CENTERA

Centera email Defence

Enhanced Threat Protection for Business Email

DATAARK DK V.1.4

Mere end 90% af alle cyberangreb og datalækager involverer e-mail, hvilket gør det til den største trussel mod virksomhedens it-sikkerhed.

IT-kriminelle udnytter din virksomheds e-mail i bestræbelser på at kompromittere din økonomiafdeling, stjæle legitimationsoplysninger, få adgang til data og inficere jeres computere med ransomware. Phishing og malware udvikler sig så hastigt og omfangsrigt at traditionelle cybersikkerhedsløsninger ikke er effektive til at identificere og stoppe alle typer cybertrusler i emails.

Centera email Defence er en effektiv løsning til at beskytte din virksomheds IT-miljø, der detekterer og blokerer nyeste e-mailtrusler som phishing, CEO-fraud, business email compromise, credential phishing, malware og ransomware.

Adapted Managed email Security

Stop Email Truslerne Tidligt

Centera email Defence giver et overblik over virksomhedens e-mail-kommunikation i relation til it-sikkerhed, hvor man kan afdække trusler, blokere cyberangreb og reducere virksomhedens overordnede sikkerhedsrisici.

Bloker truslerne før de når ind I jeres it-infrastruktur

Afdæk alle aspekter af potentielle cyberangreb fra email, ved automisteret analyse af indlejrede kommandoer, kode og sammensætning, hvormed trusler fra både vedhæftninger, sårbarheder og skadelige links neutraliseres.

24/7 Managed Service & Threat Protection

Ingen vedligehold og Adgang til dansk premium support.
Centera email Defence benytter også Centera Threat Intelligence der er en væsentlig kilde til at kunne stoppe en række målrettede cybertrusler og angreb med det samme.

Enkel Udrulning og Total Dækning

Beskyt jeres brugere uanset om de på kontoret, hjemmearbejdspladsen eller ude ved kunder, løsningen dækker alle typer enheder og netværk hvor skadelige emails kan udgøre en trussel. Enkel implementering for bla. Exchange og Office365.

Skaber Overblik Over Potentielle Trusler

Centera's Threat dashboard angiver en løbende og generel risikoscore for virksomhedens e-mails. Dette hjælper administratorer med at prioritere evt. alarmer og reagere evt. øgede risici for virksomheden. E-mail-logføring og tilknyttede data vises i realtid. Rapporter, alarmer, operativ status kan tilsendes via SMS eller e-mail.

Features

- **Cloudbaseret Platform** for scanning, analyse og blokering af skadelige emails.
- **Scanning med flere lag** af kommercielle globale antiphishing, antispam, antifraud og antimalware filtre.
- **Analyse af email med filtre fra regionale efterretninger** om email trusler, som målrettede kampagner fra IT-kriminelle og andre former for målrettede angreb via email.
- **Analyse af email med machine learning** email analyseres for trusler og nye metoder for email angreb via machine learning. Klassifikationen af en skadelig email kan efterprøves af administrator i alternative sandbox systemer.
- **email Risk & Threat View**, giver løbende status for virksomhedens risikoniveau for deres email, samt en oversigt og forensic adgang til email og trusler der udgør risici.
- **email Flow & Logs View**, giver et enkelt overblik over virksomhedens email trafik, men mulighed for at søge på tværs af email, real-tid, som historiske.
- **Danske Datacentre,** GDPR Compliant

Detekterer og Blokerer:

- **Business Email Compromise**
- **CEO Fraud**
- **Phishing**
- **ID & Credential Theft**
- Reconnaissance campaigns
- Malware
- Ransomware
- Extortionware
- Non compliant emails

Stop bedrageriforsøg og avancerede trusler fra emails

Machine learning kombineret med datafeeds fra cyber threat intelligence er grundlaget for en effektiv analyse af e-mails, der opdager og neutraliserer trusler som phishing, CEO fraud, BEC, identitetstyveri, skadelige makroer og nye sårbarheder.

Analyse af vedhæftninger

Vi benytter en række avancerede mekanismer til afdækning af trusler, som beriges med omfattende threat intelligence til at analysere enhver vedhæftet fil. Vores løsning kan karantænesætte e-mailen, indtil der er opnået en endelig analyse af om den pågældende email kan være skadelig. Alle ikke skadelige e-mails kommer frem til brugerens indbakke uden mærkbar forsinkelse, imens email med trusler logges, slettes eller sættes i karantæne.

URL Crawling & Analyse

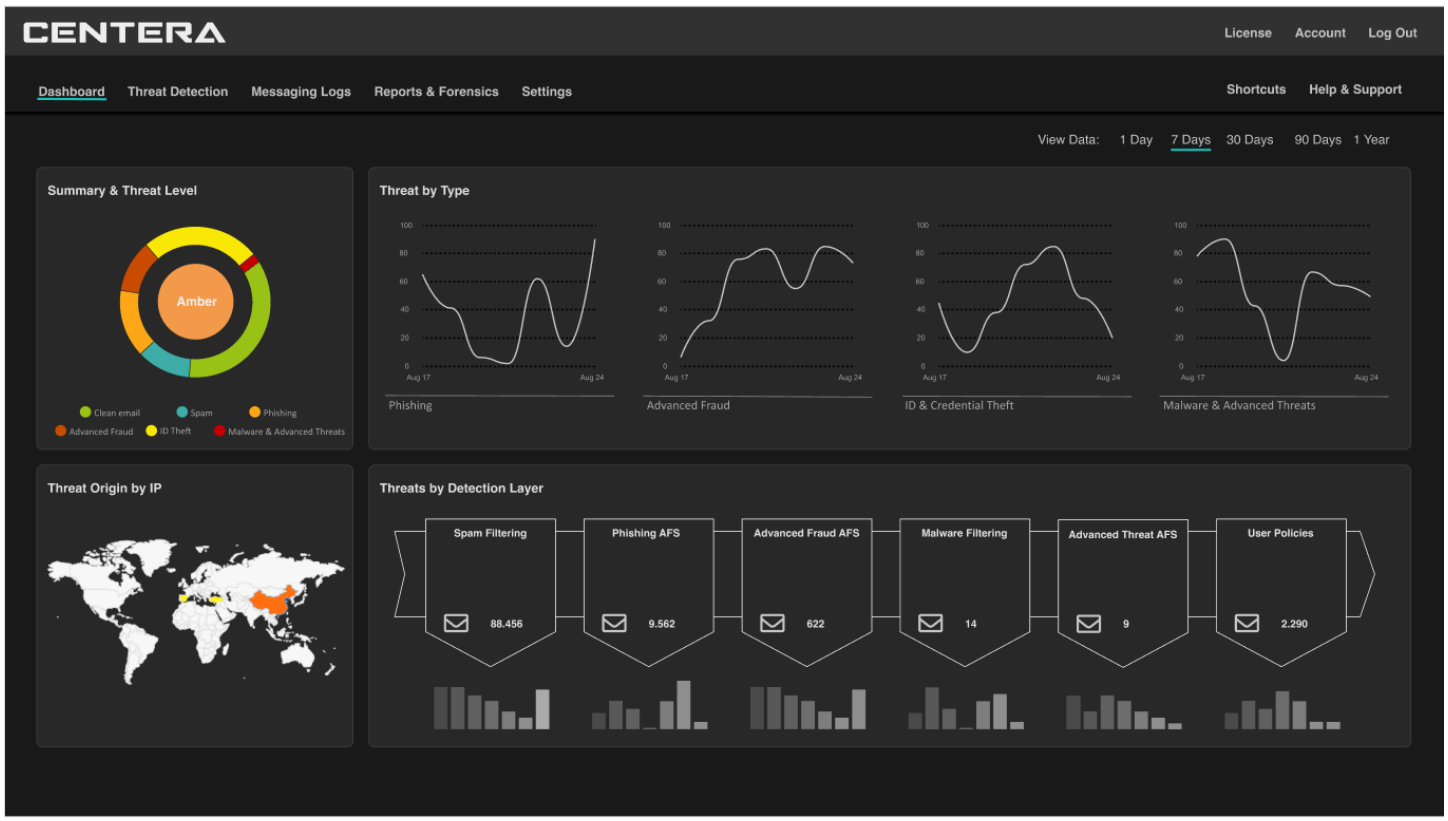
Via machine learning analyseres og opdages trusler i links. E-mails, der indeholder ondsindede links, sættes øjeblikkeligt i karantæne, mens den tilsigtede modtager kan gives mulighed for at se e-mailen i et sikret og uskadeligt format.

Centera Client Aware Threat Detection

Centera Email Defense omfatter en unik kombination af deteketions-lag med machine learning og regionaliserede efterretninger om email relaterede trusler. Hver kundes detektionsprofil tilpasses individuelt for effektivt beskytte virksomhedens e-mail mod trusler, samtidigt med at blokeringer af legitime emails holdes på et minimum.

Prøv email Defence gratis

email Defence giver fuld synlighed og rapporterer e-mail-relaterede trusler. Afprøv og udforsk løsningen i detaljer - anmod om en 15-dages gratis prøveperiode ved at kontakte os eller din IT-partner direkte.



Om Centera Security

Centera Security blev grundlagt i København i 2019. Vi er en it-sikkerhedsudvikler med fokus på nordiske virksomheder. Vores primære mål er at beskytte virksomheder og organisationer mod IT-relaterede trusler gennem bedre designede cybersikkerhedsløsninger. Centera Security kombinerer gennemprøvet teknologi med machine learning og efterretninger om målrettede cybertrusler.