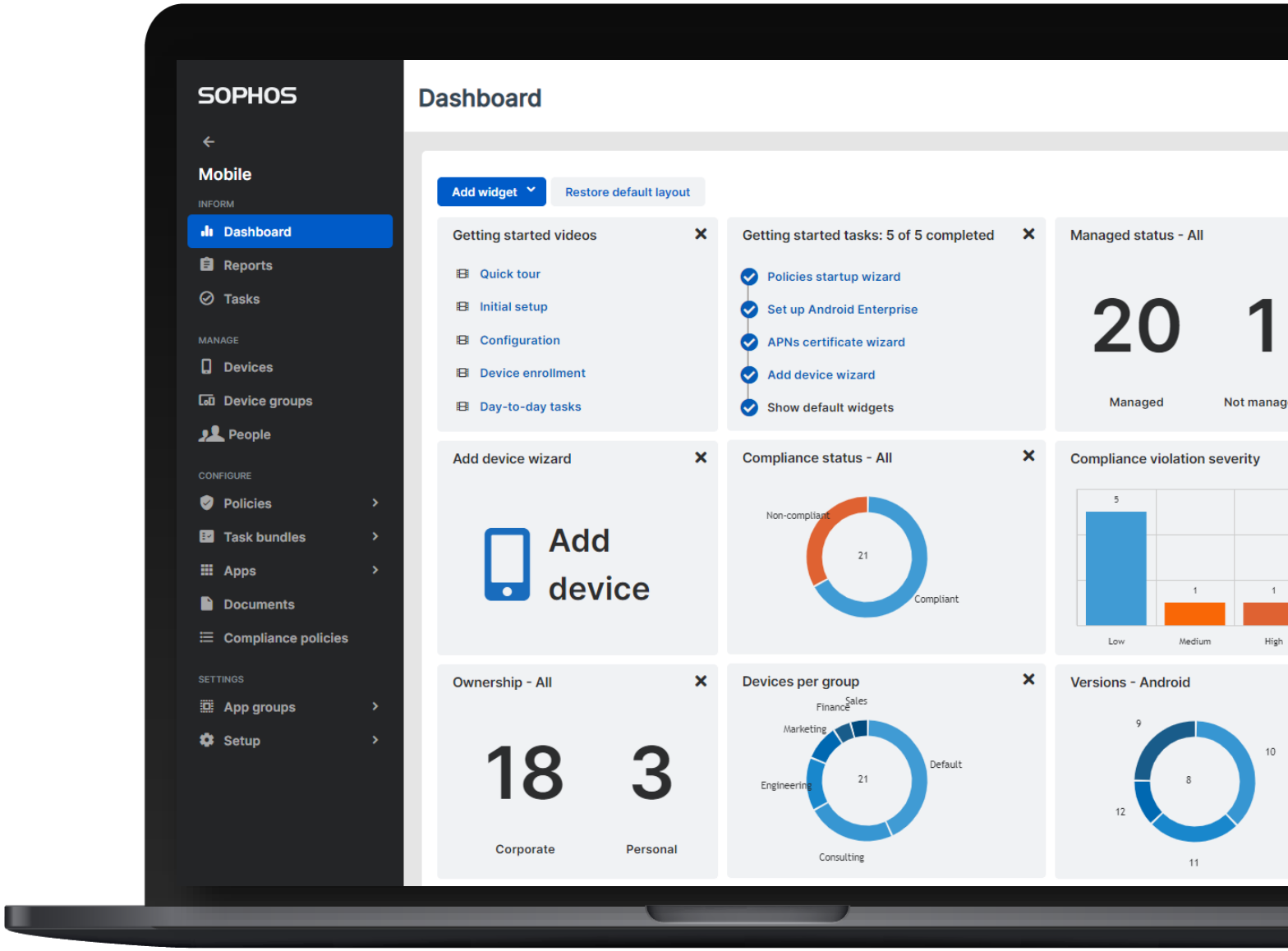
Workload Protection

Nagy hatékonyságú védelem a teljesítményre gyakorolt alacsony hatás mellett helyben, az adatközpontban és a felhőben.



Sophos Mobile

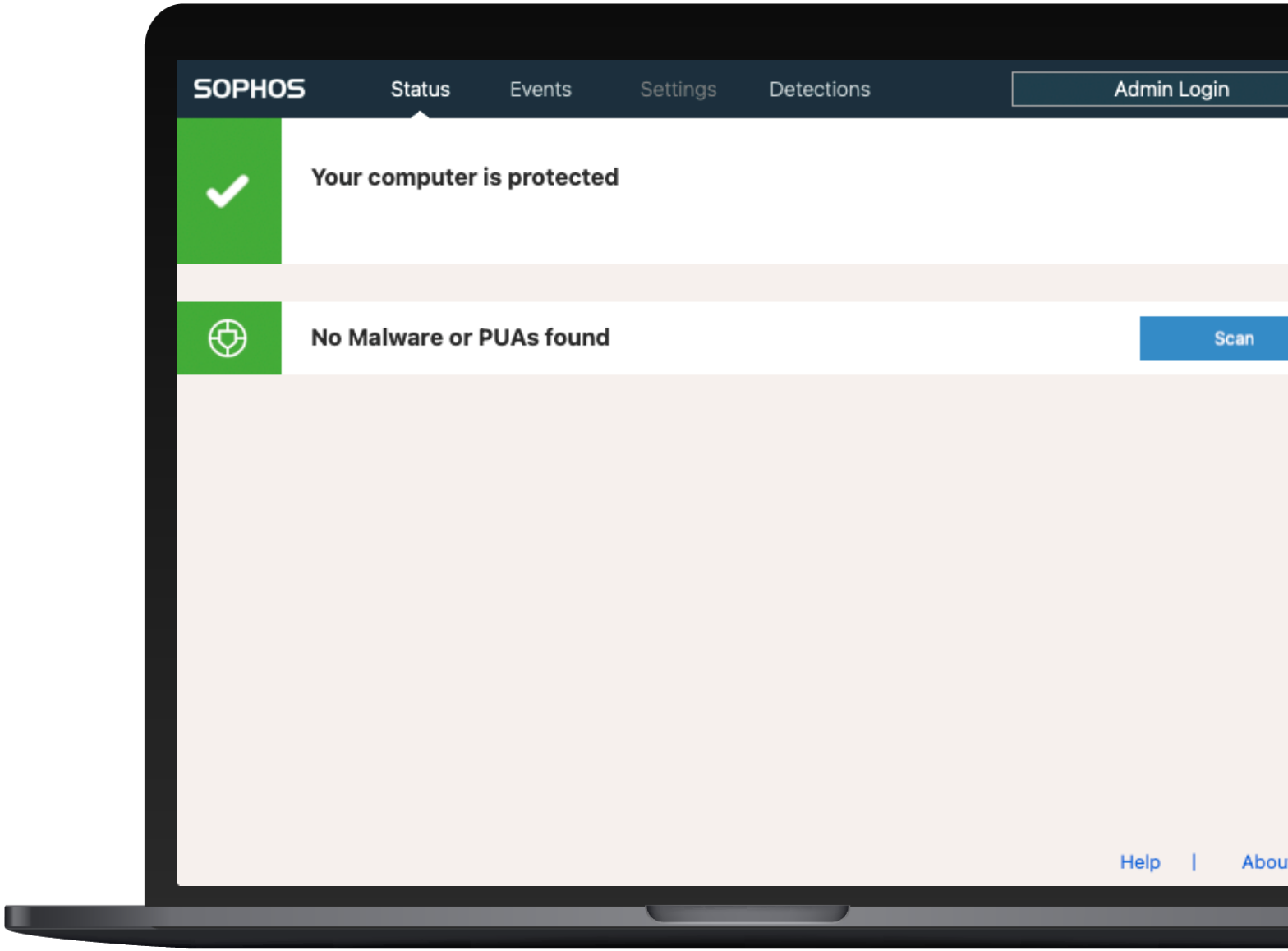
Biztonságos Unified Endpoint Management megoldás a mobil végpontok kezelésére és védelmére.



SOPHOS

Device Encryption

A BitLocker (Windows) vagy a FileVault (macOS) menedzselése Sophos Centralon keresztül.



Adaptive Cybersecurity Ecosystem (ACE)

Ep

Fw Wi ZT

Sophos XDR (EDR)

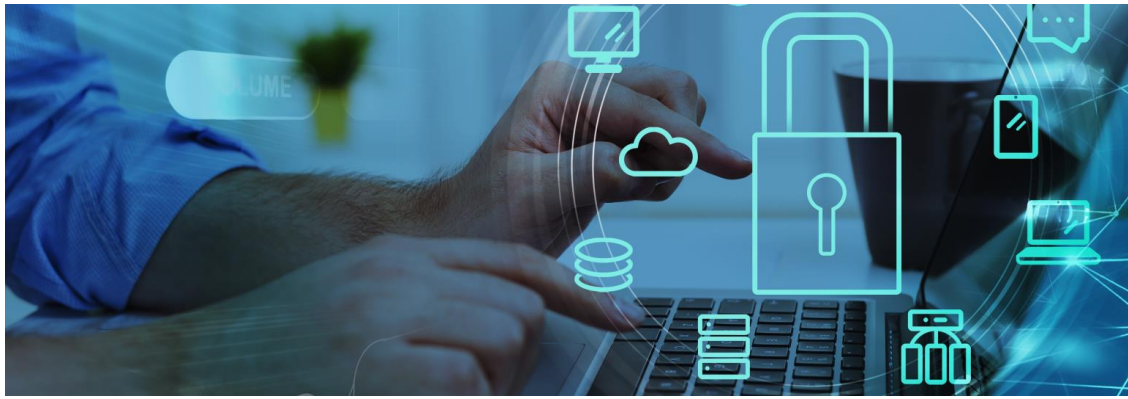
Platform a szakértőknek: összetett fenyegetések vizsgálata és kezelése az összes támadási vektoron

A Sophos erősségei

A legjobb végpontvédelmen alapul
A gépi védelem a fenyegetések magas százalékát emberi beavatkozás nélkül kezeli, ezzel csökkentve a terhelést

Széles körű kompatibilitás
A többi Sophos terméken túl számos más gyártó megoldásait is támogatja

Minden kézben hasznos eszköz
Az általános IT szakemberek és a biztonsági szakértők számára is ajánlott



MITRE | ATT&CK®
99% Detection Coverage

IDC
2024 MarketScape Leader

Leader
#1 XDR solution

Sophos MDR

Menedzselt szolgáltatás: védelem a kiemelkedően fejlett fenyegetések és magasan képzett támadók ellen

A Sophos erősségei

24/7 Detection and Response
A zsarolóvírus támadások 90%-a munkaidőn kívül történik.

Széles körű kompatibiltás
Nem szükséges az elégedetten használt meglévő védelmi rendszerek cseréje.

Teljes körű incidenskezelés
A fenyegetések megszüntetése + a támadás okának és menetének teljes visszafejtése.

MITRE | ATT&CK®
A top performing vendor

Leader
#1 MDR solution

Gartner peerinsights
Customer's Choice for MDR

- Inclusive Pricing
- $1M Breach Warranty
- Unrestricted Hunting
- Response Time SLA

SOPHOS

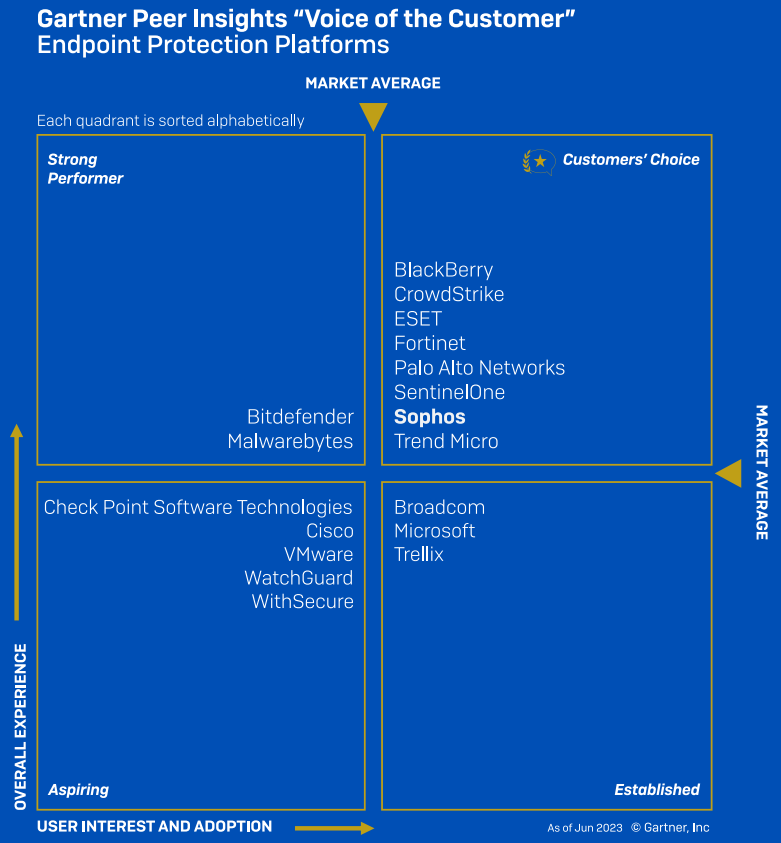
Díjak és elismerések

2023 Gartner Magic Quadrant for Endpoint Protection Platforms

A Sophos (ismét) a Gartner Leader szegmensébe került a végpontvédelmi termékek kategóriájában

- A Sophos zsinórban 14 Gartner riportban került a Leader kategóriába a végpontvédelmi szoftverek mezőnyében.
- Nincs másik gyártó, aki ennyiszer nyerte el a Leader címet ebben a kategóriában.
- A Sophos két egymást követő évben nyerte el a Gartner Customers' Choice minősítését.

Gartner Peer Insights Customers' Choice 2023



A Sophos az egyetlen gyártó, amely elnyerte a Gartner Customers' Choice címet Endpoint Protection Platforms, Managed Detection & Response Services, Network Firewalls, and Mobile Threat Defense kategóriákban egyaránt.

★★★★★
"Intercept X is hands down the best zero-day threat endpoint protection I have used to date"
IT Admin | Manufacturing

★★★★★
"Sophos Intercept X delivers sophisticated functionality coupled with a simple, intuitive user experience."
IT Head | Consumer Goods

★★★★★
"The way it detects and neutralizes the risk before it can cause any harm is really commendable."
IT Manager | Education

★★★★★
"Intercept X provides clear visibility of evils inside the network and protects from cyber threats."
Infrastructure Manager | Education

★★★★★
"Intercept X is the best software that resolved all of our security concerns."
Software Developer | Finance

★★★★★
"Intercept X detects and blocks malware and ransomware attacks before they can cause damage to the systems."
Senior Data Analyst | Miscellaneous

SOPHOS

SOPHOS