Simplify ITAR with 120.54 “End to End Encryption”

Alexander Major
Partner & Co Chair
Government Contracts & Global Trade
McCarter English

Matt Henson
Principle
Global Trade Solutions
TC Engines

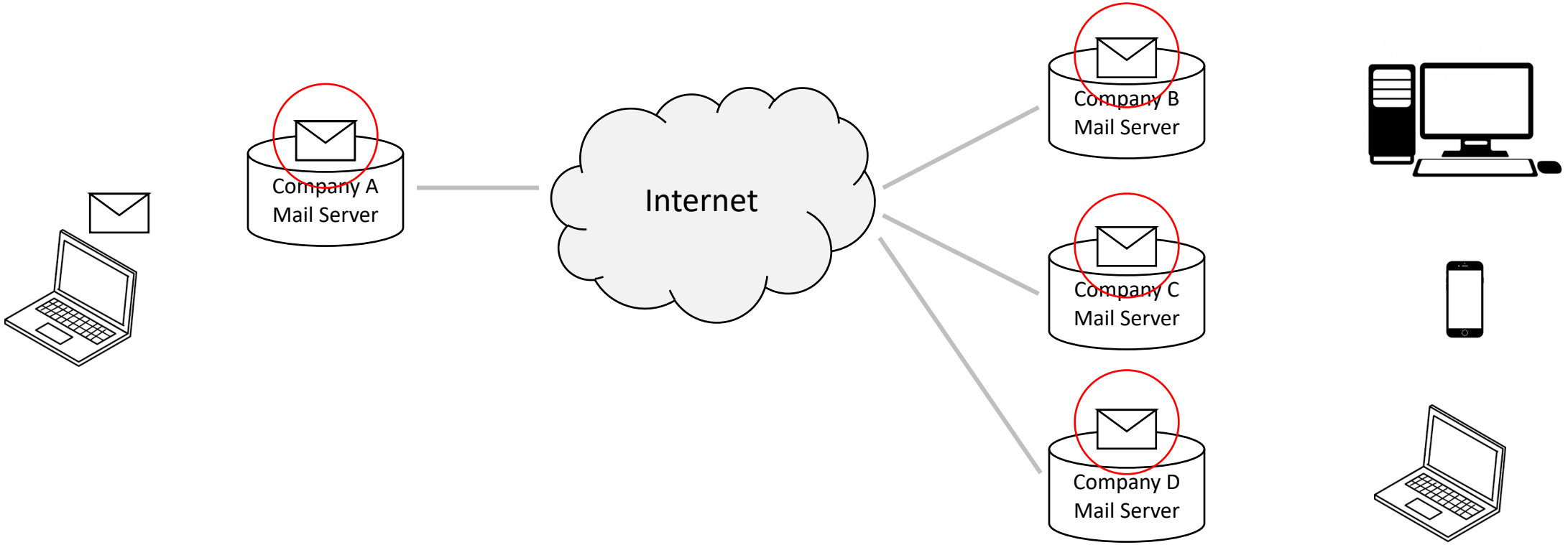
State Department ITAR Regulation 120.54

Unclassified ITAR Data may be sent, stored, shared provided:

(i) Secured using end-to-end encryption;
(ii) Secured using cryptographic modules (hardware or software) compliant with the Federal Information Processing Standards Publication 140-2 (FIPS 140-2) or its successors
(iii) The means of decryption are not provided to any third party.

https://www.ecfr.gov/current/title-22/chapter-I/subchapter-M/part-120/section-120.54

CUI on Traditional Mail Servers

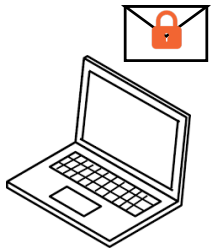


In Traditional Systems, like GCC High, O365, GSuite the Server can see Unencrypted data
So can the attacker

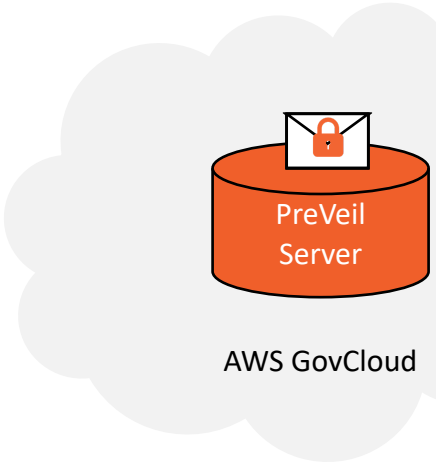
End-to-end Encryption Simplifies Security & Compliance > Zero Trust

All Emails & Files are encrypted at the sender's device and can only be decrypted by the recipient
The Servers can never decrypt the data, neither can attacker

Encrypt



Company A



Decrypt

Company B

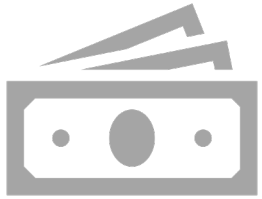
Company C

Company D

Since Data on Cloud Servers is Always Encrypted, dramatically reduces cloud server security complexity

Benefits

Enables adoption of Simpler Cloud Services vs Complex On Prem Solutions



Reduces Cost

Enhances Security Using the Gold Standard of End to End Encryption and Zero Trust