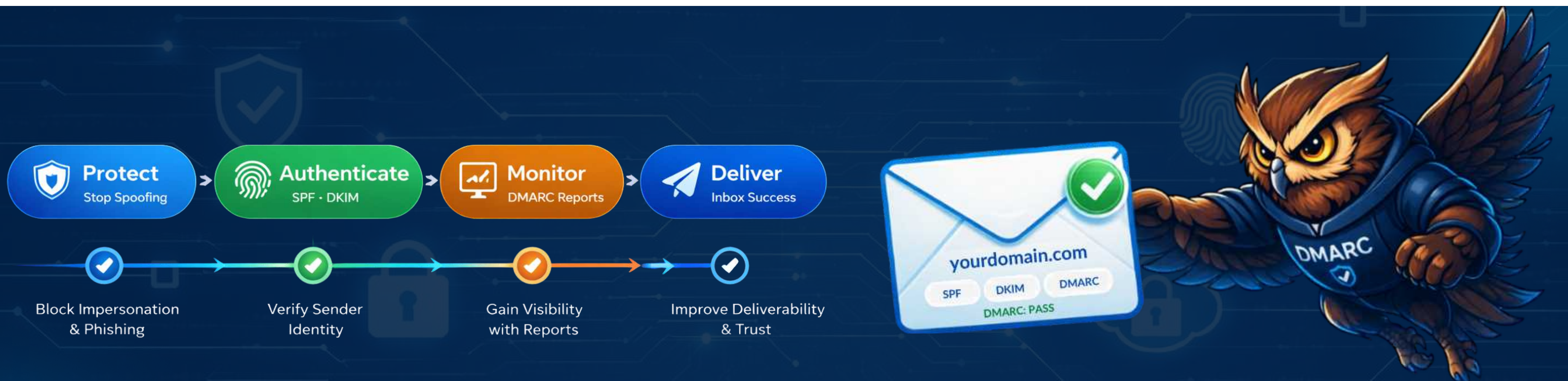


YOUR DOMAIN. YOUR REPUTATION.

Stop spoofing, phishing, and impersonation, before they damage your brand and your business.



#1

Attack vector targeting businesses globally

3-in-1

SPF, DKIM & DMARC - all under one shield

24/7

Continuous domain monitoring & protection

THE RISK

Your Domain Is a Target, Every Single Day.

Business email is the most impersonated communication channel in the world. Attackers don't need to hack your systems, they simply forge your domain, send a convincing message, and let your own reputation do the damage.

When your domain is abused, it's not just a security problem. It's a brand problem, a trust problem, and a business continuity problem.



Brand Impersonation

Attackers send emails as your domain to your customers, partners, and employees - damaging trust you've spent years building.

Phishing At Scale

Fraudulent messages that look exactly like they come from you put recipients at risk and expose your organization to liability.

Delivery Failures

Poor authentication posture causes legitimate emails to be rejected or land in spam, silently breaking business communication.

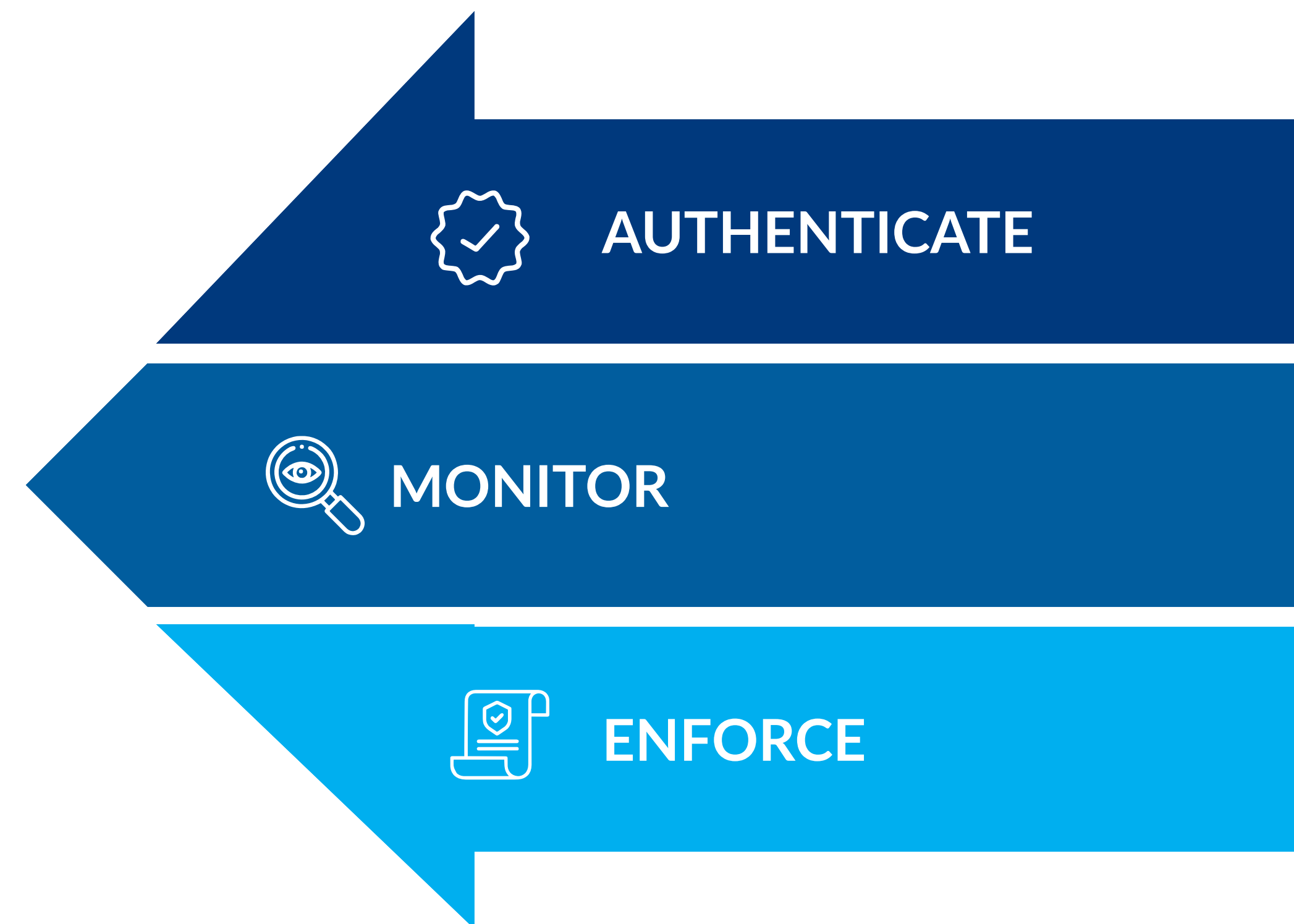
THE SOLUTION

TechOwl DMARC+ - Domain Trust, Fully Managed

TechOwl DMARC+ gives your organization complete control over who can send on behalf of your domain - and continuous visibility into everything that's happening with your domain's email authentication posture.

It's not a one-time configuration. It's an always-on layer of protection that monitors, alerts, and enforces - so your domain reputation stays intact and your communication stays trusted.

- 01 We set up and validate SPF, DKIM, and DMARC across your domain - correctly, completely, and without gaps.
- 02 Continuous 24/7 monitoring detects unauthorized senders, misconfigurations, and authentication failures in real time.
- 03 We guide you through graduated policy enforcement from visibility to quarantine to full reject at your pace.



PLATFORM CAPABILITIES

Everything You Need to Manage Human Risk

Authentication & Protection

Full SPF, DKIM, and DMARC configuration - validated and aligned across your domain. Includes BIMI setup to display your logo in supported inboxes, reinforcing brand trust at the point of delivery.

Continuous Monitoring & Visibility

Always-on detection of unauthorized senders, authentication failures, and suspicious sending sources. Know the moment something is wrong - before your recipients do.



Enforcement Readiness

We track your policy maturity and guide you through each enforcement stage so you move from monitoring to full protection without disrupting legitimate communication.

Delivery Confidence

Proper authentication directly improves inbox placement. Your legitimate messages reach where they should - reliably, without being flagged as spam or rejected.

BUSINESS OUTCOMES

What Changes When You Deploy DMARC+

Your Domain Cannot Be Spoofed

Unauthorized senders are blocked before recipients ever see a fraudulent message.

Your Brand Stays Trusted

Customers & regulators know that communication from your domain is genuinely from you.

Your Legitimate Email Gets Delivered

Strong authentication signals improve sender reputation and inbox placement across providers

Your Team Sees What's Happening

Real-time visibility into domain authentication activity - no more flying blind.

Your Compliance Posture Strengthens

Demonstrable control over official communication channels satisfies growing regulatory expectations.

Issues Are Caught Before They Escalate

Misconfiguration alerts and failure monitoring mean problems are fixed before they become incidents.



GOVERNANCE & COMPLIANCE

Built for Regulated Environments

Email authentication is no longer just a best practice - it's increasingly mandated by regulators, required by major inbox providers & expected by enterprise procurement. DMARC+ helps organizations get & stay ahead of these requirements.

Compliance Support

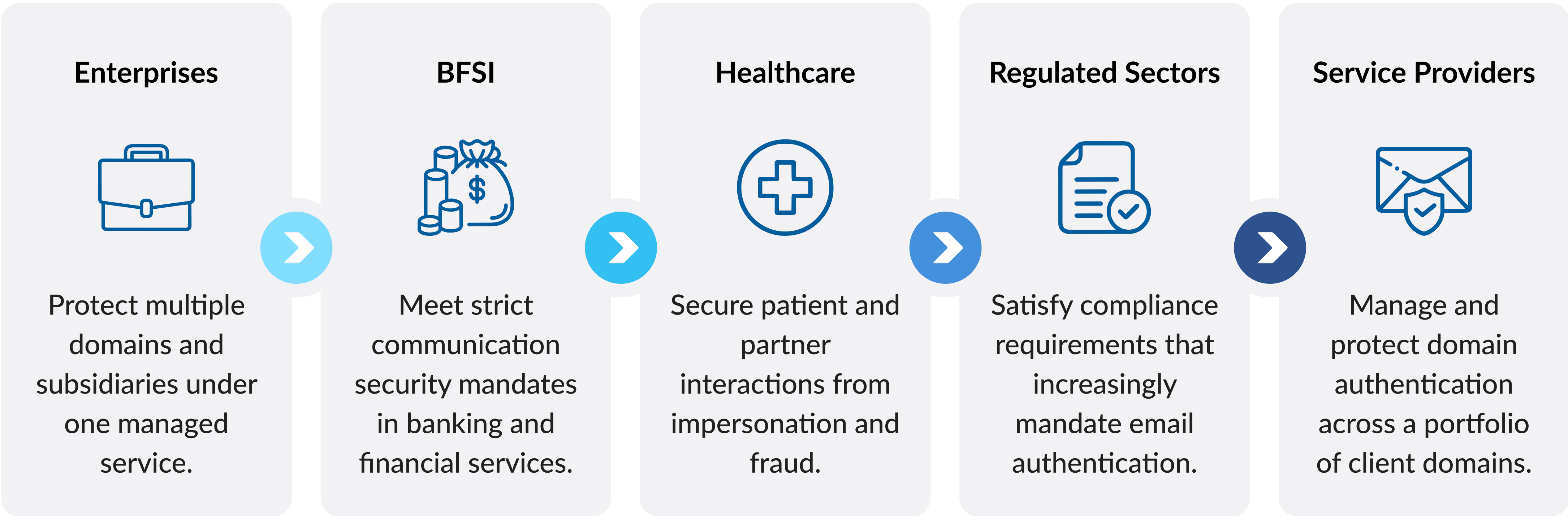
- ✓ Email security control validation
- ✓ Domain protection governance documentation
- ✓ Fraud prevention readiness evidence
- ✓ Communication integrity assurance
- ✓ Audit-ready reporting

Governance Value

- ✓ Demonstrates active enforcement of email controls
- ✓ Reduces impersonation-related business and legal risk
- ✓ Strengthens trust in official digital communications
- ✓ Supports BFSI, Healthcare & regulated sector mandates
- ✓ Helps meet modern cybersecurity governance expectations

WHO IT'S FOR

Built for Organizations Where Trust Cannot Be Compromised



WHY DMARC+

Beyond Basic DMARC - What Sets TechOwl Apart

Most organizations have some DMARC record in place. Very few have it working properly - continuously monitored, enforced, and integrated into their security posture. That's exactly the gap DMARC+ fills.

NO.	CAPABILITY	BASIC DMARC SERVICES	DMARC+ BY TECHOWL SHIELD
1	SPF / DKIM / DMARC Record Setup	✓	✓
2	Initial Configuration Support	✓	✓
3	Continuous Authentication Monitoring	✗	✓
4	Unauthorized Sender Visibility	Limited	✓ Full Visibility
5	Misconfiguration Detection	✗	✓
6	Policy Enforcement Readiness Tracking	✗	✓
7	Domain-Level Risk Visibility	✗	✓
8	Ongoing Monitoring & Support	✗	✓
9	Integrated Security Visibility	✗	✓
10	BIMI Setup & Logo Authentication	✗	✓
11	MTA-STS Configuration & Enforcement	✗	✓
12	TLS-RPT (SMTP TLS Reporting)	✗	✓

Basic DMARC setup is a starting point, not a solution. DMARC+ is the difference between having a record and having protection.

Part of the TechOwl Security Platform

 TechOwl SHIELD Attack Surface Monitoring	 TechOwl DMARC+ Email Trust Assurance	 TechOwl TPRM Third-Party Risk Intelligence	 TechOwl CSPM Cloud Security Visibility
 TechOwl Phishlens Employee Risk Readiness	 TechOwl ThreatPulse Threat Signal Intelligence	 TechOwl ThreatLab Advanced Threat Detonation	 TechOwl Simulens Continuous Breach & Attack Simulation

Secure Your Domain. Protect Your Brand.

TechOwl DMARC+ secures domain trust while ensuring your business communication reaches where it should - safely and reliably.

