STATE OF EMAIL ENCRYPTION

2022

ECHOWORX™
IT PAYS TO BE SECURE

Gartner
Peer Insights™

INTRODUCTION

Whether B2B or B2C, email communication remains the primary information sharing platform. It's a convenient way to communicate with partners and customers but isn't a secure channel on its own. Ensuring the security of email-based workflows is critical to modern business. The power to work from anywhere securely with maximum efficiency and the least possible disturbance, alongside the ability to share secure email with diverse users anywhere is top of mind for security professionals.

Echoworx and Gartner Peer Insights surveyed IT, InfoSec, and Operations leaders to find out more about the state of email encryption use across corporate environments in 2022.

DATA BREACHES AND ASSOCIATED COSTS

Worried about data breaches?

IT, security, and operations leaders are concerned about data breaches and the associated costs. Almost 60% reported that data breaches have cost their organization between $11-$50 million in 2021 alone.

With cybercrime and email breaches continuing to be an issue and customer demand for comprehensive security on the rise, email encryption is an essential technology for protecting privacy of communications and ensuring customer trust.

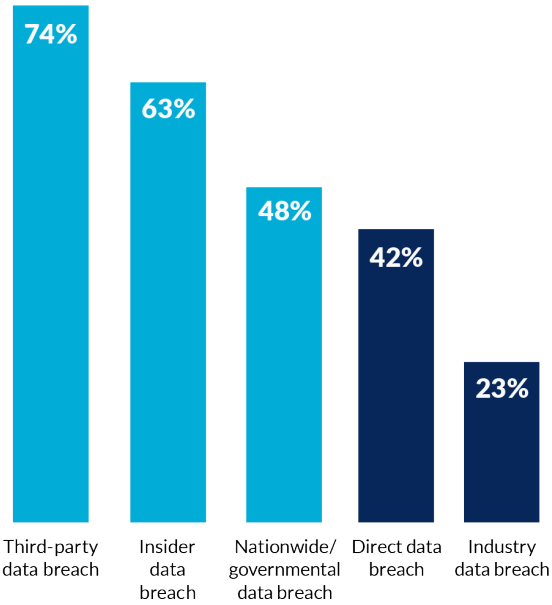
	2022
$11M - $50M	57%
$1M - $10M	29%
$1 - $1M	7%
$51M - $1B	3%

Source: Meeting Email Encryption Criteria, Gartner Peer Insights, Nov 2022

How enterprises may be liable

Third-party data breaches are a serious threat to business cybersecurity. Nearly three quarters (74%) of respondents stated their organization is most liable to a third-party data breach, followed by an insider data breach (63%). In the last five years, the email encryption market has doubled in size. While much of this demand is spurred by increased usage across business lines, support for evolving compliance requirements aid the momentum.

What kinds of cybersecurity data breaches is your organization liable for?

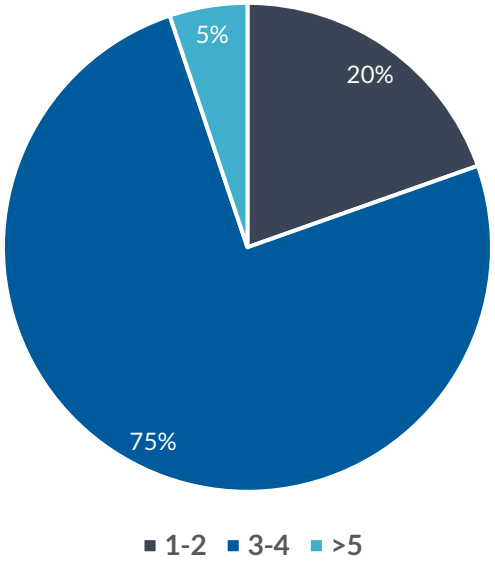


Source: Meeting Email Encryption Criteria, Gartner Peer Insights, Nov 2022

Managing global compliance

Almost 80% of leaders say their organization operates under at least three international privacy regulations. To effectively meet compliance, security, and governance requirements, deploying an email encryption platform that quickly adapts to changing compliance requirements by updating existing encryption processes simplifies maintaining compliance. Another encryption feature to aid compliance and governance is full message logging and tracking, aiding auditing and forensic investigations.

How many international privacy regulations does your organization operate under?

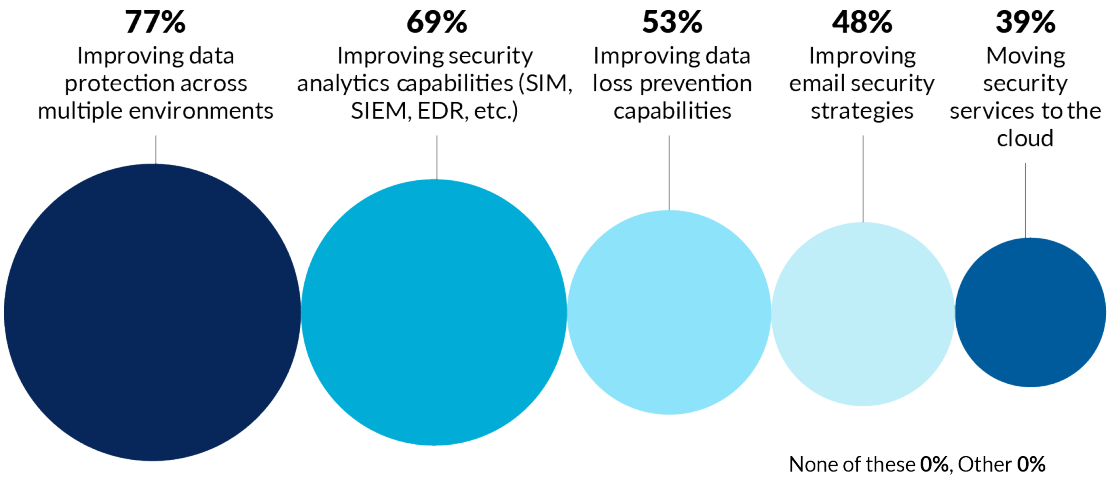


Source: Meeting Email Encryption Criteria, Gartner Peer Insights, Nov 2022

Security priorities this year

Improving data protection across multiple environments (77%) and improving security analytics capabilities (69%) are top security priorities for organizations over the next 12 months.

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

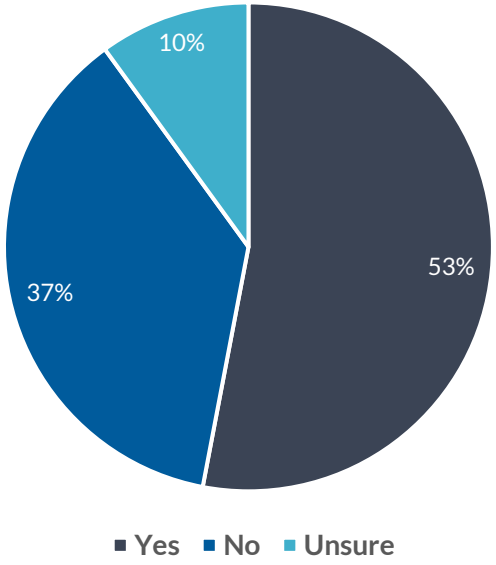


Source: Meeting Email Encryption Criteria, Gartner Peer Insights, Nov 2022

DEVELOPING ENCRYPTION STRATEGY

Over 50% of respondents state that their company has an email/document encryption strategy today.

Does your company have an email encryption strategy today?



Source: State of Email Encryption, Gartner Peer Insights, Nov 2022

The fact that organizations are implementing encryption strategies is good news, since development of such a strategy is an essential best practice. If employees are trained on what should be encrypted, and if rules for what must be encrypted are established for policy-based encryption platforms, such as Echoworx, an organization will face less risk. Enforcing encryption automatically based on customizable policy rules, makes implementing regulatory compliance measures more effective.

In fact, most enterprises today have a mature and progressing set of data privacy and compliance policies that can be the foundation of a comprehensive email encryption strategy. International privacy jurisdictions, rules and regulations often go above and beyond simply being able to send a message or document encrypted – often governing how a secure message is sent, including the use of language elements in the branding, or how a secure message is protected both in transit and at-rest.

Security solutions often sacrifice user experience for the sake of security, leading to frustration and lack of adoption. When email encryption is made easy for end users and customers, they'll use it. Private and sensitive data can be protected while not getting in the way of doing business.

Power to work from anywhere securely with maximum efficiency and least possible disturbance.

Driving encryption strategies

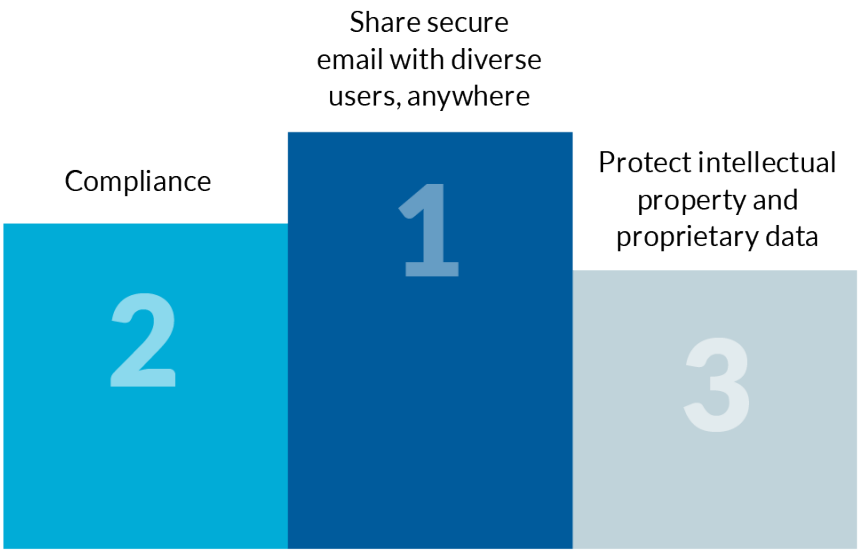
The ability to share secure email with diverse users, anywhere was the top ranked driver when it comes to the email/document encryption strategy within an organization.

This concept is transcending to our digital world where security is increasingly differentiated by user experience, in addition to the protection services rendered. And, for enterprises looking to exchange sensitive information electronically, avoiding time-consuming and irksome experiences are imperative to doing encryption right.

	2016	2022
Compliance	#1	#2
Awareness of data breaches	#2	#7
Avoid data breach costs	#3	#9

2016 Source: Osterman Research, Inc.

Rank the following from most important drivers of email/document encryption strategy at your organization to least important



Pricing **#4**,
Information governance **#5**,
Mobile encryption/containment **#6**,
Increased awareness of data breaches **#7**,
Less negative PR from data breaches **#8**,
Avoidance of costs of data breaches **#9**

Source: State of Email Encryption, Gartner Peer Insights, Nov 2022

In 2016, cost was, by far, mentioned as the main reason for deploying an email encryption strategy. Today, organizations rank other considerations seemingly unrelated to cost, like user experience, as top drivers. This suggests that the actual business value of email protection is not set solely by the lowest possible initial investment – and is instead a value-for-money equation.

MOST ARE USING EMAIL ENCRYPTION

Most organizations (80%) have deployed an email/document encryption solution. Adoption is up significantly from when we last asked in 2016, then email encryption was used by only 40% of organizations, compared to most organizations today.

	2016	2022
Yes	40%	80%
No	60%	15%

2016 Source: Osterman Research, Inc

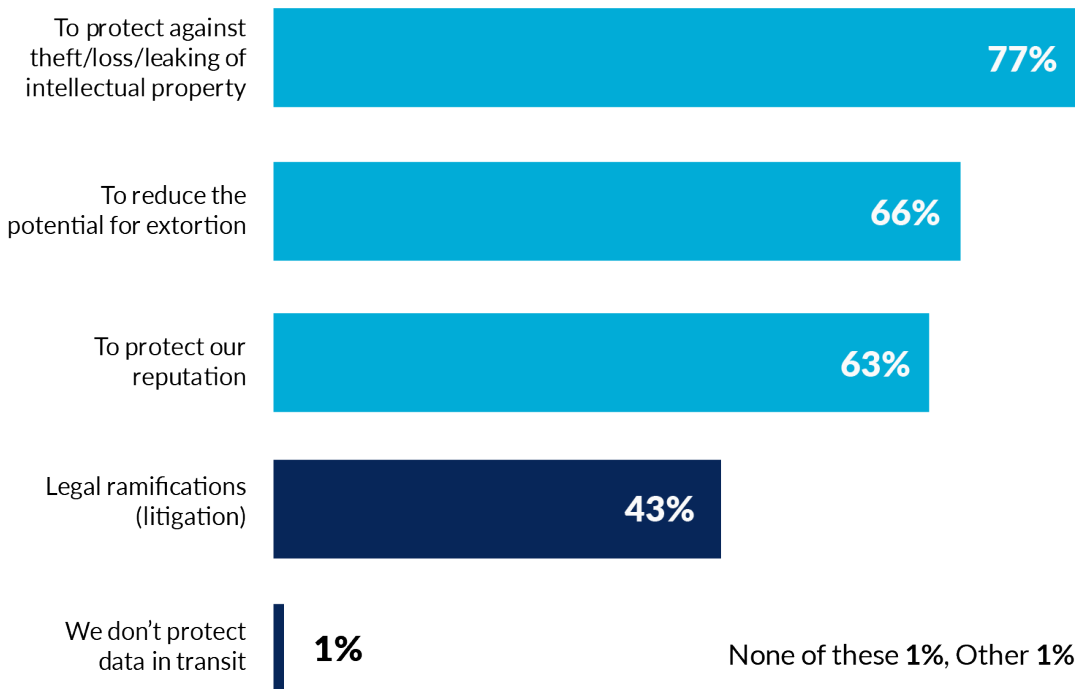
Has your organization deployed an email/document encryption solution?

Source: State of Email Encryption, Gartner Peer Insights, Nov 2022

Bad news about data breaches is driving use of encryption

The top reason why organizations protect data in transit is to ensure their intellectual property is not stolen, leaked, or lost, as reported by over three-quarters (77%) of respondents.

Why does your organization protect data in transit?



Source: Meeting Email Encryption Criteria, Gartner Peer Insights, Nov 2022

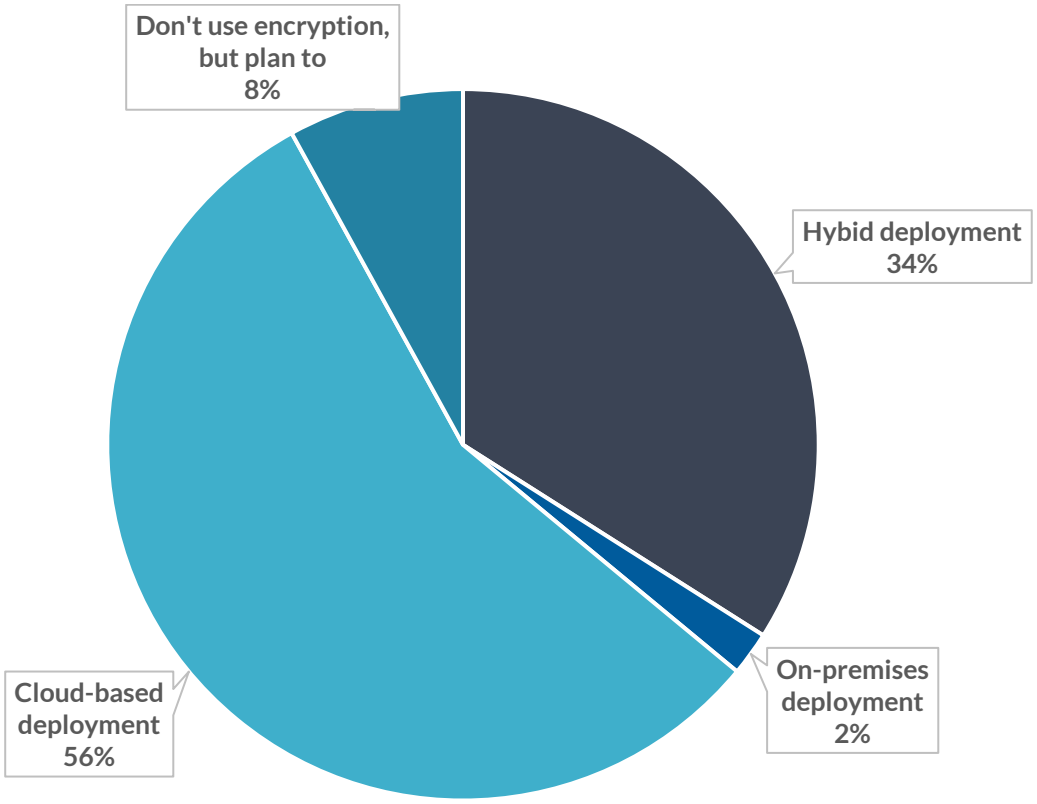
Email and document protection isn't just an IT problem, it's a business problem affecting the entire organization. With new use cases for encryption constantly being created, organizations need to look inward as email encryption is an important part of the messaging infrastructure.

Most encryption solutions are in the cloud

Only 2% deploy their email encryption on-premises. The majority (56%) responded that their deployment is cloud-based.

For many organizations, the move to the cloud is necessary to remain productive. Cloud-based email encryption offers continuous innovation while offloading maintenance allows staff-starved teams to reduce workloads, costs, and outages.

Which of the following best describes your organization's current email encryption deployment?



Source: Meeting Email Encryption Criteria, Gartner Peer Insights, Nov 2022

As use of the cloud takes over, software-as-a-service (SaaS) solutions for secure email encryption have become more prevalent and easier than ever to implement into existing business infrastructures and email-based workflows.

EMAIL ENCRYPTION USE IS EXPANDING

Over 55% of respondents state that their organization has needed to expand their email/document protection in the last five years. When asked about future, over 55% stated they're planning to switch or expand their email encryption solution in the next year. Only a small minority of organizations does not see the need for extending data protection through email encryption.

	Expanded last 5 years	Expanding in 1 year
Yes	55%	57%
No	37%	35%
Unsure	7%	7%

More organizations are realizing that all sensitive information needs to be encrypted to meet data security, legal, compliance, and governance requirements, as well as the expectations of customers. And the number of digital business processes that leverage email to communicate sensitive information is increasing. Organizations will continue to expand their use of email encryption for the foreseeable future.

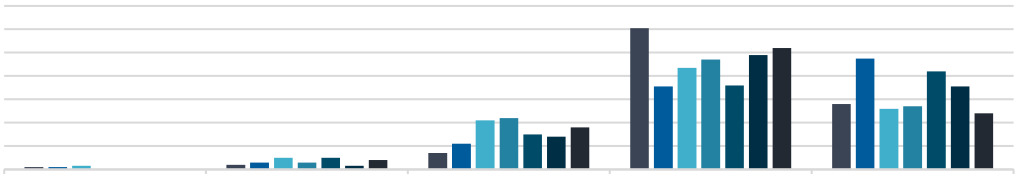
Is your organization planning on switching/ expanding your email encryption solution in the next year?

Source: Meeting Email Encryption Criteria, Gartner Peer Insights, Nov 2022

ORGANIZATIONS FACE CHALLENGES

Only 28% of respondents state that they are very satisfied with the overall security and even less with the cross-device experience (24%) of the email/document encryption in their organization.

How satisfied are you with the following aspects of email/document encryption in your organization?



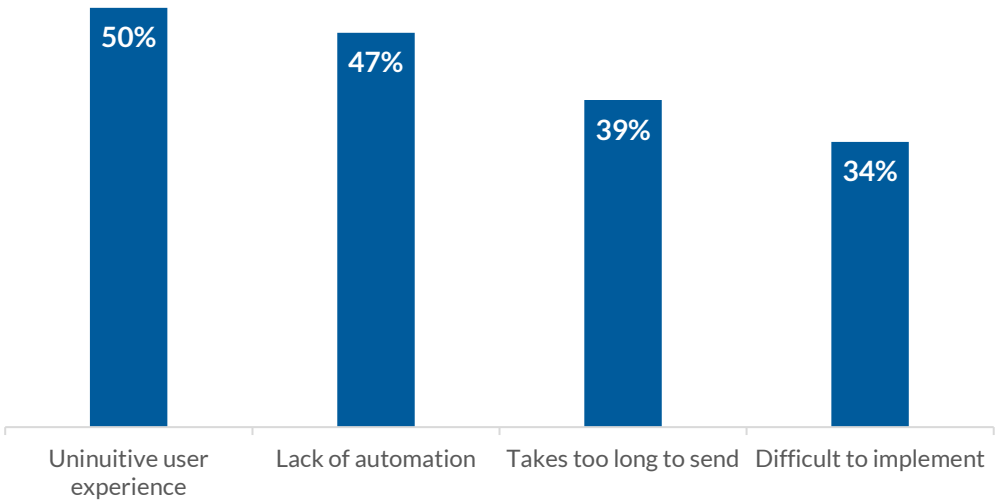
	Very dissatisfied	Moderatley dissatisfied	Neutral	Moderatley satisfied	Very satisfied
Overall security	1%	2%	7%	61%	28%
Ease of use	1%	3%	11%	36%	48%
Offline messaging	2%	5%	21%	44%	26%
Compliance maintenance	0%	3%	22%	47%	27%
Mobile experience	0%	5%	15%	36%	42%
Desktop experience	0%	2%	14%	49%	36%
Cross device experience	0%	4%	18%	52%	24%

Source: Meeting Email Encryption Criteria, Gartner Peer Insights, Nov 2022

Adoption often comes down to user-friendliness

What prompts the actual adoption challenges? Over 50% of respondents state that the biggest challenges their organizations face when it comes to their data protection tools are poor user interface design (59%) and non-intuitive user experience (50%).

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



Resource intensive **32%**,
Difficult to learn **21%**,
None of these **3%**, Other **1%**

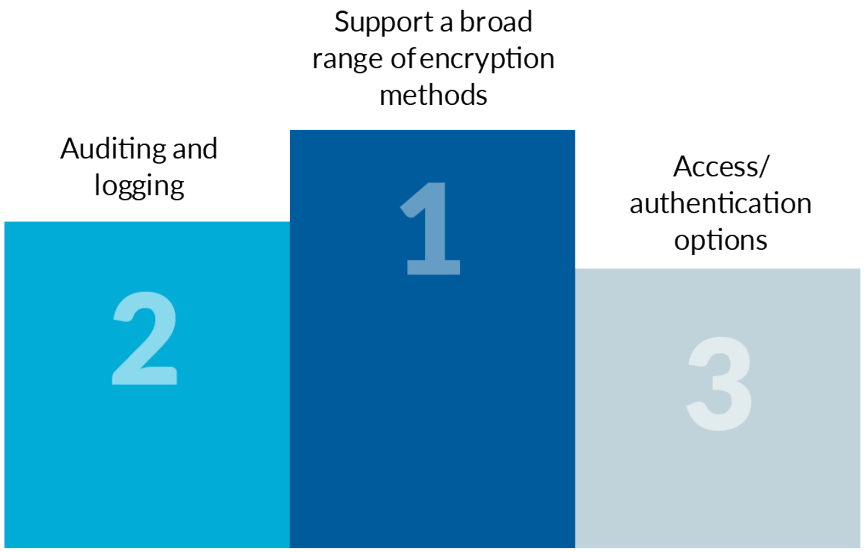
(n = 114)

Source: Meeting Email Encryption Criteria, Gartner Peer Insights, Nov 2022

MOST IMPORTANT CAPABILITIES?

Most decision makers and influencers consider a variety of features and functions to be important for encryption solutions to support, but most flagged for organizations is a solution's ability to support a broad range of encryption methods.

Rank encryption features from most to least important to your organization



Control over data storage and processing locations **#4**, Extensive branding **#5**

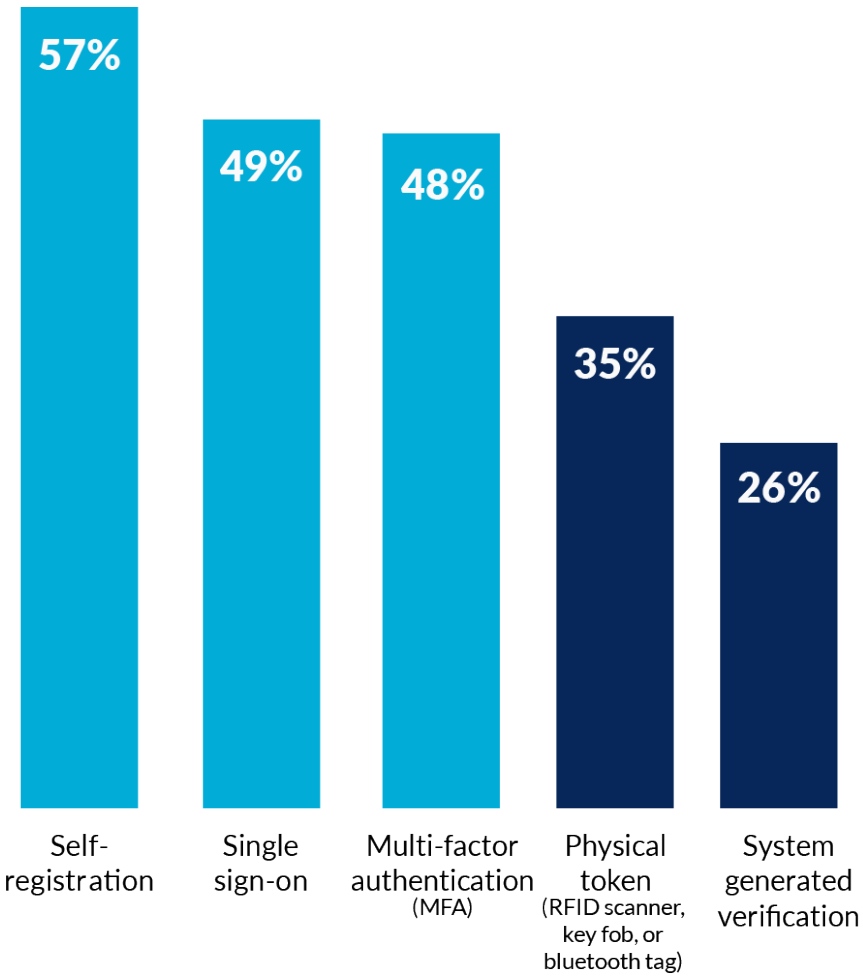
Source: State of Email Encryption, Gartner Peer Insights, Nov 2022

As more industries, more verticals and more departments continue their digital migrations, so do the numbers of business cases for exchanging secure messages and documents. To meet a whole plethora of expanding user, jurisdictional and business demands, organizations look for email encryption to deliver for a multitude of use cases and enable a flexible approach to authentication to strengthen security, while improving usability.

HOW ARE PEOPLE AUTHENTICATING?

When asked how to best authenticate employees, customers, and partners, decision-makers agreed that their organizations need several options to do so. 57% of respondents said they want the capability of self-registration. In addition, 49% also noted single sign-on, and multi-factor authentication (48%) as top options for organizations.

Which of the following email authentication options does your organization use?



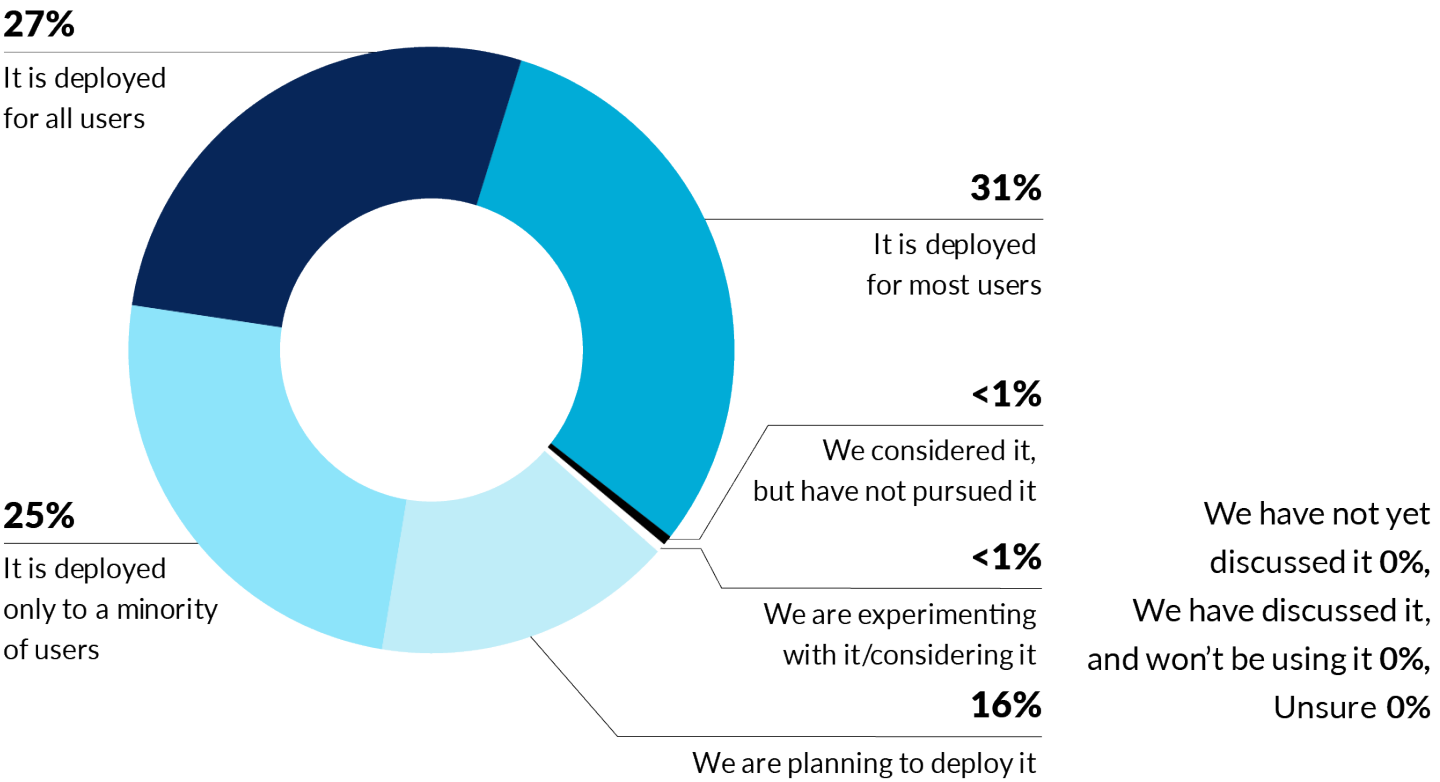
Source: State of Email Encryption, Gartner Peer Insights, Nov 2022

The emergence of streamlined authentication options is shaping the future of email encryption. By reducing authentication steps through biometrics and third-party logins, enterprises look to improve security and improve user experience.

MOST USING 2FA

When it comes to secure message access, the majority of organizations surveyed have deployed two-factor authentication, but in many of these organizations it is deployed only for a minority of users, as shown below. Less than 30% of organizations have two-factor authentication for all users. Most of the remaining organizations have deployed it to most (31%) or a minority of users (25%).

What is the deployment status of two-factor authentication in your organization?



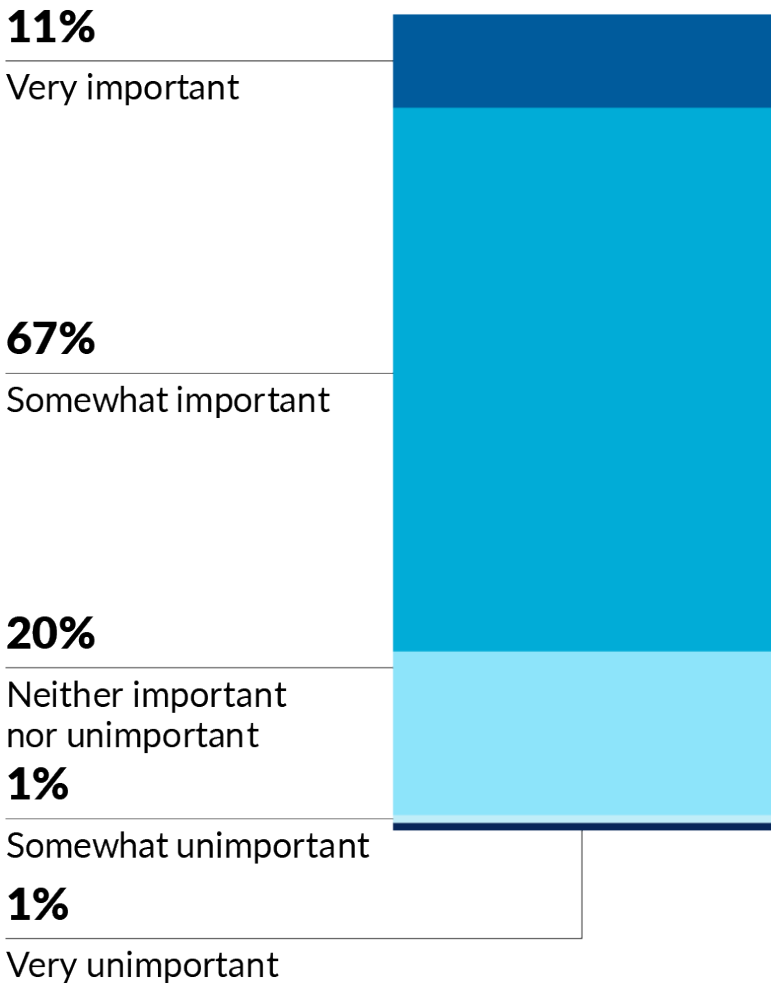
Source: State of Email Encryption, Gartner Peer Insights, Nov 2022

The vast majority of organizations have deployed two-factor authentication with the remaining 16% planning for the deployment of two-factor authentication but have not yet done so.

COMPANIES SEEK PRODUCT ROADMAPS

Almost 80% of respondents state that encryption feature roadmaps/updates are important to their organization.

How important is an encryption feature roadmap/updates to your organization?



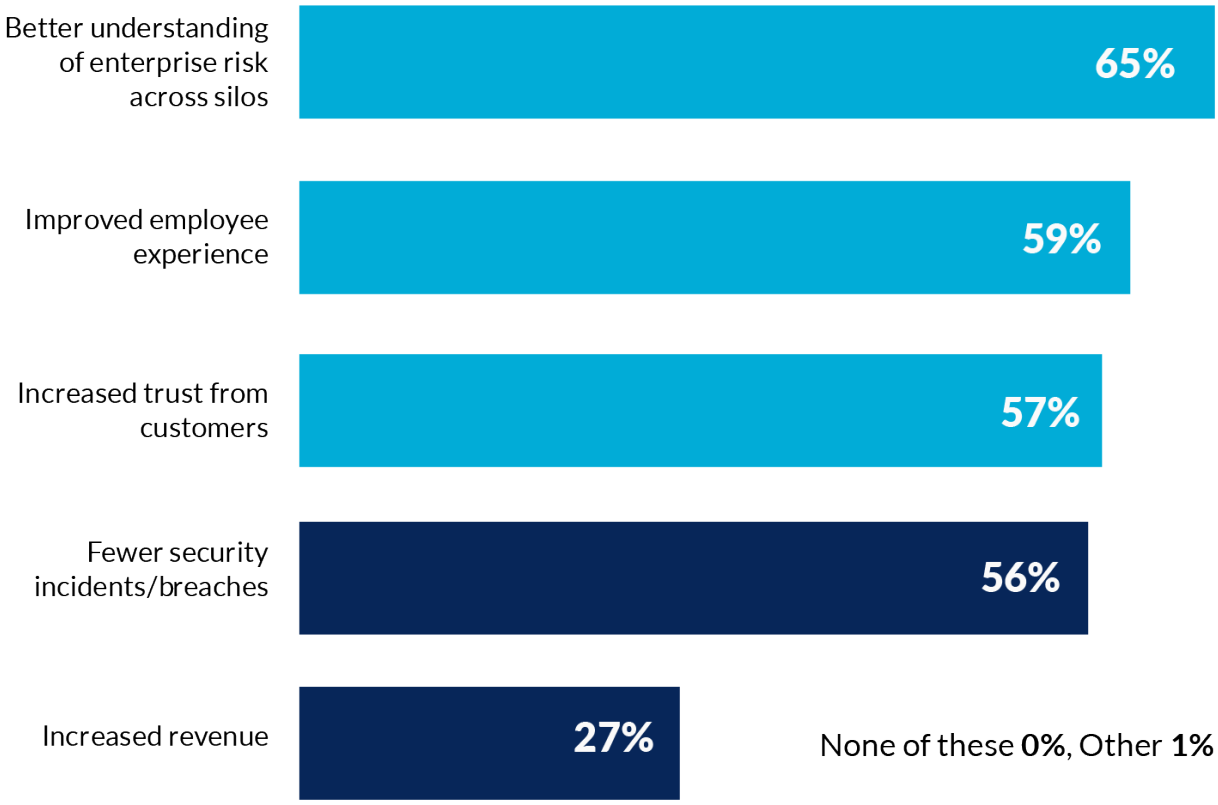
Source: State of Email Encryption, Gartner Peer Insights, Nov 2022

To meet demanding business requirements, the majority of organizations look to up-to-date product roadmaps for a commitment to the latest crypto and data protection standards to ensure the confidentiality of the messages and documents sent using email.

IMPROVING PROTECTION HAS ITS BENEFITS

Decision-makers recognize the many benefits to improving data protection capabilities - topping the list is a better understanding of enterprise risk across silos (65%). Organizations expect to drive security results by improving data protection capabilities, as 56% of decision-makers expect fewer security incidents/breaches. These security benefits not only improve employee experiences (59%), but also drive customer trust (57%).

What benefits do you anticipate from improving your organization's data protection capabilities?



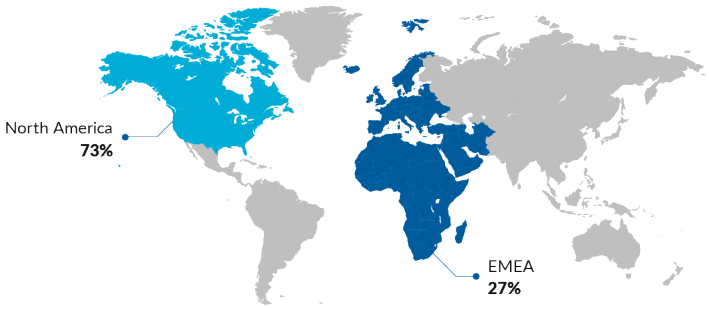
Source: Meeting Email Encryption Criteria, Gartner Peer Insights, Nov 2022

With just under a third of respondents expecting to increase revenue by improving their data protection capabilities, the ability to exchange email securely isn't just a matter of security – it's creating a competitive edge.

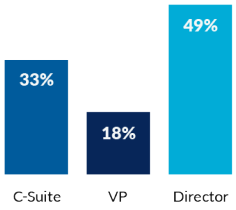
RESPONDENT BREAKDOWN

State of Email Encryption Survey

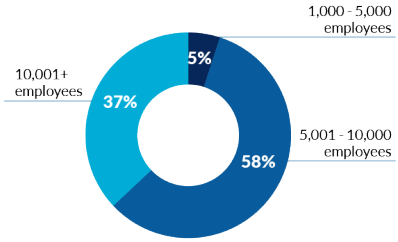
Region



Title

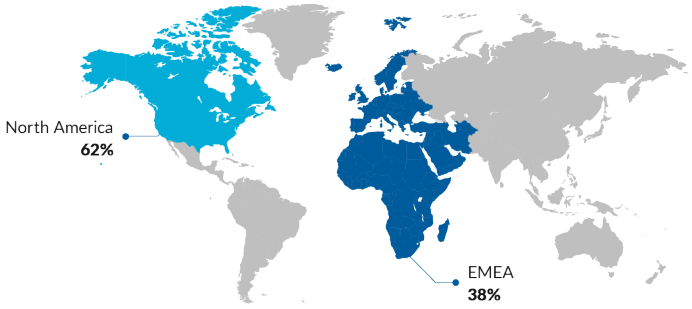


Company size

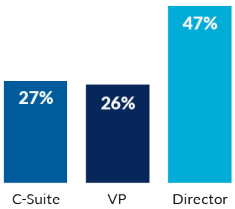


Email Encryption Criteria Survey

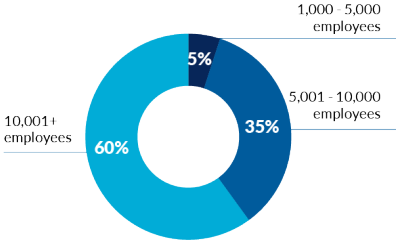
Region



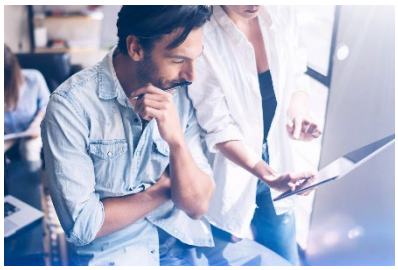
Title



Company size



TAKE THE NEXT STEPS



ESG Showcase

Enable innovative processes.

Learn more →

GigaOm Encryption Fit

Invest in the right solution.

Learn more →

Forrester Trends Study

Ensure adoption, drive results.

Learn more →

ABOUT ECHOWORX

Echoworx protects the privacy of people and businesses throughout the world by making email data protection easier. The cloud-based platform and SaaS delivery help transform communication chaos into order for world leading organizations who understand — it pays to be secure.

Echoworx focuses exclusively on providing organizations with secure email services. Adopted by the top and best in the business across more than 30 countries. It maintains a presence in prominent industries, including banking, insurance, healthcare, and government. Every security aspect runs through each required audit for AICPA/CICA WebTrust, SOC2, PCI, and FSQS. Other certifications include Microsoft and Apple Root Member. To learn more, visit Echoworx.com.

Gartner®

This content, which provides opinions and points of view expressed by users, does not represent the views of Gartner; Gartner neither endorses it nor makes any warranties about its accuracy or completeness.

Source: Gartner Peer Insights, State of Email Encryption 2022 survey and Meeting Email Encryption Criteria survey