ECHOWORX
IT PAYS TO BE SECURE

90% OF IT SECURITY EXECUTIVES ARE PRIORITIZING EMAIL DATA PROTECTION IN 2021

In an increasingly digital world, sending and receiving documents securely is top of mind for IT security professionals. Companies recognize the importance of email encryption solutions and acknowledge they need to be improved in order to achieve their future digital goals.

Pulse and Echoworx surveyed 100 IT security executives in North America and EMEA to better understand their plans for email encryption in 2021, the challenges to overcome, what features they look for in potential solutions, and how they build consensus within the buying group.

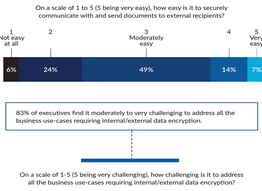
Data collected from Jan. 27 - Feb. 8, 2021

Respondents: 100 IT Security Executives

Executives are prioritizing data and document security in 2021 by allocating budget for email encryption solutions.

The majority (90%) of executives prioritize protecting data and documents sent through emails.

How high a priority is protecting data and documents sent through email for your organization in 2021?



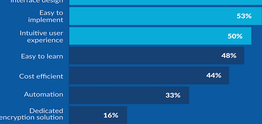
Sending secure documents isn't very easy and many executives find it challenging to address all the use-cases for encryption.

Only 7% of IT security executives find it very easy to communicate and send documents to external recipients.

On a scale of 1 to 5 (5 being very easy), how easy is it to securely communicate with and send documents to external recipients?

83% of executives find it moderately to very challenging to address all the business use-cases requiring internal/external data encryption.

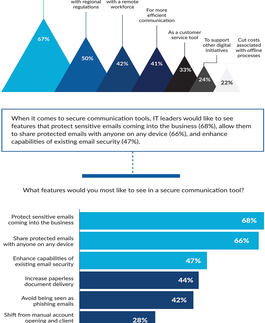
On a scale of 1-5 (5 being very challenging), how challenging is it to address all the business use-cases requiring internal/external data encryption?



A good email data protection tool must overcome roadblocks for the end user.

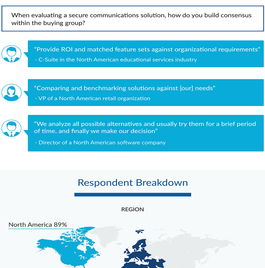
When using an email data protection tool, uninitutive user experience (51%), difficulty of implementation (42%), and lack of automation (40%) are the biggest end user roadblocks.

What are the biggest end user roadblocks to using an email data protection tool?



The top 3 must-have features in an email data protection tool are good user interface design (54%), ease of implementation (53%), and intuitive user experience (50%).

When evaluating an email data protection tool, what are the 3 most important must-have features?



The need to exchange secure digital documents is high, especially those coming into the business.

IT security executives can see their organizations using secure communication to exchange secure digital documents (67%), maintain compliance with regulations (50%), and communicate with a remote workforce (42%).

What use-cases do you see for secure communication at your organization?

When it comes to secure communication tools, IT leaders would like to see features that protect sensitive emails coming into the business (68%), allow them to share protected emails with anyone on any device (66%), and enhance capabilities of existing email security (47%).

What features would you most like to see in a secure communication tool?

When evaluating a secure communications solution, how do you build consensus within the buying group?

"Provide ROI and matched feature sets against organizational requirements"
- C-Suite in the North American educational services industry

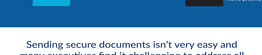
"Comparing and benchmarking solutions against [our] needs"
- VP of a North American retail organization

"We analyze all possible alternatives and usually try them for a brief period of time, and finally we make our decision"
- Director of a North American software company

Respondent Breakdown

REGION

TITLE



COMPANY SIZE