SENDMARC

Der DMARC-Vorteil für MSPs:

E-Mail-Sicherheit direkt zu den Entscheidern bringen

www.sendmarc.com

Das erwartet Sie

DMARC nutzen, um Ihr Service-Angebot zu differenzieren

Mit der Weiterentwicklung der Cyberbedrohungslandschaft hat Datenschutz für Unternehmen höchste Priorität. Wenn Vulnerability Scanning, Intrusion Detection sowie Datensicherung und -wiederherstellung nicht mehr ausreichen, um Cyberkriminalität wirksam zu bekämpfen, brauchen Sie als MSP eine zukunftsweisende Strategie und einen klaren Wettbewerbsvorteil im IT-Portfolio.

Die Lösung ist DMARC. DMARC steht für Resilienz, Reaktionsfähigkeit und das konsequente Streben nach Erfolg im Kampf gegen Cyberkriminelle.

Die globale MSP-Branche wird bis 2028 voraussichtlich ein Volumen von **mehr als 372 Milliarden US-Dollar erreichen**. Nordamerika ist dabei der größte Markt, gefolgt von Europa und der Region Asien-Pazifik. Mit diesem Wachstum werden mehr MSPs in den Markt eintreten – und der Wettbewerb wird noch härter.

Es reicht nicht mehr aus, dass Sie als MSP lediglich das naheliegende Paket aus Backup- und Schutzservices anbieten. Sie benötigen ein robustes und kompatibles Tool, das gegen die wachsende Komplexität und die zunehmende Raffinesse von Sicherheitsbedrohungen gewappnet ist.

Domain-based Message Authentication, Reporting & Conformance (DMARC) ist das bevorzugte Protokoll für aufstrebende und skalierende MSPs. Es ist ein ideales Tool, das über die klassische Firewall hinausgeht, seine Intelligenz über das Übliche hinaus erweitert und Spoofing- sowie Phishing-Angriffe unterbindet – bei gleichzeitig geringem und reibungslosem Infrastrukturaufwand.

Für MSPs ist es entscheidend, relevant und hochgradig wettbewerbsfähig zu bleiben, um das Geschäft zu skalieren und langfristige Glaubwürdigkeit sowie Vertrauen bei wichtigen Partnern aufzubauen.

Um den Vorteil zu nutzen, benötigen Sie als MSP drei strategische Schritte, um erfolgreich zu sein:

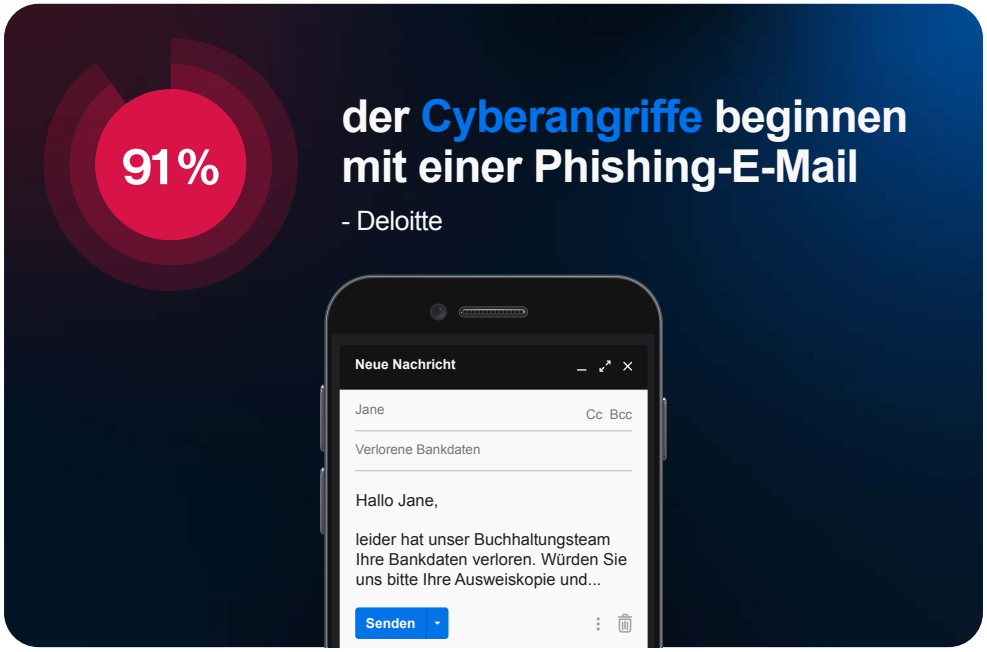
#1 Die E-Mail-Sicherheit Ihrer Kunden stärken

#2 Kundenvertrauen aufbauen und sichern

#3 Kompromisslose Präzision umsetzen

Strategischer Schritt Nr. 1

Die E-Mail-Sicherheit Ihrer Kunden stärken



E-Mails stehen an vorderster Front im Unternehmen Ihrer Kunden und sollten gegen Cyber-Eindringlinge abgesichert werden. DMARC erweist sich zunehmend als globaler Erfolg im Kampf gegen Cyberkriminalität: Insbesondere durch das Abfangen bösartiger E-Mails schützt DMARC Absender und Empfänger vor fortschrittlichen Bedrohungen, die Auslöser einer Datenschutzverletzung sein können.

Mit DMARC können Sie als MSP einen proaktiven Ansatz zum Schutz der IT-Infrastruktur Ihrer Kunden demonstrieren. So gehen Sie über rein reaktive Basismaßnahmen hinaus und arbeiten aktiv daran, potenzielle Bedrohungen zu erkennen und einzudämmen, bevor sie erheblichen Schaden verursachen. Dieser proaktive Ansatz stärkt das Vertrauen der Kunden. Gleichzeitig positionieren Sie sich als verlässlichen Sicherheitspartner.

www.sendmarc.com

Der DMARC-Vorteil für E-Mail-Sicherheit

DMARC ermöglicht die Authentifizierung und Validierung ausgehender E-Mails und reduziert so das Risiko von Phishing- und Spoofing-Angriffen.

DMARC reduziert Schwachstellen, indem es nicht autorisierte E-Mails blockiert. So werden Identitätsmissbrauch und Markenmissbrauch verhindert.

Der Einsatz einer DMARC-Plattform entlastet Sie als MSP bei der E-Mail-Sicherheit, indem Authentifizierungs- und Validierungsprozesse automatisiert und so Ressourcen frei werden. Das sorgt für eine proaktive Abwehr von E-Mail-Bedrohungen und ermöglicht es Ihren Teams, sich auf Aktivitäten mit höherer Wertschöpfung zu konzentrieren.

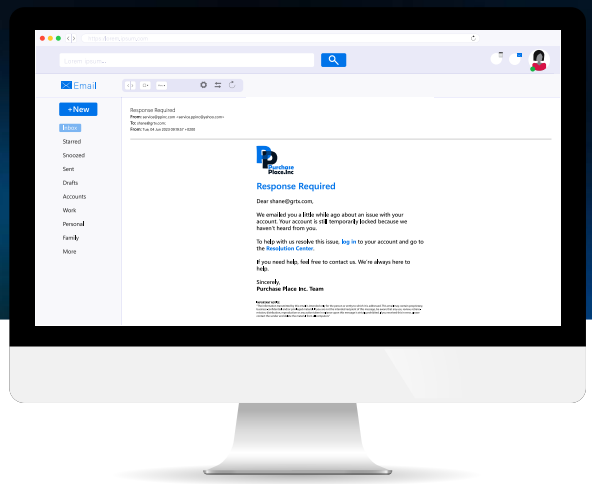
Strategischer Schritt Nr. 2

Kundenvertrauen aufbauen und sichern

Nur 19,6 % der E-Mail-Domains mit aktiviertem DMARC verfügen über vollständigen Schutz durch eine p=reject DMARC-Richtlinie. Damit bleibt die Mehrheit Cyberangriffen ausgesetzt. Das unterstreicht eine erhebliche Chance für Sie als MSP.

- dmarc.org

*Diese Statistik stammt aus einem spezifischen Datensatz, der ausschließlich Domains untersucht, die DMARC verwenden, und nicht alle E-Mail-Domains weltweit abdeckt. Es wird davon ausgegangen, dass die Trends dieses Datensatzes internetweite Entwicklungen widerspiegeln und daher wertvolle Einblicke liefern.



Als MSP gilt: Zeit ist Geld – und Geld hängt davon ab, wie schnell ein System nach einem Angriff reagieren kann. Aus diesem Grund schafft das veraltete Break-Fix-Modell kein Vertrauen mehr zwischen Ihnen als MSP und Ihren Kunden. Der Erfolgsmaßstab verlangt heute eine kompromisslose, agile Reaktion auf einen Spoofing-Angriff. Proaktiver Schutz ist Ihr Vorteil als MSP, um Kundenvertrauen aufzubauen und langfristig zu sichern.

Der DMARC-Vorteil für schnelle Reaktion

DMARC nutzt Live-Monitoring und Reporting, um in Echtzeit wirken zu können. Mit diesen Funktionen können Sie als MSP E-Mail-bezogene Vorfälle schnell erkennen und darauf reagieren, Reaktionszeiten verbessern und potenzielle Schäden reduzieren.

Eine DMARC-Plattform ermöglicht schnelle Richtlinienanpassungen. Sie vereinfacht die Umsetzung von Richtlinienänderungen über mehrere Domains hinweg und erlaubt Ihnen als MSP, Sicherheitsmaßnahmen anzupassen, sobald neue Bedrohungen entstehen. Diese Flexibilität stellt sicher, dass sich weiterentwickelnde Angriffe schnell eingedämmt werden.

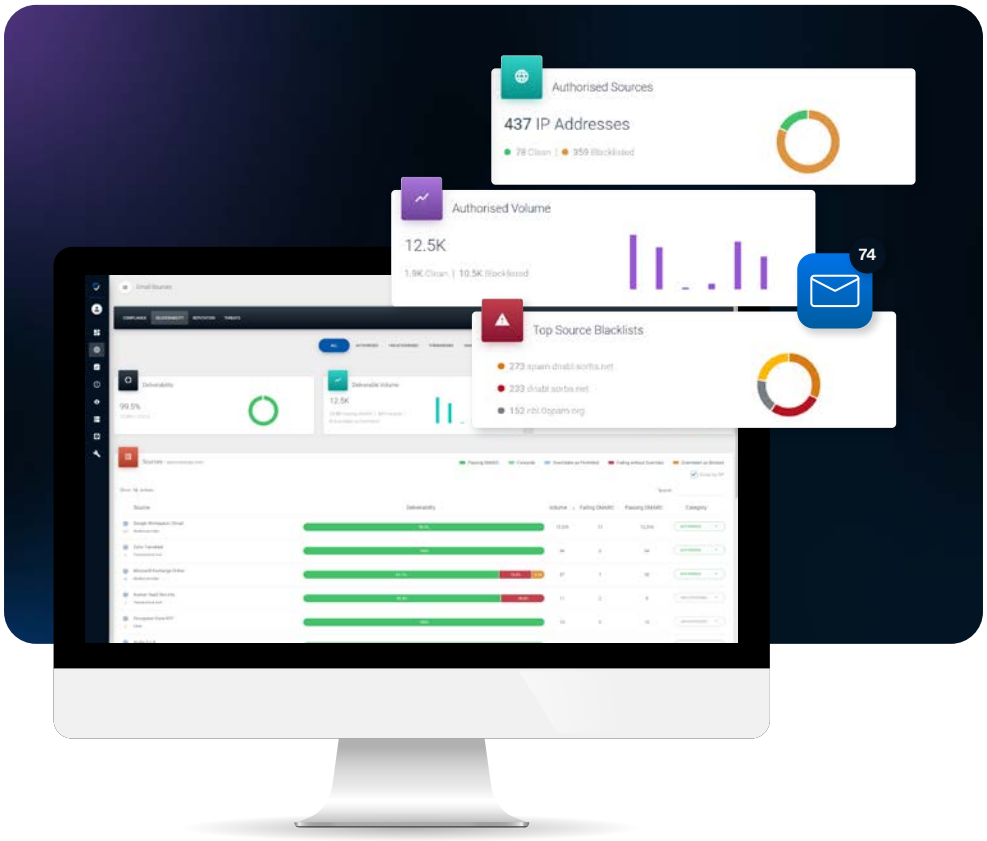
Mit einer DMARC-Plattform können Sie als MSP die Kundeninfrastruktur mithilfe automatisierter Tools proaktiv scannen sowie Logs und Warnmeldungen prüfen. Diese präventive Funktion hilft Ihnen als MSP, auf Bedrohungen zu reagieren, bevor erheblicher Schaden entsteht.

Als MSP können Sie proaktiven E-Mail-Schutz priorisieren, Vertrauen aufbauen und sich als Anbieter positionieren, der sich konsequent der Kundensicherheit verpflichtet.

DMARC ermöglicht es Ihnen als MSP, Kunden, deren Mitarbeitende und Entscheider aktiv in Cybersecurity einzubinden. Ein umfassender Ansatz bedeutet, über das klassische Firewall-Gespräch hinauszugehen und tiefgreifende, relevante Lösungen anzubieten, die Kunden weiterbilden – während sie gleichzeitig ihre Arbeit erledigen können.

Strategischer Schritt Nr. 3

Kompromisslose Präzision sicherstellen



Durch die Implementierung eines DMARC-Protokolls mit optimiertem Reporting, vereinfachter Bereitstellung, Automatisierungsinnovation und Expertenunterstützung können Sie als MSP einen kompromisslosen Ansatz etablieren, um Kunden vor E-Mail-basierten Angriffen wie Spoofing und Phishing zu schützen.

Der DMARC-Vorteil für Präzision

Optimiertes Reporting und Analyse:
Einige DMARC-Plattformen wie Sendmarc erstellen umfassende Reports und Analysen. Diese Berichte ermöglichen es Ihnen als MSP, Trends zu erkennen, Schwachstellen zu bewerten und datenbasierte Entscheidungen zur Stärkung der E-Mail-Sicherheit zu treffen.

Vereinfachte Bereitstellung und Verwaltung:
Als MSP können Sie eine benutzerfreundliche DMARC-Plattform nutzen, die intuitive Oberflächen bietet. Dadurch lassen sich DMARC-Richtlinien in unterschiedlichen Kundenumgebungen leichter bereitstellen, konfigurieren und verwalten.

Automatisierungsinnovation: Es ist wichtig, eine DMARC-Plattform zu wählen, die präzise und automatisierte Workflows unterstützt, in einem sich ständig wandelnden Markt fortschrittlich bleibt und ausreichend skalierbar ist, um zunehmenden E-Mail-Traffic sowie eine wachsende Zahl von Kunden effizient zu bewältigen.

Expertenunterstützung: Zuverlässiger Kundensupport und Zugang zu DMARC-Experten stellen sicher, dass präzise Informationen, fachkundige Unterstützung, Troubleshooting und Best-Practice-Empfehlungen verfügbar sind.

Eine profitable Ergänzung Ihres Produktportfolios

Erschließen Sie einen DMARC-Markt, der bis 2028 voraussichtlich einen Wert von 1,72 Milliarden US-Dollar erreichen wird.

DMARC ist eine profitable Ergänzung für Ihr Produktportfolio als MSP, weil es einen konkreten Bedarf Ihrer Kunden löst: die Stärkung ihrer Cyberabwehr gegen identitätsbasierte Angriffe und betrügerische Aktivitäten. Durch weniger Backend-Wartung, freigesetzte interne Ressourcen und skalierbare Implementierung über mehrere Kunden hinweg können Sie Ihre Profitabilität maximieren.

Mit vorhandener Expertise in Sicherheitsmaßnahmen können Sie als MSP DMARC nahtlos als leistungsstarkes und effizientes IT-Tool integrieren.

58 %

Die durchschnittliche Wachstumsrate bestätigter gültiger DMARC-Einträge im Jahresvergleich.

*Zur Berechnung der durchschnittlichen jährlichen Wachstumsrate von Dezember 2016 bis Juni 2022 wurde das arithmetische Mittel verwendet.

Fazit

Mit DMARC Erfolge feiern

Als MSP können Sie DMARC nutzen, um sich in einem wettbewerbsintensiven Markt abzuheben und die operative Effizienz mit einer Plattform zu verbessern, die Transparenz bietet und schnelle Änderungen zur Vermeidung von Cyberangriffen ermöglicht. Mit DMARC können Sie Phishing- und Spoofing-Angriffe ausmanövrieren und die E-Mail-Ökosysteme Ihrer Kunden absichern. Es ist der entscheidende Schritt, der Domains schützt, Sicherheit gibt und Kunden zufriedenstellt.

Die Wahl des richtigen DMARC-Partners ist entscheidend, da sie den Erfolg Ihrer E-Mail-Schutzstrategie als MSP direkt beeinflusst.

SENDMARC

Sendmarc ist ein führender DMARC-Anbieter mit einer Plattform, die auf die spezifischen Anforderungen von MSPs zugeschnitten ist. Unsere Mission ist es, MSPs mit umfassenden Tools zu unterstützen, welche die E-Mail-Sicherheit stärken, die operative Effizienz verbessern und Differenzierung in einer sich schnell entwickelnden Bedrohungslandschaft und einem wachsenden MSP-Markt ermöglichen.

Vorteile:

- **Multi-Tenant-Lösung**
- **Tools für Marketing- & Sales-Enablement**
- **Optimierte Workflows**
- **Onboarding, Training & Zertifizierung**

Kontaktieren Sie uns, um Ihre DMARC-Reise noch heute zu starten.

Prüfen Sie die Sicherheitsbewertung der E-Mail-Domain Ihres Kunden