

PowerDMARC

Email authentication: DMARC, SPF, DKIM, and BIMl

Overview

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.

What we deploy and support

- 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 customers call us

- Spoofed emails impersonating the company
- Legitimate email landing in spam
- Google and Yahoo bulk-sender authentication requirements
- SPF records that exceed lookup limits

How Massive IT works with PowerDMARC

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

PowerDMARC fits any organization that sends email from its own domain.