Managed Inbox Detection & Response (IDR)

Ensure every user-reported phishing email gets a rapid, expert response–without burdening your IT team

What Is It and Why Do You Need It?

Human error remains the #1 cause of security breaches, and phishing is often where it starts. Email filters miss things. When users spot something shady, they forward it to IT—or worse, click it. TPx Managed IDR gives your people a one-click button in Outlook and turns those reports into fast, managed action. Suspicious emails are quarantined, analyzed by advanced tooling and a 24×7 analyst team, then safely returned or removed from every impacted mailbox. You reduce risk, reinforce awareness, and take the triage burden off your IT team.

Benefits

Benefit	What It Means for You
Reduce successful phishing attempts	Malicious messages get yanked across your tenant—often within minutes—before anyone else clicks.
Lighter IT workload	TPx manages intake, analysis, and remediation so your team doesn't live in an abuse@ inbox.
Faster, clearer decisions	Users get status updates; admins get dashboards—no guesswork about what happened.
Stronger security culture	Every report becomes a teachable moment that reinforces training and good habits.
Predictable costs	All technology, management, and support under a simple per-user subscription.

How It Works

Make Reporting Effortless – We deploy the Outlook add-in so users report suspicious emails with one click—no forwarding, no tickets.

Step 2: Take Risk Out of the Inbox – Reported messages are automatically quarantined to prevent accidental clicks while analysis runs.

Step 3: Get Expert Verdicts, Fast – Advanced detection plus a 24×7 analyst team classifies each message as safe, malicious, or caution.

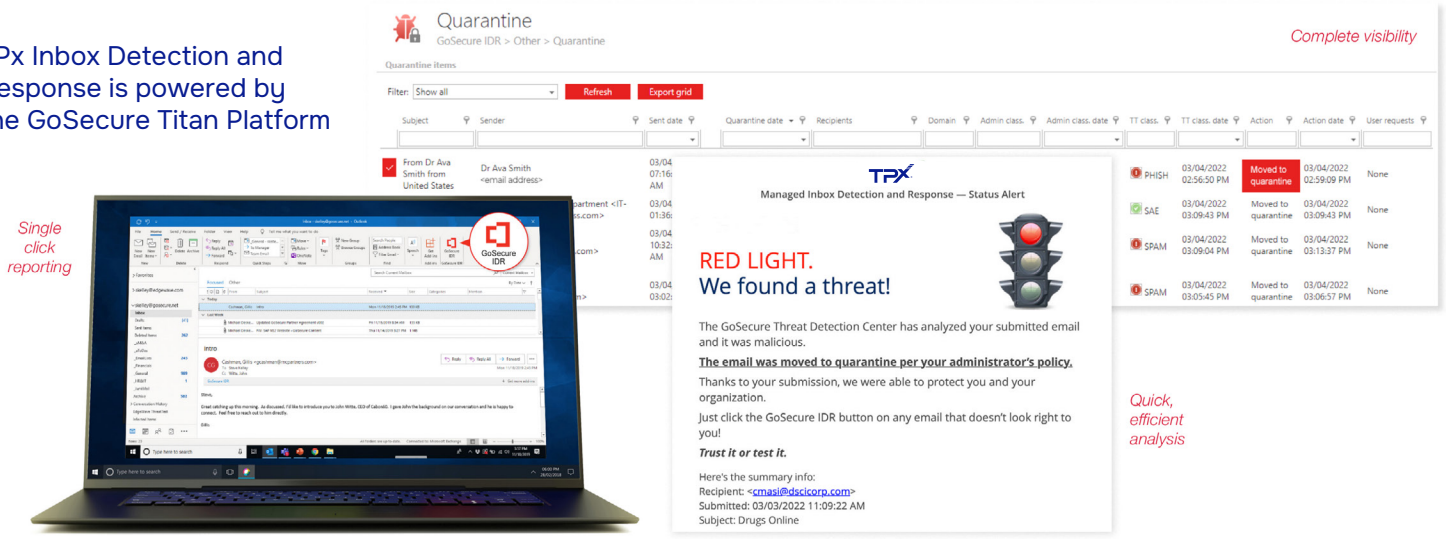
Step 4: Remediate at Scale – Safe emails return to the user; malicious/caution emails stay quarantined and are removed from all recipients across your tenant—multiplying the impact of a single report.

Step 5: See and Learn – Users receive clear status notifications; admins get dashboards and trends to track adoption and risk.

At-a-Glance (What's Included)

- Professional onboarding & runbook
- Outlook add-in deployment and tuning
- 24×7 monitoring, analysis, and classification of user-reported emails
- Tenant-wide removal of confirmed threats
- User notifications + admin dashboards
- Ongoing platform updates and support

TPx Inbox Detection and Response is powered by the GoSecure Titan Platform



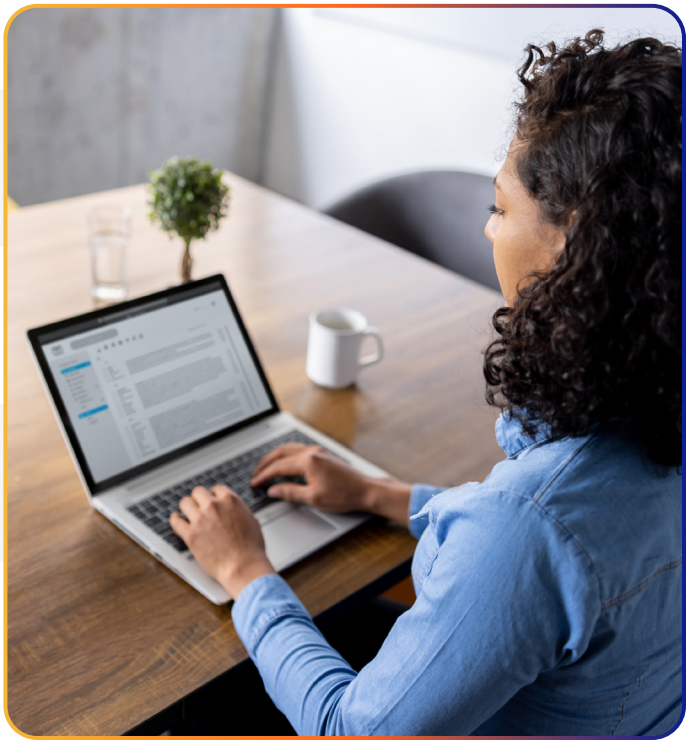
Why TPx?

Managed from Day One – We handle onboarding, configuration, license changes, and ongoing platform management.

Analyst-Backed 24×7 Coverage – Continuous evaluation and escalation by a dedicated security team—without you building a SOC.

Frictionless User Experience – One-click reporting in Outlook + automatic user notifications drive high participation.

Works Better Together – Pair IDR with TPx Security Awareness Training and Managed Endpoints to tighten the email-to-endpoint kill chain.



Endpoint, User Security and Management Services

Service Features	Description	Endpoint Manage-ment	Endpoint Security	User Security
Monitoring, Alerting, and Reporting	TPx provides automated monitoring and alerting and scheduled reports for device availability, health and performance, and inventory. Monitoring and alerting are per TPx's recommended practices. Alerts are received and actionable by either TPx or the customer, based on service level.	■		
System Patching	TPx provides managed, automated patching of operating systems and select third-party applications. Service includes operational and security patches remotely applied per TPx recommended practice. Patch status monitoring and reporting are also included.	■		
Remote System Support	TPx provides 24/7 troubleshooting and repair of covered devices. Service includes proactive support based on TPx recommended practice and responsive support for customer requests or identified alerts. Remote Systems support features may be included in the fixed monthly charge or billable based on the chosen service level.	■		
Lifecycle Management	TPx provides proactive reporting and communication of end-of-life status on covered servers. Service includes hardware warranty expiration as well as manufacturer end-of-support status for operating systems and select applications. Post-warranty hardware support packages are available at additional cost.	■		
Managed NGAV	TPx provides managed Next-Generation Antivirus support. Service includes the use and management of the NGAV software as well as monitoring, alerting, and reporting on NGAV status. Virus remediation is available as a billable service.		■	
Endpoint Managed Detection and Response	TPx provides MDR services to identify and prevent advanced security attacks. The service includes the use and management of leading EDR software, SaaS platform hosting, SOC threat hunting, alert response, and event mitigation with an industry leading 15-minute response time.		■	
DNS Protection	TPx provides DNS Protection for covered devices to combat Internet-born threats and enforce Internet usage policy. Service includes the use and management of the DNS Agent software, configuration of security policies, and monitoring and reporting on browsing activity and security events.		■	
Security Awareness Training	TPx provides automated Security Awareness Training campaigns. Service includes campaign setup, ongoing phishing simulations, and monthly training courses delivered automatically to enrolled users. Scheduled reporting of campaign status and activity is also included.			■
Inbox Detection and Response	TPx Inbox Detection and Response service allows users to easily report potential phishing emails. Reported emails are quarantined then scanned by software and SOC personnel to identify threats. Within just a few minutes, safe emails are returned to the users' inbox and malicious ones are removed			■

All service features are available in pre-packaged solution bundles to meet a variety of use cases. Endpoint Security and User Security service features are also available as stand-alone offerings.