FORRESTER®

Improved Email Security Starts With Greater Usability

Protecting Email Communication With Encryption Builds Customer Trust, But It Must Be Easy To Use

Get started ⟶

FORRESTER OPPORTUNITY SNAPSHOT: A CUSTOM STUDY COMMISSIONED BY ECHOWORX
MARCH 2022

Email Communication Remains A Vulnerability

Let's face it: While email is a communication mainstay, it is also a potential source for both intentional and unintentional data breaches. Organizations are doing many things to protect themselves, however they are still experiencing malicious attacks, data loss, and email breaches. Forrester Analytics' 2021 Business Technographics® Security Survey found that 63% of respondents experienced a data breach in the last 12 months.[1] Of those respondents, 31% said the breach was a result of an internal incident within the organization, and 18% cited a third party or partner as the source.

The impact of the global pandemic drove widespread adoption of the work-from-anywhere employment model. This not only created a more distributed workforce, but it also further complicated securing email communication.

Key Findings

Organizations are prioritizing security initiatives related to data loss and document protection, with 77% of respondents stating they need to increase email security.

Current email protection tools lack automation and are difficult to learn and implement. This makes them resource intensive.

More than half of respondents whose organizations improve their data protection capabilities expect to increase customer trust and reduce breaches.

Overview
Situation
Challenges
Solutions
Conclusion

Many Factors Are Significantly Impacting Security Strategy

Respondents listed several factors impacting their organizations' security strategies over the last 12 months. A strong majority report that their organizations' cloud adoption/migration and software-as-a-service (SaaS) strategies have had a significant impact on their security strategy over the last year. Nearly three-quarters of respondents report that the mobile environment is impacting their security strategies, while 63% are feeling the impact of the shift on remote working.

As a result, more than 50% of respondents are prioritizing data protection, DLP, moving security services to the cloud, and improving email security strategies as top priorities for the next 12 months. Respondents ranked their top priorities as the following: data protection (63%); moving security services to the cloud (59%); and improving security analytics capabilities (56%).

"How much of an impact has each of the following had on your organization's security strategy over the past 12 months?" (Positive impact)

81%	Cloud adoption/migration
79%	SaaS adoption
75%	Digital transformation
73%	Mobile environment
63%	Remote/hybrid work model

FORRESTER OPPORTUNITY SNAPSHOT: A CUSTOM STUDY COMMISSIONED BY ECHOWORX
MARCH 2022

"What are your organization's top security priorities over the next 12 months?"

63%	Improving data protection across multiple environments
60%	Improving data loss prevention capabilities
59%	Moving security services to the cloud
57%	Improving email security strategies
56%	Improving security analytics capabilities (SIM, SIEM, EDR, etc.)

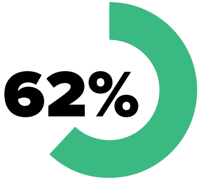
Base: 203 global managers or above with decision-making responsibility for their organizations' email security strategy
Source: A commissioned study conducted by Forrester Consulting on behalf of Echoworx, January 2022

Overview
Situation
Challenges
Solutions
Conclusion

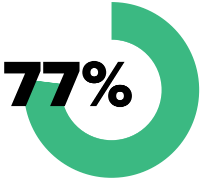
Organizations Believe Their Current Email Security Solution Is Efficient

More than half of respondents feel that their current email security/DLP solutions are efficiently preventing compromises and protecting sensitive data. However, 77% percent of security decision makers agree that their company needs to increase protection for messages and documents sent via email. As a result, respondents' organizations are investing in solutions to further protect messages and documents.

63% of respondents have either implemented or are expanding their organizations' adoption or investment in technologies to protect documents.

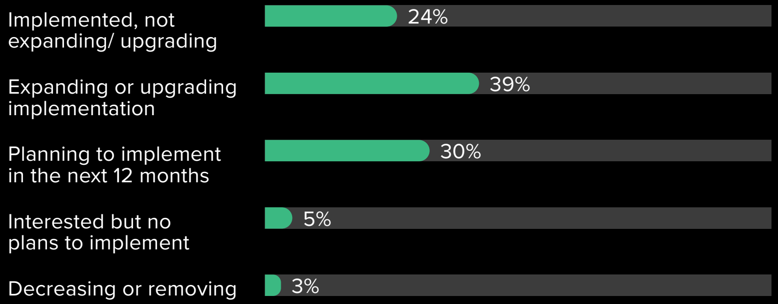


feel that their organization's current email security/DLP solutions are very efficient and efficient in preventing compromise and protecting sensitive data.



agree that their company needs to increase protection for messages and documents sent via email.

"At what stage is your company in the adoption or investment of technologies to protect documents and messages?"



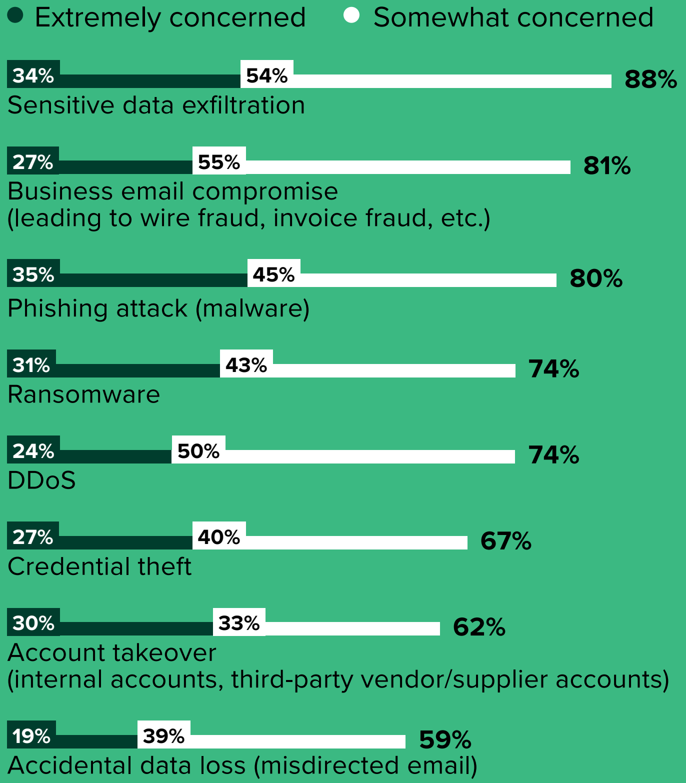
Base: 203 global managers or above with decision-making responsibility for their organizations' email security strategy
Source: A commissioned study conducted by Forrester Consulting on behalf of Echoworx, January 2022

Overview
Situation
Challenges
Solutions
Conclusion

The Focus On Privacy Might Be Leaving Companies Open To Breaches

Eighty-eight percent of respondents agree that they are concerned about sensitive data exfiltration. This same group of global managers with decision-making responsibility for their organizations' email security strategy is less concerned about traditional breach types such as phishing (80%), ransomware (74%), or distributed denial of service attacks (DDoS) (74%). Companies must focus on potential issues and at the same time find a balance between protecting customer and employee privacy while reducing privileges and locking down workflows and communications channels.

"How concerned are you that your organization is vulnerable to each of the following types of potential breaches?"



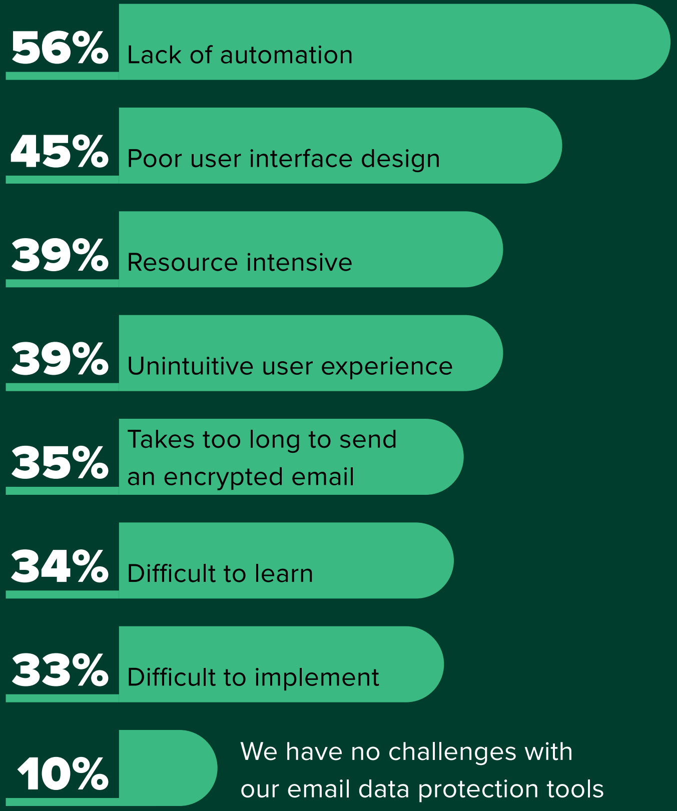
Base: 203 global managers or above with decision-making responsibility for their organizations' email security strategy
Source: A commissioned study conducted by Forrester Consulting on behalf of Echoworx, January 2022

Overview
Situation
Challenges
Solutions
Conclusion

Organizations Face Challenges With Current Email Data Protection Tools

Even though organizations want to improve their email security, most of them face challenges with their current email data protection tools. Email encryption tools lack automation and are difficult to learn and implement; this ultimately makes them time- and resource-intensive. And when a tool or a process is too cumbersome, employees may find workarounds that put data and IP at risk. More than half of respondents experience a lack of automation with their organizations' current email data protection tool.

"Which of the following challenges does your organization have with email data protection tools?"



Base: 203 global managers or above with decision-making responsibility for their organizations' email security strategy
Source: A commissioned study conducted by Forrester Consulting on behalf of Echoworx, January 2022

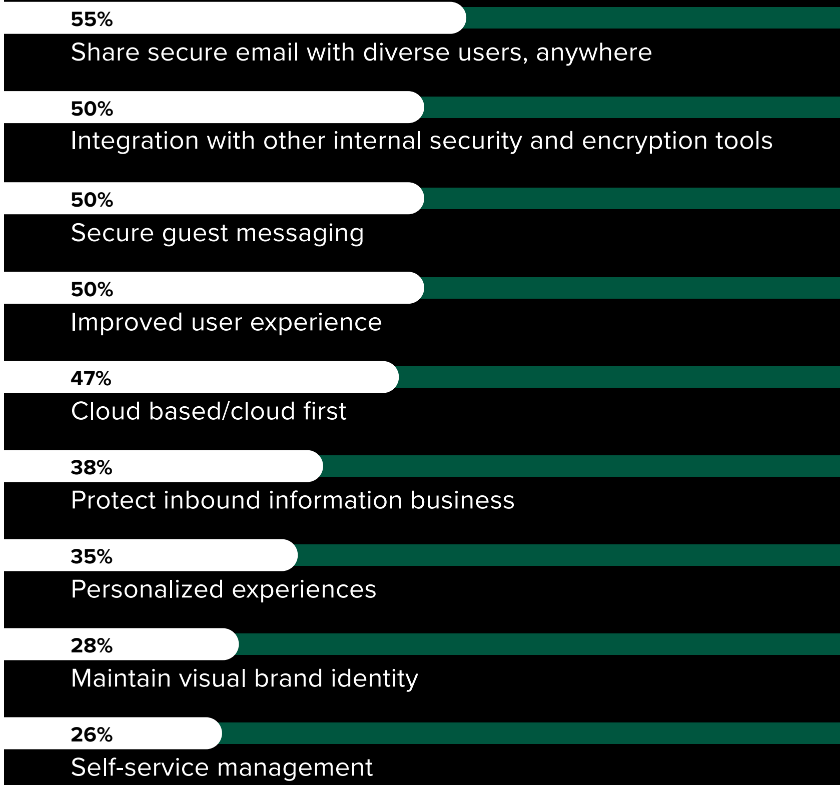
Overview
Situation
Challenges
Solutions
Conclusion

Companies Seek Specific Capabilities To Mitigate Risk

While companies have many tools in place, they're still looking for capabilities to further mitigate risk from email breaches/data loss. Fifty-five percent of respondents said that they need the capability to share secure email with diverse users. In addition, 50% also noted needing: integration with other security and encryption tools; secure guest messaging; and an improved user experience.

Additionally, when asked how to best serve employees, customers, and partners, more than half (55%) of decision-makers agreed that their organizations need several authentication options to do so.

"What capabilities does your organization need to implement to mitigate the risk of email breaches or data loss?"



Base: 203 global managers or above with decision-making responsibility for their organizations' email security strategy
Source: A commissioned study conducted by Forrester Consulting on behalf of Echoworx, January 2022

Overview
Situation
Challenges
Solutions
Conclusion

Improving Data Protection Has Multiple Benefits

Improving data protection capabilities is expected to drive security results, as 54% of respondents expect fewer security incidents/breaches. In addition, more than half of companies expect to gain a better understanding of risk across silos. These security benefits ultimately drive customer trust and improved employee experiences.

More than half of respondents expect to increase revenue by improving their data protection capabilities.

"What benefits would you expect to experience from improving your organization's data protection capabilities?"

60%	54%	53%	50%	40%
Increased trust from customers	Fewer security incidents/breaches	Increased revenue	Better understanding of enterprise risk across silos	Improved employee experience

Base: 203 global managers or above with decision-making responsibility for their organizations' email security strategy
Source: A commissioned study conducted by Forrester Consulting on behalf of Echoworx, January 2022

Conclusion

Email remains a primary communication medium, and this ensures that it remains a top attack vector year over year. To protect sensitive and valuable data, invest in and implement email encryption tools that:

Reduce employee friction. When employees try to short-circuit cumbersome security processes, security incidents and data loss occurs most often.

Increase customer trust. Change the role of security in your company from being a necessary but cumbersome fact of life to the foundation of a trusted brand. Email encryption can focus the protection of your data privacy and transaction security.

Work in concert with legacy email infrastructure and tools. Email encryption tools must ensure deliverability and easy interaction with recipients on different systems with different security controls and tools in place.

Project Director:

Andrea Mendez Otero,
Market Impact Associate Consultant

Contributing Research:

Forrester's Security & Risk research group

Overview
Situation
Challenges
Solutions
Conclusion

Methodology

This Opportunity Snapshot was commissioned by Echoworx. To create this profile, Forrester Consulting supplemented this research with custom survey questions asked of 203 global managers or above with decision-making responsibility for their organizations' email security strategy. The custom survey began and was completed in January 2022.

ENDNOTES

[1] Source: Forrester Analytics Business Technographics Security Survey, 2021.

ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester's Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit forrester.com/consulting.

Demographics

COUNTRY	
United States	**27%**
Canada	**23%**
United Kingdom	**21%**
France	**15%**
Germany	**15%**

TOP 5 INDUSTRIES	
Financial services and/or insurance	**25%**
Agriculture, food, and/or beverage	**7%**
Retail	**6%**
Consumer services	**6%**
Manufacturing and materials	**5%**

COMPANY SIZE	
1,000 to 4,999 employees	**54%**
5,000 to 19,999 employees	**34%**
20,000 or more employees	**11%**

RESPONDENT LEVEL	
C-level executive	**8%**
Vice president	**28%**
Director	**39%**
Manager	**26%**

POSITION/DEPARTMENT	
IT/security	**67%**
Operations	**33%**

FORRESTER®