User Security
Managed Inbox Detection & Response

Professional evaluation and handling of suspicious emails reported by users – right from the inbox

Phishing continues to be the number one cause of data breaches. In 2021, 53% of organizations reported a phishing-related breach[1]. Email security filters, while generally effective, are not foolproof. Increasingly, organizations are augmenting these solutions with user-driven reporting of suspicious emails. But how do already overburdened Security teams keep up with monitoring and evaluating suspicious emails that are being reported? The answer is Inbox Detection and Response (IDR).

Why should I use IDR?

Efficiently report suspicious emails IDR gives users a faster, easier way to take the guesswork out of questionable messages. Reporting suspicious emails is done with a single click right from their inbox.

Quickly validate reported emails Using advanced technology and human security experts, reported emails are validated and either returned or removed within minutes. This reinforces the users' security awareness, which better protects the organization.

Identify and remove malicious emails Reported emails that are deemed malicious are removed from the user's inbox. Other recipients of the same message will also have the message removed, even if they did not submit the email for review. This helps you minimize the opportunity for other users to fall victim to phishing attempts.

Why should I choose TPx?

Leading technology Best-in-class security technology and automated machine learning engines are used to quickly and accurately identify and mitigate malicious emails.

Advanced security analysis Inconclusive messages are further analyzed by a team of security experts 24/7/365 to accurately make a final determination.

Exceptional user experience Reporting is done via a single click using a button in the Outlook Ribbon. Regardless of whether the email is malicious or not, a clear status is communicated to the user.

Comprehensive support TPx takes care of all technical support for the solution to ensure that it works as designed and your organization receives maximum value.

[1] *Dark Reading, 2021 Strategic Security Survey*

What's included?

Onboarding Services TPx's professional onboarding process allows you to quickly achieve value for your investment. TPx configures the IDR platform, provides expert guidance to configure your Office 365 environment and manages the entire implementation project.

Technical Support TPx will manage the system to ensure that it is functioning as designed. This includes delivering platform support as well as guidance on troubleshooting Office 365 and the Outlook add-in. Our team is available 24/7/365 to assist and enhance the success of our solution for your organization.

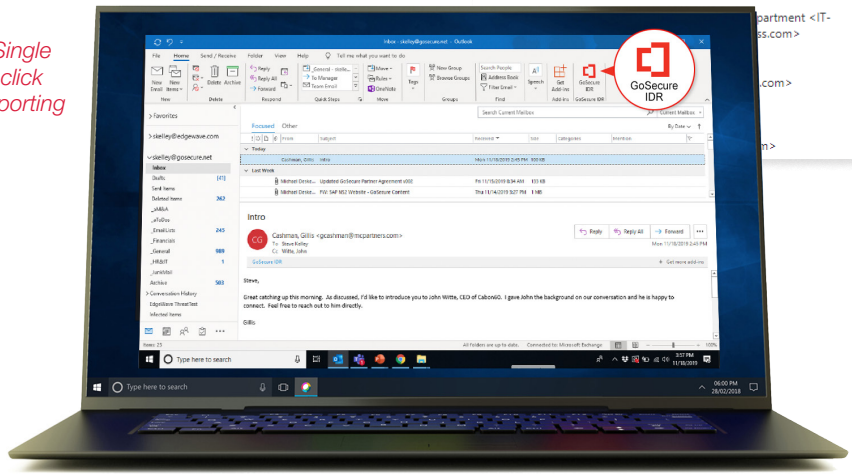
Change Management Adding new licenses and assigning users is easy. We'll handle all requests to ensure that licenses and users are added quickly and effectively.

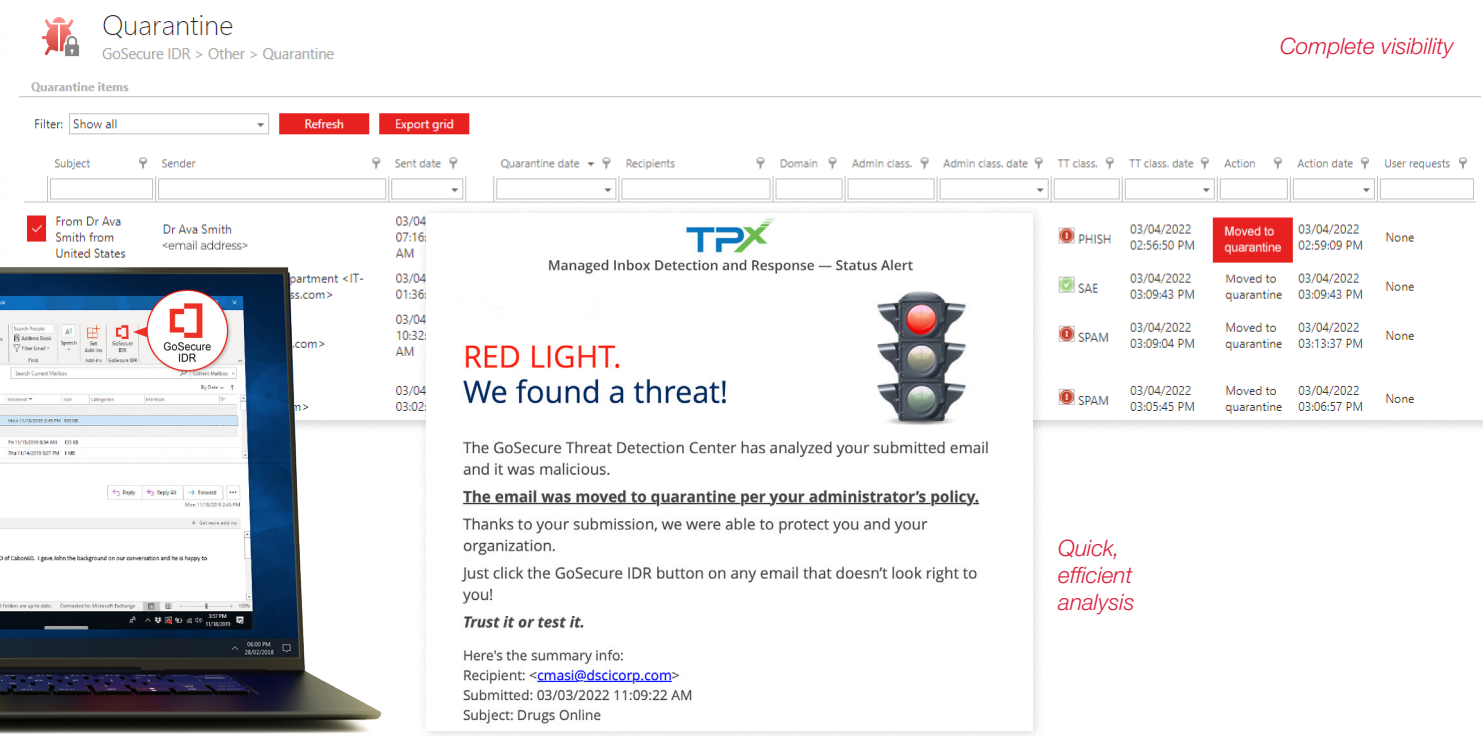
Platform Management and Updates Security threats evolve, and our solution evolves with them. Enhancements to the security capabilities and performance of the IDR platform are automatically provided to maximize efficacy.

Cost-effective Security This complete turn-key solution is provided for a fixed per-user monthly cost. You benefit from having exceptional security without the expense of acquiring and managing the technology in-house.

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

Single click reporting





Complete visibility

Quick, efficient analysis

Managed Inbox Detection and Response is an integral part of TPx's security services portfolio for protecting endpoints and users from ransomware and other cyberattacks. Bundling multiple services can increase your overall value and improve your organization's security. Below is our current portfolio of Endpoint and User Security and Management services.

Service Features	Description	Endpoint Management	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.