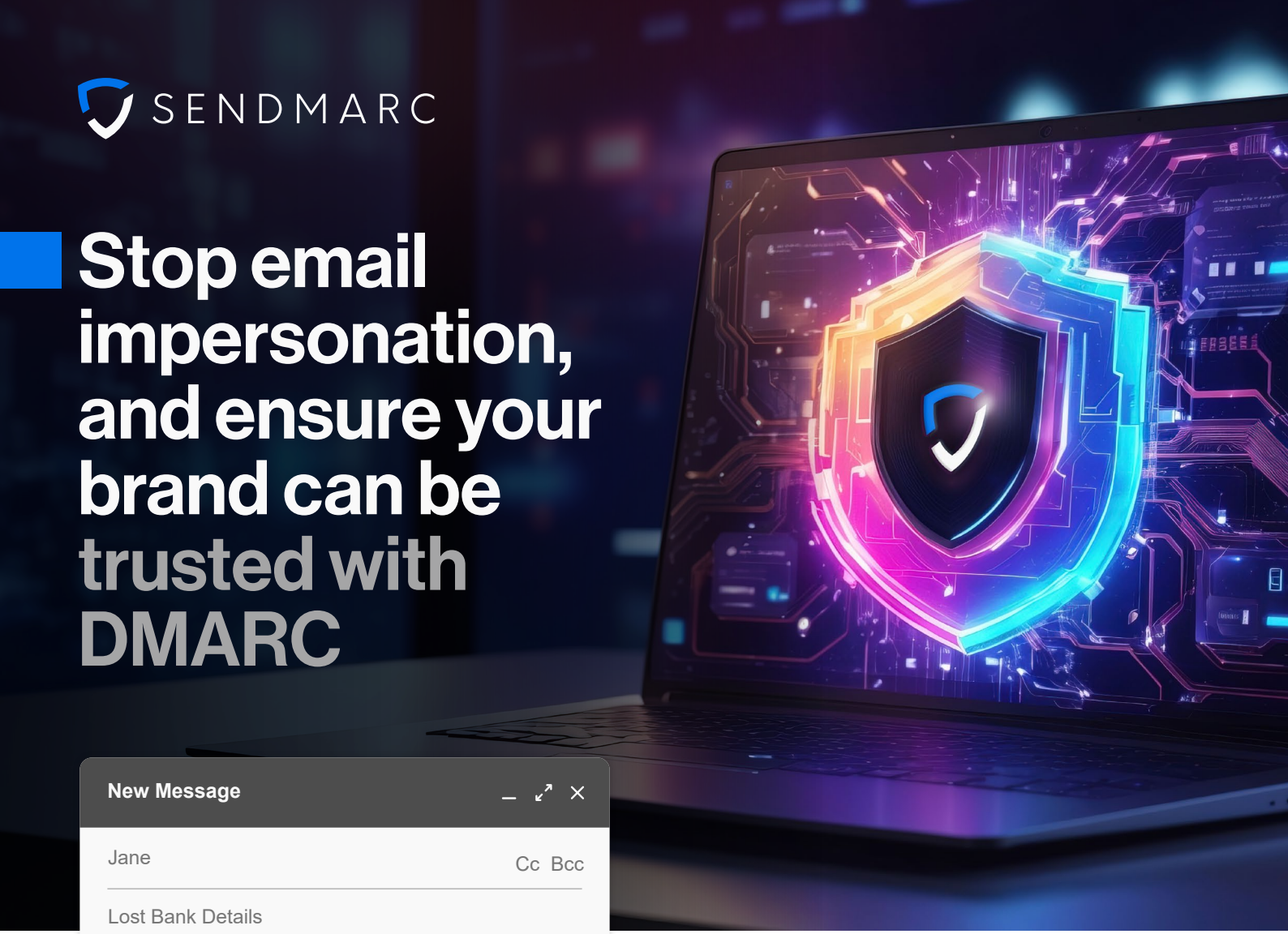
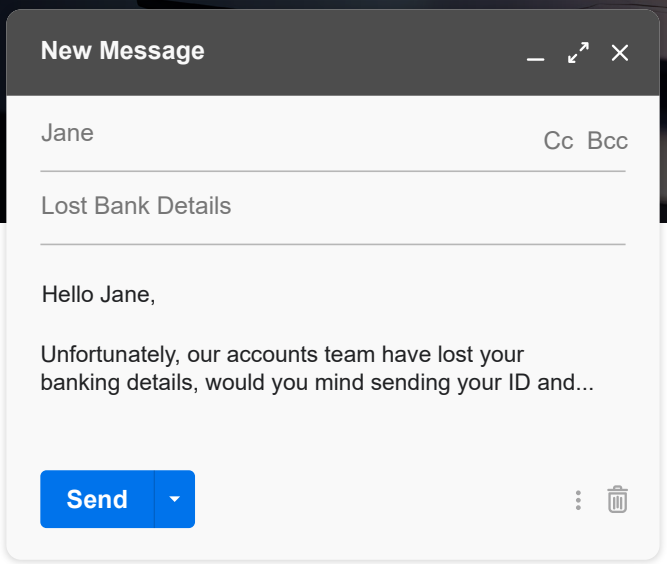
SENDMARC

# Stop email impersonation, and ensure your brand can be trusted with DMARC






Email is used in more than 91% of all network attacks with cybercriminals becoming increasingly devious at impersonating unprotected email domains. If unprotected, they can easily use brands to impersonate employees by sending emails with all the correct styling, making it virtually impossible for receivers to spot the fraudster.

An attack on your business could result in deposit fraud, ransomware attack, identity theft or reputation damage. Sendmarc mitigates this flaw using DMARC.

## How DMARC helps

## DMARC stands for Domain-based Message Authentication, Reporting and Conformance

DMARC verifies the source of an email message and determines what to do with it. It's a security check that allows only emails coming from the legitimate source to be delivered. Being DMARC compliant gives your company full visibility of and control over all emails (legitimate and illegitimate) claiming to be from your organization.

The DMARC standard confirms that the sender of the email is legitimate, that the message hasn't been compromised, and if it passes the authentication process delivers the email to the inbox and if it doesn't, rejects the email.

IGNITION
An Exclusive Networks Company

In partnership with: SENDMARC

Benefits to you

# Helping make the most used business communication tool the most trusted

## Increased visibility of email sources

DMARC reporting lets you see legitimate and illegitimate use of your email domains. Once full protection status is achieved for your domain, all illegitimate emails will be rejected and you will have constant monitoring and management of your entire email ecosystem. This means any new security threats and potential deliverability issues are actively prevented.

## Strengthened brand recognition & trust

Companies with DMARC can implement BIMI, an email authentication standard that allows for the display of your logo next to emails in the recipient's inbox. BIMI increases brand recognition and trust, and ensures effective email communication by boosting email deliverability.

## Email that is trusted by entire stakeholder community

All inbound and outbound email with your brand name is verified for authenticity, preventing cybercriminals from using your name for illicit gain, ensuring employees, customers, partners, and suppliers only ever receive legitimate email.

## Provided as a service with zero infrastructure costs

Delivered using a purpose-built platform, making deployment easier with fully automated processes, access and visibility of real-time reporting, and continuous proactive management of the entire email environment.

## Global and company-wide compliance

Globally recognized technical authentication and verification standards applied to all emails using the brand name, provide organization-wide compliance to every email service used by every department.

## Guaranteed for every customer

The same product with the same features and functionality is deployed for every customer, giving all customers the same level of security and full DMARC protection in record time.

## Improved email deliverability

Implementing the strongest authentication rules and policies ensures that all legitimate emails with your name reach the intended inbox.

## Protection for the entire email Ecosystem

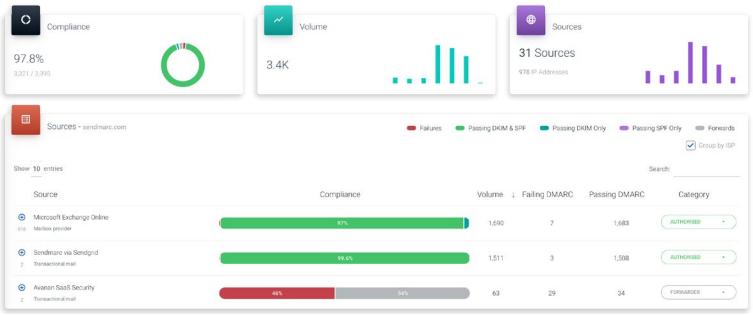
Seamless integration and implementation with all third-party providers of email services ensures an organization's entire email real-estate is secure and safeguarded.

IGNITION
An Exclusive Networks Company

In partnership with: SENDMARC

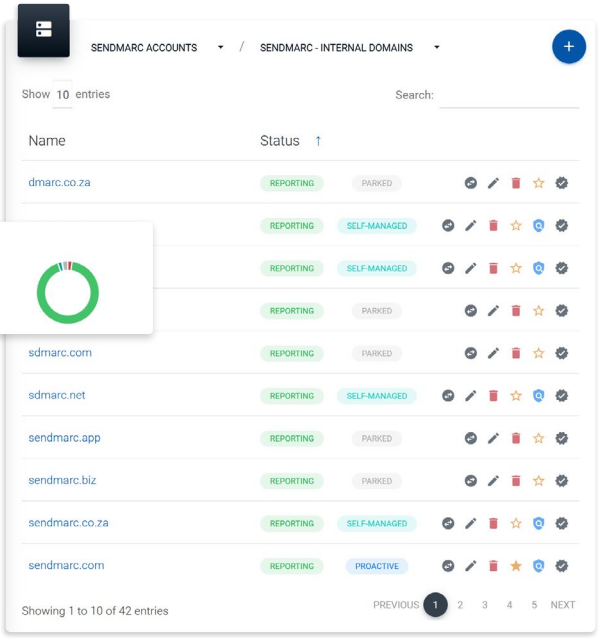
DMARC Compliant

# Get DMARC compliant with the best software and services in 90 days guaranteed*



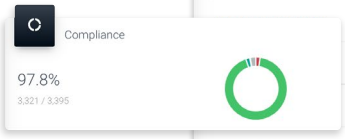

## Purpose-built platform

Our purpose-built platform ensures swift implementation of DMARC compliance for your organization, while also providing interoperability to assess and manage data from multiple email service providers.




## Rich features for ALL

Our product is built with a rich set of features and functionality that every customer receives. There are no gradings, tiers or variations of our product, because every organization large or small is vulnerable to the same cyberthreats and so require the same standards of protection.




Take control

# Six steps to protecting your brand

### 1 Publishing DMARC records

Our first step is adding DMARC records to the DNS, and then publishing these. This ensures that every time an email service receives a mail using your name, a report is sent to Sendmarc, allowing us to see who is using your domain – whether legitimate or not.

### 2 Configuring DNS (Domain Name System)

We then migrate the management of SPF and DKIM to the Sendmarc platform – ensuring that these critical authentication mechanisms are properly managed and enabling the best email deliverability possible for your legitimate senders.

### 3 Analyzing reporting

Now that we've enabled reporting, and we're able make changes to the relevant configurations, it's time to analyze the data. This gives us insight into how your email name is being used – both legitimately and illegitimately. This intelligence highlights your risk and exposure to email fraud so we can put in place the necessary measures to stop the abuse of your name by criminals as well as eliminate the associated financial, operational and reputational headaches.

### 4 Fortifying your email security

To implement and activate DMARC we configure all approved services sending email using your name. This ensures the DMARC policy is applied across your entire email environment, including all third parties that send emails on your behalf, and that only legitimate emails reach an inbox and the best email deliverability rates are achieved.

### 5 Achieve a state of full protection

The correct configuration of your entire email environment, reaching a state where all illegitimate emails are stopped from reaching an inbox and only legitimate emails are delivered is guaranteed.

### 6 Actively defending and protecting your environment

The continually increasing volume of fraudulent email activities combined with the growing adoption of cloud services for email means that DMARC cannot be a one-time configuration project, but rather requires the ongoing monitoring and updating of the email environment to achieve the highest and safest states of compliance and deliverability.

*Only applicable for customers on Sendmarc's Premium Plan.

IGNITION
An Exclusive Networks Company

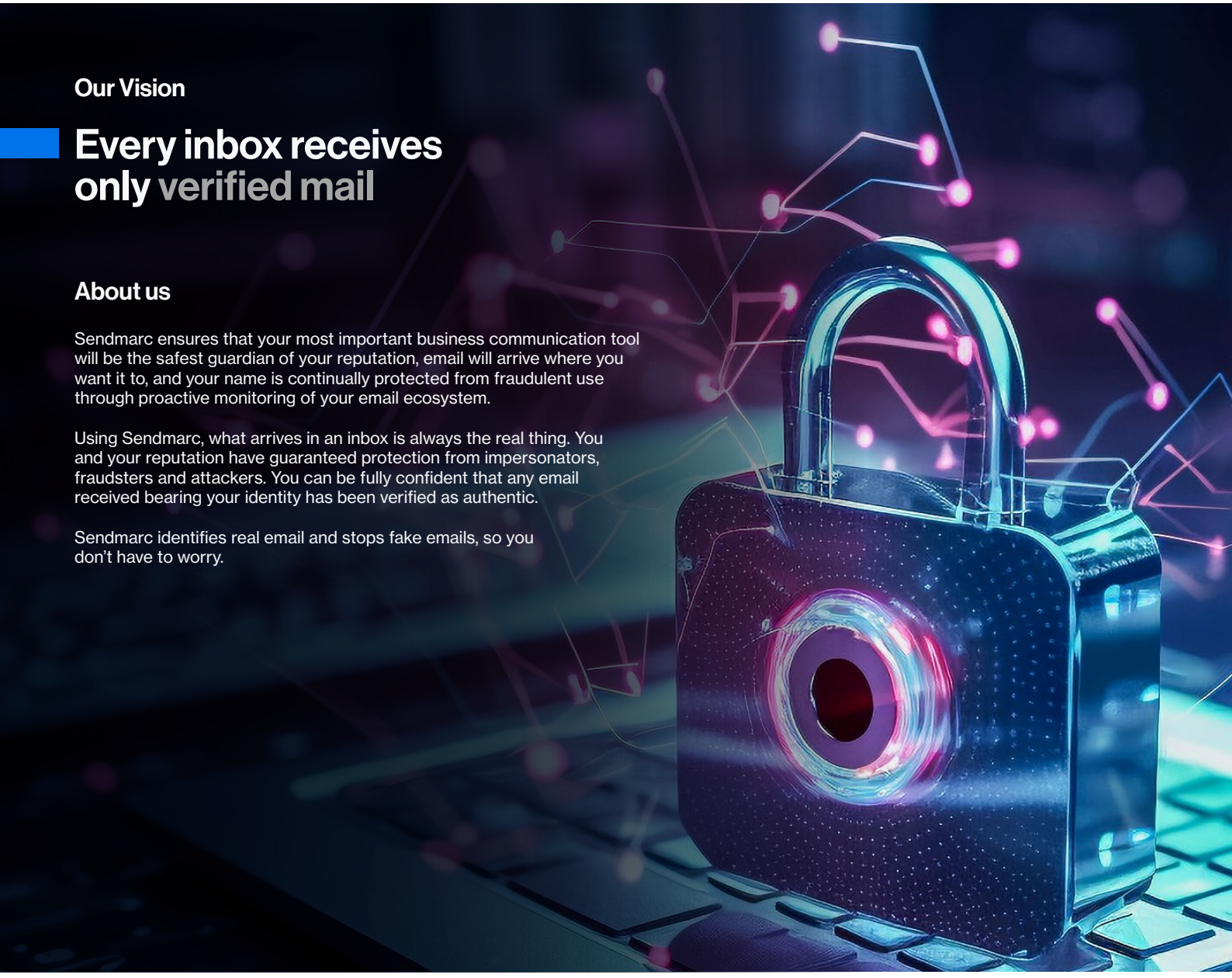
In partnership with: SENDMARC

# Thousands of companies
## trust Sendmarc

CyberDNA TOTAL SECURITY
evolve TECHNOLOGIES
Intelliworx.
CARERRA HOLDINGS
Blacktip
COMPUTER TECHNICAL SOLUTIONS
UNIVERSITY OF JOHANNESBURG
eNerds
B-LOGIC
ProfyTechnologies
SYSTEM 5
rebyC
Strategix
The Way Forward
CYBERLINX
People | Process | Technology
CHM VUWANI
Leading Edge Technology

### Our Vision

# Every inbox receives only verified mail



### About us

Sendmarc ensures that your most important business communication tool will be the safest guardian of your reputation, email will arrive where you want it to, and your name is continually protected from fraudulent use through proactive monitoring of your email ecosystem.

Using Sendmarc, what arrives in an inbox is always the real thing. You and your reputation have guaranteed protection from impersonators, fraudsters and attackers. You can be fully confident that any email received bearing your identity has been verified as authentic.

Sendmarc identifies real email and stops fake emails, so you don't have to worry.

IGNITION
An Exclusive Networks Company

In partnership with: SENDMARC