

【2016台灣資訊安全大會】

防止內鬼竊取營業秘密
符合主管單位與法規稽核要求
發現、阻斷加密勒索等惡意軟體

Varonis

檔案存取記錄、權限管理
機敏資料搜尋、即時警報
使用者行為分析軟體



Varonis 產品簡報

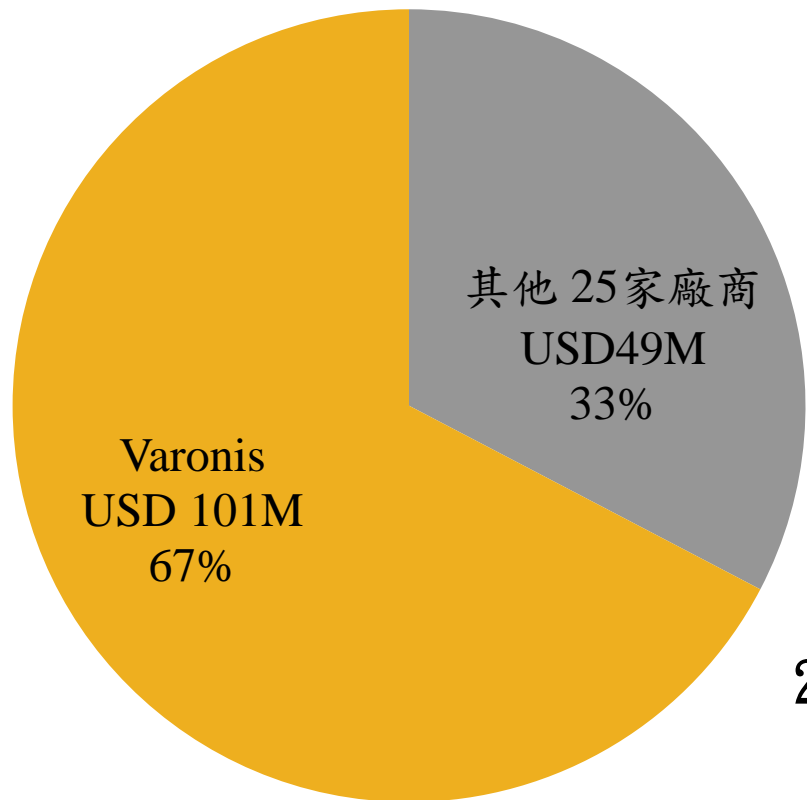
2016-03-08

商丞科技 股份有限公司
Brian Lee 02-29148001 ext 2251
brian_lee@proware.com.tw

Gartner 2015 File Analysis 市佔率最高廠商



- Varonis 擁有超過 4,300 使用客戶
- File Analysis 檔案分析市場規模在 2014年約為 \$150 million
- Varonis 佔據約 \$101 million 收入，剩下由其他 25家廠商分
享



2014年銷售分析



2015年 Network Computing Awards



**Varonis Metadata Framework Voted 2015 Software Product of the Year
Readers of U.K.'s Network Computing Magazine Select Varonis for Top
Honors**

2016年 使用者行為分析(UBA) 金牌得主



The Varonis DatAlert solution has been recognized as a Gold winner of the Info Security Product Guide's 2016 Global Excellence Awards® in the User Behavior Analytics (UBA) category.

News Release: <https://www.varonis.com/varonis-continues-to-win-recognition-for-leadership-in-user-behavior-analytics/>

企業的協作平台



電郵以及檔案共享目錄
是企業兩個最重要的協作平台

資料管控的基本問題

- **問題一** 一般企業或政府部常把最重要的資料存放在 檔案伺服器、SharePoint 與 Exchange 伺服器。但是 IT 往往 都不能夠回答以下的基本問題：
 - 誰 有權限 訪問某些 檔案、電子郵件？
 - 誰 碰過那些檔案、電子郵件？
 - 誰 應該有權限 訪問某些資料？
 - 誰是檔案跟目錄的 資料擁有人？
 - 那些檔案跟目錄存放著 敏感資料？是否有設定 權限管理？
 - 誰 在 搜尋資料？搜尋那些資料？是否搜尋 沒有 使用權限 與 敏感 的資料？
- **原因一** 權限控管很多時候已經 失控 了，現有的 檔案稽核追蹤 的方式跟本沒有效率。
 - 員工不斷的轉換 角色、團隊、功能，每次轉換IT都會新增權限，但是很少機會IT會撤銷權限。
 - 結果就是～企業裡面很多員工所擁有的權限，比他們工作所需要的多出很多。
 - 員工使用 搜尋引擎找到 沒有存取權限與機敏資料。

Varonis 能做甚麼？

1. 找出高風險區敏感資料並協助減低風險 Identify High Risk Data and Remediate Risk
2. 權限控管 Permission Management
3. 完整稽核追蹤 Complete Audit Trail
4. 使用者行為分析 User Behavior Analytics (UBA) 與 即時警報

- * 知道你的 file server 發生什麼事 (人、事、時、地、物)
- * 知道你的 file server 存放那些敏感資料與 面臨風險
- * 知道你的 mail box 發生什麼事 (人、事、時、地、物)
- * 知道誰在搜尋資料(人、事、時、地、物)
- * 知道那些人的檔案存取行為異常？是否有大量資料拷貝、刪除或加密等 情形？並立即違規阻斷行為

常用的 Varonis 應用

1. 防止內鬼

- 完整、詳細的使用者行為記錄、分析
- 檔案存取權限管理控制
- 異常行為警告、分析
- 準確的即時警告 (Real Time Alert)

2. 符合法規稽核要求

- 完整、詳細的稽核報告
- 檔案存取權限清查報告
- 機敏資料搜尋、權限設定與存取記錄報告

Varonis 產品

■ DatAdvantage 檔案存取稽核記錄、 敏感資料搜尋與權限管理

- Windows : (CIFS 協定)
- Unix/Linux : (NFS 協定)
- Sharepoint
- Exchange
- NAS 設備(CIFS 與 NFS 協定)
- Directory Service (Windows AD)
- 資料分類(Data Classification)
 - Windows : (CIFS 協定)
 - Unix/Linux : (NFS 協定):
 - Sharepoint :

■ Data Transport Engine 資料遷移

- 提高儲存效率

■ DatAnywhere 私有雲檔案分享

- 在安全與可稽核下將資料行動化

■ DatAnswers 安全的企業搜尋軟體

- 過濾權限與敏感資料的搜尋結果

■ DatAlert 即時警報通知

- 可過濾條件、準確的即時警

■ DatAlert Analytics

- 使用者行為分析 UBA

■ DataPrivilege 存取權限申請、審核 流程與道德牆

- Windows : (CIFS 協定)
- Sharepoint

Varonis for MS Office 365 產品

■DatAdvantage 檔案存取稽核記錄、敏感資料搜尋與權限管理

—DatAdvantage® for OneDrive

—DatAdvantage® for SharePoint Online

—DatAdvantage® for Exchange Online

備註：目前可用版本為下列 Lite 版本（權限檢視）

—DatAdvantage® for SharePoint Online Lite

—DatAdvantage® for Exchange Online Lite

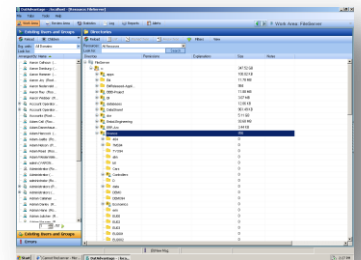
—DatAdvantage® for OneDrive Lite

—敏感資料搜尋分類 Data Classification

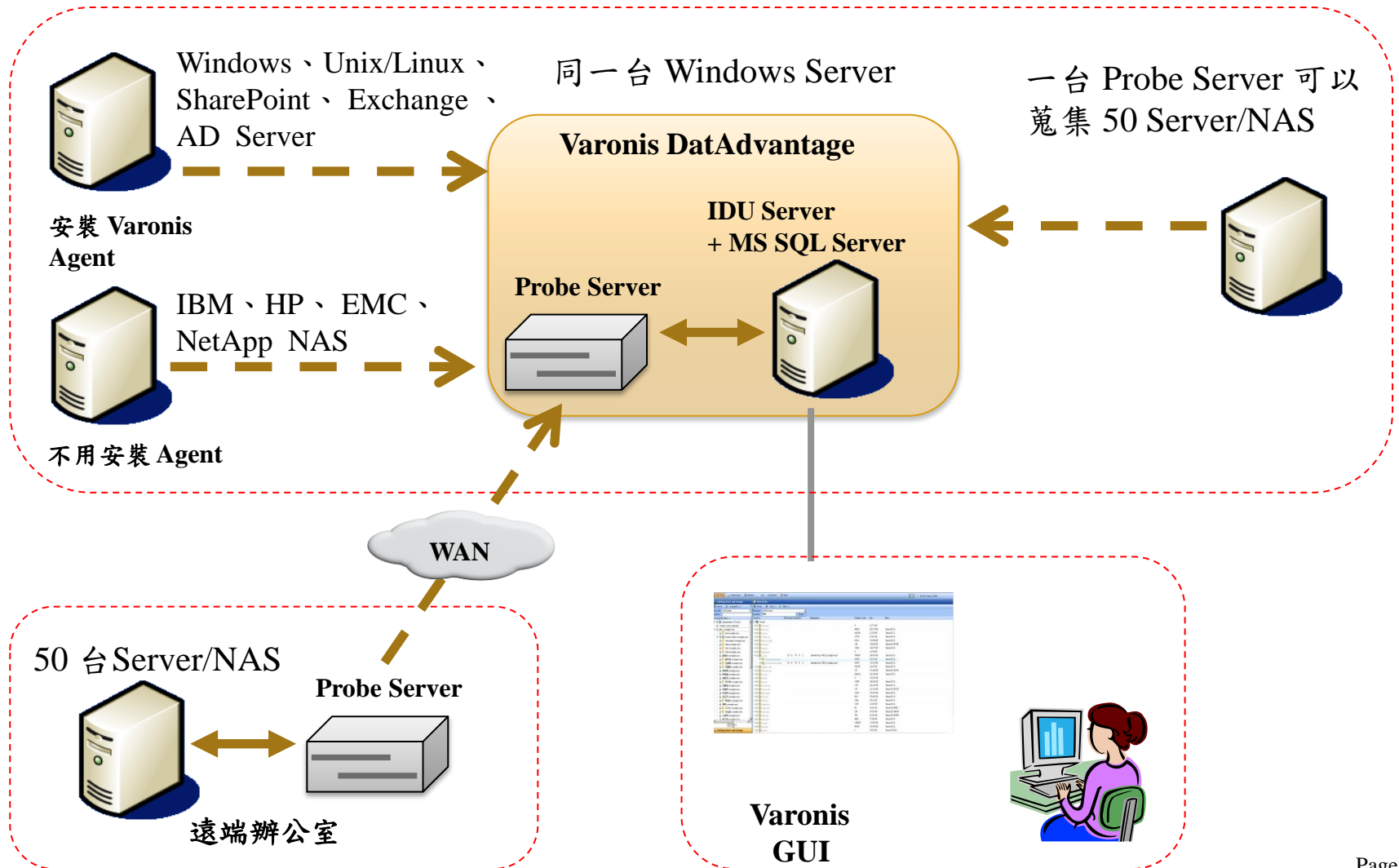
- DCF for SharePoint Online
- DCF for OneDrive

Varonis Metadata架構

- 四種類型的 Metadata 被收集、合成、加工並展示：
 - 檔案系統及權限資料
 - 用戶及群組資料
 - 存取紀錄
 - 敏感資料識別
- 可操作的資料管控信息：
 - 誰有權訪問某個資料集？
 - 誰才應該有權訪問某個資料集？
 - 誰曾經訪問過某些資料？
 - 那些資料是敏感的？是否權限設定？那些人在使用？
 - 誰才是資料的擁有人？
 - 誰在搜尋那些檔案與敏感資料？
 - 那裡我的敏感資料被過度曝露，我怎樣修正這個問題？
- 容許資料擁有人參與資料管控：
 - 自動化的權限審查
 - 授權流程



Varonis DatAdvantage 產品架構



Varonis 協助全球企業

在企業的 File Server、NAS, Exchange、SharePoint 平台上:

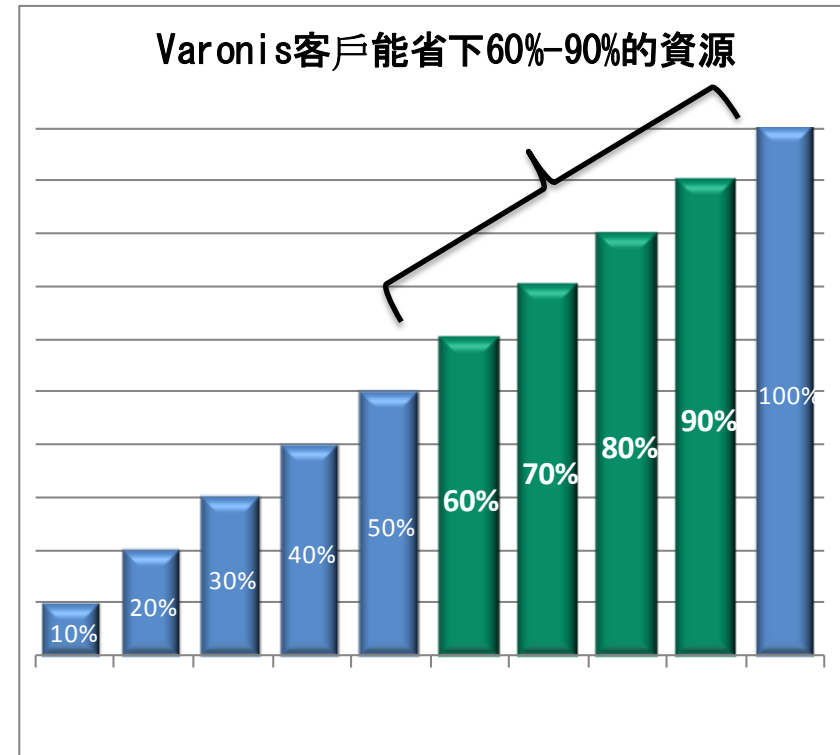
1. **提供權限管理分析**，把不適當或過多的權限清除，達到最理想的權限設定。就是應該及有需要存取資料的人才有限，沒需要或不應該取得資料的人都不會有權限去看資料
2. **提供詳盡及容易使用的稽核追蹤**，在每一個這些平台上、每一個檔案/電郵、每一個人做的每一個動作都有紀錄，而且可以用最小的資源去儲存很長時間的稽核紀錄，同時能提供精密準確的搜尋
3. **掃描出這些平台上存放著的敏感資料**，並對每一個存放敏感資料的目錄提供風險評估，還能提供修正風險的方向及順序
4. **偵測發現惡意行為**，迅速因應將危險降至最小

DatAdvantage 減低營運開支

以下的IT工作...

- eDiscovery
- AD 清理
- 資料存取管理
- 資料遷移
- 域(Domain)整合
- 識別資料擁有人
- 識別沒有擁有人的資料
- 識別非業務有關資料
- 資料存取審計
- 服務台及罪犯行為調查
- 權限審核及檢討

DatAdvantage 提供價值



與其他方案比較：有效管理 還是 應付了事

Varonis 是唯一的完整解決方案，不是僅搜集一些無法有效分析的日誌

- 支援多平台與 NAS 儲存設備：
 - Windows、Unix、EMC NAS、NetApp Filers、IBM NAS、HP NAS 與 HDS NAS
 - 使用自己寫的檔案系統過濾器(File System Filters)來截取系統活動
 - 對於 1000個用戶~每月 0.5~1GB 儲存空間與佔用 1% CPU。
- 不使用作業系統本身的查核機制
 - 使用作業系統原身的查核機制將付出效能衝擊與大量消耗儲存空間之代價
 - 如果使用作業系統本身的查核機制~約每天 10 GB與 15~20% CPU使用率。
- 完整的查核活動、資料分類解決方案
- 過度權限與異常行為警告
- 有效率的資料搜尋分類，新增與修改資料時不需全部掃描
- 找出可被全部使用者存取之敏感或關鍵資料(高風險資料)
- 找出資料的擁有者 Data Owner

顯示存取權限 - 雙向顯示

The screenshot shows a software interface with two main panes. The left pane, titled 'Existing Users and Groups', lists various users and groups. A red box highlights the 'Group:Finance' entry. The right pane, titled 'Directories', shows a table of directory permissions. A red box highlights the 'finance' directory row, which has permissions 'M R W X L' and is noted as '(Inherited from "Group:Finance")'. Another red box highlights a search field in the table. Text overlays explain the mapping between users/groups and data.

Directory	Permissions	Explanations	Size
databases	M R W X L	(Inherited from "Everyone")	1
DataShare1			9
dsr	F M R W X L	(Inherited from "Everyone")	5
Embd-Engineering			9
ERP-Arc			3
finance	M R W X L	(Inherited from "Group:Finance")	8
404			0
7MS94			0
7Y094			0
atm			0
bill			0
Cars			0
Controllers			0
n			0
data			0
CSMO			0
EU094			0
Economics			0
erin			0
EU00			0
EU02			0
EU03			0
EU200			0

從 使用者/群組...

對映到 使用者/群組

對映到 資料

從資料...

誰可以存取那些目錄、電子郵件信箱？

The screenshot displays two side-by-side windows from a Windows Server console. The left window, titled 'Existing Users and Groups', shows a list of users and their file system permissions. The right window, titled 'Directories', shows a list of directories and their contents.

Existing Users and Groups

Org. units	File System Permissions
Account Operators (CORP)	<u>Send As</u>
Administrators (CORP)	<u>Send As</u>
Allen Carey (CORP)	<u>Full Access</u> <u>Send On Behalf</u>
ANONYMOUS LOGON (Abstract)	None
Default (Abstract)	None
Domain Admins (CORP)	<u>Send As</u>
Enterprise Admins (CORP)	<u>Send As</u>
Exchange Recipient Administrators (CORP)	<u>Send As</u>
Exchange Organization Administrators (CORP)	
Administrator (CORP)	
SELF (Abstract)	<u>Full Access</u> <u>Send As</u>
SYSTEM (Abstract)	<u>Send As</u>

Directories

Directory	Explanations	Size	DC
DirectoryServices			
centos5			
Exch-prod			
Mailbox Store		1.10 GB	
AaronCalhoun - BarbaraTolle		0 Bytes	
AaronCalhoun@corp.local		17.29 KB	
AaronDanburg@corp.local		0 Bytes	
AaronHammer@corp.local		14.75 KB	
AaronJoy@corp.local		0 Bytes	
AaronNederveld@corp.local		456.42 KB	
AaronRay@corp.local		0 Bytes	
AaronWebber@corp.local		46.00 KB	
AdamCall@corp.local		156.94 KB	
AdamDanenhauer@corp.local		0 Bytes	
AdamHancock@corp.local		0 Bytes	
AdamJuette@corp.local		0 Bytes	
AdamNelson@corp.local		503.55 KB	
AdamRead@corp.local		19.10 KB	
AdamWeidenfeller@corp.local		20.60 KB	
Administrator@corp.local		9.78 KB	
AdrianCallahan@corp.local		54.04 KB	
AdrianDarley@corp.local		21.97 KB	
AdrianHane@corp.local		158.59 KB	

An arrow points from the 'Full Access' permission for Allen Carey in the left window to the 'AaronNederveld@corp.local' entry in the right window.

點擊 Aaron 的信箱可以快速查出 Allen Carey 可以 Full Access Aaron 的信箱

權限修正建議與權限移除模擬

Resources: corpfs02, centos5, http://sharepoint

Look For: Search

Directory	Permissions	Explanations	Violation Count	Size
corpfs02			356	1.64 TB
C:				1.64 TB
Share				317.85 MB
apps				1.15 GB
888-Project			1	127.14 MB
BI			0	31.79 MB
databases			0	190.71 MB
DataShare1			6	52.86 GB
dsr			0	540.35 MB
Embd-Engineering			0	19.12 GB
ERP-Arc			5	2.05 GB
finance			1	2.36 GB
404			25	76.45 GB
7MS94			0	0 Bytes
7YO94			0	0 Bytes
atm			0	0 Bytes
bill			0	0 Bytes
Cars			0	0 Bytes
Controllers			0	0 Bytes
D			8	24.12 GB
data			0	0 Bytes
DEMO			0	0 Bytes
DEMO94			0	0 Bytes
Economics			0	0 Bytes
			3	19.00 GB

依照 User

Org. units: All Domains	Permissions
sec_IT-System (CORP)	M R W X L
Group_Finance (CORP)	R W X L
Christy Venier (CORP)	
Jennifer Harris...	
Marc Farhat (CORP)	
Eugene Schaefer ...	
Eric Adler (CORP)	
Jeffrey Shaw (CORP)	
Benjamin Kasbekar...	
Andrew Weirich (...)	
Elena Cabrera (CORP)	
Michael Federle (...)	
Maria Hirasaki (CORP)	
Heather Capp (CORP)	
Margaret Coakley (CORP)	
Jane Nolan (CORP)	
Beatrice Latchford (CORP)	
Caros Kelly (CORP)	
Allen Carey (CORP)	
Erin Manning (CORP)	
Chris Overcash (CORP)	
Crystal Grove (CORP)	

相對影響目錄?

建議移除之過度權限?

稽核追蹤 ~ 詳細與完整之 稽核、追蹤記錄

Resources: All Resources
Look for: Search
Directory: FileServer

Switch to advanced mode Save/Load
Show data from: File system events From: 12/ 1/2008 12:00 AM To: 1/14/2009 11:59 PM Search

Log
Query: Date between 12/1/2008 12:00:00 AM and 1/14/2009 11:59:59 PM AND Show data from Equals 'File-system events' AND Directory Starts with 'c:\finance'

Operation Type

Time	File Server / Do...	Operation On	Operation Ty...	Change Description	Operation By	File Type	Event Cou
Operation Type: Object name changed (72)							
Operation Type: Object removed (17)							
12/24/2008 2:38...	FileServer	c:\finance\Econo...	Object removed		Root-Domain\Ann Schoenberger	xls	5
12/1/2008 10:20...	FileServer	c:\finance\Control...	Object removed		Root-Domain\Erin Manning	doc	6
12/1/2008 10:20...	FileServer	c:\finance\Control...	Object removed		Root-Domain\Erin Manning	doc	5
12/1/2008 10:20...	File	存取	Control.	存取	R	檔名與存	來源 IP
12/1/2008 10:20...	File	存取	Control.	存取	R	取次數	地址
12/1/2008 10:20...	File	存取	Control.	存取	R		
12/2/2008 9:53:0...	FileServer	c:\finance\Control...	Object removed		R		8
12/1/2008 10:20...	FileServer	c:\finance\Control...	Object removed		Root-Domain\Erin Manning	doc	50
12/2/2008 11:09...	FileServer	c:\finance\Control...	Object removed		Root-Domain\Margaret Coakley	DOC	3
12/2/2008 11:08...	FileServer	c:\finance\Control...	Object removed		Root-Domain\Anne Thornton	DOC	1
12/2/2008 11:52...	FileServer	c:\finance\Control...	Object removed		Root-Domain\Anne Thornton	DOC	1
12/1/2008 11:49...	FileServer	c:\finance\Control...	Object removed		Root-Domain\Anne Thornton	doc	1
12/2/2008 10:53...	FileServer	c:\finance\Control...	Object removed		Root-Domain\Anne Thornton	doc	1
12/1/2008 12:10...	FileServer	c:\finance\Control...	Object removed		Root-Domain\Anne Thornton	DOC	2
12/2/2008 10:46...	FileServer	c:\finance\Control...	Object removed		Root-Domain\Ann Schoenberger	xls	3
12/2/2008 4:50:0...	FileServer	c:\finance\Control...	Object removed		Root-Domain\Erin Manning	doc	1
12/3/2008 4:15:0...	FileServer	c:\finance\Control...	Object removed		Root-Domain\Eric Adler	xls	1
12/1/2008 10:47...	FileServer	c:\finance\Financi...	File open		Root-Domain\Carlos Kelly	xls	172.17.32.110
12/1/2008 10:47...	FileServer	c:\Market\Custom...	File open		Root-Domain\Kevin Pryor	xls	172.17.21.15
12/1/2008 10:10...	FileServer	c:\Mega\Corporate...	File open		Root-Domain\Alice Tanner	doc	172.17.41.13

搜尋, 分類 與 分群組

Exchange 事件記錄

- 誰刪除 訊息或 文件夾？
- 誰更改了 存取權限？
- 誰使用別人的名義發送郵件？
- 誰改變了一封電子郵件的內容並代為轉發？
- 誰開啟郵件信箱並閱讀電子郵件，然後標示為”未讀取”未讀
- 不同用戶(Outlook、OWA、iPhone等)對 Exchange 的訊息存取
- 授權/非授權 Exchange Mailbox 的開啟記錄

與 Exchange 內建稽核功能比較

Varonis Agent 提供功能

- Message opened 訊息開啟
- Send message 傳送訊息
- Send message as 代替發送訊息
- Send Message On Behalf 代理人發送訊息
- Edit message 編輯訊息
- Delete message 刪除訊息
- Move/Copy message 搬移/拷貝 訊息
- Mark as Read/Unread 標示為已讀/未讀
- Set Flags 設定旗標
- Open Folder 開啟資料夾
- Create /Delete 建立/刪除資料夾
- Add/Remove/Change Permission 增加/移除/更改 權限
- Move/Copy Folder 搬移/拷貝資料夾
- Attachment Opened 開啟附件
- Attachment Delete/Added 刪除新增附件
- Mailbox Delegate Added/Removed 信箱代理人 新增/移除
- Logon 登錄
- ADD/Remove/ Mailbox Permission 新增/移除 信箱權限

Exchange 內建稽核

- Message opened
- Send message Send message as
- Send Message On Behalf

“沒有共用資料夾 事件記錄”

完整的 Exchange 稽核

提供完整的 Exchange 稽核，包括每一個使用者對每一個郵箱的所有動作，包括電郵、行事曆、聯絡人等所有 Exchange 物件的存取。

The screenshot displays the DatAdvantage interface for monitoring Exchange activities. The main window is titled "DatAdvantage - : XCHENG-DV1 - [Resource: XC]". It features a menu bar (File, Tabs, Tools, Help) and a toolbar with icons for Work Area, Review Area, Statistics, Log, and Reports. On the left, a "Directories" pane shows a tree view with "XC" expanded to show "Mailbox Store" and "Public Folders". The central "Log" pane lists various operations such as "Exchange Folder Opened", "Logon", "Message Created", "Message Deleted", "Message Edited", "Message Marked as Read", "Message Marked as Unread", "Message Moved", "Message opened", "Message Received", and "Message Sent". The right-hand "Details" pane provides a comprehensive view of a selected event, including:

- Time:** 4/27/2011 3:14:00 PM
- File Server / Domain:** XC
- Object Type:** Message
- Path:** Mailbox Store\Ex1@xcheng.com\Inbox
- Object:** sdcs
- Operation Category:** Changed
- Operation Type:** Message Marked as Unread (Annotated with a red box: "作業類型~ 例如 訊息標示為未讀取")
- Change Description:** Message marked as Unread (Annotated with a red box: "異動說明~ 例如 訊息標示為未讀取")
- Operation By:** XCHENG.COM\Ex1 (Annotated with a red box: "使用者")
- File Type:**
- Event Count:** 1
- Last Occurrence:** 4/27/2011 3:14:00 PM (Annotated with a red box: "最後使用時間")
- IP Address/Host:** 10.10.50.142
- Mail Source:** Ex2

Navigation controls for the details pane include "Up" and "Down" arrows.

敏感資料的識別

- 關鍵字

(RD的產品名稱/代號、秘密的項目名稱，“機密文件”，“Confidential”)

- Regex 正規表達式

(個資法要求企業要重點保護的個人資料:

身份証號碼、電話號碼、銀行賬號、Visa/Mastercard 卡號)

偵測內鬼的機敏資料竊取行為


高科技業抓內鬼...奇招盡出：律師觀點，強化內控設
警示器，在原始碼中編入公司特有的記號，方便日後
認證、確認。

2015-06-01 02:33:19 經濟日報 本報綜合報導

<http://money.udn.com/money/story/6709/937547->

[%E9%AB%98%E7%A7%91%E6%8A%80%E6%A5%AD%E6%8A%93%E5%85%A7%E9%AC%BC%E2%80%A6%E5%A5%87%E6%8B%9B%E7%9B%A1%E5%87%BA](http://money.udn.com/money/story/6709/937547-%E9%AB%98%E7%A7%91%E6%8A%80%E6%A5%AD%E6%8A%93%E5%85%A7%E9%AC%BC%E2%80%A6%E5%A5%87%E6%8B%9B%E7%9B%A1%E5%87%BA)

緊急並可應用之數據

 **Classification and Priorities**

Report generated on 12/08/2009 10:17:45 AM

File Server	Access Path	Notes	File Name	Rule Name	Priority	Hit Count	Risk Priority	Detection Date
corpfs02	C:\Share\legal\Old Files (Kelly Jones)\key	Social Security Numbers (30) ,american express cards (48)			150	78	37.36	12/07/2009 08:29:49 AM
corpfs02	C:\Share\HR-Private\PRS	Social Security Numbers (30) ,american			149	78	37.36	12/07/2009 08:29:49
corpfs02								2009 49
corpfs02								2009 49

敏感資料 優先等級 敏感數量 風險指數

列出應該優先解決的目錄

- 包含大量敏感資料的目錄

-與-

- 過大/過鬆散 權限設定

機敏資料稽核追蹤~ 那些人曾經存取機敏資料?

機敏資料存取活動

Search filters: Any of (OR):
- Rule name Equals Visa
- Rule name Equals MasterCard
- Rule name Equals American Express

Time	File Se...	O...	Object	Path	O	Operation Type	Operation By	File
12/3/2010 10:38...	corpfs...		unplanned_transactio...	C:\Share\finance\Economics\Costing\2 - Inventory Report\2006\Q...		File modified	CORP\Eric Adler	txt
12/3/2010 10:19...	corpfs...		unplanned_transactio...	C:\Share\finance\Economics\Costing\2 - Inventory Report\2006\Q...		Object added	CORP\Ann Schoenber...	txt
12/3/2010 10:19...	corpfs...		unplanned_transactio...	C:\Share\finance\Economics\Costing\2 - Inventory Report\2006\Q...		File modified	CORP\Ann Schoenber...	txt
12/3/2010 10:06...	corpfs...		New price for JV-SUP...	C:\Share\finance\Financial Reports\Prices and Item Numbers		Object added	CORP\Crystal Grove	txt
12/3/2010 10:06...	corpfs...		New price for JV-SUP...	C:\Share\finance\Financial Reports\Prices and Item Numbers		File modified	CORP\Crystal Grove	txt
12/3/2010 10:41...	corpfs...		INVETNORY SUMM...	C:\Share\finance\Economics\Costing\2 - Inventory Report\2006\Q...		Object added	CORP\Eric Adler	txt
12/3/2010 10:41...	corpfs...		INVETNORY SUMM...	C:\Share\finance\Economics\Costing\2 - Inventory Report\2006\Q...		File modified	CORP\Eric Adler	txt
12/3/2010 10:54...	corpfs...		hi-speed checkweigh...	C:\Share\legal\Corporate\License Agreements		Object added	CORP\Melissa Donovan	txt

資料夾與敏感資料關係

The screenshot shows a directory tool interface with a table of folders and their violation counts. The table has columns for Directory, Permissions, Explanations, Violation Count, Size, and Notes. A red box highlights the 'Violation Count' column, and another red box highlights the 'Notes' column. A red arrow points from a text box to the 'Violation Count' column, and another red arrow points from a text box to the 'Notes' column.

Directory	Permissions	Explanations	Violation Count	Size	Notes
Share			169	75.21 MB	Social Security Numbers (65) ,american express cards (104)
apps			203	75.23 MB	Social Security Numbers (75) ,american express cards (128)
B4			34	72.00 KB	Social Security Numbers (10) ,american express cards (24)
B4Released-Applications			0	16.00 KB	
BBB-Project			0	4.00 KB	
BI			0	24.00 KB	
databases			0	3.51 MB	
DataShare1			0	68.00 KB	
dsr			0	1.09 MB	
Embd-Engineering			0	264.00 KB	
ERP-Arc			0	240.00 KB	
finance			0	5.79 MB	
Fondue			0	104.00 KB	
groups			0	156.00 KB	
HR			0	1.62 MB	
HR-Private			78	176.00 KB	Social Security Numbers (30) ,american express cards (48)
HumanResources			0	312.00 KB	
legal			91	46.60 MB	Social Security Numbers (35) ,american express cards (56)
Market			0	788.00 KB	

符合規則(敏感資料)數量

符合的規則 (敏感資料)

包括敏感資料且沒有權限控管的目錄

Directory	Permissions	Explanations	Violation...	Notes
corpfs02				
C:			203	Social Security Numbers (75) ,american ...
Share	F M R W X L	Inherited from "Everyone(Abstract)"	203	Social Security Numbers (75) ,american ...
B4			34	Social Security Numbers (10) ,american ...
BBB-Project			0	
BI			0	
databases	M R W X L	Inherited from "Everyone(Abstract)"	0	
DataShare1			0	
dsr	F M R W X L	Inherited from "Everyone(Abstract)"	0	
Embd-Engine...			0	
ERP-Arc			0	
finance			0	
Fondue			0	
groups	R W X L	Inherited from "Everyone(Abstract)"	0	
HR			0	
HR-Private			78	Social Security Numbers (30) ,american ...
HumanResources			0	
legal			91	Social Security Numbers (35) ,american ...
Market			0	

包括敏感資料的數量

權限大掃除 ~ 針對 Everyone 權限設定

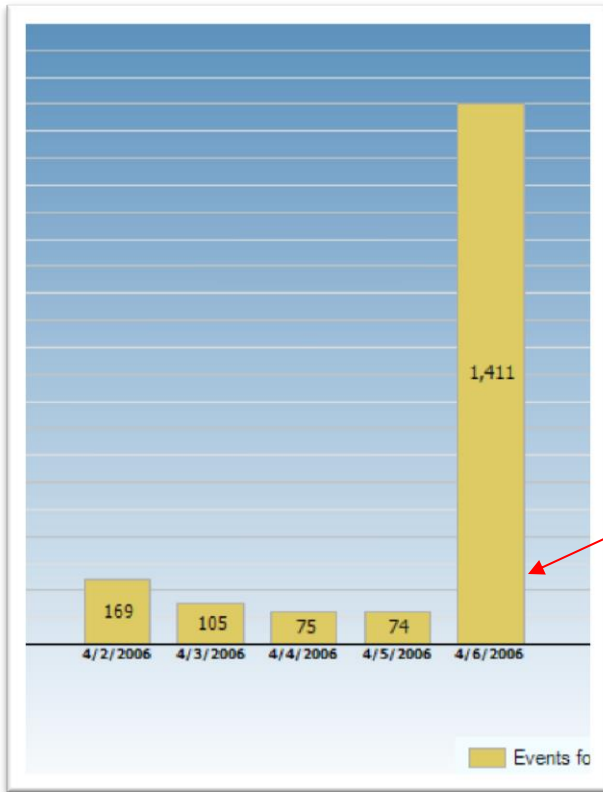
The screenshot displays a file server management application with several overlapping windows:

- Commit Dialog:** A dialog box with a table of operations. The table has columns for 'Include', 'Sequ...', 'Status', 'Description', 'BeginTime', and 'Error Description'. Two rows are visible, both with a status of 'Pending Oper...'. The second row's description is 'remove group Everyone(Abstract) FMRLXW for...'. Below the table is a 'Scheduling' section with 'Immediate' selected and a date/time picker set to 'Friday January 29 1:07 PM'. Buttons for 'Abort', 'RollBack', 'Commit', and 'Close' are at the bottom.
- Recommended Users and Groups:** A window showing a list of users and groups. The 'Everyone (Abstract)' entry is highlighted with a red box, and its permissions are listed as 'F M R W X L'.
- Login Dialog:** A dialog box for logging in, showing a text field with 'DRP\administrator' and a 'Login' button.

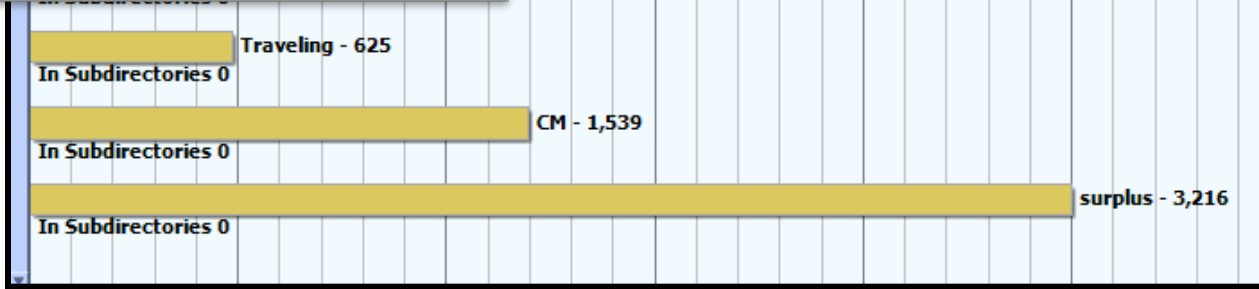
Text overlays on the screenshot include:

- '權限修正後影響' (Impact after permission correction) in the bottom left.
- '權限變更模擬' (Permission change simulation) in the bottom right.

存取活動分析



- [Root-Domain] (729)
- [Root-Domain] (786)
- [Root-Domain] (801)
- 異常行為



指派資料擁有者 ~ 快速設定 Data Owner

The screenshot shows the DatAdvantage interface for the 'finance' directory. A 3D pie chart displays the distribution of events per user. The largest slice is 32.78% for Ann Schoenberger. Other users include Andrew Carlisle (7.68%), Erin Manning (9.36%), Chris Overcash (10.42%), Margaret Coakley (6.09%), 4.72-5.7% of events (2 users), 1.47-2.57% of events (6 users), and 0-1.34% of events (7 users).

An 'Ownership Assignment' dialog box is open, asking: "Are you sure you want to set Person Ann Schoenberger as owner for Directory finance?" with 'Yes' and 'No' buttons.

A context menu is open over the chart with the following options: 'Jump To...', 'Manage Ownership...', and 'Set Ownership...'.

Overlaid text in Chinese: "點右鍵 設定所有權" (Right-click to set ownership).

Legend for the pie chart:

- Ann Schoenberger (Root-Domain) - 32.78%
- Andrew Carlisle (Root-Domain) - 7.68%
- Erin Manning (Root-Domain) - 9.36%
- Chris Overcash (Root-Domain) - 10.42%
- 4.72-5.7% of events, 2 users
- Margaret Coakley (Root-Domain) - 6.09%
- 1.47-2.57% of events, 6 users
- 0-1.34% of events, 7 users

各種存取活動、權限設定報告

Access Statistics
Report generated on 4/9/2009 9:09:47 AM

Access Path	User Name	Date	SAM Account Name	File Server	Event Count	Event Count on Subdirs
c:\HR					8	810
	Root-Domain\Ann Perrino				0	41
	Root-Domain\Don Penisson				8	721
	Root-Domain\Erica Caffrey				0	48
c:\HR-Private					0	174
	Root-Domain\Alex Weinger				0	156
	Root-Domain\Frances Weidenfeller				0	4
	Root-Domain\Melissa Cooley				0	14
c:\HumanResources					0	185
	Root-Domain\Alex Weinger				0	59
	Root-Domain\Denise Walters				0	6
	Root-Domain\Frances Weidenfeller				0	120

存取活動

Permissions for Directory 目錄的 使用者/群組

目前權限 | 建議權限 | 權限來源

使用者群組

發信給管理者 檢查目錄權限

異常活動警告

The screenshot shows the DatAdvantage Alerts interface. At the top, there is a menu bar with 'File', 'Tabs', 'Tools', and 'Help'. Below that is a toolbar with icons for 'Work Area', 'Review Area', 'Statistics', 'Log', 'Reports', and 'Alerts'. The 'Alerts' tab is active, showing 'Alerts: Ann Bowman'. A red arrow points to the 'Alerts' tab with a callout box containing the Chinese characters '警告' (Warning).

The main area displays the 'Alert List' for resources: CORPFS02, centos5, and http://sharepoint, E... The list is filtered from Tuesday, December 20, 2011, to Friday, December 23, 2011. The table below shows the alert details:

Entity Name	Type	Entity Name	Alert Type	Alert Name	Start Date
Exch-prod		Ann Bowman	Utilization	Daily Deviation	12/22/2011
CORPFS02		Kara Swales	Utilization	Daily Deviation	12/22/2011
http://sharepoint		Melissa Donovan	Utilization	Daily Deviation	12/22/2011

Below the table, there is a section for 'Ann Bowman' with a profile picture and a text box containing the following message:

User Ann Bowman was using resources increasingly 603 days ago, about 1678 times the Standard-Deviation above his/her average usage.

To the right, there is an 'Activity by Date' section with a bar chart showing the number of events for the selected object (Ann Bowman) over the last three days. The chart shows 5 events on 12/20/11, 2 events on 12/21/11, and 3,565 events on 12/22/11. A red arrow points to the 3,565 bar with a callout box containing the Chinese text '大量檔案開啟之異常行為' (Abnormal behavior of opening a large number of files).

Below the chart, it says: 'Represents the number of events occurring on the entity each day'.

DatAlert 即時警告 Real Time Alert

- 過濾 行為、內容、Active Directory、時間、次數所建立之彈性規則
- 透過 Event log、Syslog、SNMP、執行指令 等方式通知

The screenshot displays the DatAdvantage application window. The main area shows a log of events with columns for Time, Event Description, Operation By, IP / Hostname, Event Count, Object, and Path. Two events are visible, both related to 'user_2 added to group Domain Admins'. A context menu is open over the second event, with the option 'Create Real-Time Alert...' highlighted. A red arrow points to this option.

在現有日誌事件記錄上快速設定即時警告

O	Time	Event Description	Operation By	IP / Hostname	O	Event Count	E	Object	Path
	4/22/2013 9:38:0...	user_2 added to group Domain Admins	alerts.com\Administrato...	10.10.55.110		1		Domain Admins	alerts.com/Users/Domain Admins
	4/22/2013 9:56:0...	user_2 added to group Domain Admins		55.110		1		Domain Admins	alerts.com/Users/Domain Admins

DatAlert 即時警報通知 #1

搭配 Varonis 檔案稽核模組(CIFS、NFS、SharePoint、Exchange、Active Directory)功能提供即時警報通知

CIFS and NFS Events		
<ul style="list-style-type: none"> • File Create • File Delete • File Open • File Rename • File Modify • File Set Permissions • Directory Create • Directory Delete 	<ul style="list-style-type: none"> • Directory Rename • Directory Set Permissions • Access Denied - File Open • Access Denied - File Delete • Access Denied - File Set Permissions • Access Denied - Directory Delete • Access Denied - Directory Set Permissions 	<p>支援 CIFS and NFS 平台包含 Windows, NetApp, EMC VNX/Celerra, HP IBRIX, Hitachi NAS, UNIX, Linux, Solaris, AIX.</p>

SharePoint Events		
<ul style="list-style-type: none"> • File Create • File Delete • File Open • File Rename • File Modify • File Set Security 	<ul style="list-style-type: none"> • Directory Create • Directory Delete • Directory Rename • Directory Set Security • Role Set • Site Create 	<ul style="list-style-type: none"> • List Item Create • List Item Delete • List Item Open • List Item Rename • List Item Modify

備註：NetApp 不提供 Access Denied 記錄

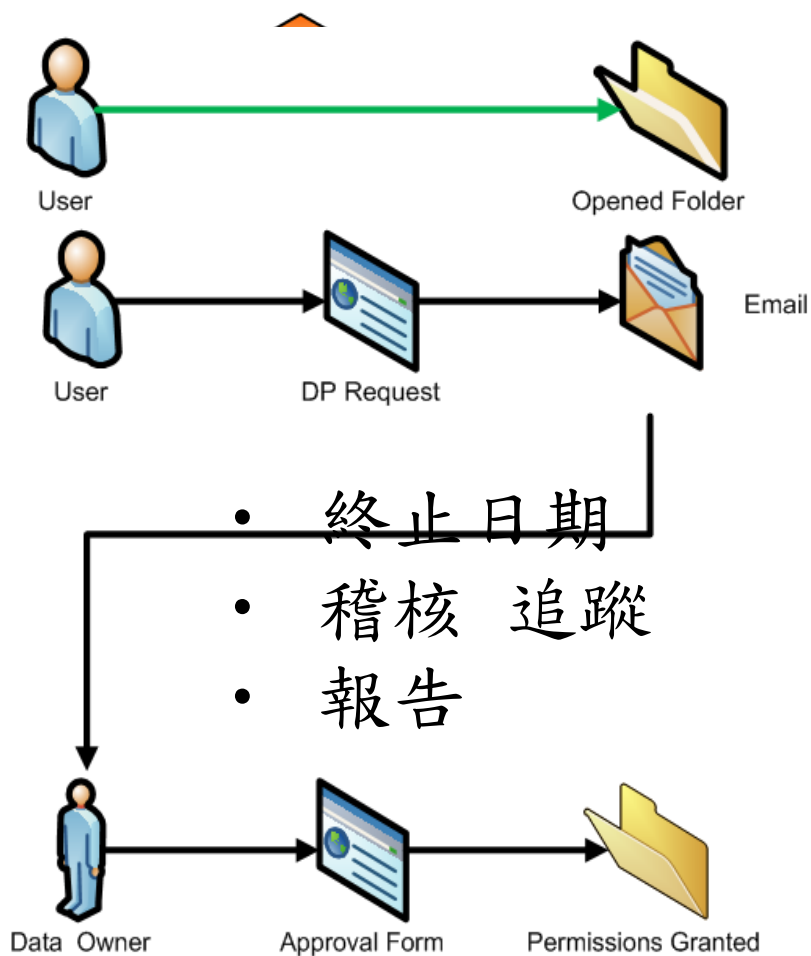
DatAlert 即時警報通知 #2

搭配 Varonis 檔案稽核(CIFS、NFS、SharePoint、Exchange、Active Directory 模組)功能提供即時警報通知

Exchange Events		
<ul style="list-style-type: none">• Open Folder• Create Folder• Delete Folder• Rename Folder• Add Folder Permissions• Remove Folder Permissions• Change Folder Permissions• Move Folder	<ul style="list-style-type: none">• Empty Folder• Copy Folder• Mark All as Read• Send Message• Send Message (On behalf of X)• Send Message (As X)• Message received• Edit Message	<ul style="list-style-type: none">• Delete Message• Copy Message• Move Message• Create Message• Message Marked as Unread• Message Marked as Read• Logon

Active Directory Events	
<ul style="list-style-type: none">• Creation and deletion of all objects• Changes in group membership• Changes in directory service object properties for any property	<ul style="list-style-type: none">• Reset password• Lock/unlock accounts• Create or delete account• Enable or disable account• Group membership changes

DataPrivilege – 授權許可的自動化流程



目錄存取權限申請
 存取目錄
 申請目錄存取權限審核
 原因

Name	Role	Status	Level	Permissions	Date
platinum3	Dir. Authorizer		1		

Request Reason	Authorization Explanation	Authorization
Project Permissive	Project modifications needed Characters left 971	<input checked="" type="radio"/> Approve <input type="radio"/> Decline

DataPrivilege：使用者目錄存取權限申請審核

Request ID: 39 權限申請

Request Operation Type: Grant Access Pending

Requested For

Entity Name: Adam Nelson
Logon Name: AdamNelson
Domain Name: CORP
Department: Engineering
Telephone Number:

權限存取目錄 存取截止日

Permissions For Directory Expiration Date ?

Path: \\CORPF502\SHARE\FINANCE

Requested: **Modify**

Membership to: Modify - sec_IT-System

Never
 On
 After 14 Days

Authorizers

Name	Role	Status	Level	Permissions	Date
Erin Manning	Dir. Owner				

授權主管

Total: 1 Record
No. Of Rows 3

Request Reason Authorization Explanation ? Authorization ?

I would like to review the accounts payable records. 申請理由

Access granted for consulting project 602. | 核准 或拒絕


Characters left 957

Approve
 Decline

OK Cancel

DataPrivilege : 資料擁有者~存取權限審查

Request ID: 3504 **Pending**
Request Type: Entitlement Review

 **Entity Name:** Group_Finance
Logon Name: Group_Finance
Domain Name: CORP

Review only objects that have changed since your last review ?

Status	User	Decision And Explanation
	Allen Carey (CORP)	<input type="radio"/> Keep <input checked="" type="radio"/> Remove <input type="text" value="Recommended for removal"/>
	Allison Schafer (CORP)	<input type="radio"/> Keep <input checked="" type="radio"/> Remove <input type="text" value="Recommended for removal"/>
	Andrew Carlisle (CORP)	<input type="radio"/> Keep <input checked="" type="radio"/> Remove <input type="text" value="Added outside DataPrivilege"/>
	Andrew Weirich (CORP)	<input type="radio"/> Keep <input checked="" type="radio"/> Remove <input type="text" value="Added outside DataPrivilege"/>

授權保留 或 移除

Total: 24 Records
No. Of Rows: 1 2 3 > Next 3 Last

Reason ?

Characters left 1000

Authorizers

Name	Role
Erin Manning	Group Owner

Total: 1 Record
No. Of Rows:

授權者

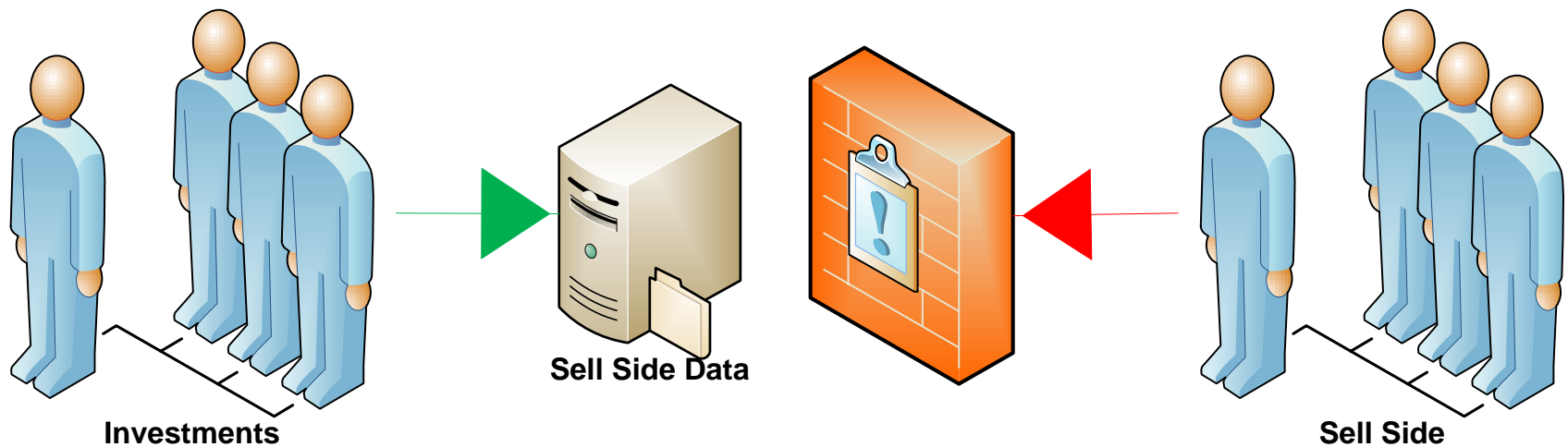
I confirm that I have reviewed the objects listed above, along with their content.
Please type the word 'Verify'.

確認已實施權限審查

Advanced >> Data last synchronized with environment: September 30, 2010 1:44:49 PM

DataPrivilege – 道德牆 Ethical Walls

- 防止利益衝突目錄資料被同一人存取
- 自動更正
- 符合合約或法規要求



Varonis 常用報表

檔案存取稽核 ~ Report 1a - User Access Log

存取概況監控 (針對某些重要目錄) ~ Report 2a – Access Statistics

群組名單 (包括權限清理建議) ~ Report 3a – Group Members

清查 Everyone / Domain Users 權限 ~ Report 4a – Effective Permissions for User or Group

權限報表 ~ Report 4b – User or Group Permissions for Directory

目錄列表 (包括資料容量) ~ Report 4f – File System Object List

找出繼承斷層 ~ Report 4f – File System Object List

異常使用行為警告 ~ Report 6a – Alert Detailed Report

監控資料增長量 ~ Report 9h – Changes in Folder Sizes

找出長期沒有人使用的目錄 ~ Report 7b – Inactive Directories by Size

找出沒有人使用的帳號 ~ Report 7a – Inactive Users

找出異常開立的共享目錄(如自行架構的 NAS) ~ Report 4n – CIFS Shares Discovery Report

敏感資料分佈 (資安盤點) ~ Report 4g – Classification and Priorities

敏感資料存取紀錄 ~ Log / Report 1a – User Access Log

非管理員群組的管理員 ~ 12C - Administrators in non-Admin Groups

提供 即將離職員工存取紀錄(敏感資料)

查詢已離職員工 (帳號已刪除) 歷史存取紀錄

查詢非上班時間檔案存取

非本人的 Exchange 郵件的開啟報告

那些檔案是加密檔案

Varonis 與 DLP 產品差異

某一家在香港上市的銀行，員工總數3500人以上，2010年業務發展到超過50家分行，總部的檔案伺服器資料容量在5年內由800GB增加至12TB，每家分行的檔案伺服器容量平均增加為100GB，總容量達到近20TB (5年增長約十倍)。

2010年初時內部稽核部門對檔案伺服器作出審核，並對管理層提出了重大的警告：“如果讓檔案伺服器這樣繼續的缺乏管理並不斷膨脹，必定會造成嚴重的資料洩漏事件。”於是資訊部接手、嘗試找出解決方案，最初的方向是希望透過DLP產品掃描並阻擋重要資料洩漏，經過半年左右的產品測試，他們得出的結論是，雖然DLP在阻擋方面的功能很強大，但是有幾個致命的弱點：

1. **DLP誤判的機會很大**，造成一般使用者很大的困擾，預期用戶反應極大。
2. DLP只能在檔案伺服器上掃描出敏感資料的所在，但是近20TB的資料量造成敏感資料列表太長，**沒有辦法判斷哪些需要優先處理**。
3. **DLP不能提供存取稽查及權限報表**，也無法回答“誰看過那些敏感資料”、“誰有權去看那些敏感資料”，或者是“那些敏感資料的權限開放得過度寬鬆”這些問題。

因為以上這幾個原因，資訊部放棄了佈署DLP產品的計畫，把目光轉到資料管控軟體(Data Governance)。

主動偵測 勒索軟體 Ransomware 異常的檔案加密行為

- 加密勒索軟體捲土重來，大舉攻擊小型企業與個人用戶，在2013年CryptoLocker出現之後，加密勒索軟體成為駭客有效的獲利模式，因此不只是大型企業，也有極高比例的中小企業遭受攻擊。超過三分之二的中小企業遭受CryptoWall攻擊。透過使用者點選釣魚郵件導致中毒，已經不是感染的唯一途徑。只是開啟瀏覽器上網，沒有下載任何檔案，也可能透過作業系統、瀏覽器、Java、Flash等的漏洞被加密勒索軟體入侵，將電腦的文件檔案全數加密勒索。資料來源出處：Ithome 文/周峻佑 | 2015-12-19發表 Ithome (<http://www.ithome.com.tw/tech/101364>)
- 會計人員誤點免費中獎iPhone 6S的釣魚郵件，導致伺服器上的資料被勒索軟體CryptoLocker加密,結果當事人與主管調離現職。圖文出處：趨勢科技全球技術支援與研發中心 <http://blog.trendmicro.com.tw/?tag=%E5%8B%92%E7%B4%A2%E8%BB%9F%E9%AB%94>
- 首款以JavaScript撰寫的跨平台勒索軟體Ransom32現身!
<http://www.ithome.com.tw/news/102452>

美國洛杉磯醫院電腦遭駭客挾持勒索360萬美元 資料來源出處：文/陳曉莉 | 2016-02-16 <http://www.ithome.com.tw/news/103903>

CNN近期發表駭客專輯，採訪全世界最頂尖駭客與分析為什麼要駭？讓您了解駭客的功力與可怕！駭客並當場示範在2分鐘內從飯店打到IT help desk 拿到存取權限。 <http://money.cnn.com/technology/superhero-hackers/?playvid=6&sr=fbmoney021616superhero-hackers0633AMVODtopVideo&linkId=21286724>

不要輕忽加密勒索軟體攻擊的危險

不要以為你不會那麼倒楣？

- 你一定會被勒索軟體攻擊，只是時間的早晚，尤其大型企業更會配合過 APT 攻擊。
- 太容易拿到變種加密勒索軟體 (加密勒索軟體懶人包 ~ 只要1000美元，甚至有小學生駭客)。
- 只要不小心點閱被駭客假冒的朋友、同事或廠商提供的網址，在2分鐘後駭客即可取得管電腦存取權限。
- 駭客被捉到的機率太低，因為駭客使用”比特幣”取得贖金，根本難以追查。

加密勒索軟體可怕之處是它不是要將客戶機敏資料偷出，而是將資料加密上鎖讓用戶無法使用，而且駭客可能先 **APT 入侵假冒你認識的朋友、同事或廠商**。所以一般的防毒軟體與 DLP 軟體無法有效防範。

不要以為只有個人電腦資料會被加密勒索，損害不會太大？

- 個人電腦往往會與公司伺服器網路連線，所以連伺服器資料也被加密。
- 如果是財務員工的電腦被入侵，那整個財務部資料可能就會被加密勒索，如果被入侵的員工帳號身份是伺服器管理者(Local或Domain Administrator)，那更不幸，因為可能公司所有伺服器資料都會被加密。

為何駭客喜歡使用勒索軟體 Ransomware ?

1. 容易達到勒索:

- 傳統駭客是要竊取出客戶重要資料，客戶可能建置 DLP、網路隔離等資安規劃來防止機敏資料被駭客竊取攜出。
- 勒索軟體卻只須將檔案加密讓使用者無法使用資料，不需要將客戶重要資料攜出與網路連線即可在客戶內部將檔案加密。

2. 更容易取得贖金:

- 傳統駭客竊取到客戶重要資料，必須找到買家。
- 勒索軟體駭客透過比特幣 Bitcoin 可以輕易、安全的拿到勒索金並可能視客戶規模與資料的重要性抬高贖金。

3. 難以防範:

- 客戶只要有作業系統或應用軟體資安漏洞、接收電子郵件、瀏覽網頁等網路行為就可能被勒索軟體勒索。
- 駭客可能先 APT 入侵你認識的朋友、同事或廠商的郵件系統假冒身份。
- 駭客組織互相傳授各種勒索軟體與方法讓勒索軟體輕易取得並不斷的變種。

Varonis 可以偵測出勒索軟體的大量檔案加密、更換權限與副檔名等異常行為並立即警告或自動執行阻斷指令!

如何緩解方法 勒索軟體 Ransomware 入侵損失？

大多數人沒有意識到他們已經被感染，直到勒索信出現，通知您的檔案已被加密勒索。當你發現你的電腦已經被感染 只能關閉電腦，並迅速採取下列解決方案。

緩解方法

1. **監控檔案系統活動 Monitor File System Activity**：停止大量的檔案刪除與加密動作。
2. **使用者行為分析 User Behavior Analytics**：監控不正常的使用者行為異常時發出警告
3. **最小權限模式 Least Privilege Model (權限盤點與特權管理)**：移除 Everyone 目錄與 Domain Users 使用者、收回一般用戶帳號的特權(Local administrator 或 Domain administrator 以防止災情擴大。

面臨勒索軟體必須採取措施。

1. **隨時更新 安全性更新 security updates**：
 - 但是總是來不及。
2. **不斷的提醒 使用者不要下載來路不明的電郵附件或瀏覽不安全網站**：
 - 但是駭客可能假冒你認識的朋友、同事或廠商。
3. **密集與連續的CDP備份重要資料並保存較長的備份歸檔**：
 - 但是客戶往往疏於資料備份，尤其大部份個人電腦都沒有備份。
 - 保存較長的備份歸檔，國外有案例用戶在入侵70天後才發現勒索軟體入侵
4. **不斷的教育訓練**：
 - 但是人總是會有警戒心鬆懈時。

Varonis 使用者行為分析 (UBA)

Varonis DatAdvantage 可選購 及時警告 DatAlert 與 DatAlert Analytics 模組提供下列使用者行為分析 User Behavior Analytics (UBA) 功能。

- 防止內部與外部威脅：
- 惡意軟體活動：偵測包括Cryptolocker 勒索軟體的檔案加密行為、重要檔案異動、權限變更等。
- 可疑行為：發現異動的檔案或系統行為並立即通知相關人員處理。
- 潛在資料洩露：找出重要與敏感的資料加以保護與備份。
- 受危及的資產：設定好存取權限與限制可使用的人員，減少災害損失。

常見的偵測方法

- 統計不尋常的用戶行為
- 發現改變管理群組
- 管理者存取一般用戶的資料
- 大量的嘗試登錄失敗
- 對敏感資料活動
- 來自外部網站的控制變動

** 產品名稱如有異動以原廠為準

Varonis UBA 威脅模型 Proactive Analytics and Predictive Threat Models

1. 異動管理員群組成員
2. 發現系統設定工具 (Recon Tools)
3. 異常的服務帳號(Service account) 行為
4. 存取久未使用之檔案
5. 存取異常郵件信箱
6. 可疑的郵件行為
7. 不正常的敏感資料存取
8. 加密勒索軟體

** 產品名稱如有異動以原廠為準

主動分析和預測威脅模型 Proactive Analytics and Predictive Threat Models

DatAlert Analytics 提供下列主動分析和預測威脅模型

Abnormal Admin / Service Account Behavior

異常的管理/服務帳號的行為

Access to atypical folder 存取異常目錄

Access to atypical files 存取異常檔案

Access to atypical mailboxes 存取不常用信箱

Access to credentials stored in files 存取憑據檔案

Suspicious Mailbox Activity 可疑電郵信箱活動

Multiple mailboxes accessed from a single host

Multiple messages marked as unread by user other than mailbox owner

Permission Changes 權限更改

Changes in a local/unmonitored/abstract domain

Permissions added or removed for a Global Group

Mass Deletions 大規模刪除操作

AD Containers, Foreign Security Principal, or GPO

Multiple Directory Service objects

** 產品名稱如有異動以原廠為準

進一步產品資訊請洽 商丞科技 Brian Lee 02-29148001 ext 2251, brian_lee@proware.com.tw

主動分析和預測威脅模型 Proactive Analytics and Predictive Threat Models

DatAlert Analytics 提供下列主動分析和預測威脅模型

Abnormal behavior for Non-Privileged Accounts

非特權帳戶的異常行為

Access to system files 存取系統檔

Access to script files 存取 script 檔

Access to startup files 存取啟動檔

Access to configuration and backup files 存取設定或備份檔

Access to atypical server 存取不常用的伺服器

Volume of Access to stale data 存取不常用的檔案數量

Volume of Access to sensitive data 存取敏感資料數量

Volume of Access to credential files 存取憑證檔案數量

Volume of Access Denied / Failed Access 拒絕存取/訪問失敗數量

Security Certificate Activity 安全憑證活動

Suspicious Files Detected 偵測到可疑檔案

Exploitation Tools 開發工具

Recon Tools 偵察工具

System Binaries in unusual locations 異常的存放位置

Suspicious Modifications 可疑的修改

Hosts File

Critical GPOs

Encryption of Multiple Files 加密多檔案

Membership to Administrative Groups 管理群組成員

Account Lockouts 帳戶鎖定

Mass accounts locked out 大量的帳號鎖定登出

Administrative or Service Account locked out 管理者或服務帳號被鎖定登出

** 產品名稱如有異動以原廠為準

Varonis 與 FireEye (TAP)TM 合作



駭客獲得使用者帳號
並存取敏感檔案



Varonis 識別可疑行為



警報發送到FireEye的威脅分析平台 (TAP)



分析人員針對事件
進行追蹤調查與補救

分析人員透過FireEye的TAP事件與Varonis警報訊息進行調查



警報發送到FireEye的威脅分析平台 (TAP)

資料來源 <https://www.fireeye.com/content/dam/fireeye-www/partners/pdfs/sb-fireeye-varonis.pdf>

Varonis DatAdvantage、DatAlert 與 DatAlert Analytics 使用者行為分析提供 FireEye (TAP)TM 下列重要訊息

- 大量的刪除與修改行為
- 感染如 CryptoLocker或Cryptowall 等惡意與勒索軟體
- 升級特權
- 不尋常的個人識別資訊 (PII)存取
- 多次的登錄失敗嘗試
- 以及更多的潛在徵兆

資料來源 <https://www.fireeye.com/content/dam/fireeye-www/partners/pdfs/sb-fireeye-varonis.pdf>

Varonis DatAlert Analytics Rules

Rules

Create rules to receive real-time alerts on specified events

Configuration
Alert Templates
Predefined Scopes
Exclusion Scopes

Search by any value in grid

Severity ▲

Rule ID	Rule Name ▲	Rule Description
▲ Severity: 0 - Emergency (3 items)		
21	Deletion: Multiple directory service objects	May indicate unauthorized attempt to damage or destroy operational forest structure, denying users access to systems
25	Encryption of multiple files	May indicate a ransomware attack underway
27	Lock-out: Multiple accounts locked-out	May indicate misconfiguration, brute force attempt to gain access or denial of service attack
▼ Severity: 1 - Alert (26 items)		
▼ Severity: 3 - Error (1 item)		
▼ Severity: 4 - Warning (2 items)		
▼ Severity: 6 - Informational (4 items)		

Edit Rule
Clone Rule
Delete Rule
Enable
Disable
Jump to Log
Recalculate

1. 大量的非授權刪除動作
2. 大量的檔案加密
3. 大量的的帳號被鎖定

** 產品名稱如有異動以原廠為準

透過 CDP 連續資料保護挽救被勒索加密檔案

使用者行為分析 UBA 雖然可以及早發現並阻止 APT 與 勒索軟體攻擊
卻無法挽救已經已經被加密勒索檔案。

客戶大多有備份伺服器，卻忽略 主管、財務、研發等重要個人電腦

商丞科技 CDP 連續資料保護方案可 **快速復原被勒索軟體檔案加密之個人電腦**。

- 密集、連續備份保護 伺服器或個人電腦。
- 縮短備份的時間間隔(最短備份時間隔為1分鐘)、並可保留長期的備份歸檔。
- 提供 整機裸機復原、檔案級復原、異機復原功能
- 最近一份備份可實體轉虛擬化(P2V) 開機開機 3~5分鐘立即復原 Instant Recovery

透過 CDP 連續資料保護來保護重要資料

本地辦公室



異地備援端



災害復原 - 雲端 或 異地端

商丞科技 All-in-one 備份/還原/
備援伺服器

商丞科技 All-in-one 備份/還原
/備援伺服器



Cloud Storage DR - 雲 或 異地歸檔
Protect • AWS S3 • Google Cloud Storage •
Google Nearline • Rackspace Cloud Files

CDP
連續資料保護(最點間隔60秒)

歸檔

最近一份備份
實體轉虛擬化

IR 立即復原



SAN 或 NAS

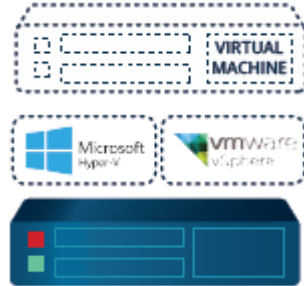


VMware 與 Hyper-V 虛擬環境

超過 100 種作業系統與資料庫環境



實體環境
(安裝 Agent)



VMware、Citrix 與 Hyper-V 虛擬環境
(Guest OS 不需安裝 Agent)

使用 商丞科技 CDP 連續資料保護復原被加密檔案

VMware 與 Hyper-V 虛擬環境
或 商丞科技 All-in-one 備份/還原/
備援伺服器



最近一份備份
實體轉虛擬化
3~5分鐘 IR 立即復原



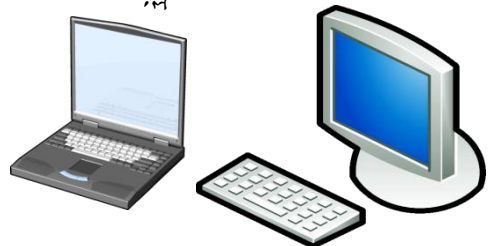
VMware 與 Hyper-V 虛擬環境

CDP
連續資料保護(最點間隔60秒)



整機復原或檔案級復原

歷史資料歸檔



Desktop, Notebook 安裝
CDP for Desktop Agent



SAN 或 NAS

商丞科技 CDP for Windows Desktop Agent 價格如下
(純軟體、不含硬體與備份硬碟與到府安裝)

- 一套軟體授權 1.2萬 (未稅)
- 一百套軟體授權 12萬 (未稅)

輕鬆保護 桌機個人電腦與筆電