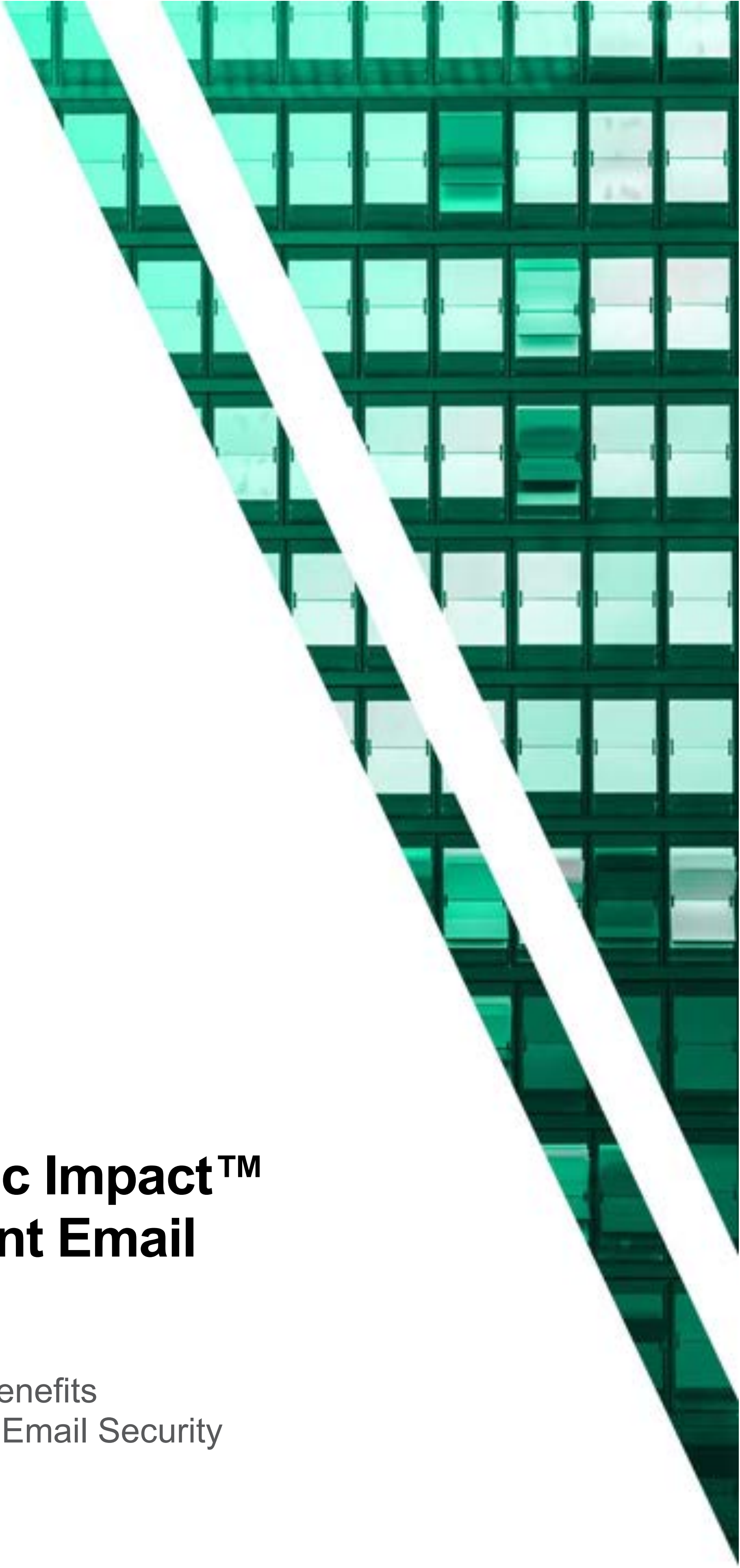
FORRESTER



The Total Economic Impact™ Of Egress Intelligent Email Security

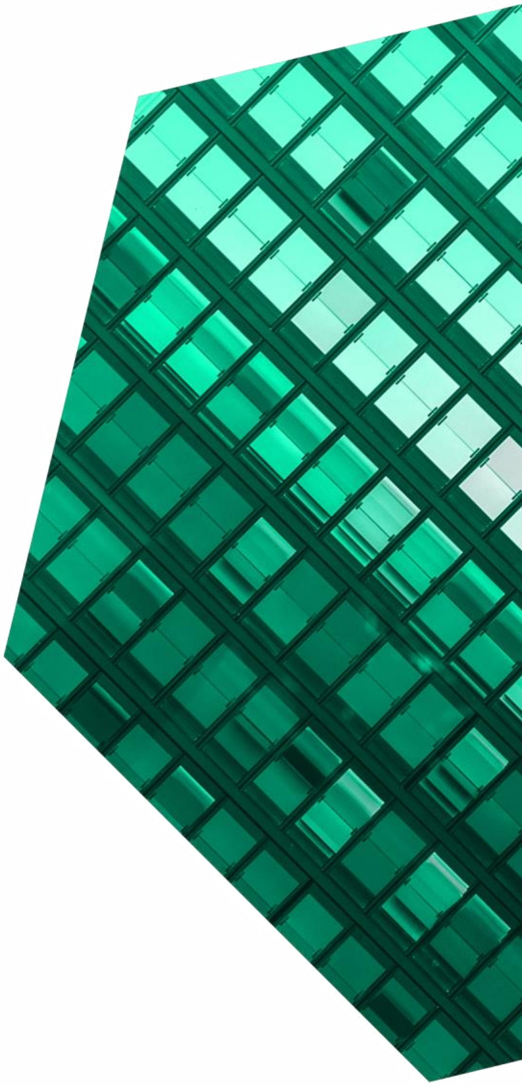
Cost Savings And Business Benefits
Enabled By Egress Intelligent Email Security

NOVEMBER 2023

A FORRESTER TOTAL ECONOMIC IMPACT™ STUDY COMMISSIONED BY EGRESS

Table Of Contents

Consulting Team: *Elina Bauwens*
Bharath Sivan



ABOUT FORRESTER CONSULTING

Forrester provides independent and objective research-based consulting to help leaders deliver key outcomes. Fueled by our customer-obsessed research, Forrester's seasoned consultants partner with leaders to execute their specific priorities using a unique engagement model that ensures lasting impact. For more information, visit forrester.com/consulting.

Executive Summary

Phishing and business email compromise are perennial problems for security leaders and professionals, with 36% of security decision-makers whose organization experienced an external attack naming phishing or social engineering as the source, according to Forrester's Security Survey, 2022.[1] Enterprise email security solutions to protect business communication and its ecosystem are evolving to enable trusted communication, block a major inroad for attackers, and protect end users from themselves.[2]

Egress Software Technologies provides an adaptive cloud email security platform that continuously assesses human risk and dynamically adapts policy controls, which prepares customers to defend their enterprises against advanced phishing attacks, outbound data loss, or exposure incidents. Egress integrates into Microsoft 365 to augment its native security capabilities and stop the inbound and outbound threats that secure email gateways (SEGs) miss while providing holistic email security reporting to surface organizational and human risk insights.

KEY STATISTICS

Return on investment (ROI)

359%

Net present value (NPV)

$4.58M

Egress Software Technologies Ltd. commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realize by deploying Egress Intelligent Email Security.[3] The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of Egress on their organizations.

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed four representatives with experience using Egress Intelligent Email Security. For the purposes of this study, Forrester aggregated the interviewees' experiences and combined the results into a single composite organization that is a global financial services organization with 9,000 mailboxes.

Prior to using Egress, the interviewees' organizations primarily depended on its endpoint protection solution and a combination of third-party software, such as secure email gateways, for threat protection and analysis. However, these solutions offered limited protection, which often led to phishing attacks, business email compromises, near-miss security incidents and additional auditing from their ecosystem partners. These limitations led the interviewees' organizations to pursue a solution that elevated the overall email security environment while retaining their existing Microsoft environment.

Egress Inbound Security Solution efficacy rate

98%

After the investment in Egress Intelligent Email Security, the interviewees' organizations were able to enhance protection against sophisticated attacks, identify and avoid breaches, prevent data loss incidents, and better monitor and analyze the email threat landscape. Key results from the investment included cost-effort avoidance related to the investigation and remediation of breaches, misdirections, and data loss incidents; productivity savings for IT security resources and end users from reduced managing and monitoring emails; and resource time savings from reduced threat analysis, reporting and auditing activities.

> **"In the past, we had a number of near misses that could have been prevented by some sort of outbound email protection, but no one could put their finger on how many there might have been. We were getting some reports, but the underlying feeling was there were more than what people admitted to."**
> *Head of information security, legal services*

KEY FINDINGS

Quantified benefits. Three-year, risk-adjusted present value (PV) quantified benefits for the composite organization include:

- **Savings of $2.9 million due to improved inbound email protection**. Egress Intelligent Email Security either blocks and automatically quarantines or neutralizes and prevents users from interacting with 98% of the 400,000 malicious incoming emails for the composite organization each year. This results in productivity savings for end users and IT security resource savings that amounts to $66,000 per year. The automatic quarantining of malicious emails also helps the composite organization reduce their spending on out-of-hours security operations center (SOC) costs year over year as Egress learns and improves. Egress's inbound protection also prevents the composite organization from facing 84 breaches each year. This helps it avoid $535,000 a year in costs associated with simple and material breaches. The additional time and cost savings amount to approximately $2.9 million for the composite organization over three years.
- **Savings of $2.7 million from enhanced outbound email protection.** Egress Intelligent Email Security prevents 2,300 misdirected emails per year for the composite. This saves significant investigation efforts by IT security resources that amounts to $1,100,000 per year. The composite organization's effort to remediate a misdirected incident is also reduced by 90%, leading to additional savings. Additionally, Egress protects the organization from 1,600 incidents that could have led to data loss. This adds to an additional savings of $913,000 associated with investigation and remediation efforts for data loss incidents. The additional time and cost savings amount to approximately $2,7 million for the composite organization over three years.

> **"[Since moving to Egress] I can't remember the last time there was an incident of a misdirected email."**
> *Head of information security, legal services*

- **Savings of $300,000 from reduced efforts in reporting, analysis, and audit.** Egress's dashboards and insights help reduce the time spent on creating security reports by 90%. The solution's insights on human risk additionally help the composite organization save 144 hours per year generating human risk analysis reports. Lastly, Egress helps the composite organization reallocate staff who were dedicated to working on answering security audit questions from partners and clients. This generates an additional savings of $121,000 per year. The additional time and cost savings amount to approximately $300,000 for the composite organization over three years.

> **"Our security program is driven not only by protecting our data and our customers' data but also by meeting our customers' security requirements."**
> *Head of information security, legal services*

Unquantified benefits. Benefits that provide value for the composite organization but are not quantified in this study include:

- An ability to utilize the existing Microsoft native tooling environment, thereby offering minimal disruption to the business environment.
- An elevated security culture and awareness within the organization from enhancing the visibility of email security risks.
- Targeted IT security training enabled by risk insights associated with user groups and individual users.
- A forensic narrative around the threat environment with dashboards and insights that offer better visibility of the email threat landscape.
- A better work-life balance for IT security team members with a reduced number of unexpected, malicious security incidents requiring emergency response.
- Reduced stress and higher work satisfaction with automated quarantining and intelligent intervention, which offers employees the ability to focus on higher value-add activities.
- A true partnership with Egress offering personalized support throughout the customer journey.

Costs. Three-year, risk-adjusted PV costs for the composite organization include:

- **Software license costs of $1.19 million.** Costs are based on the Defend and Prevent modules and the number of mailboxes protected.
- **Implementation and ongoing management costs of $84,000.** Deployment involves an initial proof of concept followed by roll-out and minimal on-going management.

The representative interviews and financial analysis found that a composite organization experiences benefits of $5.86 million over three years versus costs of $1.27 million, adding up to a net present value (NPV) of $4.58 million and an ROI of 359%.

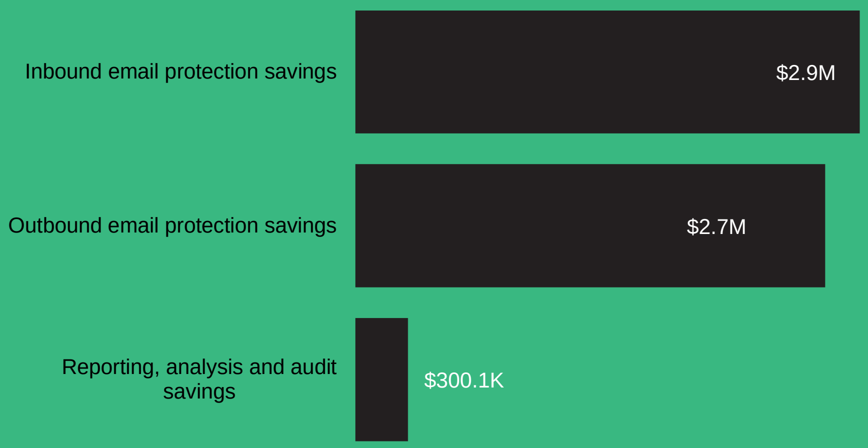
ROI
359%

BENEFITS PV
$5.86M

NPV
$4.58M

PAYBACK
<6 months

Benefits (Three-Year)



> **“The product is learning. It isn't a solution that just sits and does what it [always] has done. It actually learns about user behavior with the machine learning in it, so month over month we are seeing a reduction in breaches.”**

— Chief digital officer, healthcare services

TEI FRAMEWORK AND METHODOLOGY

From the information provided in the interviews, Forrester constructed a Total Economic Impact™ framework for those organizations considering an investment in Egress Intelligent Email Security.

The objective of the framework is to identify the cost, benefit, flexibility, and risk factors that affect the investment decision. Forrester took a multistep approach to evaluate the impact that Egress Intelligent Email Security can have on an organization.

DUE DILIGENCE

Interviewed Egress stakeholders and Forrester analysts to gather data relative to Egress Intelligent Email Security.

INTERVIEWS

Interviewed four representatives at organizations using Egress Intelligent Email Security to obtain data with respect to costs, benefits, and risks.

COMPOSITE ORGANIZATION

Designed a composite organization based on characteristics of the interviewees' organizations.

FINANCIAL MODEL FRAMEWORK

Constructed a financial model representative of the interviews using the TEI methodology and risk-adjusted the financial model based on issues and concerns of the interviewees.

CASE STUDY

Employed four fundamental elements of TEI in modeling the investment impact: benefits, costs, flexibility, and risks. Given the increasing sophistication of ROI analyzes related to IT investments, Forrester's TEI methodology provides a complete picture of the total economic impact of purchase decisions. Please see Appendix A for additional information on the TEI methodology.

DISCLOSURES

Readers should be aware of the following:

This study is commissioned by Egress and delivered by Forrester Consulting. It is not meant to be used as a competitive analysis.

Forrester makes no assumptions as to the potential ROI that other organizations will receive. Forrester strongly advises that readers use their own estimates within the framework provided in the study to determine the appropriateness of an investment in Egress Intelligent Email Security.

Egress reviewed and provided feedback to Forrester, but Forrester maintains editorial control over the study and its findings and does not accept changes to the study that contradict Forrester's findings or obscure the meaning of the study.

Egress provided the customer names for the interviews but did not participate in the interviews.

The Egress Intelligent Email Security Customer Journey

🟩 Drivers leading to the Egress Intelligent Email Security investment

Interviews

Role	Industry	Region	Employees	Revenue
VP of global IT security	Financial services	Global	12,000	$1.8B
Head of information security	Legal services	Global	6,000	$2.4B
Chief digital officer	Healthcare services	United Kingdom	7,000	$394M
Head of information security	Legal services	Global	3,500	$613M

KEY CHALLENGES

Prior to using Egress Intelligent Email Security, the interviewees' organizations primarily depended on Microsoft Defender Endpoint security and a combination of third-party software for threat protection, data-loss protection, and analysis for their business communications.

The interviewees noted how their organizations struggled with common challenges, including:

- **Phishing attacks and near-miss security incidents.** The interviewees' organizations faced numerous phishing attacks that slipped through the native email security platform or past their additional third-party security software. The organizations spent significant effort to educate users on identifying phishing emails but found that sophisticated phishing attacks were still missed and security was compromised due to the ever-evolving threat landscape. In addition, they also identified several near misses through malicious operations (MalOps) and business email compromise (BEC) incidents. This environment resulted in lots of overhead to monitor and investigate suspicious emails.

- **Investigations from clients on security environment.** Due to the highly regulated industries that the interviewees' organizations worked in and the sensitivity of the data they handled, their customers and partners had high expectations for their level of email security, especially in relation to data loss protection standards and quarantining methods. Providing proof of their organization's email security posture was time consuming and often required additional follow-up discussions with the customers and partners to alleviate their concerns.

- **Misdirected emails resulting in data loss.** The interviewees' organizations were concerned about the possibility of losing sensitive customer data through accidentally misdirected emails but had little visibility into how often this was happening and the impact of the incidents. They had a feeling that email misdirections were often

> **"Before we had the technology, we were always doing forensic analysis from a hunch….we are now much more straight to the point."**
>
> *Chief digital officer, healthcare services*

not reported to the right internal authorities but had little proof to confirm this. The risk to reputations was high, and the interviewees' organizations were also concerned with potential loss of business and/or regulatory fines.

> **"We were taken with the simplicity of the installation [for inbound messages]. When we started to look at the solution, it kind of works out of the box. It does what it says, and it is not hard to figure out."**
>
> *Chief digital officer, healthcare services*

SOLUTION REQUIREMENTS

The interviewees' organizations searched for a solution that could:

- Elevate their overall email security environment while retaining the Microsoft environment.
- Enhance their ability to meet security requirements and standards set by their partners and clients.
- Be tested before purchasing and deployed easily and with minimal disruption to business as usual.
- Had a positive reputation and footprint in their industry.
- Be seen as a true partner, not just a transactional vendor.

COMPOSITE ORGANIZATION

Based on the interviews, Forrester constructed a TEI framework, a composite company, and an ROI analysis that illustrates the areas financially affected. The composite organization is representative of the four interviewees, and it is used to present the aggregate financial analysis in the next section. The composite organization has the following characteristics:

Description of composite. It is a global financial services organization with 9,000 individual and group mailboxes and 200 staff members working in IT. It also has an annual email volume of approximately 30 million inbound emails and 13 million outbound emails. The user's email contents often include sensitive client information, personally identifiable information (PII) and critical business data, and can be time sensitive. The composite organization deploys Egress Inbound Email Security, Defend, in Year 1, and continues with the deployment of Egress Outbound Email Security, Prevent, in Year 2.

Key Assumptions

- Global financial services organization
- 9000 mailboxes
- 35M annual inbound emails
- 13M annual outbound emails
- Deploys Egress Inbound solution in Year 1
- Deploys Egress Outbound solution from Year 2

Analysis Of Benefits

🟩 Quantified benefit data as applied to the composite

Total Benefits

Ref.	Benefit	Year 1	Year 2	Year 3	Total	Present Value
Atr	Inbound email protection savings	$1,108,202	$1,162,724	$1,210,046	$3,480,973	$2,877,512
Btr	Outbound email protection savings	$0	$1,698,889	$1,698,889	$3,397,778	$2,680,441
Ctr	Reporting, analysis, and audit savings	$120,668	$120,668	$120,668	$362,003	$300,083
	Total benefits (risk-adjusted)	$1,228,870	$2,982,281	$3,029,603	$7,240,754	$5,858,036

INBOUND EMAIL PROTECTION SAVINGS

Evidence and data. Egress's inbound email security solution uses self-adapting, machine-learning-based technology to detect and flag malicious emails. The VP of global IT security at a financial services organization explained that their organization experienced a 98% efficacy rate against malicious inbound emails. This significantly reduced the number of malicious emails that reached user inboxes and offered significant productivity savings for IT security staff who monitored the malicious emails reported by end users. End users also reduced the time they previously spent verifying the legitimacy of emails.

> **"The user behavior is much more attuned to the banners. When you get the amber or red banner, people certainly start to pay attention."**
> *Chief digital officer, healthcare services*

In addition to this, Egress also offers automatic quarantining of suspicious email. The chief digital officer of a healthcare services provider mentioned that this capability helped their organization cut down its out-of-hours SOC costs by 25% in the first year alone, and they expected more savings as the solution continued to learn and enhance.

The solution was also able to reduce the number of breaches — both simple and sophisticated — experienced by customers. One of the customers interviewed mentioned the number of breaches went down from five to 10 per month to one to two per month since Egress was introduced. This led to significant savings around the investigation and remediation of such incidents.

Modeling and assumptions. Forrester estimates the following for the composite organization:

- The composite organization experiences 35 million inbound emails per year. Of those emails, 400,000 are suspicious and end up in users' mailboxes, slipping past native email security systems.
- The organization experiences an efficacy rate of 98% with Egress's inbound email protection solution.

- End users spend 2.5 minutes per email verifying its legitimacy.
- IT security resources spend an average of 20 minutes investigating a suspicious email reported by the end users.
- The composite organization experienced 84 breaches annually with its previous solution — 98% of which were simple breaches and 2% of which were material breaches.
- The cost of investigating and mitigating breaches amount to $5,000 for a simple breach and $175,000 for a material breach.
- The additional costs around fines and the loss of business involved with material breaches are exempted from this study as the interviewed customers did not experience these. However, Forrester's research indicates that these additional cost areas average approximately $650,000 per breach and are costs that the reader could consider (see Figure 1 for more details).

Risks. Efficiency gains are dependent on:

- The size and setup of the IT organization and the effort involved to review or investigate reported emails.
- The volume of suspicious emails an organization receives and number of breaches experienced can vary largely depending on the industry or organization.
- The size and nature of breaches, the type of data that was compromised, and the industry an organization operates in.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $2.9 million.

Figure 1

Additional costs associated with material breach not considered in the study.

According to Forrester's research, the average costs of response and notification, fines, damages, compliance costs, and customer compensation per material breach can amount to **$269,550.***

In addition to this, Forrester estimates, the average lost business revenues and additional costs to acquire customers per material breach could amount to an additional **$385,296** per breach.*

These additional costs typically associated with a material breach are not considered in this study as none of the interviewed customers experienced a material breach resulting in these additional expenses.

*"Forrester Consulting Cost of a Cybersecurity Breach Survey," Forrester Research, Inc., February 2021.

Inbound Email Protection Savings

Ref.	Metric	Source	Year 1	Year 2	Year 3
A1	Volume of inbound emails	Composite	35,000,000	35,000,000	35,000,000
A2	Volume of suspicious emails passing through	Interview	400,000	400,000	400,000
A3	Percentage reduction in suspicious emails received by end user	Interview	98%	98%	98%
A4	Average time spent by end user in reviewing email	Interview	0.04	0.04	0.04
A5	Average fully burdened FTE salary	TEI standard	$38	$38	$38
A6	Subtotal: End-user time savings	A2*A3*A4*A5	$625,632	$625,632	$625,632
A7	Volume of suspicious emails reported to IT Security team	2%*A2	3200	3200	3200
A8	Average time spent by security FTE investigating emails	Interview	0.33	0.33	0.33
A9	Percentage of effort saved	Interview	50%	50%	50%
A10	Average fully burdened salary of IT security FTE	TEI standard	$58	$58	$58
A11	**Subtotal: Security FTE productivity savings**	**A7*A8*A9*A10**	**$30,624**	**$30,624**	**$30,624**
A12	SOC out of hours contract fee	Interview	$160,000	$160,000	$160,000
A13	Reduction in out of hours contract fee due to automatic quarantining	Interview	25%	50%	70%
A14	Subtotal: Savings in out-of-hours SOC time reduction	A12*A13	$40,000	$80,000	$112,000
A15	Subtotal: Savings in security administration	A11+A14	$70,624	$110,624	$142,624
A16	Amount of breaches from inbound emails experienced annually	Interview	84	84	84
A17	Percentage of simple breaches	Assumption	98%	98%	98%
A18	Average cost of remediation for simple breach	Interview	$5,000	$5,000	$5,000
A19	Percentage reduction in simple breaches	Interview	80%	85%	90%
A20	**Avoided costs associated with simple breach**	**A16*A17*A18*A19**	**$329,280**	**$349,860**	**$370,440**
A21	Percentage of material breaches	Assumption	2%	2%	2%
A22	Percentage reduction in material breaches	Interview	70%	70%	70%
A23	Average cost of remediation and reporting labor cost per material breach	Interview	$175,000	$175,000	$175,000
A24	**Avoided costs associated with material breach**	**A16*A21*A22*A23**	**$205,800**	**$205,800**	**$205,800**
A25	Subtotal: Avoided costs associated with breach prevention	A20+A24	$535,080	$555,660	$576,240
At	Inbound email protection savings	A6+A15+A25	$1,231,336	$1,291,916	$1,344,496
	Risk adjustment	↓10%			
Atr	Inbound email protection savings (risk-adjusted)		$1,108,202	$1,162,724	$1,210,046
Three-year total: $3,480,973			**Three-year present value: $2,877,512**		

OUTBOUND EMAIL PROTECTION SAVINGS

Evidence and data. Egress’s outbound email protection solution used social graph and contextual machine learning technologies to model user behavior at the interviewees’ organizations. The solution then offered real-time advice to prevent user errors such as wrong attachments, misdirections, and data loss risks with outbound emails. The head of information security for a legal services organization mentioned that the organization experienced up to 1,500 instances of accidental misdirections per year, with three to four serious incidents per year. Some of these incidents required hours to remediate and rectify, which had an adverse effect on end-user productivity. These have now been avoided with Egress.

Another area of significant importance for interviewed customers was Egress's ability to prevent data loss incidents. One of the interviewees highlighted that in one quarter alone, Egress's content analysis capability helped them prevent 250 instances of accidental data loss as the solution identified issues and suggested corrections to email content to prevent incidents. The customer also shared a material data loss of this nature would result in work for an average of five days from a team of multiple resources across legal, compliance, human resources, and other concerned teams to manage and remediate the incident. With Egress, the organization could now avoid these costs.

> **“There were potentially 1,500 emails that were misdirected yearly. It only takes one or two of those to be quite serious [to have an effect] our reputation.”**
> *Head of information security, legal services*

Modeling and assumptions. Forrester estimates the following for the composite organization:

- The composite organization generates 13 million outbound emails per year.
- The composite organization faces 2,300 instances of potential misdirections that require an average of 8 hours for IT security resources to investigate.
- Yearly, the composite organization also faces five misdirection incidents. The investigations that followed require an average of 72 hours of remediation efforts to rectify the misdirection.
- The composite organization also faces 1,600 potential data loss instances a year that the Egress solution identified and corrected through content analysis.
- Efforts to remediate simple data loss is 4 hours per incident. The effort to remediate material data loss is 200 hours per incident and involves multiple resources from various teams.

Risks. Efficiency gains are dependent on:

- The complexity of processes involved in the organization to review or investigate misdirected emails.
- The volume of misdirected emails and data loss incidents experienced can vary largely depending on the industry or organization.
- The size and nature of breaches and the type of data exposed will impact the effort involved in remediation of data loss incidents.

Results. To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV of $2.7 million.

Outbound Email Protection Savings

Ref.	Metric	Source	Year 1	Year 2	Year 3
B1	Total volume of outbound emails per year	Composite	0	13,000,000	13,000,000
B2	Volume of potential misdirected emails per year	0.02% of B1	0	2,300	2,300
B3	Investigation efforts per misdirected email (hours)	Interview	0	8	8
B4	Fully loaded hourly rate for IT security staff	TEI standard	0	$58	$58
B5	Subtotal: Savings in misdirected email investigation	B2*B3*B4	$0	$1,067,200	$1,067,200
B6	Misdirected email incidents per year	Interview	0	5	5
B7	Time spent to remediate misdirected email incident	Interview	0	72	72
B8	Percentage reduction in misdirected email remediation	Interview	0	90%	90%
B9	Subtotal: Savings in misdirected email incident remediation	B6*B7*B8*B4	$0	$18,792	$18,792
B10	Volume of potential data loss events prevented by Egress	Interview	0	1,600	1,600
B11	Percentage of simple data loss incidents	Assumption	0	99%	99%
B12	Remediation efforts per simple data loss incident (hours)	Interview	0	4	4
B13	Average fully loaded salary of data loss remediation team	TEI standard	$0	$99	$99
B14	Percentage reduction in data loss events	Interview	0	95%	95%
B15	Subtotal: Avoided data loss remediation costs for simple incidents	B10*B11*B12*B13*B14	$0	$595,901	$595,901
B16	Percentage of material data loss incidents	Assumption	0	1%	1%
B17	Remediation efforts per material data loss incident (hours)	Interview	0	200	200
B18	Subtotal: Avoided data loss remediation costs for material incidents	B10*B13*B16*B17	$0	$316,800	$316,800
B19	Subtotal: Avoided data loss remediation costs	B15+B19	$0	$912,701	$912,701
Bt	Outbound email protection savings	B5+B8+B14	$0	$1,998,693	$1,998,693
	Risk adjustment	↓15%			
Btr	Outbound email protection savings (risk-adjusted)		$0	$1,698,889	$1,698,889
Three-year total: $3,397,778			**Three-year present value: $2,680,441**		

REPORTING, ANALYSIS, AND AUDIT SAVINGS

Evidence and data. The reporting and analysis capabilities offered by Egress allowed the interviewees' organizations to analyze the threat landscape easier with customizable dynamic dashboards and metrics. The chief digital officer of a healthcare organization stated that the dashboard offered metrics and statistics that helped their organization publish internal reports, which saved up to 4 hours of effort per report.

Egress also offered insights that helped quantify human risk and offered significant time savings. The VP of global IT security of a financial services organization mentioned that their organization used to spend up to 12 hours per report to collate necessary data and generate actionable insights into human risk which is now reduced to 4 hours with the help of Egress's insights.

Another key benefit interviewees highlighted was their organizations' ability to save time and effort associated with answering security audit questions. The head of information security of a legal services organization stated that their organization used to have a dedicated FTE to provide responses to security audits mandated by their customers. After investment in Egress, the organization was able to elevate its overall security environment to meet higher levels of security compliance to the point where they could repurpose the resource for other value-add activities.

Modeling and assumptions. Forrester estimates the following for the composite organization:

- The composite organization spends an average of 4 hours a month generating security reports for internal reporting and presentations in its previous environment. This is reduced by 90% with Egress Intelligent Email Security.

> **"Egress reporting is a zillion times better than what we had before. In the past, it was just through word of mouth that [we found a] user had done something wrong, and we then had to go manually to investigate it.**
> **"Now it is all in the portal and we can drill down and see exactly what the user did, what they ignored in terms of flags, etc."**
> *Head of information security, legal services*

- IT security resources spend an average of 12 hours a month developing human risk analysis reports in its previous environment. This is reduced by 60% with Egress.
- The composite organization has a dedicated resource to answer security audit questionnaires with a fully loaded salary of $120,640.

Risks. Efficiency gains for this benefit are dependent on:

- The reporting and audit needs of the industry that the organization operates in.
- The availability, use, and integration of external third-party software will impact the benefits of the human risk analysis.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $300,000.

Reporting, Analysis, And Audit Savings

Ref.	Metric	Source	Year 1	Year 2	Year 3
C1	Time spent on creating reports in the past per year	Interview	48	48	48
C2	Percentage of time saved	Interview	90%	90%	90%
C3	Fully loaded hourly CISO salary	TEI standard	$195	$195	$195
C4	Subtotal: Time savings in report creation	C1*C2*C3	$8,424	$8,424	$8,424
C5	Time spent in creating human risk analysis report (hours/year)	Interview	144	144	144
C6	Percentage of time saved	Interview	60%	60%	60%
C7	Fully loaded hourly IT security staff	TEI standard	$58	$58	$58
C8	Subtotal: Time savings in human risk analysis	C5*C6*C7	$5,011	$5,011	$5,011
C9	Reallocated resources for answering security audit question from clients/partners (FTE)	Interview	1	1	1
C10	Average fully loaded salary of IT security FTE	TEI standard	$120,640	$120,640	$120,640
C11	Subtotal: Savings in answering security audit questions	C9*C10	$120,640	$120,640	$120,640
Ct	Reporting, analysis, and audit savings	C4+C8+C11	$134,075	$134,075	$134,075
	Risk adjustment	↓10%			
Ctr	Reporting, analysis, and audit savings (risk-adjusted)		$120,668	$120,668	$120,668

Three-year total: $362,003 **Three-year present value: $300,083**

UNQUANTIFIED BENEFITS

Interviewees mentioned the following additional benefits that their organizations experienced but were not able to quantify:

- **Ability to utilize existing Microsoft-native tooling environment.** Egress's email security solutions can be seamlessly integrated into Microsoft 365, augmenting and enhancing its native security environment with minimal friction. This was particularly important to the interviewed customers whose organizations wanted to achieve faster deployments with minimal disruption.

- **Elevated security culture and awareness.** The interviewees' organizations found that their staff was more security aware and understanding of the risks involved in email security thanks to the in-the-moment notifications and detailed explanations of the security risks involved. This also helped them be more security aware in their personal lives. The visibility of the risks associated with email security also supported the security leadership's discussions with other senior management and board members about the importance of investing in security.

- **Targeted IT security training.** With the human risk score analysis from Egress, the organizations were able to clearly identify which individuals were at higher risk to specific types of phishing and could adjust their training accordingly.

- **Forensic narrative around threat environment.** Egress's dashboards offer detailed insights around threats and users, as well as actionable advice that helps organizations accelerate investigation into and management of their threat environment.

- **Better work-life balance.** The chief digital officer in healthcare noted that they got calls daily after working hours about incidents in the past. Now it rarely happens, which enables them to have a better work-life balance.

> **"Nearly every evening (in the past) I would get a phone call from our security team. Now my phone doesn't ring very often. And when it does, it's normally to advise me that something got in and they've caught it, rather than asking for help.**
>
> **"For me there has been a dramatic improvement on my work life balance. ... It makes me sleep better."**
>
> *Chief digital officer, healthcare services*

> **"What I used to get was a lot of forensic narrative. Now I get a very simple, effective report that really calls out what's in the Egress standard data set and what they have caught. It's very intuitive and easy to view and I can drill through very easily into the details."**
>
> *Chief digital officer, healthcare services*

- **Reduced stress and higher work satisfaction.** IT security workers had less stress knowing that Egress Intelligent Email Security was disabling malicious links, quarantining more emails, and catching incidents earlier in the workflow. This resulted in employees being able to focus on more meaningful work and higher work satisfaction.
- **True partnership with Egress.** The interviewees' organizations felt that Egress provided very personalized support to them throughout implementation and in regular operations. Interviewees noted how Egress acted as a true partner and not just a transactional vendor.

> **"[Egress] has been good to work with. They are in it for the long game. They understand companies like us."**
>
> *Head of information security, legal services*

> **"Partnering behavior [Egress] shared with us was the rational why we went ahead with them. Once we decided to hire them, the intimacy of the relationship was even higher."**
>
> *Chief digital officer, healthcare services*

FLEXIBILITY

The value of flexibility is unique to each customer. There are multiple scenarios in which a customer might implement Egress Intelligent Email Security and later realize additional uses and business opportunities, including:

- **Preparedness for future security risks**. The interviewees' organizations felt that they were ahead of technology threats with Egress' support and they were now able to react faster to the changing threat landscape.
- **Ability to attract more customers.** As many of the interviewees' organizations' customers required specific email security and data loss protection, having these in place enabled these organizations to do business with other similar groups.

Flexibility would also be quantified when evaluated as part of a specific project (described in more detail in Appendix A).

> **"It was becoming increasingly difficult to answer those [auditing] questions. So I could see a point where we wouldn't have continued to win business from some of those clients if we didn't have [Egress] in place."**
> *Head of information security, legal services*

Analysis Of Costs

Quantified cost data as applied to the composite

Total Costs

Ref.	Cost	Initial	Year 1	Year 2	Year 3	Total	Present Value
Dtr	Subtotal: Software license fees	$0	$292,950	$585,900	$585,900	$1,464,750	$1,190,728
Etr	Implementation and ongoing management costs	$5,104	$3,381	$61,248	$33,814	$103,547	$84,201
	Total costs (risk-adjusted)	$5,104	$296,331	$647,148	$619,714	$1,568,297	$1,274,929

SOFTWARE LICENSE FEES

Evidence and data. The primary costs associated with Egress Intelligent Email Security for the interviewees' organizations were software license fees.

Modeling and assumptions. The license fees presented in this financial model were provided by interviewed decision-makers and adjusted to the composite organization's characteristics and deployment approach. It leverages inbound protection, or Defend, in Year 1 and expands the use to outbound protection, or Prevent, in Year 2.

Risks. This cost may vary based on an organization's regions, the number of inboxes protected, the type of modules deployed, packaging, exchange rates, and change over time.

Results. To account for these risks, Forrester adjusted this cost upward by 5%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $1.19 million.

Software License Fees

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
D1	Software license fees	Interview	$0	$279,000	$558,000	$558,000
Dt	Software license fees	D1	$0	$279,000	$558,000	$558,000
	Risk adjustment	↑5%				
Dtr	Software license fees (risk-adjusted)		$0	$292,950	$585,900	$585,900
	Three-year total: $1,464,750			Three-year present value: $1,190,728		

IMPLEMENTATION AND ONGOING MANAGEMENT COSTS

Evidence and data. Egress's inbound security solution integrated transparently into Microsoft 365 via SMTP and Graph APIs at the interviewees' organizations. Installation was executed with a deployment packager that created necessary groups, app registrations, connectors and mail flow rules required to complete the set up. Deployment could be staggered by group, geography, and organizational unit. Implementation of the outbound solution was also seamless for the interviewees' organizations. The solution digested user emailing patterns silently during the initial implementation and used intelligent ML/AI to create its rules. It also offered additional customization around rule setting for the organizations' needs.

Interviewees were positively surprised by how simple the tool's implementation was, especially for the inbound email security solution. They started with a proof of capability (POC) phase without a requirement to purchase the solution. That lasted two to three weeks for inbound and a couple of months for the outbound solution. During this time, the organizations' teams did phased testing, analysis, checked for false positives, created playbooks for the SOC teams, and created custom rules before a phased roll out to the full organization. The ongoing management for the solution was minimal after deployment. The interviewees' organizations commented on the dedicated support that Egress provided both during the POC phase and after implementation.

Modeling and assumptions. For the composite organization, Forrester assumes:

- The implementation effort for inbound solution totals 80 hours during a three-month period.
- The implementation effort for the outbound solution totals approximately 21 hours a week across multiple FTEs over a five-month period.
- The ongoing effort for the inbound solution is minimal. The effort for the outbound solution remains small, but it increases to roughly half an FTE a month to fine tune the solution, create custom rules, etc.

Risks. Actual implementation and ongoing management costs may vary and can depend upon:

- The modules being deployed.
- The complexity of the security environment and internal requirements for security and governance.
- The level of customization needed.

Results. To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV of $84,000.

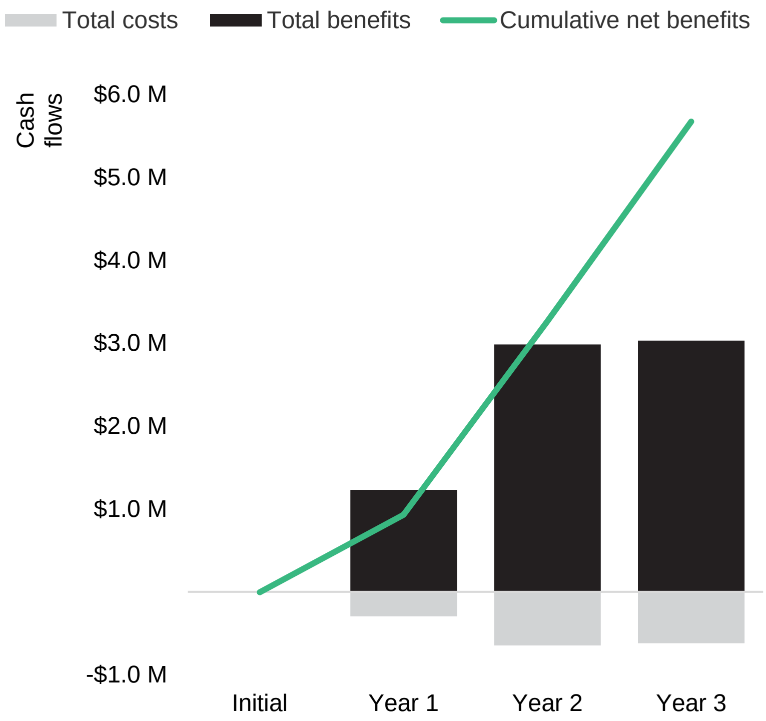
Implementation And Ongoing Management Costs

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
E1	Fully loaded hourly IT security staff	TEI standard	$58	$58	$58	$58
E2	Time spent on inbound implementation (hours)	Interview	80	0	0	0
E3	Subtotal: Inbound implementation costs	E1*E2	$4,640	$0	$0	$0
E4	Time spent on outbound implementation (hours)	Interview	0	0	430	0
E5	Subtotal: Outbound implementation costs	E1*E14	$0	$0	$24,940	$0
E6	Time spent on ongoing management	Interview	0	53	530	530
E7	Subtotal: Ongoing management costs	E1*E6	0	$3,074	$30,740	$30,740
Et	Implementation and ongoing management costs	E3+E5+E7	$4,640	$3,074	$55,680	$30,740
	Risk adjustment	↑10%				
Etr	Implementation and ongoing management costs (risk-adjusted)		$5,104	$3,381	$61,248	$33,814
Three-year total: $103,547			**Three-year present value: $84,201**			

Financial Summary

CONSOLIDATED THREE-YEAR RISK-ADJUSTED METRICS

Cash Flow Chart (Risk-Adjusted)



The financial results calculated in the Benefits and Costs sections can be used to determine the ROI, NPV, and payback period for the composite organization's investment. Forrester assumes a yearly discount rate of 10% for this analysis.

These risk-adjusted ROI, NPV, and payback period values are determined by applying risk-adjustment factors to the unadjusted results in each Benefit and Cost section.

Cash Flow Analysis (Risk-Adjusted Estimates)

	Initial	Year 1	Year 2	Year 3	Total	Present Value
Total costs	($5,104)	($296,331)	($647,148)	($619,714)	($1,568,297)	($1,274,929)
Total benefits	$0	$1,228,870	$2,982,281	$3,029,603	$7,240,754	$5,858,036
Net benefits	($5,104)	$932,539	$2,335,133	$2,409,889	$5,672,457	$4,583,107
ROI						359%
Payback period (months)						<6

Appendix A: Total Economic Impact

Total Economic Impact is a methodology developed by Forrester Research that enhances a company's technology decision-making processes and assists vendors in communicating the value proposition of their products and services to clients. The TEI methodology helps companies demonstrate, justify, and realize the tangible value of IT initiatives to both senior management and other key business stakeholders.

TOTAL ECONOMIC IMPACT APPROACH

Benefits represent the value delivered to the business by the product. The TEI methodology places equal weight on the measure of benefits and the measure of costs, allowing for a full examination of the effect of the technology on the entire organization.

Costs consider all expenses necessary to deliver the proposed value, or benefits, of the product. The cost category within TEI captures incremental costs over the existing environment for ongoing costs associated with the solution.

Flexibility represents the strategic value that can be obtained for some future additional investment building on top of the initial investment already made. Having the ability to capture that benefit has a PV that can be estimated.

Risks measure the uncertainty of benefit and cost estimates given: 1) the likelihood that estimates will meet original projections and 2) the likelihood that estimates will be tracked over time. TEI risk factors are based on "triangular distribution."

The initial investment column contains costs incurred at "time 0" or at the beginning of Year 1 that are not discounted. All other cash flows are discounted using the discount rate at the end of the year. PV calculations are calculated for each total cost and benefit estimate. NPV calculations in the summary tables are the sum of the initial investment and the discounted cash flows in each year. Sums and present value calculations of the Total Benefits, Total Costs, and Cash Flow tables may not exactly add up, as some rounding may occur.

PRESENT VALUE (PV)

The present or current value of (discounted) cost and benefit estimates given at an interest rate (the discount rate). The PV of costs and benefits feed into the total NPV of cash flows.

NET PRESENT VALUE (NPV)

The present or current value of (discounted) future net cash flows given an interest rate (the discount rate). A positive project NPV normally indicates that the investment should be made unless other projects have higher NPVs.

RETURN ON INVESTMENT (ROI)

A project's expected return in percentage terms. ROI is calculated by dividing net benefits (benefits less costs) by costs.

DISCOUNT RATE

The interest rate used in cash flow analysis to take into account the time value of money. Organizations typically use discount rates between 8% and 16%.

PAYBACK PERIOD

The breakeven point for an investment. This is the point in time at which net benefits (benefits minus costs) equal initial investment or cost.

Appendix B: Endnotes

[1] Source: "The Enterprise Email Security Landscape, Q1 2023," Forrester Research, Inc., February 2023.

[2] Source: "The Forrester Wave™: Enterprise Email Security, Q2 2023," Forrester Research, Inc., June 2023.

[3] Source: Total Economic Impact is a methodology developed by Forrester Research that enhances a company's technology decision-making processes and assists vendors in communicating the value proposition of their products and services to clients. The TEI methodology helps companies demonstrate, justify, and realize the tangible value of IT initiatives to both senior management and other key business stakeholders.

FORRESTER®