SOPHOS

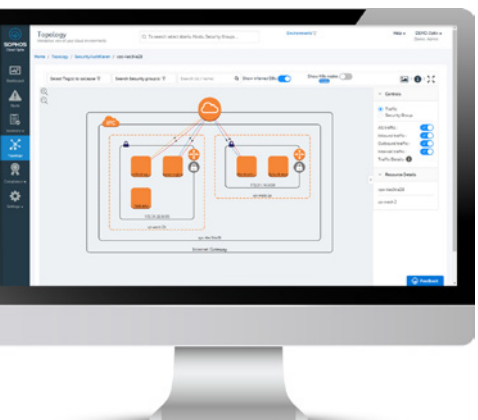
Sophos Cloud Optix

Zjednodušení cloudového zabezpečení kombinací výkonu umělé inteligence a automatizace

Řešení Sophos Cloud Optix, jakožto služba bez agenta založená na SaaS, kombinuje hluboké znalosti zabezpečení se silou umělé inteligence. Zajišťuje efektivní cloudové monitorování zabezpečení, analytiku a automatizaci shody s bezpečnostními standardy pomocí jediného snadno ovladatelného rozhraní.

Přednosti

- Nastavení služby bez agenta, založené na SaaS, v řádu minut
- Správa inventáře napříč více poskytovateli cloudů
- Kompletní vizualizace síťové topologie a síťového provozu
- Detekce chování uživatelů a anomálií síťového provozu pomocí umělé inteligence
- Průběžné vyhodnocování dodržování shody
- Široká škála hotových zásad pro dodržování shody
- Korelace výstrah pro rychlejší nápravu
- Detekce změn kriticky důležitých nastavení
- Průběžné skenování šablon infrastruktury jako kódu



Vše vidět, vše zabezpečit

Automatické odhalení aktiv vaší organizace napříč prostředími Amazon Web Services (AWS), Microsoft Azure a Google Cloud Platform (GCP) poskytující vašemu týmu možnost reagovat na bezpečnostní rizika a napravovat je v řádu minut – pomocí průběžného monitorování aktiv a kompletní vizualizace síťové topologie a síťového provozu včetně vstupního, výstupního a interního.

Aktivní postupy shody s bezpečnostními standardy v prostředí cloudu

S přesunem pracovní zátěže do cloudu je identifikace příslušných postupů dodržování shody čím dál složitější (nemluvě o tom, jak budou tyto postupy implementovány). Řešení Cloud Optix snižuje náklady a náročnost řízení, rizik a dodržování shody pomocí hotových šablon, výchozích zásad a nástrojů spolupráce.

Urychlení postupu shody s bezpečnostními standardy

Průběžné monitorování dodržování vlastních nebo výchozích šablon pro standardy typu CIS, GDPR, SOC2, HIPAA, ISO 27001 a PCI DSS.

Snazší spolupráce

Spravujte a sledujte dodržování shody, abyste zajistili, že nikdy neztratíte důležité úkoly, a to ani při vypuštění, pomocí integrací třetích stran s nástroji, jako je systém JIRA a ServiceNow.

Analytika a monitorování zabezpečení pomocí umělé inteligence

Řešení Cloud Optix zajišťuje průběžné monitorování a zjišťování stavu vašeho cloudového inventáře aktiv, konfigurací a síťového provozu. Chytré výstrahy řízené umělou inteligencí zkracují dobu reakce a pomáhají rychleji napravit bezpečnostní rizika pomocí automatizovaného řazení výstrah podle závažnosti v kombinaci s kontextovými informacemi.

- Průběžné monitorování inventáře aktiv v cloudu (Amazon Simple Storage Service (S3), Security Groups, uživatelské přístupové klíče atd.), konfigurací a protokolů skupin zabezpečení
- Identifikace anomálních vzorců chování uživatelů za účelem detekce pokročilých automatizovaných útoků kvůli ukradeným přístupovým klíčům uživatele nebo neukázněným zaměstnancům
- Předvídání síťového provozu na základě nastavení zabezpečení – prevence potenciálních bodů prolomení ještě před zahájením útoku
- Zavedení ochranných opatření k prevenci, detekci a nápravě náhodných či úmyslných změn v síťové konfiguraci

Chytřejší DevSecOps

Rychlé tempo změn v infrastruktuře jako kódu umožňuje díky průběžnému nasazování a postupům DevOps vydání nového softwaru několikrát denně. Což vyvíjí ohromný tlak na týmy zabezpečení, které by vás mohly nechat vystavené nebezpečí. Architektura řešení Cloud Optix založená na rozhraní API umožňuje týmům DevOps bezproblémovou integraci zabezpečení pomocí jejich postupů DevOps – zajišťující rychlé a bezpečné dodání.

Detekce driftů a ochranná opatření

Průběžné monitorování a detekce driftů v konfiguračních standardech a prevence změn v kriticky důležitých nastaveních, kvůli nimž by mohla být vaše organizace z hlediska bezpečnosti zranitelnou.

Aktivní skenování šablony infrastruktury

Průběžné skenování šablon infrastruktury jako kódu nasazených z řešení typu Terraform, Github nebo Bitbucket Identifikace chybných konfigurací, které by mohly vést ke vzniku zranitelné infrastruktury.

Integrace nástrojů SIEM a DevOps

Zjednodušte operace zabezpečení prostřednictvím integrace nástrojů zabezpečení třetích stran, jako jsou nástroje SIEM a DevOps pro CI/CD.

Jednoduchá správa a nasazení

Řešení Cloud Optix, jakožto služba bez agenta založená na SaaS, dokonale funguje s vašimi stávajícími obchodními nástroji.

Připojení ke cloudovým účtům v AWS, Azure nebo GCP je jednoduché díky poskytnutým pokynům a skriptům, které vytvářejí přístup Read Only skrze rozhraní API nativního cloudu. Spojení lze nastavit v řádu minut, a jakmile bude řešení Cloud Optix nasazeno, může okamžitě začít vyhodnocovat vaše cloudové prostředí a poskytovat vám cenné informace.

Zabezpečení cloudu je sdílenou odpovědností

Poskytovatelé veřejných cloudů nabízejí ohromnou flexibilitu platforem. Avšak zatímco oni odpovídají za fyzickou ochranu v datovém centru, virtuální oddělení dat a prostředí, vaší povinností je zabezpečení všeho, co do cloudu vkládáte.

Řešení Cloud Optix poskytuje průběžnou viditelnost, shodu s bezpečnostními standardy a reakci na hrozby. Více informací o úplné škále ochrany veřejných cloudů Sophos a řešeních firewallů nové generace najdete na adrese sophos.com/cs-cz/public-cloud.

Funkce řešení Sophos Cloud Optix	
Jediné integrované řešení napříč více cloudy	✓
Vizualizace topologie	✓
Pokrytí vizualizace síťového provozu	✓
Pokrytí vizualizace skupiny zabezpečení	✓
Detekce anomálií – síťový provoz	✓
Detekce anomálií – chování při přihlášení uživatelů	✓
Inventář – hostitelé, sítě, úložiště, IAM	✓
Inventář – AWS CloudTrail	✓
Inventář – bez serveru	✓
Průběžné vyhodnocování dodržování shody	✓
Zásady pro dodržování shody (CIS, FEDRAMP, FFIEC, GDPR, HIPAA, ISO 27001, PCI DSS 3.2, SOC2, EBU R 143)	✓
Zásady CIS Benchmark	✓
Vlastní zásady	✓
Výstrahy a reporting – dodržování předpisů / osvědčené postupy	✓
Náprava a ochranné prostředky	✓
Vyhodnocení skriptu DevSecOps	✓

Demo verze neboli vyzkoušejte si řešení zdarma

Všechny funkce řešení Cloud Optix na 30 dní zdarma Sophos.com/cs-cz/cloud-optix.

Obchodní zastoupení pro východní Evropu
E-mail: salesee@sophos.com

2019-05-14 DS-CZ (PC)

SOPHOS