Why old gaps in email security lead to new breaches

Persistent configuration failures cause healthcare data breaches; automated, foundational security controls are the solution

The top 3 attack patterns

75% lacked DMARC enforcement

Three-quarters of breached organizations had no policy to reject or quarantine authorized emails.

0% enforced MTA-STS

Every breached org relied on opportunistic encryption, leaving messages vulnerable to interception.

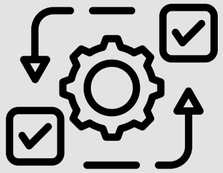
55% had permissive SPF records

Over half of orgs used “soft-fail” policies that allowed unauthorized senders into inboxes.

Default security over human judgement

Remove human decision points

Automate encryption to prevent staff from bypassing security for the sake of speed.



Eliminate workflow friction

Effective security should work in the background without requiring portals, passwords, or plugins.

Secure outbound and inbound email

Default automatic encryption ensures HIPAA compliance, and AI-powered inbound email security protects inboxes from phishing and ransomware.