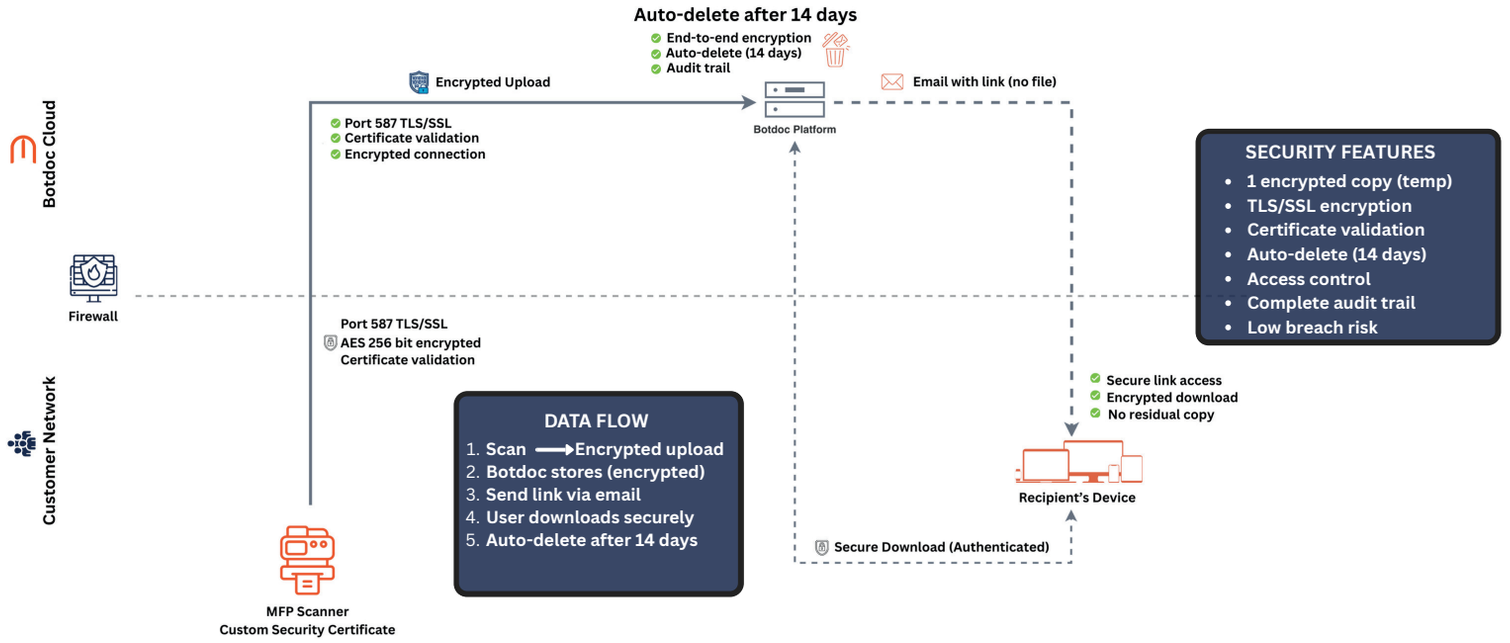
Botdoc MFP Solution

BOTDOC·iO

Eliminating the Hidden Risk in Scan-to-Email

How encrypted document delivery closes a major enterprise security gap



About Botdoc

Botdoc transports data and documents for some of the largest financial firms in the world, Fortune 100 banks, Large Education providers and the largest Healthcare platforms globally. Botdoc's technology, that is trusted by over 37,000 financial professionals every day, is now transforming the security of Multi Function Printers (MFPs) as the first security enabled "Scan to Email" capability.

End-to-End Encryption

AES-256 encryption and secure TLS protocols protect every document from the moment it is scanned through delivery. Data remains fully encrypted in transit and at rest, eliminating hop-by-hop email vulnerabilities and preventing interception, tampering, or unauthorized access.

Working With Existing MFPs

Botdoc deploys directly into your current printer environment with zero hardware changes or capital investment, securing document workflows across all major MFP brands without operational disruption.

5 Minute Deployment

With an average setup time of just 5 minutes per device, Botdoc enables rapid, enterprise-wide deployment—no complex configuration or extensive training required.

Secure Scan Replacement

Replaces insecure scan-to-email with end-to-end encrypted document delivery

Auditable Delivery Path

Delivers documents through secure, fully auditable transmission pathways

No Hardware Disruption

Delivers documents through secure, fully auditable transmission pathways.

Rapid 5-Minute Deployment

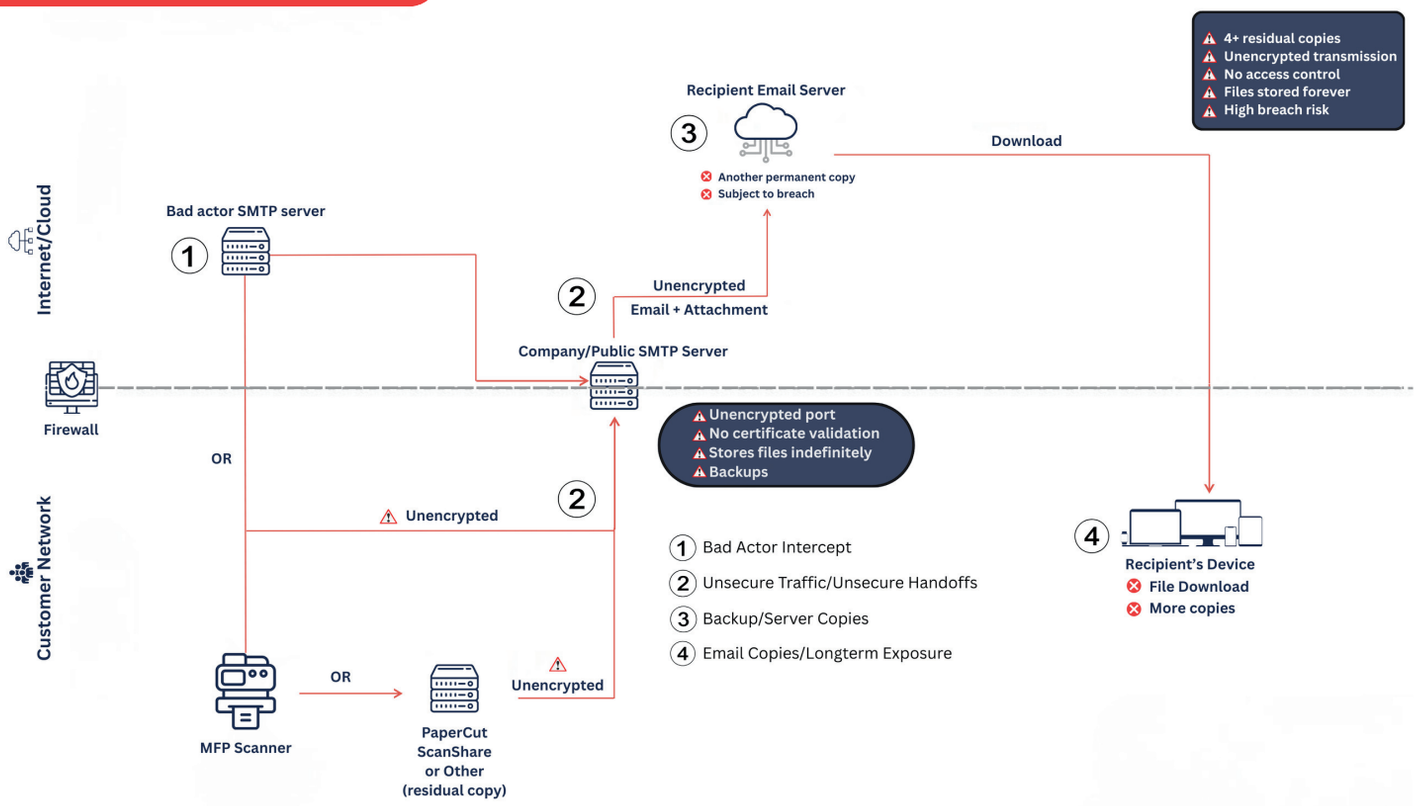
Installs in an average of just 5 minutes per device for rapid enterprise rollout

sales@botdoc.io
+1-719-960-4767

BOTDOC·iO

The Problem: Risk in Scan-to-Email

BOTDOC·iO



Scan-to-email is the default workflow for sending documents from multi-function printers (MFPs), but it introduces a major security blind spot.

Multi-Hop SMTP Exposure
Emails traverse multiple servers and inspection points where encryption can be downgraded or removed, creating repeated opportunities for interception.

Man-in-the-Middle Vulnerability
Unsecured transmission paths allow attackers to intercept, alter, or redirect scanned documents without detection.

Unencrypted Data Proliferation
Scanned files are stored unencrypted in inboxes, archives, and backups, producing uncontrolled copies that persist indefinitely.

Regulatory & Compliance Gaps
GLBA, FTC Safeguards, HIPAA, and similar frameworks require encryption in transit and strict access controls—standards scan-to-email typically fails to meet.

High-Value Target for Account Takeover
Email accounts are prime attack surfaces. A single compromised mailbox can expose years of sensitive scanned documents.

Legal & Litigation Exposure
Email systems and backups retain data long-term, making scanned documents fully discoverable and increasing legal liability.

sales@botdoc.io
+1-719-960-4767

BOTDOC·iO