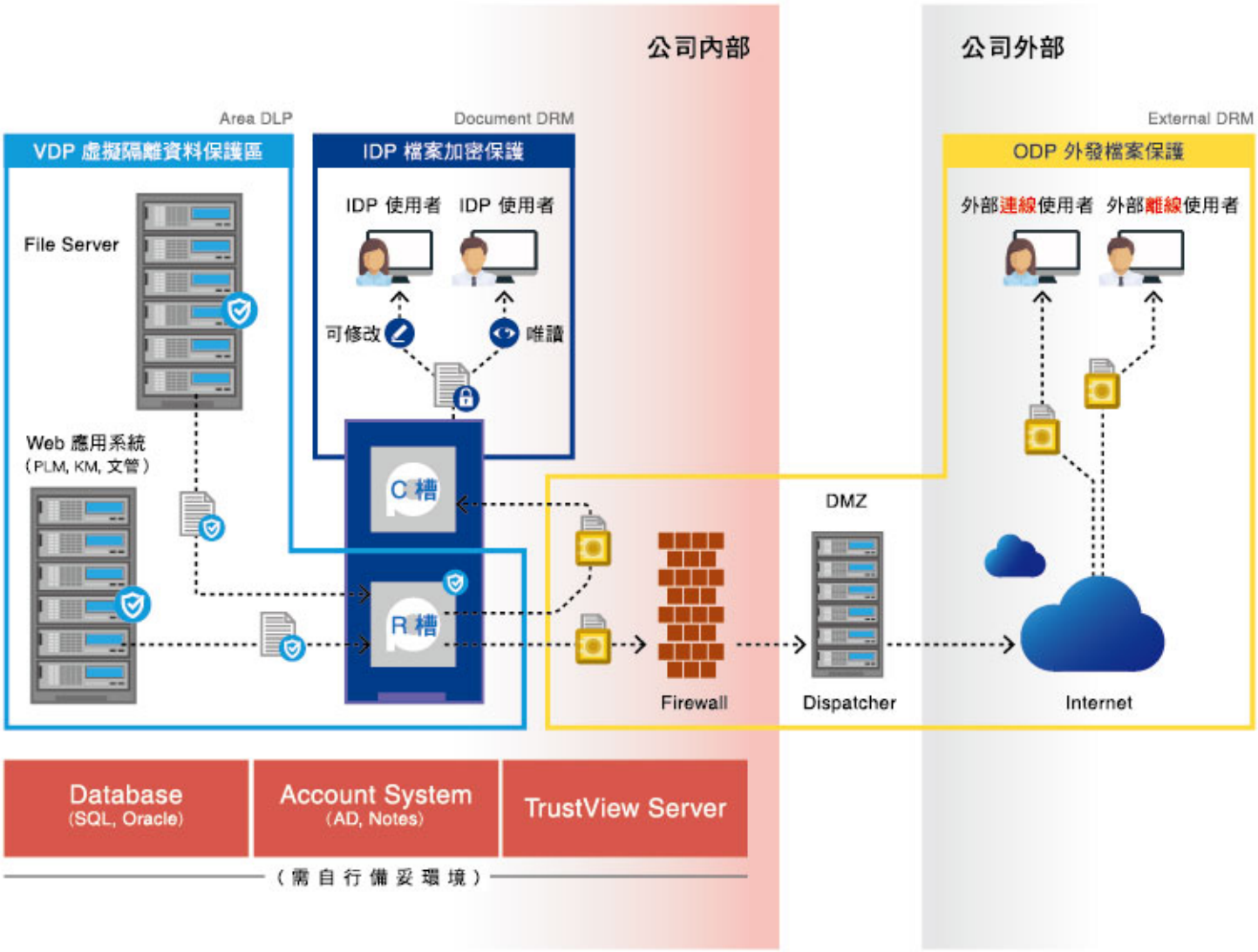
TrustView®

敬告有心人：

想偷文件，註定你來幾次失敗幾次

TrustView 全方位資料保護

TrustView 系統架構圖



資料安全的指揮中心：TrustView Server（伺服器）

高於國際標準的防護等級

- 加密演算採用 RSA 2048 bit、AES 256 bit
- 連線採用 TLS 安全傳輸通道

採取 Web-Base 集中化控管機制

- 便於管理及設定
- 完整詳細的事件紀錄，提供企業稽核的依據

提供多樣化及高可靠度容錯機制

- 提供 Active / Active、Active / Standby 機制
- 可建置 TrustServer Cluster 機制，滿足高可用性、流量分散等需求

提供跨 Site 不同金鑰，TrustServer 建立互信機制

- 可應用 Multi-Threat 方式，同時開啟來自不同 TrustServer 所加密的檔案
- 各 Site 歸各自管控，權限自由且獨立
- 方便各點文件交換分享

防止資料外洩，是企業實務運作上非常困難的挑戰

檔案數位化之後有千萬種好處，但只有在想要防止資料外流時，我們才會懷念以前只需守護一張紙、一本書或一大堆文件的年代，數位資料真是太容易流通了，企業想要防堵與便利性兼顧，真是談何容易：

Email、Skype、存到隨身碟洩密只要一個 Click：
員工可能誤寄，也可能刻意，外流的檔案有如潑出去的水，覆水難收

特殊文件不能被加密控管：
一般的文件控管或加密軟體，僅限於常見的文件格式，許多價值連城的研發設計檔、程式碼只能裸奔

基層員工就能看到太多文件：
公司裡的檔案沒有做好分層管制， 就更容易讓人起貪念

與夥伴或客戶協作文件是另一種形式的洩密：
不能不把文件與他人分享，但其實又無力管制文件日後的流向，只能靠一紙保密合約

周邊控管軟體的權限設定自成一格：
無法與 AD 或現有文管系統整合，IT 人員不僅需要重新設定，日後管理也手忙腳亂

TrustView 協助企業 —— 對的資料，在對的時間，給對的人 且跨越內外，不拘格式

TrustView 資料保護全方位解決方案，是實務上最受企業信賴的資料防護方案，目前已有橫跨台日中、超過 1,000 家企業導入，不僅擁有超過國際標準的安全加密技術，更能產出合乎法規要求的稽核報告，滿足企業安全的最高標準。

而 TrustView 解決方案最精采之處，在於三個層次的文件保護方案設計，企業可視需求獨立導入，建立最便於企業運作的文件安全防護，且不至於過度投資，當然對於文件安全要求最高的企業，三層解決方案的完美配合，將是最佳選擇。

TrustView 內部基礎防護：內部常用文件防護（IDP）

解決企業內部常用文件流通的權限控管並提供防外洩保護，適用檔案類型包括了常用的 Office 及 PDF 格式。

TrustView 內部全面防護：內部全文件防護（VDP）

完全解決企業內部各種文件的防護需求，特別是格式獨特的研發設計檔或可能因檔案加密而損壞的程式檔，採用獨家的虛擬磁區隔離技術。

TrustView 外部無限防護：外部流通全文件防護（ODP）

完全解決企業檔案外寄或外流後無法控管的恐慌，除了可針對外部使用者做權限控管外，一切操作記錄也均回傳企業，檔案就算是齊天大聖，TrustView 就是企業的緊箍咒。

TrustView 內部基礎防護：內部常用文件防護（IDP）

保護企業常用的 PDF、Word、Excel、PowerPoint 檔案

過去您保護重要文件的方式，可能是用 Office 本身的鎖檔功能，或將文件轉 PDF，使用者須輸入密碼才可閱讀或修改資料，但這種加密方式很容易被破解，而且文件量很大的時候，一份一份轉檔耗時又耗力，更無法防止合法使用者洩漏機密，TrustView 的 IDP（Individual Document Protection）可幫您解決所有困擾：

人和文件權限分明，不對的人拿到檔案也打不開

使用者對不同文件有不同權限

例如財務長對會計報表有修改權限，但對業務報表無閱讀權限，就算拿到檔案也開不了

動態權限設定 獨家專利！

Dynamic Policy Mapping：

可隨時針對可疑人員改變或收回原有的權限，將資料外洩風險降到最低

權限控管細膩

可鎖定文件閱讀、列印、複製、儲存、截圖、編輯等功能，並設定權限有效期間

支援 File Server 自動化批次加密

讓機密檔案在誕生的那一刻，就被加密保護，並在每次存檔時套用權限自動加密

整合現有系統，管理輕鬆，使用便利

支援 API 與其他系統整合

如文件管理、PLM、PDM、ERP 等

無需重建新的帳號系統

可整合現有 Microsoft AD、Notes 或 Windchill 等 LDAP 帳號

使用者無須轉檔

不必學習新的操作方法，大幅提升導入成功率

支援行動裝置

包括 Android 及 iOS 平台

應用情境

整合文件管理系統，加強版控

利用 TrustView API 將文管系統的文件進行加密保護；如有新進版的文件入庫，為了確保版本一致性，將會利用 TrustView"動態權限設定"註銷舊版文件權限，此時不管身在何處的舊版文件皆不能再次開啟，需至文管系統上重新下載新版文件。

符合 ISO 文件管理規範，特定文件特定權限

以文件為基礎對不同使用者設定不同的使用權限，讓特定文件只給對的人開啟，在對的時間內，並規範使用者做正確的行為，進而落實 ISO 文件管理規範。

TrustView 內部全面防護：內部全文件防護（VDP）

保護所有格式的文件、圖檔、影音、網頁、原始碼等

檔案加密雖可做到嚴密的權限控管，但可保護的檔案格式較少，還要擔心資料可能因為加密而毀損，而近年猖獗的勒索病毒，以加密手法綁架資料、勒索贖金，更是企業一大隱憂，TrustView 的 VDP（Virtual Disk Protection）跳脫傳統檔案加密困境，更幫您逃離勒索病毒的魔爪：

建立虛擬磁區，機密只進不出，不外洩、不被綁架

勒索軟體無法染指

在內部端點建立虛擬磁區（例如 R 槽），在內部檔案伺服器、Web 應用系統及私有雲建立虛擬隔離保護區，只有合法使用者才看得到、進得去，連勒索軟體都找不到

保護任何格式的檔案

「R 槽」可儲存任何格式的檔案，但只能進不能出，無法攜帶至保護區外（如 Email、通訊軟體、隨身碟、雲端等），只能在保護區內執行

精密的權限控管

包括鎖定列印、複製、截圖、輸出等功能，並可設定「R 槽」有效期限

不擔心資料加密毀損

「R 槽」以 AES 256 bits 加密，網路傳送以 SSL 加密，兼顧安全與效能

系統操作簡單、易用、好管理

不改變使用者操作習慣

並維持後端系統正常運作

支援行動裝置

包括 Android 及 iOS 平台

無須使用 API 整合

即可保護 ERP、SVN、PLM、PDM 等現有 Web 應用系統

成功案例

某 IC 晶片設計公司，成功保護原始碼

導入 VDP 前：

所有原始碼集中存放在版控伺服器，員工很輕易就能帶走資料

導入 VDP 後：

RD 工作流程與導入前相同，版控系統可正常使用，即使離線也能在保護狀態下正常運作

某手機平板代工大廠，成功保護設計圖檔

導入 VDP 前：

RD 和 PM 人員都可將設計圖檔從 PDM（產品研發管理系統）取出，在 PC 上修改和檢視

導入 VDP 後：

無須整合 API，就可正常使用 PDM，RD 修圖及 PM 看圖軟體也都能正常使用

TrustView 外部無限防護：外部流通全文件防護（ODP）

協同合作更安心，保護所有格式的檔案

大多數資料外洩，都是在資料的流動中發生，如果您已有 DLP 防護機制，但缺乏檔案外發後的防護方式，或上下游協力廠商、客戶無法配合安裝 Client Agent，TrustView 的 ODP（Outgoing Document Protection）可讓您放心外發檔案，檔案到哪裡，保護就到哪裡：

外發資料的虛擬保險箱，協同合作安全更方便

不對的人拿到檔案也打不開

每個 ODP 檔可包含多種檔案，不同使用者開啟 ODP 檔，會自動套用不同的權限控管，確保資料不被濫用、不外流

支援眾多格式的檔案

包括文件檔、圖檔、影音、網頁、原始碼、應用軟體等

儲存方式多元

資料可儲存在網站伺服器、檔案伺服器、光碟、磁片，或以 Email 傳送

權限控管細膩

可設定密碼保護，也可鎖定文件閱讀、列印、複製、儲存、截圖、編輯等功能，並設定權限有效期間

提供多種使用機制

如安裝版、免安裝版、連線、離線機制等，提高協同合作的便利性

企業可追蹤資料的動態

製作及使用 ODP 檔皆有稽核紀錄，掌握資料出門後的每一步

成功案例

某手機筆電代工大廠，成功保護外發圖檔

導入 ODP 前：

簽訂 NDA（保密協議）後，直接將原始圖檔提供給協力廠商作業，並無強制約束力

導入 ODP 後：

ODP加密圖檔提供協力廠商使用時，可被控管複製、列印、編輯等行為，確保外發圖檔安全。

某財團法人查驗中心，成功保護委外文件

導入 ODP 前：

簽訂 NDA（保密協議）後，將待審核文件直接寄給委員，審核完畢無法回收在外部之重要文件。

導入 ODP 後：

外發的 ODP 加密文件，可設定有效使用期限或即時註銷使用權限，讓文件變成覆水"可"收。