

# Centera DMARC Compliance; Beskyt jeres medarbejdere, brand og kunder med forbedret email sikkerhed

## Etabler og oprethold fuldstændig DMARC Compliance for virksomhedens email, der forebygger misbrug af jeres brand samt phishing angreb mod jeres virksomhed og kunder

*I mere end 90% af alle målrettede cyberangreb indgår email som en del af angrebet.<sup>1</sup>*

*Email udgør i dag den største trussel mod virksomhedens it-sikkerhed.*

*De fleste virksomheder modtager større mængder skadelige emails, der udgiver sig med en falsk identitet (spoofing) som forsøger at afdække svagheder og stjæle login oplysninger (phishing).*

*Samtidigt er de mere målrettede bedragerforsøg mod virksomheden (som CEO Fraud & Business email Compromise) et stadigt stigende problem.*

En grundlæggende forudsætning for bedre email sikkerhed er at implementere DMARC, som et regelsæt der sikrer virksomhedens udgående email er verificerbare for autenticitet hos modtagerne.

Dermed beskyttes virksomhedens egne email domæner mod misbrug som spoofing og phishing.

Ved at verificere virksomhedens indgående email med DMARC, opnår man samtidigt at virksomheden beskyttes bedre mod spoofing, phishing og andre emails fra it-kriminelle.

DMARC-regelsættet benytter eksisterende- og nye mekanismer for kontrol af emails, derudover kan brugere af DMARC udveksle rapporter om emails overholdelse eller mangel på samme for DMARC. Dette kan give virksomheden et løbende overblik og bedre kontrol over hvem der forsøger at sende e-mails på vegne af virksomheden.

DMARC opnår først sin fulde effekt ved en fuldstændig implementering (compliance), hvor virksomheden afviser eller karantænesætter alle emails i henhold til DMARC kontrollen og samtidigt opsamler rapporter for de afviste emails.

**Centera DMARC Compliance er den komplette løsning for fuldstændig DMARC compliance i virksomheden med enkel implementation, monitorering, vedligehold, samt indsamling og hosting af rapporter.**

### ► Stop Phishing

Beskyt jeres medarbejdere ved at monitorere og blokere med DMARC-validering mod it-kriminelle der forsøger at svindle virksomheden via falske emails.

### ► Overvåg muligt misbrug af jeres virksomhedsnavn

Beskyt jeres Kunder ved at opnå kontinuerlig indsigt og overblik over forsøg på at misbruge din virksomheds identitet via email.

### ► Opnå og oprethold fuldstændig compliance

Ved fuldstændig DMARC-compliance reducerer man virksomhedens risici fra email væsentligt, samtidigt med at man bidrager til gøre email hos foreningsforbindelser og kunder mindre udsat for svindel.

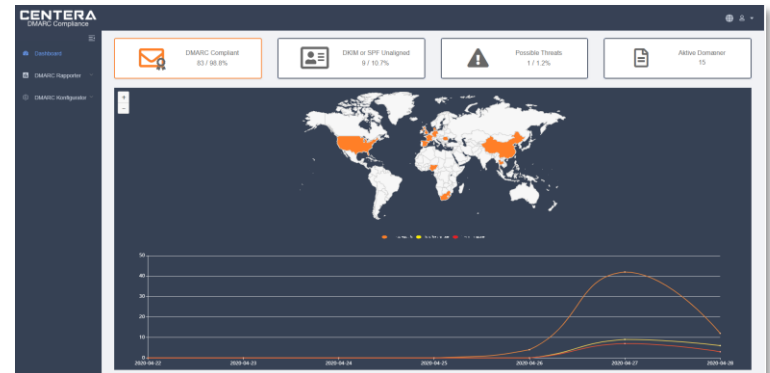
### ► Beskyt leveringsikkerheden for jeres forretningskritiske emails

Den brugervenlige administrations platform samler alle opgaver i forbindelse med DMARC, samtidigt med at rapporter indsamles og lagres så virksomheden kan gennemføre eventuelle tilretninger i jeres email infrastruktur som beskyttelse mod falske positiver ved DMARC kontrol.

<sup>1</sup> Verizon 2019 Data Breach Investigations Report

## DMARC Compliance for alle jeres email.

Centera DMARC Compliance er udviklet af danske email sikkerhedsudviklere der har rådgivet virksomheder indenfor email sikkerhed siden 2008 og DMARC siden standardens fremkomst i 2012. Løsningen er udviklet med henblik på at gøre fuldstændig gennemførelsen af DMARC Compliance så enkelt som muligt, hvormed man opnår alle fordelene ved DMARC. Platformen monitorer samtidigt imod konfigurationsfejl og manglende vedligehold, f.eks. mod falske positive eller udeladte domæner.



Dashboard giver et samlet overblik, bl.a. over evt. misbrug af jeres domænenavn

## Elementerne i Centera DMARC Compliance

- **Cloudbaseret Sikker Platform for DMARC**  
DMARC konfiguration og opnåelse af fuld DMARC Compliance
- **Monitring** for opretholdelse og vedligehold af DMARC konfiguration, derunder DNS record entries, DKIM og SPF
- **DMARC Rapportering**, der afdækker phishing og spoofede emails
- **IP Rapportering** der angiver de IP-adresser der oftest sender virksomheden emails der blokeres ved DMARC kontrol
- **Forensic View**, der afdækker misbrug af jeres virksomhedsnavn, domæneidentitet og anden Brand Abuse
- **Hosted cloud service for virksomhedens DMARC rapportindsamling**, med 60 dages fuld retention
- **SPF Protect**  
Opret og vedligehold extended SPF records for jeres domæner der sikrer DMARC funktion og compliance ved SPF records med mere end 10 DNS opslag
- **Hosted cloud service for extended SPF**
- **Dansk teknisk support via telefon og email**

The report provides detailed insights into email delivery. It includes a table with columns for Sender, Volume, DMARC Compliance, DMARC Aligned, and SPF Aligned. Below the table, there are sections for DMARC, DKIM, and SPF records, each with a status indicator (e.g., 'Aligned', 'Misaligned', 'Unaligned').

Opsamlede rapporter giver indsigt i hvilke emails der evt. Ikke overholder DMARC

The SPF Protect section displays a table of DNS records for SPF records. The table has columns for Handling, Mechanisms, Values, and Annotating. It shows records for 'centerasecurity.com' and 'centera-security.com'.

SPF Protect beskytter bl.a. jeres DMARC opsætning imod ugyldige SPF adresser