



Firewall Analyzer as a Service

(FAaaS)

Orange Cyberdefense kan tilbyde din virksomhed, på abonnementsbasis, at udnytte de stærke funktioner i **AlgoSec Firewall Analyzer, sammenkoblet med assistance fra en certificeret AlgoSec ekspert.**

AlgoSec Firewall Analyzer leverer også en automatiseret proces til sikring af kontinuerlig og korrekt konfiguration af netværkssikkerhedspolitikker for at reducere angrebsfladen og håndhæve effektiv netværkssegmentering.

Med Orange Cyberdefense FAaaS kan du snuse til, hvordan man kan automatisere og forenkle sikkerhed på tværs af virtuelle, fysiske og cloud miljøer fra adskillige producenter for at sikre synligheden og overblikket i netværket gennem automation.

FAaaS er baseret på, at en AlgoSec server installeres på kundens eget virtuelle server miljø.

Abonnementet løber minimum 12 måneder, hvorefter det kan afsluttes, fornyes eller forlænges for yderligere 12 måneder. Der er ingen opstartsgebyr og løsningen understøtter op til 1.500 firewalls.

FAaaS giver dig licenser til AlgoSec, installation og assessment af firewalls.

Du betaler kun for de firewalls, du ønsker at medtage i servicen.

Mitigering af ricisi og oprydning i regler mm. Faktureres efter forbrug. Sådan sikrer vi dig, at du ikke betaler for mere end du får.

Assessment – vi anbefaler halvårslige assesments, og har allerede inkluderet et i servicen. Ønsker du at få flere, kan det naturligvis inkluderes i aftalen.

FAaaS afregnes i en pris pr. måned.

Hvad er indeholdt i prisen?:

- Licens pr. firewall, fysisk eller virtuel, samt pr. cluster.
- Installation af AlgoSec løsningen onsite hos kunden på de aftalte firewalls, hvor vi opsætter en AlgoSec server i virksomhedens eget virtuelle servermiljø

Et assessment består af:

- Gennemførelse af Orange Cyberdefenses 10 trins firewall assessment model.
- Et assessment møde med en certificeret AlgoSec konsulent.
- Liste med anbefalede ændringer til firewalls.
- Omfattende sikkerhedsassessment rapport genereret med AlgoSecs værktøj.
- Sikkerhedsrating af hver enkelt firewall 1-100, hvor 1 er dårligst og 100 bedst.
- Compliance rapport op mod valgfri sikkerhedsstandard (eks. ISO 27001, GDPR).

Orange Cyberdefense 10 trins Firewall Assessments:

Step 1. Network zone verification

Step 2. Baseline start

Step 3. Unused Rules, Unused Objects and Covered rules

Step 4. Tightening of partly unused (to wide) rules

Step 5. Risks and risky rules

Step 6. General Firewall security

Step 7. Change requests opened during security assessment

Step 8. Security assessment baseline end

Step 9. Evaluation

Step 10. Firewall assessment report