CELLOPOINT
Secure Your Email

這封信你敢點嗎？
揭密社交工程郵件陷阱

Ken Yu 游文豪 / 專案經理

Agenda

- 網路犯罪與主要攻擊型態
- 電子郵件環境的風險與常見攻擊類別
- 電子郵件攻擊實務案例
- 電子郵件偽冒攻擊與防治方法
- Cellopoint 解決方案

網路犯罪與主要攻擊型態

CELLOPOINT
Secure Your Email

IC3 網路犯罪報告

- 美國 FBI 網路犯罪投訴中心（IC3, Internet Crime Complaint Center）
  https://www.ic3.gov/AnnualReport/Reports

- 網站內容提供 IC3 每年的「網路犯罪報告（Internet Crime Report）」：

網路犯罪報告內容涵蓋範圍
分析美國接收到的網路犯罪投訴資料，包括**詐騙、勒索病毒、商業電子郵件詐騙（BEC）、社交工程攻擊**等統計數據與趨勢。
各年度網路犯罪的**總損失金額、案件數量**，以及常見犯罪手法的變化。
提供**不同產業**（如企業、醫療、教育、金融等）受害情形。
FBI 提出給企業與個人的**資安建議**，包括預防方法與應對指南。
數據來自 IC3 所收到的**網路犯罪投訴表單**（如詐騙受害者主動通報）整理而來。

網路犯罪的受害人與損失（申訴數量）

BY COMPLAINT COUNT

Crime Type	Complaints	Crime Type	Complaints
Phishing/Spoofing	193,407	Harassment/Stalking	11,672
Extortion	86,415	Real Estate	9,359
Personal Data Breach	64,882	Advanced Fee	7,097
Non-Payment/ Non-Delivery	49,572	Crimes Against Children	4,472
Investment	47,919	Lottery/Sweepstakes/ Inheritance	3,690
Tech Support	36,002	Data Breach	3,204
Business Email Compromise	21,442	Ransomware	3,156
Identity Theft	21,403	Overpayment	2,705
Employment	20,044	IPR*/Copyright and Counterfeit	1,583
Confidence/Romance	17,910	Threats of Violence	1,360
Government Impersonation	17,367	SIM Swap	982
Credit Card/Check Fraud	12,876	Botnet	587
Other	12,318	Malware	441
*Descriptor***			
Cryptocurrency	149,686		

- 詐騙釣魚／偽冒攻擊：偽裝成合法單位誘騙帳密或點擊惡意連結。
- 勒索詐騙：以恐嚇或假冒手法勒索金錢或行動。
- 個人資料外洩：個資遭未授權存取或外洩。

網路犯罪的受害人與損失（金額損失）

BY COMPLAINT LOSS

Crime Type	Loss	Crime Type	Loss
Investment	$6,570,639,864	Extortion	$143,185,736
Business Email Compromise	$2,770,151,146	Lottery/Sweepstakes/ Inheritance	$102,212,250
Tech Support	$1,464,755,976	Advanced Fee	$102,074,512
Personal Data Breach	$1,453,296,303	Phishing/Spoofing	$70,013,036
Non-Payment/Non-Delivery	$785,436,888	SIM Swap	$25,983,946
Confidence/Romance	$672,009,052	Overpayment	$21,452,521
Government Impersonation	$405,624,084	Ransomware *	$12,473,156
Data Breach	$364,855,818	Harassment/Stalking	$10,611,223
Other	$280,278,325	Botnet	$8,860,202
Employment	$264,223,271	IPR/Copyright and Counterfeit	$8,715,512
Credit Card/Check Fraud	$199,889,841	Threats of Violence	$1,842,186
Identity Theft	$174,354,745	Malware	$1,365,945
Real Estate	$173,586,820	Crimes Against Children	$519,424
*Descriptor***			
Cryptocurrency	$9,322,335,911		

- 投資詐騙：假投資機會誘導受害者投入大量資金。
- 商業郵件詐騙：假冒公司信件騙取匯款或機敏資料。
- 技術支援詐騙：冒充客服支援人員詐騙金錢或控制設備。
- 個人資料外洩：個資遭非法存取、洩漏、販售，錢財遭盜領。
- 勒索軟體攻擊：系統或檔案遭加密，需付贖金才能解鎖。

為何 Cybercrime 持續增加？

- ✓ 沒有實體上的風險
- ✓ 沒有地理位置限制
- ✓ 工作時間任你安排
- ✓ 法律不健全，難以制裁
- ✓ 成本低，高報酬 (一次開發，修改內容又可重複使用)
- ✓ 龐大的商機 (永遠有新的使用者可以進行詐騙)

看起來 這無疑就是一份理想工作

駭客對你的影響是什麼？

個人

- 信用卡號
- 身份證字號
- 護照號碼
- 各種帳密 (可進一步登入利用)
- 各種社交資訊
- 你的電腦設備

…

公司

- 內部人員資訊
- 交易訊息
- 駭入系統
- 破壞公司
- 洩漏訊息
- 竊取高階使用者權限
- 竊取資料庫
- 勒索
- DoS
- 獲取管理階層資訊

…

電子郵件環境的風險與常見攻擊類別

CELLOPOINT
Secure Your Email

各種攻擊散播途徑

Email

SMS

Social Media

Messaging

CELLOPOINT
Secure Your Email

千奇百怪的詐欺手法（1）

Advance fee schemes	先期費用詐騙
Apartment deposit scams	租屋押金詐騙
Bitcoin scams	比特幣詐騙
Bulk-mailing opportunities	大宗郵件詐騙
Business Email Compromise	商業電子郵件詐騙（BEC詐騙）
CEO wire fraud	假冒CEO電匯詐騙
Charity fraud	慈善機構詐騙
COVID-19 scams	新冠疫情相關詐騙
Credit card fraud	信用卡詐騙
Email chain letters	電子郵件連鎖信詐騙
Facebook impersonation scam (hijacked profile scam)	假冒臉書帳號詐騙（盜用帳號詐騙）
Fake antivirus software	假防毒軟體詐騙
Fake ransomware traps	假勒索軟體陷阱
Fake shopping websites	假購物網站詐騙
Fictitious charities	假慈善機構詐騙

千奇百怪的詐欺手法（2）

Fraud involving online auctions and classified ads	網路拍賣與分類廣告詐騙
Funeral and cemetery fraud	殯葬與墓地詐騙
GoFundMe scams	GoFundMe 募款詐騙
Greeting card scams	假賀卡詐騙
Health and life insurance fraud	健康與人壽保險詐騙
Identity theft	身分盜用
IRS scams	假冒國稅局詐騙（美國稅務詐騙）
Job offer scams	假求職/工作機會詐騙
Letter of credit fraud	信用狀詐騙
Loyalty points phishing scam	假冒集點或會員點數詐騙
Nigerian Letter or “419” Fraud	奈及利亞詐騙（419詐騙）
Online dating scams	網路交友詐騙
Overpayment online scam	超額付款詐騙
PayPal and money transfer fraud	PayPal 與匯款詐騙
Phishing and smishing	網路釣魚與簡訊釣魚詐騙

千奇百怪的詐欺手法（3）

Ponzi schemes, pyramid schemes, and multilevel marketing	龐氏騙局、金字塔詐騙與多層次傳銷
Prime bank note fraud	頂級銀行票據詐騙
Reverse mortgage scams	逆向房貸詐騙
Romance scams	**愛情詐騙**
Schemes that involve reducing credit card interest or debt	假借降低信用卡利率或債務的詐騙
Tech support online scams	**假技術支援詐騙**
Telephone solicitation fraud	電話推銷詐騙
Travel and vacation fraud	旅遊與度假詐騙
Unexpected winnings scam	意外中獎詐騙
Web service and credit card cramming	網路服務與信用卡強迫收費詐騙
Work-from-home schemes	在家工作詐騙
Illegal sports betting	非法體育賭博
Investment schemes such as pump-and-dump and scalping	**投資詐騙（如拉抬出貨、短線炒作）**

透過 Email 傳播的主要攻擊類型

- Malicious URL：點擊惡意連結造成帳密被盜、安裝惡意程式
- Malware：執行惡意程式造成檔案被加密、變成殭屍電腦
- Social Engineering：建立關係，執行惡意行為
- Insider：來自內部被駭使用者，收集情報、洩漏公司資料
- Spoofing：偽冒郵件欺詐內、外部，騙取資料與金錢
- Mixed：結合以上各種攻擊型態，更精細的攻擊

常見攻擊郵件型態

釣魚

Phishing

勒索

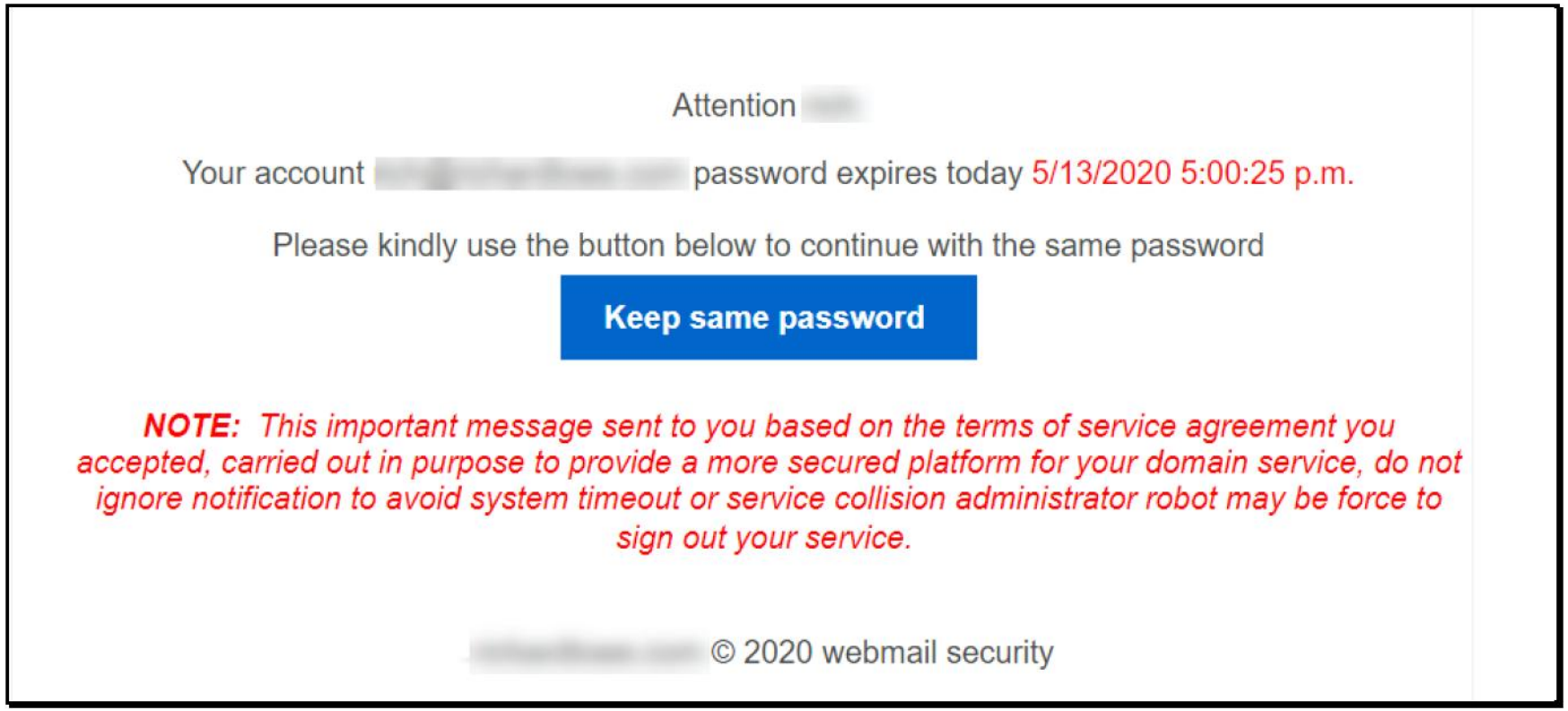
Ransomware

詐騙

Fraud

釣魚郵件基本要素

釣魚為網路詐騙、攻擊最常用的手段


Attention [redacted]

Your account [redacted] password expires today 5/13/2020 5:00:25 p.m.

Please kindly use the button below to continue with the same password

Keep same password

NOTE: *This important message sent to you based on the terms of service agreement you accepted, carried out in purpose to provide a more secured platform for your domain service, do not ignore notification to avoid system timeout or service collision administrator robot may be force to sign out your service.*

[redacted] © 2020 webmail security

Imitate

模仿已知的來源

Motivate

給予動機

Action

點擊連結、開啟附件、執行任何駭客要你做的動作

惡意郵件常見手法

結合社交工程，試圖操縱收件人，誘拐收件人去點擊惡意連結、開啟惡意檔案、提供機密資訊。

如何引誘收件人點擊連結、打開附件？

- 帳號停用與確認通知
- 帳單與交易確認
- 非法登入確認
- 軟體更新下載
- 你中毒了
- 樂透、中獎

惡意郵件常見手法

1. 虛構一個**情境**，營造很**緊急**的感覺。
2. 若不馬上處理就會有**嚴重後果**。（例如帳號要被關閉）
3. 給有限的選擇，提供**連結**、**附件**，告知開啟後可以解決問題。

What is BEC ?

BEC 是 Business Email Compromise 的縮寫

商業電子郵件詐騙：主要利用商業往來郵箱做詐騙

變臉詐騙：偽冒高階主管(CxO)，又叫 CEO Fraud

VEC：偽冒供應商(Vender) ，又叫 Supply Chain Fraud

BEC 攻擊剖析

準備 → 執行 → 行騙 → 收網

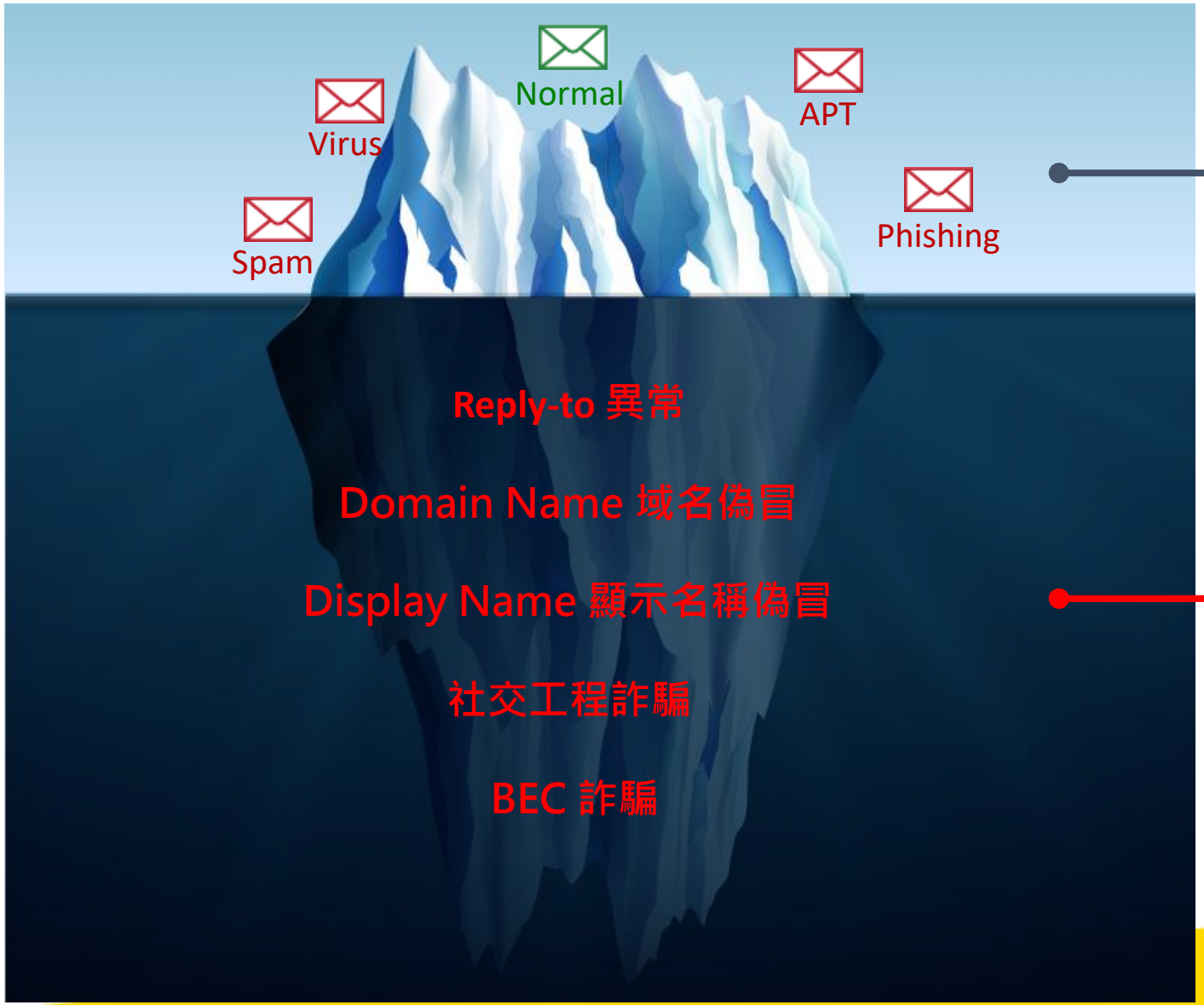
1. Build Target List
建立目標名單

2. Launch Attack
鎖定目標

3. Apply Social Engineering
利用社交工程手法釣魚獲取關鍵資訊

4.Reap Rewards
騙取財物或資料

郵件安全的現況



各位很熟悉

真的是現況嗎！？

冰山下
潛藏的風險

各種 Spoofing 比例

❶ Reply-to

52%

From Mary <mary@a.com>
To jennifer_lee@cellopoint.com
Subject 2019年08月應收帳款通知
Reply-to mary-a@gmail.com

❷ Display Name

36%

From 業務處長<sales@cellopoint.com>
To sales@cellopoint.com
Subject 請提交第三季度業務拓展計畫
Reply-to sales@xyz.com

❸ CEO/CFO Fraud

9%

From David CEO <david_wang@cellopoint.com>
To jennifer_lee@cellopoint.com
Subject 請立即處理匯款
Reply-to xyz@gmail.com

❹ Cousin Domain

1.9%

From 台灣微軟 <license@micr0soft.com>
To jennifer_lee@cellopoint.com
Subject 台灣微軟授權到期通知
Reply-to license@micr0soft.com

❺ Sender Account

0.9%

From 匯豐銀行 <notify@hsbc.com.hk>
To sales@cellopoint.com
Subject 匯豐銀行匯款通知
Reply-to notiy@xyz.com

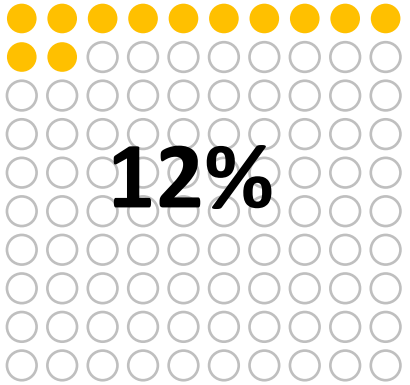
❻ Supply Chain

0.2%

From 採購供應商 <invoice@a.com>
To jennifer_lee@cellopoint.com
Subject 原物料採購驗收開立發票
Reply-to invoice@a.com

哪些帳號常被攻擊？

對外公用帳號
(published email)



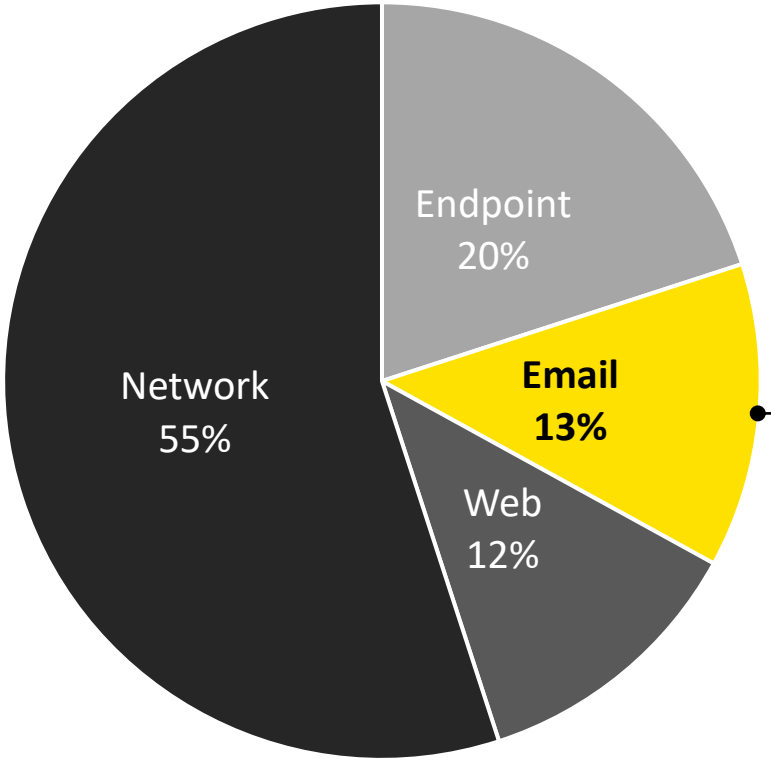
12%的帳號常受到
目標攻擊

易受攻擊的5大部門

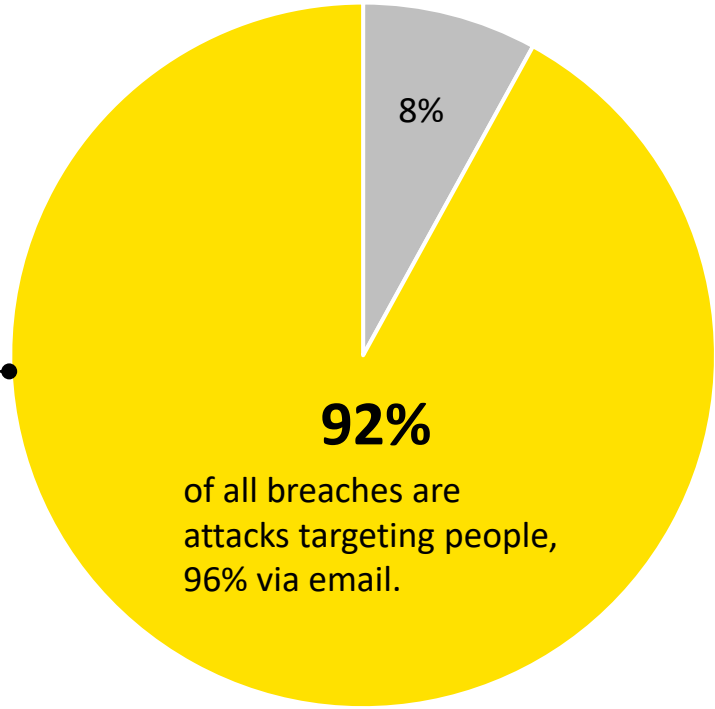
偽冒 CxO 的趨勢上升

盤點防疫破口 ~ Email 是攻擊重點

IT Security Spending



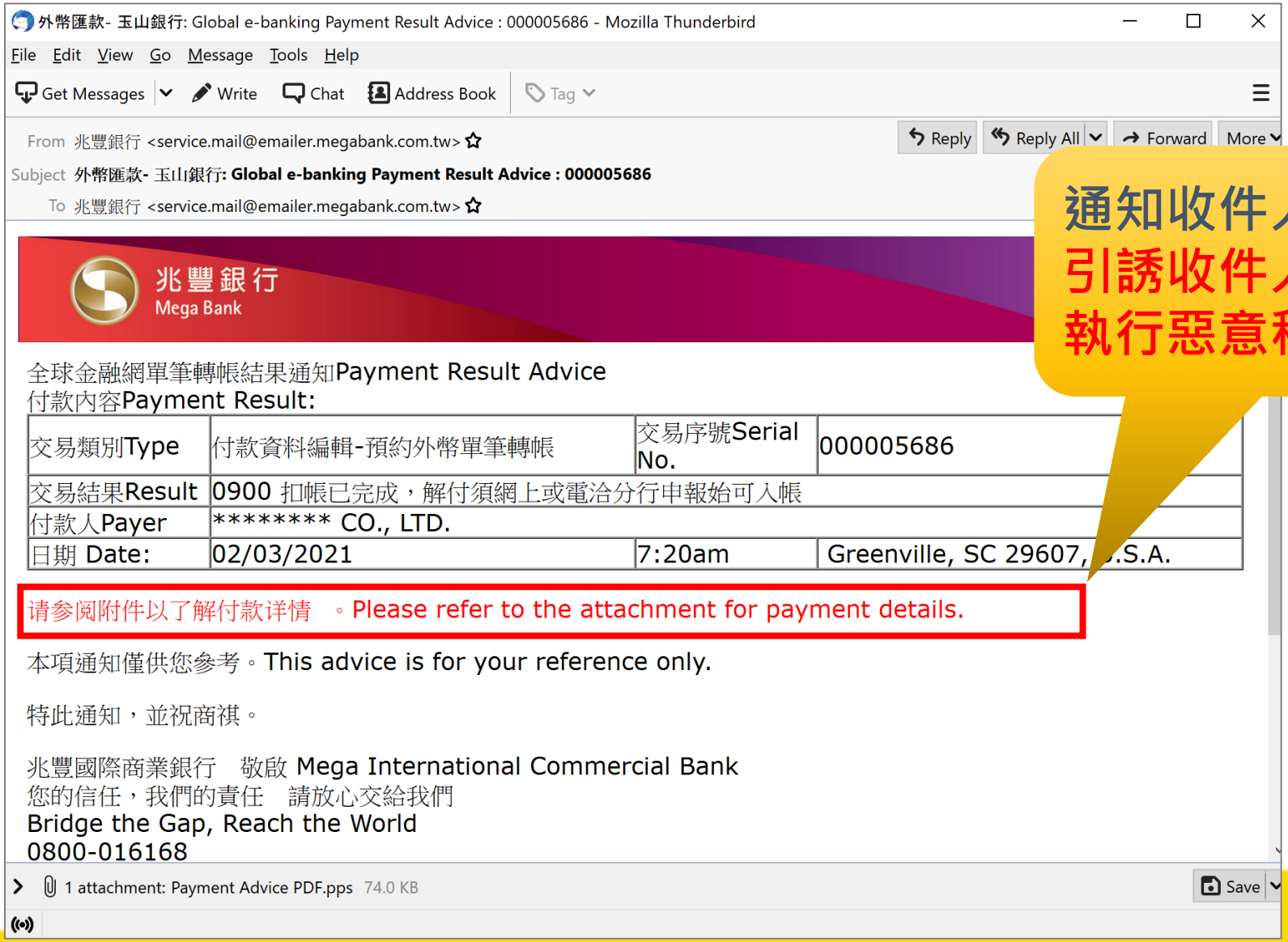
Attack Vector



電子郵件攻擊實務案例

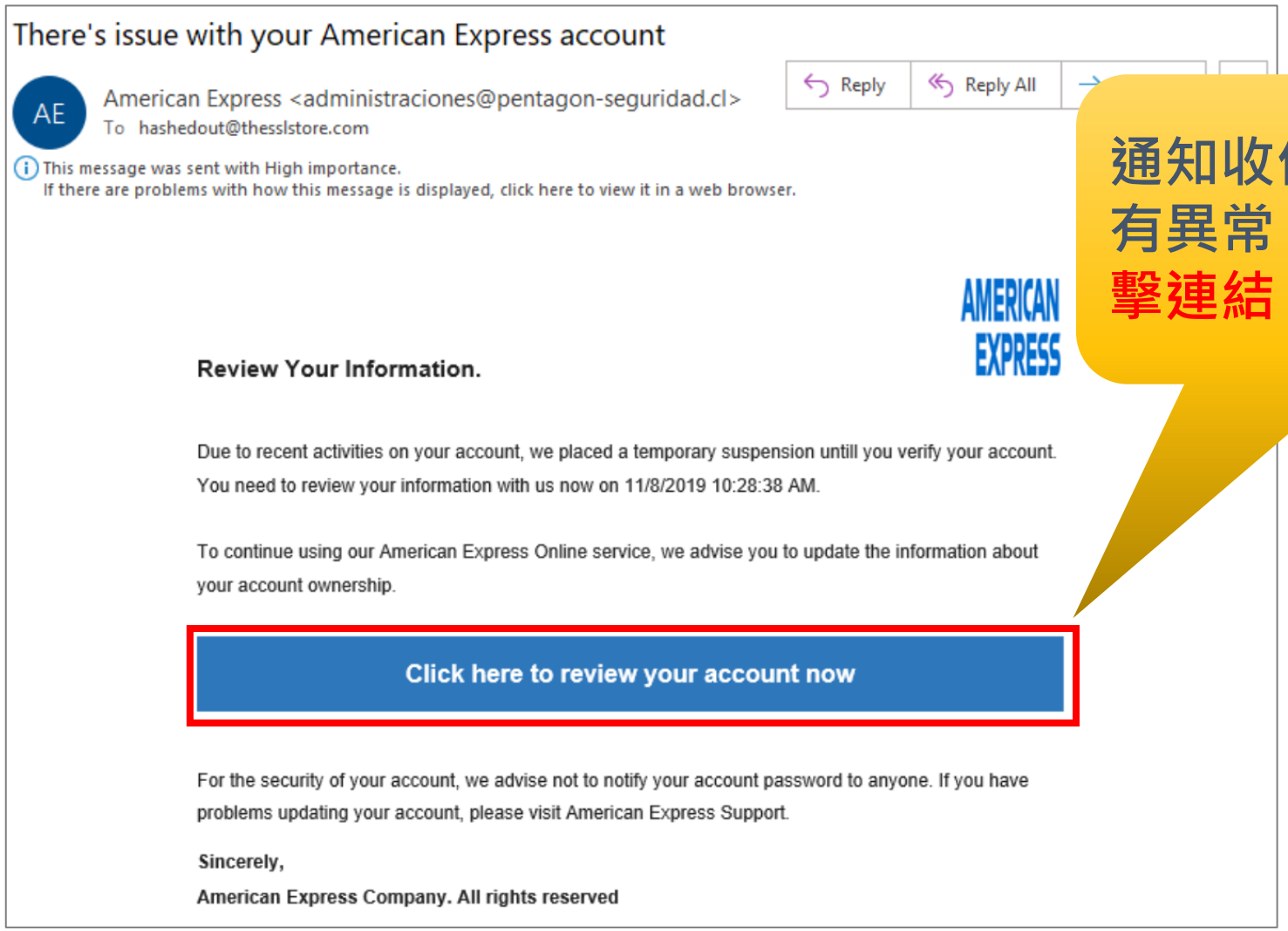
CELLOPOINT
Secure Your Email

匯款通知



通知收件人匯款完成，
引誘收件人開啟附件，
執行惡意程式。

信用卡帳戶異常通知



通知收件人信用卡帳戶有異常，引誘收件人點擊連結，騙取帳號密碼。

O365 釣魚郵件

From	Office 365 Administrator <admin@365micros0ft.com>
Subject	Your password will expire in 3 days.
To	jennifer_lee@cellopoint.com

通知收件人 O365 密碼即將到期，引誘收件人點擊連結。

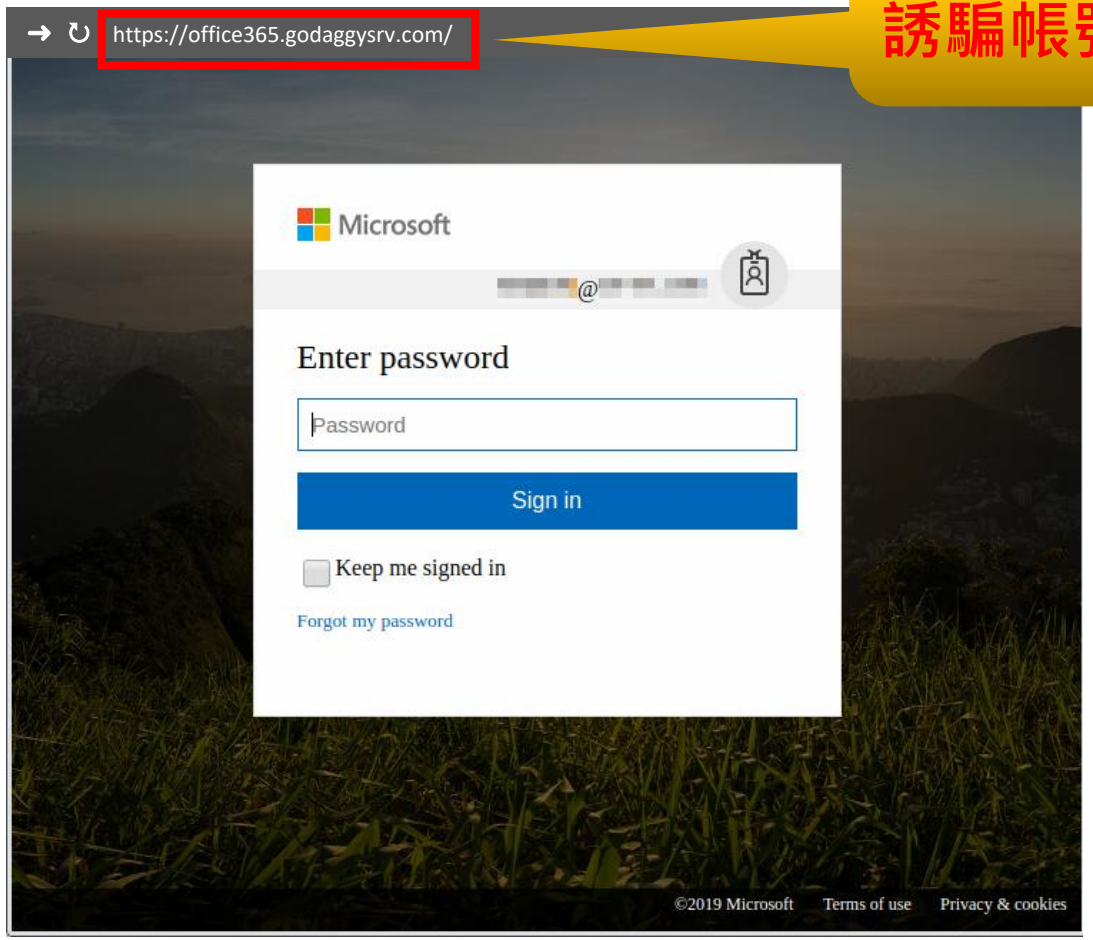
Dear Customer,

Your Office 365 e-mail Password will expire in 3 d
You can change your password through the Office 365 web portal:
https://login.microsoftonline.com/

If you need instructions on how to access the portal, please contact the administrator.

Thank you,
Office 365 Administrator

O365 釣魚郵件



重導至假網頁，試圖誘騙帳號密碼。

Google 釣魚郵件

通知收件人 Google 帳戶密碼已長期未變更，**引誘收件人點擊連結。**

Google 釣魚郵件

CELLOPOINT
Secure Your Email

BEC 詐騙新聞

化學製造公司Orion在BEC騙局中損失了6000萬美元

閱讀量 42659

發佈時間: 2024-08-15 14:24:47

譯文聲明

本文為翻譯文章，文章原作者詹姆斯·科克，文章來源：infosecurity

原文網址：https://www.infosecurity-magazine.com/news/manufacturing-

譯文僅供參考，具體內容表達及意義原文為準。

化學製造公司Orion透露，它在一次商業電子郵件洩漏（BEC）騙局中

在提交給美國證券交易委員會（SEC）的文件中，這家總部位於盧森堡

到第三方帳戶。

Orion 表示：「2024 年8 月10 日，Orion SA 確定一名非具名執行官的

欺性地向未知第三方控制的帳戶進行出站電匯。

在8月12日的文件中沒有提供有關BEC攻擊的進一步細節。

Orion表示，它正在與執法部門合作，透過所有合法手段追回資金，包

沒有證據表明存在其他詐欺活動，也沒有證據表明攻擊者獲得了對公司

BEC 是代價最高的攻擊媒介之一

BEC 攻擊是指詐欺者聯繫有權存取組織資金的員工，通常會冒充高階管

美國聯邦調查局（FBI） 的《*2023 年網路犯罪報告*》發現，BEC 攻擊

為第二大最具破壞性的網路犯罪。

保險公司Coalition 在2024 年4 月透露，BEC 和資金轉移詐欺（FTF）

深度偽造技術的發展增強了這些攻擊，使詐欺者能夠透過電話準確地冒

此外，生成式AI 工具已被用於為BEC 攻擊創建令人信服的虛假電子郵件。

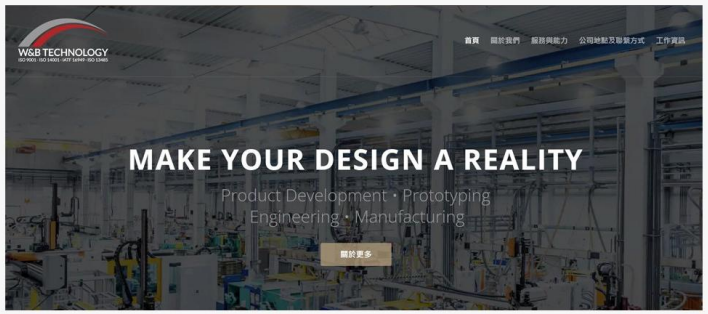
新聞

崴寶精密科技與其客戶遭遇BEC詐騙，駭客冒名發送電子郵件騙走3千萬，所幸及時凍結接收匯款的人頭帳戶

近期有臺灣企業揭露自身遭遇BEC詐騙事件，有駭客冒名崴寶精密科技公司發送電子郵件通知客戶，要求將原本要給付的100多萬美元（3,000多萬）款項匯至另一收款帳戶

文/ 羅正漢 | 2024-07-09 發表

讚 44 分享



關於BEC商業電子郵件詐騙案，過去國內很少有企業揭露這方面的資安事故，通常只有警政署公布統計資訊，或以去識別化的案例來宣導，又或是等到主管機關揭露，像是之前臺灣銀行洛杉磯分行通報金管會遭遇BEC詐騙案。

國內也曾傳出BEC詐騙，但很少浮出檯面讓外界得知，難得有公司主動公布發生這樣的事故，不過，現在隨著證交所對臺灣上市櫃公司資安重訊發布的要求條件擴大，企業BEC詐騙事件可望有更多公開揭露的機會。

今年4月才剛在國內證券櫃檯買賣中心申請成為公開發行公司的崴寶精密科技，雖然他們尚未成為上市櫃公司，在6月28日仍透過證交所公開資訊觀測站發布重大訊息，說明遭遇冒名通知客戶更改收款帳戶的事件。根據公告內容來判斷，我們認為這起事故就是典型的BEC詐騙。

迄今為止最大BEC騙局被偵破！國際刑警組織為企業追回4,100 萬美元

FreeBuf

2024-08-07 13:35 發佈於 FreeBuf官方帳號

+關注

讀需4分鐘

一個"全球止付機制"，協助企業追回了4100萬美元，這是迄今為止商業攻擊事件中涉及到的最大金額。

中旬，一家總部位於新加坡的大宗商品公司成為BEC 騙局的受害者之

的，惡意行為者有時會透過冒充可信人物，利用電子郵件誘騙目標匯款授權存取財務人員或律師事務所的電子郵件帳戶以發送假髮票，或冒充第三方供應商以電子郵件發送虛假帳單。

BEC 詐騙新聞

新聞

臺銀海外分行爆發商業電郵詐騙千萬，臺銀列為人為疏失，金管會要求加強控管

行員在家上班導致匯款流程未再確認，專家呼籲可採DMARC減少企業接到釣魚郵件風險

讚 6.1 萬 按讚加入iThome粉絲團 讚 670 分享

文/ 黃彥棻 | 2020-05-13 發表

臺灣銀行洛杉磯分行因為員工在家上班，導致匯款流程未再確認，遭到電子商業郵件詐騙千萬元。

臺灣銀行洛杉磯分行日前向金管會通報4月24日爆發資安事件，該分行行員收到往來客戶要進行匯款轉帳的的電子郵件，因為實施居家辦公無法轉帳，便將該封匯款郵件轉到分行承做，不過，該指示匯款電郵與原本客戶電郵有一個字母差異，在分行並未確認匯款資料正確性便進行轉帳，導致該分行遭到詐騙約美金45萬美元（約新臺幣1,350萬元）。

雖然說，該起事件是因為洛杉磯下達禁足令，導致許多行業很多員工都必須在家上班，但不具名資安顧問卻認為，不應該以「在家上班」模糊事件焦點。他指出，Email電子郵件是串連銀行內部與外部連繫的重要管道，傳統資安防護措施置重兵於組織邊界的作法，未來將更難應付駭客精心設計的釣魚郵件。該名資安顧問則建議，銀行可以師法國外推動DMARC（Domain-based Message Authentication, Reporting & Conformance）等作法，來降低釣魚郵件的威脅。

新聞

豐田子公司遭BEC商業郵件詐騙攻擊，損失40億日圓

生產汽車椅套及門內飾件的豐田紡織，因內部聽信詐騙郵件指示匯款給第三方，損失近10億元新臺幣

讚 6.1 萬 按讚加入iThome粉絲團 讚 718 分享

文/ 林妍溱 | 2019-09-09 發表

示意圖（Photo by The Los Angeles County District Attorney's Office on https://vimeo.com/222209148）

日本汽車大廠豐田旗下生產汽車椅套及門內飾件的子公司豐田紡織（Toyota Boshoku），上個月遭到假冒商業郵件的詐騙攻擊（Business Email Comprise，BEC），損失將近40億日圓（約合台幣11.7億元）。

豐田紡織上周五（9月6日）發佈公告指出，該公司歐洲子公司在8月14日遭惡意第三方匯款詐欺，導致公司財務損失。豐田紡織在付款後發現為詐欺行為，立即成立包括法務人員

新聞

挪威國家投資基金遭BEC詐騙，被盜走1千萬美元

挪威國家投資基金Norfund因先前曾發生資料外洩事件，讓駭客得以掌握該組織與其他機構的郵件往來內容，進而偽造出逼真的匯款要求詐騙信件

讚 6.1 萬 按讚加入iThome粉絲團 讚 239 分享

金Norfund坦承遭遇商業電子郵件詐騙Compromise，BEC），損失1千萬美元。

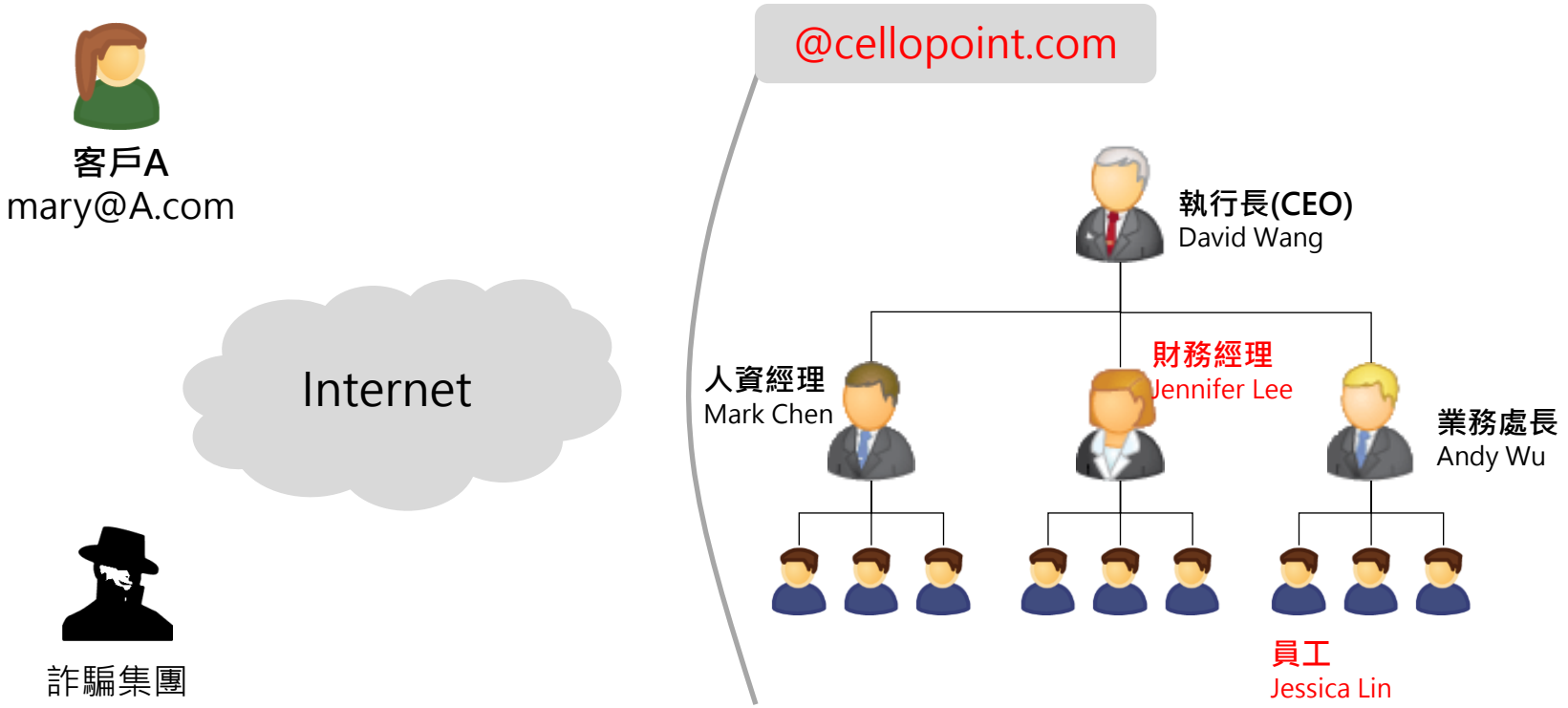
會建立的私募基金，直屬挪威外交部，資金

und是先發生資料外洩事件，使得駭客得以補寨一家小額信貸公司之間的郵件往來，並內容及所使用的語言，再偽造文件與支付細

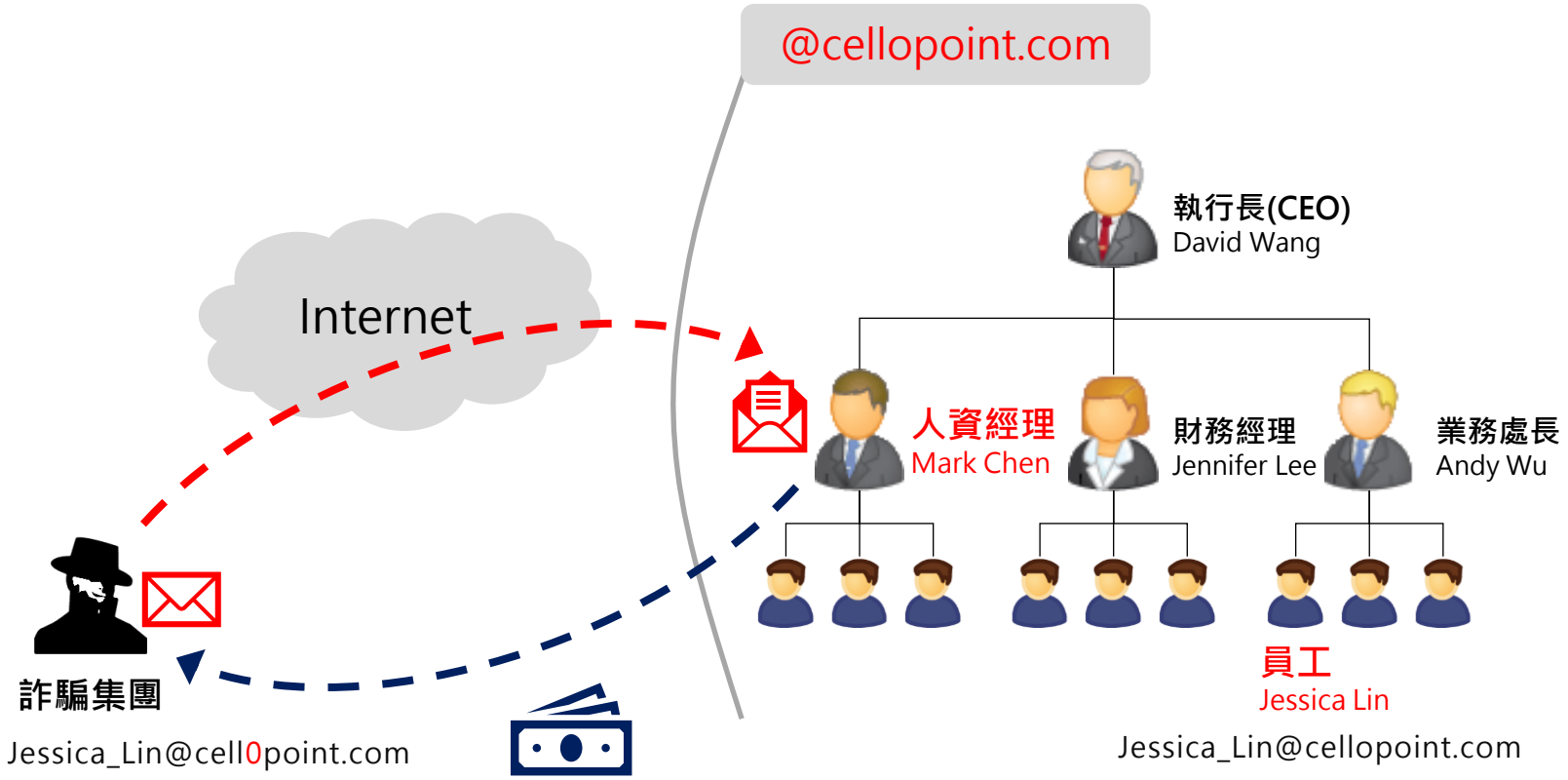
客早在數月前就入侵了Norfund基金的通往系統內直到有機可趁。在3月16日當天誘導元匯入與該小額信貸公司同名的帳號，並很

CELLOPOINT
Secure Your Email

BEC 詐騙 ~ 與組織架構相關



情境 1：偽冒內部員工，詐騙內部同仁



情境 1：偽冒郵件

Display name	Jessica Lin
From address	Jessica_Lin@cellop0int.com
Reply-to	Jessica_Lin@cellop0int.com
To	Mark_chen@cellopoint.com
Subject	業務部Jessica Lin_薪資轉帳帳戶更改

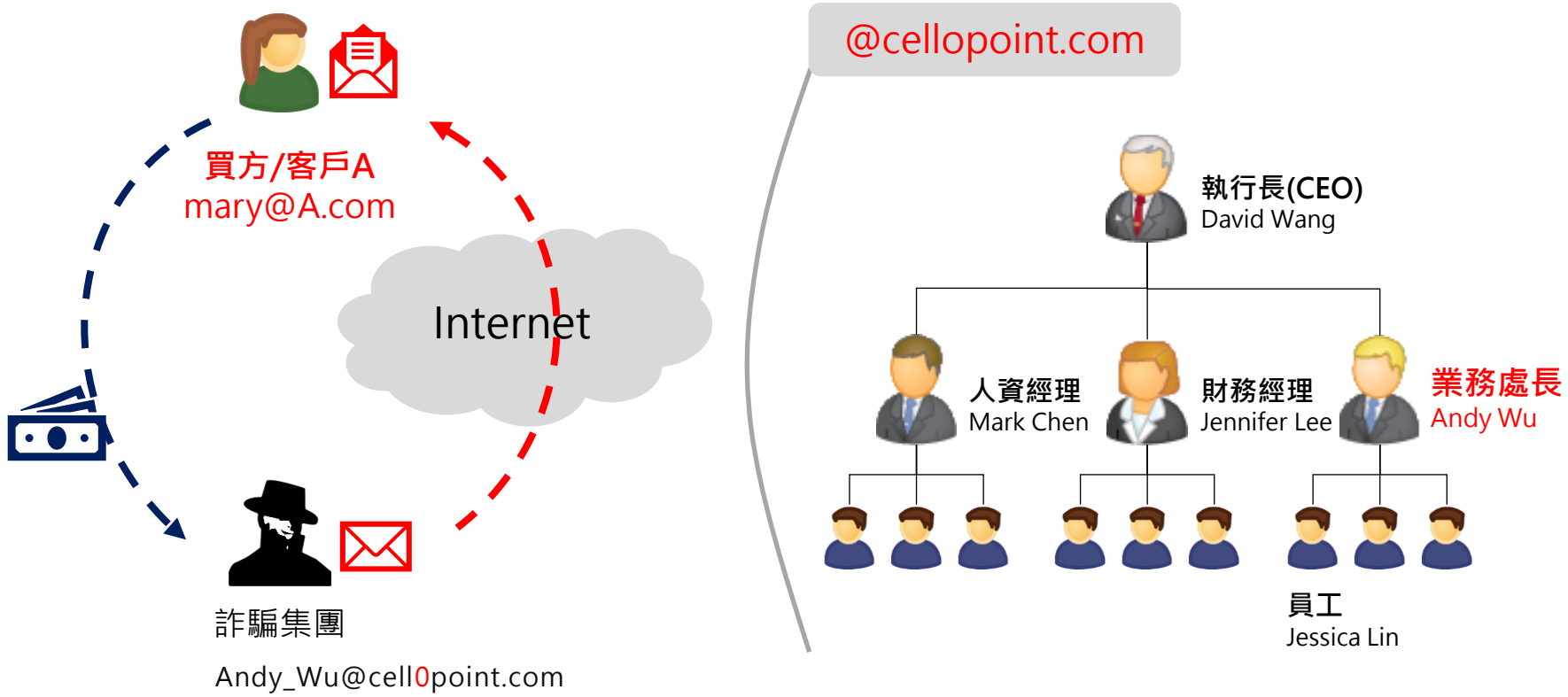
Dear Mark，

我的銀行帳戶資訊有變更，
請協助更新並自本月起將薪資轉入此帳戶，
麻煩了，感謝您!

SWIFT:XXYYZZ
Bank account: 201900310-9876543210

Jessica Lin
業務部
基點資訊股份有限公司

情境 2：偽冒貴公司人員，詐騙 A 客戶



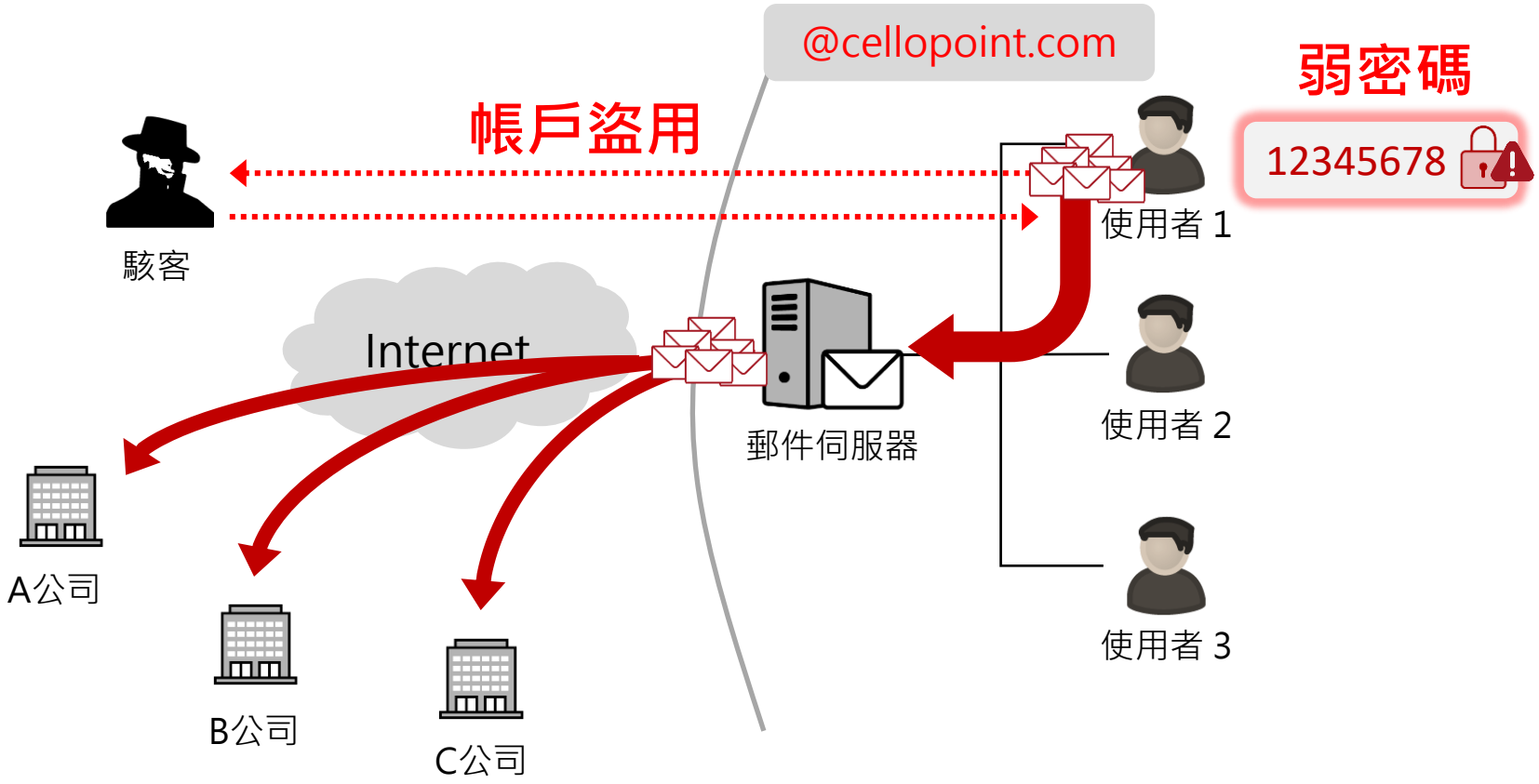
情境 2：偽冒郵件

Display name	Andy
From address	Andy_Wu@cellopoint.com
Reply-to	Andy_Wu@cellop0int.com
To	mary@a.com
Subject	Cellopoint 2021年01月份_應收帳款通知

Dear Mary，
貴公司訂單號碼：20210111-001，總金額為200,000U$。
請依照合約需於2021年03月01日前匯款。
由於本公司在香港滙豐銀行新增境外美金帳戶，請將此筆匯款匯到：
SWIFT code: xxxxxx
戶名： Cellopoint-Hong-Kong-HSBC
帳號：xxxxxxxxxxxxx

Andy Wu
業務處長
基點資訊股份有限公司

弱密碼遭盜用，發送大量惡意郵件



電子郵件偽冒攻擊與防治方法

CELLOPOINT
Secure Your Email

郵件需要檢查的地方

資料來源：
https://www.knowbe4.com/what-is-social-engineering
https://www.knowbe4.com/hubfs/22RedFlags.pdf?hsLang=en

Social Engineering Red Flags

FROM

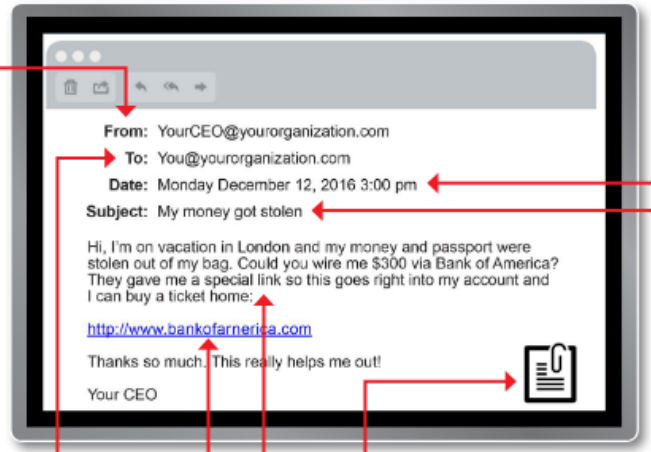
- I don't recognize the sender's email address as someone **I ordinarily communicate with**.
- This email is from **someone outside my organization and it's not related to my job responsibilities**.
- This email was sent from **someone inside the organization** or from a customer, vendor, or partner and is **very unusual or out of character**.
- Is the sender's email address from a **suspicious domain** (like micorsoft-support.com)?
- **I don't know the sender personally** and they **were not vouched for** by someone I trust.
- **I don't have a business relationship** nor any past communications with the sender.
- This is an **unexpected or unusual email** with an **embedded hyperlink or an attachment** from someone I haven't communicated with recently.

TO

- I was cc'd on an email sent to one or more people, but **I don't personally know** the other people it was sent to.
- I received an email that was also sent to an **unusual mix of people**. For instance, it might be sent to a random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses.

HYPERLINKS

- I hover my mouse over a hyperlink that's displayed in the email message, but the **link-to address is for a different website**. (This is a **big** red flag.)
- I received an email that only has **long hyperlinks with no further information**, and the rest of the email is completely blank.
- I received an email with a **hyperlink that is a misspelling** of a known web site. For instance, www.bankofarnerica.com — the "m" is really two characters — "r" and "n."



DATE

- Did I receive an email that I normally would get during regular business hours, but it was **sent at an unusual time** like 3 a.m.?

SUBJECT

- Did I get an email with a subject line that is **irrelevant** or **does not match** the message content?
- Is the email message a reply to something **I never sent or requested**?

ATTACHMENTS

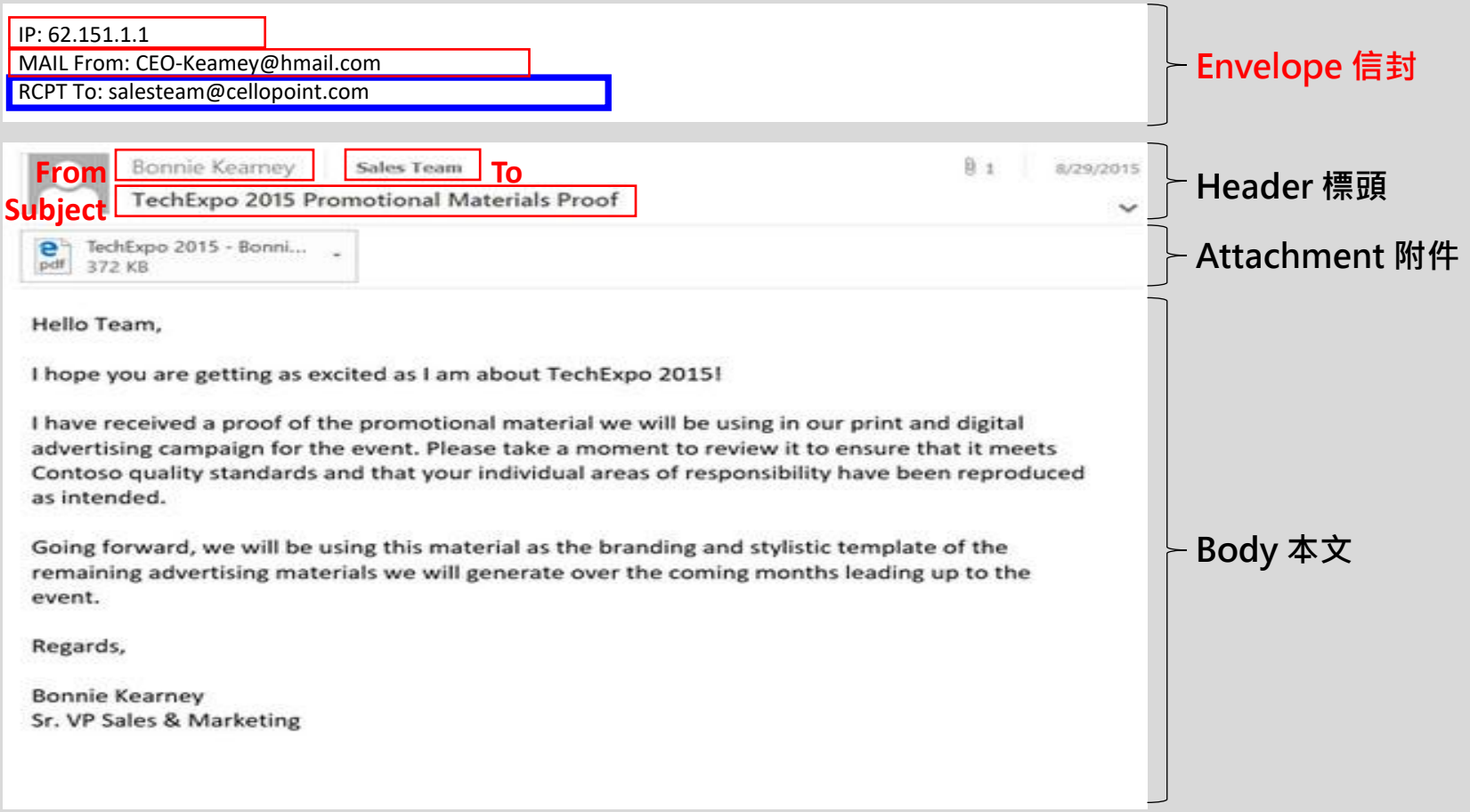
- The sender included an email attachment that **I was not expecting** or that **makes no sense** in relation to the email message. (This sender doesn't ordinarily send me this type of attachment.)
- I see an attachment with a possibly **dangerous file type**. The only file type that is **always safe to click on is a .txt** file.

CONTENT

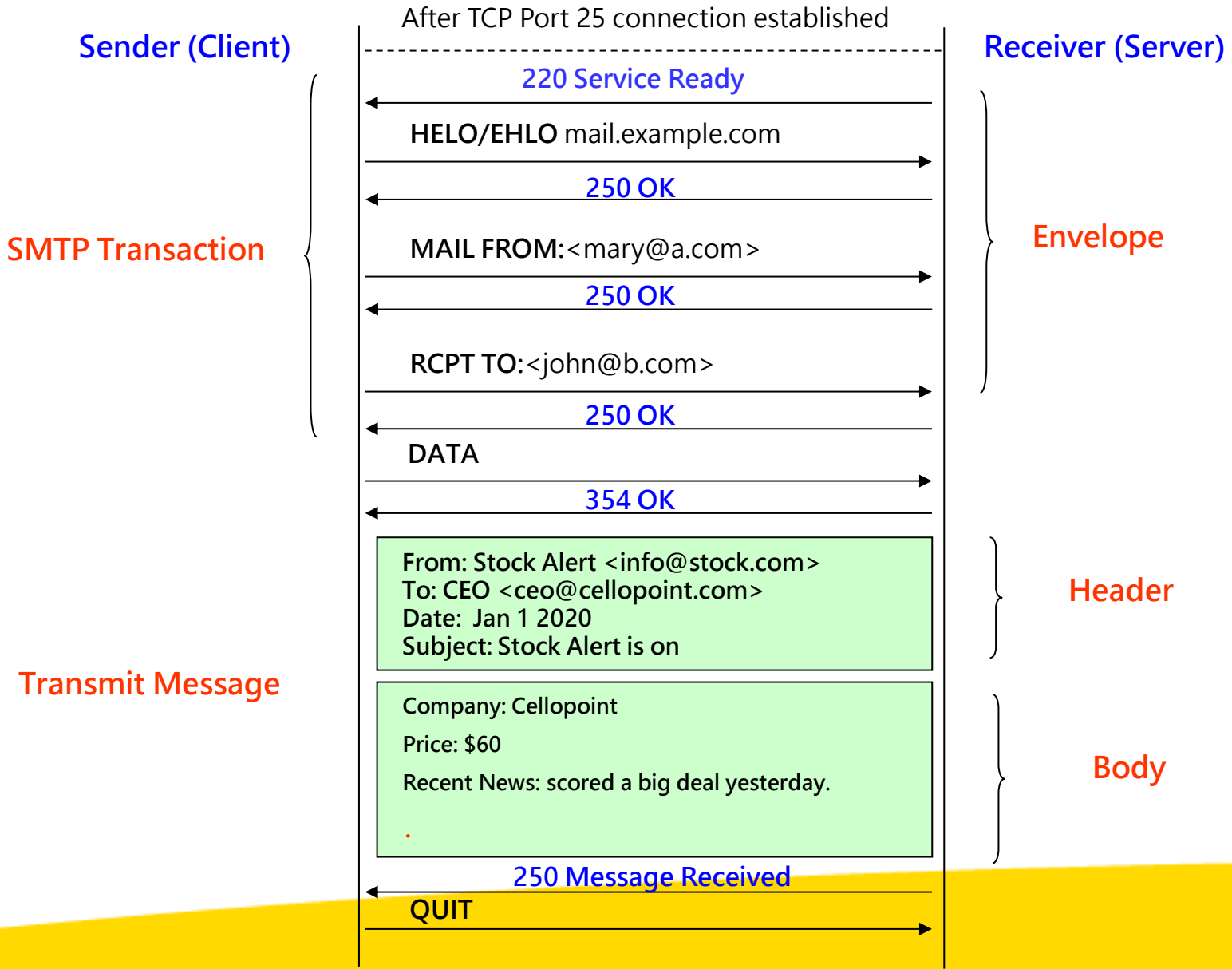
- Is the sender asking me to click on a link or open an attachment to **avoid a negative consequence** or to **gain something of value**?
- Is the email **out of the ordinary**, or does it have **bad grammar** or **spelling errors**?
- Is the sender asking me to click a link or open up an attachment that **seems odd** or **illogical**?
- Do I have an **uncomfortable gut feeling** about the sender's request to open an attachment or click a link?
- Is the email asking me to look at a **compromising or embarrassing picture** of myself or someone I know?

CELLOPOINT
Secure Your Email

為什麼 Email 容易詐騙

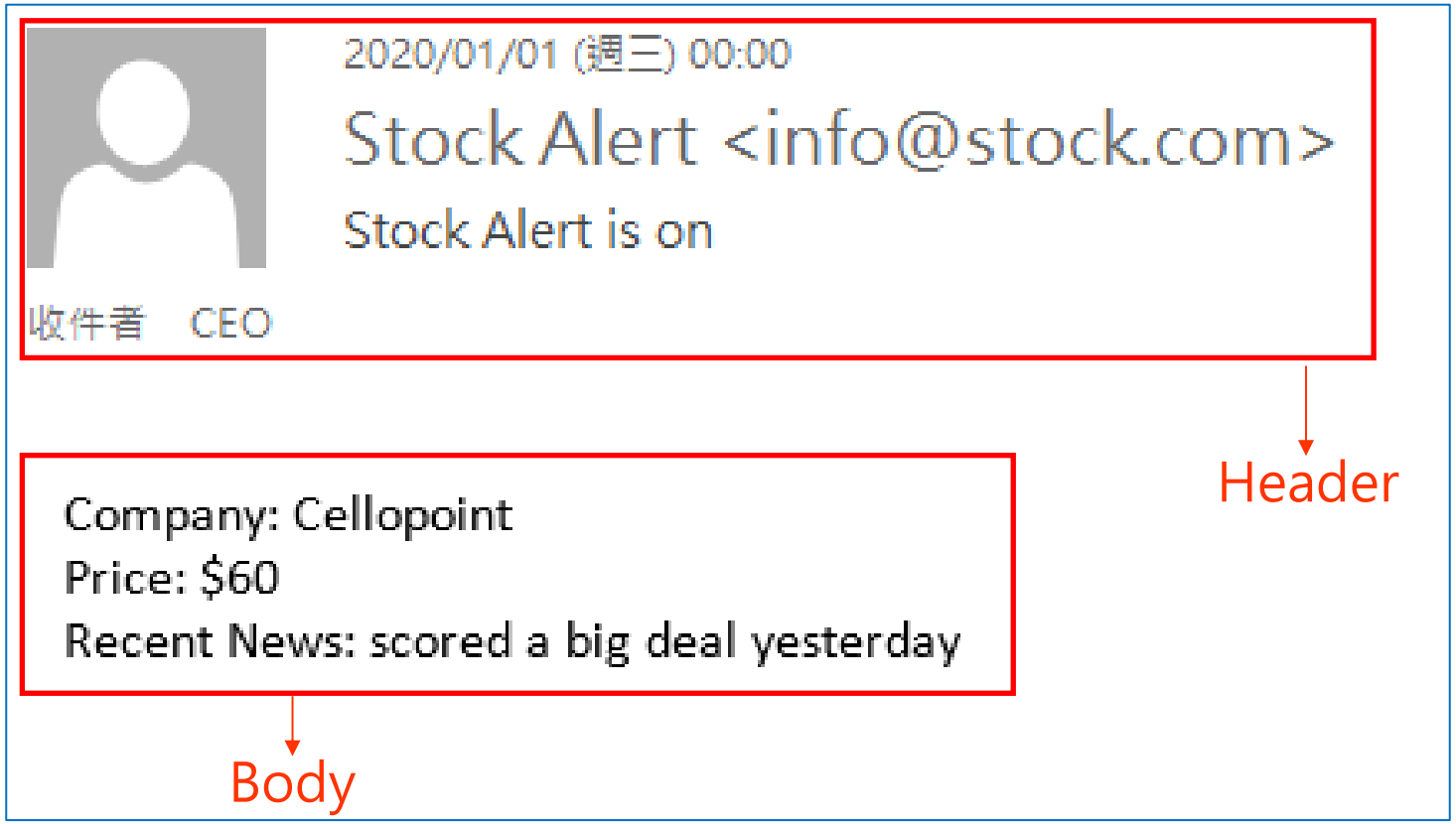


SMTP 交談流程 (RFC 5321)



Mail Client 解析郵件

只有 SMTP Client 端的 IP 和收件人（rcpt to:）是可信的



郵件防偽冒三大機制

SPF (Sender Policy Framework)

- 檢查寄信 IP 是否被網域授權，根據 SMTP 的 MAIL FROM（envelope）驗證。
- 防止冒用寄件伺服器位址發信。

DKIM (DomainKeys Identified Mail)

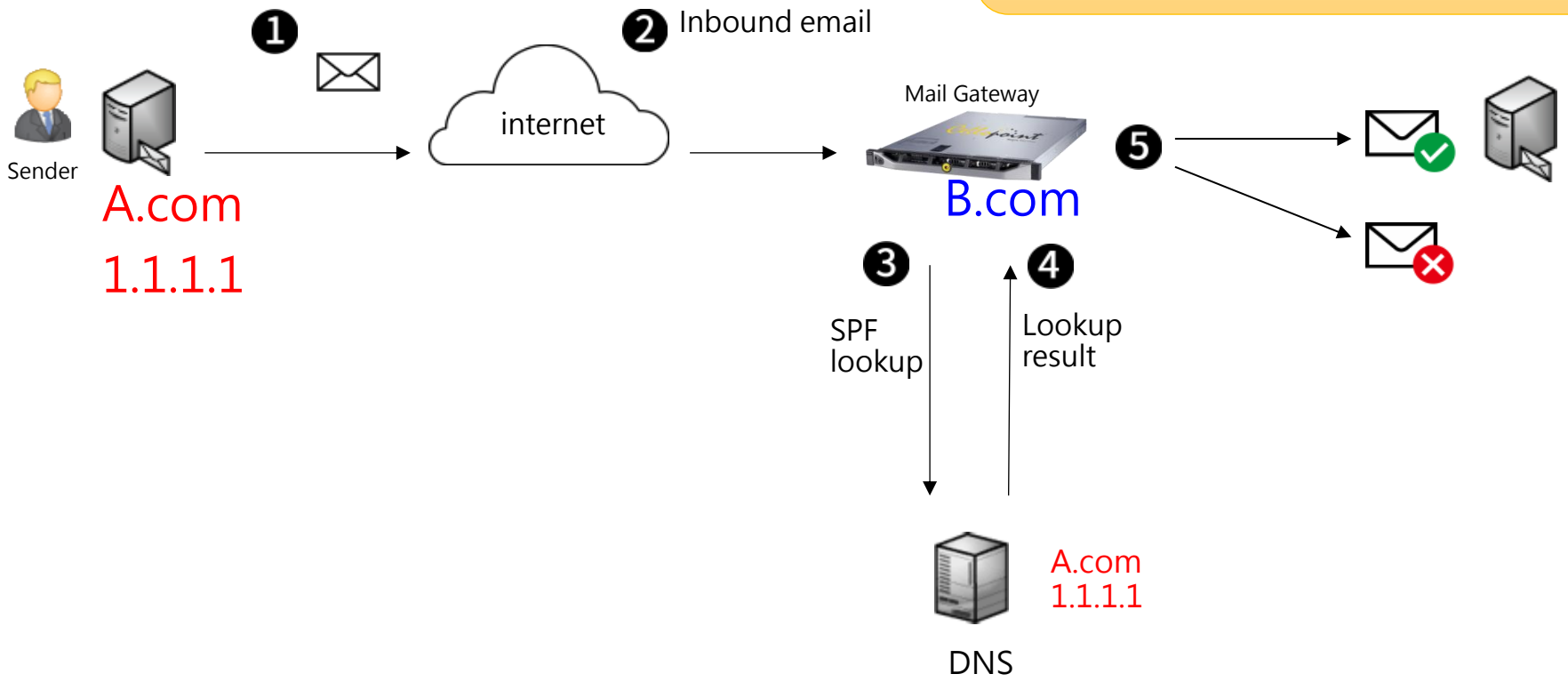
- 使用私鑰對郵件簽章，驗證內容未被竄改。
- 收件端透過 DNS 公開金鑰驗證簽章，確保郵件來源可信、內容完整。

DMARC (Domain-based Message Authentication, Reporting & Conformance)

- 整合 SPF 與 DKIM 結果，檢查寄件人一致性。
- 設定驗證失敗時的處理策略（none、quarantine、reject），提供報告機制，協助監控偽冒行為。

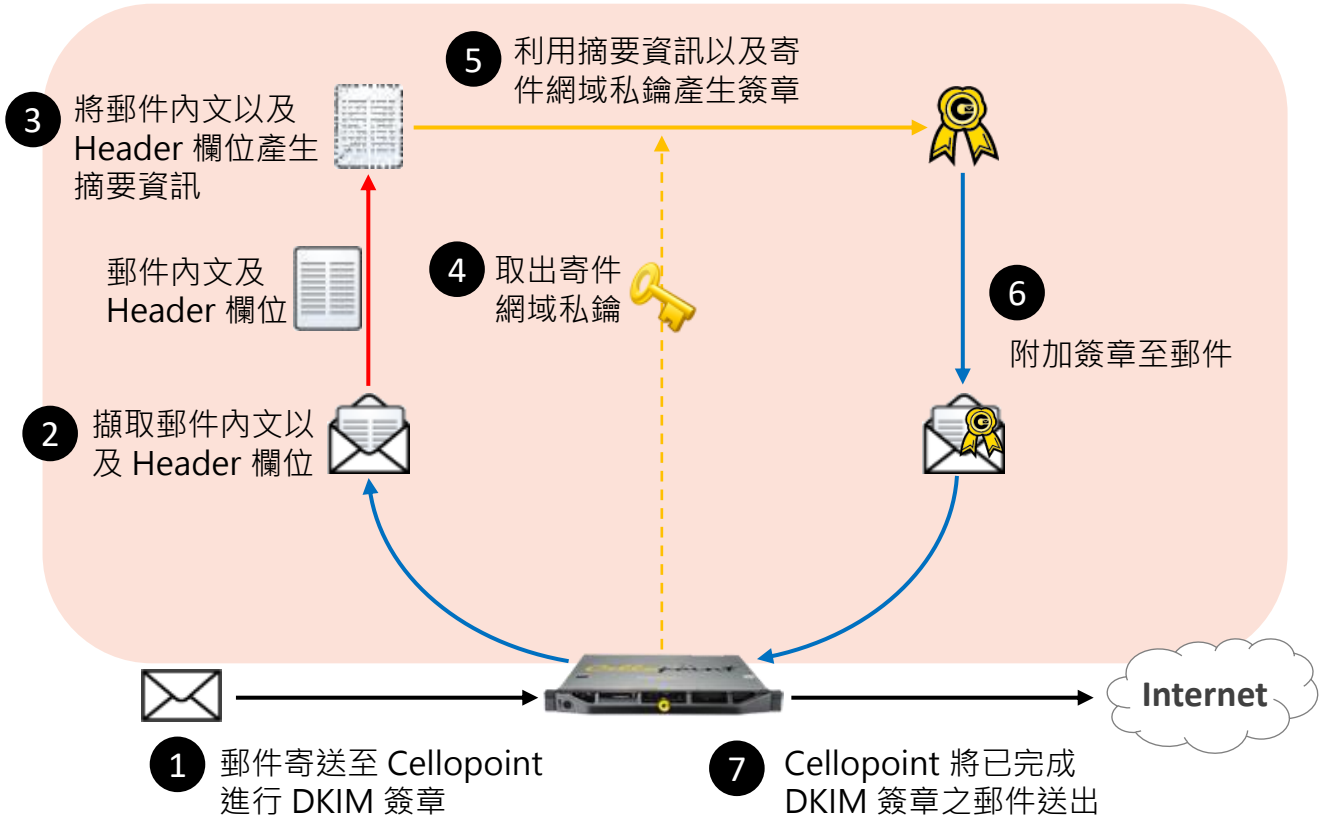
防偽冒攻擊：SPF

B 公司 Mail Gateway 啟用 SPF 檢查：
驗證宣稱 A.com 網域的郵件
是否真的由被授權的主機 IP 發送



防偽冒攻擊：DKIM

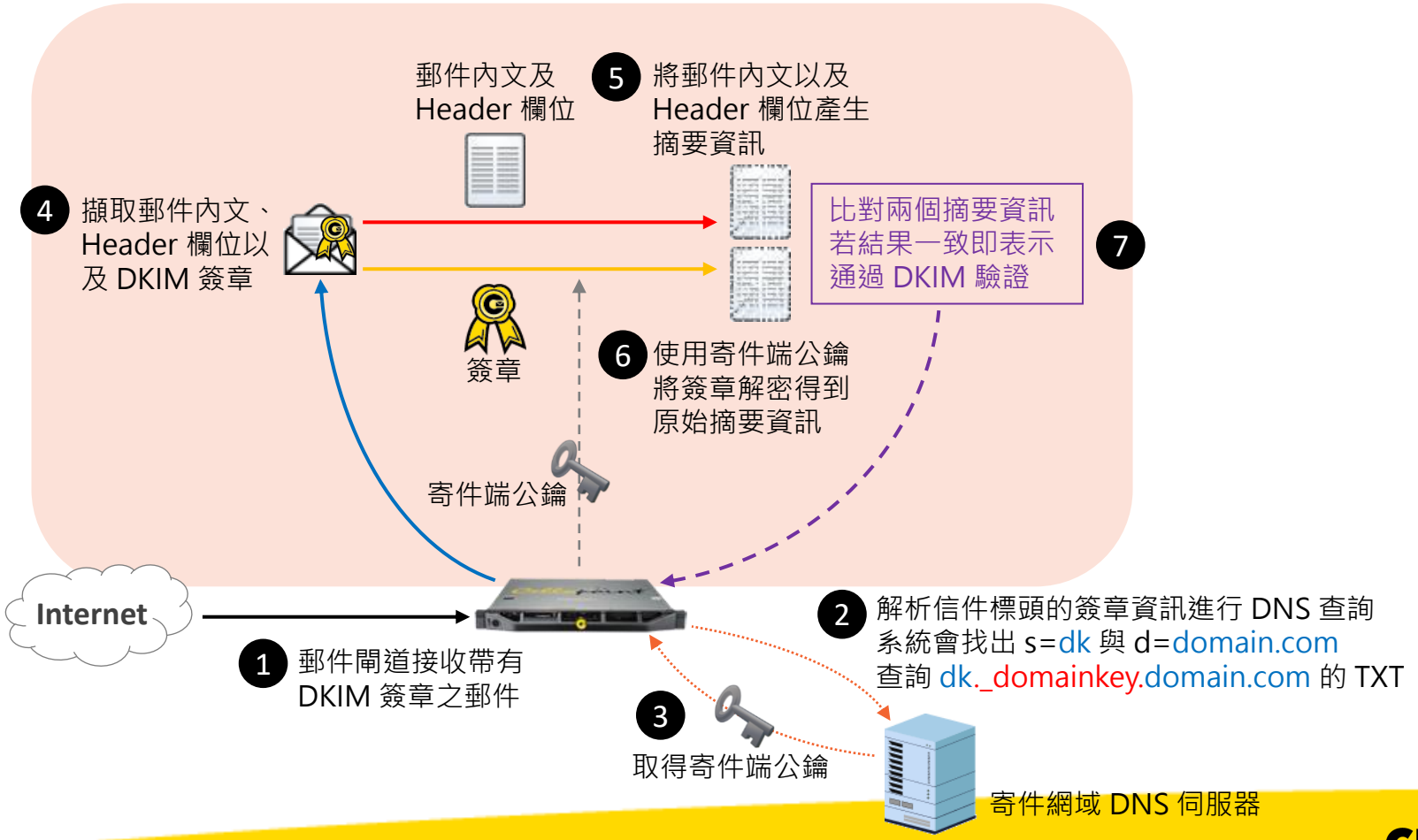
DKIM 簽章「寄件端」處理流程



參考資料：https://dkimcore.org/specification.html

防偽冒攻擊：DKIM

DKIM 簽章「收件端」處理流程



CELLOPOINT
Secure Your Email

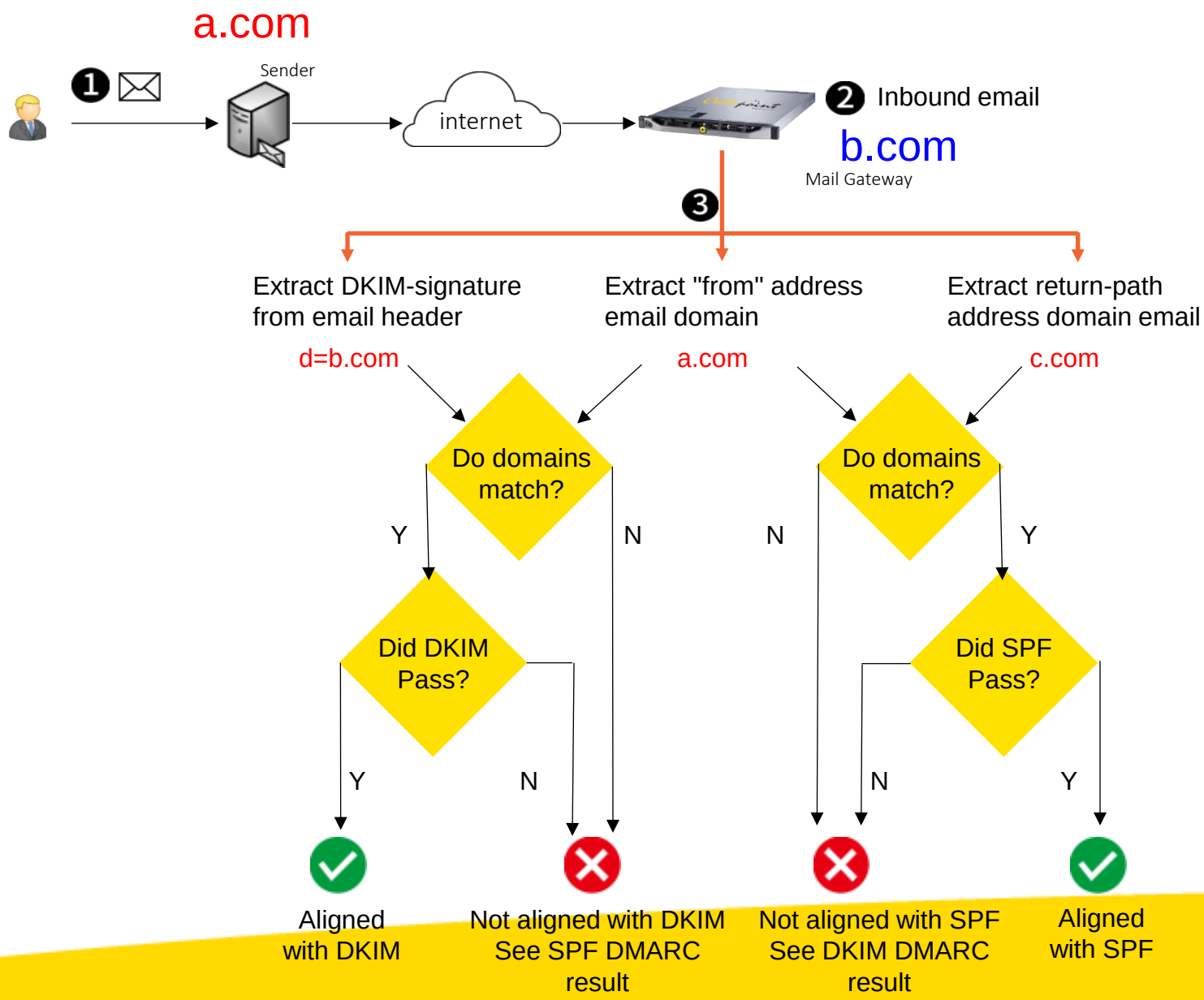
防偽冒攻擊：收件端檢查 DKIM 方式

```
Return-Path: <prvs=1989897722=kai.liao@cellopoint.com>
Received: from mailgw.cellopoint.com (mailgw.cellopoint.com. [202.153.184.150])
        by mx.google.com with ESMTPS id u70si2461161pgu.119.2019.04.02.23.45.17
        for <cellopoint.kai@gmail.com>
        (version=TLS1_2 cipher=ECDHE-RSA-AES128-GCM-SHA256 bits=128/128);
        Tue, 02 Apr 2019 23:45:17 -0700 (PDT)
Received-SPF: pass (google.com: domain of prvs=1989897722=kai.liao@cellopoint.com designates 202.153.184.150 as
permitted sender) client-ip=202.153.184.150;
Authentication-Results: mx.google.com;
       dkim=pass (test mode) header.i=@cellopoint.com header.s=dk2048 header.b=AXVb3F0v;
       spf=pass (google.com: domain of prvs=1989897722=kai.liao@cellopoint.com designates 202.153.184.150 as
permitted sender) smtp.mailfrom="prvs=1989897722=kai.liao@cellopoint.com";
       dmarc=pass (p=NONE sp=NONE dis=NONE) header.from=cellopoint.com
X-UUID: 3521c70c47e34827af91d04ef4b8ac74-20190403
DKIM-Signature: v=1; a=rsa-sha256; q=dns/txt; c=relaxed/relaxed; d=cellopoint.com; s=dk2048; h=Content-Type:MIME-
Version:Subject:Message-ID:To:From:Date; bh=FX87mODpgNJ3jM2LOW5iyEljz84VGE+zW2uhfCx1G8k=;
b=AXVb3F0vPzgfrYFp0zIwc5aROtk0r+oWbOU4c5Irv/1eYeIk/8caPIWhJcNdalVaRhN3Tm0HohB8Q1gOuwj4EUgcA0bSM1v1k
/atcBQL7fIAKR35W3sZ70f17U++lzdzLsHoWHKx9Htm2GTU3uQ3uIF7Dme/s5IWz6ify9NqwSoS1BudTz3RPgTRg8e
/LS4voBaAv1YKIKNQhsMgjtxnmeT/yqZKZvfR22ckGoyO8K
/FsBB3wi8fnb6HBSAPENhatmy5zI2MszvQNzaHrQFIQdo6GQVatVbUUS7mD1VEEXN9+yDF7CP6XLtHPFTx/mNAtdj6X5zY3+ulB2Zpgzo0Cw==;
X-UUID: 3521c70c47e34827af91d04ef4b8ac74-20190403
Received: from mail.cellopoint.com [(192.168.200.17)] by mailgw.cellopoint.com (envelope-from
<prvs=1989897722=kai.liao@cellopoint.com>) (Cellopoint E-mail Firewall v4.1.8 Build 0321) with ESMTP id 1680144426;
Wed, 03 Apr 2019 14:45:14 +0800
Date: Wed, 3 Apr 2019 14:45:14 +0800 (CST)
From: Kai <kai.liao@cellopoint.com>
To: Liao Kai <[redacted]>
```

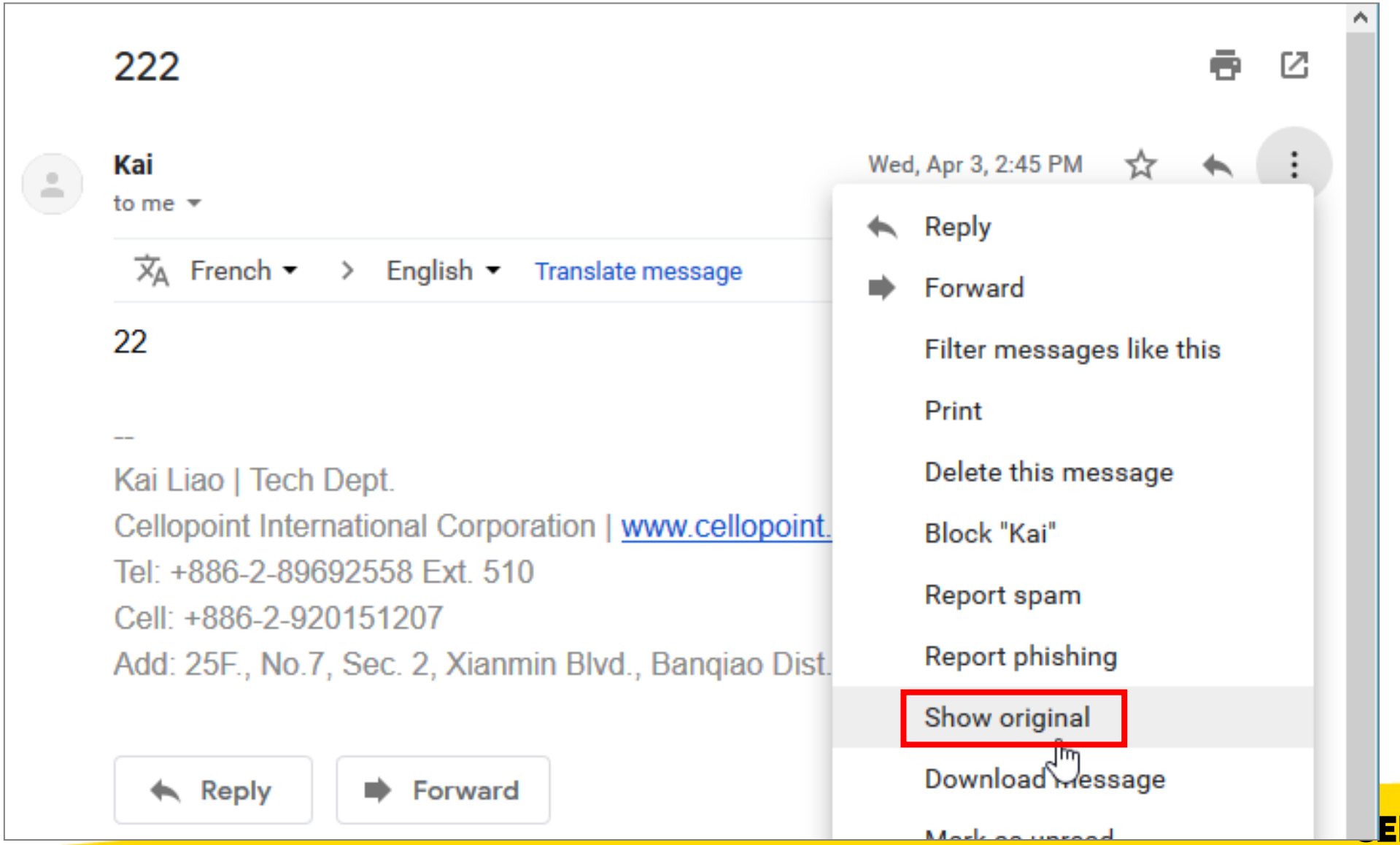
防偽冒攻擊：收件端檢查 DKIM 方式

```
C:\Users\Ken>nslookup -q=txt dk2048._domainkey.cellopoint.com 8.8.8.8
伺服器:  dns.google
Address:  8.8.8.8

未經授權的回答:
dk2048._domainkey.cellopoint.com        text =

        "v=DKIM1; k=rsa; t=y; p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAtFUY0MbkNd0yy6K2GKppqkhENcZJtP7rZdDqbB1tgIHm
KIDSJSqQg1WfZNdFWN7xGsh9voVY6IIObCnfIZAX2zJXecuITOpVg3o6E0hRF9nNataWkDQto4tLRvPEFmj6ItqkIQfOeGpOAz7sztdrE6YRWuXysUEuQ4Fv
SkaHHiv4bD41qKSWBNO1+"
        "YCHSFuZW8hQcaV4B5fcDOaT6lmH/LCjVImQNvnTcyqTDmO1P5lAZXVRBqjEIUBPAA0jH056FzA9gPsZ3ygPJgQM7TUJ2tWuOQs5vqNer/PBFOsv
dS8UT6EE82KzuFKg0W/qA7XIhTpkHh68xSO4Ceis3djI9QIDAQAB"

C:\Users\Ken>
```

防偽冒攻擊：DMARC



郵件服務商都已支援防偽冒標準



郵件服務商都已支援防偽冒標準

Original Message

Message ID	<381585178.1383240.1554273914217.JavaMail.zimbra@cellopoint.com>
Created at:	Wed, Apr 3, 2019 at 2:45 PM (Delivered after 4 seconds)
From:	Kai <kai.liao@cellopoint.com> Using Zimbra 8.8.11_GA_3780 (ZimbraWebClient - GC73 (Win)/8.8.11_GA_3780)
To:	Liao Kai <cellopoint.kai@gmail.com>
Subject:	222
SPF:	PASS with IP 202.153.184.150 Learn more
DKIM:	'PASS' with domain cellopoint.com Learn more
DMARC:	'PASS' Learn more

判斷 Authentication-Results

Authentication-Results 標頭是**由接收郵件伺服器加入**。
用來記錄信件的**驗證結果**，判斷該信件是否通過如 SPF、DKIM、DMARC 等驗證機制。這對於判別是否為詐騙或偽冒郵件非常關鍵。

基本格式

Authentication-Results: **驗證者主機名稱**;
spf=**結果** smtp.mailfrom=**寄件人信箱**;
dkim=**結果** header.d=**簽章網域**;
dmarc=**結果** (policy=xxx) header.from=**寄件人網域**

判斷 Authentication-Results

驗證成功

Authentication-Results: mx.example.com;
spf=**pass** smtp.mailfrom=sender@domain.com;
dkim=**pass** header.d=domain.com;
dmarc=**pass** header.from=domain.com

驗證失敗

Authentication-Results: mx.example.com;
spf=**fail** smtp.mailfrom=spoofed@fake.com;
dkim=**fail** header.d=fake.com;
dmarc=**fail** (policy=reject) header.from=fake.com

判斷郵件 Header 資訊

```
Return-Path: <prvs=1989897722=kai.liao@cellopoint.com>
Received: from mailgw.cellopoint.com (mailgw.cellopoint.com. [202.153.184.150])
        by mx.google.com with ESMTPS id u70si2461161pgu.119.2019.04.02.23.45.17
        for <cellopoint.kai@gmail.com>
        (version=TLS1_2 cipher=ECDHE-RSA-AES128-GCM-SHA256 bits=128/128);
        Tue, 02 Apr 2019 23:45:17 -0700 (PDT)
Received-SPF: pass (google.com: domain of prvs=1989897722=kai.liao@cellopoint.com designates 202.153.184.150 as
permitted sender) client-ip=202.153.184.150;
Authentication-Results: mx.google.com;
       dkim=pass (test mode) header.i=@cellopoint.com header.s=dk2048 header.b=AXVb3F0v;
       spf=pass (google.com: domain of prvs=1989897722=kai.liao@cellopoint.com designates 202.153.184.150 as
permitted sender) smtp.mailfrom="prvs=1989897722=kai.liao@cellopoint.com";
       dmarc=pass (p=NONE sp=NONE dis=NONE) header.from=cellopoint.com
X-UUID: 3521c70c47e34827af91d04ef4b8ac74-20190403
DKIM-Signature: v=1; a=rsa-sha256; q=dns/txt; c=relaxed/relaxed; d=cellopoint.com; s=dk2048; h=Content-Type:MIME-
Version:Subject:Message-ID:To:From:Date; bh=FX87mODpgNJ3jM2LOW5iyE1jz84VGE+zW2uhfCx1G8k=;
b=AXVb3F0vPzgfrYFp0zIwc5aROtk0r+oWbOU4c5Irv/1eYeIk/8caPIWhJcNda1VaRhN3Tm0HohB8Q1gOuwj4EUgcA0bSM1v1k
/atcBQL7fIAKR35W3sZ70f17U++1zdzLsHoWHKx9Htm2GTU3uQ3uIF7Dme/s5IWz6ify9NqwSoS1BudTz3RPgTRg8e
/LS4voBaAv1YKIKNQhsMgjtxnmeT/yqZKZvfR22ckGoyO8K
/FsBB3wi8fnb6HBSAPENhatmy5zI2MszvQNzaHrQFIQdo6GQVatVbUUS7mD1VEEXN9+yDF7CP6XLtHPFTx/mNAtdj6X5zY3+u1B2Zpgzo0Cw==;
X-UUID: 3521c70c47e34827af91d04ef4b8ac74-20190403
Received: from mail.cellopoint.com [(192.168.200.17)] by mailgw.cellopoint.com (envelope-from
<prvs=1989897722=kai.liao@cellopoint.com>) (Cellopoint E-mail Firewall v4.1.8 Build 0321) with ESMTP id 1680144426;
Wed, 03 Apr 2019 14:45:14 +0800
Date: Wed, 3 Apr 2019 14:45:14 +0800 (CST)
From: Kai <kai.liao@cellopoint.com>
To: Liao Kai <[redacted]>
```

Cellopoint 解決方案

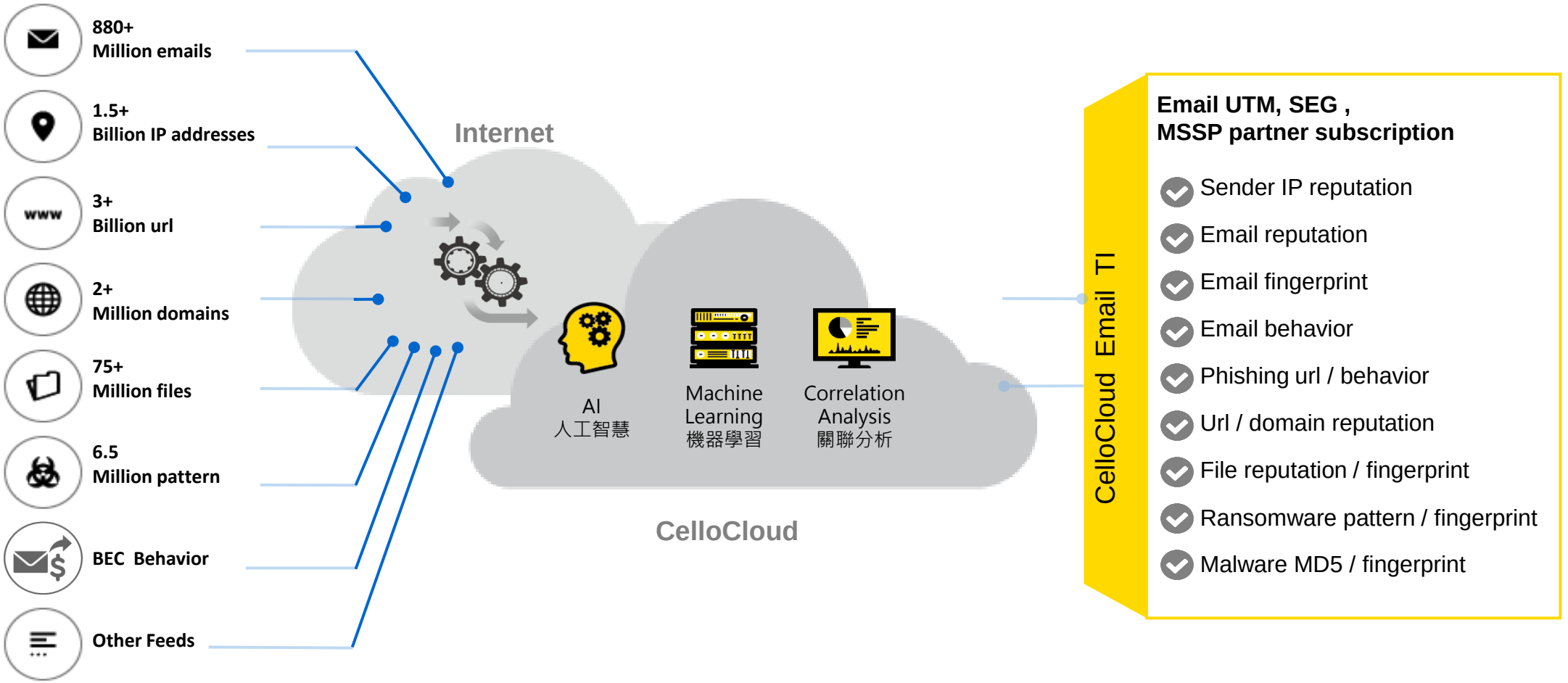
CELLOPOINT
Secure Your Email

七大部署架構

部署	M365 補強方案	寄內郵件安全	寄外郵件DLP	郵件歸檔
SaaS服務	❶ **Cellopoint Defender** - 有效偵測M365 漏攔威脅，如釣魚、勒索、詐騙郵件 - 即時偵測機敏寄外郵件 - 郵件審核，DLP遵循法規	❷ **COP** **雲端寄內郵件安全** - COP- Standard 標準版 - COP-Advanced 進階版 - COP-Complete 完整版	❸ **CODLP** **雲端寄外郵件DLP** - COAUD 寄外稽核 - OCR 圖檔辨識引擎 - COENC 寄外加密	❹ **COA** **雲端郵件歸檔** - 雲端郵件歸檔及合規 - 數位資產保存 - 數位證據查找
公有雲部署		❺ **SEG** **郵件安全閘道器** - AG防垃圾郵件 - AV郵件病毒掃描 - APT-URL防護 - APT-File防護 - BEC變臉詐騙防護	❻ **DLP** **資料外洩防禦** - AUD 寄外稽核 - OCR 圖檔辨識引擎 - ENC 寄外加密	❼ **MA** **電子郵件歸檔** - CAS 郵件案件管理 - GDS 大數據網格搜索 - 數位資產保存 - 數位證據查找
地端部署				
郵件系統	Microsoft 365 Exchange Online	Microsoft 365 Exchange Online Exchange Google Workspace zimbra		

CELLOPOINT Secure Your Email

電子郵件~威脅情報網 CelloTI



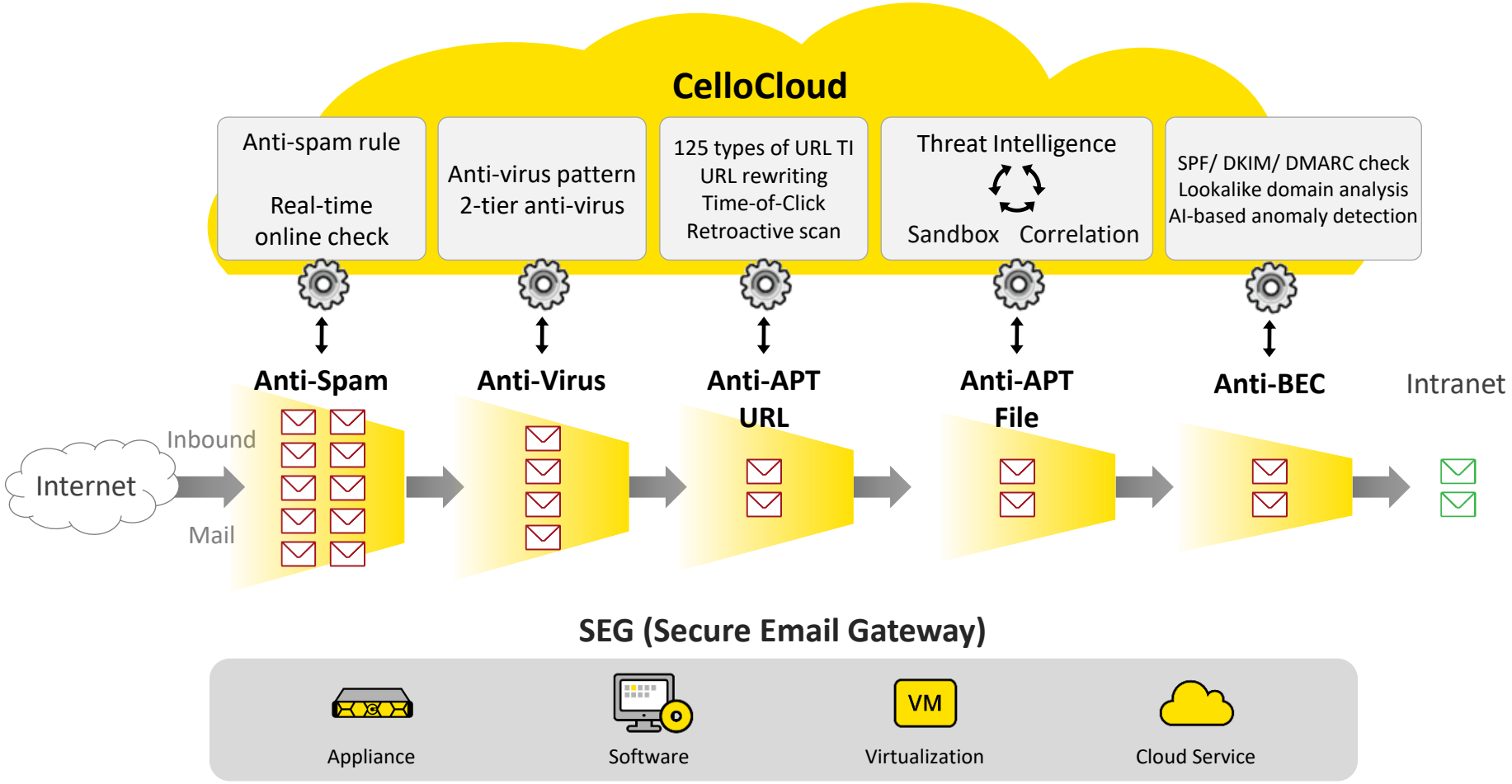
Big Data Sources

Analytics

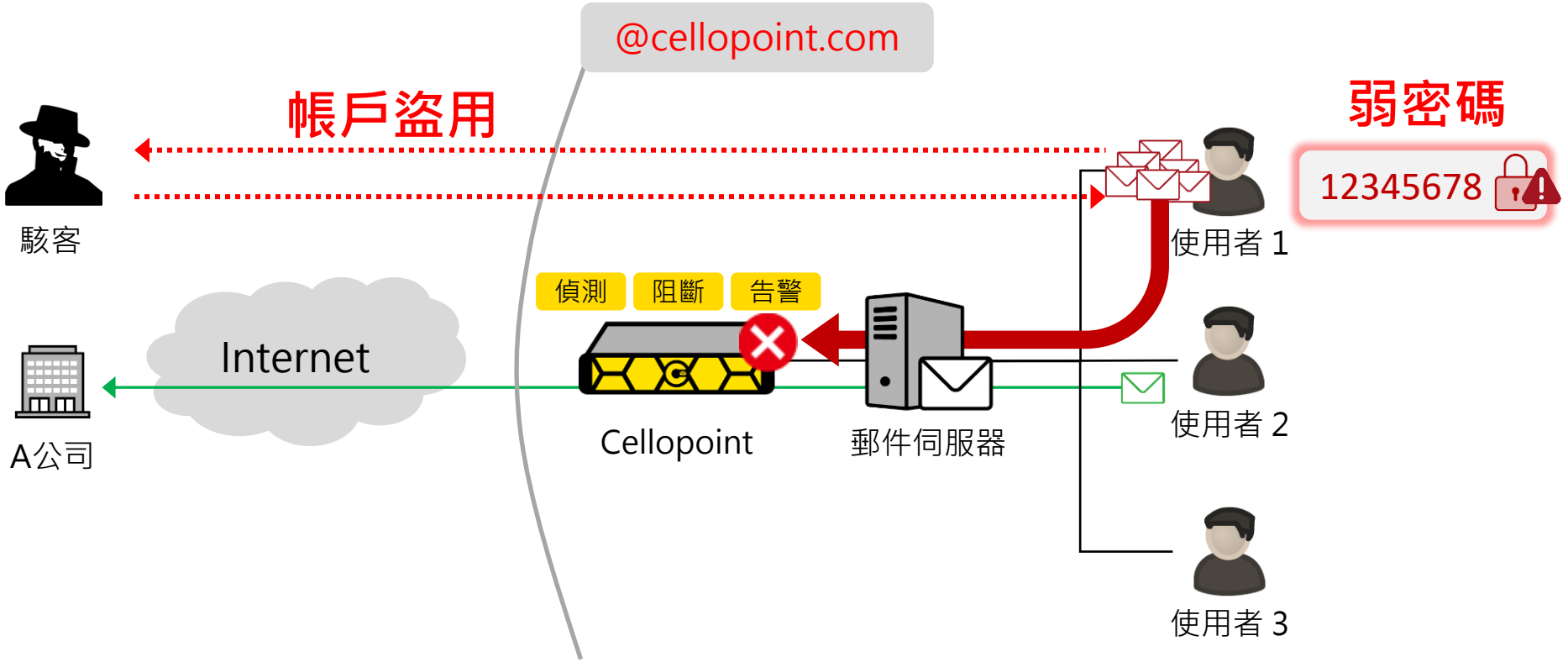
Threat Intelligence

CELLOPOINT
Secure Your Email

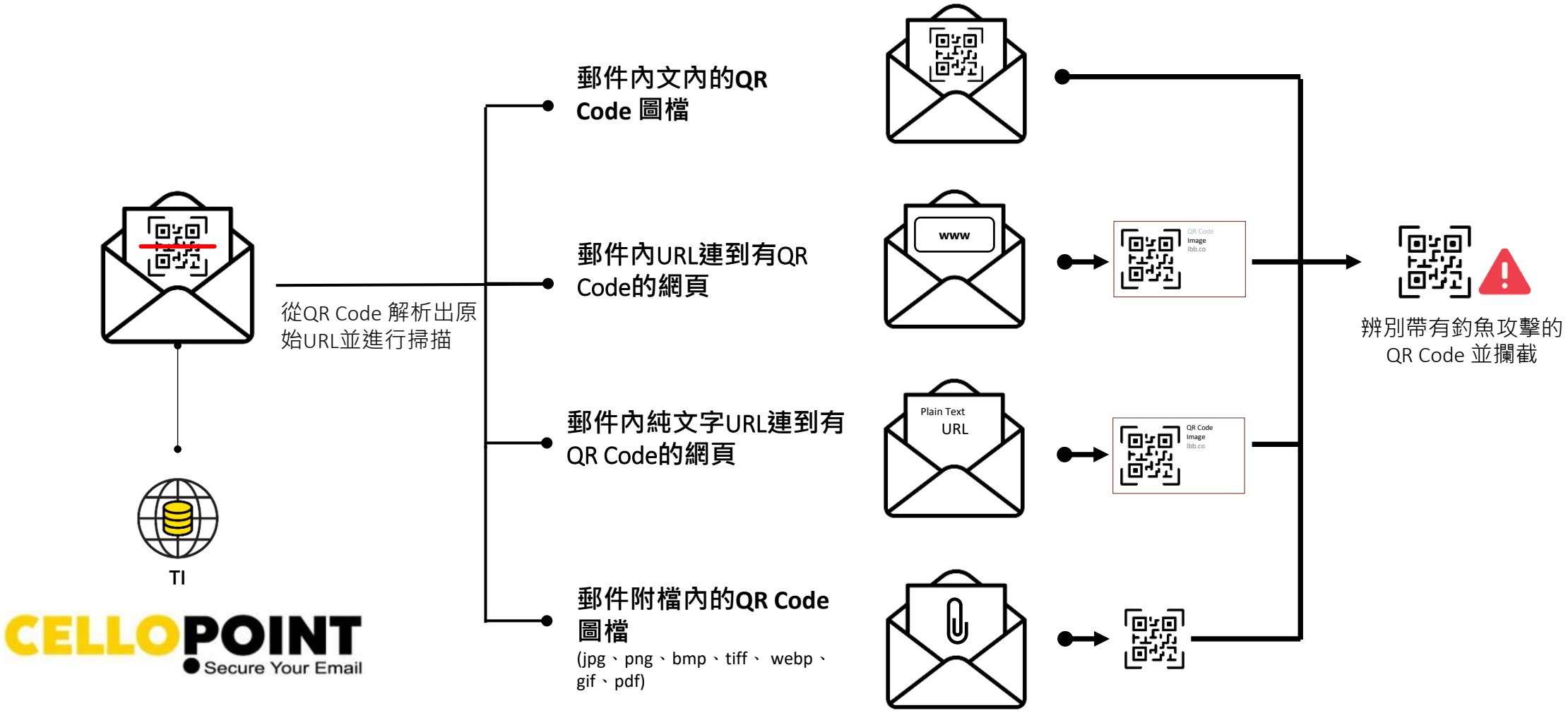
SEG 五層縱深防禦 (完全滿足Gartner 郵件安全新標準)



Cellopoint Outbound Anti-Spam



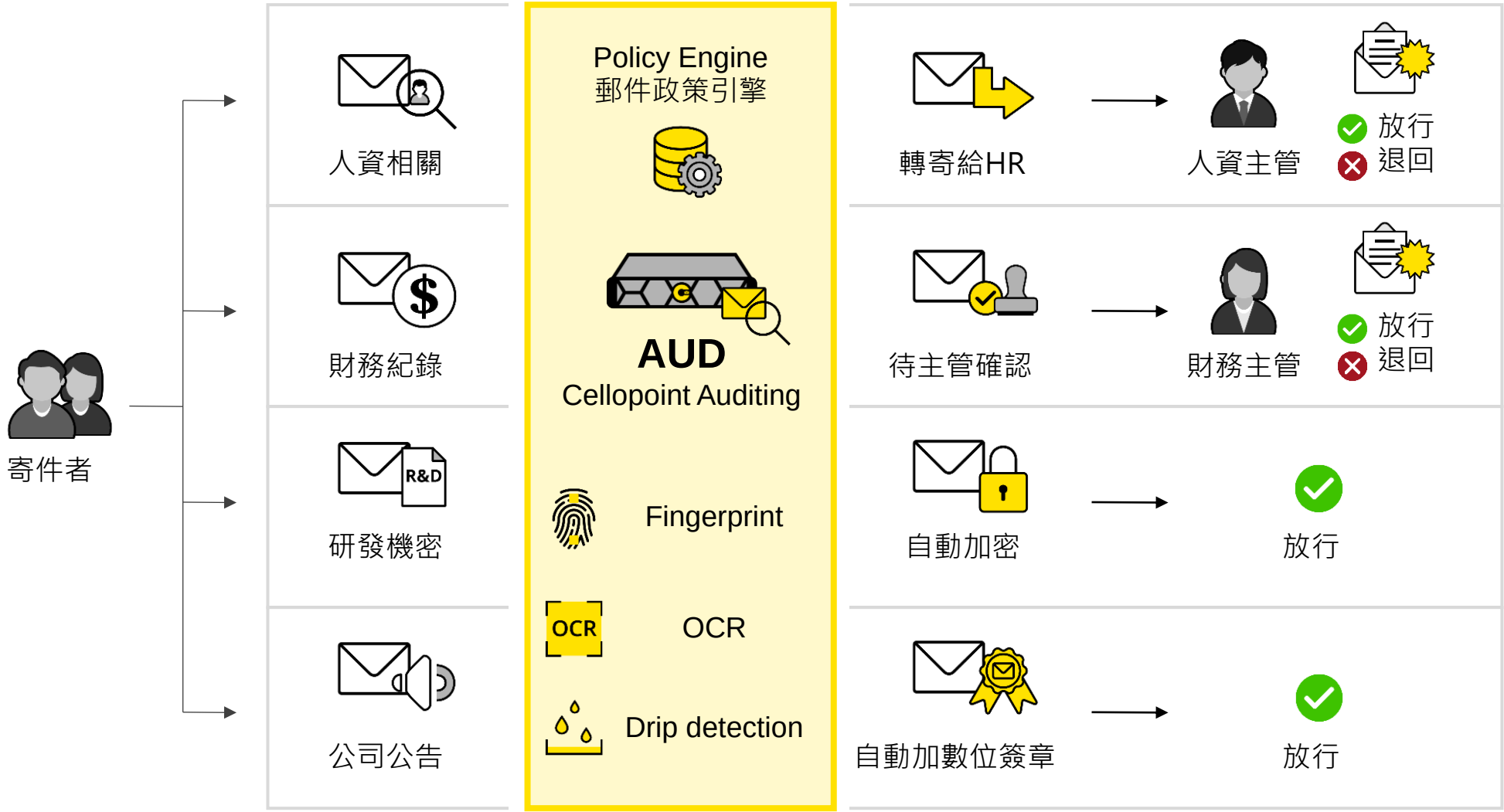
QR Code 釣魚攻擊防護



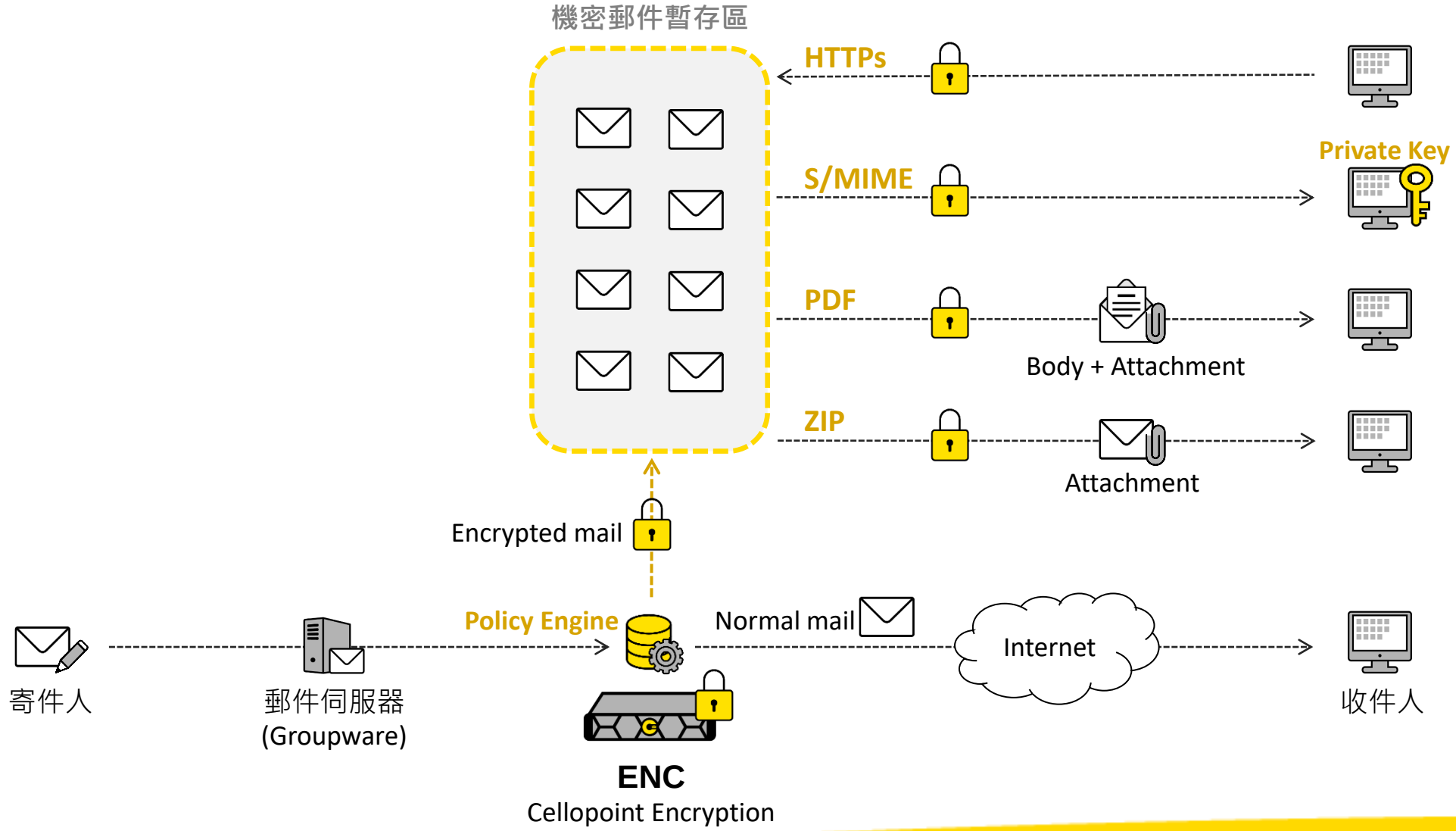
CELLOPOINT
Secure Your Email

CELLOPOINT
Secure Your Email

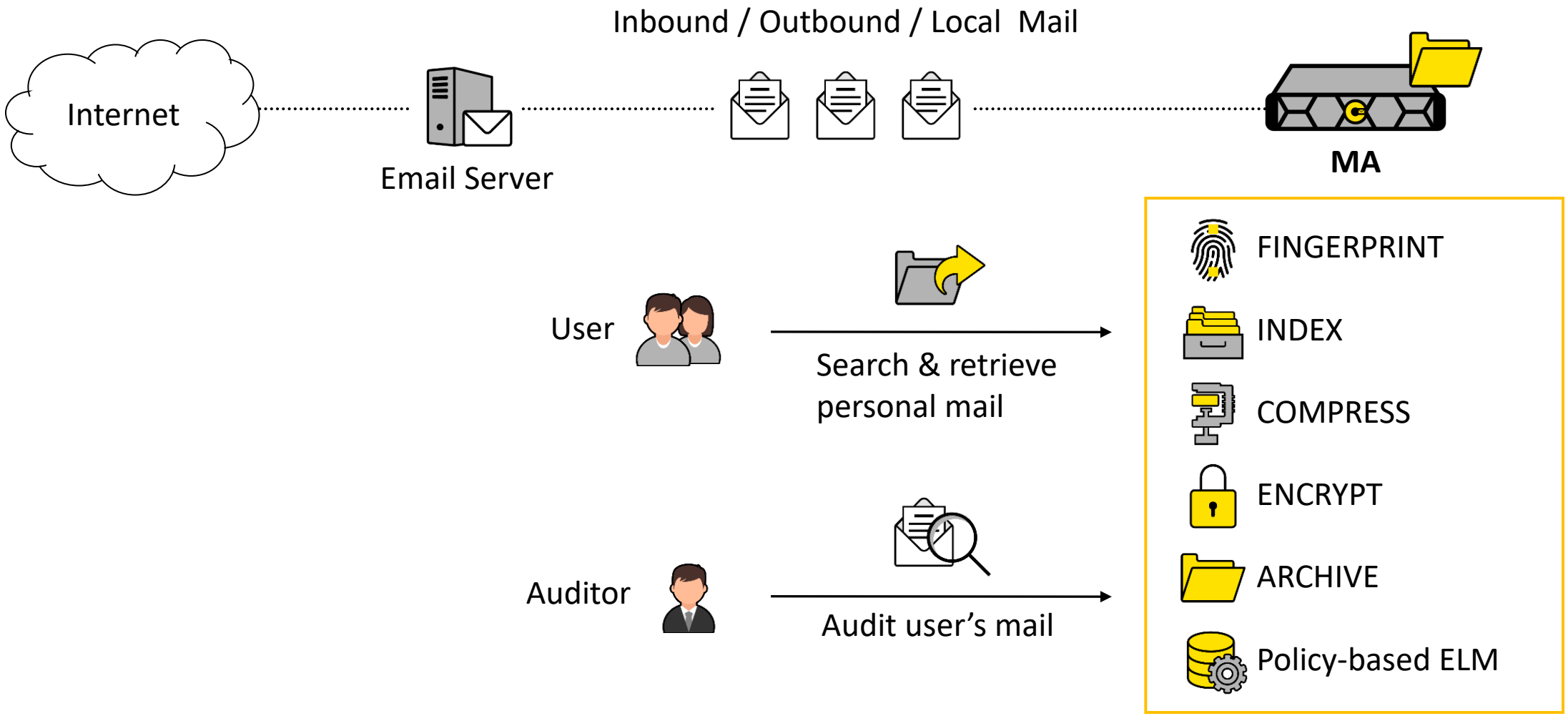
電子郵件稽核 (AUD)


寄件者
人資相關
財務紀錄
R&D
研發機密
公司公告
Policy Engine
郵件政策引擎
AUD
Cellopoint Auditing
Fingerprint
OCR
OCR
Drip detection
轉寄給HR
人資主管
放行
退回
待主管確認
財務主管
放行
退回
自動加密
放行
自動加數位簽章
放行

電子郵件加密 (ENC)


機密郵件暫存區
HTTPs
S/MIME
Private Key
PDF
Body + Attachment
ZIP
Attachment
Encrypted mail
Policy Engine
Normal mail
Internet
寄件人
郵件伺服器
(Groupware)
收件人
ENC
Cellopoint Encryption

電子郵件歸檔 Mail Archiver (MA)



郵件安全治理~四大面向

硬實力 : 五層縱深防禦

- Anti-spam
- Anti-virus
- Anti-APT-URL
- Anti-APT-File
- Anti-BEC

軟實力 : 提升員工開啟郵件警覺心

- 制定郵件安全使用規範
- 郵件安全資安宣導
- 郵件社交工程演練
- 演練統計數字檢討
- 演練後資安講習訓練

關聯威脅分析

- 五層縱深防禦統計分析
- Syslog / CEF log 送往SIEM分析
- 異常事件分析
- 受攻擊對象TopN分析
- 重要對象高風險指標分析

CIO / CISO / CFO / CEO 動起來

- 資訊長推動郵件使用規範
- 資安官推動郵件安全防禦
- 財務長重新檢視匯款SOP
- 執行長支持公司資安動起來

About Cellopoint

- 成立於 2003 年
- 超過 4800 個單位組織客戶
- 卓越研發團隊 (台灣研發製造)
- 中大型企業市佔率第一名
- 佈建全球電子郵件威脅情報網 (Email TI, Threat Intelligence)
- **榮獲國際權威研究機構 Gartner 三項報告肯定**

R&D Center
Sales & Technical Support Office

Taipei Office
(Headquarters)

Gartner
2022 端點安全技術成熟度曲線報告
2022 Hype Cycle for Endpoint Security

Gartner
2023 郵件安全市場指南
2023 Gartner Market Guide for Email Security

Gartner
2023 電子郵件安全供應商推薦列表
2023 Gartner Vendor Identification Tool for Email Security

CELLOPOINT
Secure Your Email

榮獲 Gartner 客戶滿意度 4.9 分評價

Gartner
Peer Insights™

Cellopoint Reviews

4.9 ★★★★★

5.0 ★★★★★ Review Source: ⓘ

Cellopoint's Email Security: Offering Swift Solutions to IT Challenges

Reviewed on Feb 21, 2025

Reviewer Function: Engineering - Other | Company Size: 500M - 1B USD | Industry: Manufacturing Industry

Cellopoint's all-in-one interface is extremely simple and user-friendly, enabling us to quickly and accurately identify email-related issues. With various defens modules, it significantly enhances email security and reduces the likelihood of attacks. In the event of an issue, the IT team ...

Read Full Review

5.0 ★★★★★ Review Source: ⓘ

A Cloud-Based Email Security That Enhances Protection and Simplifies Management.

Reviewed on Mar 10, 2025

Reviewer Function: IT Security and Risk Management | Company Size: 50M - 250M USD | Industry: Healthcare and Biotech Industry

A comprehensive cloud-based email security and DLP solution that effectively addressed the challenges we faced before implementation. It simplifies management, enhances protection against threat, and data loss.

Read Full Review

5.0 ★★★★★ Review Source: ⓘ

Reliable email security with responsive technical support.

Reviewed on Apr 1, 2025

Reviewer Function: IT Security and Risk Management | Company Size: 10B - 30B USD | Industry: Banking Industry

Cellopoint UTM solution effectively stops inbound threats and allows customized settings for enterprise email system protection. Cellopoint high availability transmission rules enable seamless integration with exising systems and email routing for our internal server integration ...

Read Full Review

Thank You

更多產品資訊請見官網: www.cellopoint.com
或來信至: sales.tw@cellopoint.com

CELLOPOINT
Secure Your Email