



Fuld DNS-beskyttelse med Forseti (Secure DNS)

DNS blokeringsstjenesten fungerer som et eksternt opslagsværk, så websider med skadeligt indhold ikke kan tilgås af organisationen eller virksomhedens medarbejdere.

Forseti beskytter perimeteren og dermed alle endpoints, telefoner og anden IOT, der er logget på virksomhedens netværk.

Forseti logger alle DNS opslag, også dem der ikke bliver blokeret. Dermed vil man altid gå tilbage i loggen og eksempelvis finde frem til, hvornår man fik en infektion, der ikke blev blokeret.

»» Forseti



FORSETI



- Ingen klient installation
- Opdager avancerede netværkstrusler
- Nem implementering
- Ingen efterfølgende administration og vedligeholdelse for kunden.
- Kører i både aktive og passive tilstande
- Machine learning
- Forhindrer dataleakage, hvis netværk inficeres
- Blokerer websites med ondsindet indhold

“Sikkerhedsnet, som beskytter alt, der er logget på dit netværk”

»» DarkLayer Guard™ og VectorN Detection™

DarkLayer Guard™ og VectorN Detection™ blokerer downloads, hvis endpoint er inficeret med malware.

I modsætning til en antivirusløsning kigger Darklayer GUARD™ ikke på filer, men på de infrastrukturer, der bruges af hackere. DarkLayer Guard-funktionen har en tovejs trafikscanningsmotor i realtid, der overvåger alle DNS-, HTTP- og HTTPS-pakker. Forseti forhindrer inficerede klienter i at kommunikere med hackerens command and control servere.

Sådan beskytter VectorN Detection



Analysere netværkstrafikken



Beskytter alle endpoints



Advarer og rapporterer



Opdager skjult malware