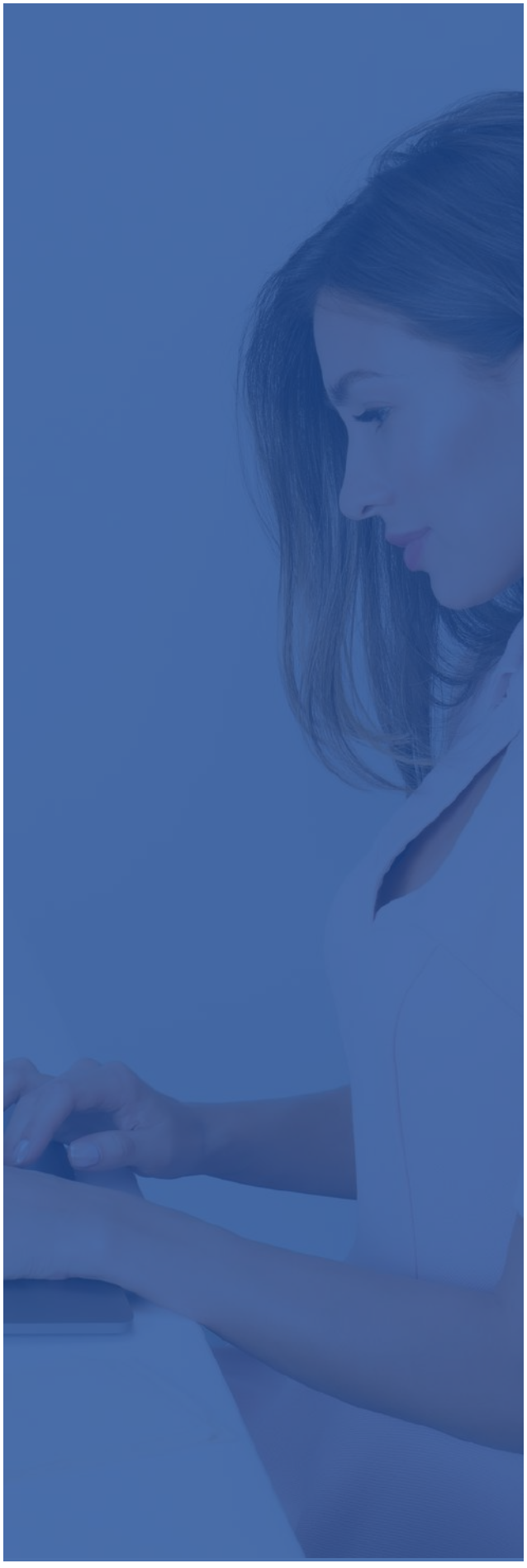
Retruster

Next generation online protection



Security starts here

How do over 90% of cyber attacks start?

With a phishing email. Ransomware, malware, financial fraud. All from phishing emails. These emails are getting more sophisticated, and the tools available just can't keep up. These tools grew out of the anti-spam world of the 90's and are generally rule-based, slow to respond, require massive servers, and are ill-equipped to deal with modern threats. Attackers are agile: leveraging automation, artificial intelligence and machine learning.

Isn't it time those tools were used against them?

The right to know

How do you know if an email is legitimate?

Answer: you don't.

With around 15% of phishing emails getting through the well-known email security products, you're taking a chance every time you open an email. If an email is not stopped by these solutions, it's trusted by the end user. There's no last line of defense, no further information given, no safety net.

Introducing Retruster

What is Retruster?

Retruster is the next-generation in email protection. It's a product that's purpose-built to protect against phishing emails, leveraging the latest technology: including Artificial Intelligence and Machine Learning.

Crucially, it connects this proprietary advanced technology to the user in a meaningful way – resulting in a solution that is seamless, effective and intuitive.

The Retruster advantage

Your last line of defense

Retruster truly is a last line of defense. A user thinks that phishing emails that got through filtering solutions are automatically safe. Retruster keeps them aware & protected.

Previously Unseen First-time Threats

Other solutions classify emails as they go through their servers. Now malware automation means classification is becoming irrelevant as malware mutates constantly, meaning no two instances are alike. Retruster's architecture enables it to deal with Previously Unseen First-time Threats.

"Retruster truly is a last line of defense, keeping users aware & protected – constantly."

Retruster

The last line of defense

To use a soccer metaphor:
If your current
email protection product
is the defense,
Retruster is the
goalkeeper.

The Business Case for Specific Email Protection

Well-known solutions like Mimecast and Proofpoint are excellent at stopping spam, archiving, and email continuity.

They're not particularly strong in specifically addressing phishing emails.*

- Retruster is a **specific anti-phishing product** that **works with Mimecast, Proofpoint, or any other platform** to stop phishing attacks - and their consequences.
- The *average* cost of the consequences of a phishing email: $1.6 million - $3.9m.
- For larger organizations up to $300m.

**Due to a number of factors including product design and architecture, the way the world of malware has changed due to automation, and the complexity of identifying phishing emails while not interrupting business continuity.*

- Traditional email security companies route all emails through their servers
- They have to decide "threat or not threat" (binary)
- If not a threat, email is released to user
- User now trusts the email even if phishing
- However can take up to 48 hours to classify new threats
- All of this means these solutions are:
  - Expensive
  - Difficult to set up
  - Not effective regarding previously unseen threats

Many Retruster clients use Mimecast/Proofpoint/other solutions in addition to Retruster.

*The number of phishing emails Retruster **still** identifies – even after emails have been through these other products' checks –*

shows the effectiveness of a combined approach.

Retruster architecture

Using the Microsoft Graph API with proprietary algorithms, Retruster detects anomalies in real-time.

It gives users context-specific warnings about potential threats and allows users to find out more information should they wish to.

It can be used in addition to any other security product, resulting in an elegant, effective solution.

This allows Retruster to be deployed with any other security product, or as a standalone phishing protection platform.

This means

- No settings changes, no changes to DNS or MX records
- Seamlessly integrates with Office 365 and G Suite
- Supports cloud, on-prem, hybrid
- 98% reduction in clicks on phishing emails
- No emails are routed through Retruster servers
- No disruption

Benefits of Retruster

- Effective immediately
- No settings changes
- No changes to DNS or MX records
- Seamlessly integrates with Microsoft Office 365 and Google G Suite
- Supports cloud, on-prem, hybrid
- No disruption, ever
- Completely seamless
- No ongoing maintenance required
- No manual rules or exceptions, everything completely automated and smooth

Works with existing solutions

No need to "rip and replace". Just add Retruster to your current stack, it's as simple as that. Retruster can be deployed as a standalone product, or together with other well-known email security products to provide comprehensive – and much needed – specific advanced anti-phishing capabilities and the most robust security posture possible.

The proof is in the thousands of phishing attacks that Retruster has stopped that evaded well-known solutions when Retruster is deployed together with these products.

Retruster customers

Retruster protects organizations large and small across the globe. Financial institutions, healthcare providers, manufacturers, educational institutions and other organizations in every industry benefit from Retruster protection. With thousands of phishing attacks stopped, millions of dollars saved, and a loyal customer base, Retruster continues to add value to its clients every single email.

About Retruster

Retruster's mission is to protect those vulnerable against the threats of malicious actors. Not enough was being done by existing products, and too many innocent individuals and businesses were exposed and being taken advantage of.

Retruster leveraged its founding team's deep technical knowledge and experience to provide a solution that levels the playing field and utilizes advanced technology to provide continuous and effective protection against cyber threats.

Retruster is privately owned and operates in most countries worldwide.

Specific product comparisons

Retruster	Mimecast/Proofpoint/ Others
Picks up warning signs immediately, even before a new threat classified	Can take up to 48 hours to recognize & classify Previously Unknown First-Time Threats
Users are warned immediately, and the likelihood of threats passing through stealthily is almost zero	Malware like Dridex and Emotet are being automated to pass through current filtering/classification
Where Mimecast misses an email, Retruster will at the very least label it as a first-time sender, providing early warning for users	Effective in ~85% of cases - meaning 15 in every 100 malicious emails gets through to users
Suspicious emails are always labeled - users will not be caught off-guard	Users are aware the solution is in place - therefore if an email is delivered, they assume it's safe
No business interruption - no fetching from quarantine	Suspicious emails need to be "fetched" by the user
Quick integration with no impact on performance. Simply add or remove permissions globally	More lengthy and resource-heavy integration