Why

CELLOPOINT
Defender

Cellopoint Defender uses artificial intelligence and machine learning technologies to learn your organization's known good and spot anomalies through senders' identity, intention, behavior, and relationship, effectively blocking advanced and targeted email threats.

Cellopoint offers a next-generation cloud-native email security solution and is proud to be the only vendor in the Asia Pacific region recognized by Gartner as a representative vendor in the Integrated Cloud Email Security category in the 2023 Gartner Market Guide for Email Security.

Cellopoint Defender + Microsoft 365
Protect against the full spectrum of email attacks together

Effectively stop phishing, ransomware, and BEC scams

CELLOPOINT
RECOGNIZED IN THREE GARTNER REPORTS

Gartner
2022 Hype Cycle
for Endpoint Security

Gartner
2023 Gartner
Market Guide
for Email Security

Gartner
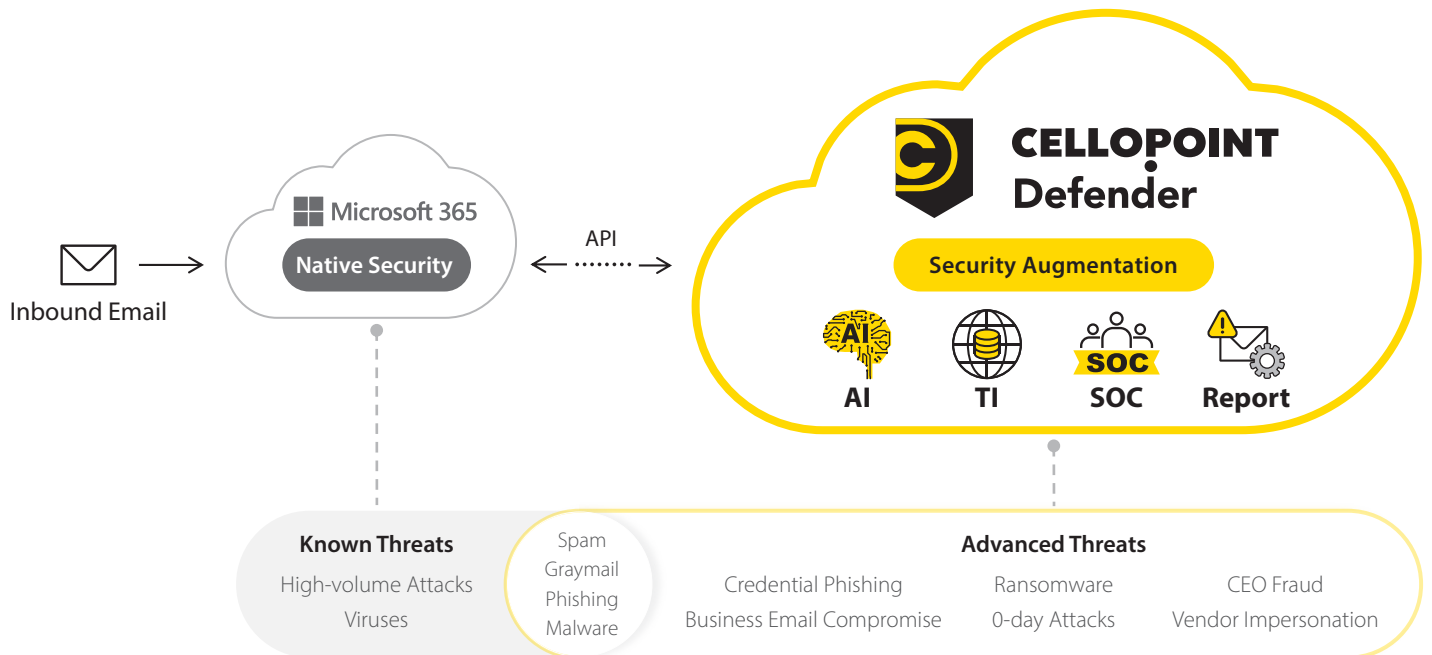2023 Gartner Vendor
Identification Tool
for Email Security

1. Challenges

Top 3 Email Security Challenges for Security Teams

1 As cybercriminals constantly evolve tactics and techniques, novel attacks, including zero-day phishing, ransomware, and business email compromise (BEC) scams are on the rise in both frequency and damage.

2 The adoption of Microsoft 365 is growing rapidly. However, relying solely on Microsoft's native email security controls could be risky as Microsoft is not 100% effective in blocking all email threats.

3 Legacy secure email gateways (SEG) rely on rule-based detection approaches which are not effective at addressing modern advanced email attacks. SEGs are also complex to deploy and maintain.

2. Our Solution

Cellopoint Defender for Microsoft 365 seamlessly integrates with Microsoft via API and can be deployed in minutes. It uses AI-powered, cloud-native approach and combines threat intelligence, Cellopoint SOC team analysis, and false positives and missed attack reports to identify and block advanced email threats—which often bypass Microsoft and reach your mailbox.

Inbound Email

Microsoft 365
Native Security

API

CELLOPOINT Defender

Security Augmentation

AI   TI   SOC   Report

Known Threats
High-volume Attacks
Viruses

Spam
Graymail
Phishing
Malware

Advanced Threats
Credential Phishing   Ransomware   CEO Fraud
Business Email Compromise   0-day Attacks   Vendor Impersonation

3. Features

AI-Powered Detection

Leverages behavioral AI and machine learning model to analyze senders' identities, intentions and behaviors. Effectively identifies and stops phishing, BEC and advanced email attacks.

API-Enabled Architecture

Seamlessly integrates with Microsoft 365 via API. Easy implementation in minutes and fast protection without requiring email routing or MX record changes.

Cloud Native Protection

Enables high scalability and agility. Automatically learns about organizations' user titles/ groups and communication patterns to profile known good behaviors and identify anomalies.

4. Capabilities

Effectively detect M365-missed attacks

Our AI-based email security solution uses known good models to identify anomalies in sender identity, intention, and behavior. We complement Microsoft 365's native email security with comprehensive detection mechanisms including threat intelligence analysis, SOC team analysis, and user and admin reporting features, blocking advanced threats like zero-day phishing, ransomware, and BEC scams missed by Microsoft 365.

Auto investigate and remediate your mailboxes

Cellopoint Defender's Auto Investigation and Remediation (AIR) automatically investigates all inboxes within your organization when a new threat is detected. AIR identifies hidden threats by comparing patterns of the new threat and based on the policies, will auto remediate them accordingly, such as adding warning banners and deleting or moving emails to the junk folder to reduce the security team's investigation time and their burden.

Auto remediate M365 false positives

Cellopoint Defender not only scans the emails in the inbox but also scans the emails in the junk folder to detect safe emails mislabeled as spam by M365. If a safe email (false positive) is detected in the junk folder, Cellopoint will auto remediate it by moving it to the inbox and adding a low-risk warning banner. This ensures that important emails are not missed, improving the organization's efficiency and productivity.

Provide educational warning banners

Cellopoint Defender provides recipients with contextual warning banners containing clear and concise information about potential threats, which can help increase their email security awareness and reduce organizational risks. Additionally, recipients can report suspicious emails directly through the banners, allowing for rapid adjustments to detection effectiveness and saving time for security teams.

Granular Visibility into Risk

Cellopoint Defender provides detailed reports and allows security teams to seamlessly access communication-focused insights and intelligence: e.g. top threats, most targeted VIPs, and most attacked employees.

Learn what email threats are in your Microsoft 365's mailboxes

Apply for a Back Scan PoC today to:

1. Get a free Back Scan PoC report to have an overview of your organization's email hygiene

2. Discover email threats that got past your existing email security protection

3. Identify the most vulnerable VIPs or employees in your organization

"

5.0 ★★★★★

Outstanding Next Gen Email Security Solution

Consumer Goods Industry | **IT Security and Risk Management**

"

5.0 ★★★★★

Great email security vendor to work with!

Hardware Industry | **IT**

"

5.0 ★★★★★

AI solution for email security and archiving

Manufacturing Industry | **IT**

CELLOPOINT
● Secure Your Email

Cellopoint is a leader in next-generation email security solutions, using AI-based technology to protect users against advanced email attacks such as phishing, ransomware, and BEC scams.

Contact Us   +886-2-89692558 | sales@cellopoint.com

Visit our website for more information.
www.cellopoint.com