

Breached healthcare orgs leave email authentication unenforced

74% of breached organizations had missing or unenforced DMARC. Over half also ran permissive or missing SPF records.

What we found

74% of breached organizations had missing or unenforced DMARC.

Of breached organizations, 41% had no DMARC at all and 33% ran it in monitoring-only mode, so unauthorized senders were never blocked. SPF was more common but often permissive: 46% used soft-fail policies and 9% had no record, letting spoofed mail still reach the inbox.

What it means for buyers

⊗ **DMARC rarely enforced**

74% of breached organizations had missing or unenforced DMARC, 41% with none and 33% monitor-only.

🔒 **SPF left permissive**

56% ran permissive or missing SPF, with 46% soft-fail and 9% no record at all.

⚠️ **Spoofed mail still lands**

Without enforcement, messages from unauthorized servers are delivered instead of rejected.

WHY PAUBOX

8,000+

healthcare organizations rely on Paubox to secure inbound and outbound email.

🛡️ **Inbound Email Security**

Behavioral AI catches phishing and impersonation that passed sender checks.

🔒 **ExecProtect blocks impersonation**

Patented detection of name and role spoofing in inbound email.

✅ **HITRUST certified**

Annual third-party audit of every control.