egress

Preventing email data loss in Microsoft 365

Augmenting Microsoft 365's native security to minimize outbound email data loss

Inside the report

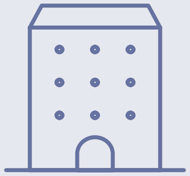
At a glance

Organizations must augment their existing Microsoft 365 architecture with additional intelligent data loss prevention technology to keep client and company data secure on email.

In the last 12 months...

85%

of organizations have had an outbound **email data breach**



67%

acknowledge an **increase in the number of incidents**

Remote employees were almost **twice as likely to accidentally leak data by email**

61%

of IT leaders say clients are asking whether they have **email DLP in place**

100%

of IT leaders are **frustrated by traditional static DLP rules**

A major problem for IT leaders is that traditional data loss prevention (DLP) tools alone aren't enough to mitigate all email data loss incidents

Introduction

Data loss is on every IT leader's mind. If they're not already dealing with the fallout of a breach, they're busy preventing future incidents. Especially when it comes to one of the most common and difficult to stop sources of data loss: outbound email.

A major problem for IT leaders is that traditional data loss prevention (DLP) tools alone aren't enough to mitigate all email data loss incidents.

With 200 million active users, Microsoft 365 is the go-to productivity platform and has seen major uptake since the COVID-19 pandemic. It's simple, easy-to-use and can boost efficiency across entire networks. And it does come with some security features. However, like all traditional email DLP tools there are security gaps that organizations need to augment.

Microsoft 365's native email DLP functionality uses static rules. On its own, this can help you to mitigate incidents that you can predict and to enforce policies across large user bases (for example, for the whole organization or departments). However, it's difficult to predict the unpredictable using static rules, such as the tired or stressed user who accidentally adds the wrong recipient because their name looks similar to the authorized recipient.

We've taken results from the 2021 Egress Data Loss Prevention Report looking at organizations using Microsoft 365, so we can help you identify risks and augment your email DLP strategy using the right security solutions. All research was conducted independently by Arlington Research on behalf of Egress, among 500 IT leaders and 3,000 remote workers across a variety of industries in both the UK and US.

Find out how both your own and your clients' data is put at risk via email – and what you can do to augment your email DLP strategy in Microsoft 365.

How often do users leak data by email?

The short answer is often! Our results show that 83% of businesses reported their data had been put at risk via email over the last 12 months.

Sensitive data was leaked via email in 85% of these organizations, and 15% had more than 500 incidents within the 12 months.

It's not simply the amount of breaches organizations are experiencing that's concerning – but the fact that the rate at which they're occurring appears to be increasing.

85% of employees have increased their reliance on email communications since the pandemic began. 80% say email is their preferred channel for sharing sensitive data.

More emails equals more risk. Added to this, three-quarters (73%) of employees say they feel more tired, stressed and under greater pressure since the pandemic began, increasing the chances of both accidental and intentional data loss.

It's not just the number of breaches that's concerning but also the rate they're occurring at is increasing

The impact of email data loss

The impacts of a breach can be serious. So it should be worrying that a huge 93% of IT leaders had reported a negative impact from email data breaches.

Breaches tie up a lot of internal resources. When the average email data breach takes ~60 hours to resolve, too many hours are wasted remediating them. We found that 37% of organizations had gone through internal remediation and investigation following an email data breach.

The impacts from client data being breached are even more concerning for IT leaders. Out of the surveyed organizations, 37% had experienced client churn as a direct result of an email data breach and 47% had suffered damage to their reputations.

It's also clear that clients are becoming increasingly aware of the need for their supplier organizations to enhance their email DLP strategies. 28% of the organizations we spoke to said that client data was the most likely type of data to be exposed via email, which has contributed to 61% of organizations being asked by clients if they have email DLP tools in place.

93% of organizations have experienced negative impacts from email data loss

Remote working and data loss

For many organizations, a year of remote working has only made the data loss situation worse. Remote workers during the pandemic have been more stressed, more tired, and under more pressure to be responsive out of hours. As all of us know, it's easier to make mistakes when we're stressed and tired – and using email is no exception.

77% of IT leaders believe mobile devices increase the risk of email data loss

IT leaders also share a lack of confidence around the security of employees working on devices such as mobiles and tablets. Remote workers have more ways to access emails than ever before – which is handy for the employees themselves. However, 77% of IT leaders believe remote workers are more likely to leak data from a mobile device versus a desktop.

Will these issues be mitigated once pandemic-related stress lowers and we see a partial return to the office? IT leaders are not so sure. 76% of them believe remote and hybrid working will make it harder to prevent email data loss in the future.

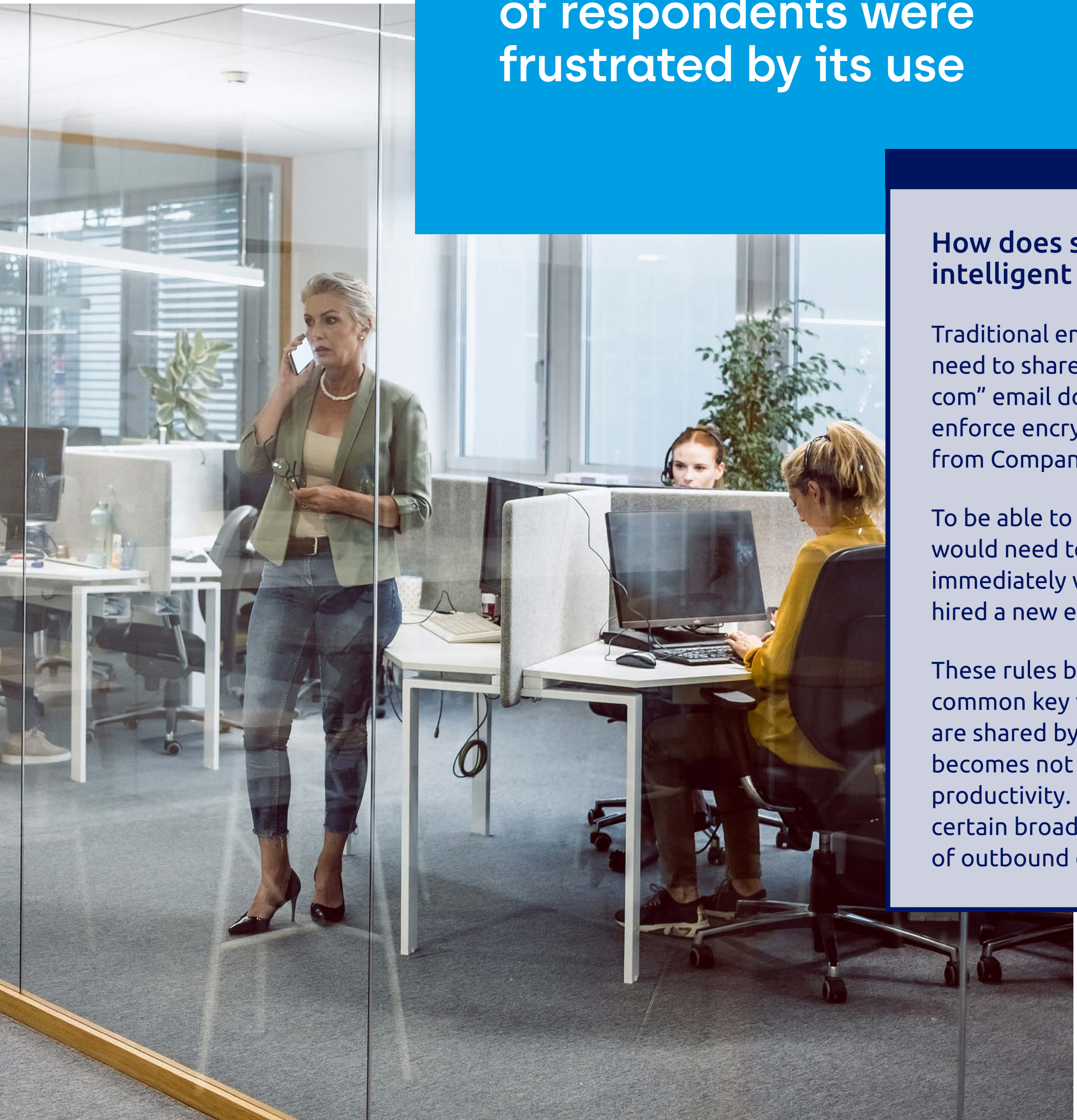
Limitations of static email DLP

Static DLP technologies can mitigate some email data loss incidents – but alone they're not enough to dynamically mitigate incidents in the way current email use requires. Out of the IT leaders we spoke to using static DLP, an incredible 100% of respondents were frustrated by its use. Every IT leader we spoke to was struggling with a similar set of issues.

When we got into the detail of their frustrations, 43% said that static DLP tools required a high level of admin to maintain and 26% said they created friction for their users. Because of these issues, 38% of IT leaders users had resorted to downgrading their rules to make them more workable.

In a particularly worrying statistic, 42% said that half of all incidents won't be detected by their static DLP tools. How can we trust tools that miss nearly half of all incidents? It's not simply a question organizations should ask themselves; it's on the minds of existing and prospective customers too.

Out of the IT leaders we spoke to using static DLP within Microsoft 365, an incredible 100% of respondents were frustrated by its use



How does static DLP work – and why do organizations need intelligent DLP too?

Traditional email DLP tools rely on static rules. For example, User A might need to share financial data with different contacts with "@companyB.com" email domains. Static rules can allow these emails to be sent and even enforce encryption, but they won't detect if User A has added the wrong user from Company B or, in most cases, attached the wrong document.

To be able to detect these types of breaches using static DLP, administrators would need to create high numbers of rules per employee and update them immediately when any circumstance changes. For example, if Company B hired a new employee who also needs to receive certain data.

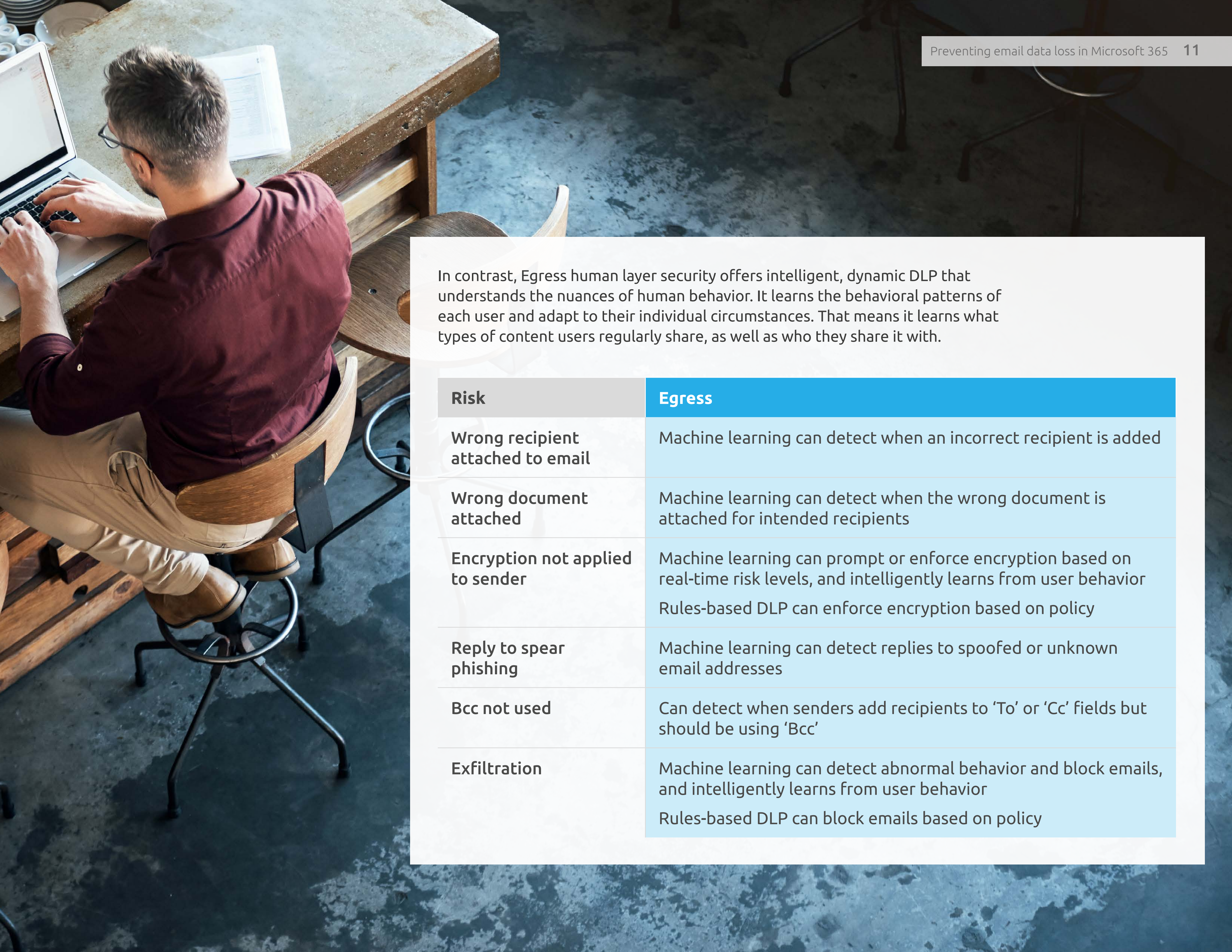
These rules become restrictive and unworkable, particularly when based on common key words - such as brand names that have a secondary meaning or are shared by more than one company. Very rapidly, static rules-based DLP becomes not only a significant administrative overhead but detrimental to productivity. So, organizations opt to not implement it or to only implement certain broad rules that are consequently unable to detect the vast majority of outbound email security incidents.

The solution

The problem with traditional approaches to email DLP is that human behavior (and mistakes) are context driven. Rigid rules can't predict what tired, stressed people working on mobile devices will do. That means some of the most common and easy ways for email breaches to occur aren't covered.

The majority of outbound email data breaches come from the most basic, everyday human errors. These are just some of the incidents that can slip through static DLP rules:

- **Adding the wrong recipient** (including through Microsoft Outlook autocomplete)
- **Attaching the wrong file or not removing data** (including hidden cells in Microsoft Excel)
- **Replying to spear phishing attacks**
- **Misuse of Bcc**



In contrast, Egress human layer security offers intelligent, dynamic DLP that understands the nuances of human behavior. It learns the behavioral patterns of each user and adapt to their individual circumstances. That means it learns what types of content users regularly share, as well as who they share it with.

Risk	Egress
Wrong recipient attached to email	Machine learning can detect when an incorrect recipient is added
Wrong document attached	Machine learning can detect when the wrong document is attached for intended recipients
Encryption not applied to sender	Machine learning can prompt or enforce encryption based on real-time risk levels, and intelligently learns from user behavior Rules-based DLP can enforce encryption based on policy
Reply to spear phishing	Machine learning can detect replies to spoofed or unknown email addresses
Bcc not used	Can detect when senders add recipients to ‘To’ or ‘Cc’ fields but should be using ‘Bcc’
Exfiltration	Machine learning can detect abnormal behavior and block emails, and intelligently learns from user behavior Rules-based DLP can block emails based on policy

What next for organizations using Microsoft 365?

Our findings have shown that outbound email data breaches are worryingly common and frequently have severe impacts. Remote working has only amplified these issues and looks set to set to continue for many organizations post-pandemic.

Organizations need to urgently examine their email DLP strategies and augment the static rules-based approach that's currently being implemented. The answer lies in an additional security layer that leverages intelligent DLP and uses contextual machine learning to mitigate the everyday human mistakes that do so much harm.

Egress Intelligent Email Security allows organizations to keep the productivity benefits of Microsoft 365, while augmenting its outbound email security functionality to reduce more risk and ensure your sensitive data remains secure.

Organizations need to augment their email DLP strategies using intelligent technology

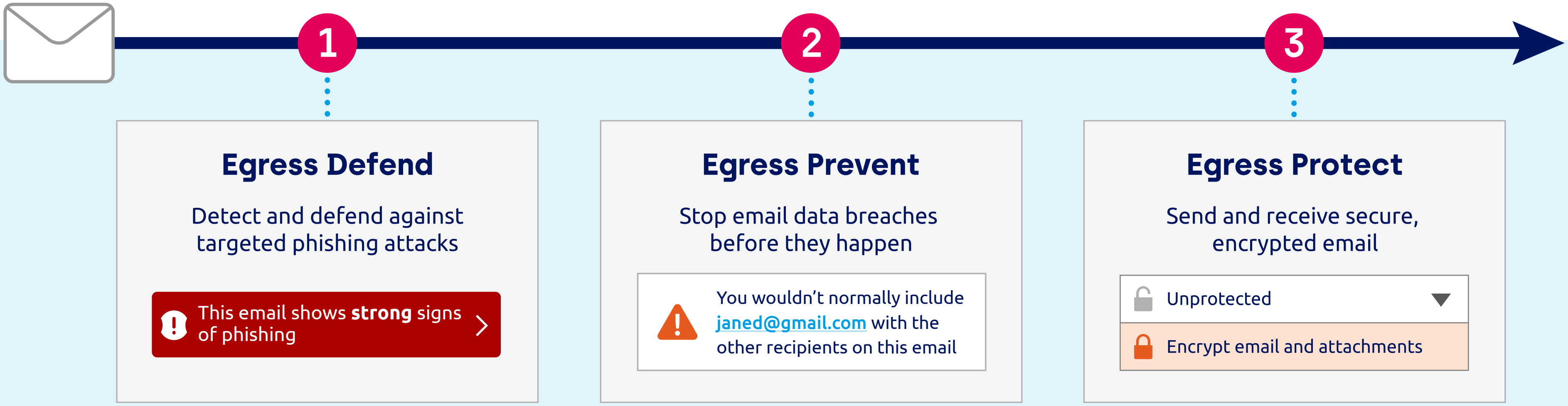
Egress Intelligent Email Security

Empowering your people to be your greatest security asset – wherever they're located

Egress offers the only human layer security platform that is designed to prevent breaches and protect sensitive data. Our intelligent technology combines contextual machine learning and powerful encryption, empowering employees to remain productive while being totally secure. We can detect and prevent accidental data loss and intentional exfiltration in real time, while also automating email security to reduce the risk to data in transit and at rest.

Our analytics technology accurately demonstrates risk reduction through using Egress, as well as areas for targeted remediation, and enables administrators to run thorough compliance reporting.

Book your free demo today



Egress Defend

Detect and defend against targeted phishing attacks

This email shows **strong** signs of phishing

Egress Prevent

Stop email data breaches before they happen

You wouldn't normally include janed@gmail.com with the other recipients on this email

Egress Protect

Send and receive secure, encrypted email

Unprotected

Encrypt email and attachments

Learn more

Learn more

Learn more

Want to find out how our intelligent technology can help you? The Egress Team would be happy to discuss the top benefits of our solution for your organization, including:

- ✓ **Enhancing service delivery to your clients**
- ✓ **Supporting your employees however and wherever they work, including on mobile**
- ✓ **Ensuring corporate and compliance data privacy requirements are met**
- ✓ **Making email security a competitive differentiator**
- ✓ **Protecting your employees from career-limiting mistakes**

Talk to us today ›

About Egress

Our mission is to eliminate the most complex cybersecurity challenge every organization faces: insider risk. We understand that people get hacked, make mistakes, and break the rules. To prevent these human-activated breaches, we have built the only Human Layer Security platform that defends against inbound and outbound threats. Using patented contextual machine learning we detect and prevent abnormal human behavior such as misdirected emails, data exfiltration and targeted spear-phishing attacks.

Used by the world's biggest brands, Egress is private equity backed and has offices in London, New York and Boston.

www.egress.com | info@egress.com | in EgressSoftware

egress