Openfind™

MAILGATES 郵件防護系統

全方位郵件防護：效能·控管·備援

郵件詐騙防護模組

網擎資訊

TAIWAN EXCELLENCE 2008

vmware READY

citrix ready

IPv6 READY

Openfind™ Software Engineered for Growth™

Agenda

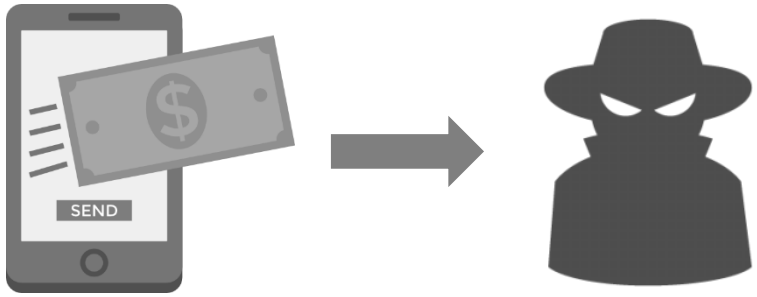
- 什麼是商務電郵詐騙 (BEC)
- BEC 防護機制如何運作
  - BEC 防護政策
  - 信件語意偵測
  - 信件行為分析
- BEC 防護機制畫面

Agenda

- 什麼是商務電郵詐騙 (BEC)
- BEC 防護機制如何運作
  - BEC 防護政策
  - 信件語意偵測
  - 信件行為分析
- BEC 防護機制畫面

什麼是商務電郵詐騙 (BEC)

商務電郵詐騙（Business Email Compromise）又稱**變臉詐騙**，係指透過電子郵件**冒充高階主管**或**合作供應商**藉以騙取金錢或機敏資料



商務電郵詐騙資料統計

- 台灣商務電郵詐騙 2018 年企業損失超過 **2 億元**

2018 年 至 10 月止共 45 件 可能受害案件

2017 年 已回報案件共 54 件

※資料來源：刑事警察局 165 統計，iThome 整理，2018 年 10 月

BEC 高風險群

跨國性
貿易企業

時差隔閡
遠距交易

未能即時
以電話取得聯繫

BEC 攻擊 4 部曲

鎖定目標並研究

- 商業活動
- 合作供應商
- 社交媒體

精心偽造郵件

- 社交工程
- 時間點
- 個人化

急迫性事件

- 無法分辨
- 緊急的
- 合法的

難以預防的結果

- 無法偵測
- 無病毒
- 難以追蹤

BEC 攻擊情境

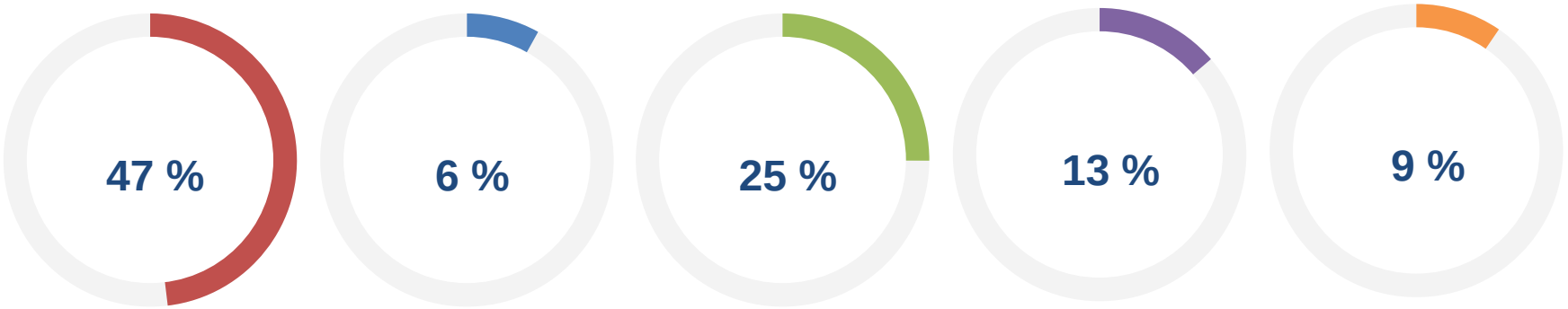
Dear Partner,

匯款帳戶變更通知，請盡快將款項匯到此帳戶，以利後續出貨作業，謝謝。

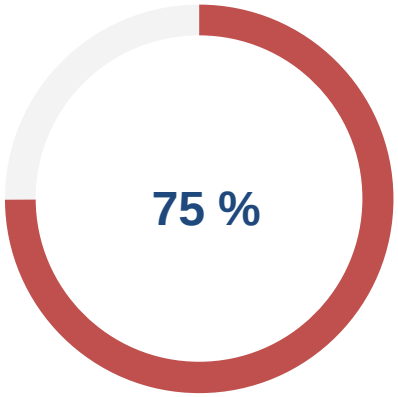
Bill

擔心案件被延誤
情急下趕快匯款

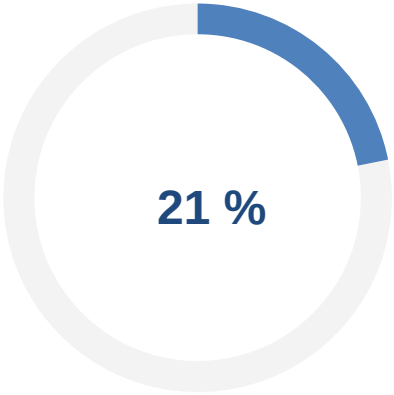
誰被鎖定



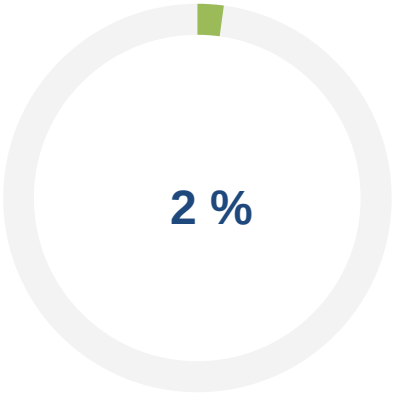
BEC 攻擊手法



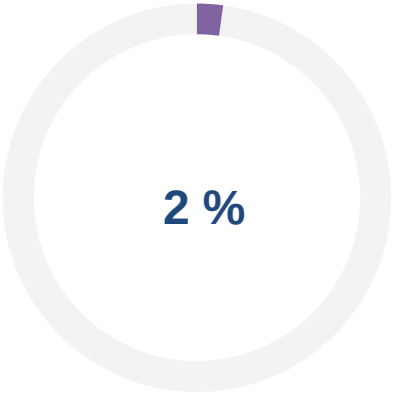
偽造 From 標頭



Reply-to 不符



No Reply-to



相似網域

這封信有什麼問題？

……
From: sales sales@mypartner.com
To: finance finance@mycompany.com
Reply-to: sales sales@spoofing.com
Subject: Urgent! Payment Slip

Dear Sir

Payment have been made and attached is the wire transfer receipt.

Please confirm receipt of payment.

Kind Regards

Johnathon Howson

PRAISE EXPORTS HOLDINGS LLC.
TEL : 011 893 37134
……

郵件內文（收件者看到的部分）

```
EHLO spoofing.com
……
MAIL FROM: evil@spoofing.com
250 Sender evil@spoofing.com OK
RCPT TO: finance@mycompany.com
250 Recipient finance@mycompany.com OK
data
……
From: sales sales@mypartner.com
To: finance finance@mycompany.com
Reply-to: sales sales@spoofing.com
Subject: Urgent! Payment Slip

Dear Sir

Payment have been made and attached is the wire transfer receipt.

Please confirm receipt of payment.


Kind Regards

Johnathon Howson

PRAISE EXPORTS HOLDINGS LLC.
TEL : 011 893 37134
……
```

郵件標頭

郵件內文（收件者看到的部分）

```
EHLO spoofing.com
……
MAIL FROM: evil@spoofing.com ——→ ※信件真實來源，不易假造
250 Sender evil@spoofing.com OK
RCPT TO: finance@mycompany.com
250 Recipient finance@mycompany.com OK
data
……
From: sales sales@mypartner.com ——→ ※偽造的寄件者
To: finance finance@mycompany.com
Reply-to: sales sales@spoofing.com
Subject: Urgent! Payment Slip

Dear Sir

Payment have been made and attached is the wire transfer receipt.

Please confirm receipt of payment.


Kind Regards

Johnathon Howson

PRAISE EXPORTS HOLDINGS LLC.
TEL : 011 893 37134
……
```

郵件標頭

郵件內文（收件者看到的部分）

```
EHLO spoofing.com
……
MAIL FROM: evil@spoofing.com ──────→ ※信件真實來源，不易假造
250 Sender evil@spoofing.com OK
RCPT TO: finance@mycompany.com
250 Recipient finance@mycompany.com OK
data
……
From: sales sales@mypartner.com ──────→ ※偽造的寄件者
To: finance finance@mycompany.com
Reply-to: sales sales@spoofing.com ──────→ ※回覆位址不同
Subject: Urgent! Payment Slip
         ※緊急
Dear Sir

Payment have been made and attached is the wire transfer receipt.
                                                ※匯款請求
Please confirm receipt of payment.


Kind Regards

Johnathon Howson

PRAISE EXPORTS HOLDINGS LLC.
TEL : 011 893 37134
……
```

郵件標頭

郵件內文（收件者看到的部分）

```
EHLO spoofing.com
……
MAIL FROM: evil@spoofing.com ──────→ ※信件真實來源，不易假造
250 Sender evil@spoofing.com OK
RCPT TO: finance@mycompany.com
250 Recipient finance@mycompany.com OK
data
……
From: sales sales@mypartner.com ──────→ ※偽造的寄件者
To: finance finance@mycompany.com
Reply-to: sales sales@spoofing.com ──────→ ※回覆位址不同
Subject: Urgent! Payment Slip
         ※緊急
Dear Sir

Payment have been sent and attached is the wire transfer receipt.

Please confirm receipt of payment.                    ※匯款請求


Kind Regards

Johnathon Howson

PRAISE EXPORTS HOLDINGS LLC.
TEL : 011 893 37134
……
```

疑似詐騙信件

BEC 防護機制

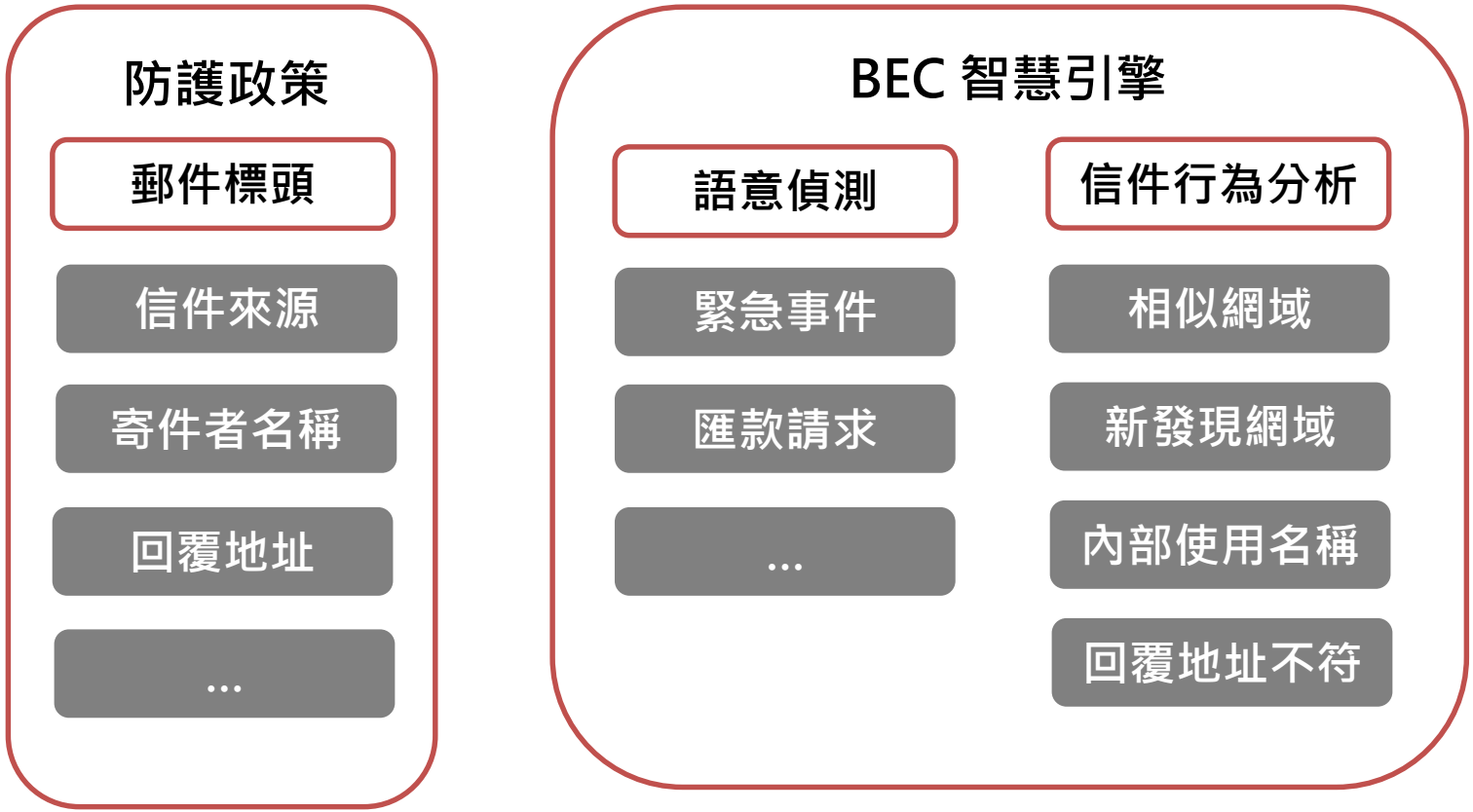
郵件標頭

郵件內文（收件者看到的部分）

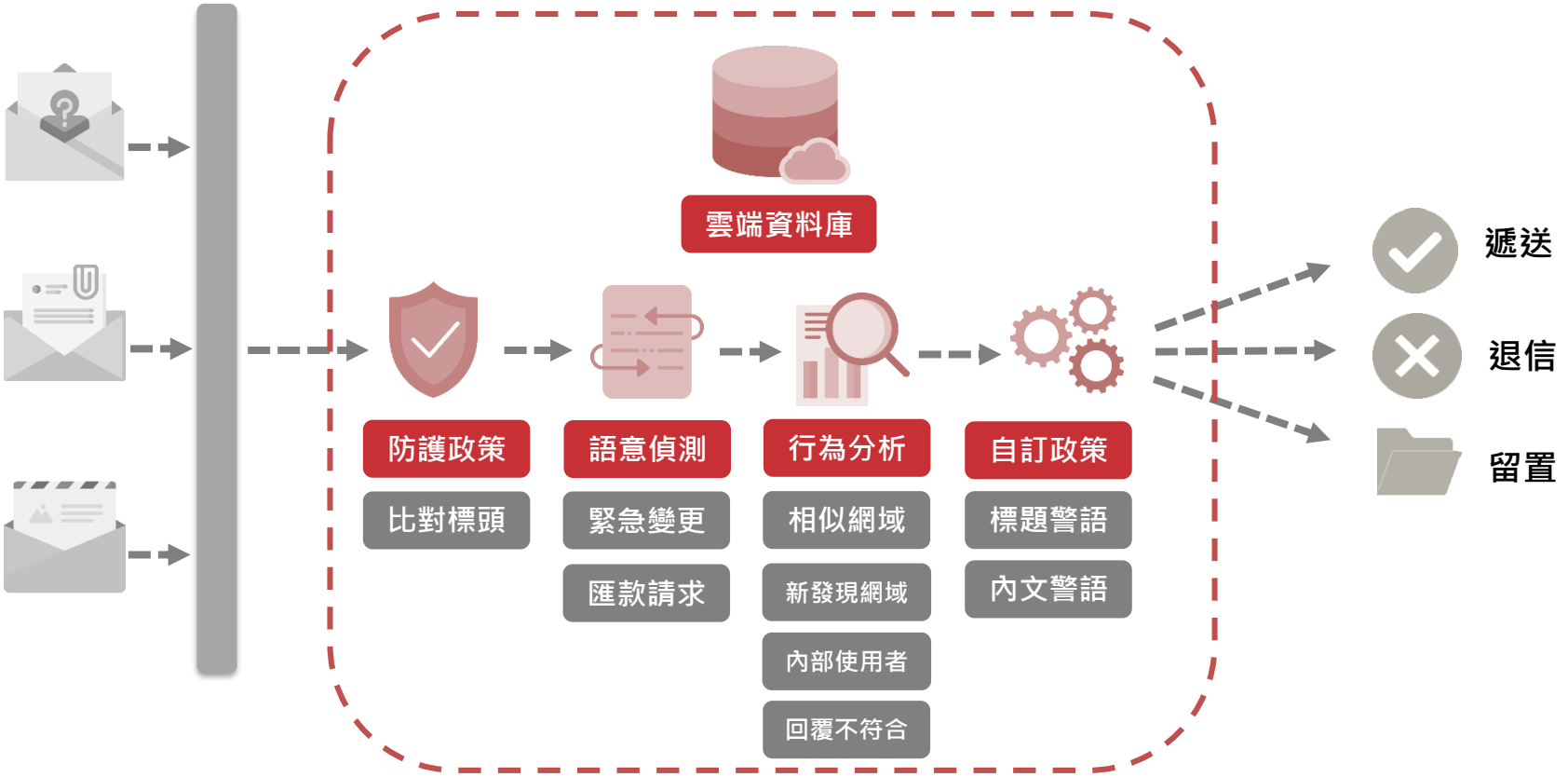
Agenda

- 什麼是商務電郵詐騙 (BEC)
- BEC 防護機制如何運作
  - BEC 防護政策
  - 信件語意偵測
  - 信件行為分析
- BEC 防護機制畫面

BEC 防護機制


防護政策
郵件標頭
信件來源
寄件者名稱
回覆地址
...
BEC 智慧引擎
語意偵測
緊急事件
匯款請求
...
信件行為分析
相似網域
新發現網域
內部使用名稱
回覆地址不符

BEC 防護示意圖



BEC 防護機制

BEC 防護政策 (白名單)

說明：**限制郵件標頭**，若不符合則於標題加上警語。適用於已知往來對象。

範例：

envelope-from : bounce@ofbank.com
mail-from：no-reply@ofbank.com
reply-to：service@ofbank.com

語意偵測 (威脅字典檔)

- 語意偵測
- 緊急、請求
- 變更、更新
- 匯款、轉帳

說明：偵測內文、標題中是否有匯款相關語意

範例：

匯款帳戶變更通知，請盡快將款項匯到附件中的帳戶，以利後續出貨作業，謝謝。

行為分析 – 相似網域

- 行為分析
- 相似網域
- 新發現的網域
- 內部使用者
- 回覆地址不符

說明：偵測是否為相似網域

範例：相似網域的樣式

mailcloud.com.tw -> mailc1oud.com.tw
l ➔ 1 (數字)
openfind.com.tw -> openfind.corn.tw
m ➔ rn
mail2000.com.tw -> mail2000.c0m.tw
o ➔ 0 (數字)

行為分析 – 新發現的網域

- 行為分析
- 相似網域
- **新發現的網域**
- 內部使用者
- 回覆地址不符

說明：偵測寄件者網域是否為新的網域

範例：以 14 天為閥值

10 天前曾寄給 vendor.com (舊網域)

30 天前曾寄給 partner.com (新發現)

未曾寄給 spoofing.com (新發現)

行為分析 – 內部使用者

- 行為分析
- 相似網域
- 新發現的網域
- **內部使用者**
- 回覆地址不符

說明：local-part 是否跟內部使用者相同

peter@internal.com

local-part　　domain-part

範例：
From：peter <peter@internal.com>
內部使用者 peter
From：peter <peter@external.com>
外部網域意圖假冒 peter

行為分析 – 回覆地址不符

- 行為分析
- 相似網域
- 新發現的網域
- 內部使用者
- 回覆地址不符

說明：偵測 From 與 Reply-to 是否一致

範例：

From: sales <sales@mypartner.com>
Reply-to: sales <sales@spoofing.com>
回覆位址不一致

註：Gmail, Hotmail 等免費信箱
沒有 Reply-to 標頭則不檢查

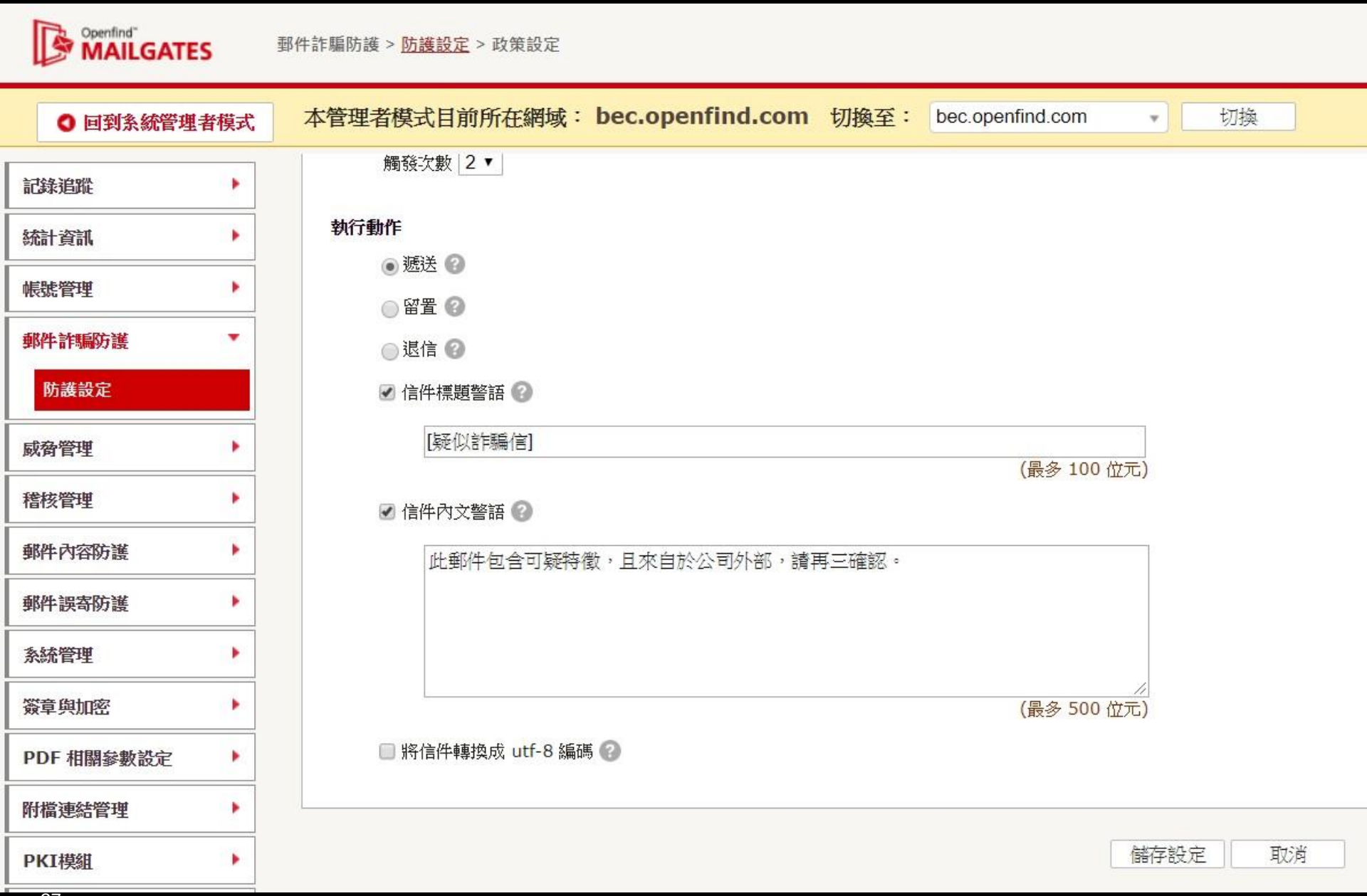
Agenda

- 什麼是商務電郵詐騙 (BEC)
- BEC 防護機制如何運作
  - BEC 防護政策
  - 信件語意偵測
  - 信件行為分析
- BEC 防護機制畫面

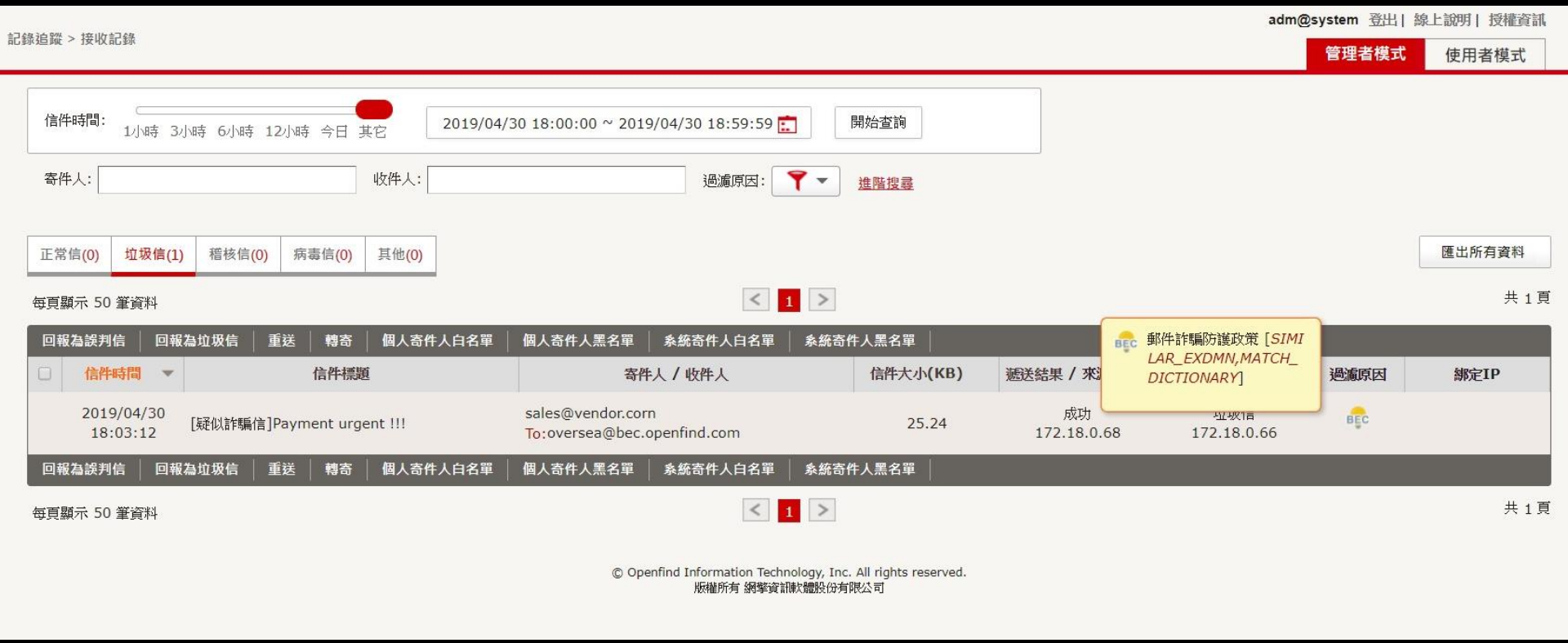
郵件詐騙防護政策


Openfind MAILGATES
郵件詐騙防護 > 防護設定 > 政策設定
回到系統管理者模式
本管理者模式目前所在網域： bec.openfind.com
切換至：
bec.openfind.com
切換
記錄追蹤
統計資訊
帳號管理
郵件詐騙防護
防護設定
威脅管理
稽核管理
郵件內容防護
郵件誤寄防護
系統管理
簽章與加密
PDF 相關參數設定
附檔連結管理
PKI模組
相似外部網域
vendor.com #合作廠商
(最多 100 筆)
新發現的網域
內部使用者名稱
回覆地址不吻合
針對性威脅字典檔
MailGates 威脅字典檔
自訂威脅字典檔
(最多 1000 筆)

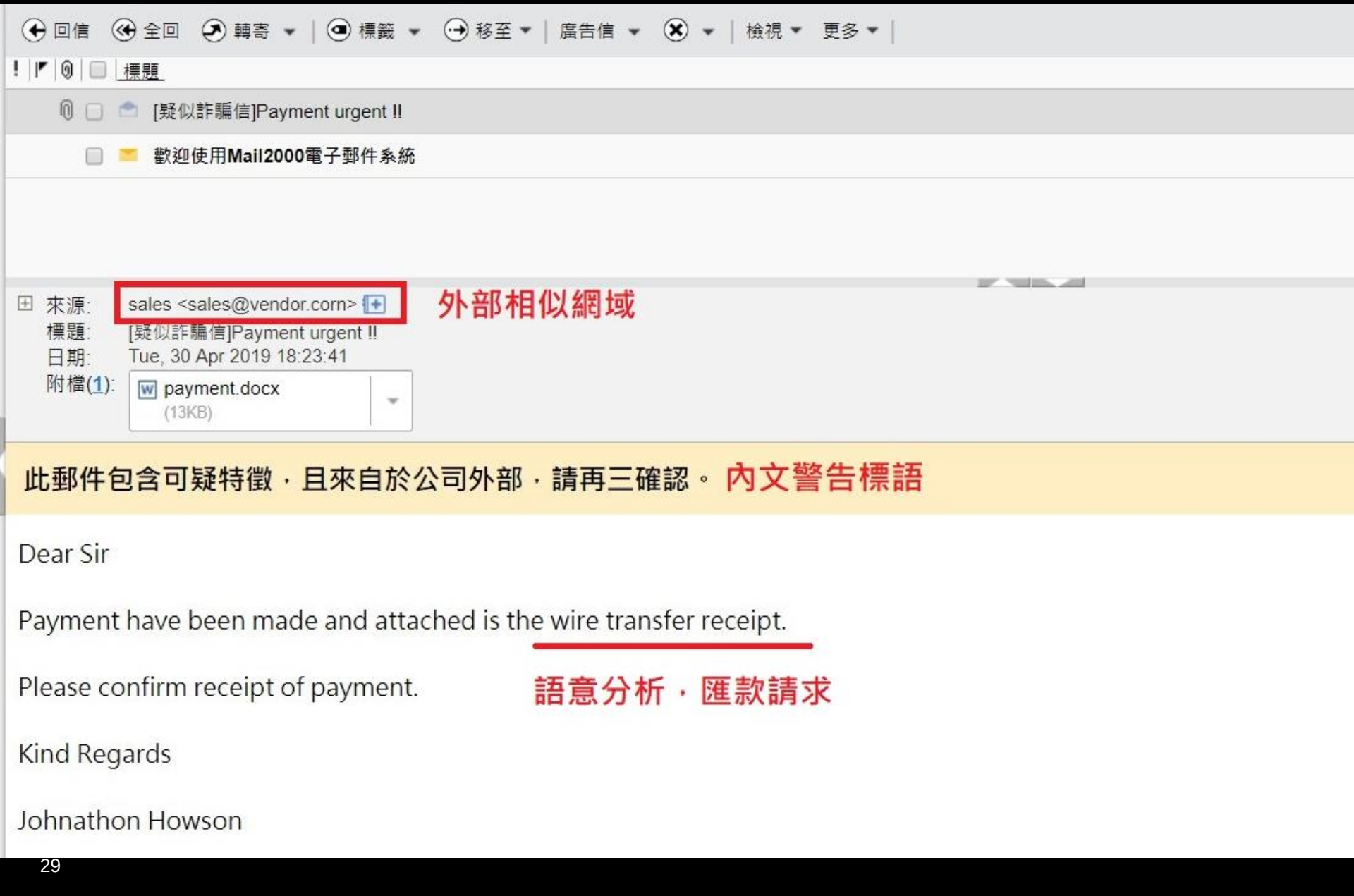
郵件詐騙防護政策


Openfind MAILGATES
郵件詐騙防護 > 防護設定 > 政策設定
回到系統管理者模式
本管理者模式目前所在網域： bec.openfind.com 切換至： bec.openfind.com
切換
記錄追蹤
統計資訊
帳號管理
郵件詐騙防護
防護設定
威脅管理
稽核管理
郵件內容防護
郵件誤寄防護
系統管理
簽章與加密
PDF 相關參數設定
附檔連結管理
PKI模組
觸發次數 2
執行動作
遞送
留置
退信
信件標題警語
[疑似詐騙信]
(最多 100 位元)
信件內文警語
此郵件包含可疑特徵，且來自於公司外部，請再三確認。
(最多 500 位元)
將信件轉換成 utf-8 編碼
儲存設定
取消

觸發郵件防護政策


adm@system 登出 | 線上說明 | 授權資訊
記錄追蹤 > 接收記錄
管理者模式
使用者模式
信件時間:
1小時 3小時 6小時 12小時 今日 其它
2019/04/30 18:00:00 ~ 2019/04/30 18:59:59
開始查詢
寄件人:
收件人:
過濾原因:
進階搜尋
正常信(0)
垃圾信(1)
稽核信(0)
病毒信(0)
其他(0)
匯出所有資料
每頁顯示 50 筆資料
1
共 1 頁
回報為誤判信 | 回報為垃圾信 | 重送 | 轉寄 | 個人寄件人白名單 | 個人寄件人黑名單 | 系統寄件人白名單 | 系統寄件人黑名單
郵件詐騙防護政策 [SIMILAR_EXDMN,MATCH_DICTIONARY]
信件時間
信件標題
寄件人 / 收件人
信件大小(KB)
過濾原因
綁定IP
2019/04/30 18:03:12
[疑似詐騙信]Payment urgent !!!
sales@vendor.corn
To:oversea@bec.openfind.com
25.24
成功
172.18.0.68
垃圾信
172.18.0.66
BEC
回報為誤判信 | 回報為垃圾信 | 重送 | 轉寄 | 個人寄件人白名單 | 個人寄件人黑名單 | 系統寄件人白名單 | 系統寄件人黑名單
每頁顯示 50 筆資料
1
共 1 頁
© Openfind Information Technology, Inc. All rights reserved.
版權所有 網擎資訊軟體股份有限公司

詐騙信件提醒

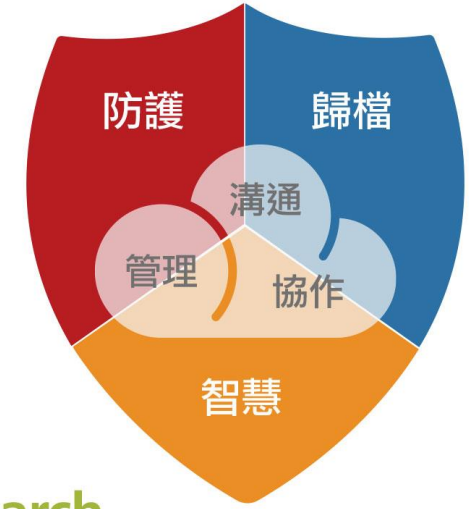

回信
全回
轉寄
標籤
移至
廣告信
檢視
更多
標題
[疑似詐騙信]Payment urgent !!
歡迎使用Mail2000電子郵件系統
來源:
sales <sales@vendor.corn>
外部相似網域
標題:
[疑似詐騙信]Payment urgent !!
日期:
Tue, 30 Apr 2019 18:23:41
附檔(1):
payment.docx
(13KB)
此郵件包含可疑特徵，且來自於公司外部，請再三確認。
內文警告標語
Dear Sir
Payment have been made and attached is the wire transfer receipt.
Please confirm receipt of payment.
語意分析，匯款請求
Kind Regards
Johnathon Howson

Openfind™ MailGates 郵件防護系統

Openfind™ Mail2000 電子郵件系統

Openfind™ MailCloud 企業雲端服務

Openfind™ Enterprise Search 企業搜尋探勘系統



Openfind™ MailAudit 郵件稽核系統

Openfind™ MailCloud Messenger 企業溝通平台

Openfind™ ArkEase Pro 雲端儲存服務

Openfind™ MailBase 郵件歸檔管理系統

Q&A

Email: sales@openfind.com
URL: www.openfind.com