

Vodacom[™]



POWERDMARC

Aftenposten 8 SEP 2023

Aftenposten Nyheter Oslo Meninger A-magasinet Vink E-avis Valg 2023 [Bli abonnent](#)

ANNONSE

Boliglån med **personlig** rådgivning **DNB**

Norge | Datasikkerhet

Syv av ti e-postdomener hos norske virksomheter kan misbrukes

 **Lytt til saken** • 5 minutter  **1X** 

Ville du ha latt deg lure av en e-post fra politiet eller banken din? Svært mange norske virksomheter har ikke sikret seg mot at andre kan sende e-post fra deres adresser.

Ubeskyttede domener blir stadig brukt til svindel og bedrag:

Nettavisen **Nyheter.** Nyheter Økonomi Sp...

150.000 svindel-eposter sendt til Telenor-kunder: – Slett e-posten så raskt som mulig

Svindelmail sendt fra online.no

– Vi har sett tilfeller der svindlerne klarer å lure BankID-koder og andre engangspassord ut fra ofrene sine ved å følge med i sanntid.



Flyselskapet Widerøe advarer mot et omfattende angrep via epost som har **support@wideroe.no** som avsender.

blokkert konto



Kjære kunde,

Vi sender deg denne meldingen for å informere deg om at "Kontoer / kort" dessverre er deaktivert på grunn av mistenkelig aktivitet på kontoen din.

Vi informerer deg om at fra den angitte datoen kan ingen operasjoner utføres.

Slik aktiverer du tilgangen din på nytt:

[Logg inn](#)

Det eneste som stopper dette er DMARC med Policy REJECT:

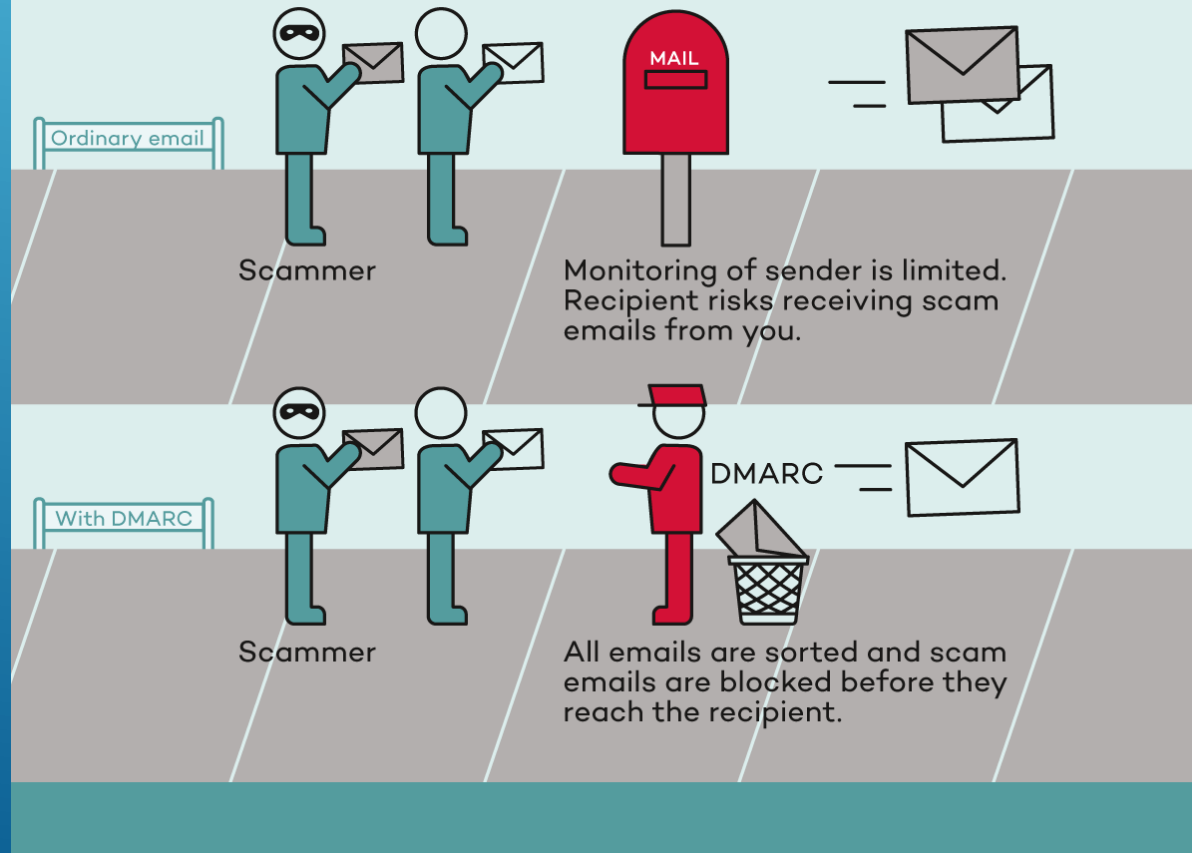


DMARC → Postkasse vs Postmann

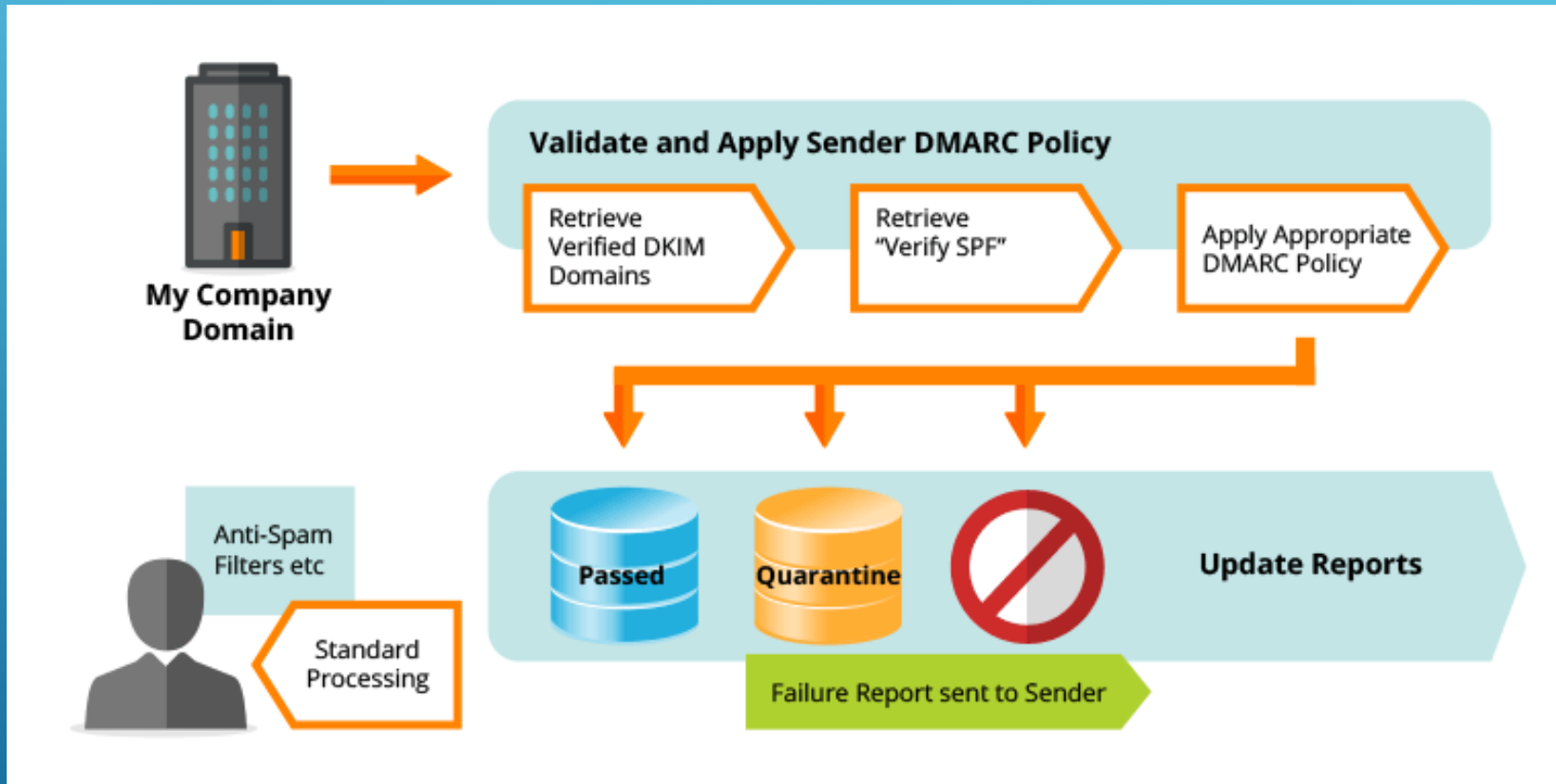
SECURE EMAIL WITH **DMARC**



DMARC reveals false emails sent from your domain name. It's like when the postman checks your identity when you send letters.

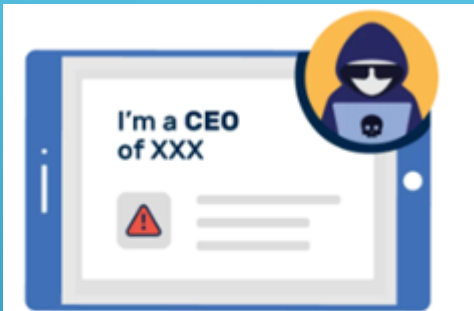


DMARC - Domenebasert meldingsautentisering, rapportering og overensstemmelse



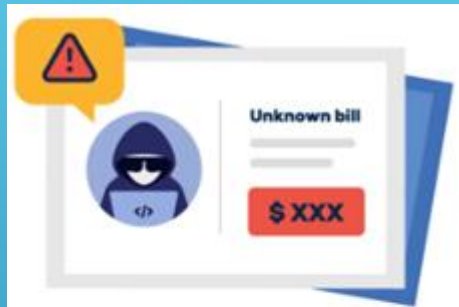
Domene Message Authentication Reporting and Conformance, eller DMARC, er en e-postautentiseringsmetode som fokuserer på å håndtere problemet med e-postforfalskning ved å beskytte både avsenderen og mottakeren. Din DMARC-post instruerer mottaksserveren om ikke å akseptere en e-post hvis den mislykkes i DKIM- og SPF-sjekker.

KRIMINELLE KAN TA OVER DIN MERKEVARE



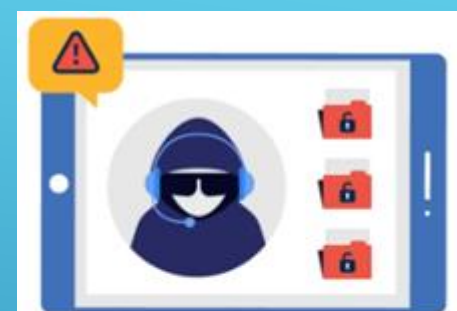
CEO Fraud

The attacker, pretending to be a top-level executive, sends emails to your employees requesting money transfers or access to confidential databases.



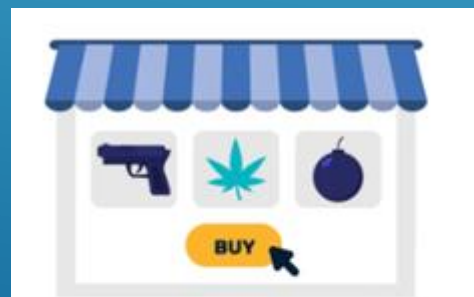
Fake Invoices

A hacker impersonating one of the organisation's vendors could raise fake invoices that cost companies millions of dollars.



Login Credential Theft

By pretending to be from customer support at your business, an attacker can steal information from your partners and customers.



Selling Illegal Goods

Attackers can use your domain to sell illegal goods online like drugs or weapons, which could land you in serious trouble.



Spreading Ransomware

Malicious emails often contain fake links or attachments that can install ransomware on the target's device.

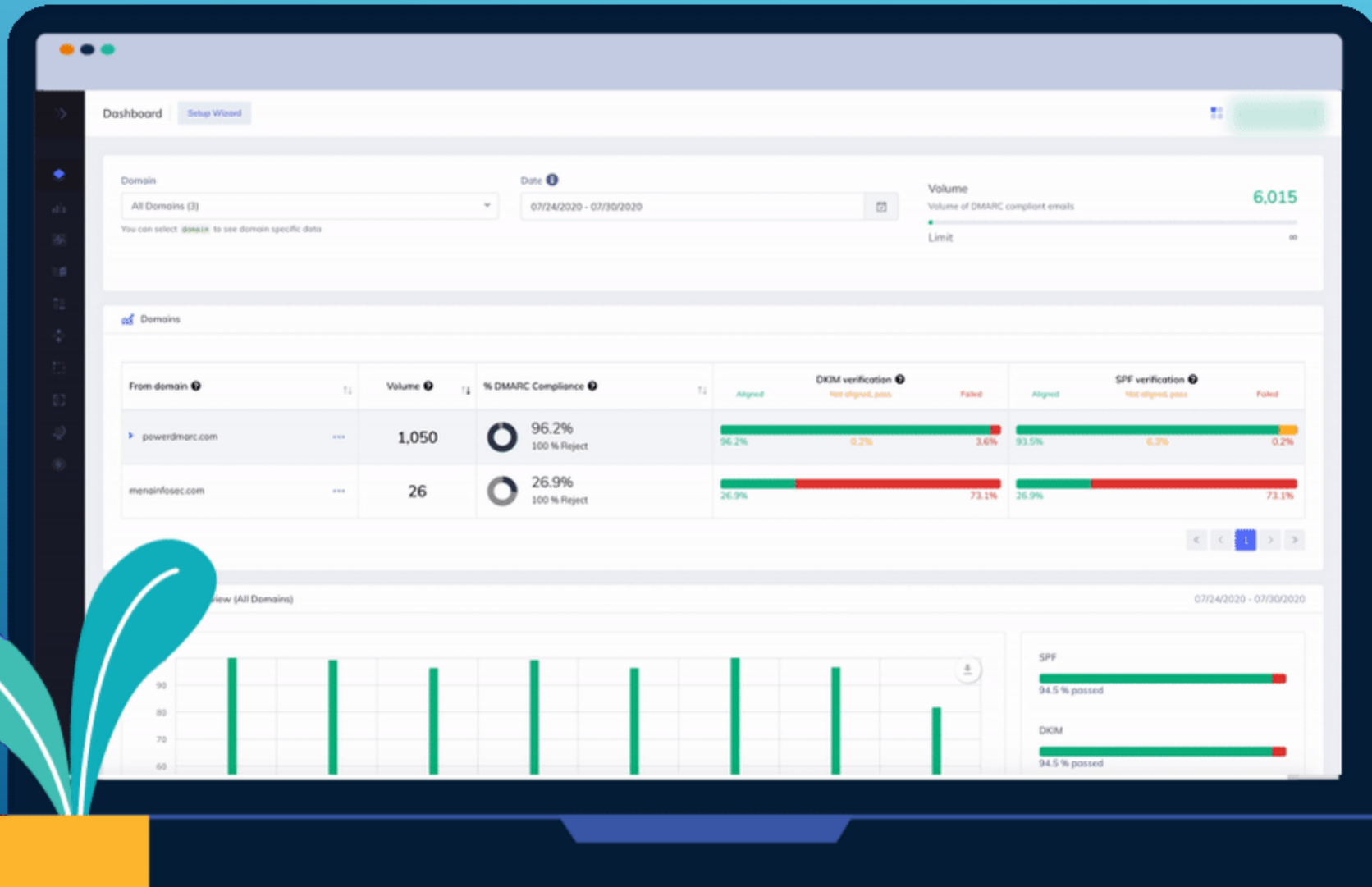


Legal Risks

When hackers use your domain to steal money or data from people, it can lead to lawsuits against your organization.

PowerDMARC Dashboard

An overview of your entire domain on a single pane of glass. Get total visibility on everything happening in your domain, and dive deep into the smaller details with our interactive charts and widgets.



DMARC Compliance

The percentage of emails sent from your domain that align with DMARC

SPF & DKIM alignment

Percentage of emails that align with SPF and DKIM respectively

PowerDMARC Top 5 Threats

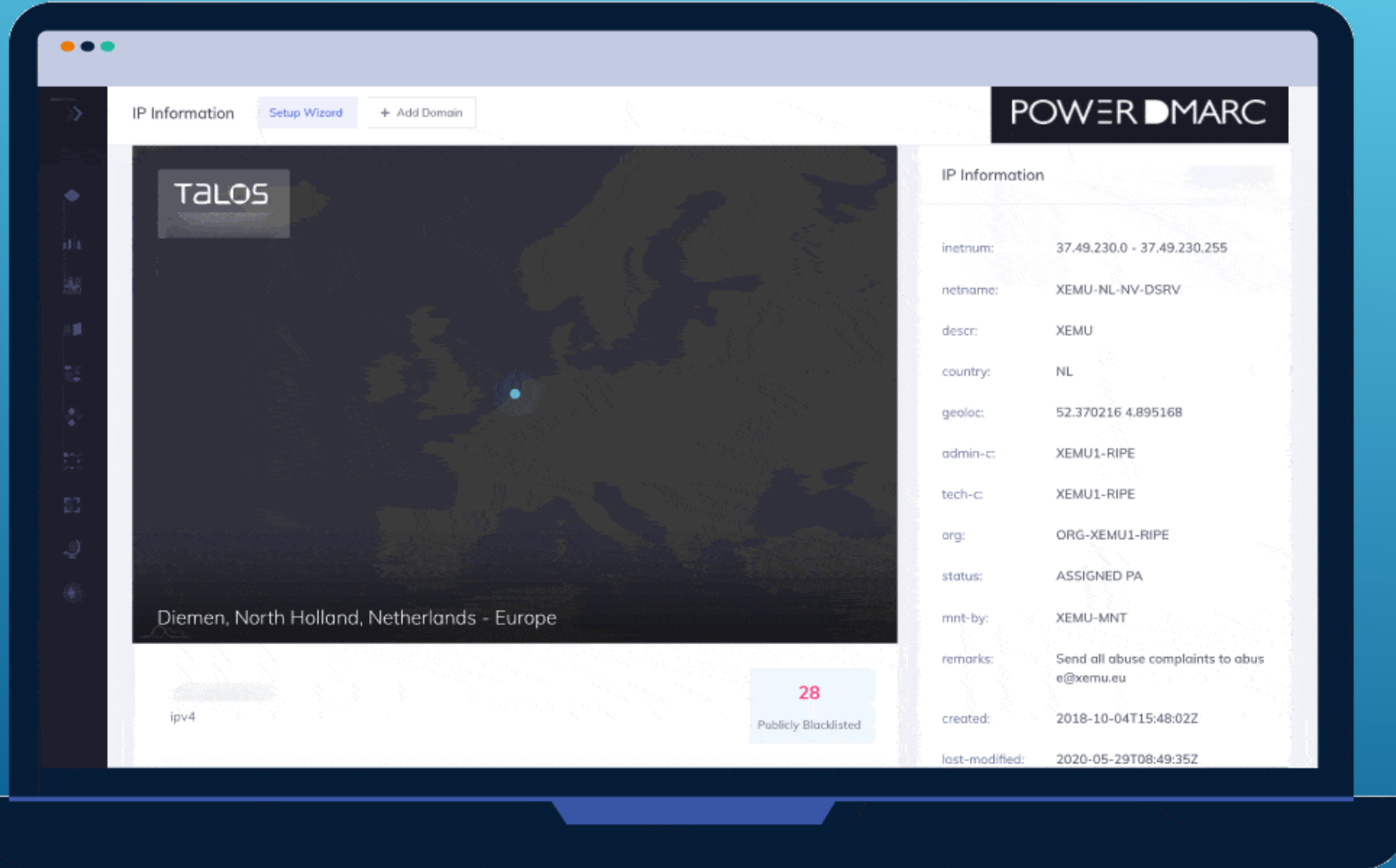
5 IP addresses that pose the biggest potential threats to your domain

Outbound Email Overview

View the proportion of your emails that are passing DMARC

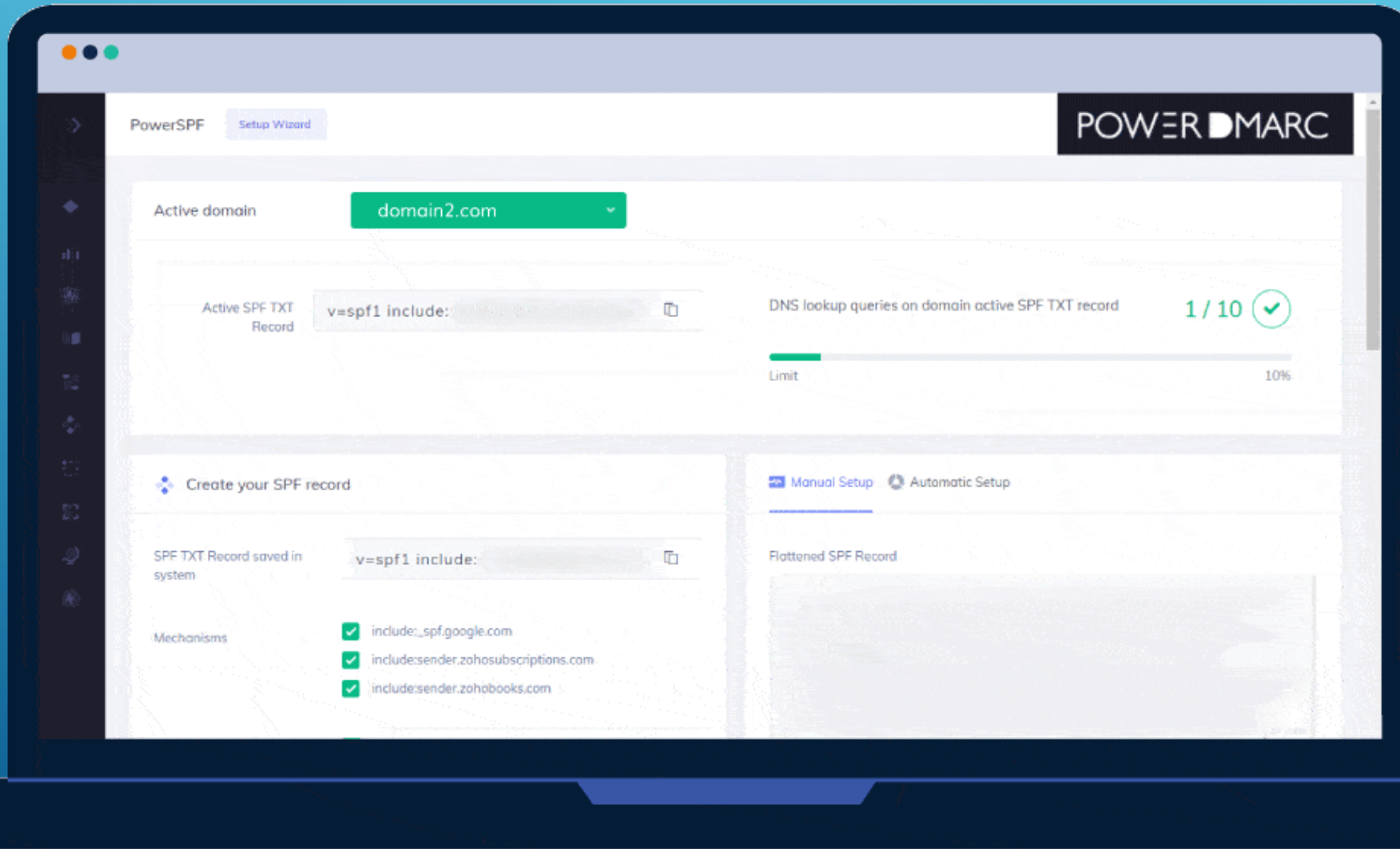
Trusselintelligens

Forbi et visst punkt blir det upraktisk å overvåke hver enkelt IP-adresse som utgjør en forfalskningsfare for domenet ditt. Ikke bare må du vite når en ny ondsinnet kilde dukker opp, men du må bli varslet når et angrep pågår.



PowerDMARC's proprietære DMARC Threat Intelligence (TI)-motor er din personlige vakt på døgnavakt, 24/7. Vår AI-baserte trusseloppdagelsestjeneste bruker spesialiserte algoritmer for raskt å identifisere de globale svartelistene som hver IP er plassert på, samt den sendende vertsnavnets e-post omdømme. Alt fungerer på et detaljnivå som et menneske aldri kunne matche.

Null risiko PowerSPF

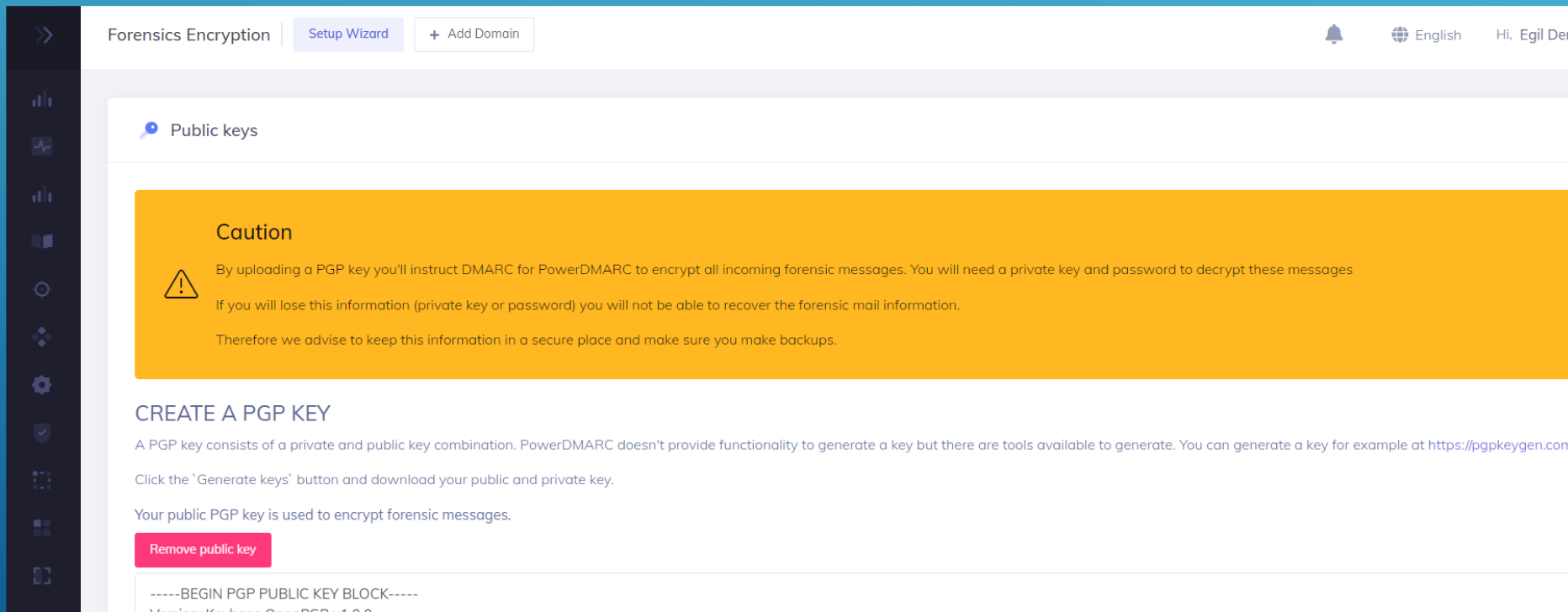


Én-klikks automatisk SPF med ubegrensede oppslag som aldri overskrider 10 oppslagsgrensen! En automatisk tilnærming til din Sender Policy Framework.

KRYPTERING

PowerDMARC lar deg kryptere alle dine DMARC Forensic RUF-rapporter mens de genereres. For å gjøre det enda sikrere, kan du generere ditt eget nøkkelverdi-par for å kryptere RUF-dataene dine. Vi har null tilgang til krypteringsnøkkelen din.

RUF-rapporter kan potensielt inneholde noe personlig informasjon fra e-posten. Dette inkluderer: Ditt 'Fra' domene Tidspunktet e-posten ble mottatt IP-adressen til serverne som sendte e-posten Emnefeltet DMARC, SPF, DKIM bestått/ikke bestått resultater Overskriftene til den mislykkede e-posten



The screenshot shows the 'Forensics Encryption' interface. At the top, there are navigation links for 'Setup Wizard' and '+ Add Domain'. The main content area is titled 'Public keys' and features a prominent yellow 'Caution' box. The caution message states: 'By uploading a PGP key you'll instruct DMARC for PowerDMARC to encrypt all incoming forensic messages. You will need a private key and password to decrypt these messages. If you will lose this information (private key or password) you will not be able to recover the forensic mail information. Therefore we advise to keep this information in a secure place and make sure you make backups.' Below the caution box, there is a section titled 'CREATE A PGP KEY' which explains that a PGP key consists of a private and public key combination and provides instructions on how to generate one. A 'Remove public key' button is visible at the bottom of the section.

HOSTED DMARC

DMARC Policy

Set the enforcement policies to protect your domain.



None

Outgoing emails that are not authorized will still be accepted by the receiving server and will be placed in the recipient's mailbox



Quarantine

Outgoing emails that are not authorized will be placed on the spam folder of the recipient's mailbox



Reject

Outgoing emails that are not authorized will not be accepted by the receiving server and won't be placed in the recipient's mailbox

DMARC Policy percentage

The policy percentages defines how strict the policy will work. You can set the preferred percentage by using the slider below.

100%



Kart over trusler



Verktøy for sanntids overvåking av DMARC for e-postforfalskingsangrep som finner sted på ulike steder rundt om i verden.

Med vårt avanserte DMARC-overvåkningsverktøy får du full synlighet på ditt domene.

PowerAlerts genererer varslinger :

PowerDMARC's varslingsystem overvåker ditt domene og gjør deg oppmerksom på domenerelaterte hendelser i sanntid. Du spesifiserer hvilken type DNS-endringer og metrikker du ønsker å spore, og en e-postvarsling sendes til den angitte adressen din når en slik varsling utløses. På denne måten trenger du ikke å logge inn gjentatte ganger på portalen din for å få synlighet. Du vil kunne overvåke domenene dine eksternt fra e-postkontoen din, og dermed handle raskere mot eventuelle problemer.

PowerAlerts Generates Alerts Pertaining to 3 Different Categories:



PDF rapporter

The screenshot displays the 'Basic Reports' interface in the PowerDMARC dashboard. It includes a search bar for domains, a reporting period selector (07/14/2020 - 07/20/2020), and an 'Export pdf report' button. Below this is a table for 'Scheduled Reports' which is currently empty, showing columns for Domain, Frequency, Emails, and Date Of Next Scheduled Report. A 'PDF' icon is visible in the top right corner of the report preview area.

Basic Reports

Export your basic DMARC overview reports or schedule them to be sent by email

Domain: [input field] Reporting Period: 07/14/2020 - 07/20/2020 [calendar icon] **Export pdf report**

You can select domain to see domain specific data

+ Add Schedule

Scheduled Reports

Domain	Frequency	Emails	Date Of Next Scheduled Report
No records found			

PDF

3.0 DMARC deployment status

1.1 Domain protected powerdmarc.com **1.2 DMARC policy** p = reject

2.0 Reporting period 14 Jul 2020 - 20 Jul 2020

3.0 Results

3.1 DMARC Compliance overview

Category	Value
Invalid emails sent	~5
Compliance rate	~95

3.2 Outbound email overview

Category	Percentage
Threats/Unknowns	0%
DMARC compliant emails	96.1%
Forwarded emails	1.9%

Document Classification: Confidential
www.powerdmarc.com

Med PowerDMARC kan du konvertere rapportene dine til praktiske PDF-dokumenter som kan deles med hele teamet ditt. Du kan planlegge å få dem sendt regelmessig til e-posten din, eller bare generere dem etter behov.

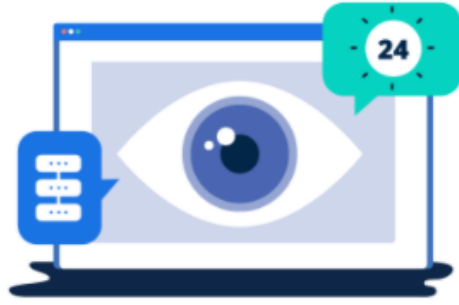
Implementere PowerDMARC



1

Setting Up PowerDMARC

Configure your domain, DMARC policy and aggregate reporting, then publish the DMARC record to your DNS



2

PowerDMARC Analysis

Over 1-2 weeks, you will get full visibility and analysis of whom and what is sent across the Internet on behalf of your organization domain.



3

Enforce DMARC

By analyzing your reports, we authorize legitimate sources & identify malicious ones



4

100% DMARC Compliance

With a policy of p=quarantine or reject, you're safe from domain spoofing!



Uten DMARC i policy REJECT så er det risiko for at:

- Ditt domene blir brukt til dataangrep på andre inkludert kunder, leverandører og samarbeidspartnere.
Konsekvens: Tap av kunder og business, og tap av virksomhetens omdømme og merkevare. Risiko for søksmål.
- Dine sendte epost blir feilaktig klassifisert som spam av mottaker.
Konsekvens: Viktig epost, tilbud, kontrakter eller annet kommer ikke frem eller blir forsinket
- Markedsmail og massemail får inntil 10 % lavere leveringsrate.
Konsekvens: Tap av business og inntekter
- Du kan selv bli angrepet av falske epost som bruker ditt eget domene.
Konsekvens: Økt sjans for å bli utsatt for dataangrep, ransomware, datatap, nedetid og svindel