SOPHOS

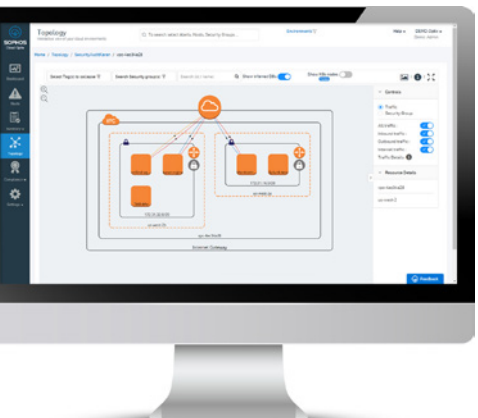
Sophos Cloud Optix

Egyszerűsítse felhőbeli biztonság rendszerét a mesterséges intelligencia és az automatizálás előnyeit ötvözve

A Sophos Cloud Optix ügynök nélküli, SaaS-alapú szolgáltatás a Deep Security-szakértelmet és a mesterséges intelligencia erejét egyesíti. Felhőalapú biztonsági figyelést, elemzést és megfelelőségi automatizálást kínál egyetlen, egyszerűen használható felületen, magas folyamathatékonyság mellett.

Főbb jellemzők

- Percek alatt beállítható, ügynök nélküli, SaaS-alapú szolgáltatás
- Egységes készletkezelés több felhőszolgáltatásban
- Teljes hálózati topológia és forgalmi adatfolyam-vizualizáció
- AI-alapú felhasználóviselkedés- és forgalom-rendellenesség-észlelés
- Folyamatos megfelelőségi értékelés
- Beépített megfelelőségi szabályzatgyűjtemények
- Riasztási korreláció a gyorsabb kármentesítés érdekében
- Kritikus beállítások módosításának észlelése
- Kódként használt infrastruktúrák (IaC) sablonjainak folyamatos vizsgálata



Minden látható, minden biztonságban tudható

A szervezet eszközeinek automatikus észlelése Amazon Web Services- (AWS), Microsoft Azure- és Google Cloud Platform-környezetekben (GCP), aminek köszönhetően csapata percek alatt reagálhat a biztonsági kockázatokra, és orvosolhatja őket a folyamatos eszközfigyelés, valamint a hálózati topológia és forgalom (beleértve a bejövő, a kimenő és a belső forgalmat) teljes vizualizációja révén.

Proaktív felhőalapú megfelelőség

Ahogy a munkafolyamatok átkerülnek a felhőbe, egyre nehezebben állapítható meg, hogy mely megfelelőségi folyamatokra lesz szükség a jövőben, és hogyan kell majd őket végrehajtani. A Cloud Optix eredeti, beépített sablonok, egyéni szabályzatok és együttműködési eszközök segítségével csökkenti az adatgazdálkodással, a kockázatkezeléssel és a megfelelőséggel kapcsolatos költségeket és munkaterheket.

A megfelelőségi folyamat felgyorsítása

Szabványokhoz (például CIS, GDPR, SOC2, HIPAA, ISO 27001 és PCI DSS) készült egyéni vagy beépített sablonokkal végzett folyamatos megfelelőségfigyelés.

Egyszerűsített együttműködés

Külső felektől származó integrációs megoldások (például a Jira vagy a ServiceNow) segítségével kezelheti és nyomon követheti a megfelelőségi előírásokat annak érdekében, hogy még kibocsátás idején se vesszenek el fontos feladatok.

AI-alapú biztonsági elemzések és figyelés

A Cloud Optix folyamatosan figyeli és tanulja a felhőalapú eszközök készletét, a konfigurációkat és a hálózati forgalmat. Az AI-alapú intelligens riasztások az automatizált riasztási rangsorok alkalmazásával és környezetfüggő információk segítségével csökkentik a válaszidőt, és segítenek a biztonsági kockázatok gyorsabb megoldásában.

- A felhőalapú eszközök készletének (Amazon Simple Storage Service (S3), biztonsági csoportok, felhasználói hozzáférési kulcs stb.), a konfigurációknak és a biztonsági csoportok naplóinak folyamatos figyelése
- Rendellenes felhasználói viselkedésminták azonosítása a felhasználói hozzáférési kulcsok ellopása vagy az illetéktelen alkalmazottak tevékenysége nyomán indított magas szintű automatizált támadások ellen
- A hálózati forgalom lehetséges folyásának előrejelzése a biztonsági beállítások alapján, még a támadások indítása előtt kiiktatva a potenciális behatolási pontokat
- Védőkorlátok felállítása a hálózati konfigurációban beállt véletlen vagy rosszindulatú módosítások megelőzése, észlelése és kijavítása érdekében

Okosabb DevSecOps

Az IaC folyamatos fejlesztések és a DevOps-gyakorlatok miatti drasztikus változásainak következtében naponta többször is kiadhatók új szoftverek. Ez óriási terhet ró a biztonsági csapatokra, ami sebezhetővé teszi szervezetét a támadásokkal szemben. A felhőalapú Optix API-vezérelt architektúrájának köszönhetően DevOps-csapatai zökkenőmentesen integrálhatják DevOps-folyamataikat a biztonsági rendszerbe, garantálva a gyors és biztonságos teljesítést.

Csúszásészlelés és védőkorlátok

Folyamatosan figyelheti és észlelheti a konfigurációs szabványokhoz viszonyított csúszásokat, és megakadályozhatja a kritikus beállítások módosítását, így megelőzheti, hogy szervezetében biztonsági rések alakuljanak ki.

Proaktív infrastruktúrasablon-vizsgálat

Folyamatosan figyelheti az olyan megoldások IaC-sablonjait, mint a Terraform, a Github vagy a Bitbucket. Azonosíthatja a helytelen konfigurációkat, amelyek veszélynek kitett infrastruktúrák üzembe helyezését eredményeznék.

SIEM- és DevOps-eszközintegráció

Integráció külső felektől származó biztonsági eszközökkel, mint amilyen a SIEM vagy a DevOps a CI/CD-hez, a leegyszerűsített biztonsági műveletek érdekében.

A kezelés és az üzembe helyezés leegyszerűsítése

A Cloud Optix ügynök nélküli, SaaS-alapú szolgáltatás tökéletesen működik korábbi üzleti eszközeivel.

A felhőalapú AWS-, Azure- vagy GCP-fiókokhoz való kapcsolódás egyszerű folyamattá válik a szolgáltatás részét képező leírásoknak és parancssoroknak köszönhetően, amelyek csak olvasási jogosultságot biztosító hozzáférést adnak a natív felhőalapú API-k használatával. A kapcsolatok percek alatt felállíthatók, és amint létrejöttek, a Cloud Optix azonnal elkezdi az Ön felhőkörnyezetének kiértékelését, és értékes információkkal szolgál.

A felhőbeli biztonság közös felelősség

A nyilvános felhőszolgáltatók nagy fokú platformrugalmasságot kínálnak. De míg ők az adatközpont fizikai védelméért, valamint az adatok és a környezetek elkülönítéséért felelnek, addig a felhőbe kerülő adatok biztonságát Önnek kell biztosítania.

A Cloud Optix folyamatos láthatóságot, megfelelőséget és veszélyforrás-kezelést biztosít, de a következő oldalon a Sophos nyilvános felhőbeli munkafolyamatokat érintő védelmi szolgáltatásainak és következő generációs tűzfalmegoldásainak teljes köréről is részletes információkat találhat: sophos.com/hu-hu/public-cloud.

A Sophos Cloud Optix-jellemzői	
Egyetlen felület minden felhőszolgáltatáshoz	✓
Topológiavizualizáció	✓
Hálózati forgalom vizualizációs réteg	✓
Biztonsági csoport vizualizációs réteg	✓
Rendellenesség-észlelés – hálózati forgalom	✓
Rendellenesség-észlelés – felhasználói bejelentkezések figyelése	✓
Készlet –állomások, hálózatok, tárhelyek, IAM	✓
Készlet – AWS CloudTrail	✓
Készlet – kiszolgáló nélküli	✓
Folyamatos megfelelőségi értékelés	✓
Megfelelőségi szabályzatok (CIS, FEDRAMP, FFIEC, GDPR, HIPAA, ISO 27001, PCI DSS 3.2, SOC2, EBU R 143)	✓
CIS benchmark-szabályzatok	✓
Egyéni szabályzatok	✓
Megfelelőségi/ajánlott eljárásokkal kapcsolatos riasztások és jelentéskészítés	✓
Szervizelés és védőkorlátok	✓
DevSecOps-parancssor-értékelés	✓

Demó- vagy próbaverzió ingyenes kipróbálása

Az összes Cloud Optix-funkció 30 napig ingyenes Sophos.com/hu-hu/cloud-optix.

Sales Eastern Europe
Email: salesee@sophos.com

2019. 05. 14. DS-HU (PC)

SOPHOS