GROUP-IB

Business Email Protection

Detect and disrupt cyber threats with unprecedented speed and accuracy to reduce your cyber risk

Email Protection

EMAILS ANALYZED

MALICIOUS EMAILS

Endpoint protection

ENDPOINT DETECTION AND RESPONSE

Detect attacks on the host level, leveraging intelligence data, signature and behavioral analysis, and malware detonation capabilities. Prevent and respond to threats.

Network protection

NETWORK RESEARCH & PROTECTION

- East-West and North-South traffic analysis
- Cnc, covert channels, and lateral movement detection
- Visibility in communication and traffic metadata

Emails Processing Time Statistics

This week

519.4 k All Emails

● 0 – 120 sec	448765
● 120 – 240 sec	34458
● 240 – 360 sec	15964
● 360 – 480 sec	5081
● 480+ sec	15104

Trending malware

Updated · 19:15

Data sheet

Business Email Protection

Preventing credential-based ransomware attacks
at the earliest possible stage

The challenge

Ransomware often seems to strike out of the blue, yet breaches usually begin much earlier — when an infostealer is delivered through a trusted email account. Attackers compromise supplier or partner mailboxes and continue seemingly genuine threads, often using AI to help them sound more convincing. Once they gain access to the mailbox, criminals profile the contact list, send simple phishing emails to low-value users, and deploy infostealers to high-value targets whose credentials unlock privileged access.

Users are made to believe they are interacting with a familiar sender. Meanwhile, the infostealer extracts browser passwords, cloud tokens, VPN credentials, and email histories. The stolen details, which later appear in infostealer logs and darknet marketplaces, are the most common source of credentials used in human-operated ransomware, as confirmed by Group-IB Threat Intelligence.

Given that the email originates from a trusted relationship, most email security tools treat it as legitimate. Traditional email defenses rely on reputation scoring, trusted-sender rules, and static scanning. They rarely analyze real attachment behavior, assess conversation context, or check whether the sender's account appears in compromised-account or infostealer datasets. Such oversights create blind spots that allow infostealer campaigns to establish an early foothold inside the organization, later used by ransomware affiliates.

84%

increase in global infostealer distribution campaigns year over year

30%

of compromised systems found in infostealer logs are enterprise devices

46%

of compromised accounts mix personal and corporate login

The solution

Group-IB Business Email Protection focuses on the earliest stage of an attack by evaluating every email with behavioral detection, real-world detonation, and continuously updated threat intelligence. Sender identity is validated against compromised-account datasets, collections of leaked credentials, and infostealer distribution intelligence that is updated hourly. Thread logic and communication patterns are analyzed to identify unusual continuity or AI-generated imitation.

Attachments (including encrypted archives) are decrypted, unpacked, and executed in the Malware Detonation Platform. The platform mirrors real corporate environments by morphing profiles, regional exit nodes, and dynamic execution parameters that expose behavior able to evade basic sandboxing. URLs undergo time-of-click detonation to reveal delayed activation tactics. Delivered emails remain under retrospective monitoring, which means that emerging threats are removed automatically.

By intervening when credential theft would occur, Business Email Protection breaks the chain of events required for reconnaissance, lateral movement, and ransomware deployment.

Value

Strengthen early-stage ransomware prevention
Expose infostealers lurking within trusted conversations and everyday business files.

Reveal threats overlooked by legacy tools
Analyze embedded loaders, encrypted archives, delayed activation, QR-based lures, and prompt-injection attempts in a realistic execution environment.

Enhance security without increasing complexity
Deploy through MX or API integration and support investigations with clear behavioral reporting and automatic post-delivery remediation.

Feature details

Detection of compromised senders and BEC

- Intelligence-led detection of compromised supplier and partner accounts
- Analysis of thread continuity and communication structure
- Detection of AI-generated imitation

Detection of malware and infostealers

- Realistic detonation of more than 500 file types in an adaptive environment
- Password extraction from email bodies, attachments, and neighboring emails in the same thread
- Exposure of hidden loaders and infostealer behavior
- Memory, process, and command-and-control analysis

Protection against URL and web threats

- Link rewriting and time-of-click detonation
- Detection of delayed activation
- Analysis of QR codes, redirects, calendar links, and concealed payload paths

Administration and visibility

- Reports mapped to MITRE ATT&CK®
- Threat intelligence enrichment for senders and indicators
- Post-delivery threat removal
- Policy customization for high-risk users

Use cases

Compromised supplier thread

Threat actors used AI-generated messages to continue a legitimate email thread with a clean-looking Excel file. Business Email Protection detonated the file and revealed the infostealer payload.

Delivery of an encrypted archive

Threat actors used a password-protected ZIP payload with the password stored in a previous message. Business Email Protection extracted the password automatically, decrypted the archive, detonated the file, and blocked the attack.

Internal email compromise

Malicious emails were sent from a compromised company mailbox to other employees. Business Email Protection analyzed internal email traffic, detonated attachments and links, and prevented lateral spread within the organization.

AI-driven hijacking of an email thread

Threat actors sent emails drafted using stolen mailbox history to mimic the sender's writing style. Business Email Protection detected unnatural thread logic and blocked the message.

Delayed weaponization

Threat actors used URLs that remained clean at delivery but became activated during business hours. Time-of-click detonation identified the payload and prevented credential theft.

QR-code and prompt-injection attacks

Threat actors used payloads hidden behind QR codes or instructions for AI-enabled mail clients. Business Email Protection downloaded, detonated, and stopped the threat.

GROUP-IB

Group-IB is a creator of cybersecurity technologies to investigate, prevent and fight digital crime.

1,550+	Successful investigations of high-tech crime cases
500+	Employees
60	Countries
$1 bln+	Saved by our client companies through our technologies
#1*	Incident Response Retainer vendor
11	Unique Digital Crime Resistance Centers

*According to Cybersecurity Excellence Awards

Global partnerships

- INTERPOL
- EUROPOL
- AFRIPOL

Recognized by top industry experts

- FORRESTER®
- Aite Novarica
- KuppingerCole ANALYSTS
- Gartner®
- IDC
- FROST & SULLIVAN

Fight against cybercrime

GROUP-IB.COM
INFO@GROUP-IB.COM

APAC
+65 3159 4398

EU & NA
+31 20 226 90 90

MEA
+971 4568 1785