

# ACTIVE CARE DMARC MANAGED SERVICE

Safeguard your organization and its third-party ecosystem against email impersonation attacks

Email is still the most important communication channel for any organization, regardless of size or industry. But because of its success, it is also one of the most common ways cyberattackers strike.

A key factor for a successful email attack is gaining trust. Attackers create emails that impersonate organizations like yours — pretending to be you, your partners, or your employees. The consequences? Identity theft, payment fraud, ransomware distribution, disrupted communications, and serious damage to your brand and reputation.

DMARC (Domain-based Message Authentication, Reporting & Conformance) is a security protocol that protects your domain from email impersonation and is crucial for every organization. It ensures that only senders you authorize can send emails using your domain name.

DMARC works through a DNS record that tells email servers how to check if a message truly comes from you — and what to do if it doesn't: reject it, quarantine it, or allow it.

Without DMARC, your domain is exposed to attacks. On top of that, major email providers like Google, Microsoft, and Yahoo require organizations to have DMARC policies for proper email delivery, while compliance with important regulations such as PCI-DSS and GDPR also demands it.

However, setting up DMARC correctly can be complicated and time-consuming. With our Active Care DMARC Managed Service, our security experts take full control of the journey for you.

We help you identify authorized email senders and configure your SPF and DKIM records to ensure only legitimate sources can send emails from your domain. We continuously monitor your email traffic, detect unauthorized senders and look-alike domains attempting to impersonate you, identify issues early, and proactively protect your brand and reputation. Our mission is to safely guide your domain to a full strict DMARC policy ("reject policy"), ensuring secure, uninterrupted email communication.

## SERVICE BENEFITS

- Complete email traffic visibility
- Guaranteed deliverability of legitimate emails
- Advanced impersonation attack detection
- Established trust with partners and customers
- Elevated brand awareness and credibility
- Seamless and secure user experience

Managed Services are available through the Inter Engineering partner channel.

### SET UP DMARC POLICY

Strengthen your email security by enforcing a strict DMARC policy that blocks unauthorized senders from using your domain.

### ACHIEVE COMPLIANCE

With major email providers (Google, Yahoo, Microsoft, etc.) and legal frameworks (e.g. GDPR and PCI-DSS).

### SUITABLE FOR EVERYONE

Designed for organizations of all kinds and sizes.

### NO ADMINISTRATION

This is a service managed entirely by Inter Engineering security experts.

### NO HIDDEN COSTS

All you pay is a subscription based service. We won't ask you to pay for extra features or upgraded service levels.

### REPORTING


On a regular basis, we will provide you with a report detailing all actions performed to protect your organization

### BREACH DETECTION

Monitors sources like the dark web to identify stolen or leaked business data, credentials, or personal information — whether from your systems or third parties. (add-on option)

### LOOK ALIKE DOMAIN DEFENSE

Detects domains mimicking yours, helping you quickly act. (add-on option).

Powered by:  
 SENDMARC