Tjedan 14.4. - 18.4.

#seminar2

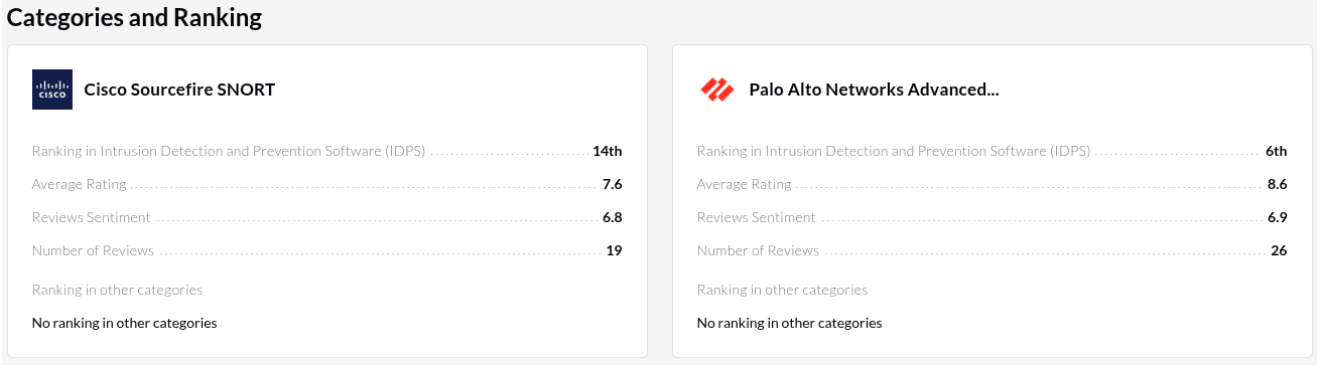
Obrađeno: https://www.peerspot.com/products/comparisons/cisco-sourcefire-snort_vs_palo-alto-networks-advanced-threat-prevention
Autor: PeerSpot
Pristupljeno: 16.4.2025

TL:DR
Usporedba Snorta i Palo Alto mrežnog naprednog alata za sprječavanje prijetnji.

Značajke:
Cisco Sourcefire SNORT se ističe prilagodljivim pravilima, dubinskom inspekcijom paketa i fleksibilnošću otvorenog koda. Palo Alto Networks nudi integrirano sprječavanje prijetnji, kombinirajući vatrozid, antivirus i obavještajne podatke o prijetnjama, s automatiziranim odgovorom i ažuriranjima u stvarnom vremenu.

Prostor za poboljšanje:
Cisco Sourcefire SNORT mogao bi imati koristi od ublažavanja krivulje učenja i poboljšanja sofisticiranosti korisničke podrške. Palo Alto Networks bi se mogao poboljšati smanjenjem visokih početnih troškova i povećanjem dostupnosti naprednih značajki korisnicima bez tehničke stručnosti.

Udio na tržištu
Snort - 3.3%
Palo Alto NATP - 7.4%



Snort

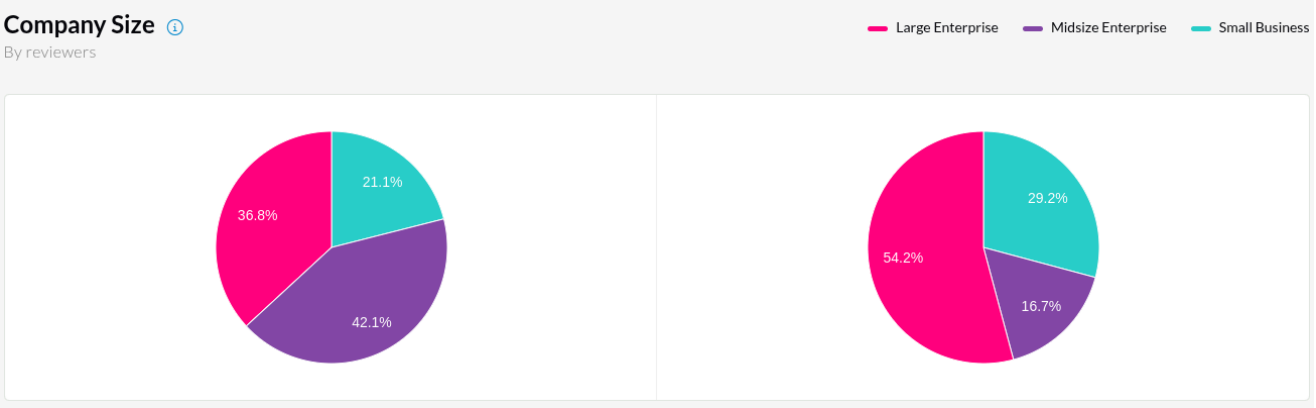
Prednosti	Mane
Jednostavno skaliranje za veće radne okoline	Integracija sa ostalim alatima (uključujući i Ciscove alate)
Tehnička podrška je izuzetno korisna	Cijena
Jako dobra usluga filtriranja prometa i URL-ova kao i zaštita od *malware*-a	Uređivanje pravila se može pojednostaviti
Detekcija prijetnji izuzetno dobra (malo FP-a)	Performanse se mogu poboljšati i alarmi mogu biti informativniji
Jednostavan za konfiguraciju i *deployment*	Početno postavljanje može biti kompliciranо za razliku od sličnih proizvoda (ovisi o okruženju)

Izvor: https://www.peerspot.com/products/cisco-sourcefire-snort-pros-and-cons#pro-aspect-container

Palo Alto NATP

Prednost	Mane
Robustna zaštita protiv zlоćudnog koda	Manjak tehničke podrške
Najnapredniji vatrozid sa korisnim značajkama i intuitvnim korisničkim sučeljem	Početna instalacija i implementacija mogu biti složene
Kvaliteta upravljanja aplikacijama i propusnost mreže	Licenciranje je skupo, a cijena hardvera visoka (otežano skaliranje)
Filtar sadržaja, upravljanje IP adresama i inteligentni vatrozidi	Nedostaje podrška za ICAP protokol
Korištenje strojnog učenja poboljšava otkrivanje nepoznatih prijetnji.	

Usporedba



Kao što vidimo velika i mala poduzeća čine najveći udio klijenata Palo Alto NATP-a dok su klijenti Snorta najviše srednje velika poduzeća.

Zaključak

SNORT je fleksibilno i prilagodljivo rješenje s dobrim mogućnostima detekcije, pogodno za tehnički potkovane korisnike. Palo Alto NATP nudi naprednu zaštitu i automatizaciju, ali uz visoke troškove i složeniju implementaciju. Odabir ovisi o veličini poduzeća, budžetu i tehničkim potrebama.