Stay ahead. 先馳得點

Innovate2013
開發者大會

企業智能防護策略

趨勢科技
新事業開發暨產品行銷協理
曾昆一

Innovate2013
The IBM Technical Summit
開發者大會

Stay ahead. 先馳得點

過去…

僅需使用者管理與工作站電腦

壁壘分明的企業網路環境

固定環境: 實體主機伺服器,企業資料

病毒爆發,蠕蟲,垃圾郵件與簡訊

周邊安全,存取控管,病毒防護與垃圾郵件過濾

現在…

使用者使用多重設備與個人裝置並且無時無刻的存取

分散式網路與彈性的邊界

動態且多重架構: 移動裝置、虛擬化、雲端

更多複雜與目標式的攻擊行為

以裝置為中心的安全解決方案

→ *不足以防護新的威脅且更加難以管理!!*

何謂智能防護策略? (Triple S)

Smart protection
防護竊取與遺失

- ✓ 分層防護
- ✓ 互聯機制
- ✓ 即時防護
- ✓ 透明化

Simple
彈性的管理與佈署

- ✓ 集中管理
- ✓ 自動化
- ✓ 輕量級
- ✓ 靈活具彈性

Security that fits
一個持續發展的防護體系

- ✓ 開放
- ✓ 優化
- ✓ 聚焦問題
- ✓ 創新架構

智能防護緣起於全球化雲端機制

- 白名單
- 網路流量規則
- 行動裝置APP信譽評等
- 系統與應用程式漏洞/攻擊防護
- 威脅行為研究
- 進階版的檔案信譽評等
- 進階版的網頁信譽評等

海量資料
分析導向
全球智能主動威脅防護
Now

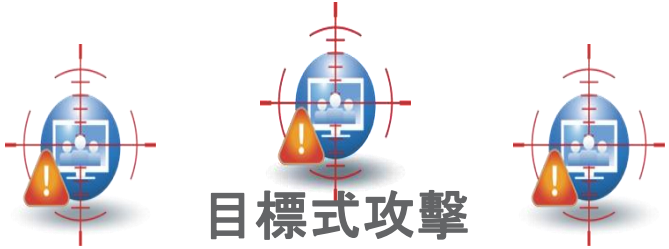
- 郵件信譽評等
- 檔案信譽評等
- 網頁信譽評等

雲端架構基礎
全球威脅分析與回饋
智能防護架構

2008

特徵式基礎
病毒防護技術

1988 - 2007



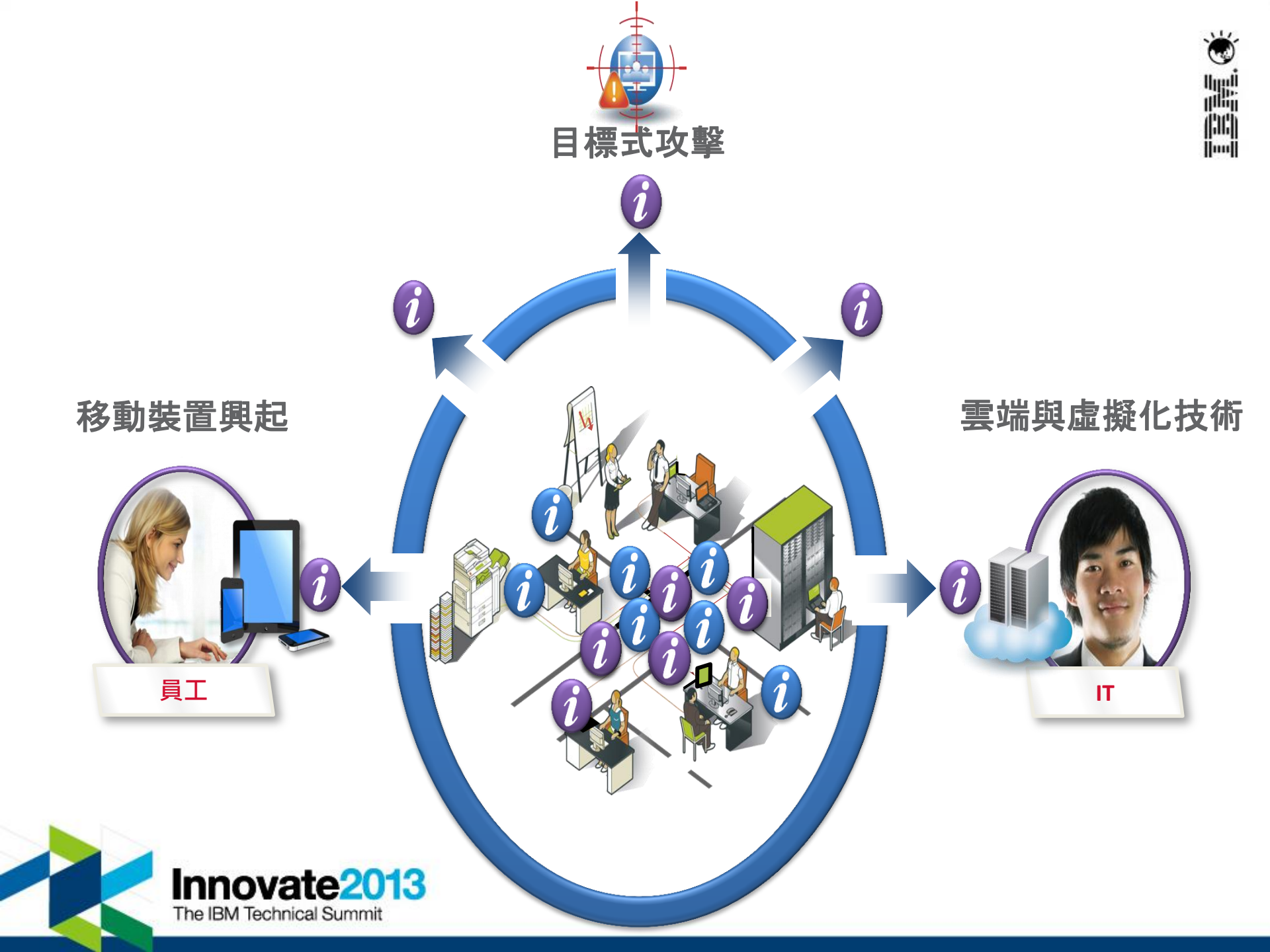
目標式攻擊

移動裝置興起

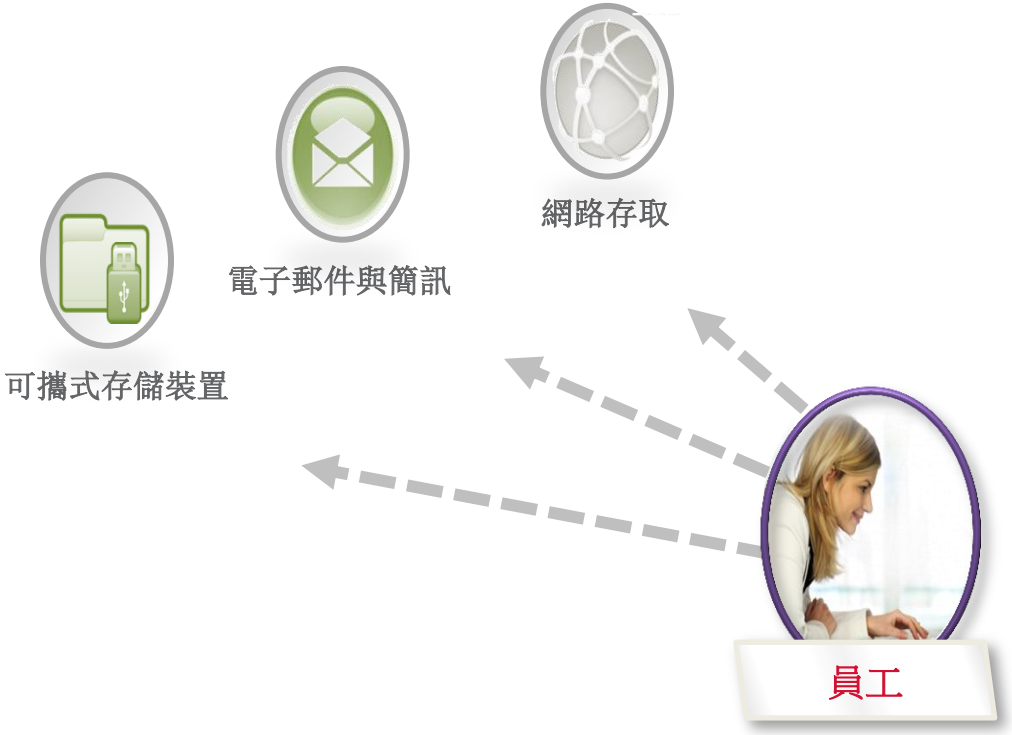
員工

雲端與虛擬化技術

IT

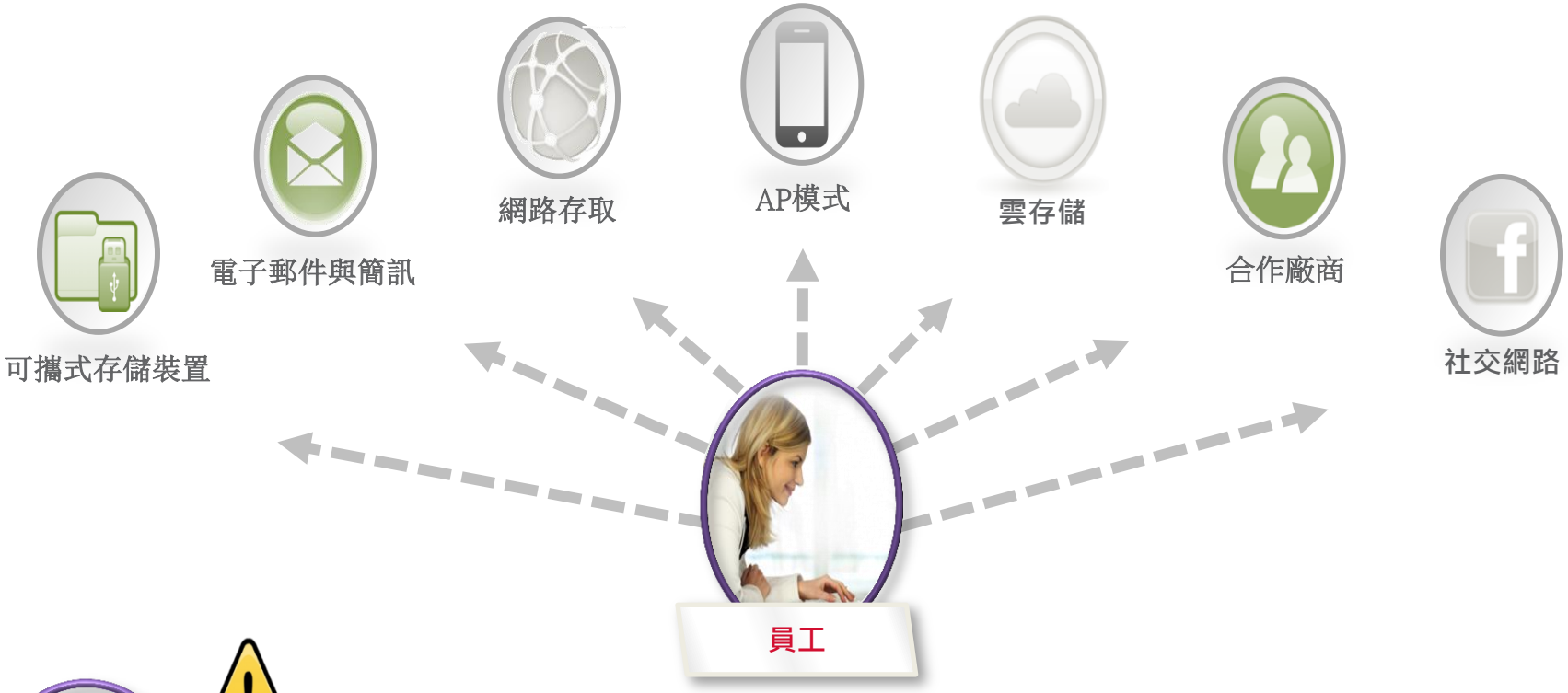

目標式攻擊
移動裝置興起
雲端與虛擬化技術
員工
IT

過去...



現在..


網路存取
AP模式
雲存儲
電子郵件與簡訊
合作廠商
可攜式存儲裝置
社交網路
員工
IT 管理者
vmware
Office
Office 365
Google Docs
EVERNOTE
box



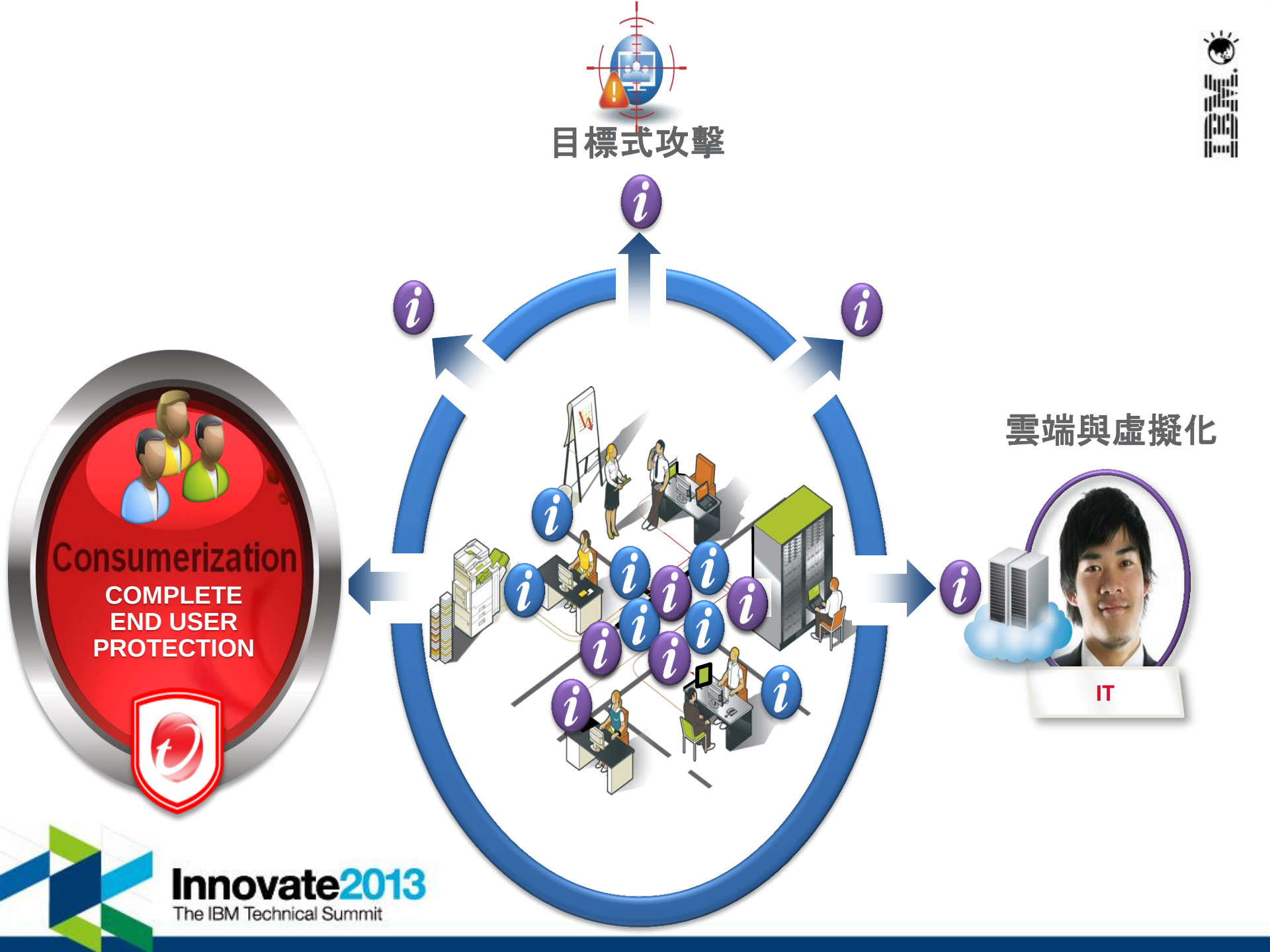
91% 目標式攻擊採取釣魚郵件(Spear-Phishing)

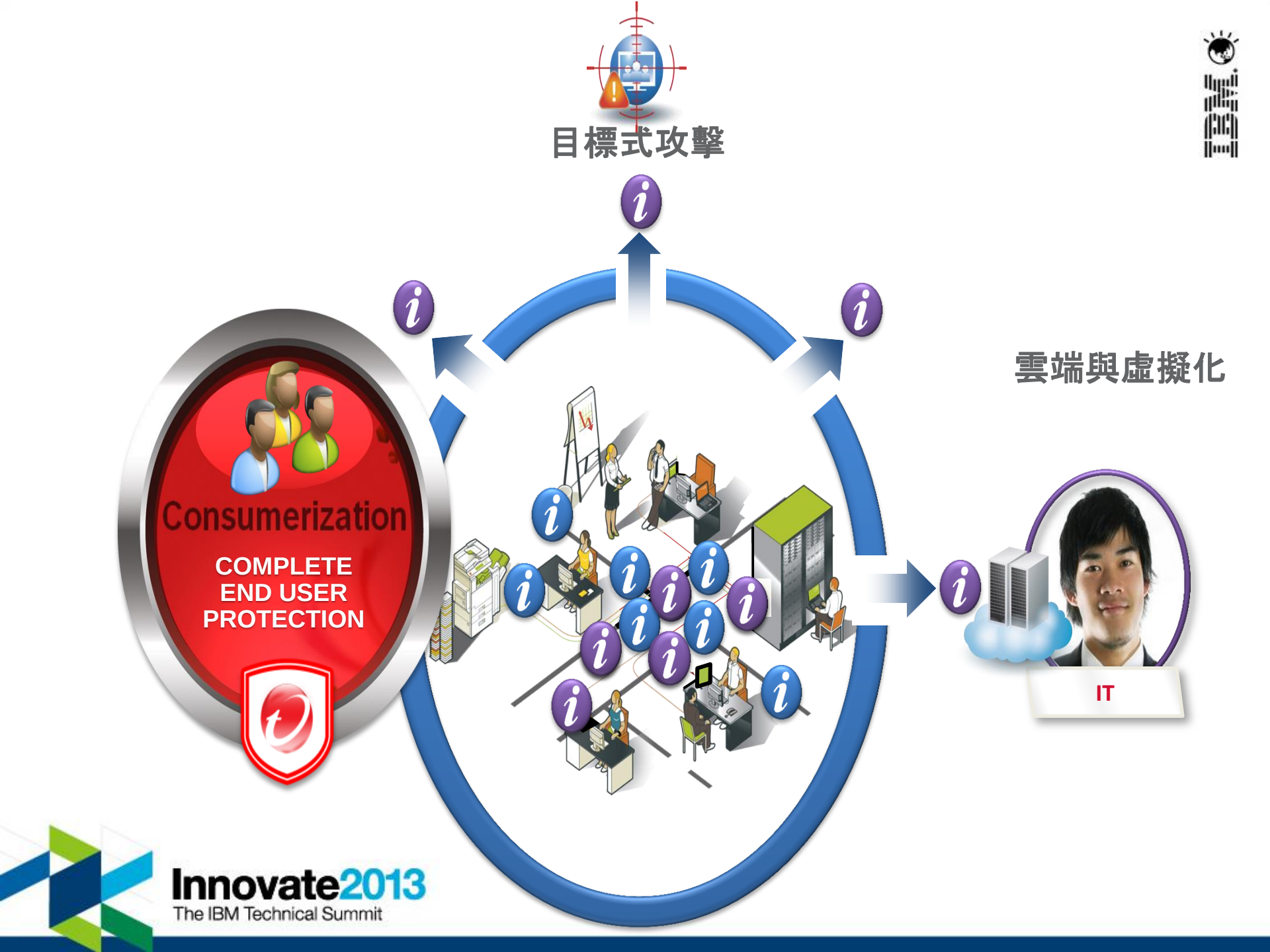
1 million Android 惡意apps將會產生於2013年底

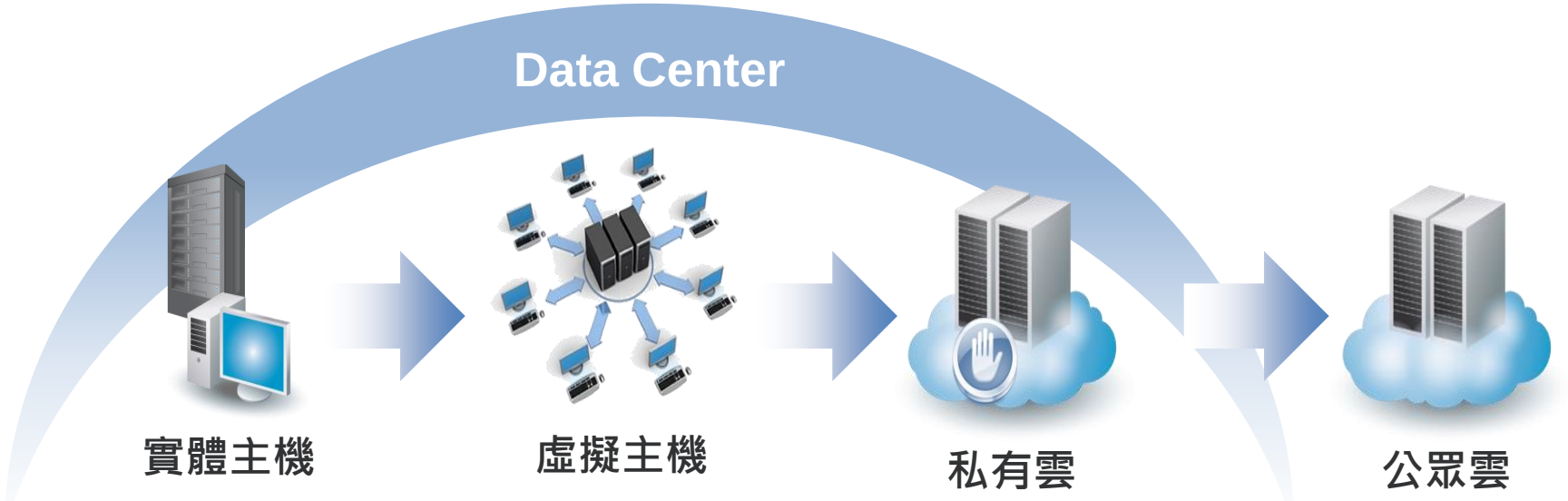
1 in 5 在工作中使用 Dropbox 雲存儲服務

1: Trend Micro: "Spear Phishing Email: Most Favored APT Attack Bait", Nov 2012
2: **Trend Micro Threat Predictions for 2013**
3: Global survey of 1300 enterprise customers; "Shadow IT in the Enterprise", Nasuni, Sept 2012


可攜式存儲裝置
電子郵件與簡訊
網路存取
AP模式
雲存儲
合作廠商
社交網路
Any device, any app, anywhere
員工
惡意程式防護
內容過濾機制
資料外洩防護
磁碟加密
檔案加密
設備控管
應用程式控管
Complete End User Protection
TREND MICRO
SMART
PROTECTION
NETWORK
資安稽核
IT 管理者


目標式攻擊
Consumerization
COMPLETE
END USER
PROTECTION
雲端與虛擬化
IT


目標式攻擊
雲端與虛擬化
Consumerization
COMPLETE
END USER
PROTECTION
IT

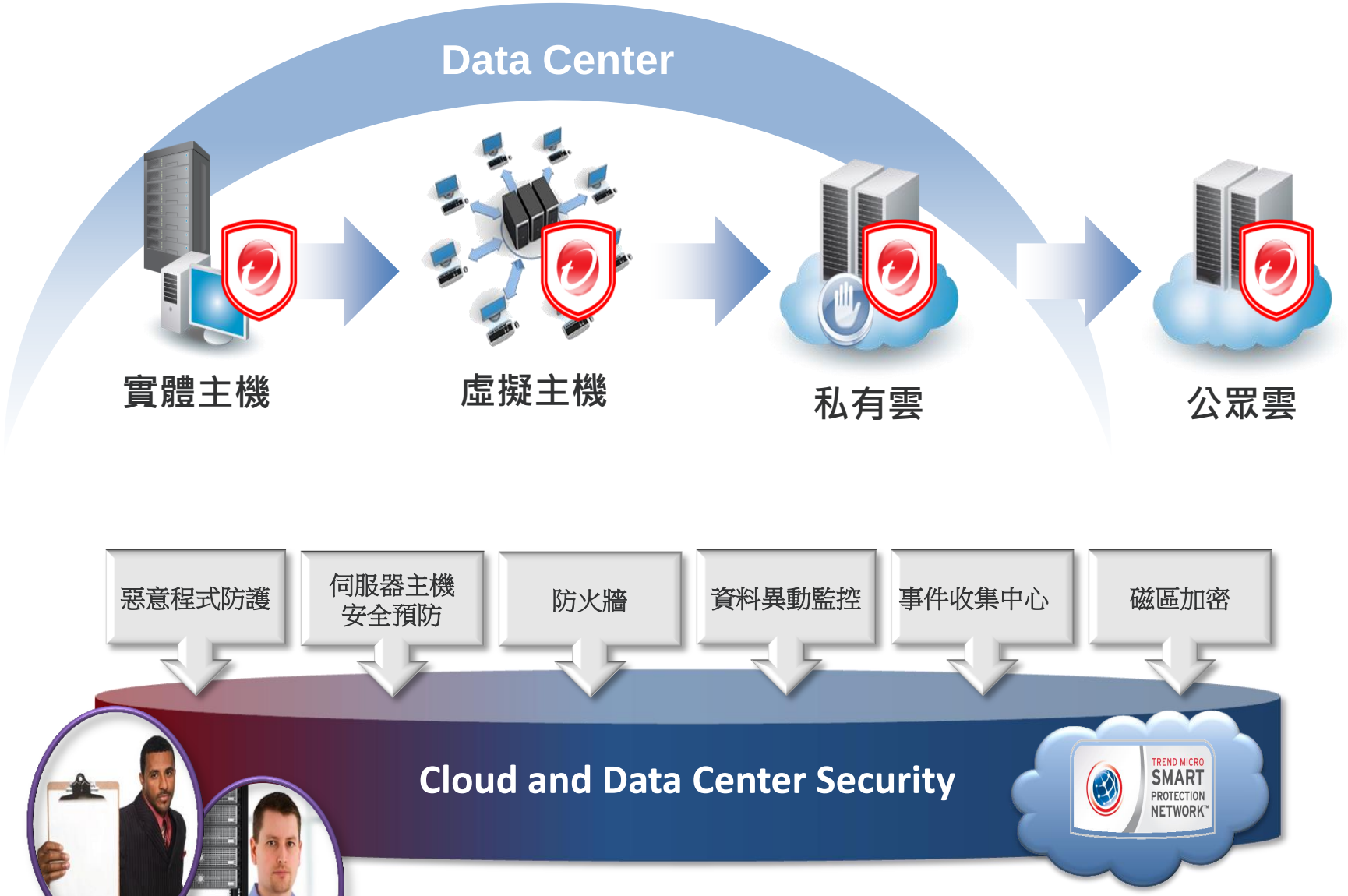


By 2016, **71%** of server workloads will be **virtualized***;

Organizations can cut costs by **74%** by storing data in the cloud*

Sources: Gartner, Forecast Analysis: Data Center, Worldwide, 2010-2016 1Q12 Update, Jonathon Hardcastle, 16 May, 2012

- 伺服器與虛擬主機的安全性
- 資安政策執行確實性
- 資料保護(特別是私有雲或公眾雲)
- 效能與可管理性

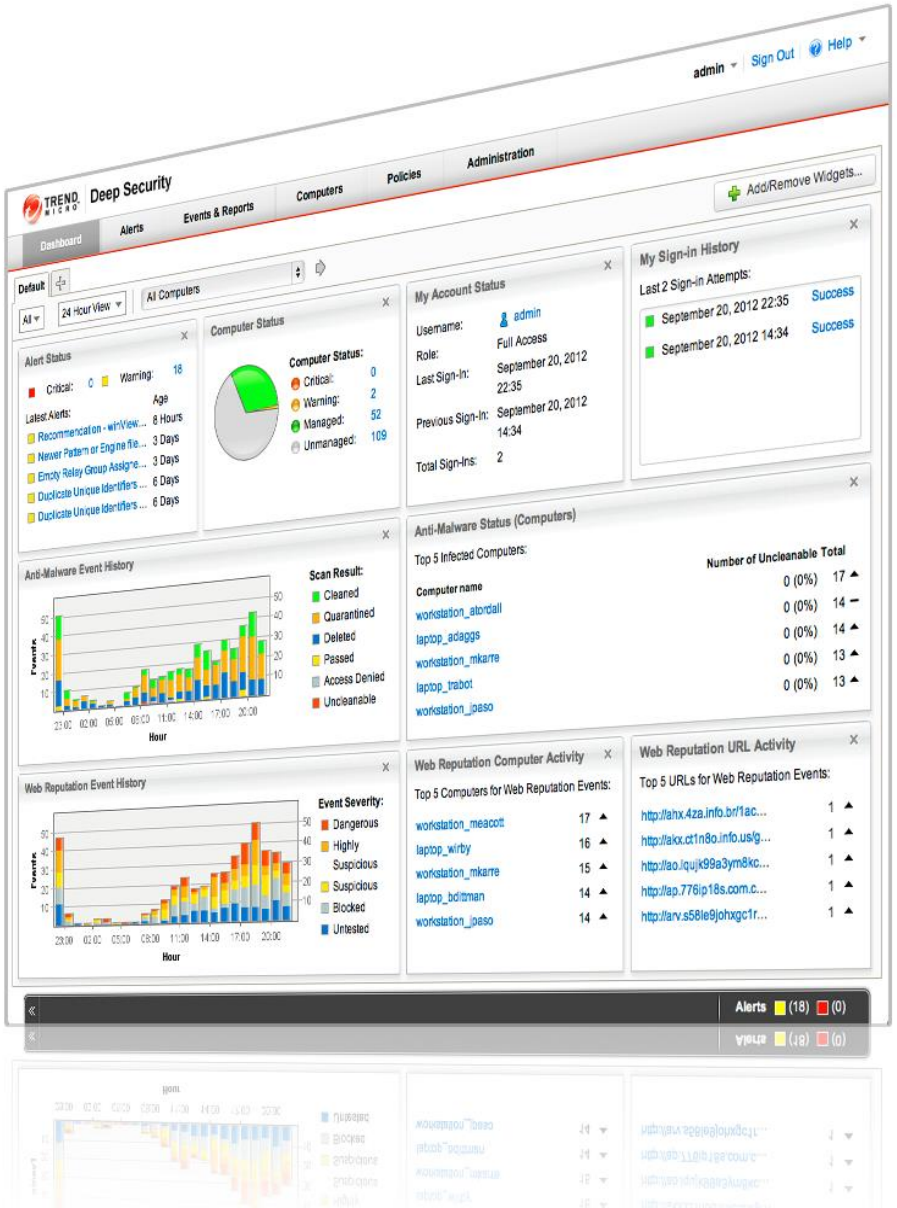

Data Center
實體主機
虛擬主機
私有雲
公眾雲
惡意程式防護
伺服器主機
安全預防
防火牆
資料異動監控
事件收集中心
磁區加密
Cloud and Data Center Security
TREND MICRO
SMART
PROTECTION
NETWORK
資安稽核
Data Center Ops

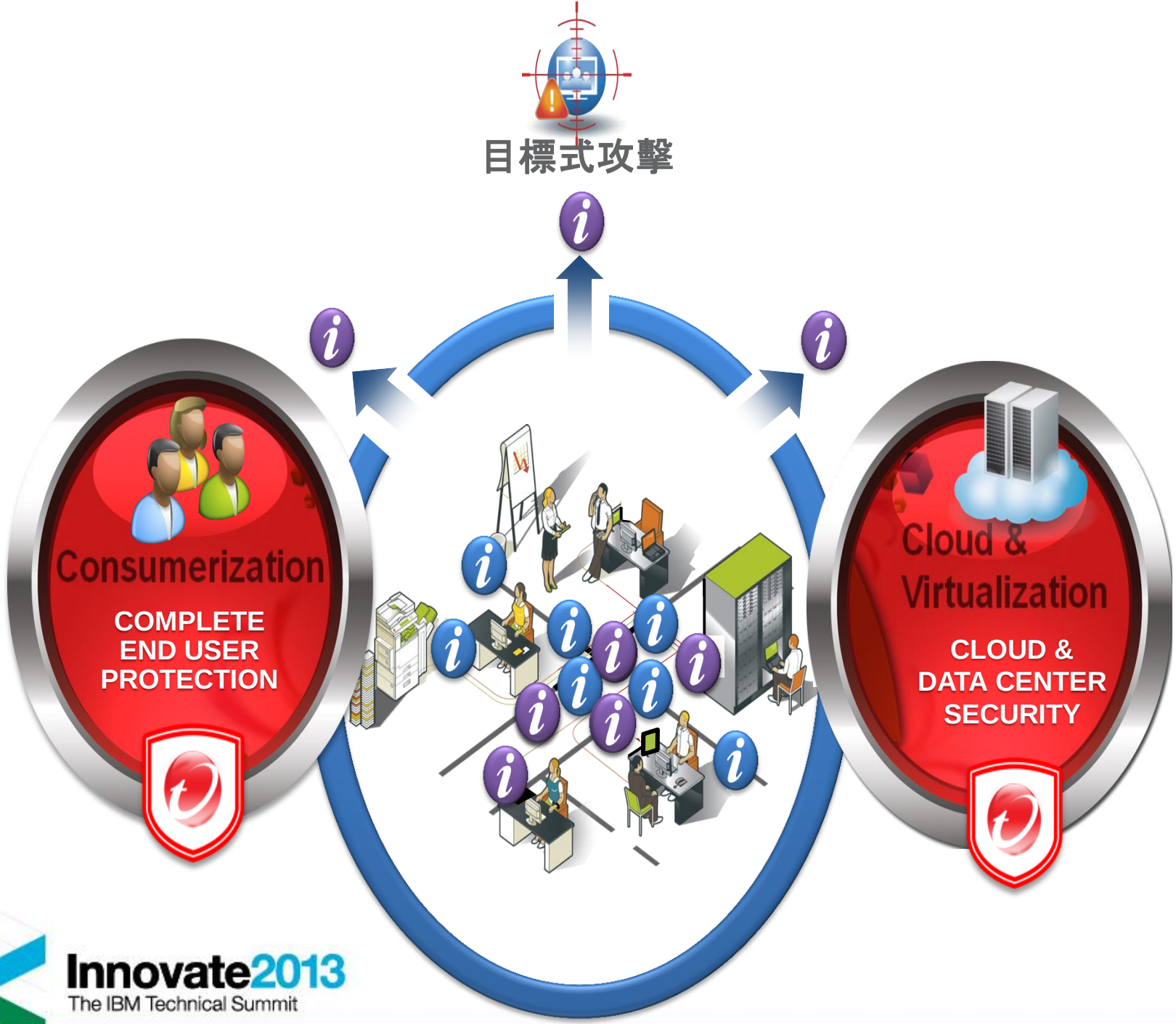
Deep Security：同時提供虛擬與實體防護

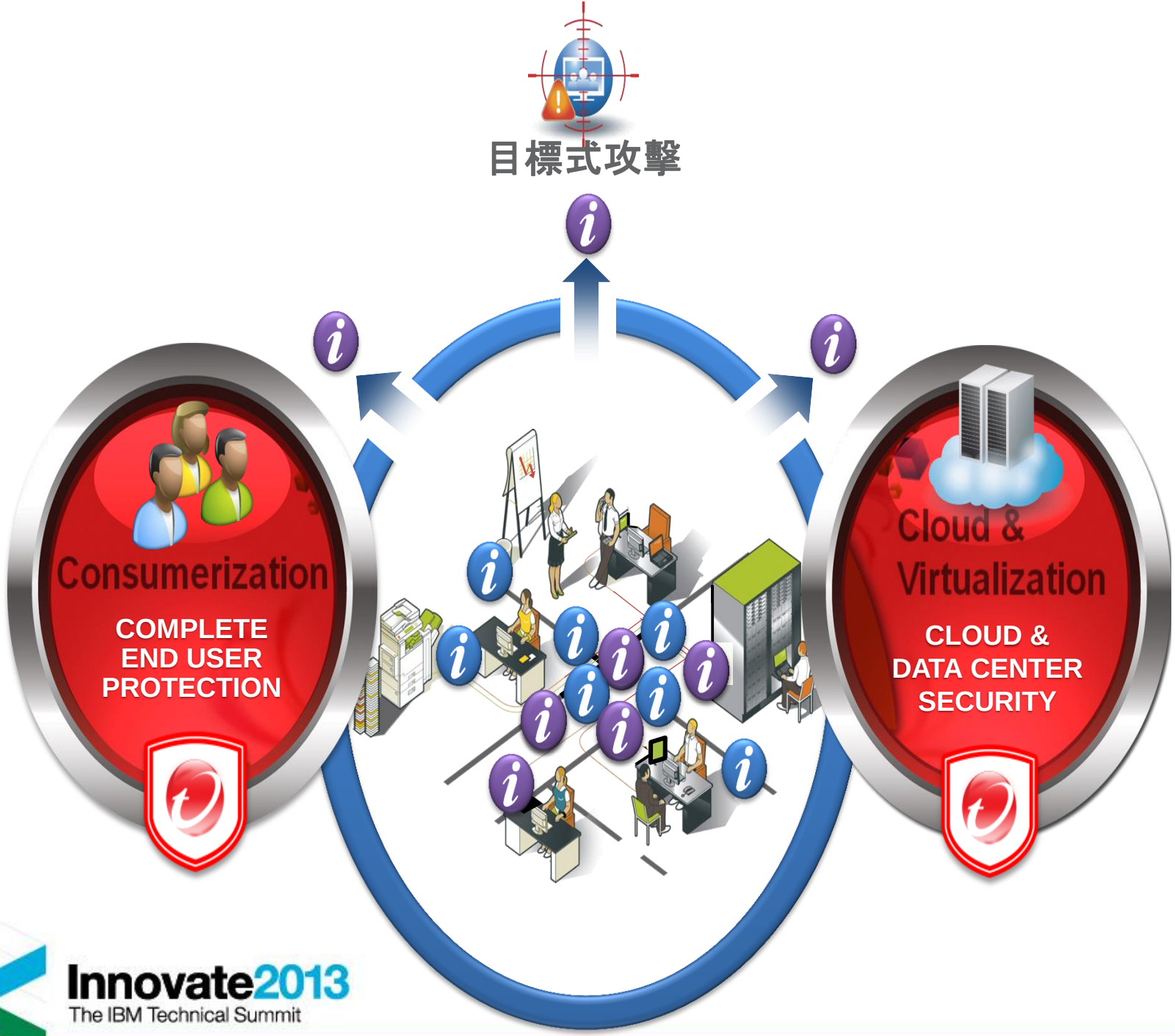
- 單一平台提供虛擬主機與實體主機甚至雲端OS管理

New:

- 進一步區分VMware的優化
- 改進的性能（高速緩存，去除重複）
- 更強的保護（自動虛擬補丁，虛擬機管理程序的完整性監控）
- 混合雲管理為AWS和vCloud




目標式攻擊
Consumerization
COMPLETE
END USER
PROTECTION
Cloud &
Virtualization
CLOUD &
DATA CENTER
SECURITY


目標式攻擊
Consumerization
COMPLETE
END USER
PROTECTION
Cloud &
Virtualization
CLOUD &
DATA CENTER
SECURITY

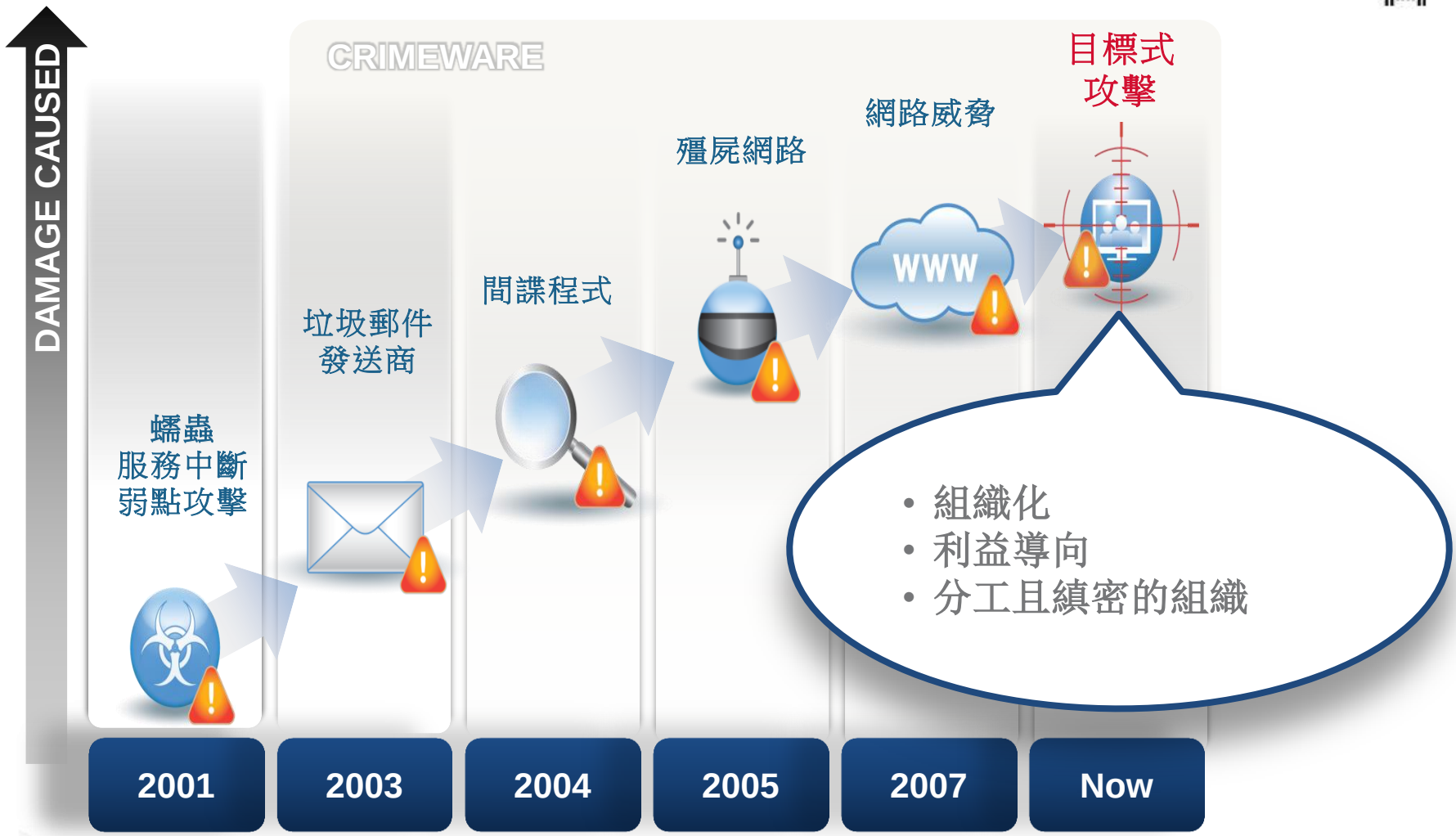
威脅的驅動力

- 企業遭受損失，但駭客行為並不是利益導向、某個程度上是為了自我成就
- 大多數駭客的最大原動力是; ‘because they could’ !

蠕蟲
服務中斷
弱點攻擊

2001

威脅的驅動力


DAMAGE CAUSED
CRIMEWARE
蠕蟲
服務中斷
弱點攻擊
垃圾郵件
發送商
間諜程式
殭屍網路
網路威脅
目標式
攻擊
WWW
• 組織化
• 利益導向
• 分工且縝密的組織
2001
2003
2004
2005
2007
Now

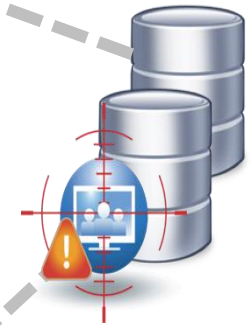
今日的攻擊模式: 社交工程,複雜手法,低調隱密!

透過網際網路與社交網路
收集目標的相關訊息

攻擊者

潛伏可長達數月到數年，伺機竊取有價資訊

$$$$

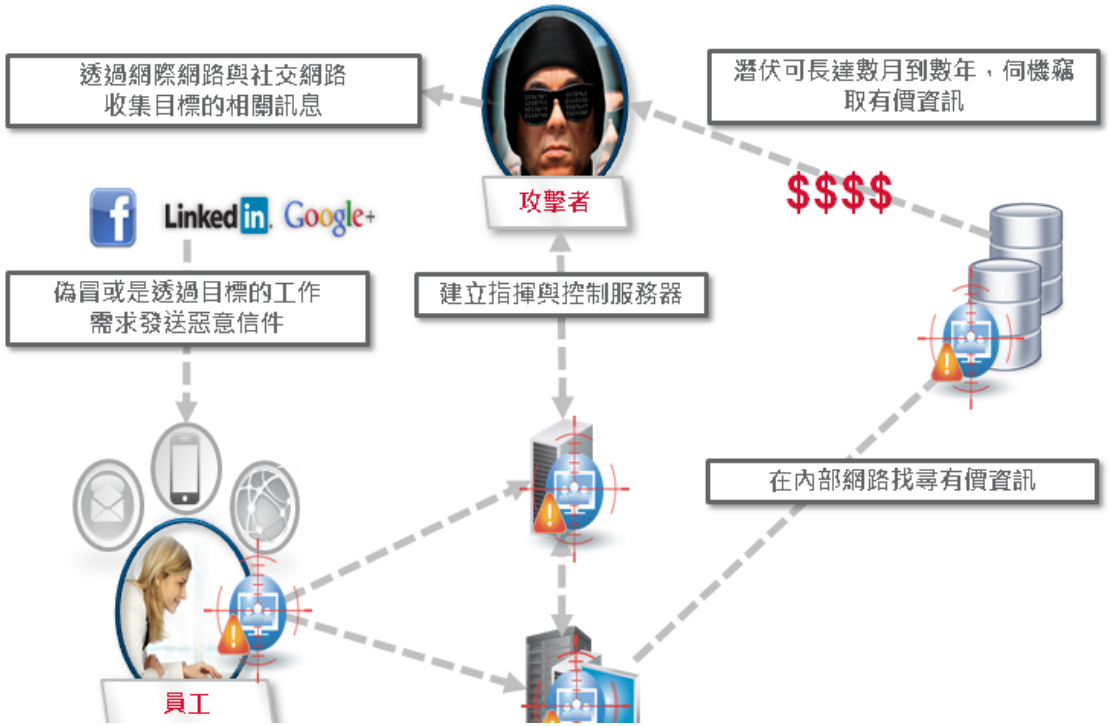


偽冒或是透過目標的工作需求發送惡意信件

建立指揮與控制服務器

員工

在內部網路找尋有價資訊

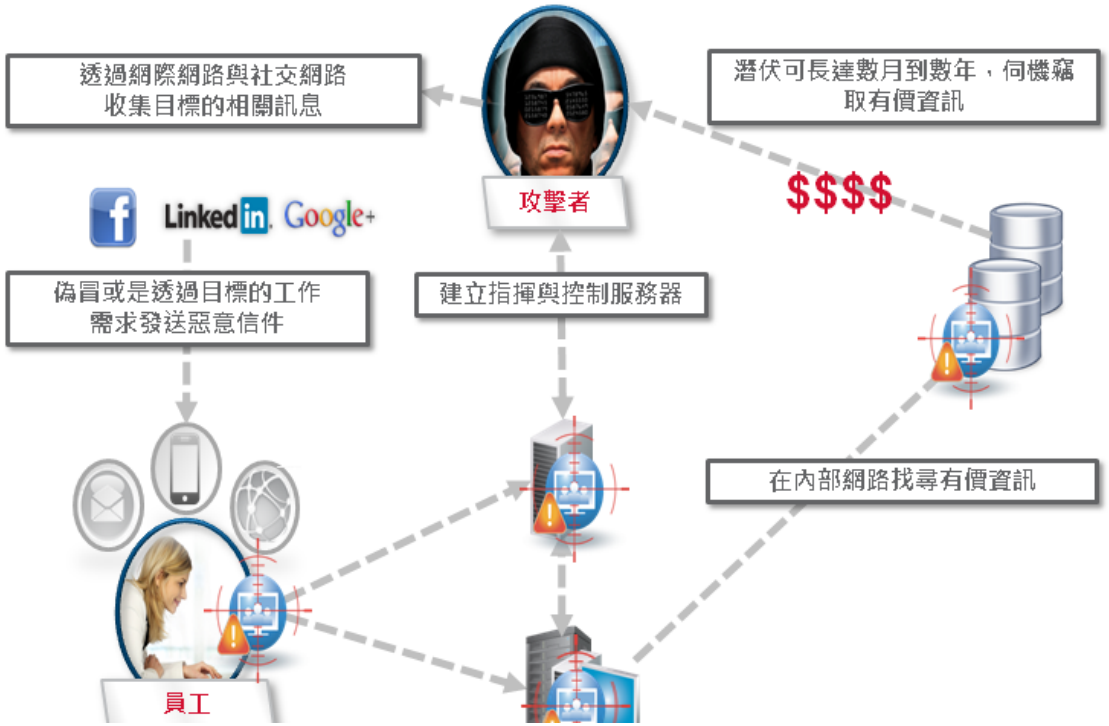


1.8 個目標或企業每周平均被入侵

$8.9M in the US / **$5.15M** in Japan

每年平均損失金額

Sources: 2012 Ponemon, Cost of Cyber Crime Study



A *Custom* Attack needs a *Custom* Defense!

目標攻擊的完整的防護週期與架構

Detect
惡意程式活動與行為判斷，惡意檔案分析與阻擋

Analyze
分析攻擊和攻擊的風險和特點

Adapt
自動化的安全更新 (IP 黑名單, 客製化特徵…)

Respond
使用分析的情資並用以回並產出解藥與防護機制

網路匝道偵測 | 客製化的沙箱系統 | 威脅情資 | 進階的威脅分析 | 自動化的防護更新 | 威脅工具與服務

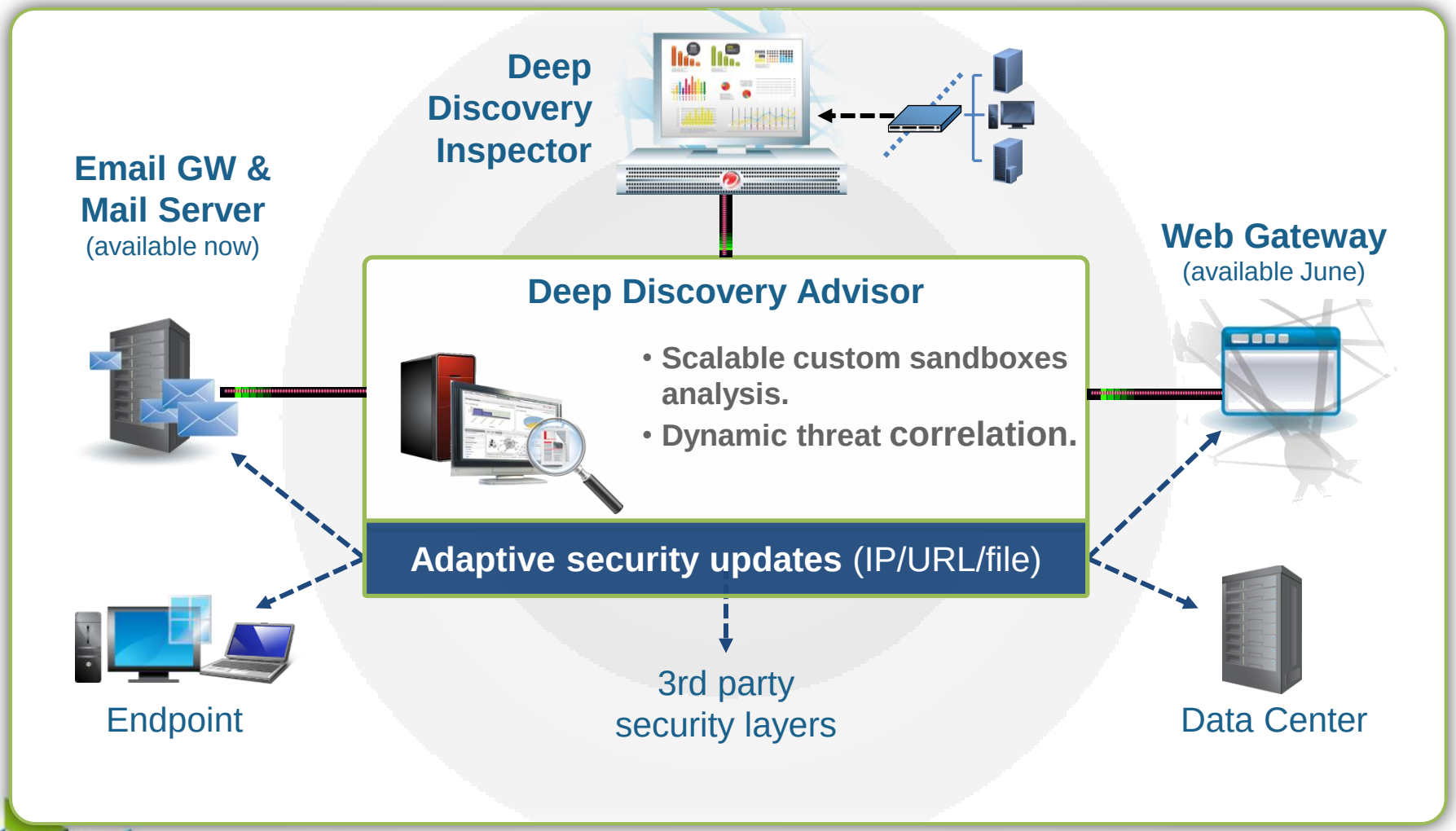
資安稽核

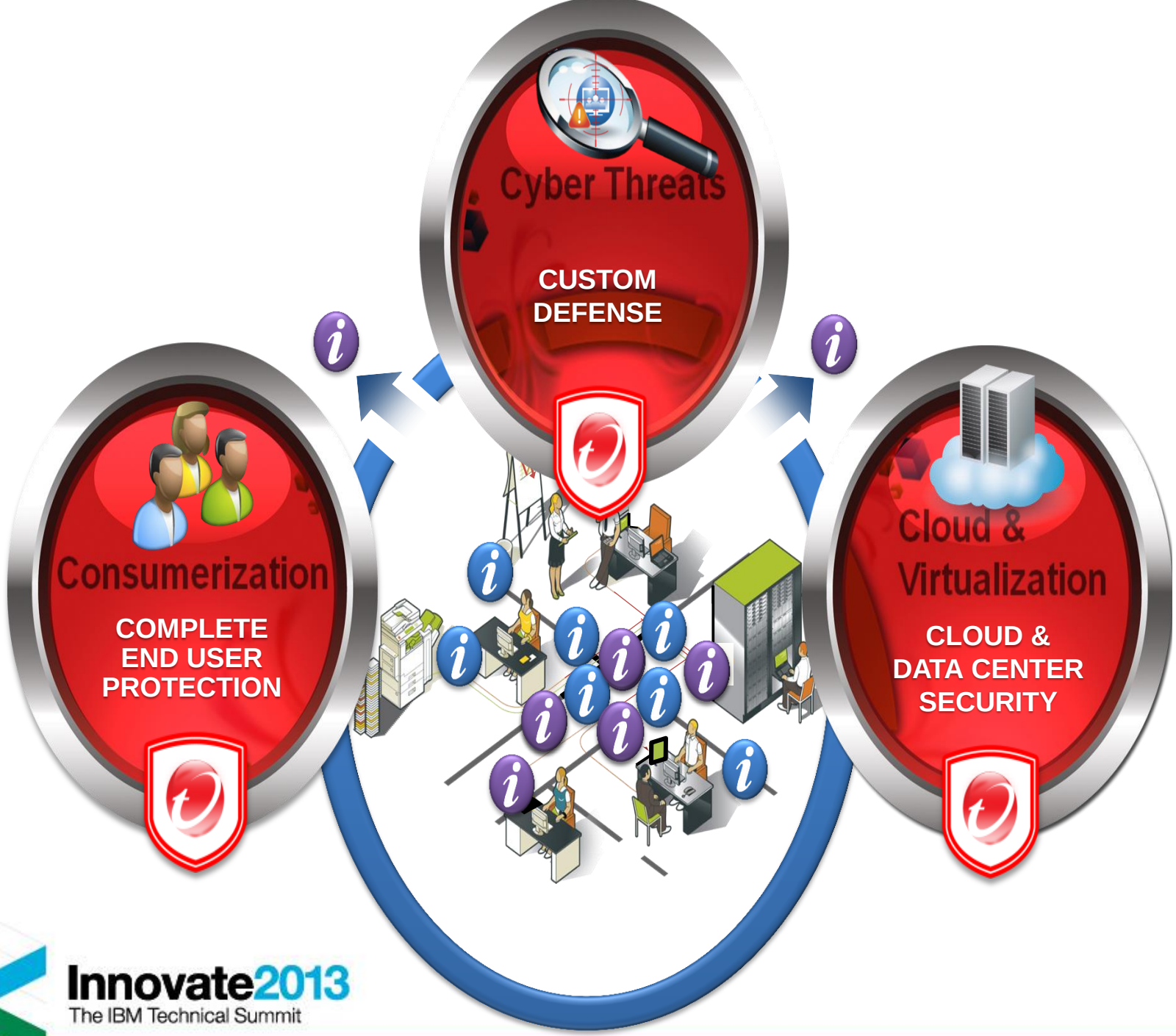
網路管理者

Custom Defense

TREND MICRO SMART PROTECTION NETWORK™

Trend Micro Custom Defense Detects Framework




Cyber Threats
CUSTOM DEFENSE
Consumerization
COMPLETE END USER PROTECTION
Cloud & Virtualization
CLOUD & DATA CENTER SECURITY

Smart Protection: Smart, Simple, Security that Fits

Thank You