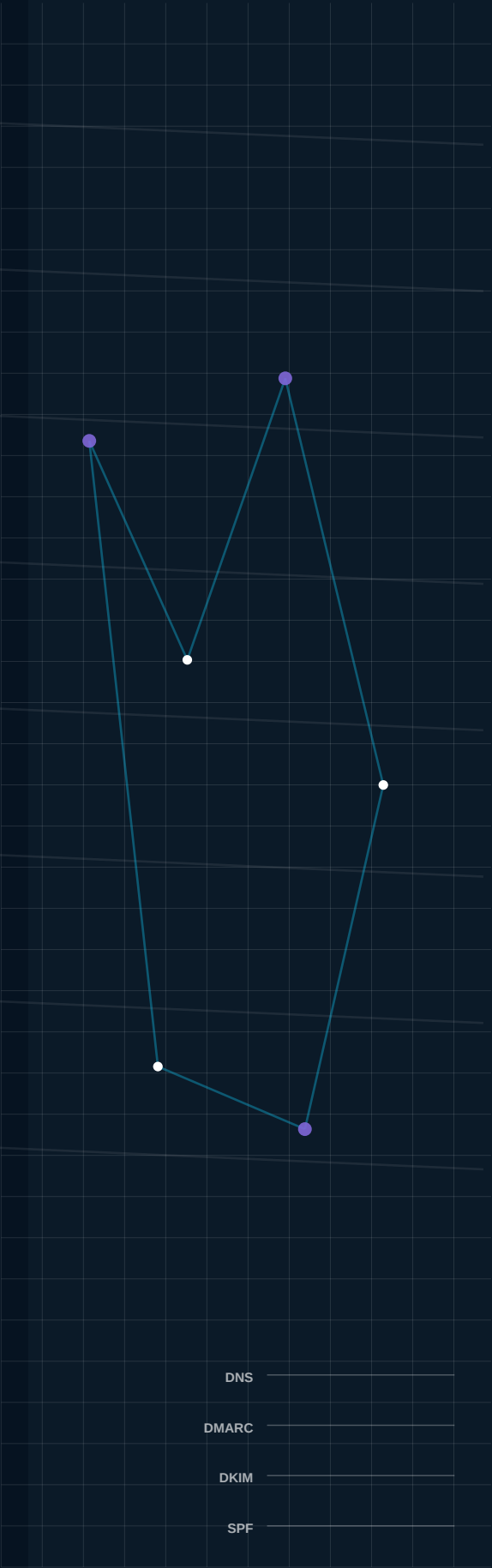


SERVICE OVERVIEW

Trust Monitor

Ongoing review of authentication, policy, sending-source changes and trust-layer drift.



WHY MONITORING MATTERS

Email authentication environments change as businesses change.

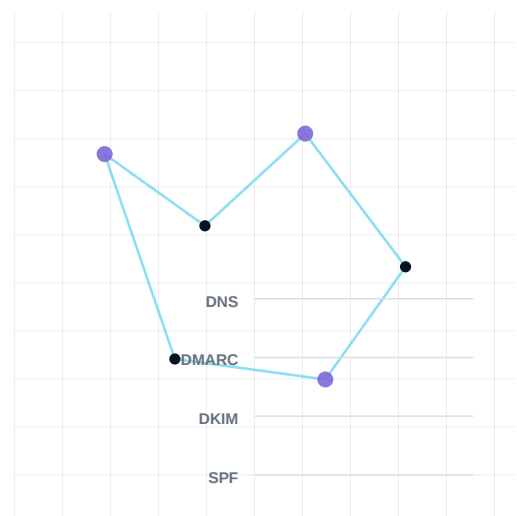
Businesses add CRMs, billing platforms, support systems, website services and new subdomains. Old services can remain authorized after they are no longer used. Configuration and policy can drift without creating an obvious problem straight away.

Trust Monitor keeps the authentication and domain trust layer under review so meaningful changes can be investigated and acted on.

Monitoring is not a dashboard.

RDA reviews the signals, investigates meaningful changes and recommends action when needed. The value is interpretation and accountability, not automated alerts alone.

Ongoing value comes from change review, investigation and specialist accountability.



WHO THIS IS FOR

Who this is for

Trust Monitor is designed for suitable businesses that want a specialist to remain accountable for the email authentication and domain trust layer after a baseline has been established.

- | | | | |
|----|--|----|--|
| 01 | Businesses that completed remediation | 02 | Organizations with several legitimate sending systems |
| 03 | Firms that regularly add or change business platforms | 04 | Businesses where trusted client or financial email matters |
| 05 | Environments where policy progression or ongoing review is appropriate | 06 | Organizations that want continued specialist oversight |

The emphasis is continuity: understand meaningful changes, investigate what matters and keep the environment documented.

SCOPE OF WORK

Monitoring and assurance scope

01	Authentication and Policy Monitoring	Keep SPF, DKIM, DMARC, alignment and policy position under review using the available monitoring data and verified baseline.
02	New or Unexpected Sending-Source Review	Review newly observed or unexpected sources and determine whether they are legitimate, stale or require investigation.
03	Change and Drift Detection	Identify meaningful changes to the known authentication and domain trust environment.
04	Meaningful Failure Investigation	Investigate relevant authentication failures or changes and recommend the appropriate next step.
05	Policy Position and Progression Review	Review readiness for stronger DMARC policy where appropriate. Progression is based on evidence, not the passage of time.
06	Periodic Assurance Summary and Recommendations	Document meaningful changes, work completed, unresolved items and recommended next actions.

PRICING AND DELIVERABLES

Ongoing scope and monthly fee

PRICE

From \$199 / month

Final monthly scope is confirmed after baseline review. More complex environments may be quoted separately.

Suitable clients may first enter a defined Post-Remediation Assurance period where evidence needs to be observed over time.

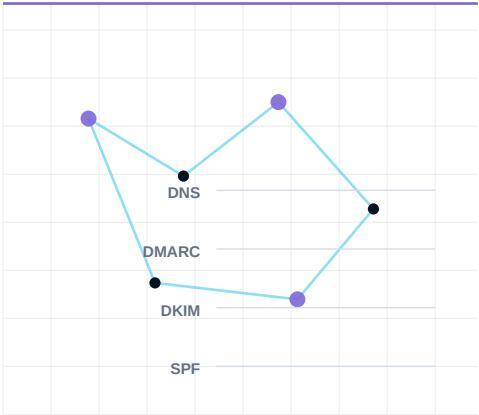
ONGOING VALUE

Authentication and policy monitoring	Ongoing
Sending-source and drift review	Ongoing
Meaningful change alerts	As detected
Failure investigation	As needed
Assurance summary	Periodic
Recommendations and next actions	As needed

HOW TO GET STARTED

Best started after remediation or an established baseline.

Trust Monitor is not a substitute for fixing known issues. RDA first establishes a verified baseline. Where evidence must be observed after remediation, we may recommend a defined Post-Remediation Assurance period before ongoing monitoring. DMARC policy progression is evidence-led, not calendar-led.



STARTING STEPS

- 01 Confirm the domain and known sending environment
- 02 Establish or verify the baseline
- 03 Confirm the monitoring scope and monthly fee
- 04 Activate monitoring and review
- 05 Receive meaningful alerts, investigations and periodic assurance summaries

RDA

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