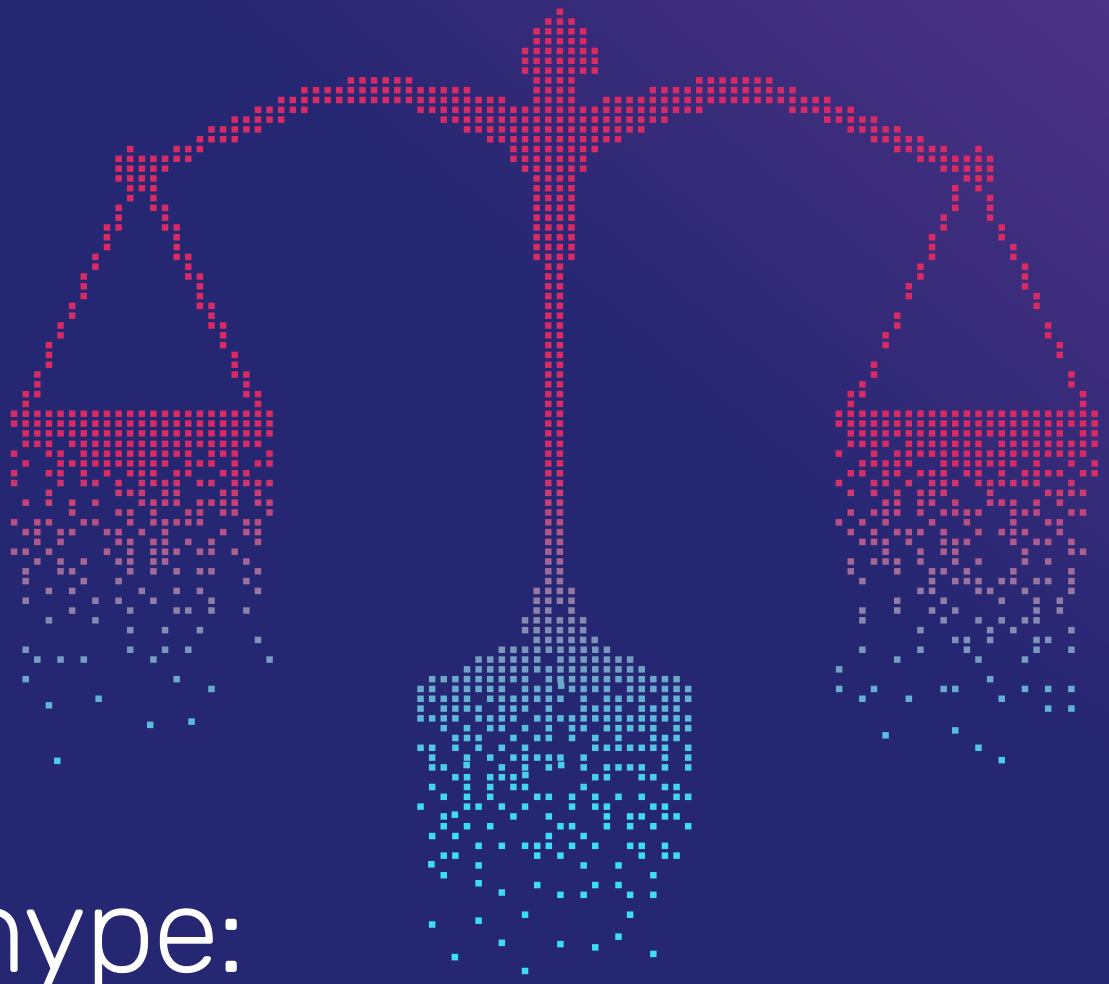
egress



Cybersecurity hype: How to manage **expectations vs reality**

AN EGRESS WHITE PAPER

Inside the report

INTRODUCTION

Managing cybersecurity hype

Despite ongoing investment in security technology and SA&T, organizations remain vulnerable to human activated risk. Existing technology has not been effective at stopping breaches arising from human behavior, such as falling for phishing attacks, data loss via human error, and deliberate exfiltration. Likewise, training people periodically using generic content hasn't been effective in helping organizations understand and reduce their risk.

Organizations continue to invest resources in mechanisms that promise to stop security incidents. Technology vendors say they can do this with new security technology; training vendors will make the same claims for their SA&T courses. However, Q4 of 2020 saw 53 million data breaches worldwide, so claims and reality aren't lining up. [1]

Buyers are faced with a crowded and complex market, needing to continually layer new security products into their environment to achieve defense-in-depth, assess new and emerging AI technologies, and continually re-invest in SA&T. IT Security buyers don't have as much time as they'd like to research and choose security solutions – a situation exacerbated by vendors that exaggerate their capabilities and sell products that don't meet expectations.

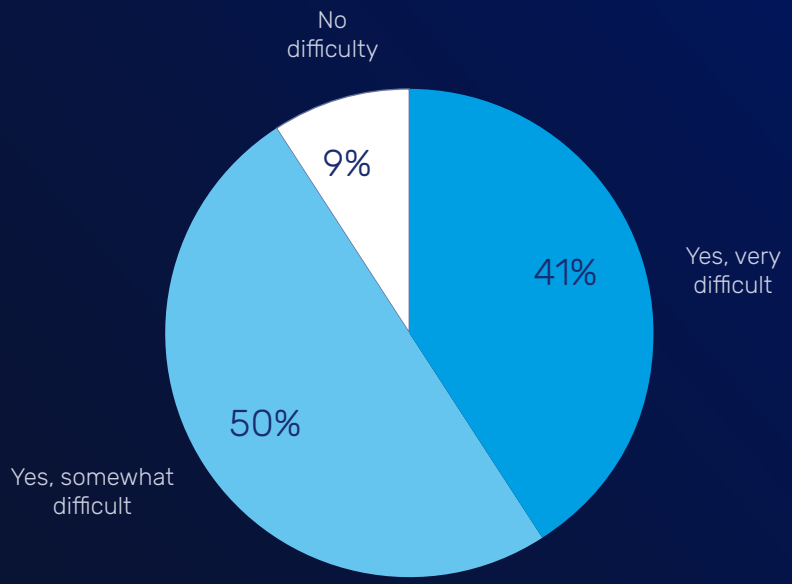
In this report, we present new research findings from a survey of 800 cyber security and IT leaders. 91% said they found it very, or at least somewhat difficult, to select cybersecurity vendors because their marketing is unclear about their specific offerings. And it's only getting more difficult. The cybersecurity industry is a hotbed of start-ups bringing new technologies to market that aim to solve the complex problems created by a rapidly evolving threat landscape.

[1] statista, Number of data records exposed worldwide from 1st quarter 2020 to 2nd quarter 2022

However, these vendors often struggle to articulate how their technologies work, instead resorting to marketing buzzwords, hype, and unsubstantiated claims. Start-up vendors in particular can be guilty of making bold claims and spreading marketing FUD (fear, uncertainty, and doubt) as they try to compete in a highly competitive market, and without the legal teams that exist in larger organizations to rein them in. As a cyber technology buyer, it can be hard to know what to trust, without having time to dig into all the details for every vendor.

So how do you accurately weigh up cybersecurity expectations versus reality? This report explores how cyber technology buyers can navigate this complex market and cut through the hyperbole. We'll discuss the expectations and reality of three hot topics in the cybersecurity industry: defense-in-depth, AI, and security awareness training.

Do you find it difficult to select cybersecurity vendors because their marketing is unclear about their specific offerings?



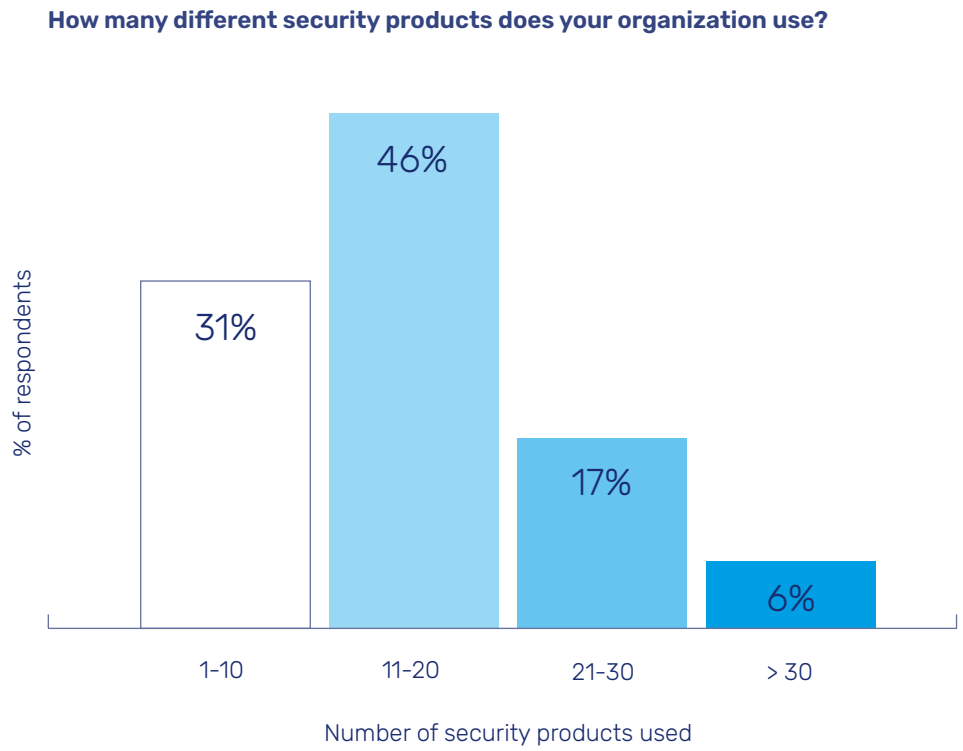
Defense-in-depth: Is it still the answer?

Defense-in-depth is a common phrase used in cybersecurity marketing. For decades, it's been recognized that the more layers of defense you have, the better your chances of detecting and preventing threats. And then if you are hit by a cyberattack, you've got a higher chance of containing, remediating, and recovering from the incident.

But are vendors accurately highlighting how their product fits into an organization's defense-in-depth strategy? Or is it being used as a buzzword?

Our survey of 800 cyber security and IT leaders shows 92% of organizations already implement a defense-in-depth strategy. As evidenced in the chart on the right, they also told us it's common for their security teams to manage between 10 and 30 different security products. So is adding more layers of security only ever a good thing? The truth is a little more nuanced.

92% of organizations implement a defense-in-depth strategy.



Why do vendors talk about defense-in-depth?

Defense-in-depth means security technology is deployed across all infrastructure and applications, including perimeter, network, host/endpoint, plus on-premises and cloud applications. The theory is that if there's a vulnerability in one part of the infrastructure, or one security/software vendor, then it won't affect the other parts.

Ultimately, defense-in-depth helps to prevent data breaches by protecting information and people. It also helps organizations to meet regulatory compliance and cyber insurance pre-requisites. There's an acceptance that total prevention of cybercrime is impossible, so security teams must deploy security technologies to achieve their goal of prevent where possible – then investigate, contain, respond to, remediate, and recover where prevention has failed.

Some common technologies include:

- EPP and EDR to protect devices
- SEG and SWG for email and web protection
- Network IPS/IDS to detect and block attacks
- Host IPS to lock down applications
- DLP to block exfiltration of sensitive information
- SIEMs to correlate alert information and help identify the root cause of an attack
- SOARs to help automate incident response and remediation

Of course, this is also a helpful argument when selling new cybersecurity products. Vendors might argue adding a new product will contribute to defense-in-depth. On the surface this can true, but adding more technology into your infrastructure isn't always the best move.

More tech, more problems?

Cybersecurity involves a risk versus cost argument, with factors including business and user friction, IT/Security team resources, and time. With this in mind, adding ever-increasing layers of security has three key potential drawbacks.

1. Increased attack surface

49% of our surveyed IT leaders said their organization suffers from vendor sprawl. One result of vendor sprawl is an increased attack surface. For every additional technology, whether a security control or productivity application, the likelihood of a vulnerability or misconfiguration being exploited by a bad actor increases.

Misconfigurations can lead to vulnerabilities and a lack of integration between technology controls exacerbates the problem further. This leads to a situation where yet more technologies and products are added to help integrate the existing ones.

2. Added complexity and overhead

Introducing additional technology means more management overhead for security teams. Each new product leads to more training, additional admin, and another set of alerts to monitor. Alert fatigue is a very real issue suffered by security analysts, as each new security technology introduces yet another flow of notifications.

Our survey data shows 49% of IT leaders feel their security stack is overly complex and almost the same amount (48%) believe their security team finds it difficult to manage their existing technologies.

3. Commercial risks

Commercial risks also need to be considered when onboarding multiple vendors – especially start-ups. The cybersecurity landscape has always been dominated by start-ups, and these new companies are at higher risk of failing commercially. In other cases they may be acquired, leading to products and functionality that your organization relies upon not being supported, patched and updated, and ultimately being withdrawn entirely.

Out of 800 cyber security and IT leaders:

49% suffer from **vendor sprawl**

49% feel their security stack is **overly complex**

48% say their security stack is **difficult to manage**

Do you really need another cybersecurity vendor?

If a vendor is using defense-in-depth as a key argument for why a new product(s) will benefit your organization, it's important to dig deeper and understand how they'll specifically improve your existing strategy. As there may be a simpler way to solve the problem in question.

It can often be beneficial for organizations to focus their efforts on auditing existing suppliers and controls, understanding that they have underutilized functionality, then filling security gaps with additional technology where necessary. For many businesses, Microsoft is the vendor organization of choice to consolidate around.

Instead of adding evermore layers of security, focusing on better integration between existing technologies can help organizations realize a better ROI on their overall security infrastructure.
One way to do this is consolidation around fewer vendors and filling gaps with additional technology only where required.
Consolidating around single, or a few, vendor suites can remove integration challenges, reduce attack surfaces, and minimize risk.

Defense-in-depth remains key to cybersecurity strategies and it's often raised by vendors in their marketing. However, it's important to keep the points discussed in this section in mind before adding more technology to your security stack. Sometimes consolidation and streamlining is the more valuable and risk-averse strategy – this should be kept in mind when a vendor uses defense-in-depth as a key selling point for their additional piece of cybersecurity technology.

Consolidating around single, or a few, vendor suites can remove integration challenges, reduce attack surfaces, and minimize risk.

AI: Weighing up hype vs. value

"AI innovation is happening at a rapid pace, with an above-average number of technologies on the Hype Cycle reaching mainstream adoption within two to five years," said Shubhangi Vashisth, senior principal research analyst at Gartner.[2] "Innovations including edge AI, computer vision, decision intelligence, and machine learning are all poised to have a transformational impact on the market in coming years."

77% of IT leaders are already using a cybersecurity product with AI.

AI and its various sub-categories are playing an increasingly major role in cybersecurity – 77% of IT leaders told us they're already using a cybersecurity product with AI. But how can organizations understand whether AI-based technologies are relevant to their specific use cases? When vendors present AI technologies as black box solutions, it can sometimes be difficult to separate hype from reality.

Out of 800 cyber security and IT leaders:

66%

'fully understand' how AI makes their security products more effective

52%

think vendors are 'very clear' in how they market AI capabilities

Where does AI have real-world cybersecurity utility?

AI is used to discover new, unknown threats that evade detection by other technologies. It can also speed up and improve the accuracy of incident investigation, and reduce user friction. In addition, machine learning algorithms are used to analyze relationships and behaviors across multiple parameters and large datasets, including network traffic and communications, user activities, file structure and content, and URL structure.

Applications use continuous behavioral analytics and user/activity risk to determine when to step up authentication. Natural language processing can also be used to identify signs indicative of social engineering in, for example, phishing emails. Computer vision can be used to identify logos of frequently impersonated brands on phishing sites and in phishing emails.

[2] Gartner, Gartner Identifies Four Trends Driving Near-Term Artificial Intelligence Innovation

It's important to look under the hood of cyber security products and make sure the reality matches up to the claims.

Good solutions can use learned behaviors to detect anomalies and similarities, such as patterns of known malware, malicious URLs, or suspicious traffic flows. They can also detect anomalous behaviors indicative of human error that could result in data breach, such as misdirected emails or incorrect attachments. This speeds up time-consuming tasks for security teams, such as triaging and prioritizing threats flagged as suspicious by other security controls.

While all this is possible – when talking to vendors it's important to look under the hood of cybersecurity products and make sure the reality matches up to the claims.

Assessing the real value of products using AI

The challenge facing most organizations when separating expectations from reality is understanding the use cases where AI is most effective and how to evaluate the available technologies. Despite over three-quarters (77%) of our surveyed IT leaders using an AI cybersecurity product, only 66% said they fully understood how AI made their security product(s) more effective.

One of the issues is how vendors market their technology. Only 52% of IT leaders thought cyber security vendors were 'very clear' in how they market their AI capabilities.

Many vendors present AI as a black box solution, so how do you qualify risks and benefits? Cutting through the hype and marketing surrounding AI is difficult because most IT teams do not employ data scientists who know which questions to ask vendors selling solutions that claim to use AI.

There are also technical challenges associated with the use of AI and securing it. Adversarial system manipulation and poisoning of the data used to train algorithms can result in undetermined and incorrect outcomes and bias. Like any technology, it presents an attack surface, so you need to understand exactly what vendors are offering and the risks associated with it.

Organizations should look for vendors that are able to:

- Use simple language to articulate their value proposition
- Explain clearly how their solution can help meet a customers' real-world needs
- Educate customers on how AI helps with specific use cases

Are organizations expecting too much from SA&T?

Of the 800 cyber security and IT leaders we surveyed for this report, 96% believe training can make long-term, positive changes to their employees' behavior. Despite these beliefs, other data we've discovered suggests that these expectations may be divorced from reality – and inflated expectations of SA&T can be exacerbated by vendors.

In our 2022 report 'Fighting Phishing: The IT leader's view,' 98% of the surveyed organizations told us they carried out at least some form of SA&T.[3] 55% percent of IT leaders said they carried out training a few times a year, while 38% have monthly training. SA&T is big business – and Cybersecurity Ventures predicts the global spend on SA&T to reach $10 billion by 2027, with new vendors flocking to the industry.[4]

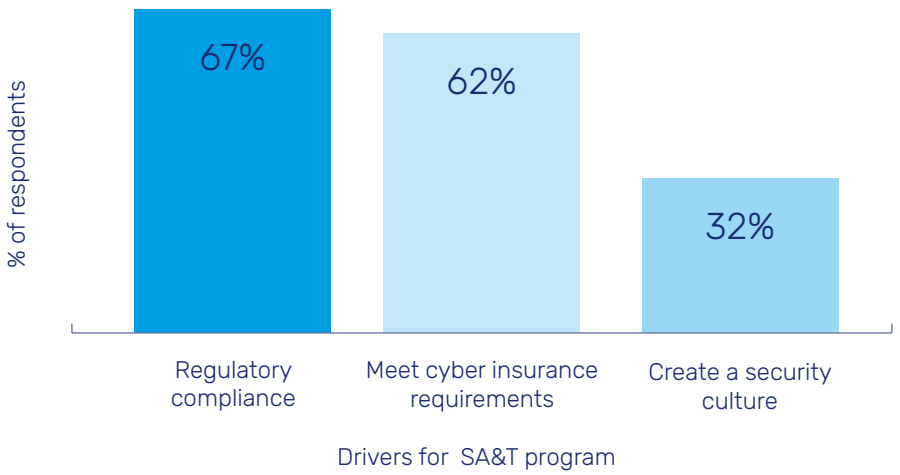
However, 84% of the same IT leaders also told us they'd been victims of successful phishing attacks in the past 12 months – so SA&T clearly isn't stamping out breaches. There are limitations to SA&T as it currently exists and improvements are needed if organizations want to create true security cultures.

98% of organizations carry out some form of SA&T.

'Box-ticking' SA&T won't bring real change

Despite almost all surveyed IT leaders (96%) telling us they believe training can make long-term positive change, only 32% said creating a culture of security is the driver for their SA&T program. Far more acknowledged that ticking boxes for regulatory compliance (67%) and cyber insurance (62%) was their priority. If the goal is changing people's behavior, some organizations may need a reality check.

What drives the need for your organization's security awareness program?



[3] Egress, Fighting Phishing: The IT leader's view

[4] Cybercrime Magazine, Security Awareness Training Explosion

According to Jinan Budge, Vice President and Principal Analyst at Forrester Research, behavioral change is rarely the outcome for organizations' SA&T programs. At the Egress Human Activated Risk Summit 2022, she explained: "At Forrester Research, we reviewed 46 standards and frameworks around the world which required organizations to do SA&T.

Watch the full on-demand webinar with Jinan Budge here.

"Among other details, they wanted to understand the purpose of the training. According to the research, the purpose is often to make people understand, retain knowledge, and make them aware. Behavior and culture, on the other hand, were only mentioned a handful of times. We found most frameworks were created between five [and] 20 years ago and had not updated for modern times."

Jinan continued: "Awareness and understanding are not the same. One-off SA&T sessions actually disengage employees from the topic and security at large. This doesn't result in long-term behavior change. The goal should be to achieve culture change – not simply meeting a compliance requirement. How can you tell if behavior has changed by stating 99% of employees have completed SA&T? SA&T is an activity, not an outcome."

Egress research also shows that 45% of organizations change training supplier on a yearly basis.[5] Does that mean they're always on the lookout for something more effective? Or perhaps some see SA&T as a box-ticking exercise and simply want the most affordable option? This is plausible when organizations are bound by regulations and contractual requirements that means they have to, for example, have phishing simulations in place.

In turn, this means organizations are spending money on SA&T without seeing ROI in the form of understanding organizational risk, and the meaningful behavior change that reduces the number of security incidents.

[5] Egress, Fighting Phishing: The IT leader's view

How to make SA&T meet expectations

There are many SA&T vendors on the market – and as evidenced in the previous sections, almost every organization carries out SA&T of some form, and many frequently change vendors. However, there are three key considerations to make sure that whatever SA&T you invest in actually brings about real organizational change and creates a security culture.

1

Measure outcomes rather than activity

Real outcomes need to be measured, not just SA&T participation as a statistic. It's possible to define desired employee behaviors and then measure whether they change after training efforts. Enabling encryption, using a password manager, using MFA, backing up data, following security warnings, and turning auto-updates on are all things that can be measured to give a true value of whether behavior is actually changing over time after SA&T.

2

Tailor training to the individual

It's important to understand individuals' needs and offer them targeted coaching. There are different risks associated with each individual that come from many sources. For example, you might be able to use security questionnaires to get an initial baseline of risk across your organization. But someone's job role and level of seniority should also be considered to see how likely they are to be targeted by cybercriminals or accidentally or intentionally cause a security incident involving privileged data or systems.

Organizations also need to consider people's historic behavior related to activities like falling for phishing emails, sending misdirected emails or those with incorrect attachments, malicious website access, VPN usage, credential hygiene, and AUP (Acceptable Use Policy) violations. It's then possible to meaningfully target each individual with the right SA&T/coaching at the right time via the right mechanism.

How to make SA&T meet expectations

3

Combine SA&T with real-time teachable moments

Transformative and engaging content has its place but it's an activity not an outcome. This needs to be combined with interventions or nudges where they're most needed – when people are carrying out risky actions in real time. However, our survey data shows that many organizations are not doing this, with only 40% offering fixed frequency SA&T combined with real-time interventions, such as alerts just before a user makes a mistake, such as replying to a phishing email.

Intelligent software can be used to send 'nudges' to engage people when they're about to perform a risky action. At Egress, we call these real-time teachable moments. For example, Egress Intelligent Email Security adds real-time banners to both inbound and outbound emails. They pop up in genuine moments of risk, such as when someone is about to click on a phishing link, send an email to the wrong address, or use an inappropriate level of encryption.

These teachable moments are designed to not only stop breaches in the moment, but also educate people in real time as to why an action has been flagged, reinforcing SA&T, and boosting the ROI of training efforts. They also enable organizations to genuinely understand their risk on a per person basis, rather than at an organizational level only.

Buyer tips for managing cybersecurity expectations

Think carefully before adding new products for defense-in-depth reasons alone. Vendor sprawl, added complexity, and alert fatigue bring their own risks. Consider consolidating and streamlining around a select few trusted vendors and only then, fill the gaps.

AI has come a long way in recent years and products can provide real-world value. But make sure you arm yourself with the right questions to ask vendors. They should be able to simply explain their value proposition and how they'll support your specific use cases.

SA&T as a box-ticking exercise won't bring real security culture change. Organizations need to combine SA&T with real-time teachable moments, tailor programs to individual needs based on user risk, and measure real-world outcomes rather than participation statistics.

The combined value of Microsoft and Egress

Together, Microsoft's cloud-native email security capabilities and Egress' advanced email protection capabilities help organizations optimize their email protection investments and reduce human activated risk by:

- Reducing unnecessary email infrastructure cost and complexity by avoiding duplication of functionality between cloud-native capabilities and secure email gateways (SEGs)
- Complementing cloud-native security features with modern techniques like AI and natural language processing to stay a step ahead of sophisticated threat actors
- Bringing the once disparate activities of inbound and outbound email protection together into a unified model
- Turning users into allies by educating and guiding them in non-intrusive and mutually beneficial ways

Book a demo

Egress
Defend

Detect and defend against targeted phishing attacks

Learn more

Egress
Prevent

Stop data breaches before they happen

Learn more

Egress
Protect

Send and receive secure, encrypted email

Learn more

Inbound threat protection

Outbound threat protection

About Egress

Egress makes digital communication safer for everyone. As advanced and persistent cybersecurity threats continue to evolve, we recognize that people get hacked, make mistakes, and break the rules. Egress's Intelligent Cloud Email Security suite uses patented self-learning technology to detect sophisticated inbound and outbound threats that protect against data loss, resulting in the reduction of human activated risk.

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

Methodology

New research for this report was carried out by Pollfish on behalf of Egress. 800 cyber security and IT leaders were interviewed from a range of industries, with respondents coming from the UK and US.

www.egress.com | EgressSoftware