Communicate Better©

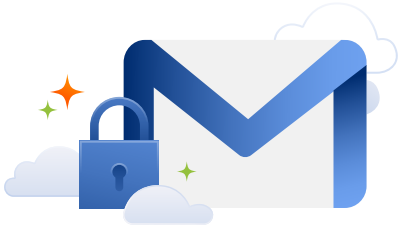
IT • MOBILE • TELEPHONY • TELEMATICS

Advanced Email Security

For Acronis Cyber Protect Cloud

Prevent Email Threats with Cloud Security

Acronis Cyber Protect Cloud helps block email threats – including spam, phishing, business email compromise (BEC), malware, advanced persistent threats (APTs), and zero-days – before they even reach your Microsoft 365, Google Workspace, Open-Xchange, or on-premises mailboxes.



STOP PHISHING AND SPOOFING ATTEMPTS

Minimise email risks with powerful threat intelligence, signature-based detection, URL reputation checks, unique image-recognition algorithms, and machine learning with DMARC record checks.

CATCH ADVANCED EVASION TECHNIQUES

Detect hidden malicious content by recursively unpacking attached or embedded files and URLs, separately analysing each with dynamic and static detection engines.

PREVENT APTS AND ZERO-DAY ATTACKS

Prevent advanced threats that evade conventional defenses with Perception Point's unique CPU-level technology, which blocks exploits before the malware is released and delivers a clear verdict in seconds.

Protect your emails with unmatched detection technologies

Spam filter

Block malicious communications with anti-spam and reputation-based filters, leveraging the combined data of several market-leading technologies.

Anti-evasion

Detect malicious hidden content by recursively unpacking the content into smaller units (files and URLs) which are then dynamically checked by multiple engines in under 30 seconds – much faster than the 20+ minutes of legacy sandboxing solutions.

Threat intelligence

Stay ahead of emerging threats with the combined threat intelligence of six market-leading sources and Perception Point's unique engine that scans URLs and files in the wild.

Static signature-based analysis

Identify known threats with best-of-breed signature-based antivirus engines enhanced with a unique tool by Perception Point to identify highly complex signatures.

Anti-phishing engines

Detect malicious URLs based on four leading URL reputation engines in combination with Perception Point's advanced image recognition technology to validate the legitimacy of URLs.

Anti-spoofing

Prevent payload-less attacks such as spoofing, look-alike domains, and display name deception with unmatched precision through machine-learning algorithms with IP reputation, SPF, DKIM, and DMARC record checks.

Next-generation dynamic detection

Stop advanced attacks such as APTs and zero-days with Perception Point's unique, CPU-level analysis that detects and blocks them at the exploit stage by identifying deviations from normal execution flow during runtime.

X-ray insights

Leverage a holistic view of the threat landscape across organizations with forensics data for each email, proactive insights on threats seen in the wild, and analysis of any file or URL on which the service delivery team needs forensics.

Incident response service

Gain direct access to cyber analysts who act as an extension of your service delivery team. Monitor all customer traffic and analyze malicious intent with ongoing reporting and support, including handling false positives, remediating, and releasing when required.

Reporting

Demonstrate your value to customers with easily accessible and manageable datasets, as well as weekly, monthly, and ad-hoc reports from the Incident Response Team.

Ad-hoc email analysis for end-users

Enable end-users to directly consult with Perception Point's email security experts for suspicious emails before taking reckless action.

End-user contextual help

Flag emails with customizable banners based on policies and rules to provide end-users with additional contextual information to increase their security awareness.