

# 以人為本的資訊安全解決方案

專案規畫:采易資訊系統股份有限公司

專案經理:李昆龍 Anderson. Lee

# 解決方案大綱

解決方案一：移動式裝置洩密與應用程式管制解決方案

解決方案二：eDetective 網際網路資料側錄系統

解決方案三：TrustView 資料加密與離線資料鎖定解決方案

解決方案四-即時通訊管制與強制聲明解決方案

## 解決方案一：移動式裝置洩密與應用程式管制解決方案

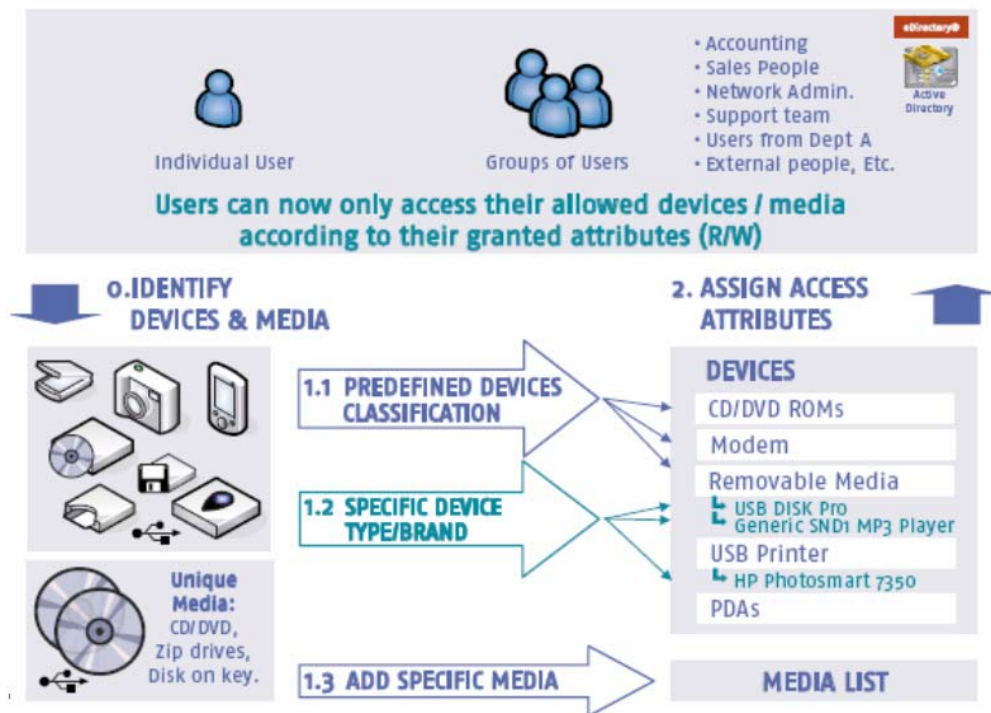
### SDC Solution - Device Control & Application Control

需求:在移動式裝置管理部份,可防止員工透過

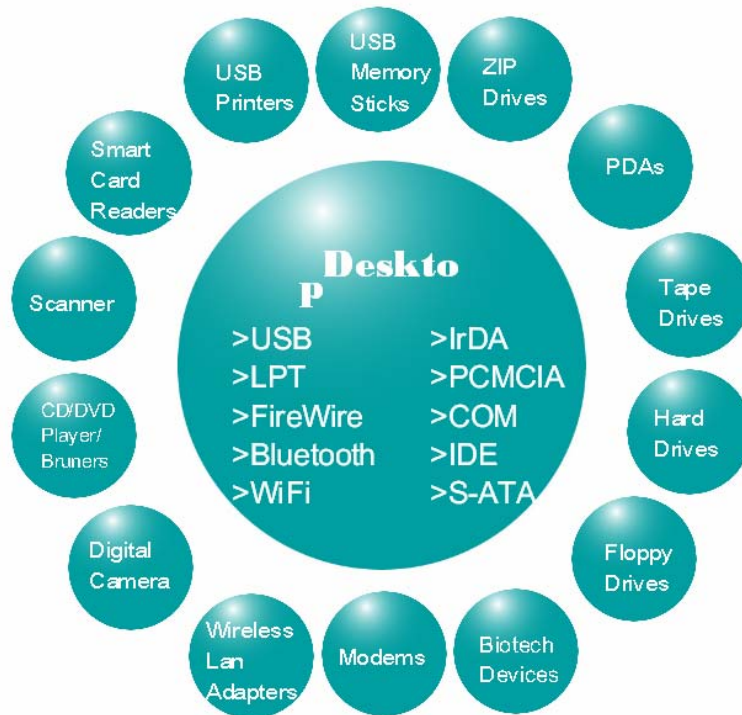
USB. DVD-Writer. Floppy. MO 或是印表機將機密資料輸出至移動式裝置,並藉此攜出公司而造成公司的智慧財產損失.

在應用程式管制部份,可防止使用者任意的下載與執行非法的應用軟體,造成中毒與違法授權的事情發生亦可能因為感染病毒而影響整體網路速度.

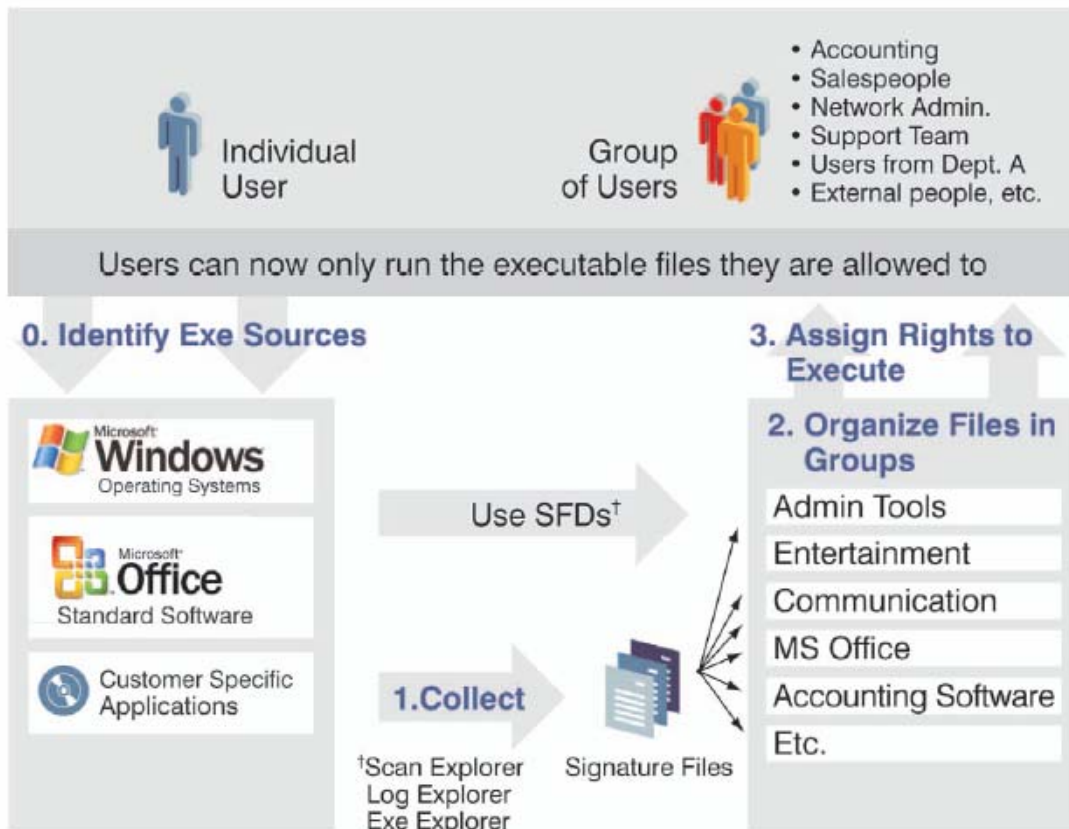
方案架構圖:透過使用者身份來管制移動式裝置的存取權限



可控制的移動式裝置列表：



軟體的管制是依據身份來設定針對軟體的限制與開放名單



解決方案效益：解決方案效益：提供針對 I/O 裝置進行封鎖的與管理，

可針對特定的使用者來管制那些 I/O 裝置可被那些使用者所讀、寫或使用？並且可細部份類到群組，個人並搭配時間可作到何人在何時具備那些 I/O 權利，完全符合資安全保密規定，並可透過此項解決方案管理包含 VD、FLOPPY、硬碟、磁帶、無線、讀卡機、USB、掃描器……等等裝置，以有效遏止資料洩密的資安風險。

可透過使用者帳號來控制那些 AP 應用程式可被那些使用者所開啟執行，有效的避免不當的授權違法與不明程式中毒問題發生，更可透過此解決方案有效進行 AP 管制以有效減少不當的軟體授權支出成本，此方案更可透過中央機制有效回報 AP 的使用情形與次數提供企業網管與 AP 應用的重要參考依據。

### 綜合以上解決方案功能匯總：

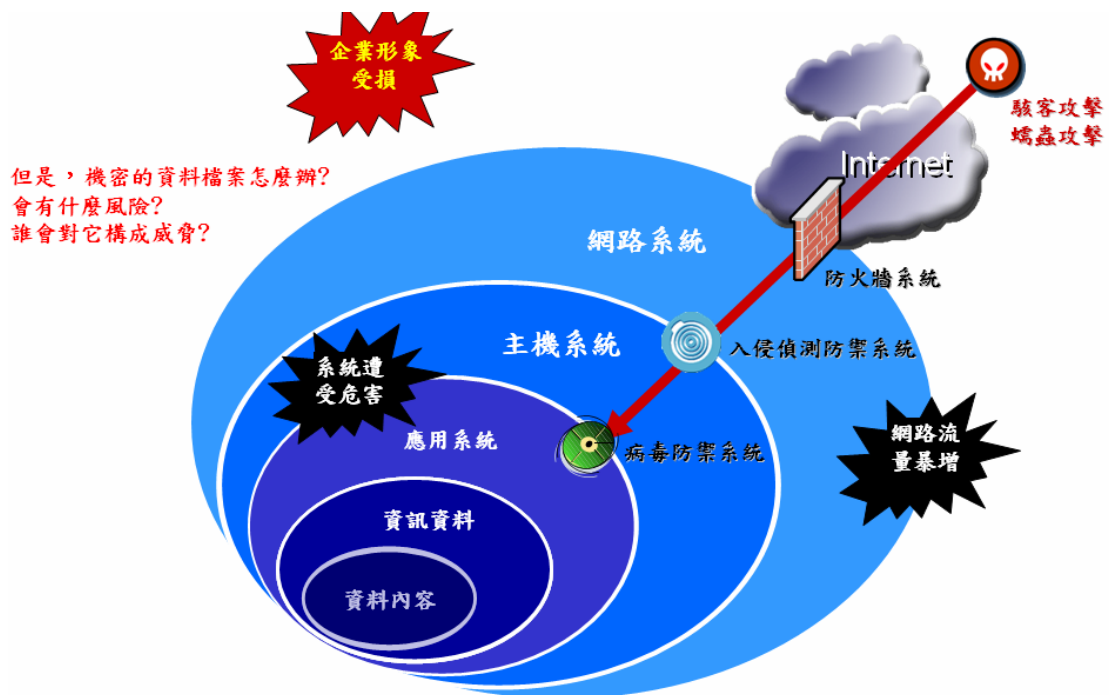
1. 可集中控管 Windows 的所有 I/O 設備，包括 USB, CD/DVD... 各式各樣的輸出輸入設備。
2. 權限管理可依 Local User, AD 或 eDirectory 中的使用者來控管，也可以電腦為依據來設定權限。
3. 可以控制只能讀，或者允許讀和寫。允許寫入時，也可以設定 Shadow 功能，將複製到外接設備的資料另複製一份存檔，做為稽核使用。
4. 可設定設備白名單，只允許已知的設備使用權限，可有效防止未知的設備或媒體資料入侵企業。
5. 可設定應用程式白名單，預設所有程式皆不能執行，只允許白名單中的應用程式才可以被執行。
6. 可以設定臨時性的開放，例如允許使用者在特定的時間使用 USB 硬碟，然後在時間到期後自動關閉。
7. 完整的稽核報表功能，可以針對管理者，使用者與無權限使用者的使用行為做詳盡報表。
8. 離線控管，在未連線狀態下，會依上線時的權限持續控管該電腦週邊設備。
9. 限制資料複製數量，管理者可以允許設備使用，但是限制可以複製的數量。
10. 事件通知訊息，當使用者被拒絕使用裝置時，可立即顯示自訂的中文訊息，讓使用者了解公司的政策。
11. 完整支援 USB、1394 FireWire、藍芽、WiFi... 等所有外接連接埠。

## 解決方案二：eDetective 網際網路資料側錄系統

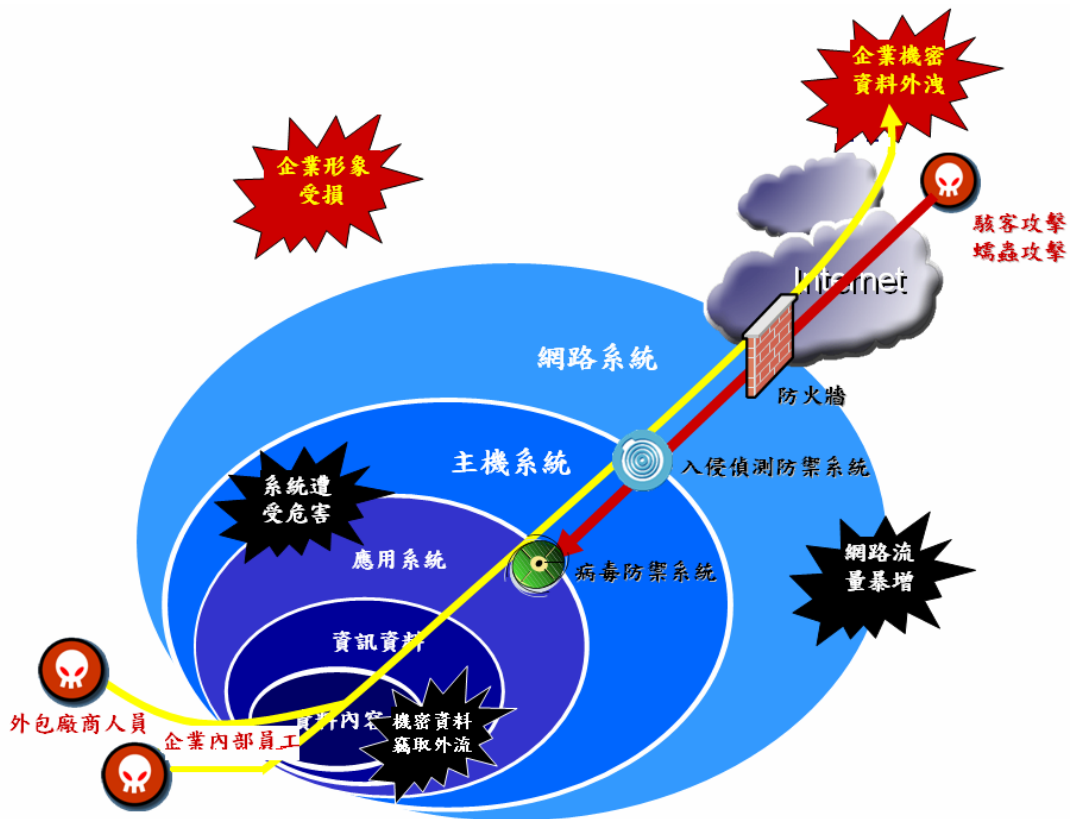
需求：

- ✓ 有一套可管理企業資訊或資料傳遞的系統，以避免洩漏商業機密
- ✓ 該系統可以監控大量的訊息傳遞行為，以避免企業網路資源的誤用
- ✓ 系統於發現異常或違反企業安全政策時，可以即時的發出警告訊息的安全通報功能
- ✓ 擁有一套的證據保存機制，以因應資訊犯罪行為發生時訴訟程序上的需求

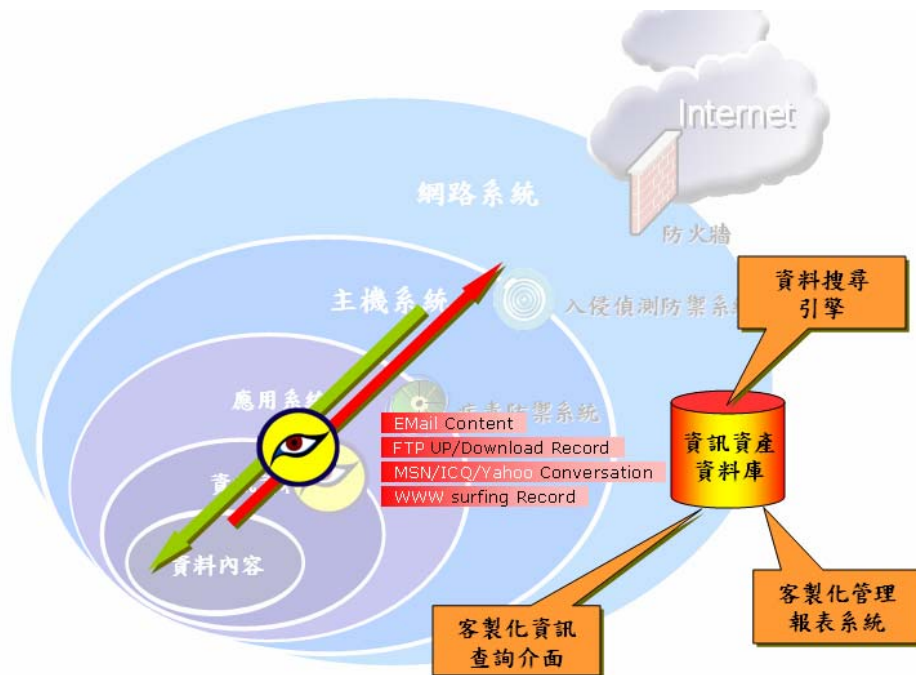
現況架構：



## 透過網際網路洩密攻擊的情況



導入 eDetective 後自動監控與記錄所有存取網際網路的服務資料, 包含 e-mail/Yahoo. MSN. QQ Messenger. WWW. FTP. 與 WebMail 有效作到即時的資安稽核機制. 並且可自訂關鑑字串當發生洩密事件時自動通知稽核人員予以嚴辦.



## 方案效益：

- 即時側錄網路上訊息傳遞的內容(Email、FTP、MSN、ICQ、Hotmail、Web Mail、Web、Telnet)
- 完整的備份企業訊息傳遞的內容及附帶的資料檔案\*\*
- 完整的保留網路存取及傳輸行為，為日後檢調單位進行蒐證的重要依據
- 透過完整的網路行為紀錄，可清楚的了解重要資料被傳送的途徑
- 透過網路使用規則，可制定網路行為適用政策
- 透過個人或整體稽核分析報表，可提供管理或稽核單位進行內稽內控的依據
- 透過資料探勘技術(Data Mining)，可於數量龐大的資料內搜尋關鍵性的訊息
- 提升員工工作效益，節省企業的網路資源
- 可自行定義在指定的時間內，指定範圍電腦不可做特定事項的規則
- 若違反規則，則會自動寄出系統警示糾正信函給違規人員及通報管理者，節省管理者心力時間
- 可自訂糾正信函的內容
- 規則違反的判定可包括：特定網站、收 email、發 email、上傳檔案、下載檔案、網路聊天 ICQ、MSN 及 Web Mail
- 規則可多人及多重設定、可多重自訂警示糾正信函內容。

## 解決方案三：TrustView 資料加密與離線資料鎖定解決方案

需求：員工將公司伺服器上的資料攜帶或是 e-mail 出去以洩漏公司重要的機密文件，造成公司的嚴重損失。

✿ 文件政策、實體檔案分離文件政策雖邏輯上是跟著實體檔案，但實體上須分開管理因此當檔案離開公司還能必加密！

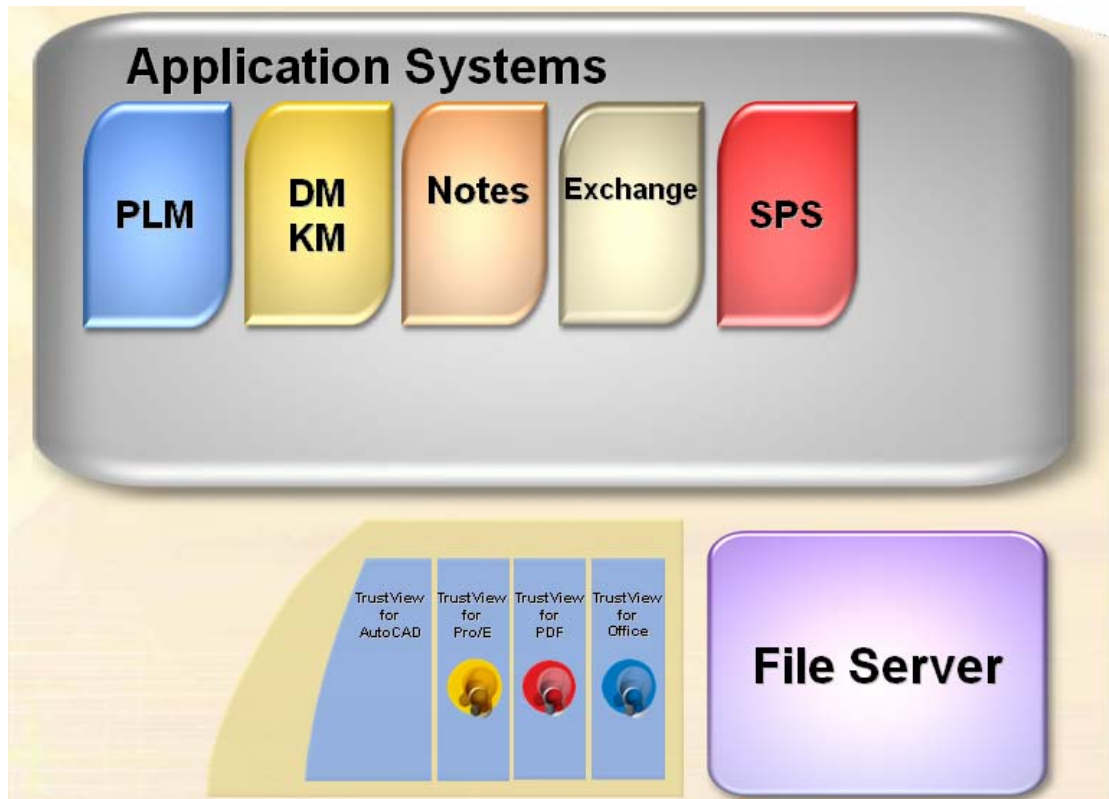
✿ 可動態／及時地更改文件政策權限

- 當然，要有權限的人才能更改，且所有的更動都有紀錄善加利用文件回收、角色管理 善加利用三種認證模式連線 有帳號離線 無帳號離線
- 需要人員離職、異動均可適用

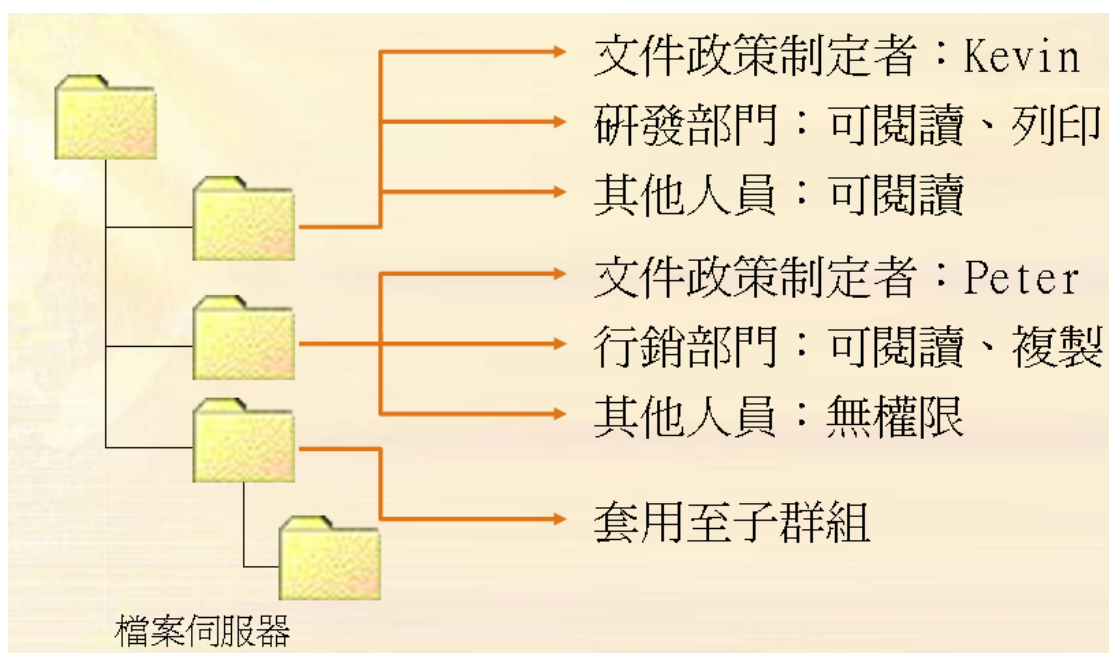
方案可支援的文件類型：

包含 AutoCAD, ProE, PDF, Office 文件依據每種文件來購買授權

以減少不當的成本浪費。



可制定不同的部份或是使用者給予不同的文件權利



## 方案效益：

1. 可自動加密機密文件, 作到文件離開公司網路就開不起來
2. 可設定機密文件的生存時間超過幾天後就再也開不起來
3. 可設定文件的權利, 例如不可螢幕拷貝. 列印. 修改. 另儲新檔
4. 可整合原公司檔案伺服器
5. 可整合原公司 AD 帳號資料庫

## 解決方案四-即時通訊管制與強制聲明解決方案

需求:即時通訊的洩密.傳檔.語音已造成企業嚴重的資安威脅,另外無法強制性的於與客戶進行即時訊息傳送前立即發佈資安聲明另外無法將使用者的 MSN. YAHOO 帳號與實際身份作對映,造成管理相當的困難. 另外 IM 威脅的擴散社交工程導致一般使用者的高感染率感染最常來自於公用的 IM 網路 (AOL、MSN、Yahoo!) 內部擴散會發生於公用與企業 IM 伺服器上混合式威脅利用網路與電子郵件通訊因應的安全方法不足 感染 50 萬台主機所需時間紅色警戒: 14 小時 Slammer: 20 分鐘 IM 病毒: 30-40 秒



### 即時通訊是企業與消費者間重要的通訊工具

- 根據報告, **85%** 的組織有使用 IM
- 全球每天有超過 **3 億 9300 萬** 位 IM 使用者, 送出 **138 億** 則訊息\*



### IM 為企業創造高投資報酬率及競爭優勢

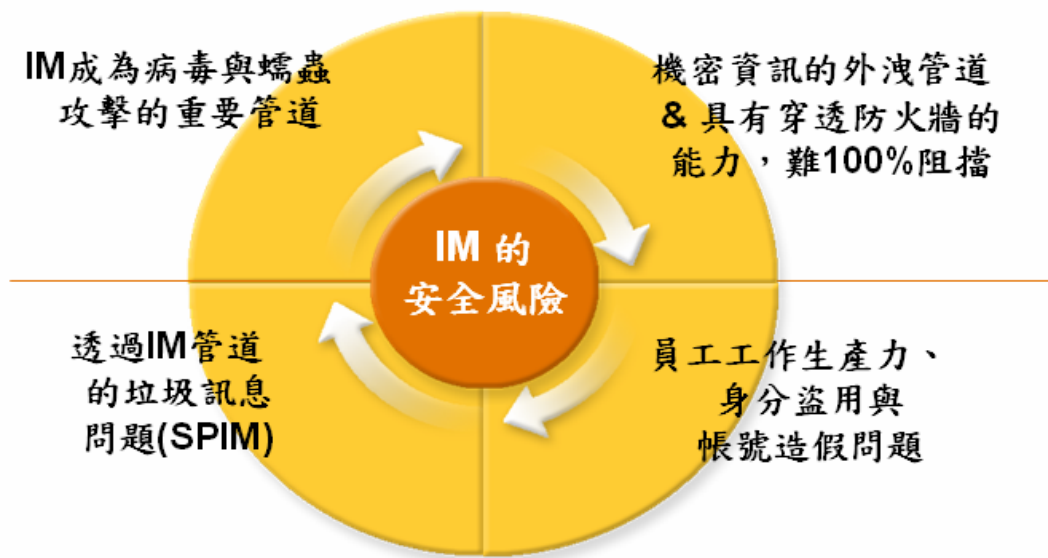
- 在客戶服務與支援上節省 **20%** 的支出
- 減少電子郵件、長距離及差旅支出



### IM 的使用必須滿足企業目前的安全及遵循需求

- 未受保護的 IM 容易遭到病毒與垃圾訊息的攻擊
- IM 亦需遵守電子郵件法規要求
- **90%** 的組織對 IM 沒有任何的 IT 控制

## IM 管理的困擾 & 安全可能風險



### 方案效益:

- 制定公司中的 IM 使用政策, 禁止非授權的使用者使用
- 支援 MSN, Yahoo, AOL, ICQ, Google, IBM Sametime, 微軟 LCS, Routers, Jabber 等即時通訊通訊協定的管理
- 與企業 AD, LDAP 等人員目錄整合, 含使用者認證與政策設定
- IM 顯示名字(Screen Name)的註冊與管理
- 可以依據政策阻擋點對點文件或檔案的傳遞
- 針對交談的訊息內容與附件進行 100%的訊息擷取與備存
- 關鍵字過濾與附檔防毒
- 彈性的政策設定, 可以依據不同的 User/Group 制定
- 內容的審核(獨立的 Auditor 查詢介面)
- **威脅防護與安全**
- 病毒掃描與精細的檔案控管
- IM 病蟲、垃圾郵件與惡意軟體的攔截
- 使用者驗證與授權
- 即時通訊路由
- 用戶端版本控管
- 自動的安全資料庫更新
- **遵循與法務**
- 100% 交談內容擷取率

- 即時的遵循內容過濾
- 記錄、稽核並註解 IM 內容
- 匯出至協力廠商的系統
- 插入法律免責聲明 (Legal Disclaimers)
- **系統管理**
- 即時監控的集中式儀表板(dashboard)
- 細部系統報告與分析
- 使用者註冊與身份識別管理
- 預測式政策強制執行
- IM 使用的可見度與報告
- **通訊與協同合作**
- 聯盟企業的通訊
- 整合式通訊主控台

## 畫面截錄

Display Name	IM Name	IM Network	When Logged In	Duration (hh:mm:ss)	Host Relay Service	Client Version
郭嘉宏	53547701	ICQ	May 30 2006 12:59:55:000PM	47:34:15	10.1.1.212:9091	1.0.703
朱家榮	charles@hotmail.com	MSN	May 30 2006 11:34:33:000AM	48:59:37	10.1.1.212:9091	7.0.0816
楊宗翰	daniel@ms1.hinet.net	MSN	May 30 2006 11:32:52:000AM	49:01:18	10.1.1.212:9091	7.5.0324
江佳蓉	elizabeth@hotmail.com	MSN	May 30 2006 11:28:33:000AM	49:05:37	10.1.1.212:9091	7.5.0324
徐明哲	george@hotmail.com	MSN	May 30 2006 11:18:13:000AM	49:15:57	10.1.1.212:9091	7.5.0324
李志豪	john@hotmail.com	MSN	May 30 2006 11:29:44:000AM	49:04:26	10.1.1.212:9091	7.5.0324
傅佳穎	linda@hotmail.com	MSN	May 30 2006 11:08:34:000AM	49:25:36	10.1.1.212:9091	7.5.0324
江佳蓉	elizabeth@hotmail.com	MSN	May 30 2006 11:28:33:000AM	49:05:37	10.1.1.212:9091	7.5.0324

**Enable Client Version Control**

**Blocked Client Action**

Block the login, and do not send a notification

Allow the login, but block messages and send a notification

Notification message to internal users:

該版本之即時傳訊軟體不被公司所允許, 請更新版本. The version of IM client being used is not supported by your I.T.

Notification message to external users:

對方目前不被允許使用即時傳訊軟體. This recipient is not permitted to use IM.

Type	Name	Value	Groups	Priority	Active	Controls
Disclaimer On/Off	顯示法律聲明	Disclaimer is enabled (and formatted): 基於安全政策, 您的交談內容將被紀錄與稽核. (This c...	<div style="border: 1px solid red; padding: 2px;">           測試群組 (calvin), 測試群組 (lambert)         </div>	1	Active	
				2	Active	

1. 自訂適合的描述

2. 可以為不同的群組設定聲明訊息顯示文案

3. 支援多國語言同時顯示

功能表列	SDC	eDetective	TrusteView	IMM
管制 USB/DVD/Printer	Yes	No	No	No
管制應用程式執行權利	Yes	No	No	No
顯示應用程式使用報告	Yes	No	No	No
防止資料外洩至移動式裝置	Yes	No	No	No
可設定被管制時的中文警告訊息	Yes	No	No	No
可針對寫入 USB 或 CD 之資料進行加密,讓此 USB 或 CD 離開公司網路即無法開啓	Yes	No	No	No
裝置可依據使用者身份與時間來管制,例如業務人於於下安時間無法使用 USB	Yes	No	No	No
監控使用者上網側錄	No	Yes	No	No
監控使用者 FTP 側錄	No	Yes	No	No
監控使用者 Telnet 側錄	No	Yes	No	No
監控使用者 MSN 訊息側錄	No	Yes	No	No
監控使用者 Yahoo 訊息側錄	No	Yes	No	No
監控使用者 QQ 訊息側錄	No	Yes	No	No
監控使用者 WebMail 側錄	No	Yes	No	No
當郵件內容違法規訂時立即警告通知	No	Yes	No	No
主管可以監控屬下訊息資料分層級來監控	No	Yes	No	No
可列出訊息與郵件報告	No	Yes	No	No
可對伺服器檔案加密	No	No	Yes	No
文件離開公司就無法開啓	No	No	Yes	No
文件超過設定的限制時間就無法開啓	No	No	Yes	No
可限制文件無法螢幕拷貝	No	No	Yes	No
可限制文件無法列印	No	No	Yes	No
可限制文件無法修改	No	No	Yes	No
可限制文件無法另儲新檔	No	No	Yes	No
可整合 AD 帳號	No	No	Yes	No
可監控 Yahoo and MSN	No	No	No	Yes
可限制 MSN 不能傳檔	No	No	No	Yes
可限制 Yahoo 不能傳檔	No	No	No	Yes

可強制發出公司聲明	No	No	No	Yes
可整合 IM 列出實際 AD 帳號 與 IM 帳號之對映	No	No	No	Yes
可列出 IM 統計報告	No	No	No	Yes
可設定關鑑字攔截與警告	No	No	No	Yes
150User 預估成本	45 萬	45 萬	60 萬	38 萬

#以上報價為預估未稅價格,實際價格以當時報價為主

#以上方案采易資訊都提供專業且免費的測試與評估報告