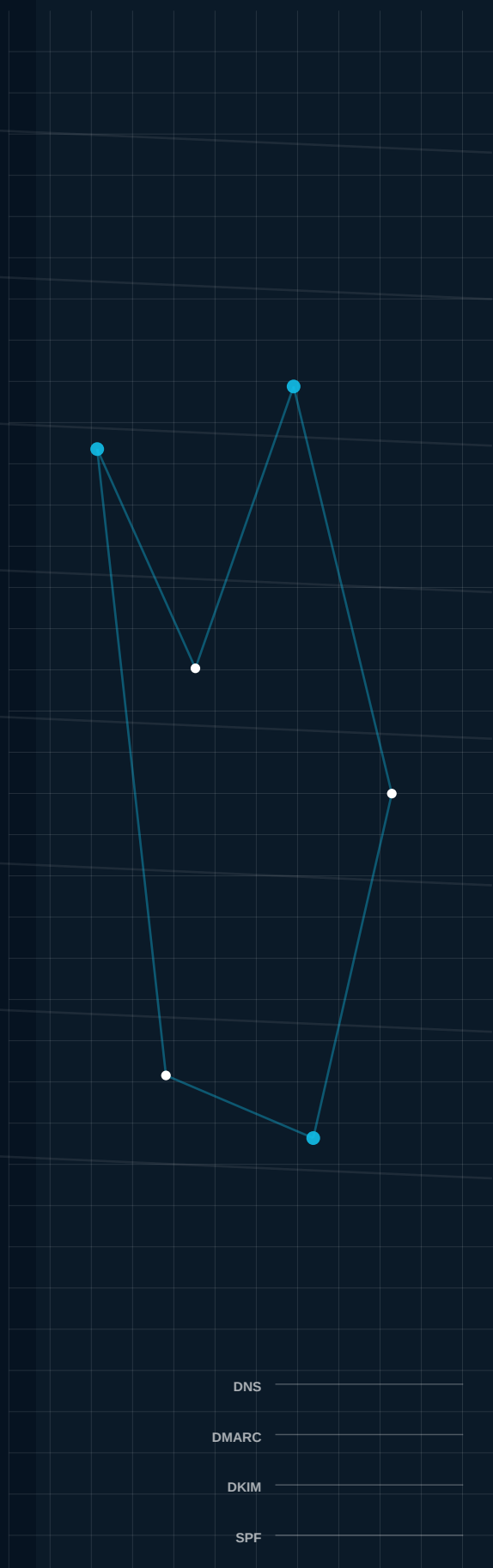


SERVICE OVERVIEW

Remediation & Strengthening

Planned correction of email authentication, alignment, authorized sending sources and relevant domain configuration.



WHAT IT IS

We correct what the assessment shows needs attention.

Remediation begins after the environment and its dependencies are understood. RDA plans agreed corrections across SPF, DKIM, DMARC, authentication alignment, authorized sending sources, relevant email-related DNS and sending subdomains.

The implementation route depends on risk and the client's environment. RDA may implement directly, lead the client's IT provider through the change, or use specialist support where complexity requires it.

Controlled changes, verified results.

RDA does not implement a technical change it cannot explain, verify, understand the likely impact of and reverse if necessary.

Remediation is evidence-led. RDA plans the work, agrees the implementation route and verifies the result.



COMMON REASONS

Common reasons clients need remediation

Remediation is considered when an assessment or reliable current evidence shows that the authentication and domain trust environment needs corrective work.

01	Health Check identified meaningful weaknesses	02	SPF is incorrect, duplicated, over-broad or approaching technical limits
03	DKIM is missing, inconsistent or not aligned across confirmed legitimate senders	04	DMARC is absent, invalid or not at the appropriate policy position
05	Legitimate sending systems are not correctly authenticated or aligned	06	Stale or unnecessary sender authorization remains in the environment
07	New platforms or subdomains have changed the sending environment	08	Policy progression or another material change requires planned verification

The emphasis is controlled correction: understand the environment, make the right change and verify the result.

SCOPE OF WORK

What remediation covers

01	Remediation Plan and Change Control	Define the agreed issue, dependencies, implementation route, approval point and rollback position before changes begin.
02	SPF Correction and Authorization Cleanup	Correct SPF structure and remove confirmed stale or unnecessary authorization where appropriate.
03	DKIM Deployment or Correction	Support correct DKIM deployment for confirmed legitimate sending systems where the required access and evidence are available.
04	DMARC Implementation and Policy Progression	Implement or correct DMARC and progress policy only when the evidence shows the environment is ready.
05	Authentication Alignment and Sending Sources	Correct agreed alignment problems and authentication issues across legitimate sending systems.
06	Relevant DNS and Sending Subdomains	Correct email-related DNS and relevant sending-subdomain issues within the approved scope.
07	Coordinated Implementation	RDA may implement directly, lead the client's IT provider or use specialist support according to risk and complexity.
08	Post-Change Verification and Documentation	Verify agreed changes, record the outcome and document the next recommended step.

PRICING AND DELIVERABLES

Scope, implementation and verified results

PRICE

Quoted

After assessment

Project pricing is based on scope, complexity, risk, relevant sending systems and the agreed implementation route. Timing is confirmed after scope; straightforward corrections may take days, while staged policy progression or complex environments can take longer.

INCLUDED IN REMEDIATION

- Agreed remediation plan and change sequence
- Authentication and alignment corrections within scope
- Sending-source and authorization cleanup
- Coordination with client IT or specialist support where required
- Post-change verification
- Plain-English completion summary and next-step recommendation

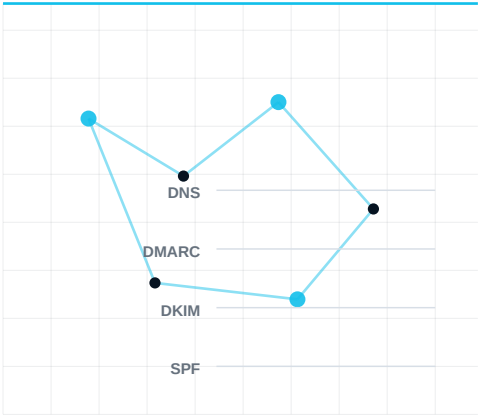
IMPORTANT NOTES

- The \$495 Health Check is separate and is not automatically credited against remediation.
- RDA only makes approved changes where the required access or client cooperation is available.
- High-risk or complex environments may require expert review or specialist execution.
- Active outages, incident response, migrations, hybrid or on-premises Exchange, major MX or routing changes and other out-of-scope work require separate handling.
- Remediation improves authentication and domain trust. It does not guarantee inbox placement or prevent every form of fraud.

HOW TO GET STARTED

Start with a Health Check or provide current findings.

If current, reliable findings already exist, RDA can review them and decide whether direct remediation scoping is appropriate. Otherwise, the Email Trust Health Check provides the baseline before changes begin. Where evidence needs to be observed over time, RDA may recommend a defined Post-Remediation Assurance period.



STARTING STEPS

- 01 Complete an Email Trust Health Check or provide current findings
- 02 RDA confirms the scope, risk and implementation route
- 03 Approve the proposal and provide the required access or cooperation
- 04 Agreed changes are implemented through the approved route
- 05 RDA verifies, documents and recommends the next assurance step

RDA

rdadeliverability.com
info@rdadeliverability.com
+27 76 311 1590