Vollständiger DMARC-Schutz

/LIBRAESVA

Übernehmen Sie die Kontrolle über Ihre E-Mail-Reputation und sichern Sie die Zustellung Ihrer Nachrichten mit DMARC.

Jeden Tag werden schätzungsweise 3,4 Milliarden Phishing-E-Mails verschickt, und Spoofing - E-Mails, die mit einer gefälschten Absenderadresse verschickt werden - wird bei 50 % der Betrugsfälle im Bereich der Cybersicherheit eingesetzt. DMARC ist ein Protokoll zum Schutz von Domains vor unbefugter Nutzung. Es zeigt an, ob Nachrichten durch SPF und/oder DKIM geschützt sind, und teilt dem Empfänger mit, ob er Nachrichten in den Papierkorb werfen oder zurückweisen soll. Mit Libraesva LetsDMARC ist es unglaublich einfach Ihre Marke zu schützen und Sie erhalten einen sofortige Einblick in Ihren E-Mail-Strom, so dass Sie Ihre Domain unter Kontrolle haben.

VISIBILITÄT ERHALTEN

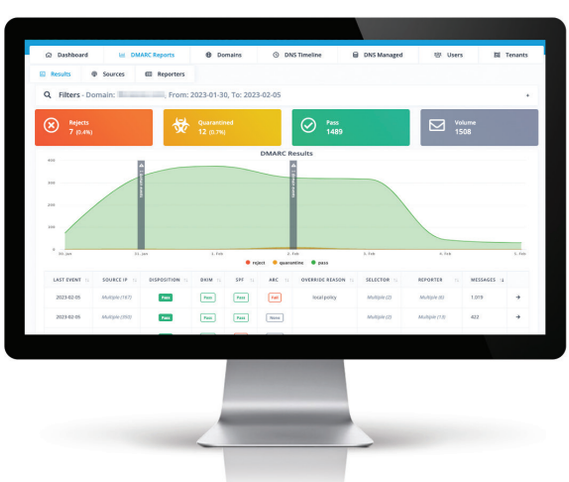
Verschaffen Sie sich einen Überblick über die Quellen und E-Mail-Ströme der von Ihrer Domain gesendeten Nachrichten. Erkennen Sie gültige Absender - wie E-Mail-Marketing, CRM, Support und andere von Ihnen genutzte Dienste - und decken Sie jede nicht autorisierte Nutzung Ihrer Marke auf.

- Erkennen Sie die detaillierten XML-RUA-Daten, die von ISPs gesendet werden, mit leicht verständlichen Dashboard-Visualisierungen
- Erkennen Sie alle Quellen, die E-Mails im Namen Ihrer Domain senden, und identifizieren Sie den Ursprung des E-Mail-Verkehrs, der nicht authentifiziert wurde.
- Erhalten Sie einen Überblick über den Nachrichtenfluss im Zeitverlauf, mit E-Mail-Volumen, Durchlass-, Quarantäne- und Ablehnungsraten
- Drill-Down-Erklärung der Gründe für Authentifizierungsfehler

KONTROLLE ÜBERNEHMEN

Identifizieren Sie legitime Quellen, die berechtigt sind, in Ihrem Namen E-Mails zu versenden, und authentifizieren Sie diese. Überwachen Sie und nehmen Sie Anpassungen im Beobachtungsmodus vor - setzen Sie dann Richtlinien durch, um ISPs anzuweisen, fehlgeschlagene Nachrichten abzulehnen oder zu verwerfen.

- Verwalten Sie DMARC, DKIM und SPF über ein intuitives Portal, ohne auf Ihr DNS zugreifen zu müssen.
- Ermitteln Sie Ausrichtungs- und Konfigurationsfehler. Intelligente "Was ist passiert"-Analysen liefern leicht verständliche Erklärungen und Anleitungen für die nächsten Schritte
- Sehen Sie jede Änderung an DMARC, DKIM und SPF - sowie an Domänen von Drittanbietern, die in SPF enthalten sind - mit Vorher- und Nachher-Werten, die in der DNS-Zeitleiste verfolgt und hervorgehoben werden.



- ☑ Geführte Konfiguration, so dass keine DNS-Kenntnisse erforderlich sind
- ☑ Verwalten Sie DMARC, DKIM, SPF von einer einzigen Konsole aus
- ☑ Automatisches Parsen und Aggregieren von RUA-Berichten
- ☑ Das Dashboard bietet Einblicke in den E-Mail-Fluss
- ☑ Intelligente Ausrichtungsanalyse zur Fehlererkennung
- ☑ Was geschah Erklärungen zu fixen Konfigurationen
- ☑ SPF-Abflachung zur Überwindung der 10-Datensatz-Grenze
- ☑ DNS-Überwachung verfolgt jede DMARC-, DKIM- und SPF-Änderung
- ☑ Eine Zeitleiste bietet einen Überblick über DNS-Änderungen
- ☑ Personalisieren Sie die Benutzeroberfläche mit Ihrer Marke

Vollständiger DMARC-Schutz

/LIBRAESVA

MÜHELOSES DMARC MIT GEFÜHRTER KONFIGURATION…

IDENTIFIZIEREN

Identifizieren
Legitime Quellen IDENTIFIZIEREN und sie authentifizieren

OBSERVE

Überwachen
& einstellen

AKTIVIEREN

Aktivieren
um fehlgeschlagene Nachrichten abzulehnen oder zu verwerfen

SICHERHEIT ERHÖHEN

Verhindern Sie, dass Cyberkriminelle betrügerische E-Mails an Ihre Geschäftspartner, Mitarbeiter und Kunden senden, indem sie Ihre Absenderdomänen fälschen oder sich als solche ausgeben.

- Blockieren Sie die Zustellung von E-Mails, die Ihre "Absender"-Adresse fälschen, um E-Mail-Betrug zu verhindern
- Überwinden Sie das Limit von 10 SPF-Einträgen und erhöhen Sie die Sicherheit, indem Sie Ihre autorisierten Absenderquellen mit SPF-Flattening verbergen

ZUSTELLBARKEIT VERBESSERN

Wenn nicht autorisierte Quellen daran gehindert werden, im Namen Ihrer Domäne zu senden, wird Ihr Ruf als E-Mail-Versender gestärkt, was zur Verbesserung der Zustellbarkeit Ihrer E-Mails beiträgt.

- Verbessern Sie den Ruf Ihrer Marke bei ISPs, indem Sie Spam und Bounces reduzieren und das E-Mail-Engagement erhöhen
- Erhöhen Sie die Zustellbarkeitsraten für Ihren echten E-Mail-Verkehr

GEGEN WELCHE BEDROHUNGEN SCHÜTZT DMARC?

Ohne DMARC können Spoofers persönlich identifizierbare Informationen (PII) stehlen, indem sie E-Mails versenden, die scheinbar von Ihrer Domäne zu stammen scheinen. Sie tun dies, indem sie die "Von"-Adresse in der Kopfzeile fälschen - das ist die sichtbar im Von: Feld.

Ready to get started?

sales@libraesva.com

www.libraesva.com

Libraesva ist ein preisgekröntes E-Mail-Sicherheitsunternehmen, das als „Category Leader" für 2022 in E-Mail-Sicherheit von GetApp, einem Gartner-Unternehmen, ausgezeichnet wurde. Libraesva wird regelmäßig von Virus Bulletin als eines der besten E-Mail-Sicherheitssysteme zertifiziert und wird von führenden Marken auf der ganzen Welt vertraut.

/LIBRAESVA
LetsDMARC