

Certifica la tua reputazione email e proteggi la consegna dei messaggi con DMARC.

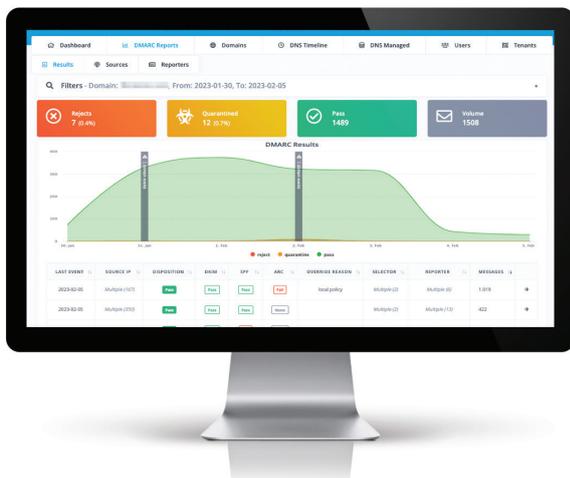
Si stima che ogni giorno vengano inviate 3,4 miliardi di email di phishing e lo spoofing, ossia l'invio di email con un indirizzo mittente contraffatto, rappresenta il 50% delle frodi di cybersecurity. Il DMARC è un protocollo che protegge i domini dall'utilizzo non autorizzato, certificando che i messaggi sono protetti da SPF e/o DKIM e offrendo al destinatario la possibilità di rigettare o contrassegnare come sospette le email che non superano questa verifica. Libraesva LetsDMARC rende incredibilmente facile l'impostazione del DMARC per proteggere il proprio dominio, con approfondimenti immediati sui flussi di posta elettronica, così da assicurarne il controllo.



OTTIENI VISIBILITÀ

Ottieni la visibilità sulle fonti e sui flussi di email che utilizzano il tuo dominio. Riconosci i mittenti validi, come i servizi di email marketing, CRM, assistenza e altri servizi utilizzati, e scopri qualsiasi uso non autorizzato o erroneamente configurato.

- Aggregazione dei dati RUA XML dettagliati inviati dagli ISP, con visualizzazioni della dashboard di facile comprensione
- Offre la possibilità di conoscere tutte le fonti che inviano email per conto del proprio dominio e di identificare l'origine del traffico email che fallisce il controllo.
- Consente una visualizzazione immediata del flusso di messaggi nel tempo, con il volume delle email, i tassi di accettazione, quarantena e rifiuto
- Descrive dettagliatamente i motivi del fallimento dell'autenticazione



ASSUMI IL CONTROLLO

Libraesva LetsDMARC identifica le fonti legittime autorizzate ad inviare email per vostro conto. Offre la possibilità di monitorare e apportare modifiche in modalità osservazione e, in seguito, di aumentare il livello della policy per indicare agli ISP di rifiutare o contrassegnare come sospetti i messaggi non conformi.

- Rende possibile la gestione di DMARC, DKIM e SPF da un portale intuitivo senza dover accedere continuamente al proprio DNS e separarne la gestione per la parte legata al servizio email
- Individua gli errori di allineamento e configurazione; l'analisi intelligente di "cosa è successo" fornisce spiegazioni di facile comprensione ed indicazioni sui passi successivi da compiere
- Permette la visualizzazione di ogni modifica apportata ai record DMARC, DKIM e SPF, nonché quelle effettuate da terze parti derivate da inclusioni nel record SPF, con valori precedenti e successivi tracciati ed evidenziati nella timeline del DNS



- ✓ Configurazione guidata, non richiede competenze in materia di DNS
- ✓ Gestione dei record DMARC, DKIM e SPF da un'unica console
- ✓ Analisi e aggregazione automatica dei report RUA
- ✓ Dashboard con visibilità del flusso di email
- ✓ Analisi intelligente dei risultati per identificare gli errori

- ✓ Descrizioni degli eventi e indicazioni sull'efficacia in consegna delle email
- ✓ Ottimizzazione SPF per superare il limite delle 10 risoluzioni all'interno del record
- ✓ Monitoraggio DNS con storico di ogni modifica DMARC, DKIM e SPF
- ✓ Timeline intuitiva delle modifiche al DNS e del loro impatto sui risultati DMARC
- ✓ Personalizzazione dell'interfaccia utente con logo e colori aziendali

DMARC SENZA SFORZO CON LA CONFIGURAZIONE GUIDATA...



AUMENTA LA SICUREZZA

Impedisce ai criminali informatici di inviare email fraudolente a partner, dipendenti e clienti della vostra azienda, effettuando lo spoofing o impersonando i vostri domini di invio.

- Blocca la consegna delle email che falsificano il vostro indirizzo "da", per ridurre le frodi basate sulle email
- Supera il limite di 10 risoluzioni nel record SPF e migliora la sicurezza nascondendo le fonti di invio autorizzate con l'ottimizzazione del record SPF

MIGLIORA L'EFFICACIA IN CONSEGNA

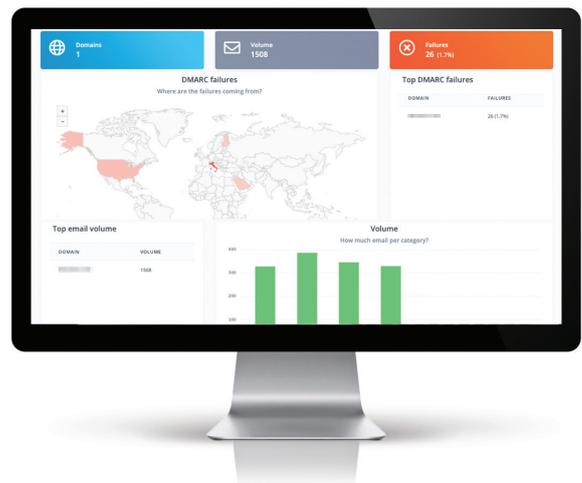
Blocco delle fonti non autorizzate che inviano per conto del proprio dominio; la reputazione come mittente di email sarà migliore, contribuendo così ad ottimizzare l'efficacia in consegna.

- Migliora la reputazione presso gli ISP riducendo lo spam e i bounce ed aumentando il coinvolgimento nelle email
- Aumenta i tassi di efficacia in consegna per il traffico email autentico



DA QUALI MINACCE PROTEGGE IL DMARC?

Senza DMARC, gli spoofer possono rubare informazioni di identificazione personale (PII) inviando email che sembrano provenire dal proprio dominio; questo avviene falsificando l'indirizzo "da" dell'intestazione, cioè quello visibile nel campo Da.



Ready to get started?

sales@libraesva.com

www.libraesva.com



Libraesva è un'azienda pluripremiata nel campo della sicurezza delle email, nominata Leader di categoria Email Security per il 2022 da GetApp, una società di Gartner. Inoltre, Libraesva è costantemente certificata da Virus Bulletin come uno dei migliori sistemi di sicurezza delle email e gode della fiducia di marchi leader in tutto il mondo.

/LIBRAESVA

LetsDMARC 