

PowerDMARC

Email authentication: DMARC, SPF, DKIM, and BIMl.

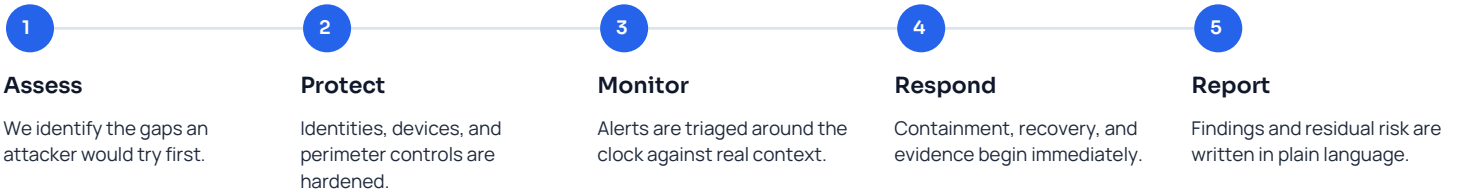


Service illustration • Cybersecurity

POWER DMARC

Email spoofing lets attackers impersonate your domain to customers and vendors. PowerDMARC simplifies DMARC, SPF, DKIM, and BIMl so domains can be locked down. Massive IT uses PowerDMARC to take customer domains to full enforcement safely.

A clear path to delivery



Product areas & practical applications

Product area	Practical application
DMARC reporting and analytics	visibility into who is sending email as your domain
Hosted SPF and DKIM	simplified management of sender authentication records
DMARC enforcement	staged move to quarantine and reject policies
BIMl and MTA-STs	brand logos in inboxes and stronger transport security

When to talk to us

- Spoofed emails impersonating the company
- Legitimate email landing in spam
- Google and Yahoo bulk-sender authentication requirements

Deployment & ongoing support

Massive IT inventories every legitimate sending service, fixes SPF and DKIM, monitors DMARC reports, and moves domains to enforcement without disrupting legitimate mail.

Scope and licensing vary by environment. Product availability and support terms are confirmed during planning.