Microsoft® Forefront™

連動防禦、制敵機先 ー 新一代的全方位資安防禦系統 Forefront Code name：Stirling

謝育倫 (Joseph Hsieh)
技術專員
台灣微軟

大綱

- 目前的資訊安全挑戰
- 微軟的安全解決方案演進
- 新一代的資訊安全防禦
  - 全方位的防護
  - 統合的管理
  - 安全問題的洞悉力
- 總結
- Q&A

Microsoft® Forefront™

目前的資訊安全挑戰

安全管理與存取的挑戰

安全管理挑戰

威脅與風險增加

- 更危險的威脅
- 更大量的攻擊
- 被利益驅使

安全規劃更細分

- 更多類型產品
- 產品與產品間溝通困難
- 缺乏整合性

更複雜的管理與佈署

- 管理介面眾多
- 缺乏整合的報表
- 複雜且TCO高

存取安全挑戰

行動連線需求增加

- 更多的使用者
- 更複雜的環境跟設備
- 內部與外部同時存取

傳統VPN存在風險

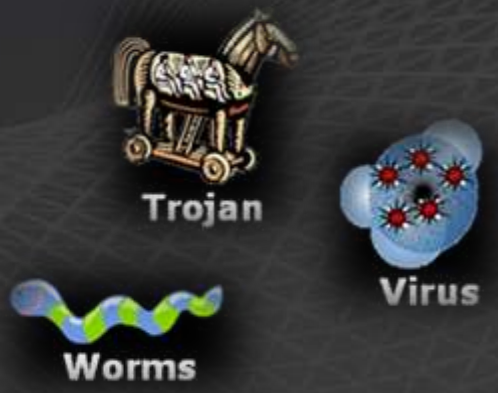
- 完整連線所帶來風險
- 缺乏應用程式整合
- 連線不穩定

難以強制原則執行

- 法律規則時時變動
- 企業單位原則改變
- 不易區分清楚

Conficker攻擊

- 攻擊未安裝patch的電腦
- 攻擊administrator密碼設定過於簡單的電腦
- 透過USB隨身碟散佈
- 偽造domain admin身分攻擊企業內部電腦
- 自動上網下載惡意程式
- 開啟後門等待接收駭客指令



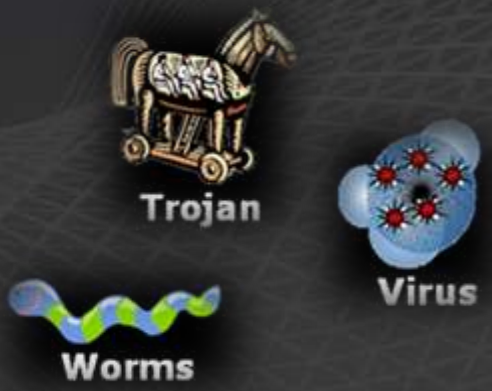
USB病毒與IMBOT

USB病毒

- 利用目前最常見的USB存取裝置
- 中毒電腦會繼續散布病毒
- 執行特殊程式

IMBOT

- 利用多種管道讓電腦成為殭屍電腦
- 透過即時通訊來控制電腦
- 影響包含Yahoo即時通、Google Talk以及MSN



Microsoft® Forefront™

微軟安全解決體系

Microsoft® Forefront™

一套完整的企業安全性產品可用來協助企業經由深度整合與簡化管理的方式取得更完善的防護

作業系統防護

Microsoft® Forefront™ Client Security

應用伺服器防護

Microsoft® Forefront™ Security for Exchange Server

Microsoft® Forefront™ Security for SharePoint™

Microsoft® Forefront™ Server Security Management Console

閘道防護

Microsoft® Internet Security & Acceleration Server 2006

Intelligent Application Gateway 2007

"Stirling" Forefront進化再升級

全面性防護體系

作業系統防護

Microsoft® Forefront™ Client Security

vNext

應用伺服器防護

Microsoft® Forefront™ Security for Exchange Server

vNext

Microsoft® Forefront™ Security for SharePoint®

vNext

Microsoft® Forefront™ Security for Office Communications Server

閘道防護

Microsoft® Forefront™ Threat Management Gateway

vNext

Microsoft® Forefront™ Unified Access Gateway

vNext

Microsoft® Forefront™ Code Name "Stirling"

完全整合之安全系統

Management & Visibility

動 態 回 應 機 制

Shared Information

Action

Action

作業系統防護	應用伺服器防護	閘道防護
		
Microsoft® Forefront™ Client Security	Microsoft® Forefront™ Security for Exchange Server Microsoft® Forefront™ Security for SharePoint™	Microsoft® Forefront™ Threat Management Gateway Microsoft® Forefront™ Unified Access Gateway

功能概觀

Microsoft® Forefront™ Client Security

- 惡意程式防護
- 端點防火牆
- 端點入侵防禦系統 (HIPS) (GAPA)
- 設備控管
- 整合網路存取保護(NAP)
- 軟體限制

Microsoft® Forefront™ Security for Exchange Server

- Exchange 2007 & E14 惡意程式防護
- 進階垃圾郵件過濾

Microsoft® Forefront™ Security for Office Communications Server

Microsoft® Forefront™ Security for SharePoint®

- SharePoint & OCS 2007 惡意程式防護
- 內容過濾

Microsoft® Forefront™ Threat Management Gateway

- 防火牆
- 網站(URL) 過濾
- HTTP/FTP 防毒
- 入侵防禦 (GAPA)
- 遠端存取
- 整合網路存取保護(NAP)

GAPA (由Microsoft Research提出)

Generic Application-Level Protocol Analyzer and its Language

Nikita Borisov, David Brumley, Helen J. Wang, Chuanxiong Guo
February 2005

Application-level protocol analyzers are important components in tools such as intrusion detection systems, firewalls, and network monitors. Currently, protocol analyzers are written in an ad-hoc fashion using low-level languages such as C, incurring a high development cost and security risks inherent in low-level language programming. Motivated by the large number of application-level protocols and new ones constantly emerging, we have architected and prototyped a Generic Application-level Protocol Analyzer (GAPA), consisting of a protocol specification language (GAPAL) and an analysis engine that operates on network streams and traces. GAPA

GAPA包含了語言與分析引擎，可以在網路串流中運作

development specification documents and supports both binary and text-based protocols. The GAPA design goals include expressiveness, ease of use, safety, and low overhead; it is intended to operate well in an adversarial environment. Our evaluation demo

GAPA可用於入侵偵測、防火牆、網路監控以及自動弱點防禦等部分

traffic. We have already found GAPA to be useful in intrusion detection, firewall, and networking monitoring contexts, and we envision additional applications, such as automatic vulnerability signature generation.

http://research.microsoft.com/apps/pubs/default.aspx?id=70223

Microsoft® Forefront™
Code Name "Stirling"

一套高度整合的安全系統，
提供企業從作業系統、伺服器到閘道端，一個全方位且富協調性的完整防護。

全方位的防護

- 提供作業端、應用端與閘道的整合式防護
- 動態回應機制有效防禦新型態惡意行為
- 次世代保護技術

統合的管理

- 簡化的單一管理控制
- 資產與原則導向的管理
- 整合現有的基礎架構

安全問題的洞察力

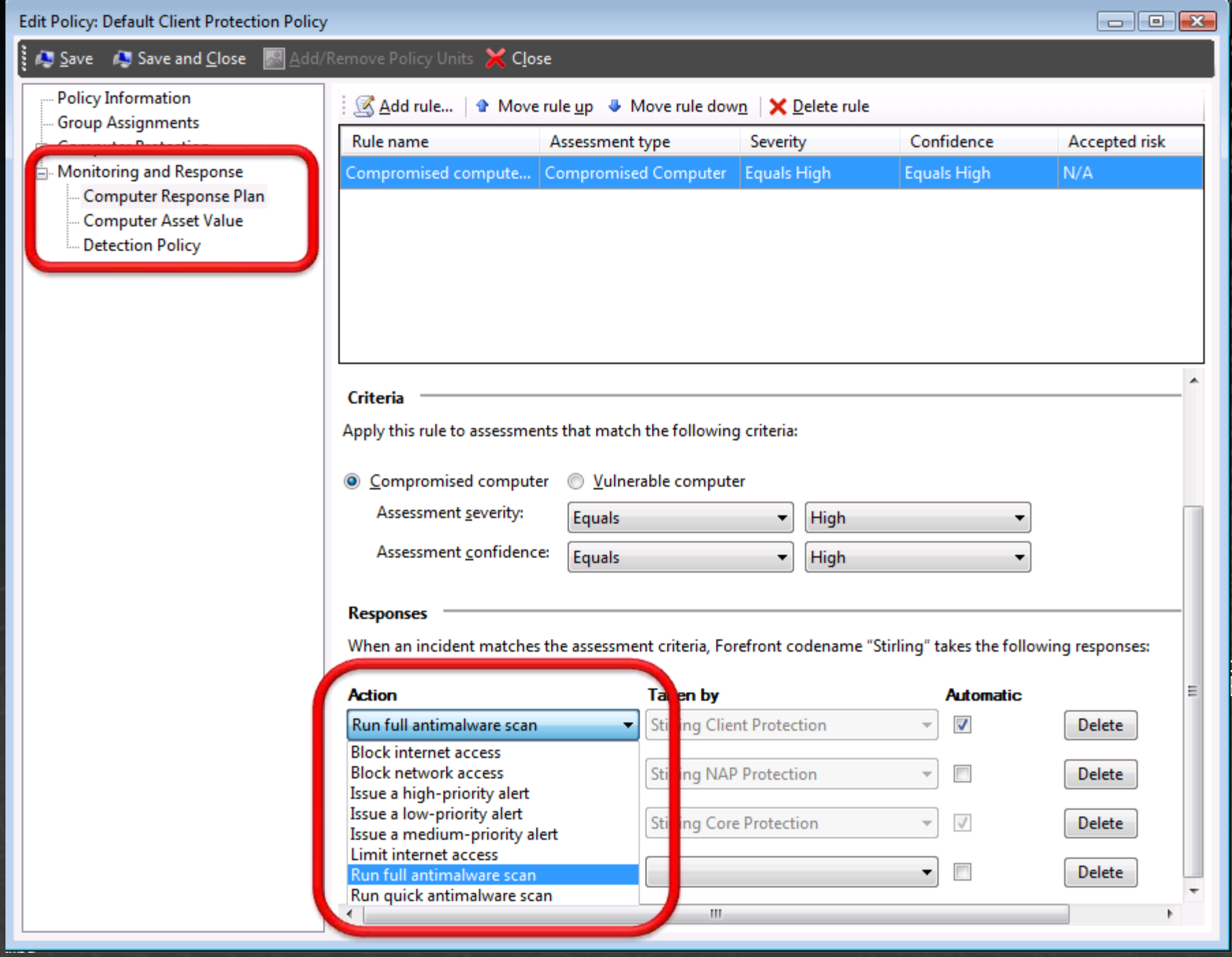
- 即時洞悉您單位的安全狀態
- 深入透徹的報表以及弱點評估
- 監控與修補資訊安全的能力

Microsoft®
Forefront™

全方位的防護

零時差攻擊防禦手法(現在)

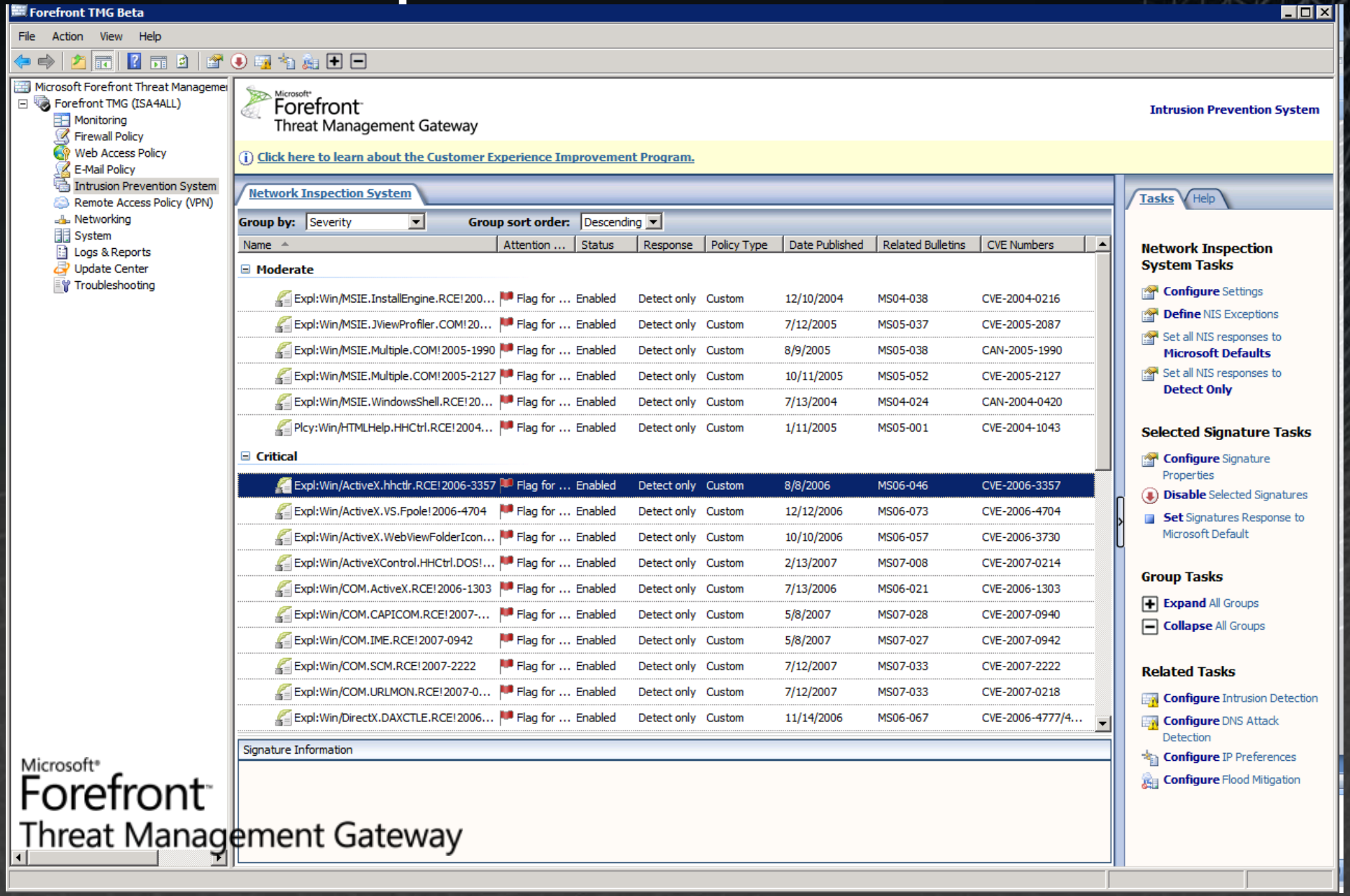
零時差攻擊防禦手法(Stirling)


Edit Policy: Default Client Protection Policy
Save
Save and Close
Add/Remove Policy Units
Close
Policy Information
Group Assignments
Monitoring and Response
Computer Response Plan
Computer Asset Value
Detection Policy
Add rule...
Move rule up
Move rule down
Delete rule
Rule name
Assessment type
Severity
Confidence
Accepted risk
Compromised compute...
Compromised Computer
Equals High
Equals High
N/A
Criteria
Apply this rule to assessments that match the following criteria:
Compromised computer
Vulnerable computer
Assessment severity:
Equals
High
Assessment confidence:
Equals
High
Responses
When an incident matches the assessment criteria, Forefront codename "Stirling" takes the following responses:
Action
Taken by
Automatic
Run full antimalware scan
Client Protection
Delete
Block internet access
Block network access
NAP Protection
Delete
Issue a high-priority alert
Issue a low-priority alert
Core Protection
Delete
Issue a medium-priority alert
Limit internet access
Delete
Run full antimalware scan
Run quick antimalware scan

Microsoft® Forefront™

動態回應機制

對未安裝patch電腦之防護



NIS 的運作模式

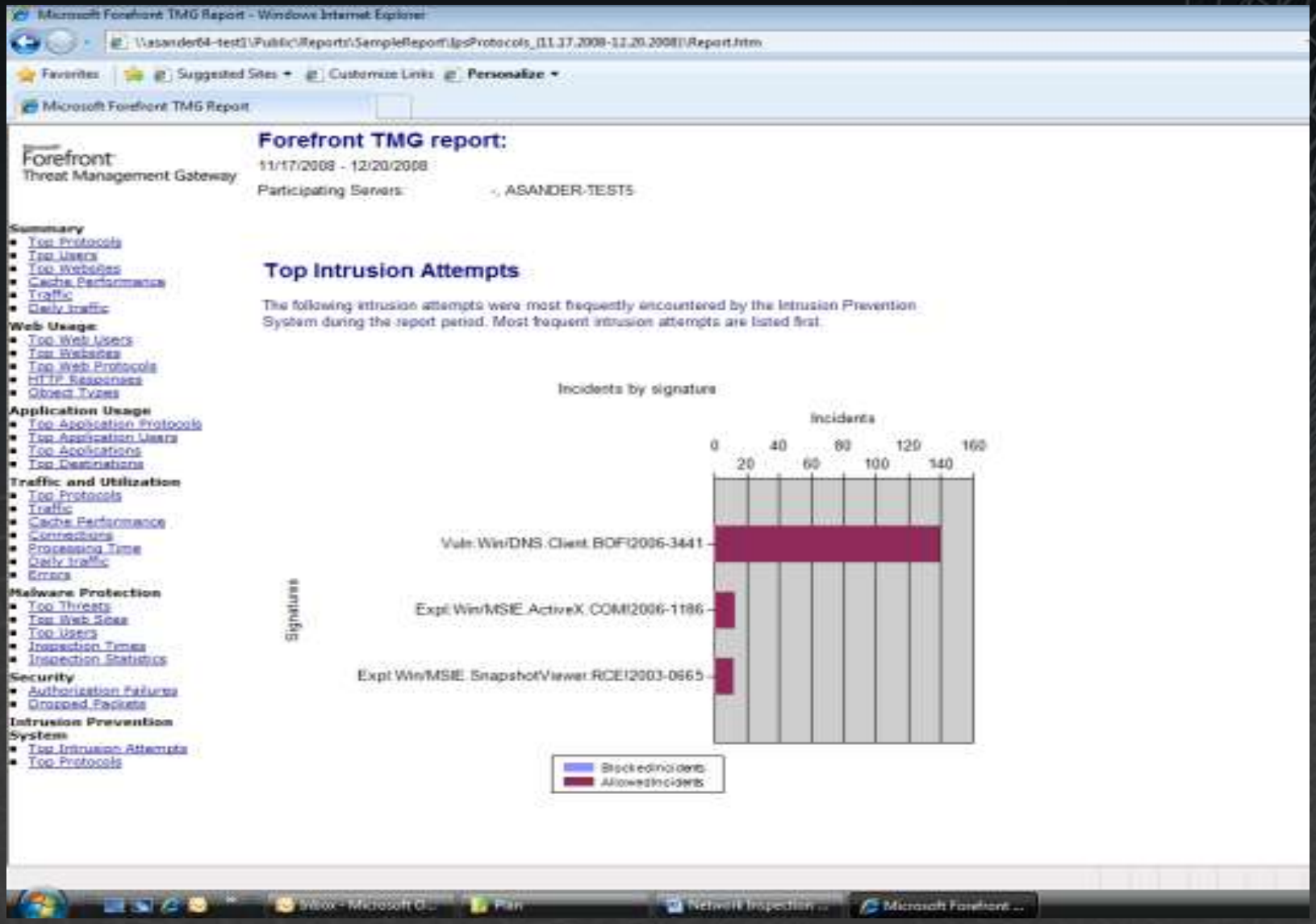
- 在閘道端與主機端，針對已知的 **弱點攻擊** 做出防禦
- NIS的定義更新與patch修正更新 **同時** 發布
- 避免在測試或佈署patch修正之前，遭受到可能的惡意攻擊，尤其是當...
  - Patch需要更完整的測試才能佈署
  - 使用者有安裝疑慮的時候

Microsoft® Forefront™

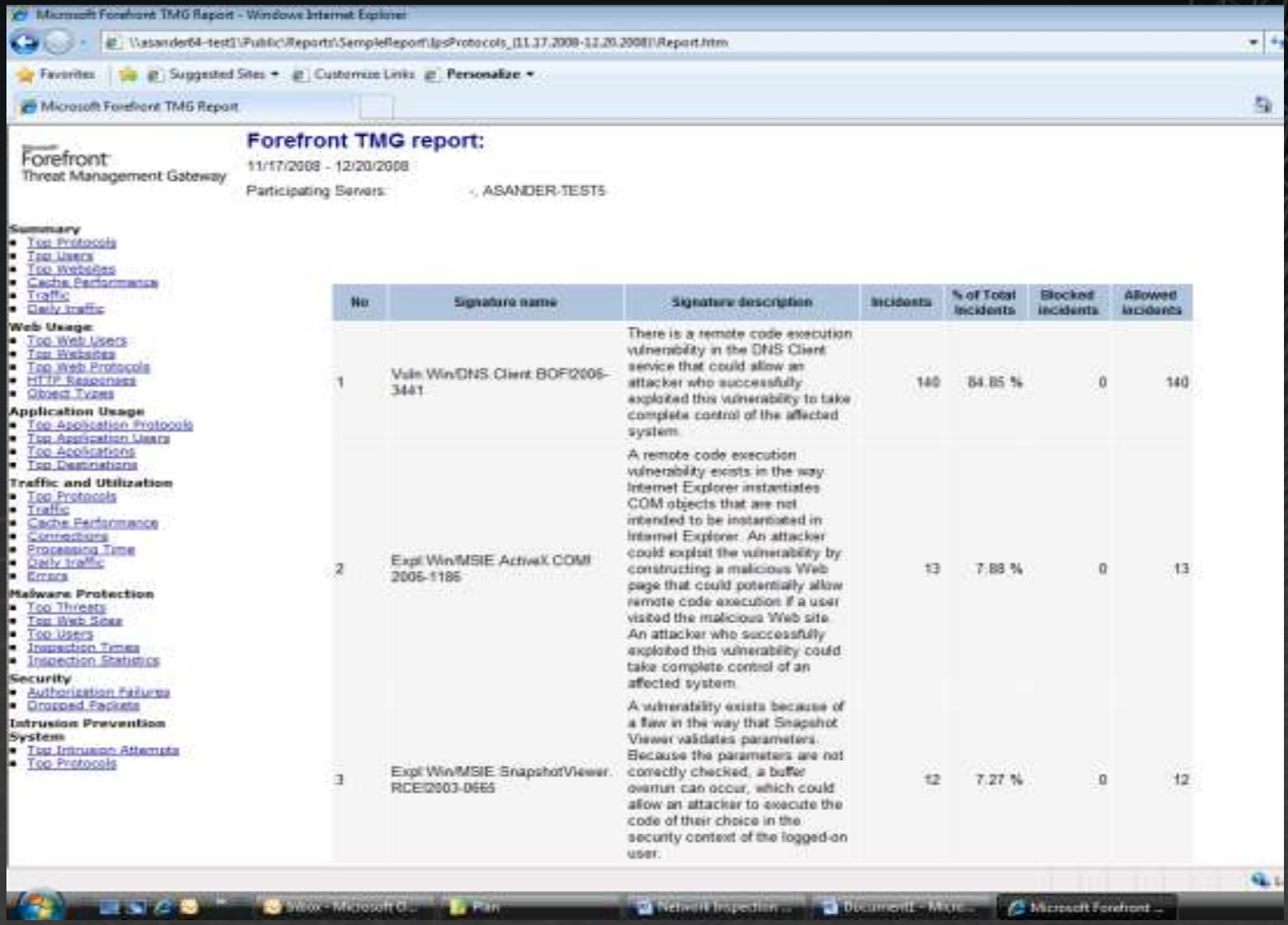
demo

Network Inspection System

Top Attacks Report

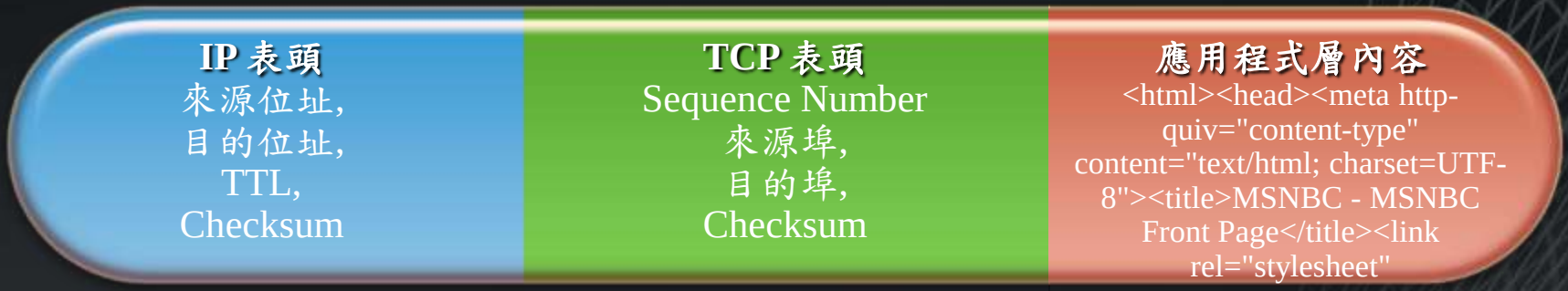


Top Attacks Report



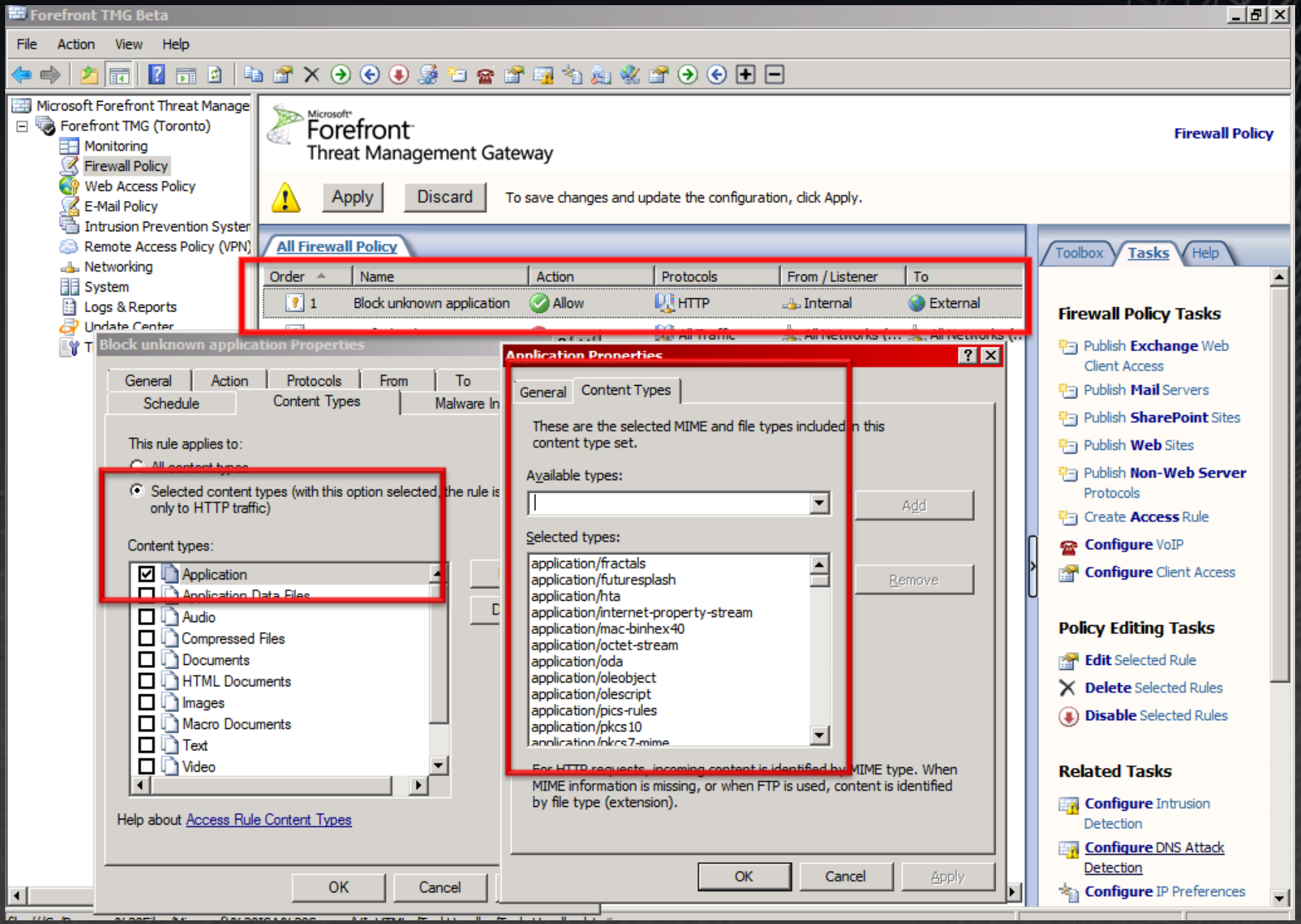
TMG: HTTP封包內容過濾

- 檢查封包表頭與應用程式層內容

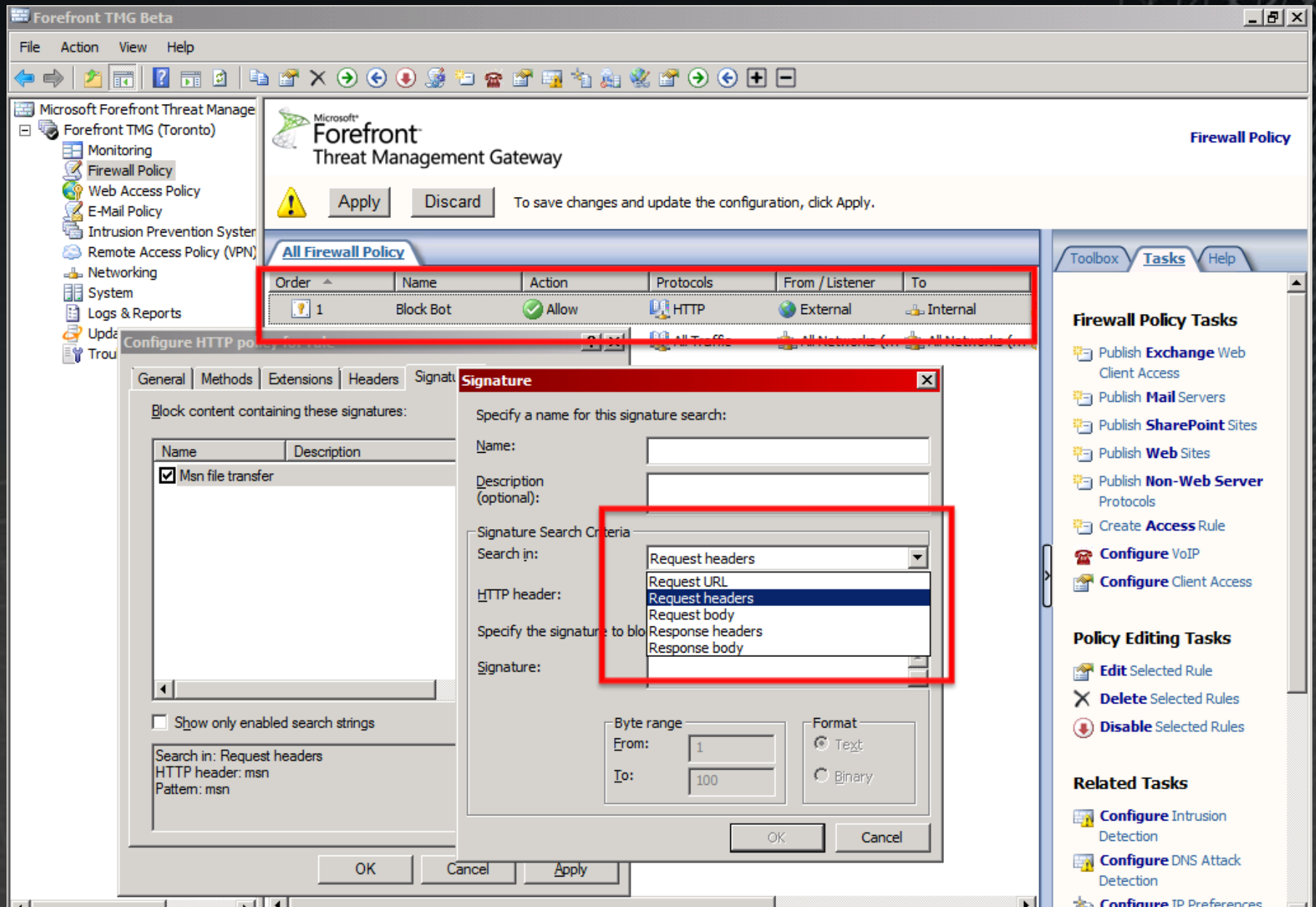


- 依內容決定傳送
  - 只有通過合法與允許的流量

HTTP封包內容過濾


Forefront TMG Beta
File Action View Help
Microsoft Forefront Threat Manage
Forefront TMG (Toronto)
Monitoring
Firewall Policy
Web Access Policy
E-Mail Policy
Intrusion Prevention Syster
Remote Access Policy (VPN)
Networking
System
Logs & Reports
Update Center
Microsoft Forefront Threat Management Gateway
Firewall Policy
Apply
Discard
To save changes and update the configuration, click Apply.
All Firewall Policy
Order
Name
Action
Protocols
From / Listener
To
1
Block unknown application
Allow
HTTP
Internal
External
Toolbox
Tasks
Help
Firewall Policy Tasks
Publish Exchange Web Client Access
Publish Mail Servers
Publish SharePoint Sites
Publish Web Sites
Publish Non-Web Server Protocols
Create Access Rule
Configure VoIP
Configure Client Access
Policy Editing Tasks
Edit Selected Rule
Delete Selected Rules
Disable Selected Rules
Related Tasks
Configure Intrusion Detection
Configure DNS Attack Detection
Configure IP Preferences
Block unknown application Properties
General
Action
Protocols
From
To
Schedule
Content Types
Malware In
This rule applies to:
Selected content types (with this option selected, the rule is only to HTTP traffic)
Content types:
Application
Audio
Compressed Files
Documents
HTML Documents
Images
Macro Documents
Text
Video
Help about Access Rule Content Types
OK
Cancel
Application Properties
General
Content Types
These are the selected MIME and file types included in this content type set.
Available types:
Add
Selected types:
Remove
application/fractals
application/futuresplash
application/hta
application/internet-property-stream
application/mac-binhex40
application/octet-stream
application/oda
application/oleobject
application/olescript
application/pics-rules
application/pkcs10
MIME information is missing, or when FTP is used, content is identified by file type (extension).
OK
Cancel
Apply

HTTP封包內容過濾


Forefront TMG Beta
File Action View Help
Microsoft Forefront Threat Manage
Forefront TMG (Toronto)
Monitoring
Firewall Policy
Web Access Policy
E-Mail Policy
Intrusion Prevention Syster
Remote Access Policy (VPN)
Networking
System
Logs & Reports
Microsoft Forefront Threat Management Gateway
Firewall Policy
Apply
Discard
To save changes and update the configuration, click Apply.
All Firewall Policy
Order
Name
Action
Protocols
From / Listener
To
1
Block Bot
Allow
HTTP
External
Internal
Configure HTTP policy for rule
General
Methods
Extensions
Headers
Signature
Block content containing these signatures:
Name
Description
Msn file transfer
Show only enabled search strings
Search in: Request headers
HTTP header: msn
Pattern: msn
OK
Cancel
Apply
Signature
Specify a name for this signature search:
Name:
Description (optional):
Signature Search Criteria
Search in:
Request headers
Request URL
Request headers
Request body
Response headers
Response body
HTTP header:
Specify the signature to blo
Signature:
Byte range
From:
1
To:
100
Format
Text
Binary
OK
Cancel
Toolbox
Tasks
Help
Firewall Policy Tasks
Publish Exchange Web Client Access
Publish Mail Servers
Publish SharePoint Sites
Publish Web Sites
Publish Non-Web Server Protocols
Create Access Rule
Configure VoIP
Configure Client Access
Policy Editing Tasks
Edit Selected Rule
Delete Selected Rules
Disable Selected Rules
Related Tasks
Configure Intrusion Detection
Configure DNS Attack Detection

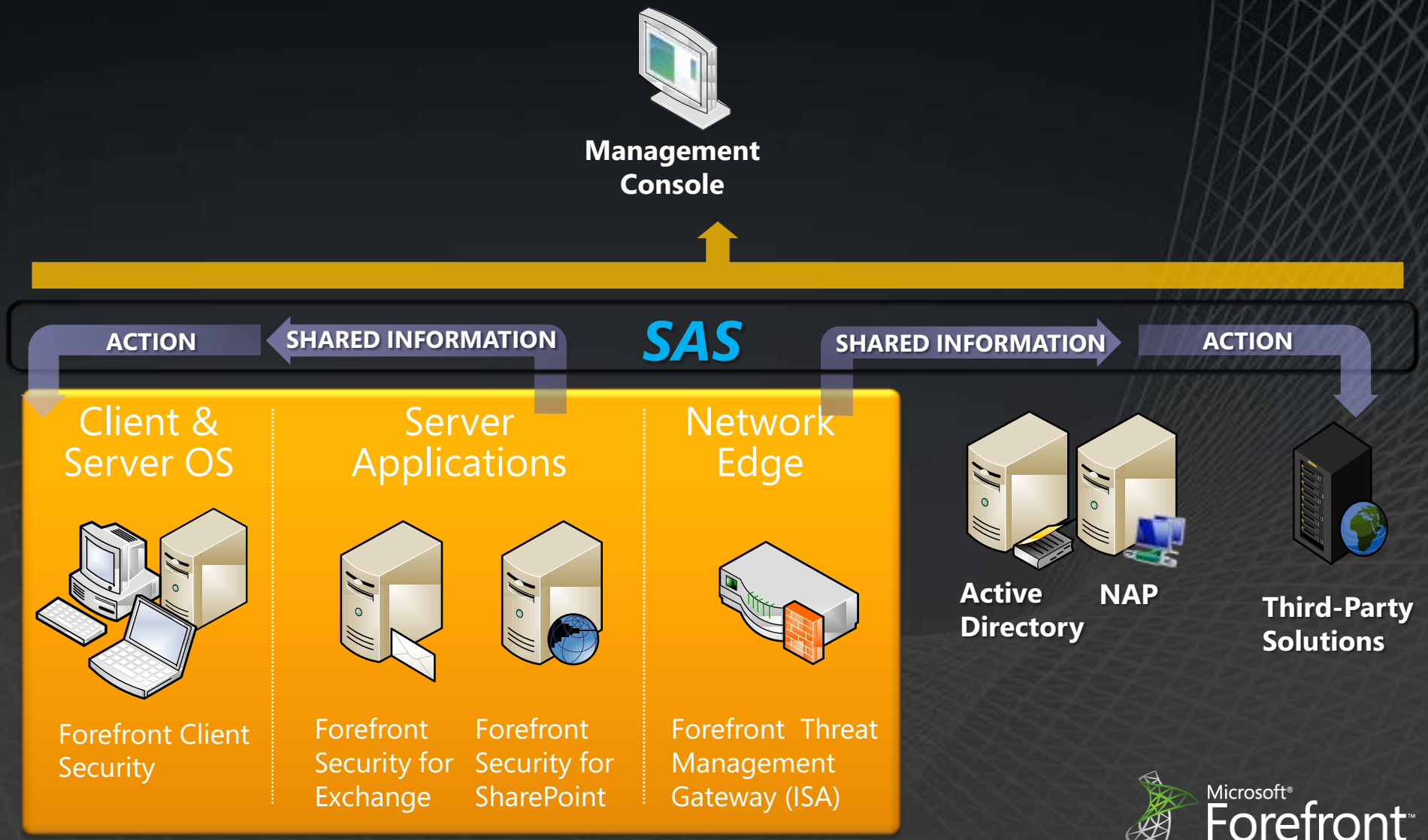
Microsoft® Forefront™

統合的管理

現今的安控管理界面

- 需要在不同管理控制台切換
  - 每種管控台有自己的管理風格
  - 彼此之間的資訊無法互通或整合
- 缺少整體評估的整合觀
- 難以釐清問題根本點

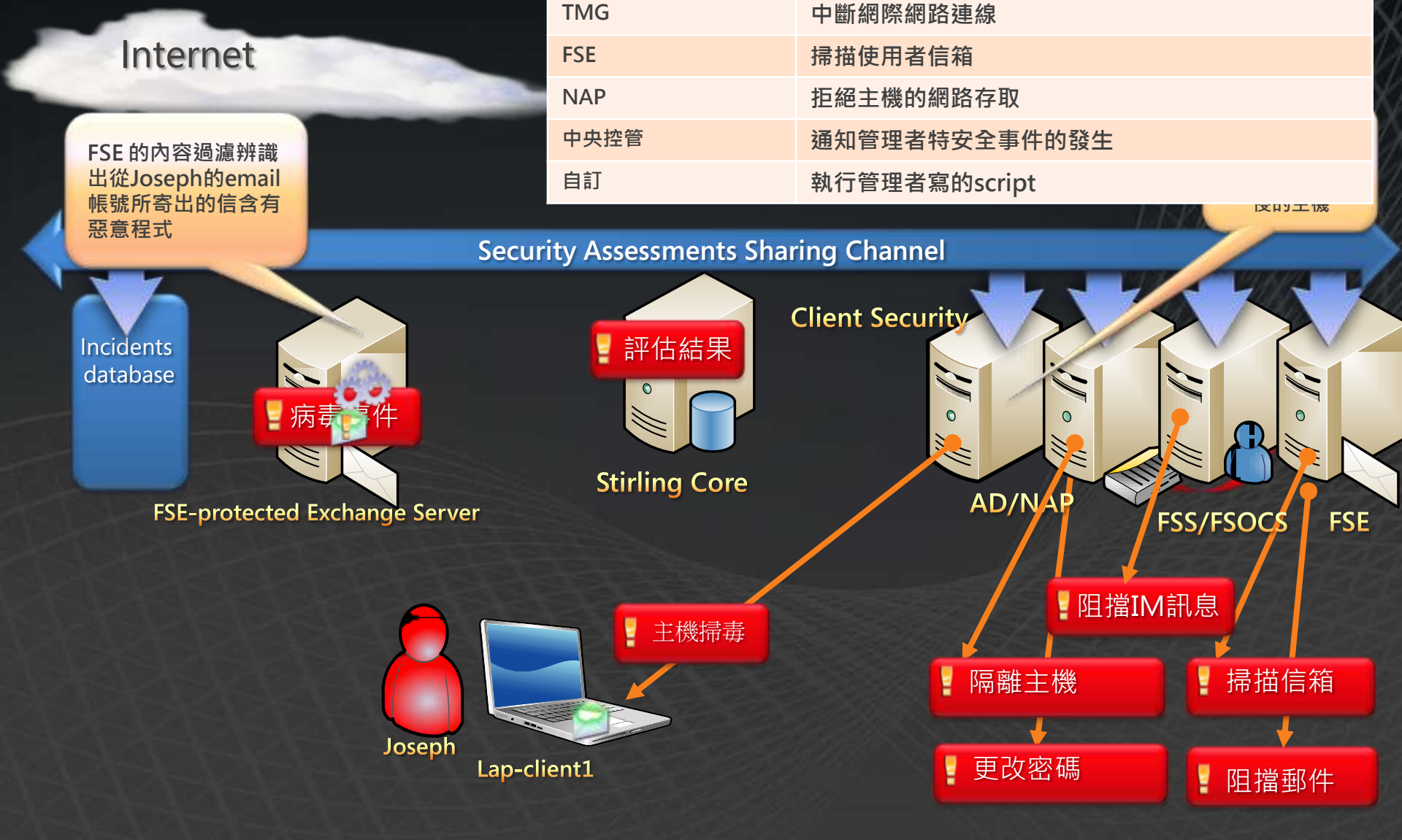
解決方案：Security Assessments Sharing



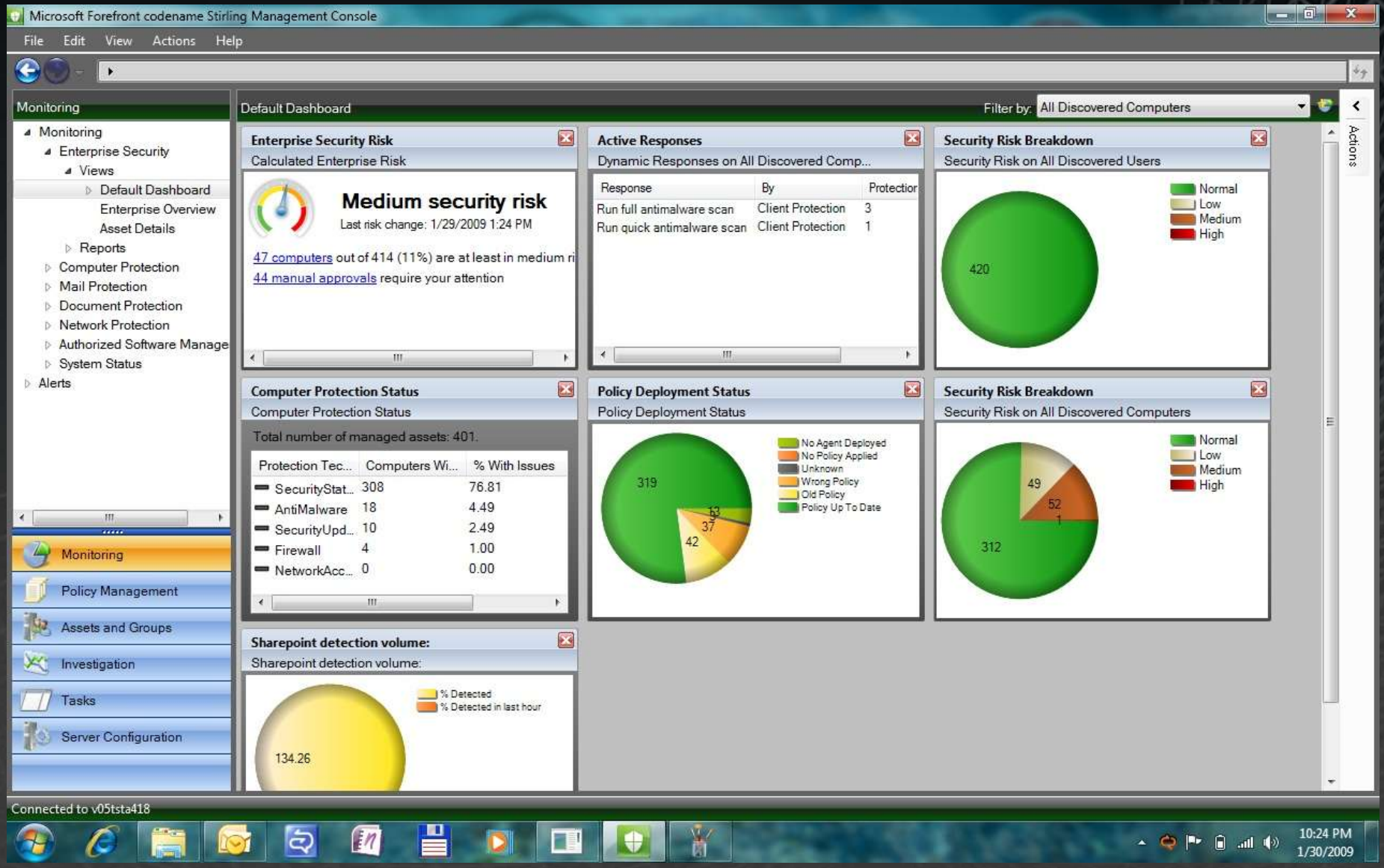
Microsoft® Forefront™

病毒郵件的防堵機制

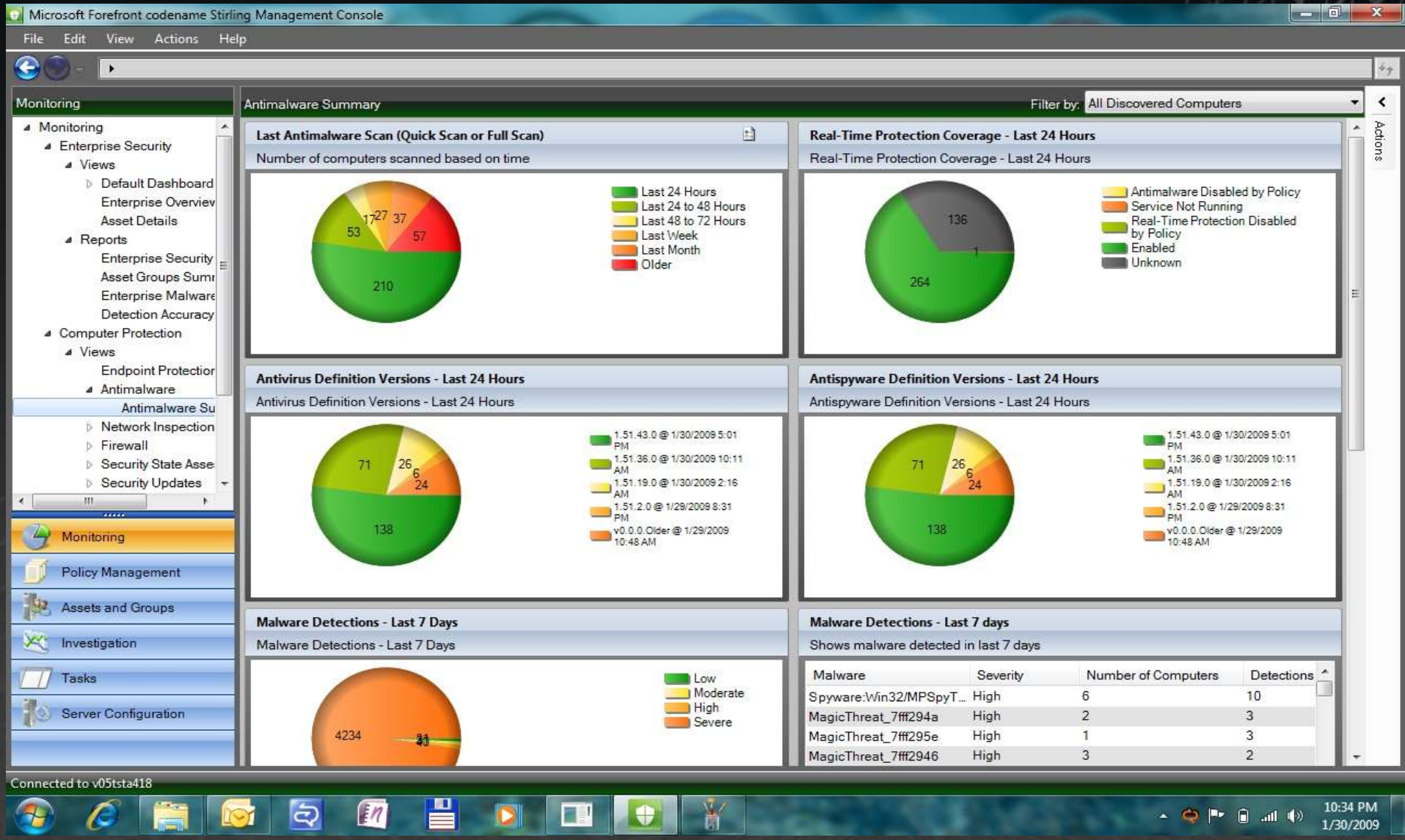
技術	回應
主機防惡意程式	Quick Scan/Full Scan
TMG	中斷網際網路連線
FSE	掃描使用者信箱
NAP	拒絕主機的網路存取
中央控管	通知管理者特安全事件的發生
自訂	執行管理者寫的script



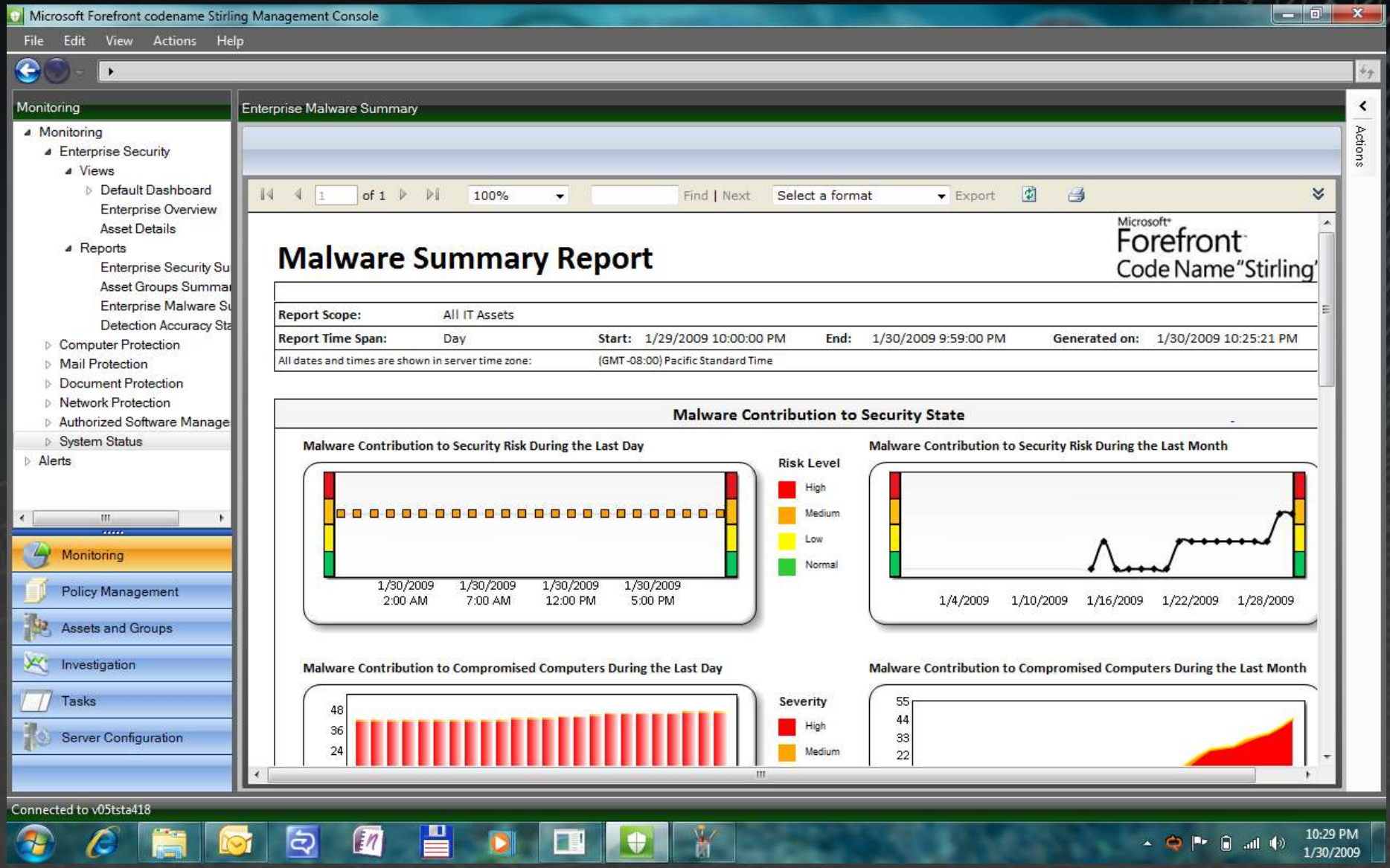
Stirling Dashboard



Stirling Antimalware Summary

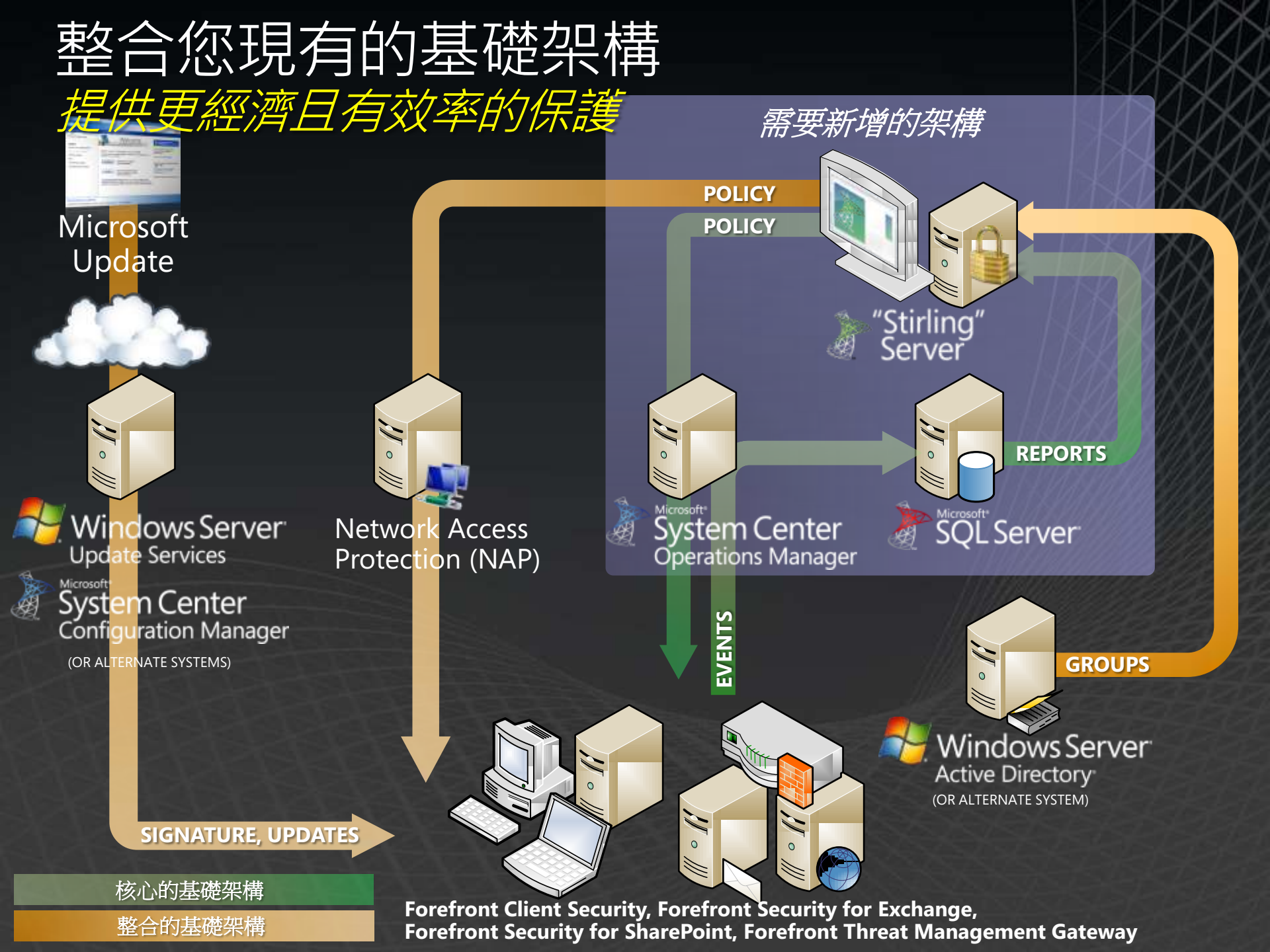


Stirling Reporting



整合您現有的基礎架構

提供更經濟且有效率的保護



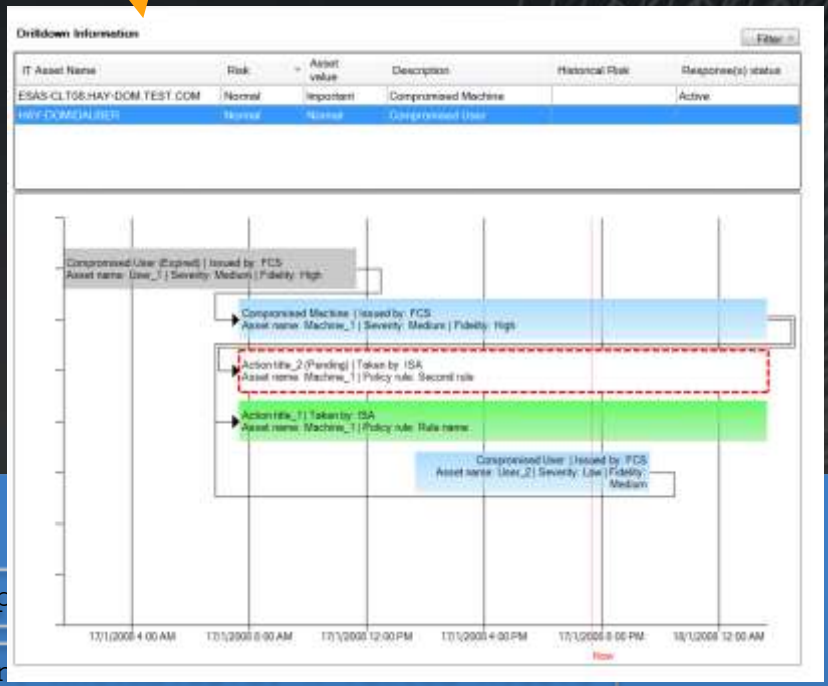
Microsoft®
Forefront™

安全問題的洞察力

從內到外評估目前的系統安全狀況

對於目前的系統安全狀況 " 一目了然"

- 對於所有的資產評估安全風險
  風險 = 安全狀態 X 資產重要度
- 從內而外涵蓋所有的防護
  Clients, Servers, Network



階層式的深入透視

- 可一層一層檢視報表與做出對應的管控
- 超過 60 種可自訂的管控 (參考下面)

Policy Deployment: User Status

Firewall: Port Excep

Security Assessment Check: Failed Remediation

Clien

Forefront for SharePoint: Malware Incidents

Forefront for Exchange: Quarantine Items

NAP: Computers with restricted network access

Security Updates: Approved and Missing

Client Antimalware: Protection Coverage

Authorized Software Management: Unknown Applications

自動化，加速管理者採取處置的時效

可遠端修正安全問題

警告提醒:

需要管理者注意的事件

- 可以透過 email, 呼叫, IM 或是管控界面中的警告來告知管理者
- 由受管理的資產自動回報的問題 (舉例: FSE 引擎更新失敗)
- 由 “Stirling” 系統所產生的問題 (舉例: 系統失效)
- 由 SAS 自動產生的警告 (舉例: 電腦受到入侵)

解決方案:

“Stirling” 可以自動去取消警告，當

- 系統自動解決問題之後
- 問題停止發生

管理者可以手動去執行特定的工作來解決警告

- 工作可以從管控畫面以及報表中來執行
- 超過50種以上的工作可以從遠端來執行

Install Missing Security Updates | Force Reboot | FSSP: Add user to block list | Turn on UAC

Trigger a quick scan | FSE: Update Signatures | NAP Evict a computer | Get Exchange Role

Block unknown application | FSSP: Delete Quarantine File | Get Public Folders | FSE Start Scan

安全問題的洞察力
深入了解問題

- 查看完整且詳細的報表，了解目前的安全狀態
- 調查並提出安全報表(Investigation view)
- 可就資產(Asset)深入了解問題發生時間點

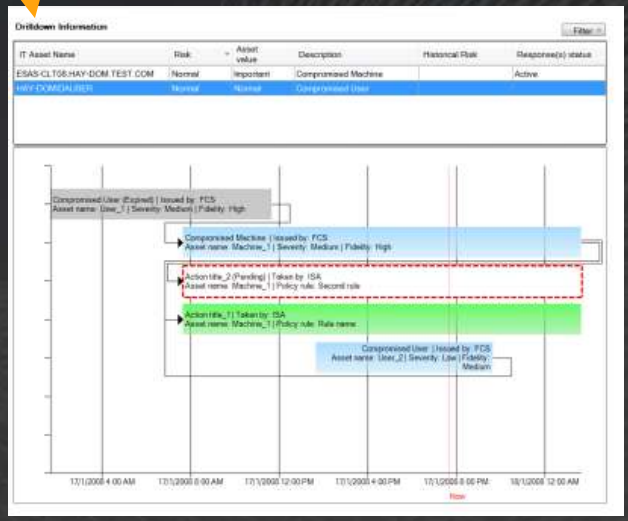
Microsoft® Forefront™

demo

Investigation View

風險管控儀表板

- 風險指數= 安全狀態 x 資產價值
- 透過Stirling的安控原則了解風險的所在
- 在相同的基準線上了解企業資產與安全狀態



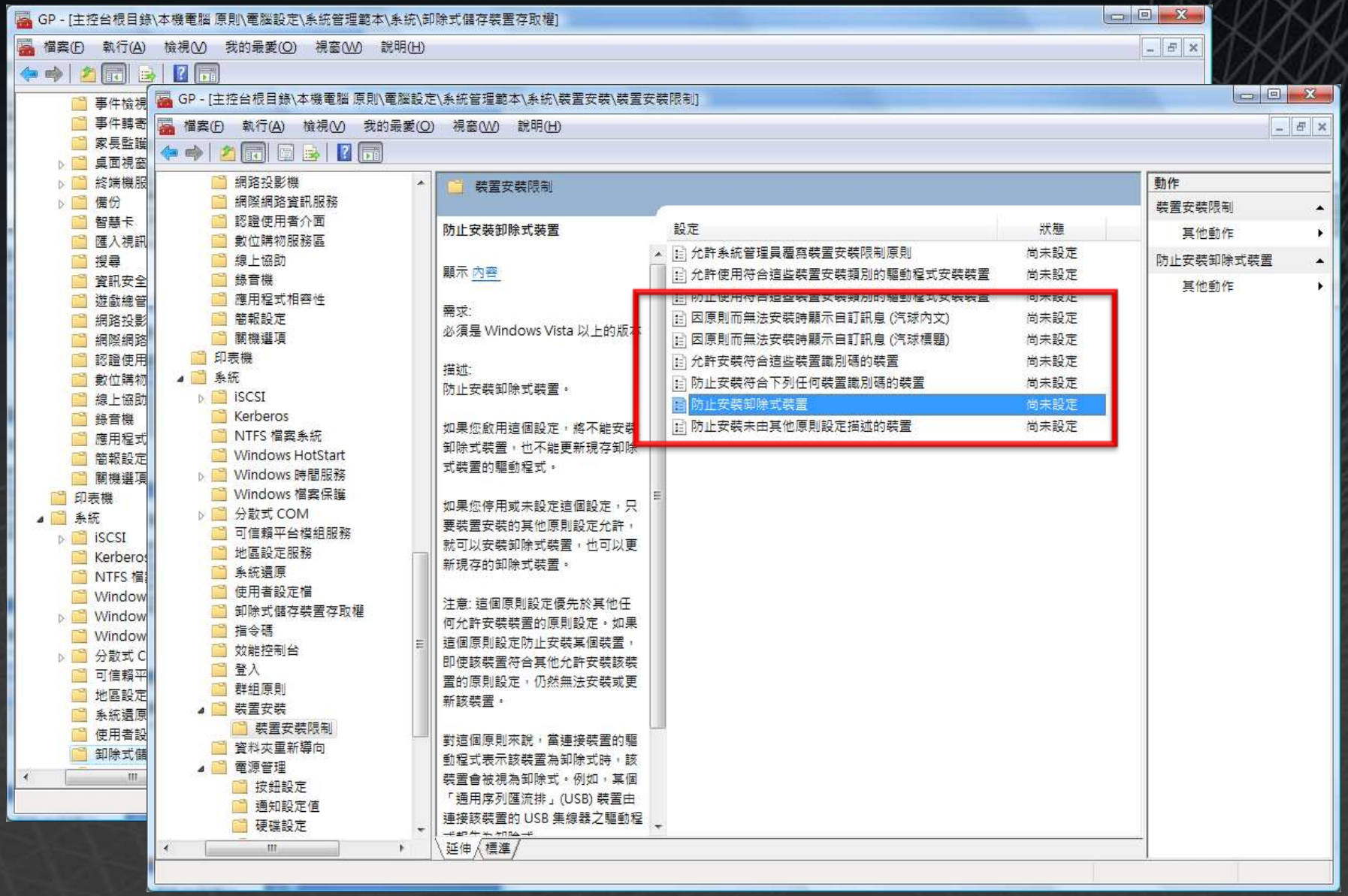
Microsoft® Forefront™

demo

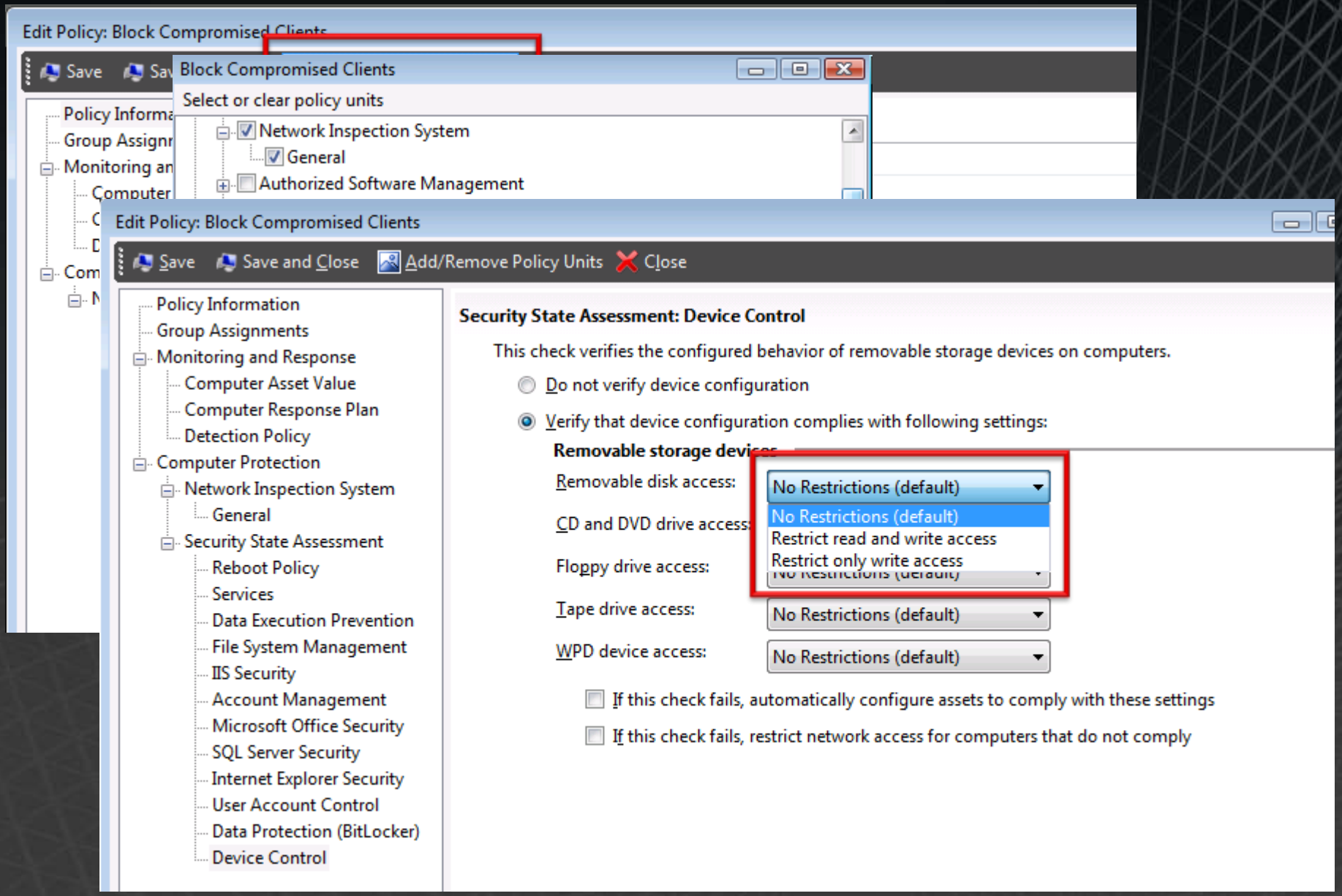
風險管控報告

安全狀態綜合評估
Security State Assessment(SSA)

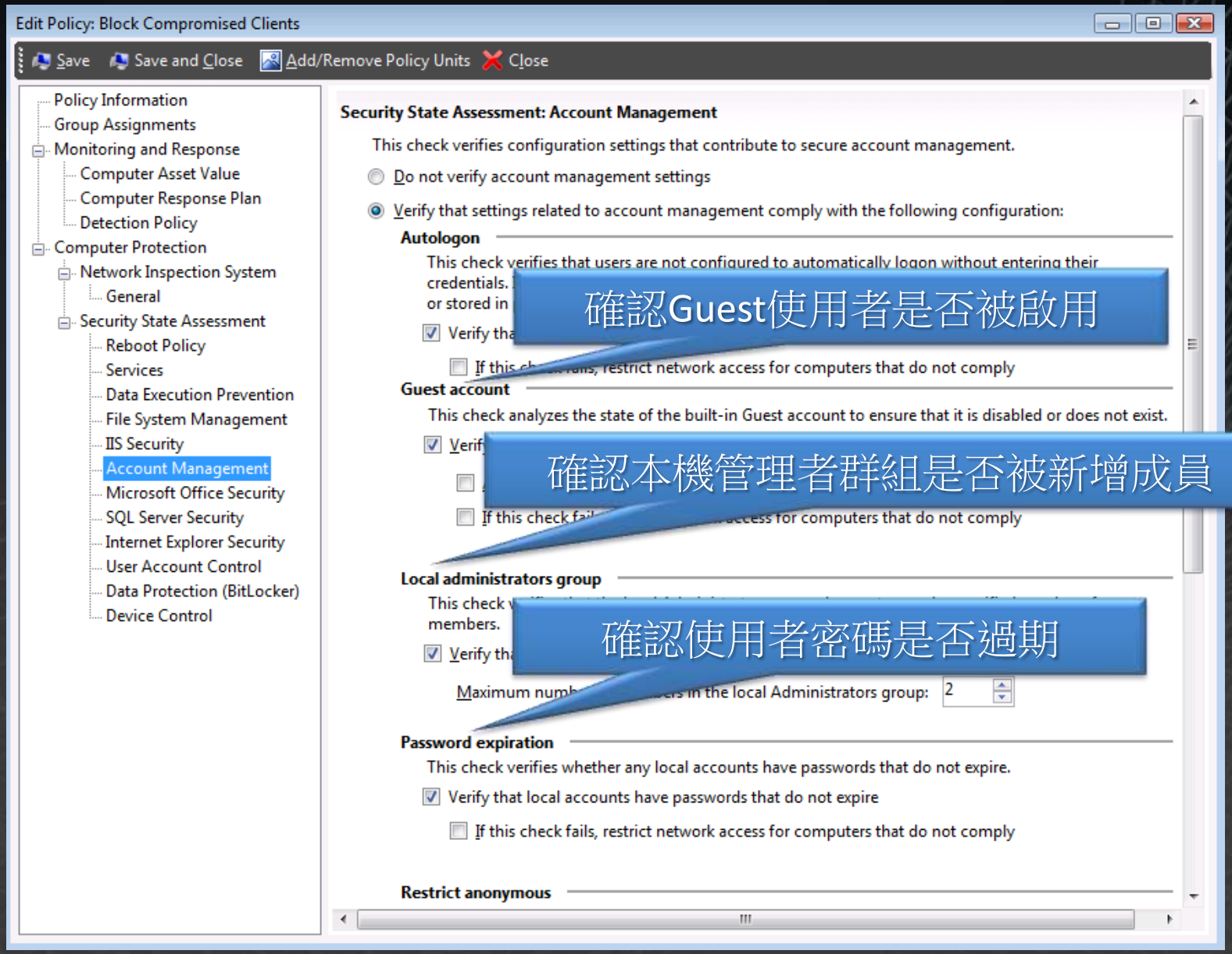
行動裝置的群組原則設定



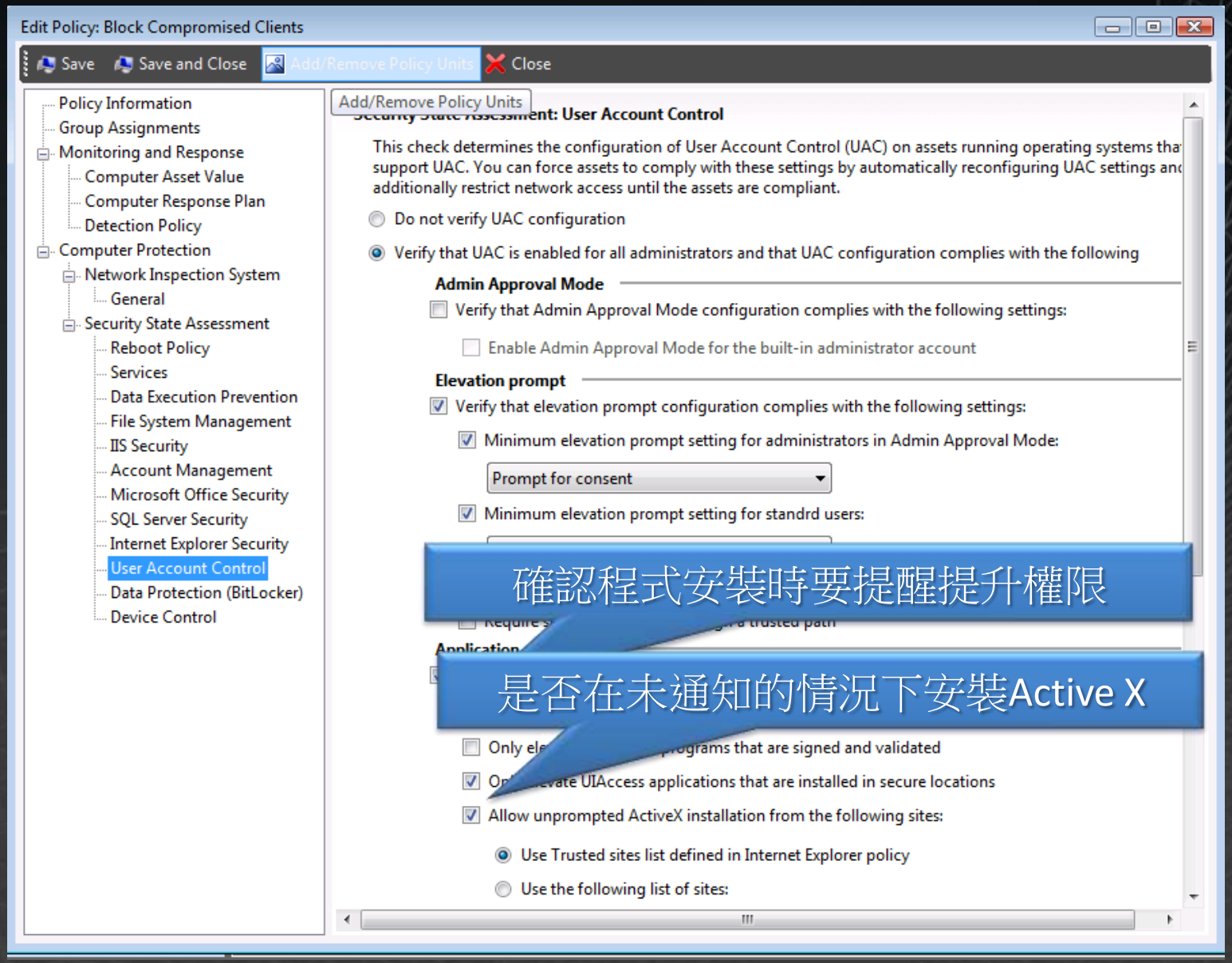
行動裝置的原則檢查


Edit Policy: Block Compromised Clients
Save
Block Compromised Clients
Select or clear policy units
Network Inspection System
General
Authorized Software Management
Edit Policy: Block Compromised Clients
Save
Save and Close
Add/Remove Policy Units
Close
Policy Information
Group Assignments
Monitoring and Response
Computer Asset Value
Computer Response Plan
Detection Policy
Computer Protection
Network Inspection System
General
Security State Assessment
Reboot Policy
Services
Data Execution Prevention
File System Management
IIS Security
Account Management
Microsoft Office Security
SQL Server Security
Internet Explorer Security
User Account Control
Data Protection (BitLocker)
Device Control
Security State Assessment: Device Control
This check verifies the configured behavior of removable storage devices on computers.
Do not verify device configuration
Verify that device configuration complies with following settings:
Removable storage devices
Removable disk access:
No Restrictions (default)
No Restrictions (default)
Restrict read and write access
Restrict only write access
CD and DVD drive access:
Floppy drive access:
Tape drive access:
No Restrictions (default)
WPD device access:
No Restrictions (default)
If this check fails, automatically configure assets to comply with these settings
If this check fails, restrict network access for computers that do not comply

使用者狀態的原則設定


Edit Policy: Block Compromised Clients
Save
Save and Close
Add/Remove Policy Units
Close
Policy Information
Group Assignments
Monitoring and Response
Computer Asset Value
Computer Response Plan
Detection Policy
Computer Protection
Network Inspection System
General
Security State Assessment
Reboot Policy
Services
Data Execution Prevention
File System Management
IIS Security
Account Management
Microsoft Office Security
SQL Server Security
Internet Explorer Security
User Account Control
Data Protection (BitLocker)
Device Control
Security State Assessment: Account Management
This check verifies configuration settings that contribute to secure account management.
Do not verify account management settings
Verify that settings related to account management comply with the following configuration:
Autologon
Guest account
This check analyzes the state of the built-in Guest account to ensure that it is disabled or does not exist.
Local administrators group
Maximum number of members in the local Administrators group:
2
Password expiration
This check verifies whether any local accounts have passwords that do not expire.
Verify that local accounts have passwords that do not expire
If this check fails, restrict network access for computers that do not comply
Restrict anonymous
確認Guest使用者是否被啟用
確認本機管理者群組是否被新增成員
確認使用者密碼是否過期

UAC的原則設定

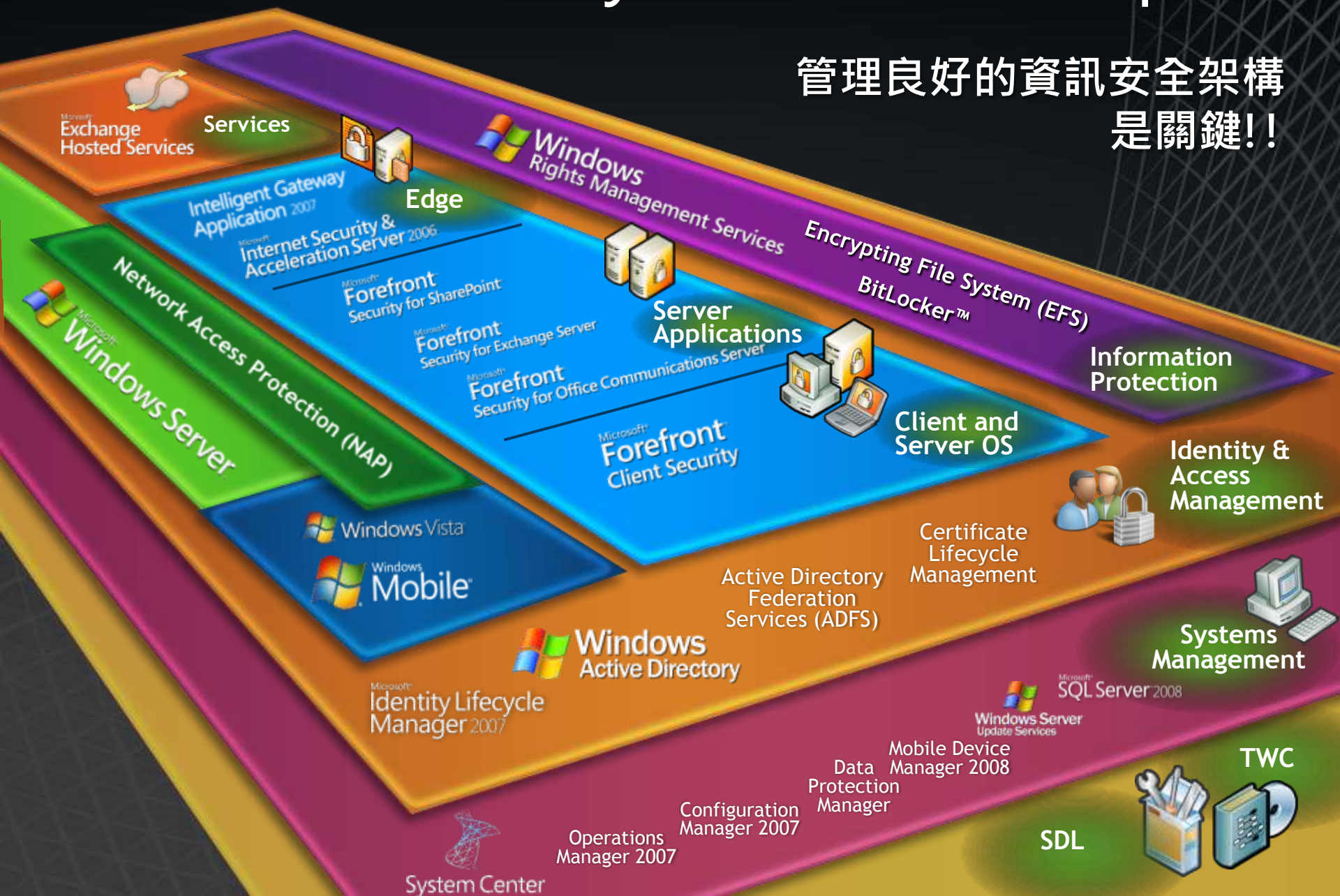

Edit Policy: Block Compromised Clients
Save
Save and Close
Add/Remove Policy Units
Close
Policy Information
Group Assignments
Monitoring and Response
Computer Asset Value
Computer Response Plan
Detection Policy
Computer Protection
Network Inspection System
General
Security State Assessment
Reboot Policy
Services
Data Execution Prevention
File System Management
IIS Security
Account Management
Microsoft Office Security
SQL Server Security
Internet Explorer Security
User Account Control
Data Protection (BitLocker)
Device Control
Add/Remove Policy Units
User Account Control
This check determines the configuration of User Account Control (UAC) on assets running operating systems tha
support UAC. You can force assets to comply with these settings by automatically reconfiguring UAC settings an
additionally restrict network access until the assets are compliant.
Do not verify UAC configuration
Verify that UAC is enabled for all administrators and that UAC configuration complies with the following
Admin Approval Mode
Verify that Admin Approval Mode configuration complies with the following settings:
Enable Admin Approval Mode for the built-in administrator account
Elevation prompt
Verify that elevation prompt configuration complies with the following settings:
Minimum elevation prompt setting for administrators in Admin Approval Mode:
Prompt for consent
Minimum elevation prompt setting for standrd users:
確認程式安裝時要提醒提升權限
是否在未通知的情況下安裝Active X
Allow unprompted ActiveX installation from the following sites:
Use Trusted sites list defined in Internet Explorer policy
Use the following list of sites:

Microsoft® Forefront™

總結

Microsoft Security: Defense In Depth

管理良好的資訊安全架構
是關鍵!!



總結

Stirling：一套綜觀端點防護、應用伺服器防護、閘道防護的完整企業營運安全性產品，可用來協助企業經由深度整合與簡化管理的方式取得更完善的防護。

- 以**管理**資安為本質，並非單純是資安產品 (No Management, No Security)
- 動態協同回應機制
- 統合的管理介面
- 以資產(Asset)為基礎的風險評估
- 條理清楚並連貫的訊息報表

Microsoft®
Forefront™

Q&A

Microsoft®

Your potential. Our passion.™