CYREN

Cyren Inbox Security

Enterprise Security SaaS

Advanced phishing security for Office 365—continously monitor, detect and remediate user inboxes for today's evasive phishing emails

Cyren Inbox Security finds the phishing threats your existing defenses have missed through a combination of:

- Continuous monitoring of user mailboxes for threats
- Active real-time scanning and ongoing analysis of linked landing pages
- Time-series analysis of email sender and recipient behavior to identify anomalies and threat patterns
- User-powered crowd-sourced detection and reporting of new, emerging threats

Counter Today's Sophisticated Phishing

By leveraging the native API integration offered by Office 365, Cyren is able to detect email threats on a continuous basis, as well as provide a powerful set of remediation capabilities to identify and mitigate the types of phishing messages which legacy perimeter defenses find challenging to stop, including:

- Phishing emails utilizing evasive techniques, like delayed URL activation, URLs hidden in attachments, use of strong encryption, use of real and valid SSL certificates, etc.
- Spoofed spear phishing messages impersonating employees or trusted partners
- BEC and CEO fraud and other targeted social engineering attacks
- New zero-day phishing campaigns
- Account takeovers

CIS currently supports Office 365, with future API platform integrations planned to extend mailbox-level behavioral analysis to other Microsoft applications, and then to other cloud-based enterprise communications and collaboration applications like G-Suite, Salesforce, Slack, and others.

Quick Two-Step Deployment

CIS is an easy-to-use, non-intrusive security solution-as-a-service that complements your existing secure email gateway without the need for any MX record changes. Get up and running in just a few clicks—simply 1) authorize Cyren to access your email flow and 2) then configure your preferred filtering and remediation policies, including flexibly applying different rules-based policies for different users and groups.

CYREN Inbox Security

A New Vision for Email Security

Inbox Detection and Reponse (IDR) is an emerging technology area which allows organizations to apply a defense-in-depth paradigm to email security. Instead of only attempting to prevent an email-initiated attack at the perimeter, with IDR enterprises can now add a post-delivery layer of phishing security. IDR can also aid incident response by:

1. Alerting email administrators for immediate investigation
2. Exporting all IOC and incident artefacts to your SIEM for wider use by the SOC analysts
3. Learning from incidents and user behaviours – using past events to feed machine learning algorithms, thus enabling prediction and prevention of future phishing and other advanced threats

Cyren Inbox Security is an IDR solution that is part of a complete email protection SaaS platform, including our secure email gateway service, advanced threat protection capabilities, and email archiving.

www.Cyren.com

sales@cyren.com

25B
Security Transactions Daily

1.3B
Users Protected

300M
Threats Blocked Daily

CYREN

CYREN **INBOX** SECURITY

Enterprise Security SaaS

CYREN Inbox Security

ENHANCED PHISHING PROTECTION

- Real-time URL access simulation
- Impostor protection
- BEC detection
- Cloud sandbox array

CONTINUOUS DETECTION

- Persistent mailbox re-scanning
- Mailbox Behavior Analysis
- Smart clustering *(polymorphic emails)*

AUTOMATED REMEDIATION

- Granular remediation policies
- Cross-organization remediation
- Incident and case management
- Detailed forensics (exportable)

CROWDSOURCED USER DETECTION

- Scan/report phishing add-in
- Gamification
- Virtual SOC *(Cyren Security Lab)*
- Simulated phishing attacks

THE MAIN CAPABILITIES OF THE CYREN INBOX SECURITY SERVICE ARE:

Enhanced Phishing Protection

CIS uses a broad set of Cyren's cloud computing and security technologies to identify today's evasive phishing and deliver the most advanced detection capabilities, including machine learning, recurrent pattern detection, IP reputation, heuristic clustering, natural language processing, cloud sandboxing and impostor protection. Cyren's threat visibility is unsurpassed, with our global security cloud processing 25 billion email and web security transactions every day, and identifying 9 new threats and blocking over 3,000 known threats each second.

Continuous Detection

Cyren Inbox Security protects from new, previously unknown threats by continuously scanning every email in every user's mailbox. It monitors behaviours and user interactions in the mailbox and identifies anomalies. All of this data is then correlated to determine whether an email is malicious and an action should be taken.

Automated Remediation

CIS's automated remediation and incident management capabilities ensure that threats are removed from your organization quickly and comprehensively via automated, cross-enterprise remediation of phishing outbreaks, removing suspicious messages from ALL infected mailboxes across the organization. A policy-based remediation framework supports a broad set of actions including tag and deliver, move to folder, delete, and send alert, reinforced by robust incident and case management workflow and extensive IOC and forensics information for rapid response and analytics.

Crowdsourced User Detection

Cyren's service includes a simple to install and use Outlook plugin that removes much of the burden of user support from the IT help desk and incorporates the "wisdom of the crowd" to identify and protect from a phishing attack. Any user can perform an automated, on-demand scan of any email they believe suspicious at the click of a button, and immediately receive results. If the response is negative and the user disagrees, the user can click to send the email in question to the Cyren Security Lab for security analyst review. If the on-demand scan or analyst review results in the email being reclassified as suspicious, it will be automatically remediated across all user inboxes. All forensics data is made available for any needed further investigation.