PAUBOX RESEARCH

PAUBOX

Opportunistic TLS is attempted encryption, never guaranteed

None of the breached organizations enforced MTA-STS, so email fell back to plaintext whenever a receiving server could not encrypt.

What we found

None of the breached organizations enforced MTA-STS.

Opportunistic TLS attempts encryption but sends unencrypted when the receiver cannot support it, so protection is never guaranteed. In a downgrade attack, an interceptor forces that fallback and reads or alters the message in transit. MTA-STS closes the gap by refusing delivery over an unencrypted connection.

What it means for buyers

MTA-STS enforced by none
Not one breached organization enforced MTA-STS, leaving transport encryption optional.

Plaintext is the fallback
Opportunistic TLS sends unencrypted whenever the receiving server cannot encrypt.

Downgrade attacks exploit it
An interceptor can force the fallback and read or alter PHI in transit.

WHY PAUBOX

100%

of outbound Paubox email is encrypted by default, secured at TLS 1.2 or higher.

TLS enforced, never downgraded
PHI transits only over modern, authenticated TLS, or routes to a patented Secure Message Center.

No silent plaintext fallback
When encryption cannot be established, PHI routes to a secure path instead of the open internet.

HITRUST certified
Annual third-party audit of every control.

Sources: Paubox 2026 research, 2026 Healthcare Email Security Report (analysis of 2025 healthcare email breaches).