SENDMARC

The DMARC advantage for MSPs:

Placing email security at the stakeholder’s feet

brigantia

What to expect

brigantia

Leveraging DMARC to differentiate your MSP

As the cyberthreat landscape evolves, data protection is a top priority for businesses. When vulnerability scanning, intrusion detection, and data backup and recovery are no longer enough to tackle the cybercrime arena, your MSP requires a cutting-edge strategy and competitive edge in its IT bouquet to ensure best play.

The solution is DMARC. It embodies resilience, responsiveness, and a relentless pursuit of victory against cybercriminals.

The global MSP market is expected to reach over $372 billion by 2028, with North America being the largest market followed by Europe and Asia-Pacific. With this growth, more MSPs will join the playing field, making competition even tougher.

It's no longer enough for your MSP to offer the obvious bouquet of backup and protection services, without the support of a combative and compatible tool that rises up against the growing complexities and sophistication of security threats.

Domain-based Message Authentication, Reporting, and Conformance (DMARC) is the protocol of choice for the emerging and scaling MSP. It's an ideal tool that transcends the traditional firewall, and stretches its intelligence beyond the norm, clamping down on spoofing and phishing attacks, while keeping infrastructure maintenance low and seamless.

As an MSP, staying relevant and highly competitive is essential to scaling business and building long-term credibility and trust among key stakeholders.

To gain the advantage, your MSP requires three strategic moves to play and win by:

#1 Strengthen client's email security

#2 Build and retain client trust

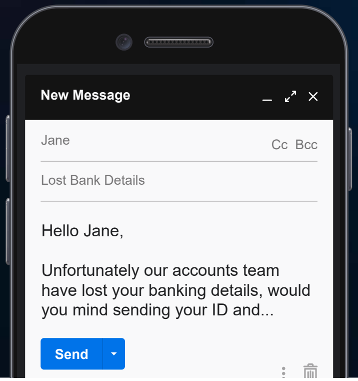
#3 Implement no-nonsense accuracy

Strategic move #1

Strengthen client's email security

91%

of **cyberattacks** begin with a phishing email - Deloitte



New Message

Jane

Cc Bcc

Lost Bank Details

Hello Jane,

Unfortunately our accounts team have lost your banking details, would you mind sending your ID and...

Emails are stationed at the frontline of your client's business and should be secured against cyberintruders. DMARC is quickly proving to be a global victory against cybercrime, with its particular interception of email crimes protecting senders and recipients from advanced threats that could be the source of an email data breach.

Using DMARC, your MSP can demonstrate a proactive approach to safeguarding clients' IT infrastructure. This enables you to go beyond basic reactive measures and actively work to identify and mitigate potential threats before they cause significant harm. This proactive approach enhances client confidence and establishes your MSP as a trusted partner in security.

The DMARC edge on email security

✓ **DMARC enables the authentication** and validation of outgoing emails, lessening the risk of phishing and spoofing attacks.

✓ **DMARC reduces vulnerability** by blocking unauthorized emails, preventing impersonation and brand abuse.

✓ **Using a DMARC platform** will lighten your MSP's email security workload by automating authentication and validation processes, freeing up resources. This ensures proactive defense against email threats and allows your team/s to focus on higher value-add activities.

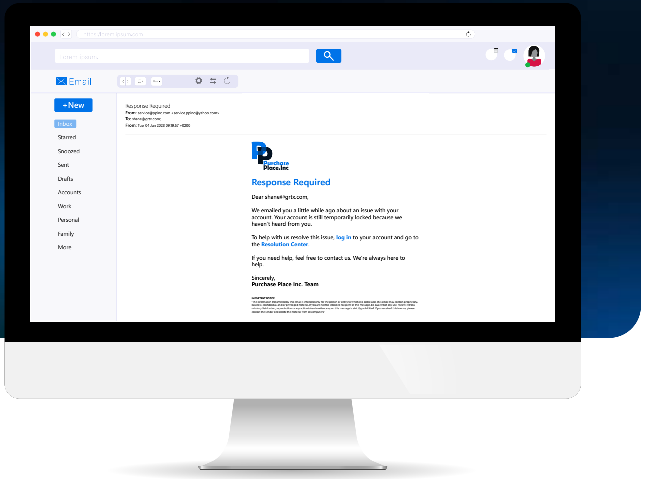
Strategic move #2

Build and retain client trust

Only 19.6% of email domains with DMARC enabled have full protection with a p=reject DMARC policy, leaving the majority exposed to cyberattacks. This highlights a significant opportunity for your MSP.

- dmarc.org

*This statistic comes from a specific dataset that examines only domains that use DMARC and doesn't cover all email domains globally. This dataset's trends are believed to represent internet-wide trends and so provide valuable insight.



Response Required
From: service@ppinc.com <service.ppinc@yahoo.com>
To: shane@grtx.com;
From: Tue, 04 Jun 2023 09:19:57 +0200

Response Required

Dear shane@grtx.com,

We emailed you a little while ago about an issue with your account. Your account is still temporarily locked because we haven't heard from you.

To help with us resolve this issue, log in to your account and go to the Resolution Center.

If you need help, feel free to contact us. We're always here to help.

Sincerely,
Purchase Place Inc. Team

IMPORTANT NOTICE
"The information transmitted by this email is intended only for the person or entity to which it is addressed. This email may contain proprietary, business-confidential, and/or privileged material. If you are not the intended recipient of this message, be aware that any use, review, retransmission, distribution, reproduction or any action taken in reliance upon this message is strictly prohibited. If you received this in error, please contact the sender and delete the material from all computers"

As an MSP, time is money, and money is dependent on the response time a system provides after an attack. For this reason, the outdated break-fix model no longer builds trust between your MSP and its customer, since the metric for success now calls for a no-nonsense, agile response to a spoofing attack. Proactive protection is your MSP's edge to building and retaining client trust.

brigantia

The DMARC edge on a speedy response

✓ **DMARC uses live monitoring and reporting** for real-time impact. Leveraging these capabilities, your MSP can quickly detect and respond to email-related incidents, improving response times and reducing potential damage.

✓ **A DMARC platform allows for rapid policy adjustments,** simplifying the process of implementing policy changes across multiple domains and allowing your MSP to adapt security measures as new threats emerge. This flexibility ensures quick mitigation of evolving attacks.

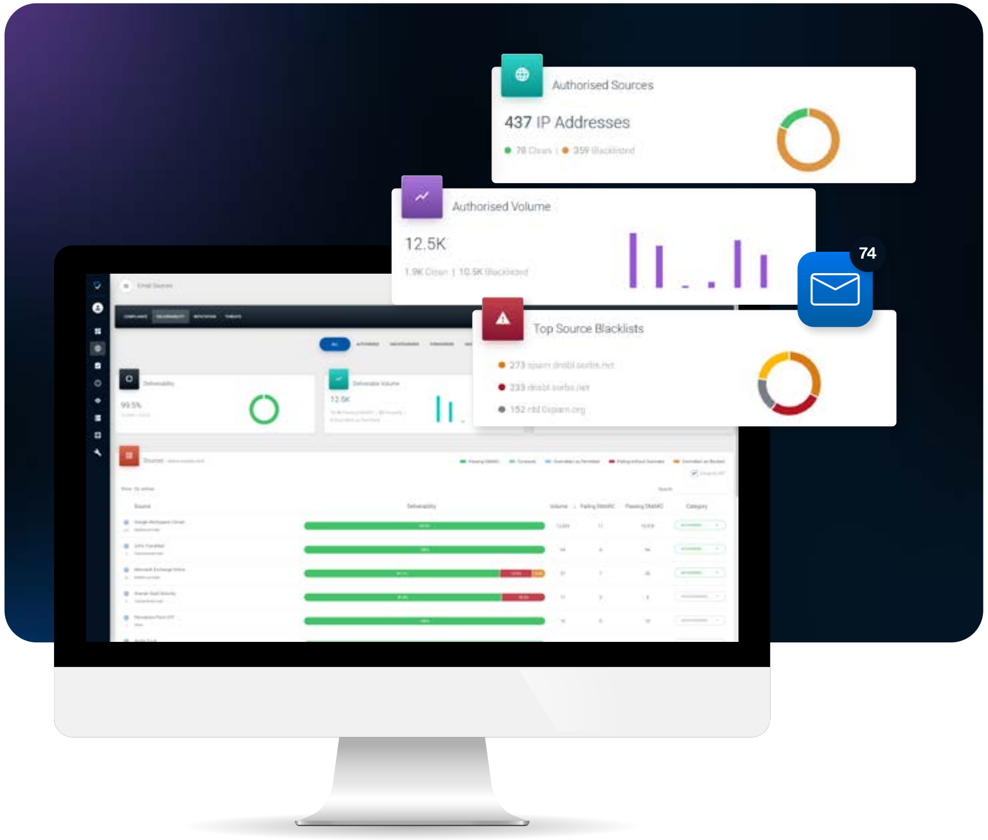
✓ **With a DMARC platform, your MSP can proactively scan** the client's infrastructure using automated tools, reviewing logs and alerts. This preventative functionality will help your MSP respond to threats before any significant damage takes place.

✓ **Your MSP can prioritize proactive email protection** by offering DMARC implementation, building trust, and setting yourself apart as a provider committed to client security.

✓ **DMARC will enable your MSP to engage clients**, their employees, and stakeholders in cybersecurity. Having a more comprehensive approach means building upon the standard firewall conversation, offering deeper, more relevant solutions that educate clients whilst still doing their jobs.

Strategic move #3

Ensure no-nonsense accuracy



By implementing a DMARC protocol with streamlined reporting, simplified deployment, automation innovation, and expert support, your MSP can establish a no-nonsense approach to protect clients against impersonation, spoofing, and phishing attacks.

brigantia

The DMARC edge on accuracy

Streamlined reporting and analysis: Some DMARC platforms, like Sendmarc, generate comprehensive reports and analytics. These reports enable your MSP to identify trends, assess vulnerabilities, and make data-driven decisions to strengthen email security.

Simplified deployment and management: Your MSP can leverage a user-friendly DMARC platform that provides intuitive interfaces, making it easier to deploy, configure, and manage DMARC policies across diverse client environments.

Automation innovation: It's important to choose a DMARC platform that supports accurate and automated workflows, remains progressive in an ever-evolving market, and can scale enough to handle an increasing amount of email traffic and clients efficiently.

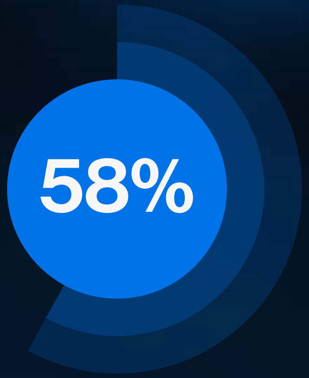
Expert support: Reliable customer support and access to DMARC experts ensures accessibility to accurate information, expert support, troubleshooting, and overall best practice guidance.

A profitable addition to your product stack

Tap into a DMARC market expected to be worth $1.72 billion by 2028

DMARC will be a profitable addition to your MSP's product stack because it solves a need for your customers by strengthening their cyber defenses against impersonation attacks and fraudulent activities. By reducing backend maintenance, freeing up internal resources, and enabling scalable implementation across multiple clients, you can maximize your profitability.

With existing expertise in security measures, your MSP can seamlessly incorporate DMARC as a powerful and efficient IT tool.



The average year-over-year growth rate of confirmed valid DMARC records

*The arithmetic mean was used to calculate the average annual growth rate from December 2016 to June 2022.

Achieving victory with DMARC

Your MSP can leverage DMARC to stand out in a competitive market and enhance operational efficiencies using a platform that offers visibility and enables quick changes to prevent cyberattacks. With DMARC in place, you can outmaneuver phishing and spoofing attacks, securing your client's email ecosystems. It's the winning move that keeps domains protected, peace of mind intact, and clients happy.

Choosing the right DMARC partner is crucial, as it directly impacts the success of your MSP's email protection strategy.

SENDMARC

Sendmarc is a leading DMARC provider with a platform that was built to cater to the unique needs of our MSP partners. Our joint mission is to empower MSPs by offering comprehensive tools that strengthen email security, improve operational efficiency, and enable differentiation in a rapidly evolving threat landscape and growing MSP market.

Benefits:

- Multi-tenant solution
- Marketing & sales enablement tools
- Streamlined workflows
- Onboarding, training & certification

Learn more about the Sendmarc Platform here.

Use Sendmarc's free tools to check your customers domain.

brigantia