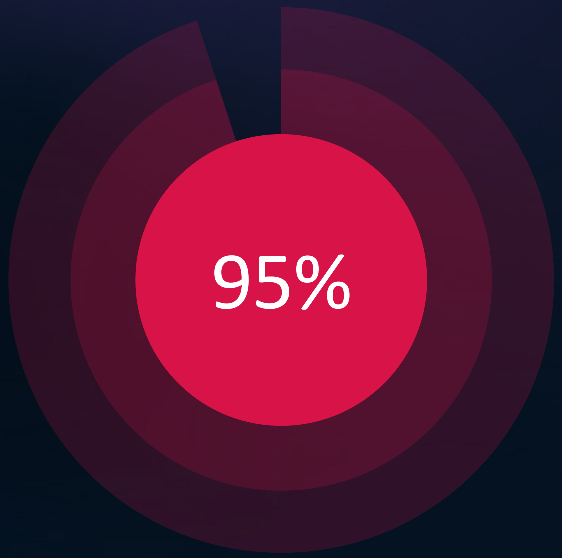
SENDMARC

MSPs

Lead the Email Security Charge & Strengthen Client Trust with DMARC



of cybersecurity breaches result from human error

Costs of data breaches for companies smaller than 500 up by 13.4% last year

IBM

The Problem

The Email Problem

There is a fundamental security flaw in the way email was designed. 91% of cybercrimes initiated with email.

91%

Impersonation

Attackers can send email from your domain defrauding, staff, customers & suppliers

Interception

An email can be intercepted and changed without the recipient knowing

Delivery

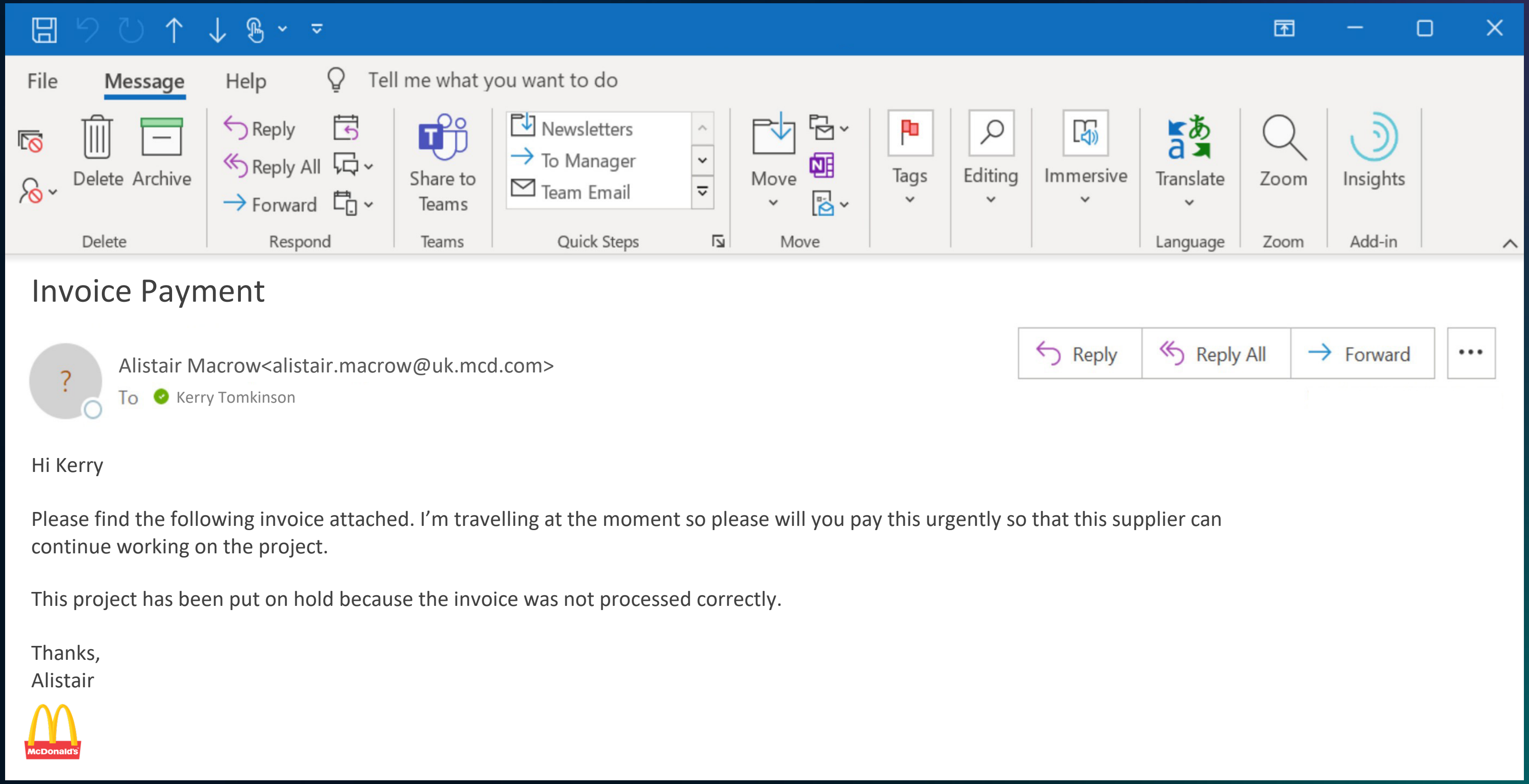
Legitimate email often lands in Spam and false positives cause business disruption

Visibility & Audit

Companies have no active visibility on which providers are sending email from their domain

Impersonation Example

Simulation of what an impersonation email looks like when sent by a cyber-criminal using your domain.



Invoice Payment

Alistair Macrow<alistair.macrow@uk.mcd.com>
To Kerry Tomkinson

Hi Kerry

Please find the following invoice attached. I'm travelling at the moment so please will you pay this urgently so that this supplier can continue working on the project.

This project has been put on hold because the invoice was not processed correctly.

Thanks,
Alistair

SENDMARC

How vulnerable are you?

https://partner.sendmarc.com/impersonation/mmat35o4

The Damage

Deposit Fraud

Ransomware Distribution

Identity Theft

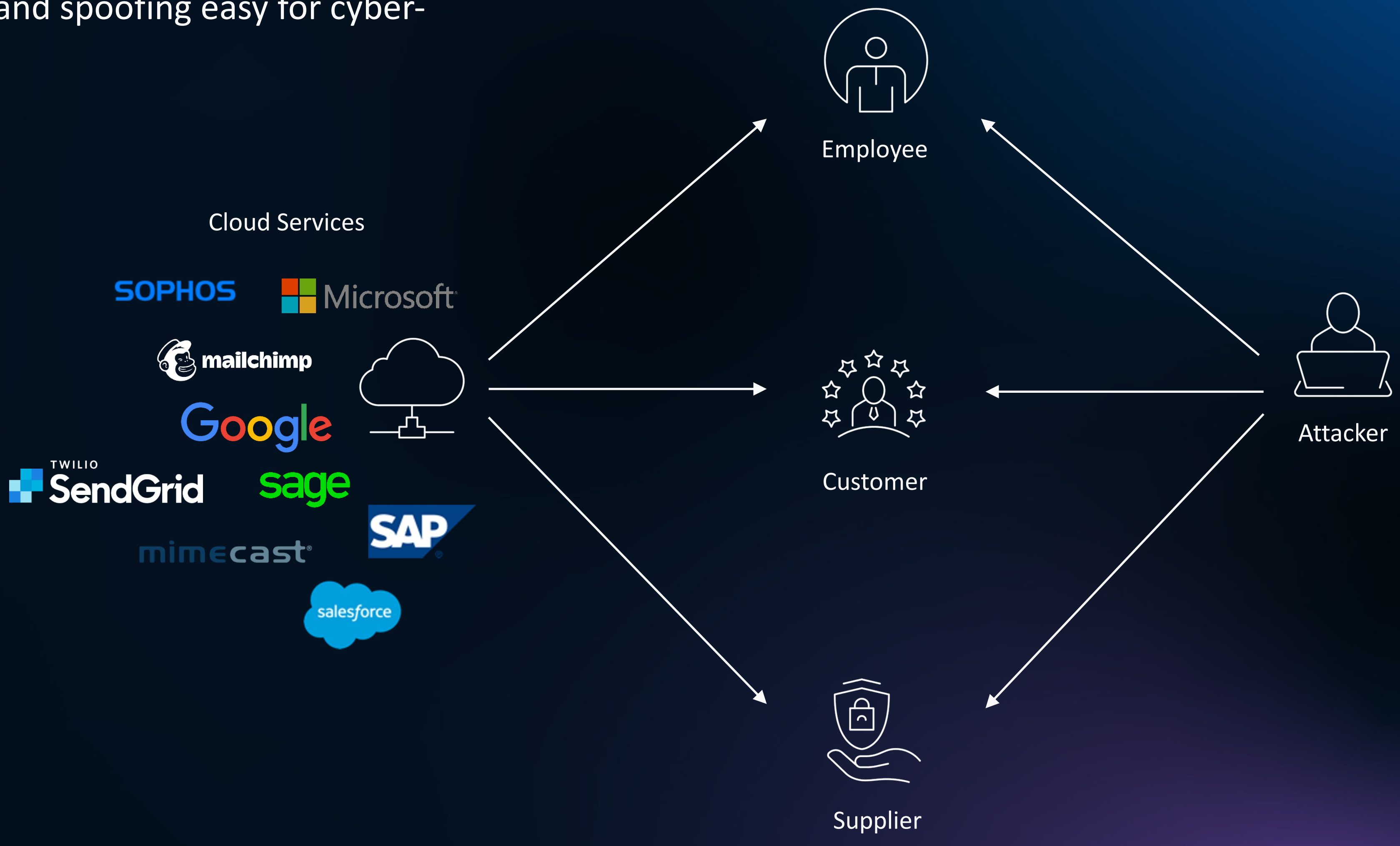
Reputation Damage

Nov. 2021

‘Ian’ loses his entire life savings to an attacker impersonating his wealth manager.

How Does This Happen?

The distributed nature of the internet and cloud services makes email impersonation and spoofing easy for cyber-criminals to achieve.



Existing Protection

Your staff might be protected by your existing anti-spam provider or perimeter protection but your customers, suppliers and the rest of the world are not.

Providers

Microsoft

Google

Abnormal

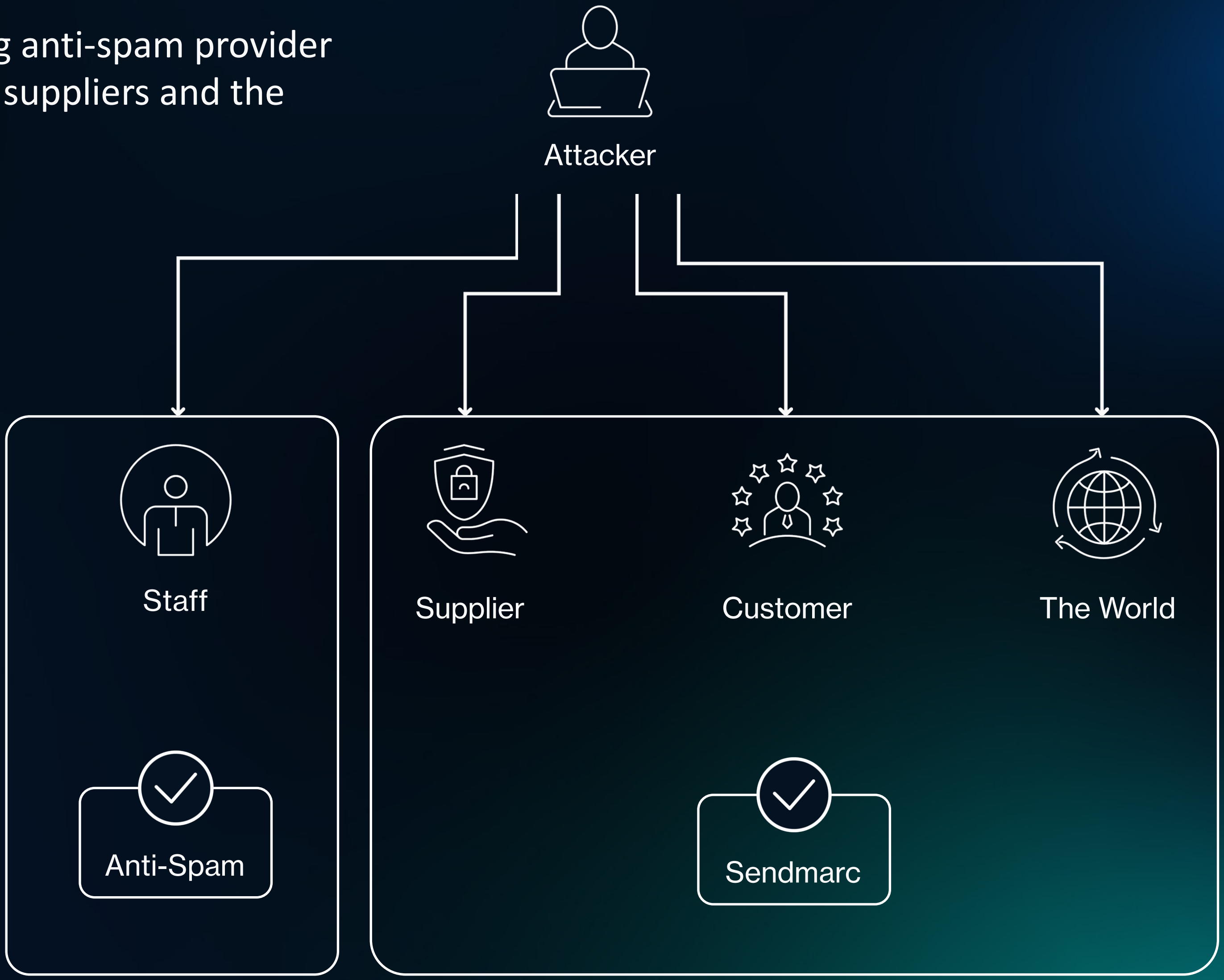
proofpoint.

mimecast

SOPHOS

HORNETSECURITY

Any Provider



The Solution

DMARC

Sendmarc stops email impersonation in Partnership with MSPs

Get access to our software platform, professional services & enablement

Solve Impersonation

Forces a whitelist of IP addresses that are authorized to send emails from your domain (SPF)

Detect Interception

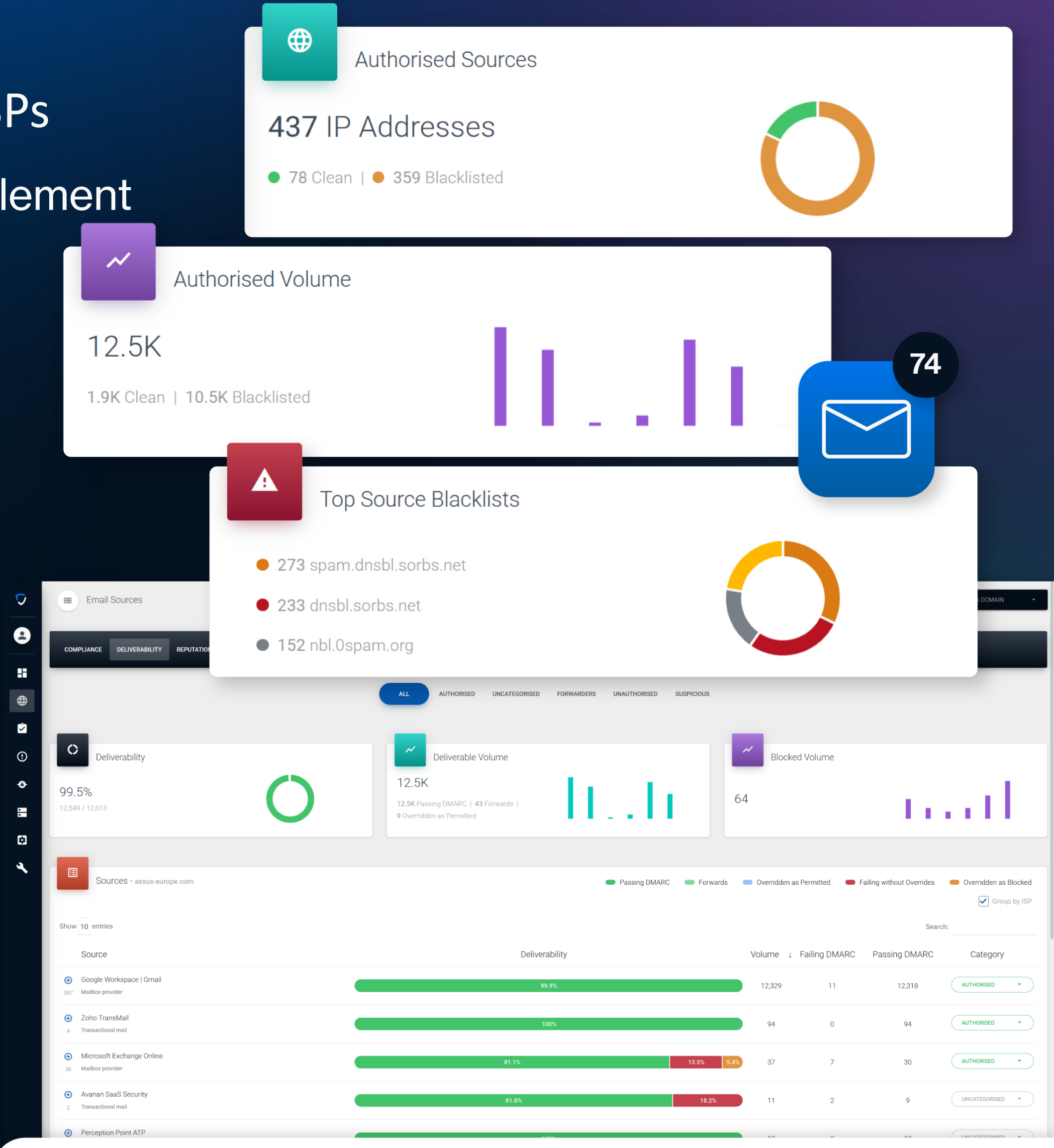
Every email carries a cryptographic signature to ensure anti-tampering (DKIM)

Improve Delivery

Legitimate email is delivered successfully more often because servers can tell that you’re a trusted sender

Increase Visibility

Domain owners can now get a consolidated, global visibility of every sender - both good and bad, then take action



Authorised Sources

437 IP Addresses

● 78 Clean | ● 359 Blacklisted

Authorised Volume

12.5K

1.9K Clean | 10.5K Blacklisted

74

Top Source Blacklists

● 273 spam.dnsbl.sorbs.net

● 233 dnsbl.sorbs.net

● 152 nbl.0spam.org

Deliverability

99.5%

12,549 / 12,613

Deliverable Volume

12.5K

12.5K Passing DMARC | 43 Forwards | 9 Overridden as Permitted

Blocked Volume

64

Sources - aexus-europe.com

● Passing DMARC ● Forwards ● Overridden as Permitted ● Failing without Overrides ● Overridden as Blocked

☑ Group by ISP

Show 10 entries

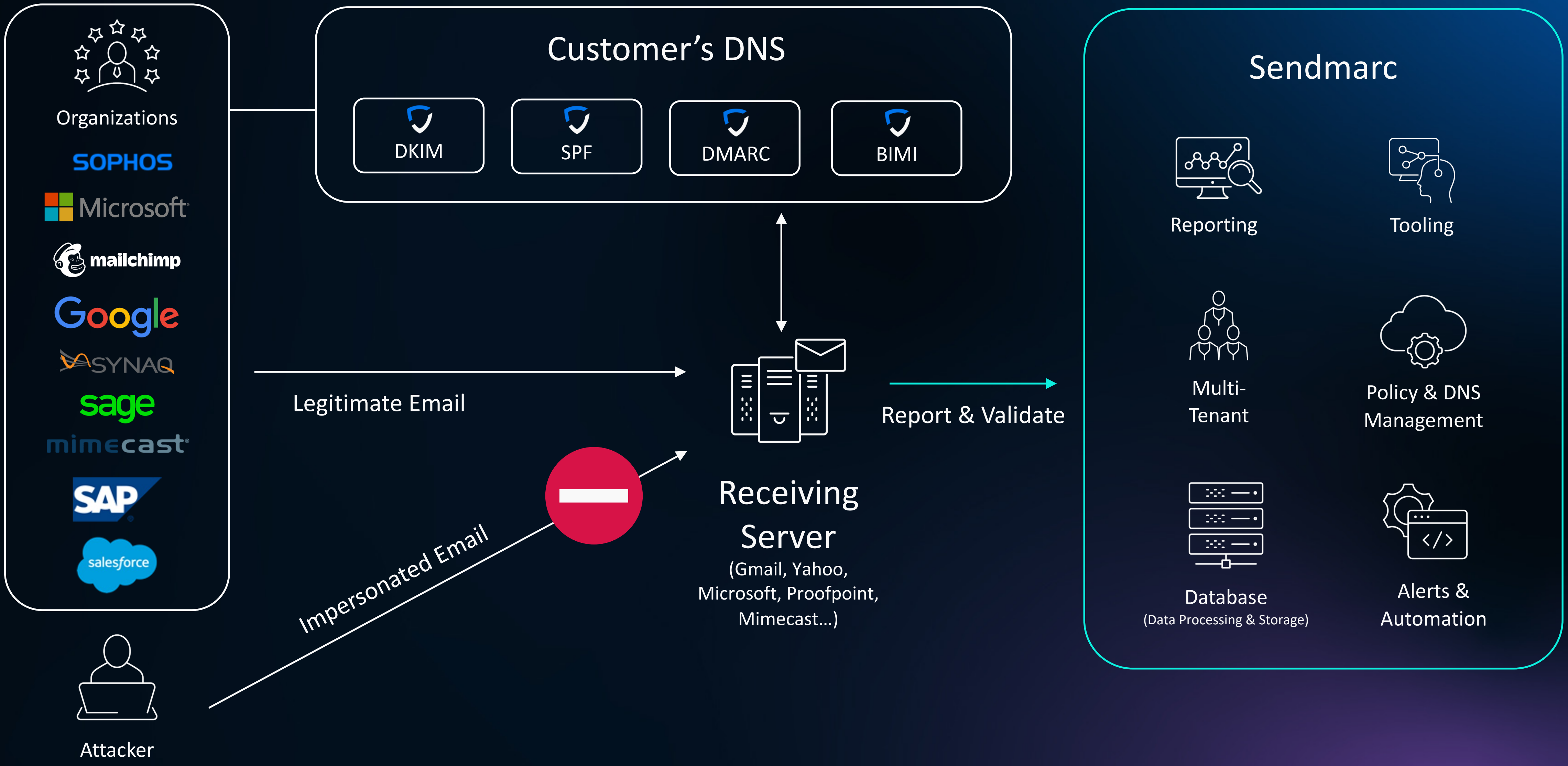
Search:

Source	Deliverability	Volume ↓	Failing DMARC	Passing DMARC	Category
Google Workspace | Gmail 397 Mailbox provider	99.9%	12,329	11	12,318	AUTHORISED
Zoho TransMail 4 Transactional mail	100%	94	0	94	AUTHORISED
Microsoft Exchange Online 36 Mailbox provider	81.1% 13.5% 5.4%	37	7	30	AUTHORISED
Avanan SaaS Security 2 Transactional mail	81.8% 18.2%	11	2	9	UNCATEGORISED
Perception Point ATP	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

Integrates with

Office 365 proofpoint. mimecast GSuite Symantec SOPHOS solarwinds SYNAQ

How DMARC Works



What’s Your Score 0 - 5?

How vulnerable are you?

0/5 No protection. Highly vulnerable

1/5 Your domain is vulnerable

2/5 Your domain is vulnerable

3/5 Visibility. WIP. Vulnerable.

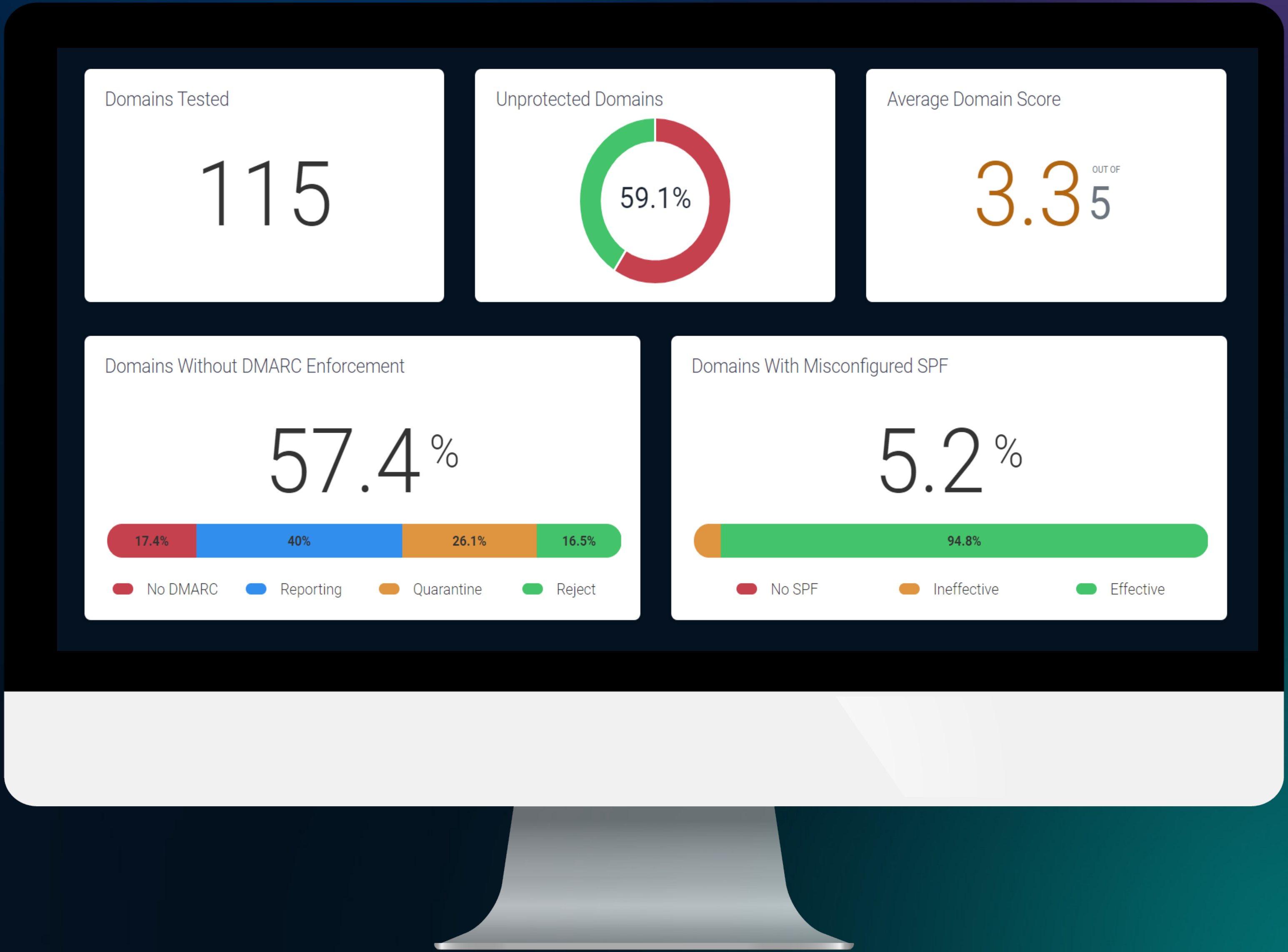
4/5 One more change required

5/5 Totally protected & compliant

Secure Your Ecosystem

Understand your email network and evaluate its incoming protection status.

Here’s a high-level look at the domains from the event registrations.



Domains Tested

115

Unprotected Domains

59.1%

Average Domain Score

3.3 OUT OF 5

Domains Without DMARC Enforcement

57.4 %

17.4% | 40% | 26.1% | 16.5%

🟥 No DMARC 🟦 Reporting 🟧 Quarantine 🟩 Reject

Domains With Misconfigured SPF

5.2 %

94.8%

🟥 No SPF 🟧 Ineffective 🟩 Effective

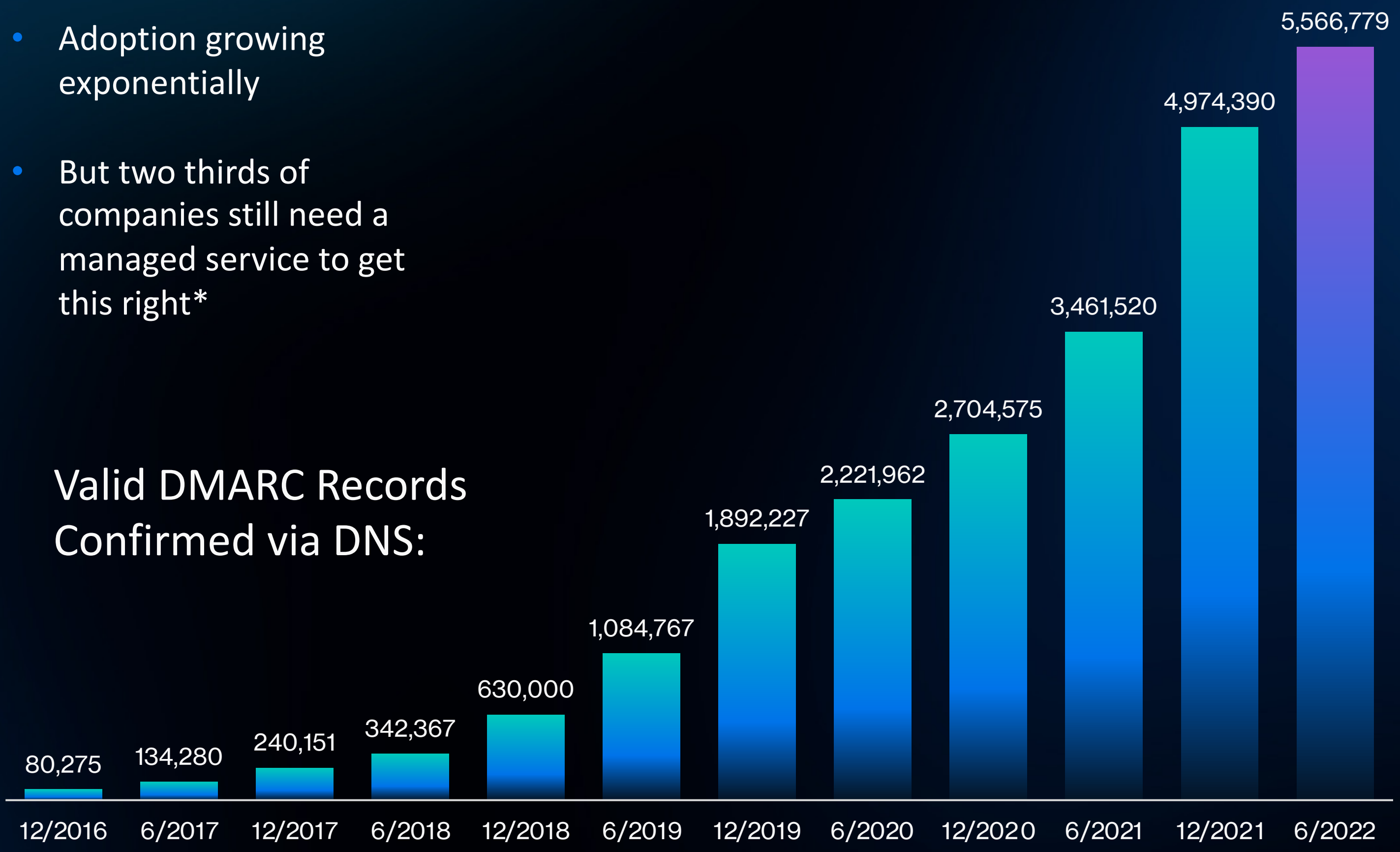
Market & Revenue Potential

Global Adoption

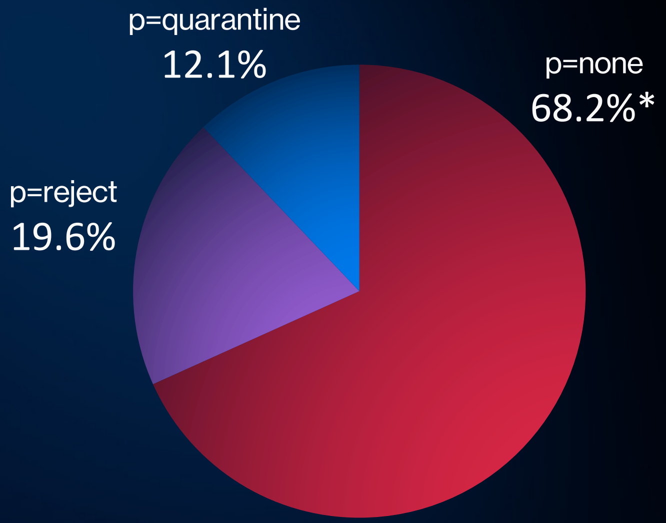
- Adoption growing exponentially

- But two thirds of companies still need a managed service to get this right*

Valid DMARC Records Confirmed via DNS:



Exponential growth

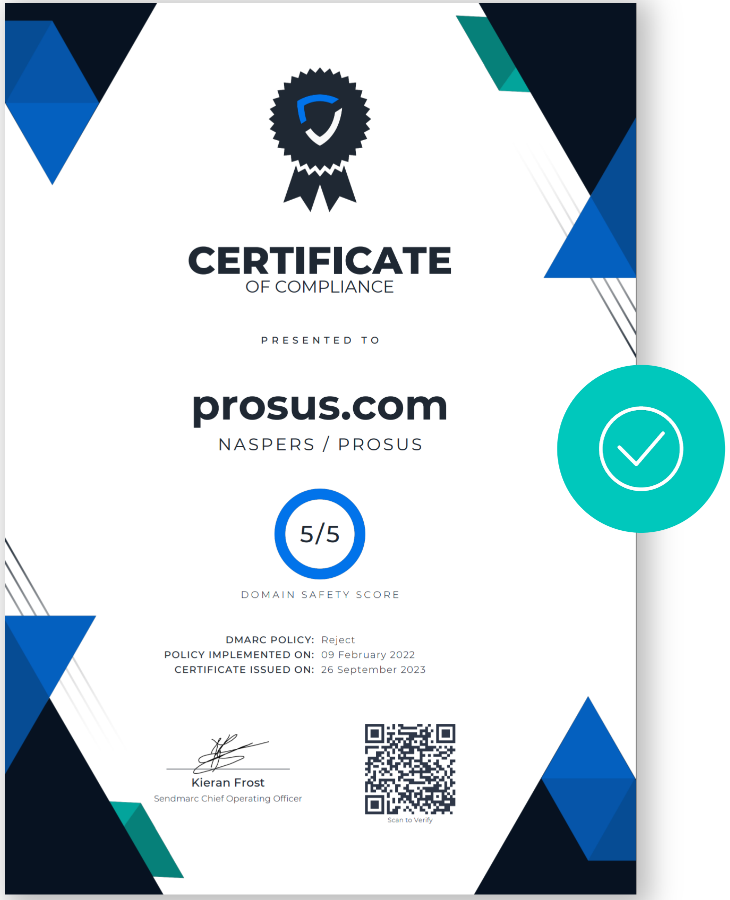


DMARC MSPs needed desperately

*Monitoring mode only. Email can still be impersonated. Skills required!

Source: DMARC.org

Regulators, institutions & large receiver/senders pushing for DMARC compliance



CERTIFICATE
OF COMPLIANCE

PRESENTED TO

prosus.com
NASPERS / PROSUS

5/5
DOMAIN SAFETY SCORE

DMARC POLICY: Reject
POLICY IMPLEMENTED ON: 09 February 2022
CERTIFICATE ISSUED ON: 26 September 2023

Kieran Frost
Sendmarc Chief Operating Officer

Scan to Verify

*Sendmarc offers a guarantee of full compliance to all managed customers.

Government Digital Service

European Commission
GDPR
General Data Protection Regulation

Gmail

yahoo!

computer emergency response team
CERT-EU
for the EU institutions, bodies and agencies

FINRA
Financial Industry Regulatory Authority

IETF
The INTERNET ENGINEERING TASK FORCE

PCI Security Standards Council®

FEDERAL TRADE COMMISSION ★ UNITED STATES OF AMERICA ★ MCMXV ★

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
CISA

U.S. DEPARTMENT OF HOMELAND SECURITY

gfma
GLOBAL FINANCIAL MARKETS ASSOCIATION

SENDMARC

The UK Market

Top 5,000 Companies: September 2023

The Good News!

1,233

Are protected

25%

The Bad News!

3,767

Can be impersonated

75%

SENDMARC

Managed DMARC

Expected Revenue Growth

The Next 5 Years

£ 280m

Per Year at end 2023

£ 1 .4bn

By end 2028

How we serve the MSP?

- ✓ With MSP centric DMARC software
- ✓ Supported by MSP centric DMARC experts
- ✓ Certifying MSPs & enabling them to deliver managed DMARC

1 Promote & Educate

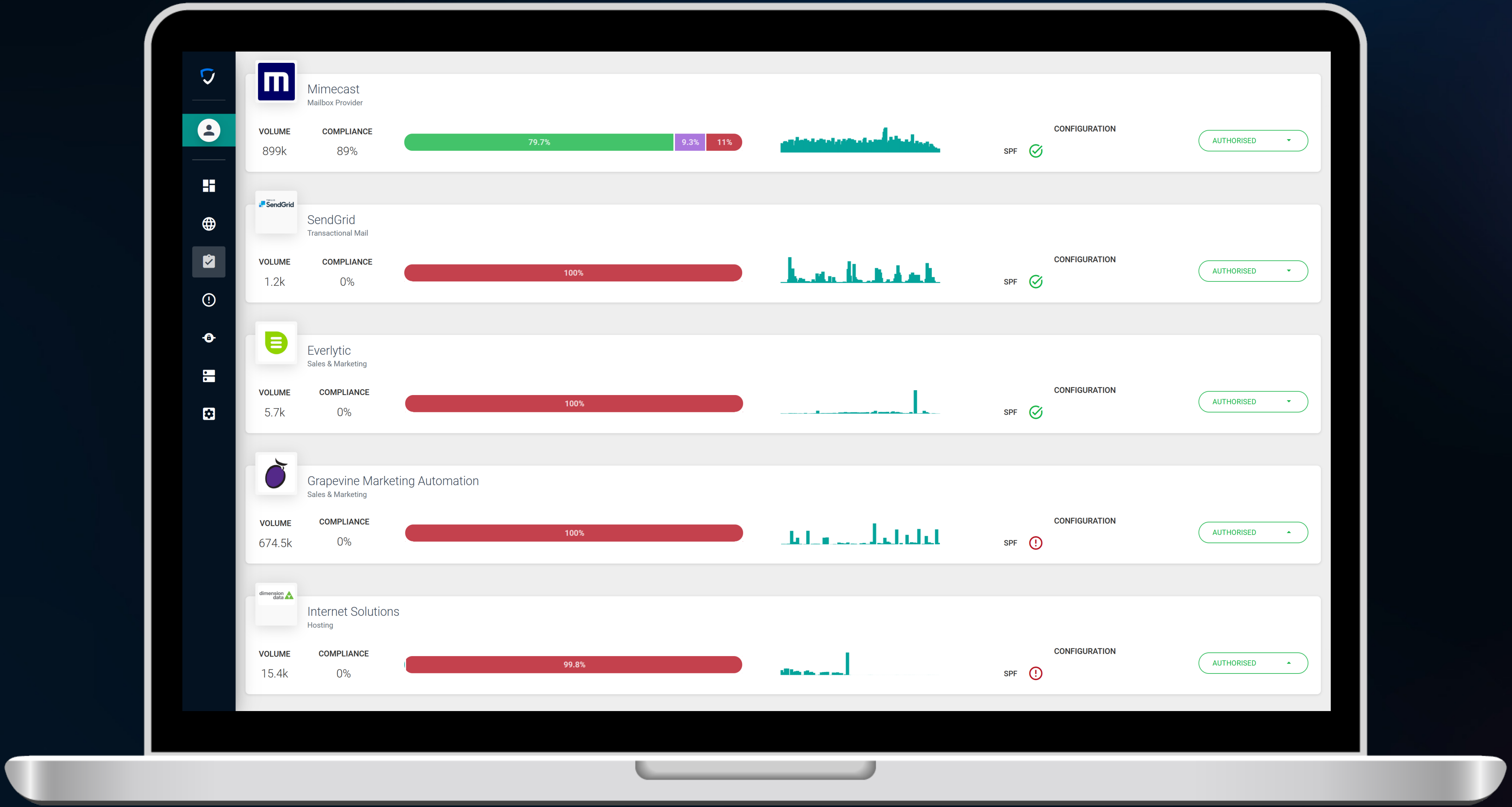
2 Generate Leads and online sign up

3 Target Prospects

4 Co-Sell

5 Implement & Support

What does MSP centric software mean?



Mimecast
Mailbox Provider
VOLUME 899k
COMPLIANCE 89%
79.7% 9.3% 11%
SPF ✓
CONFIGURATION
AUTHORISED

SendGrid
Transactional Mail
VOLUME 1.2k
COMPLIANCE 0%
100%
SPF ✓
CONFIGURATION
AUTHORISED

Everlytic
Sales & Marketing
VOLUME 5.7k
COMPLIANCE 0%
100%
SPF ✓
CONFIGURATION
AUTHORISED

Grapevine Marketing Automation
Sales & Marketing
VOLUME 674.5k
COMPLIANCE 0%
100%
SPF !
CONFIGURATION
AUTHORISED

Internet Solutions
Hosting
VOLUME 15.4k
COMPLIANCE 0%
99.8%
SPF !
CONFIGURATION
AUTHORISED

1 Multi-tenanted

2 Co-branded

3 Automate DNS tasks without leaving Sendmarc

4 Alerts, notifications and integrations

5 Task management 1-click deployment

Together with our MSP Partners, Sendmarc solves this problem for millions of users worldwide, making 10bn+ emails safer every year

phs	Virgin active	Bupa	prosus	YPO	Bidvest	ALTRON
CONCENTRIX	MultiChoice ENRICHING LIVES	EOH	NASPERS	Tiger Brands	OUT SURANCE	BRAIT
CHEDRAUI cuesta menos	Banco Promerica	Condor	BIM Banco Inmobiliario Mexicano	Remgro Limited	PRUDENTIAL	sappi
AOS	WEBBER WENTZEL in alliance with > Linklaters	UTComp	EuroAmerica	Solidarity Fund Unity in action	ARC AFRICAN RAINBOW CAPITAL	BOWMANS THE VALUE OF KNOWING

SENDMARC
Toronto
SENDMARC
Raleigh
SENDMARC
Amsterdam
SENDMARC
Buenos Aires
SENDMARC
Johannesburg
SENDMARC
Cape Town
SENDMARC
Brisbane
SENDMARC
Sydney

How can we help?