IBM Security

IBM

分秒必爭！當威脅勒索軟體入侵時，該透過哪些關鍵技術做因應？

崔友經
資訊安全顧問

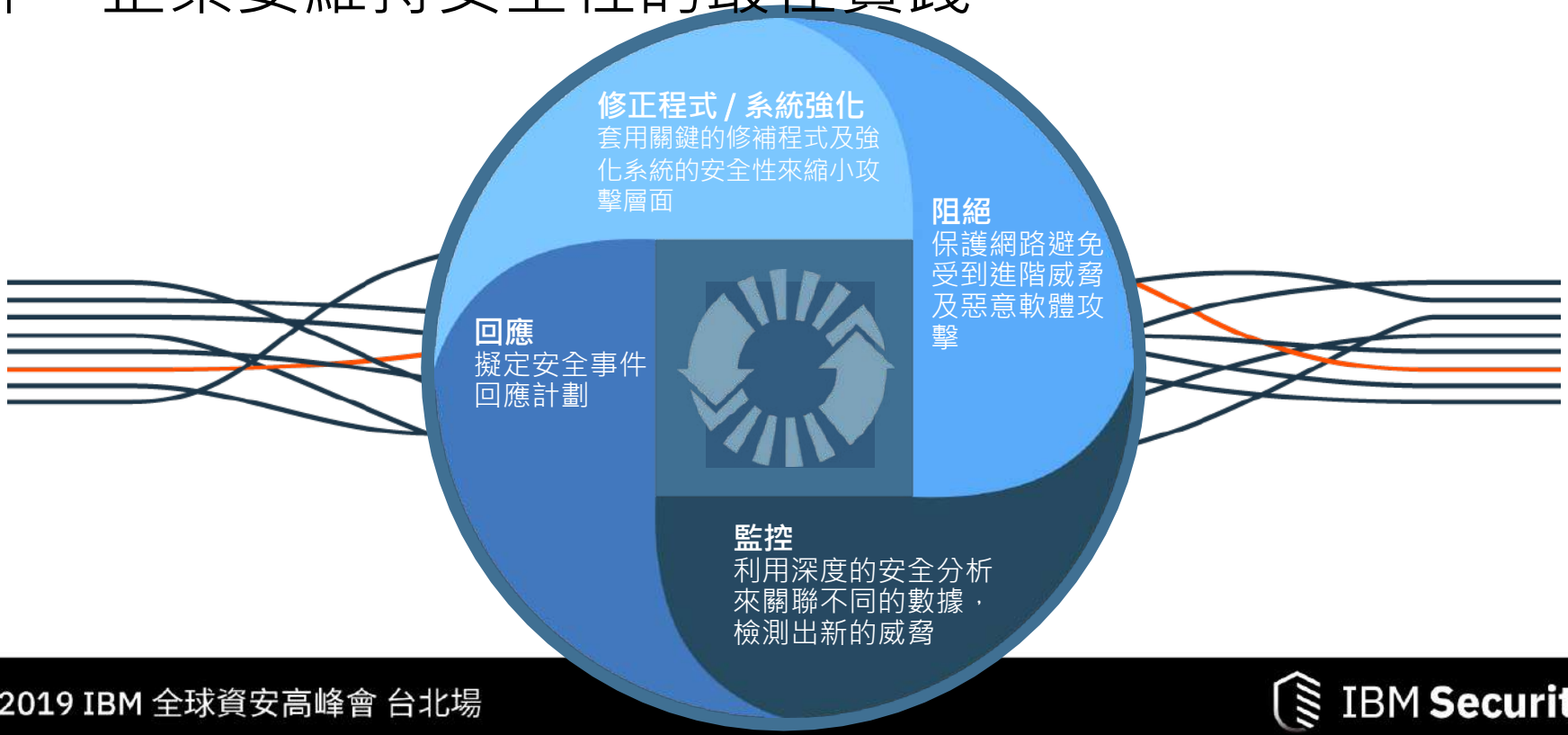
勒索軟體的數量不斷成長及傳播方式不斷改變，

勒索軟體的傳播方式：
- 釣魚郵件
- 系統漏洞
- 執行巨集
- 蠕蟲感染
- 下載檔案

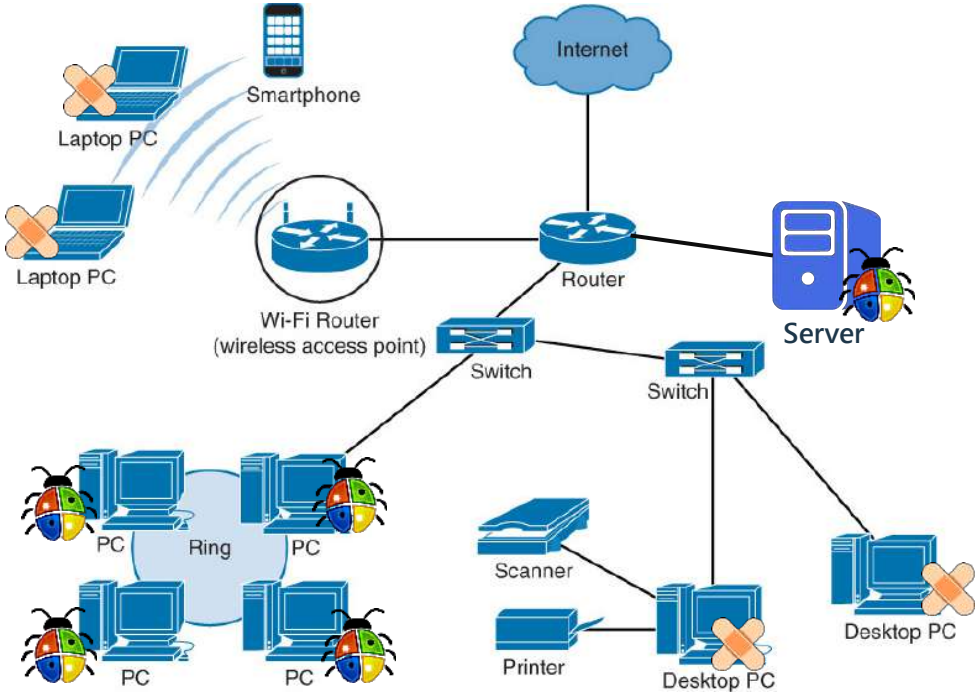
勒索軟體的綁架方式：
- 文件加密
- 開機鎖定
- 裝置鎖定
- 螢幕鎖定
- 瀏覽器鎖定

資料來源：IBM X-Force, 2016

面對層出不窮的勒索軟體及其他攻擊事件，企業要維持安全性的最佳實踐



在企業範圍內套用關鍵的修補程式以降低攻擊面

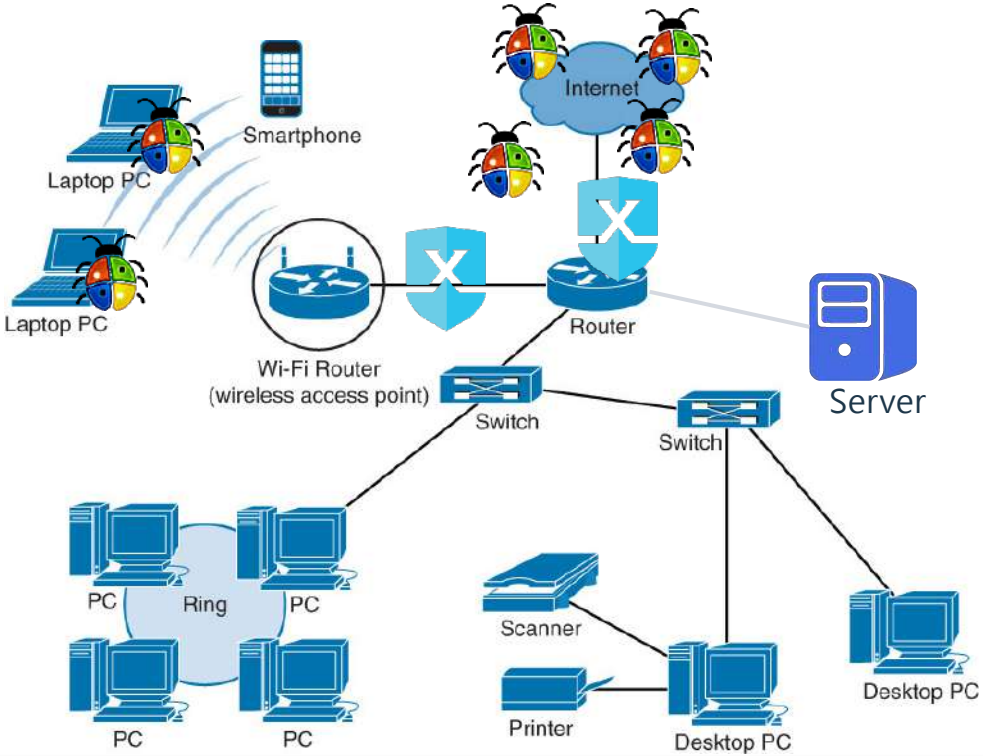


1. 確保無論地點及網路頻寬，都能夠發現及回報所有用戶端狀況 (包含未納管的用戶端)
2. 儘可能地將修補程式自動化佈署到受衝擊的用戶端
3. 使用封閉 (Closed-loop) 驗證方式確保修補成功
4. 涵蓋所有用戶端、啟用持續性的安全執行政策以縮小攻擊面

用戶端安全與管理機制的提升

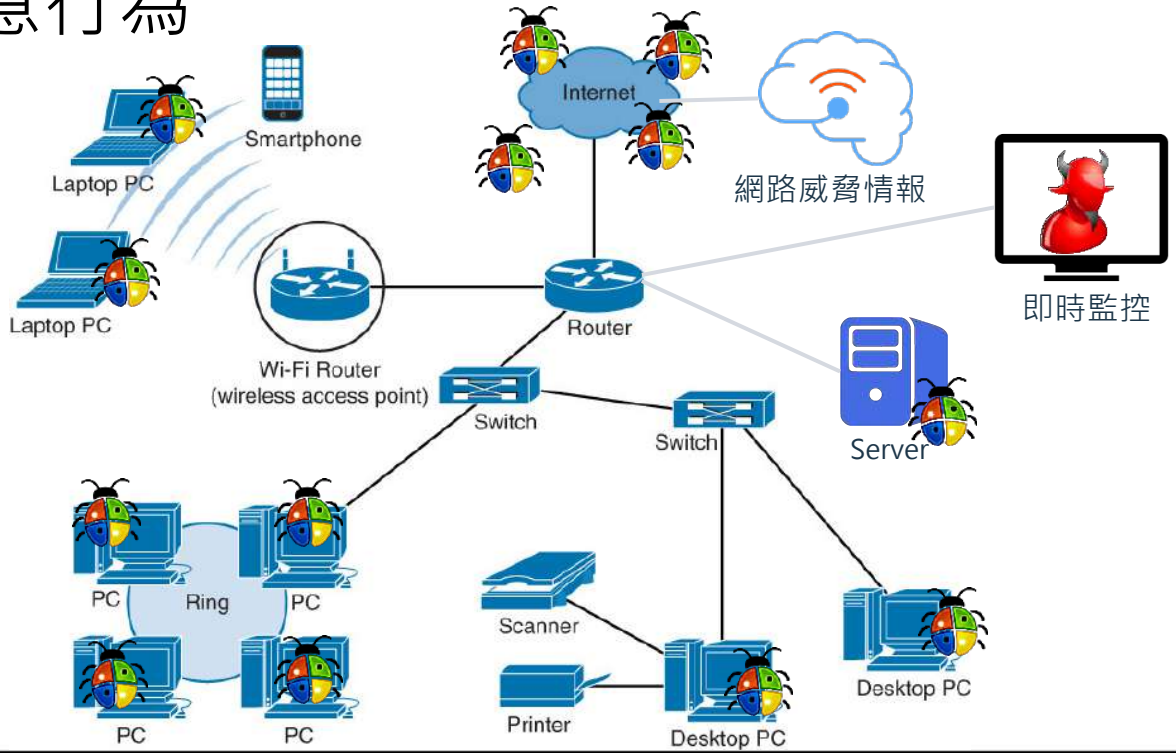
- **持續完整的了解用戶端活動和安全狀態**
  - ✓只有部份用戶端系統的最近狀況是不夠的
- **持續縮小攻擊面、並提供系統符合性報告**
  - ✓立即永久地降低風險
- **促成系統維運管理人員與資安管理人員之間的協同合作**
  - ✓更有效率的主動與配合執行管理程序

阻止惡意軟體及進階威脅進入您的網路



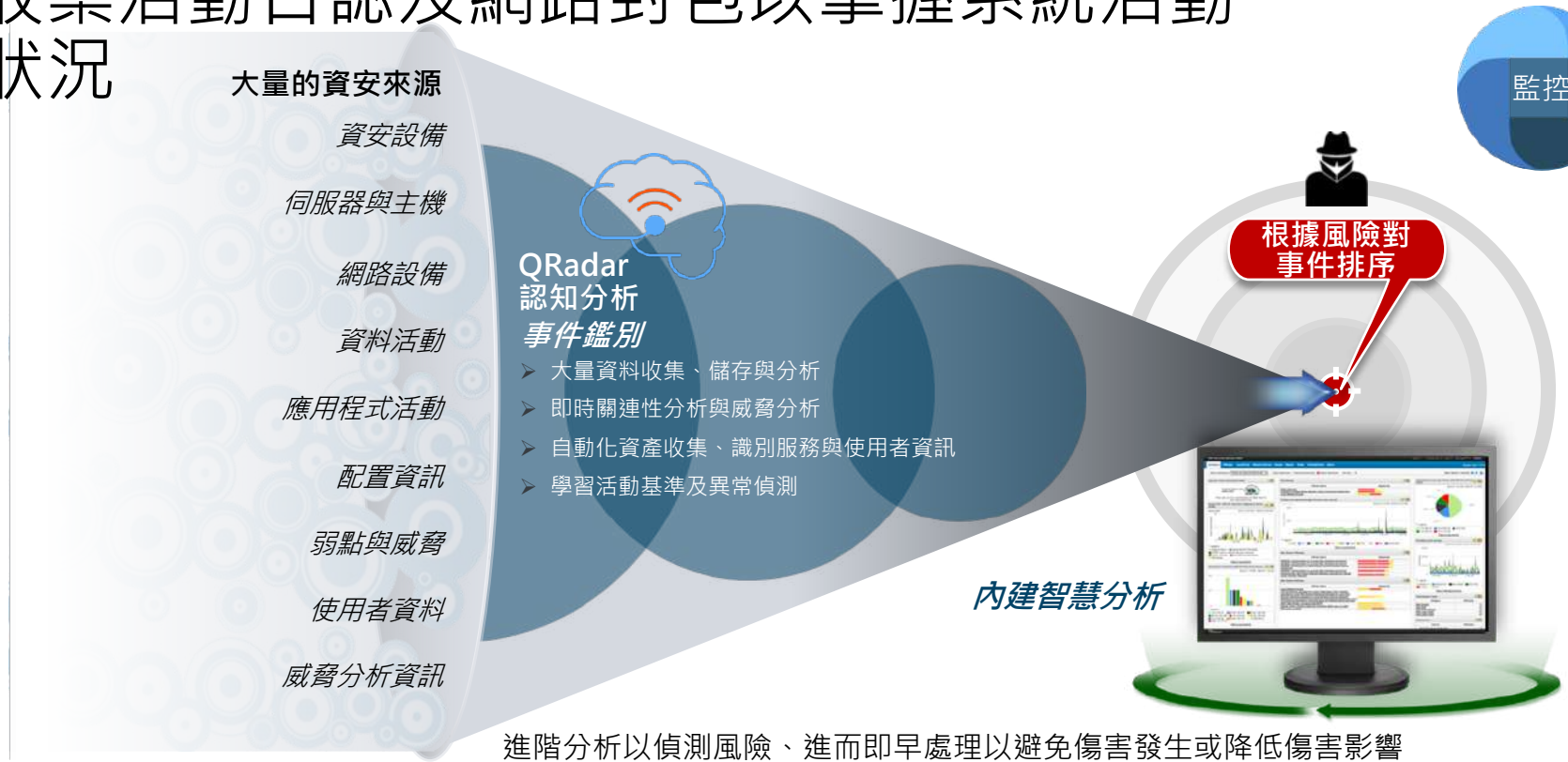
1. 串接企業網路佈署網路防護裝置
2. 確保 IP 信譽和 URL 過濾資訊持續更新，以自動阻止惡意網站存取
3. 確保網路防護簽名 (Signatures) 及韌體 (Firmware) 是最新版本

監視與偵測嘗試進入網路的惡意軟體及惡意行為



1. 收集內部設備日誌及網路封包以集中管理分析
2. 擬定關連性分析原則，檢視可疑程式與行為
3. 整合網路情報資訊以確認可疑程式行為與感染範圍

收集活動日誌及網路封包以掌握系統活動狀況



進階分析以偵測風險、進而即早處理以避免傷害發生或降低傷害影響

重組網路封包進行深度分析

FLOWS

- Source and destination IP and port information
- IP protocol
- Byte / packet counts
- Time of first / last packets
- IP Class of service
- VLAN information
- IP reputation

ENRICHED FLOWS

- Application identification
- Usernames, e-mail, chat IDs
- URLs
- Search arguments
- Host information
- HTTP analysis
- DNS queries / responses
- File name, type, size, hash
- Configurable Suspect Content

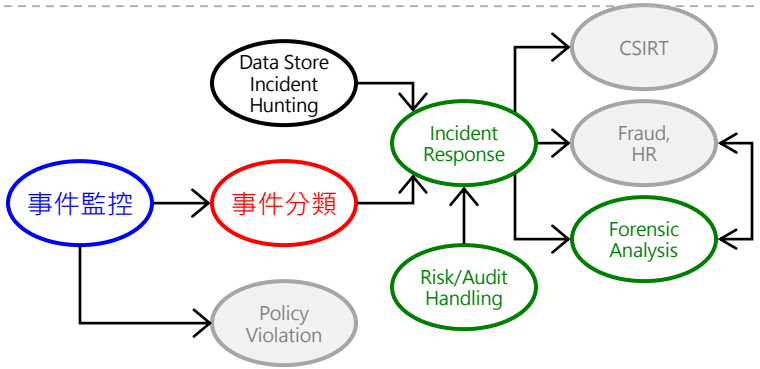
CONTENT ENRICHED FLOWS

- Personal information detection
- Confidential data detection
- Embedded scripts
- Redirects
- Configurable Content-based Suspect Content

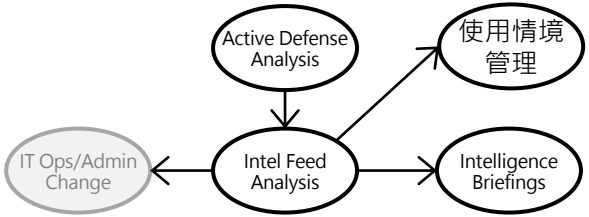
企業應擬定資安事件的通報與處理組織及流程，以確保事件均受到適當的處理

SOC 管理 | 資安智慧分析 | 監控 | 分類 | 回應 | 資安管理 | IT維運/其他

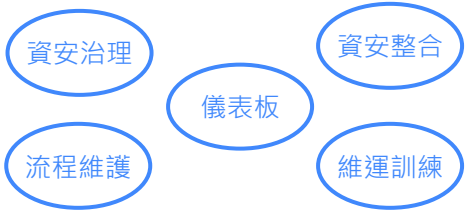
核心資訊安全服務



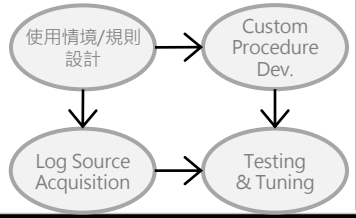
INTELLIGENCE SERVICES



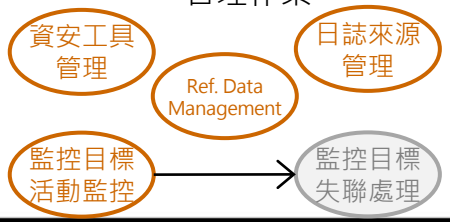
SOC 管理



SERVICE DEPLOYMENT

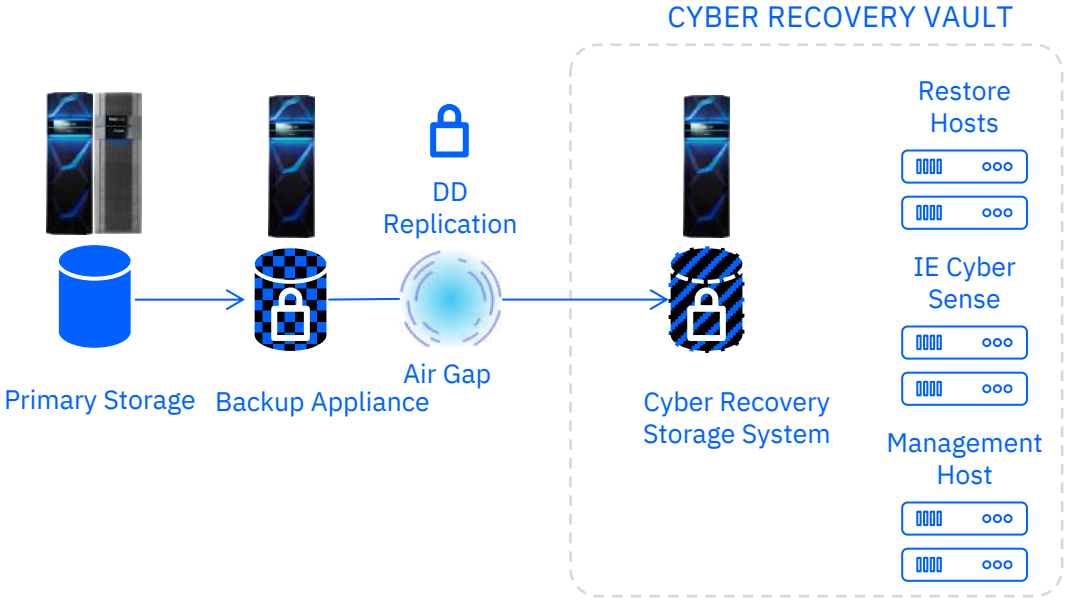


管理作業



ITIL 流程

Cyber Vault 解決方案



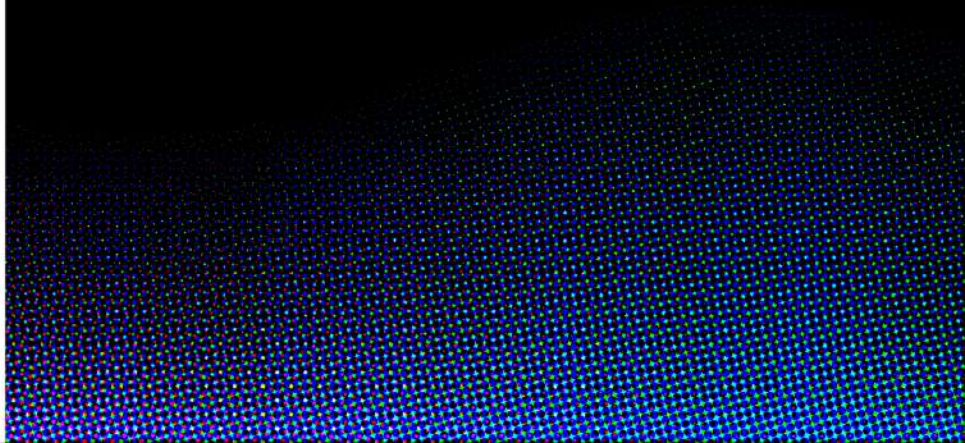
- Create backup of data
- RESTful API for open automation and analytics
- Enable data link and replicate to isolated system
- Complete replication and disable data link
- Maintain WORM locked restore points
- Security analytics on data at rest -- Index Engines CyberSense Analytics on Vault Data
- IBM Orchestration recovers and mounts apps/DB's
- IBM Services

IBM Security

IBM

你改變世界 我守護安全

You change the world, we secure it.



2019 IBM 全球資安高峰會 台北場