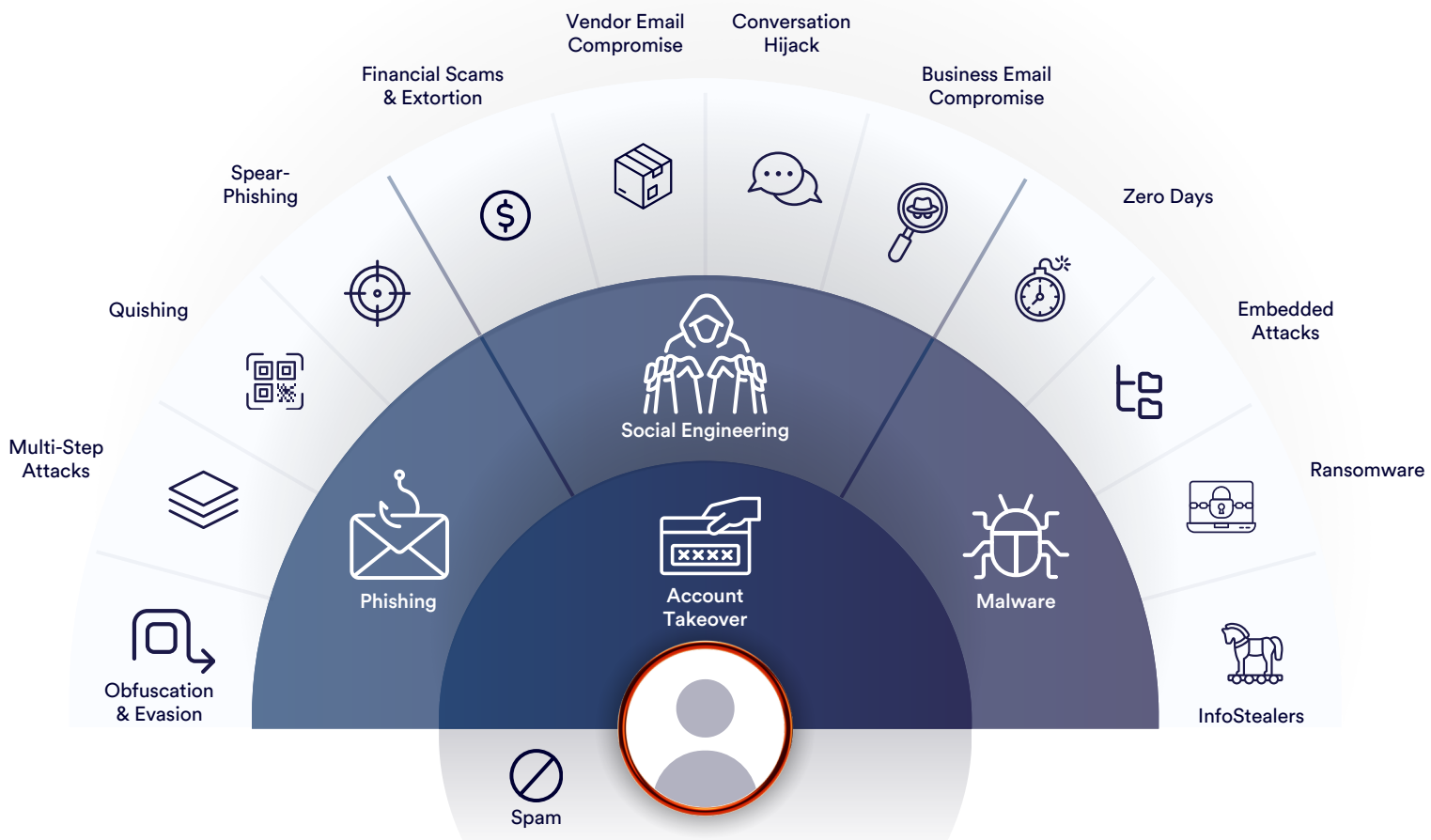


TECHNICAL DATASHEET

# Advanced Email Security

Protect More. Manage Less.

Email is by far the most attacked channel in the user's workspace. Organizations of all sizes are targeted by zero hour phishing attacks, GenAI-fueled social engineering schemes, and highly evasive malware. As **threat actors** continue to innovate and introduce new delivery techniques and attack vectors (e.g. QR codes), **defenders** face significant challenges in optimizing detection levels while juggling between limited cloud point solutions and legacy gateways that generate added overhead, false positives and management hassle.



## Powered by AI. Empowered by People.

**Perception Point Advanced Email Security** is a leading integrated Email Security Platform (ESP) designed to provide enterprise-grade protection against the wide range of email threats for Microsoft 365, Google Workspace and other cloud or on-prem services. Perception Point employs multi-layered threat prevention, leveraging Large Language Models (LLM), computer vision, patented dynamic scanning and anti-evasion algorithms to detect and neutralize email threats with ultimate precision before they reach their target inbox.

Fully managed and supported 24/7 by a natively included Human Incident Response service, the cloud platform alleviates email security overhead for SOC/IT teams and MSPs, cutting operational resources by up to 75%.

**Gartner**

2019-Present

Email Security Market Guide  
Representative Vendor

F R O S T  
&  
S U L L I V A N

2024

Frost Radar™ for Email Security  
Innovation & Growth Leader

**kuppingercoie**  
ANALYSTS

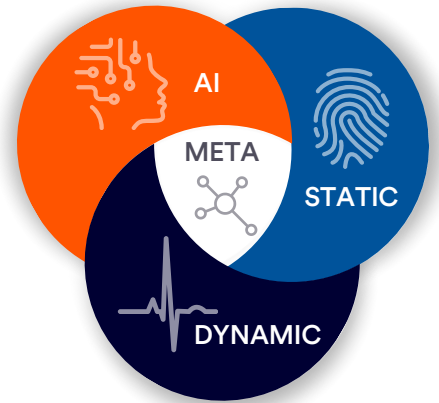
2023

Email Security Leadership Compass  
Overall Leader

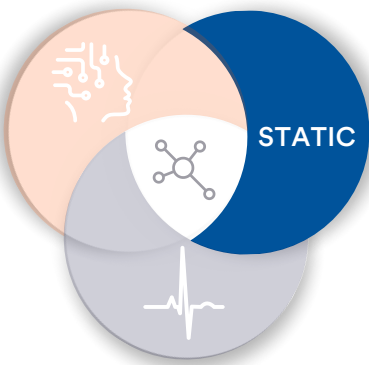
# Protect More. Prevention at First Sight.

Advanced Email Security positions itself between the threat and the employee's inbox, leveraging a multi-layered detection framework for comprehensive protection against a wide range of email-borne threats. Perception Point uniquely combines artificial and human intelligence with static and dynamic analysis to deliver unmatched defense against known, unknown, and payload-less email threats.

As the only fully Managed Email Security Platform, Advanced Email Security not only leverages cutting-edge tech but also offers companies of all sizes with a robust Incident Response service to dramatically reduce the required resources and time to deliver enterprise grade email protection.

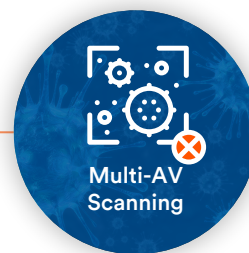


**Threat Actors use GenAI and human expertise to breach organizations – Perception Point uses them to protect yours.**



## STATIC ANALYSIS

Combining proprietary detection engines and threat intelligence, Perception Point examines code, files, URLs and email senders, utilizing market-leading reputation and anti-spam filters to swiftly flag and filter out junk messages and known attacks. The static layer employs authentication protocols (DMARC, DKIM, and SPF) and reputation checks to instantly verify senders integrity. It incorporates best-in-class signature-based AV engines along with multiple threat intelligence sources and in-house algorithms to identify known malicious patterns, indicators of compromise (IOCs), and complex signatures.



State Of The Art Technology. We did a very detailed evaluation about 15+ email security solutions that can be plugged into Microsoft 365 and EOP. The vendor was new to us but we compared capabilities in a very fact based approach. The solution showed both in prevention capabilities and in Incident response support capabilities the best results on the market.”

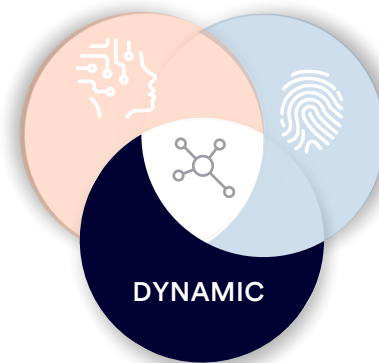


4.9 ★★★★★

-Security Architect, Red Bull

## DYNAMIC ANALYSIS

Detonating attachments and URLs in a unique proactive manner to effectively prevent unknown and highly evasive threats. Leveraging a patented dynamic scanning engine that ensures every piece of content's behavior is analyzed with minimal latency, while avoiding the common delays found in traditional sandbox solutions. Proprietary anti-evasion algorithms simulate end-user interactions with the content to uncover and neutralize threat actors' evasion maneuvers and deeply embedded attacks. Real-time analysis of web pages' behavior provides inline detection of zero hour malicious payloads and spear phishing attempts.



### Recursive Unpacker (Anti-Evasion)

Executes user-like actions to uncover and neutralize sophisticated evasion techniques that easily circumvent legacy and point solutions. It recursively extracts embedded files and URLs at any level deep down to the nested malicious payload (archive files, PDFs, LNK files, password-protected, clickable elements on webpages, etc.).

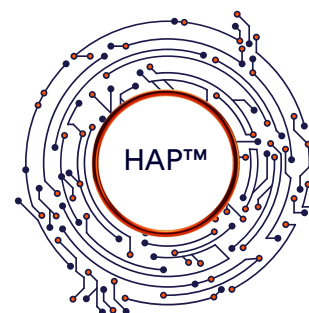


### Dynamic URL Analysis

In-line dynamic analysis of URLs offers real-time threat detection with reduced false positives, enhanced user experience and without rewriting the URLs. Perception Point browses to the links found within the email body/file attachments to catch zero hour threats using a myriad of advanced AI detection models (see "AI Analysis").

## HAP™: Fast and Precise

Perception Point's patented Hardware Assisted Platform™ revolutionizes threat prevention, emulation and detonation with near-real-time dynamic scanning, processing malicious files and URLs to a clear deterministic verdict in an average of just 15 seconds - far surpassing the speed and precision of traditional dynamic scanning and virtualization methods.

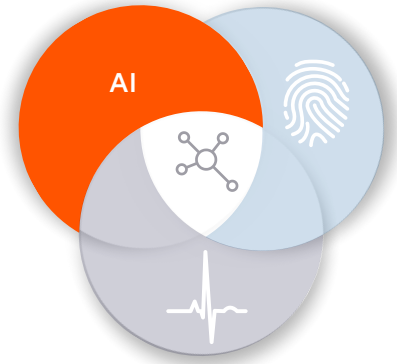


### Key Features:

- **CPU-level Anomaly Detection:** Utilizes Intel Processor Tracing to monitor and detect deviations from the legitimate execution flow of applications and prevent hijacking attacks.
- **Dropped File Scanning:** Analyzes files created or modified during execution to catch malware attempting to evade initial detection.
- **Syscall Analysis:** Uses ML to assess system calls for signs of anomalous activity, detecting threats at the OS level.
- **Memory Analysis:** Captures and compares runtime memory against known malware signatures to identify in-memory threats.
- **Network Analysis:** Inspects network traffic for abnormal activities and potential data exfiltration, highly effective against C2 communications.
- **Ransomware Activity Detection:** Monitors for encryption and content deletion attempts.
- **Built-in Anti-Evasion:** Employs user behavior emulation and machine-level techniques to analyze even the most evasive malware - undetected.

## AI ANALYSIS

Blending machine learning algorithms, computer vision and Large Language Models (LLMs) to autonomously identify social engineering and “payload-less” threats that easily circumvent common ESPs. By analyzing the email content, context, visuals and sender behavior anomalies, the AI layer detects zero hour phishing attempts, Business Email Compromise (BEC), supply chain attacks, vendor impersonation and spoofed brands.



### Natural Language Processing & LLMs

Developed to **understand** your organization’s unique relationships and communication patterns.



#### GenAI Decoder

Recognizes AI-generated emails and malicious pattern similarity within textual content.



#### Subject Analyzer

Classifies email subjects using deep learning techniques.



#### Supply-Chain Identification

Analyzes business communication to automatically identify domains of your business partners and vendors.



#### Thread Hijack Protection

Prevents conversation hijacking and vendor impersonation via anti-spoofing correlation algorithms.



### Computer Vision Algorithms

Designed to **see through** advanced phishing and brand impersonation attacks.



#### Logo Recognition

Compares email/URL/ file screenshots, images, and favicons to known brands.



#### Quishing Protection

Extracts QR codes in emails or attachments to dynamically scan hidden URLs.



#### Two-Step Phishing

Examines “clean” web pages to identify clickable elements for further scanning.

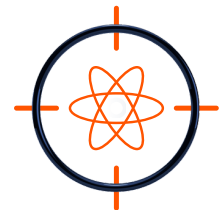


#### URL-Obfuscation Detection

Detects URL evasion attempts and homograph attacks.

## GPThreat Hunter™: Putting the AI in EMAIL Security

Blending the precision of AI with the insight of human experts, Perception Point’s autonomous detection model\*, GPThreat Hunter™, powered by GPT-4, elevates threat detection and remediation to new levels.



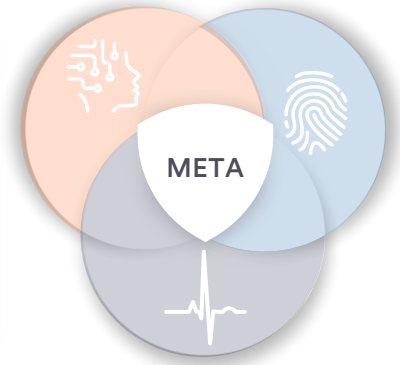
### Key Features:

- **Autonomous Precision:** GPThreat Hunter™ autonomously resolves ambiguous incidents with a level of speed and accuracy that has set a new industry standard.
- **Empowering Human Service:** By efficiently managing a significant volume of security cases, GPThreat Hunter™ allows Perception Point’s Incident Response experts to focus on the nuanced, complex investigations that may require a human touch.
- **Evolving with Every Catch:** Each interaction with GPThreat Hunter™ enriches the system, making our AI smarter and more responsive to new and emerging attacks.
- **Truly Explainable:** The GenAI model provides detailed explanations and reasoning for verdicts to educate admins and end-users, fostering resilience against future attacks.

## META ANALYSIS

Perception Point's Meta Analysis introduces groundbreaking innovation in email threat remediation, uniquely positioned to aggregate and analyze events and data points from other detection layers (Static, Dynamic, and AI) and across multiple workspace channels (email, browser, SaaS apps and EDRs). Meta Analysis provides security and IT professionals with unprecedented investigation and remediation capabilities of potential security incidents across the organization.

The XDR-like approach leverages a big data warehouse infrastructure and proprietary machine learning to set a new industry standard for email security.



### Multi-channel Event Detection

Cross-analysis of email, web browsing, and other channels allows for detection of multi-vector threats (i.e. phishing that transitions from email to web).



### Account Takeover (ATO) Protection

Detecting compromised user inboxes using contextual signals and anomalies that indicate malicious activity.



### Holistic Threat View

Aggregating insights from various engines to offer a complete picture of sophisticated threats. This enables security teams to understand the full context of an attack, including its origin, methods, and targets, leading to more informed and effective responses.



### Graphical Representation

The platform uses advanced graphical representations to visualize threat data, making it easier for analysts to interpret and act on the information.



## THE ULTIMATE COMBO: EMAIL + BROWSER SECURITY

Secure your users and data with Perception Point's browser & email security synergy. Combine **Advanced Email Security** with the **Advanced Browser Security** extension to elevate threat prevention to new heights.



### Detecting the Most Evasive Threat

Scanning threats from the user's point of view renders the most advanced evasion techniques ineffective. Geofencing, CAPTCHAs, password-protection or time-based tactics designed to evade detection are prevented in real-time once the user encounters the malicious website/payload on the browser. Contextual evidence gathered from email (e.g. sender, domain, etc.) is leveraged to enhance detection and users' awareness of web-borne attacks - and vice versa.



### Tracing Attacks Back to Their Source and Identifying Impacted Users

Combining live browsing data with email events allows security professionals to easily and visually "connect the dots" and investigate the impact of an attack or an ongoing incident: Which users inserted their credentials? Who clicked/downloaded the malicious content? What unsanctioned apps do my employees use?



### Rapid Remediation of Security Incidents + Enhanced Email DLP

Faster, more efficient remediation of "phished" users and Account Takeover incidents with login events monitoring and visibility. Weaponized files or URLs scanned by the extension "in the wild" get automatically remediated from all inboxes. Warn or prevent end users from email-related data exfiltration, audit sensitive email attachments (e.g. employee offboarding) and receive email DLP alerts.

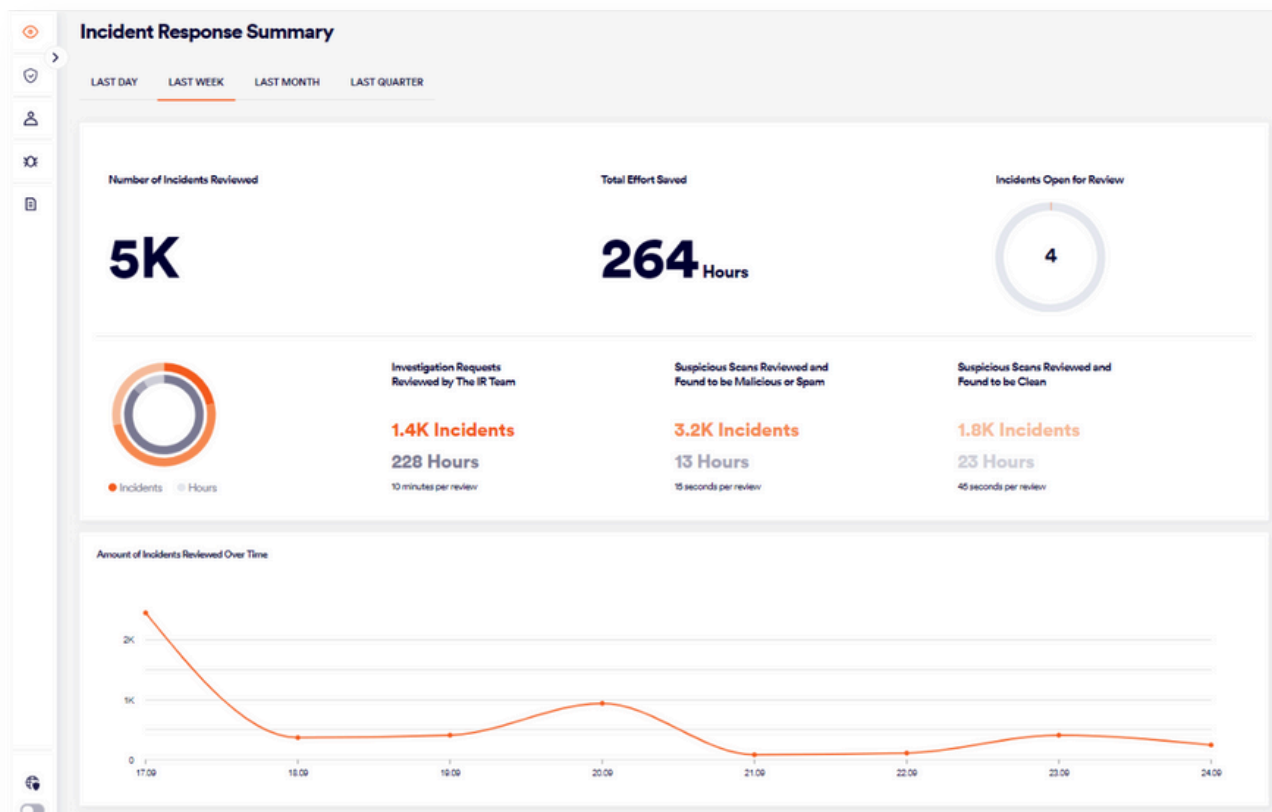
# Manage Less. Managed Incident Response Service.

Perception Point is the only solution on the market to natively offer managed Incident Response services, at no additional cost. Acting as a 24/7 extension of your IT/security team, providing continuous monitoring, analysis, and remediation of threats, the team of cybersecurity experts handle all ongoing email security activities, including remediation and containment of incidents, reporting, and more.



## Key Benefits:


- **Detection Optimization:** Continuous fine-tuning of detection and policies based on real-world attacks.
- **Active False Positive/Negative Hunting:** Our human experts adjust verdicts and take appropriate action to address false positives and negatives so you don't need to.
- **Resource Saving and Efficiency:** Reduces overhead and frees up your SOC teams to focus on strategic tasks while Perception Point manages day-to-day email security tasks.
- **Expert Support:** Provides access to advanced cybersecurity expertise, enhancing overall security posture.

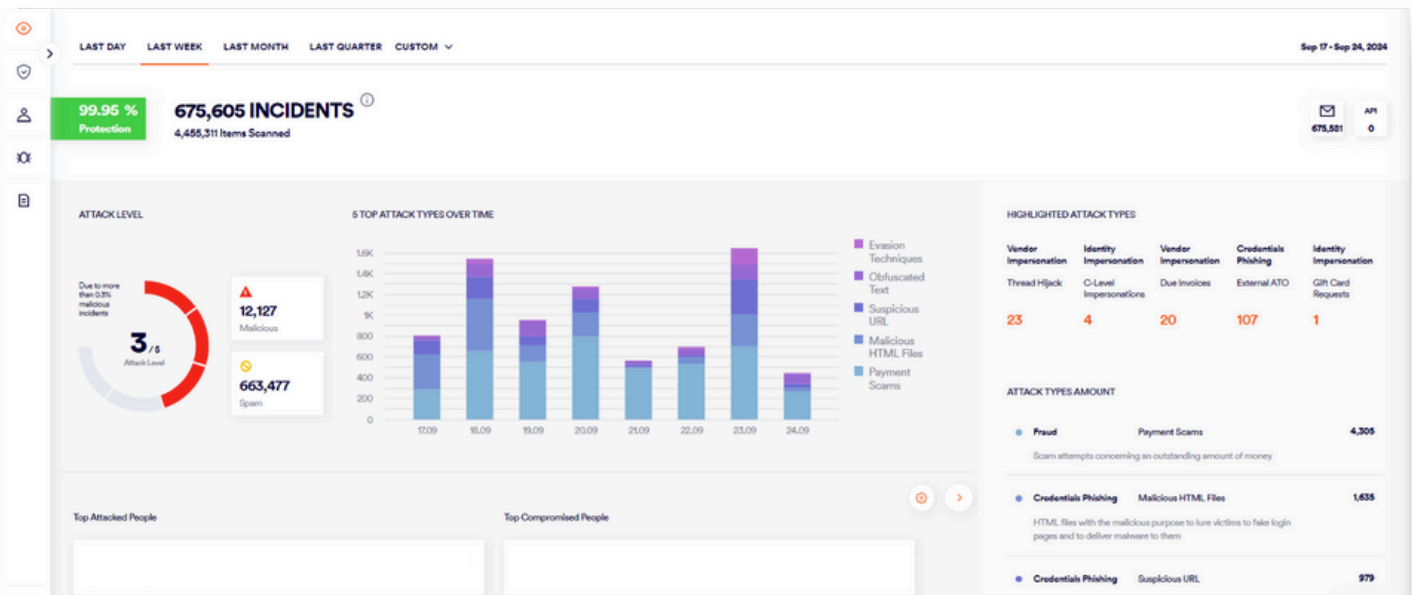


# The X-Ray

Comprehensive management console to control, customize and monitor your organization's email security posture.



- Advanced set of investigation and reporting tools provide comprehensive insights into the nature and scope of threats your organization faces.
- Detailed forensic analysis for each malicious email scan, including cross-referencing of email metadata, screenshots, attachment behavior, and URL interactions, MITRE ATT&CK® matrix and more.
- Holistic view of the threat landscape of your email security posture with actionable data, such as most attacked users, top impersonated vendors, granular details and visual attack flows of all security events.
- Customizable detection and alerting preferences.
- Multi-language support on user interfaces: 



## ELIMINATE SECURITY BLIND SPOTS WITH 360° CHANNEL COVERAGE

Beyond Advanced Email Security, Perception Point provides advanced threat protection to your standard browsers, cloud collaboration & messaging apps, storage platforms, CRMs, proprietary apps and unsourced file streams and uploads.

All modules can work separately or together to provide maximal protection via a X-Ray, displaying threats and live incident insights all in one place.



# Uncompromising Email & Workspace Security



## Superior Prevention

AI-powered threat detection with proven accuracy of 99.95%. 100% of the email traffic is scanned dynamically preventing malicious emails from reaching the inbox.



## Workspace Security-Ready

Leveraged with Advanced Browser Security and cloud app protection, to holistically protect your user-centric attack vectors against advanced threats.



## Seamless Cloud Deployment

Deployed within minutes, with zero-fuss to IT teams or user experience designed to leverage the full speed & scale of the cloud.



## Managed Email Security

An all-included incident response & support service alleviates the overhead and fully supports your team 24/7, to provide enterprise-grade email security and save up to 75% in operational resources.

## Advanced Email Security - Available On:








## Regulatory Compliance





# About Perception Point

Perception Point is a leading provider of AI-powered threat prevention solutions that safeguard the modern workspace against sophisticated threats. The unified security solution protects email, web browsers, and SaaS apps. By uniquely combining the most accurate threat detection platform with an all-included managed incident response service, Perception Point reduces customers' IT overhead, improves user experience, and delivers deep-level cybersecurity insights.

Deployed in minutes, with no change to the organization's infrastructure, the cloud-native service is easy to use and replaces cumbersome, traditional point systems. Perception Point proactively prevents phishing, BEC, ATO, malware, spam, insider threats, data loss, zero-days, and other advanced attacks well before they impact the end-user. Fortune 500 enterprises and organizations across the globe are protecting more and managing less with Perception Point.