BATTLE CARD

USER SECURITY: INBOX DETECTION & RESPONSE (IDR)

CHANNEL PARTNERS ONLY

What is IDR?

IDR enables staff to flag suspicious emails with a special Outlook plug-in. When such an email is flagged, it's investigated for safety within minutes. A short time later, whoever reported the email gets a status message — threat or no threat — and the email is either verified or removed.

What differentiates our solution?

A great user experience encourages more reporting

One button reporting Much easier than reporting through an email distribution list.

Receive instant feedback and a final response within minutes When will a user hear back from their IT team about their submission?

Automatically quarantine reported messages This eliminates a user mistakenly clicking a link later.

Advanced software/security resources boost effectiveness

Leading software We use GoSecure IDR software which includes machine learning engines to scan reported emails.

Experienced security analysts Further analysis is conducted by expert resources 24/7 to identify threats that even the best software can't catch.

Global email redaction If a reported email is malicious, it is automatically removed from all users' inboxes.

Turn-key managed service reduces cost

A complete service provided for a low monthly cost per user. TPx Managed IDR service includes all the technology, security analysis services, technical support and administration needed. The cost is a fraction of what it costs to acquire and manage similar solutions.

How can I position this successfully?

TPx Managed IDR offers unique value as a standalone solution

TPx Managed IDR helps employees strengthen their overall security posture.

A great user experience encourages use, which further enhances effectiveness.

Prevent more phishing attacks using advanced software and expert resources.

Start the security discussion with TPx Managed IDR, then upsell

TPx Managed IDR delivers compelling value that is easy to understand.

Customers will recognize immediate and continued value through consistent interaction with the solution.

TPx Managed IDR has excellent synergies with other TPx solutions, such as Security Awareness Training, Microsoft 365, and MDR.

Bundle other services to differentiate TPx vs. the competitors

Add Managed IDR to Managed Microsoft 365 sales. Email filters are not foolproof.

Security Awareness Training helps users to recognize suspicious emails. IDR gives them a way to leverage that knowledge to enhance your security.

Endpoint Managed Detection and Response (MDR) blocks attacks from executing on endpoints. IDR minimizes instances of phishing, which is the #1 cause of cyberattacks.

TPx®

How do I achieve effective email security?

Security requires a layered approach. To successfully defend against advanced phishing attacks customers must:

Catch malicious emails before they hit their network (email filters)

Recognize when something looks suspicious to avoid falling victim to an attack (Security Awareness Training)

Report suspicious emails, and identify and remove malicious emails (TPx IDR)

Prevent attacks from executing on endpoints (EDR/MDR)

Competitor or complimentary service?

Email filters, such as Defender for Microsoft 365, should not be considered competitors, but rather complimentary solutions. Filters are necessary and catch what they can before the email hits your inbox. They are not fool-proof. IDR is an additional defense to address those emails that get through.

Many Security Awareness Training vendors claim to compete because they offer a similar reporting capability to TPx's IDR solution. That is where the similarity ends — they simply offer easy reporting, not a full security solution.

What to ask	What to listen for	What to say
How are you currently preventing phishing attacks from being launched through malicious emails?	"I don't know", "We use [Defender, Proofpoint, Barracuda (Email filters)]	It's important to create an email security solution that includes multiple opportunities to identify and prevent attacks. Email filters are an important solution — one that we always recommend because it can stop attacks before they reach your users' inboxes…But what happens to those emails that make it through? That's where IDR becomes so important [explain the value]
How do your employees currently report suspicious emails?	"We don't", "We use an email distribution list", we use a plugin provided by our Security Awareness Training vendor [Knowbe4, infosec, Mimecast…]"	Would you be interested if I could show you a solution that will increase your email reporting rates? [if using a plugin already]..Great — that makes reporting easy but that's only part of the battle. Would you be interested in a solution that can provide fast and effective 24/7/365 analysis of those emails so you can determine which are malicious?
What happens when someone reports a suspicious email?	"Our IT team looks at it", "I don't know", "We have an outside team of experts look at it"	Once an email is reported it's important to take quick and effective action to prevent the attack. Would you be interested in learning about a solution that leverages advanced software, and expert 24/7/365 analysis to quarantine malicious emails and remove them from all users' inboxes?
Do you currently provide Security Awareness Training to your employees?	"Yes" "No"	That's great. Security Awareness Training can help users recognize potential phishing attacks. Would you be interested to learn about a solution that compliments this by giving users a way to use that knowledge? Arming users with knowledge to recognize a phishing attack is an important part of any security strategy. That's why TPx provides this. But we also provide another valuable solution that many overlook — IDR — which gives employees an easy way to report suspicious emails and provides fast and effective analysis.