



# 連動防禦、制敵機先 — 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



Trojan



Virus



Worms

# 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



Trojan



Virus



Worms



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



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™

閘道防護



Microsoft®  
**Forefront™**  
 Threat Management Gateway  
 Microsoft®  
**Forefront™**  
 Unified Access Gateway

Action

Action

# 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 development

GAPA包含了語言與分析引擎，可以在網路串流中運作

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

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

demonstrates that such development is possible and allows online analysis of protocol 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.

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)





- Policy Information
- Group Assignments
- Monitoring and Response
  - Computer Response Plan
  - Computer Asset Value
  - Detection Policy

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	Stirling Client Protection	<input checked="" type="checkbox"/>	Delete
Block internet access	Stirling NAP Protection	<input type="checkbox"/>	Delete
Issue a high-priority alert	Stirling Core Protection	<input checked="" type="checkbox"/>	Delete
Issue a low-priority alert		<input type="checkbox"/>	Delete
Issue a medium-priority alert		<input type="checkbox"/>	Delete
Limit internet access		<input type="checkbox"/>	Delete
Run full antimalware scan		<input type="checkbox"/>	Delete
Run quick antimalware scan		<input type="checkbox"/>	Delete



Microsoft®  
Forefront™

*demo*

---

動態回應機制

# 對未安裝patch電腦之防護

Microsoft Forefront Threat Management Gateway

Intrusion Prevention System

[Click here to learn about the Customer Experience Improvement Program.](#)

### Network Inspection System

Group by: Severity Group sort order: Descending

Name	Attention	Status	Response	Policy Type	Date Published	Related Bulletins	CVE Numbers
<b>Moderate</b>							
Expl:Win/MSIE.InstallEngine.RCE!200...	Flag for ...	Enabled	Detect only	Custom	12/10/2004	MS04-038	CVE-2004-0216
Expl:Win/MSIE.JViewProfler.COM!20...	Flag for ...	Enabled	Detect only	Custom	7/12/2005	MS05-037	CVE-2005-2087
Expl:Win/MSIE.Multiple.COM!2005-1990	Flag for ...	Enabled	Detect only	Custom	8/9/2005	MS05-038	CAN-2005-1990
Expl:Win/MSIE.Multiple.COM!2005-2127	Flag for ...	Enabled	Detect only	Custom	10/11/2005	MS05-052	CVE-2005-2127
Expl:Win/MSIE.WindowsShell.RCE!20...	Flag for ...	Enabled	Detect only	Custom	7/13/2004	MS04-024	CAN-2004-0420
Plcy:Win/HTMLHelp.HHCtrl.RCE!2004...	Flag for ...	Enabled	Detect only	Custom	1/11/2005	MS05-001	CVE-2004-1043
<b>Critical</b>							
Expl:Win/ActiveX.hhctr.RCE!2006-3357	Flag for ...	Enabled	Detect only	Custom	8/8/2006	MS06-046	CVE-2006-3357
Expl:Win/ActiveX.VS.Fpole!2006-4704	Flag for ...	Enabled	Detect only	Custom	12/12/2006	MS06-073	CVE-2006-4704
Expl:Win/ActiveX.WebViewFolderIcon...	Flag for ...	Enabled	Detect only	Custom	10/10/2006	MS06-057	CVE-2006-3730
Expl:Win/ActiveXControl.HHCtrl.DOS!...	Flag for ...	Enabled	Detect only	Custom	2/13/2007	MS07-008	CVE-2007-0214
Expl:Win/COM.ActiveX.RCE!2006-1303	Flag for ...	Enabled	Detect only	Custom	7/13/2006	MS06-021	CVE-2006-1303
Expl:Win/COM.CAPICOM.RCE!2007-...	Flag for ...	Enabled	Detect only	Custom	5/8/2007	MS07-028	CVE-2007-0940
Expl:Win/COM.IME.RCE!2007-0942	Flag for ...	Enabled	Detect only	Custom	5/8/2007	MS07-027	CVE-2007-0942
Expl:Win/COM.SCM.RCE!2007-2222	Flag for ...	Enabled	Detect only	Custom	7/12/2007	MS07-033	CVE-2007-2222
Expl:Win/COM.URLMON.RCE!2007-0...	Flag for ...	Enabled	Detect only	Custom	7/12/2007	MS07-033	CVE-2007-0218
Expl:Win/DirectX.DAXCTLE.RCE!2006...	Flag for ...	Enabled	Detect only	Custom	11/14/2006	MS06-067	CVE-2006-4777/4...

Signature Information

Microsoft Forefront Threat Management Gateway

### Network Inspection System Tasks

- Configure Settings
- Define NIS Exceptions
- Set all NIS responses to Microsoft Defaults
- Set all NIS responses to Detect Only

### Selected Signature Tasks

- Configure Signature Properties
- Disable Selected Signatures
- Set Signatures Response to Microsoft Default

### Group Tasks

- Expand All Groups
- Collapse All Groups

### Related Tasks

- Configure Intrusion Detection
- Configure DNS Attack Detection
- Configure IP Preferences
- Configure Flood Mitigation

# 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™

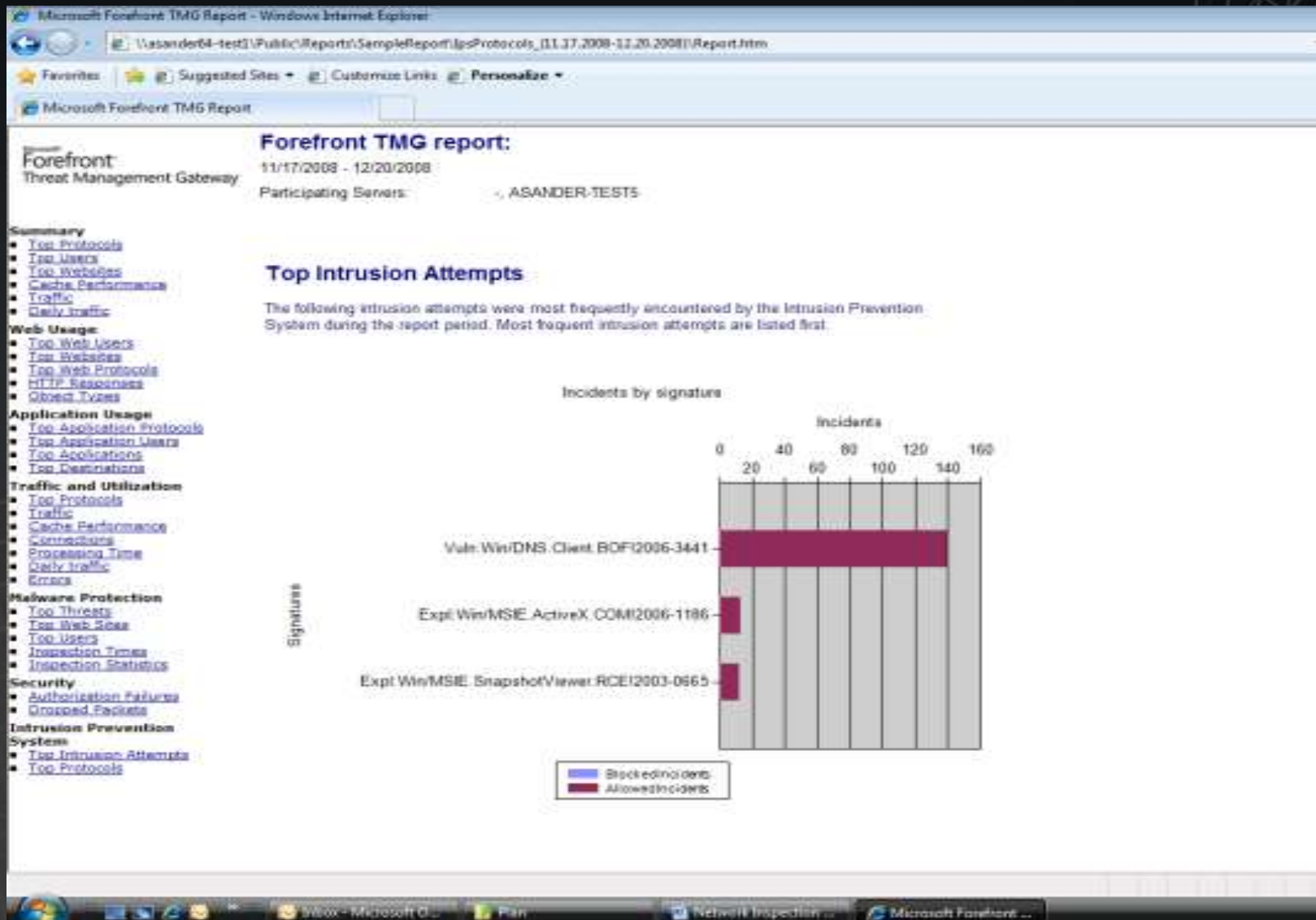
*demo*

---

Network Inspection System

---

# Top Attacks Report



# Top Attacks Report

Microsoft Forefront TMG Report - Windows Internet Explorer  
Vasander64-test1\Public\Reports\SampleReport\IpsProtocols\_11.17.2008-12.20.2008\Report.htm

Microsoft Forefront TMG Report

**Forefront**  
Threat Management Gateway  
11/17/2008 - 12/20/2008  
Participating Servers: ASANDER-TESTS

**Summary**

- Top Protocols
- Top Users
- Top Websites
- Cache Performance
- Traffic
- QoS Traffic

**Web Usage**

- Top Web Users
- Top Websites
- Top Web Protocols
- HTTP Responses
- Object Types

**Application Usage**

- Top Application Protocols
- Top Application Users
- Top Applications
- Top Destinations

**Traffic and Utilization**

- Top Protocols
- Traffic
- Cache Performance
- Connections
- Processing Time
- QoS Traffic
- Errors

**Malware Protection**

- Top Threats
- Top Web Sites
- Top Users
- Inspection Times
- Inspection Statistics

**Security**

- Authorization Failures
- Quarantined Objects

**Intrusion Prevention System**

- Top Intrusion Attempts
- Top Protocols

No	Signature name	Signature description	Incidents	% of Total Incidents	Blocked Incidents	Allowed Incidents
1	Vuln Win/DNS Client BOF(2005-3441)	There is a remote code execution vulnerability in the DNS Client service that could allow an attacker who successfully exploited this vulnerability to take complete control of the affected system.	140	84.85 %	0	140
2	Exploit Win/MSIE ActiveX COM(2005-1195)	A remote code execution vulnerability exists in the way Internet Explorer instantiates COM objects that are not intended to be instantiated in Internet Explorer. An attacker could exploit the vulnerability by constructing a malicious Web page that could potentially allow remote code execution if a user visited the malicious Web site. An attacker who successfully exploited this vulnerability could take complete control of an affected system.	13	7.88 %	0	13
3	Exploit Win/MSIE Snapshot Viewer RCE(2003-0565)	A vulnerability exists because of a flaw in the way that Snapshot Viewer validates parameters. Because the parameters are not correctly checked, a buffer overrun can occur, which could allow an attacker to execute the code of their choice in the security context of the logged-on user.	12	7.27 %	0	12

Taskbar: www - Microsoft C... | Pan | Network Inspection... | DocumentL - Micro... | Microsoft Forefront...

# 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

The screenshot displays the Microsoft Forefront Threat Management Gateway (TMG) Beta interface. The main window shows the 'Firewall Policy' configuration for 'All Firewall Policy'. A table lists the policy rules:

Order	Name	Action	Protocols	From / Listener	To
1	Block unknown application	Allow	HTTP	Internal	External

The 'Block unknown application Properties' dialog box is open, showing the 'Content Types' tab. The 'Selected content types (with this option selected the rule is only to HTTP traffic)' radio button is selected. The 'Content types' list includes:

- Application
- Application Data Files
- Audio
- Compressed Files
- Documents
- HTML Documents
- Images
- Macro Documents
- Text
- Video

The 'Application Properties' dialog box is also open, showing the 'Content Types' tab. The 'Available types' dropdown is empty. The 'Selected types' list includes:

- 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
- application/pkcs7-mime

The 'Firewall Policy Tasks' panel on the right includes tasks such as 'Publish Exchange Web Client Access', 'Publish Mail Servers', 'Publish SharePoint Sites', 'Publish Web Sites', 'Publish Non-Web Server Protocols', 'Create Access Rule', 'Configure VoIP', and 'Configure Client Access'. The 'Policy Editing Tasks' panel includes 'Edit Selected Rule', 'Delete Selected Rules', and 'Disable Selected Rules'. The 'Related Tasks' panel includes 'Configure Intrusion Detection', 'Configure DNS Attack Detection', and 'Configure IP Preferences'.

# HTTP封包內容過濾

The screenshot displays the Microsoft Forefront Threat Management Gateway (TMG) Firewall Policy configuration interface. The main window shows a table of firewall rules, with one rule 'Block Bot' selected. A 'Signature' dialog box is open, showing search criteria for 'Request headers'.

**Firewall Policy Table:**

Order	Name	Action	Protocols	From / Listener	To
1	Block Bot	Allow	HTTP	External	Internal

**Signature Dialog Box:**

Block content containing these signatures:

Name	Description
<input checked="" type="checkbox"/> Msn file transfer	

Specify a name for this signature search:

Name:

Description (optional):

Signature Search Criteria

Search in: **Request headers**

HTTP header:

Specify the signature to block:

Signature:

Byte range

From:

To:

Format

Text

Binary

Buttons: OK, Cancel, Apply



Microsoft®  
Forefront™

# 統合的管理

# 現今的安控管理界面

## 端點防護

控制台



報表中心



## 應用伺服器防護

控制台



報表中心



## 閘道防護

控制台



報表中心



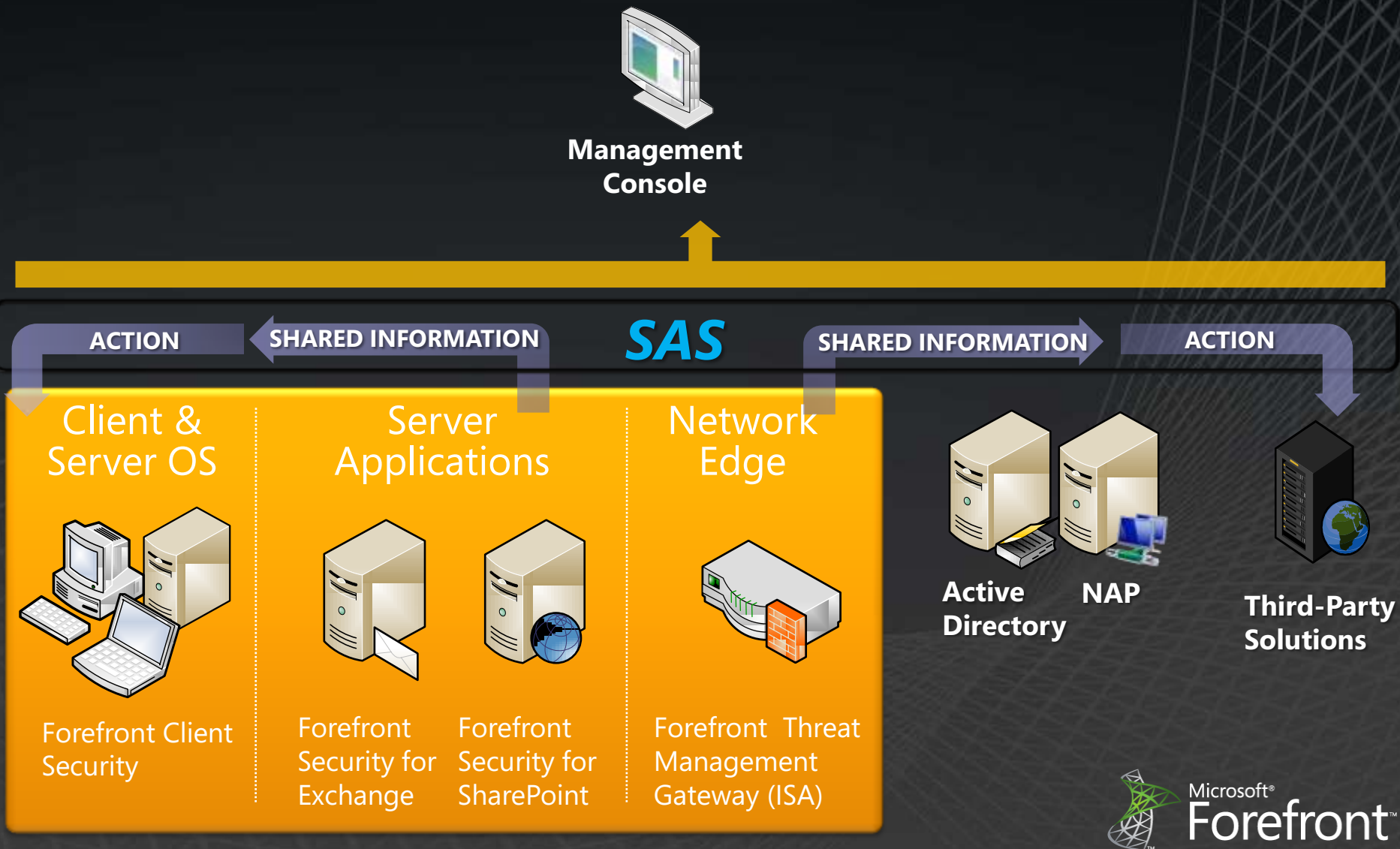
## 弱點評估

控制台



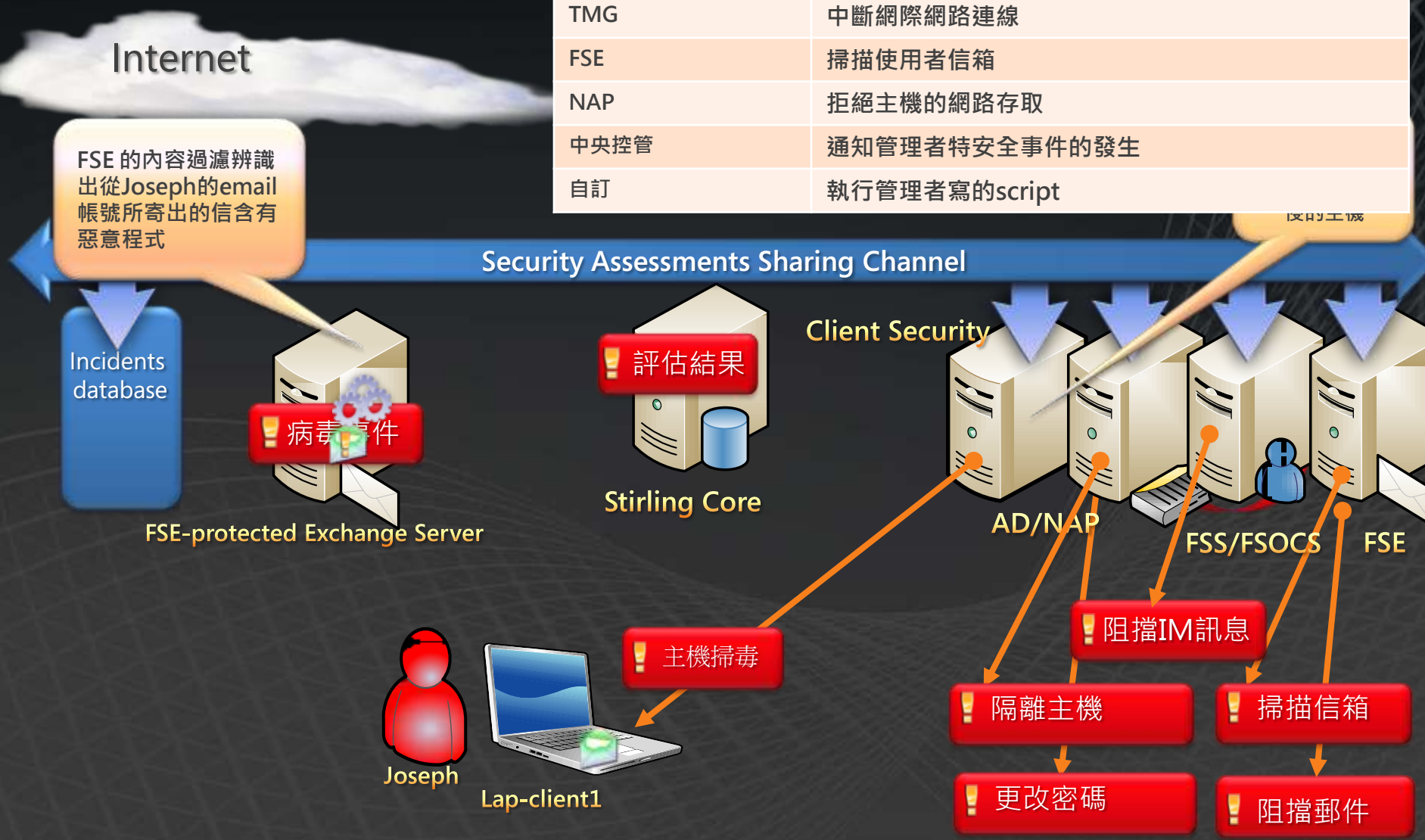
- ▶ 需要在不同管理控制台切換
- ▶ 每種管控台有自己的管理風格
- ▶ 彼此之間的資訊無法互通或整合
- ▶ 缺少整體評估的整合觀
- ▶ 難以釐清問題根本點

# 解決方案：Security Assessments Sharing



# 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



反的工機

# Stirling Dashboard

Microsoft Forefront codename Stirling Management Console

File Edit View Actions Help

Monitoring


- Monitoring
  - Enterprise Security
    - Views
      - Default Dashboard
      - Enterprise Overview
      - Asset Details
    - Reports
      - Computer Protection
      - Mail Protection
      - Document Protection
      - Network Protection
      - Authorized Software Manage...
      - System Status
    - Alerts

Default Dashboard

Filter by: All Discovered Computers

### Enterprise Security Risk

Calculated Enterprise Risk



**Medium security risk**  
Last risk change: 1/29/2009 1:24 PM

[47 computers](#) out of 414 (11%) are at least in medium risk  
[44 manual approvals](#) require your attention

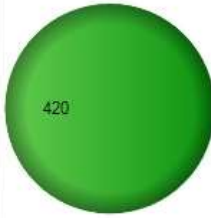
### Active Responses

Dynamic Responses on All Discovered Comp...

Response	By	Protection
Run full antimalware scan	Client Protection	3
Run quick antimalware scan	Client Protection	1

### Security Risk Breakdown

Security Risk on All Discovered Users



420

- Normal
- Low
- Medium
- High

### Computer Protection Status

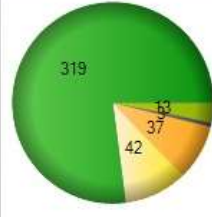
Computer Protection Status

Total number of managed assets: 401.

Protection Tec...	Computers Wi...	% With Issues
SecurityStat...	308	76.81
AntiMalware	18	4.49
SecurityUpd...	10	2.49
Firewall	4	1.00
NetworkAcc...	0	0.00

### Policy Deployment Status

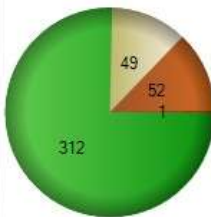
Policy Deployment Status



- No Agent Deployed
- No Policy Applied
- Unknown
- Wrong Policy
- Old Policy
- Policy Up To Date

### Security Risk Breakdown


Security Risk on All Discovered Computers



- Normal
- Low
- Medium
- High

### Sharepoint detection volume:

Sharepoint detection volume:



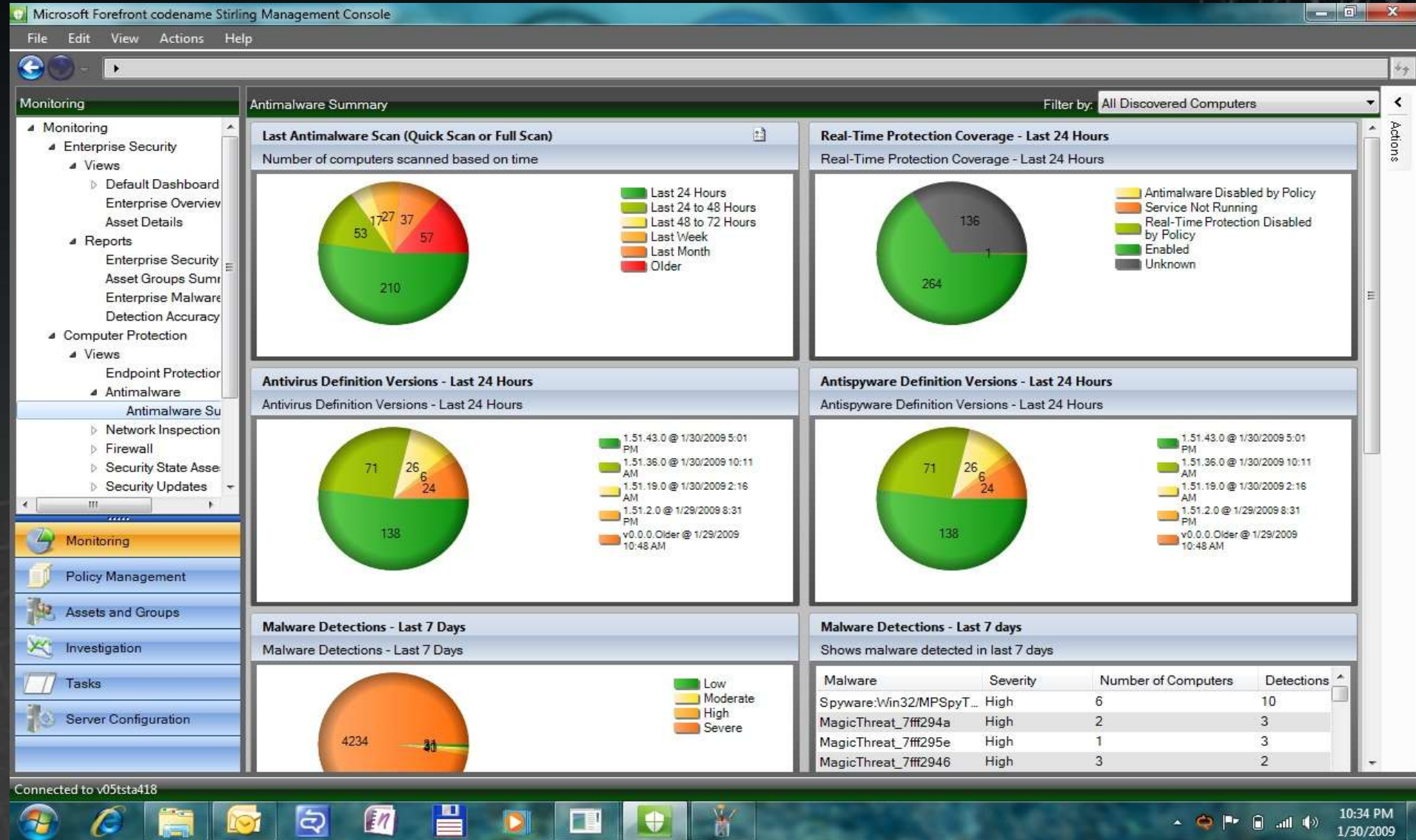
134.26

- % Detected
- % Detected in last hour

Connected to v05tsta418

10:24 PM 1/30/2009

# Stirling Antimalware Summary





# Stirling Reporting

Microsoft Forefront codename Stirling Management Console

File Edit View Actions Help

Monitoring

- Monitoring
  - Enterprise Security
    - Views
      - Default Dashboard
      - Enterprise Overview
      - Asset Details
    - Reports
      - Enterprise Security Summary
      - Asset Groups Summary
      - Enterprise Malware Summary
      - Detection Accuracy Summary
    - Computer Protection
    - Mail Protection
    - Document Protection
    - Network Protection
    - Authorized Software Management
    - System Status
  - Alerts
- Policy Management
- Assets and Groups
- Investigation
- Tasks
- Server Configuration

Enterprise Malware Summary

1 of 1 100% Find | Next Select a format Export

## Malware Summary Report

Microsoft Forefront Code Name "Stirling"

Report Scope:	All IT Assets			
Report Time Span:	Day	Start: 1/29/2009 10:00:00 PM	End: 1/30/2009 9:59:00 PM	Generated on: 1/30/2009 10:25:21 PM
All dates and times are shown in server time zone: (GMT-08:00) Pacific Standard Time				

### Malware Contribution to Security State

#### Malware Contribution to Security Risk During the Last Day

Risk Level

- High
- Medium
- Low
- Normal

1/30/2009 2:00 AM 1/30/2009 7:00 AM 1/30/2009 12:00 PM 1/30/2009 5:00 PM

#### Malware Contribution to Security Risk During the Last Month

1/4/2009 1/10/2009 1/16/2009 1/22/2009 1/28/2009

#### Malware Contribution to Compromised Computers During the Last Day

Severity

- High
- Medium

48 36 24

#### Malware Contribution to Compromised Computers During the Last Month

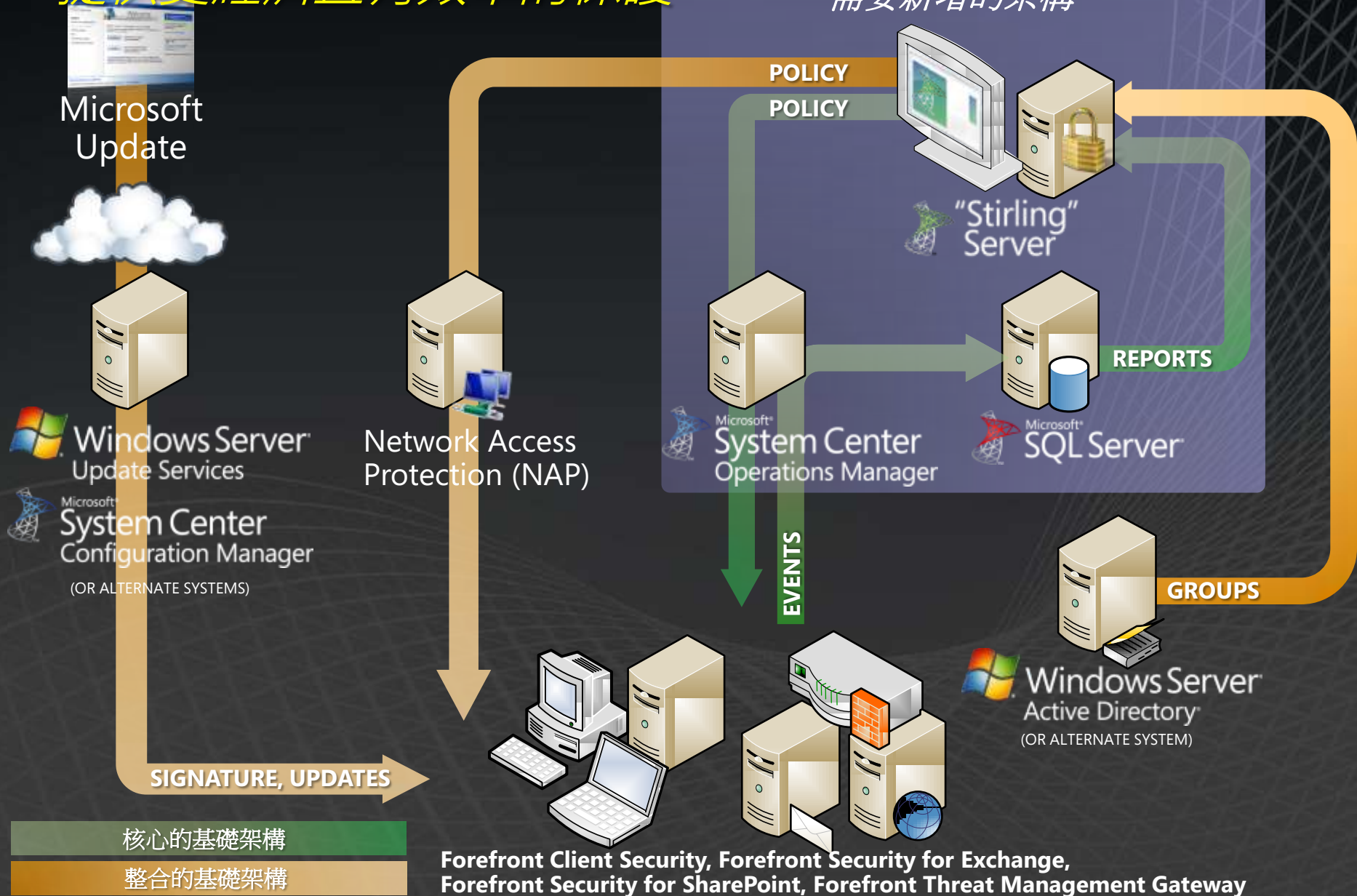
55 44 33 22

Connected to v05tsta418

10:29 PM 1/30/2009

# 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  
 $風險 = 安全狀態 \times 資產重要度$
- 從內而外涵蓋所有的防護  
*Clients, Servers, Network*

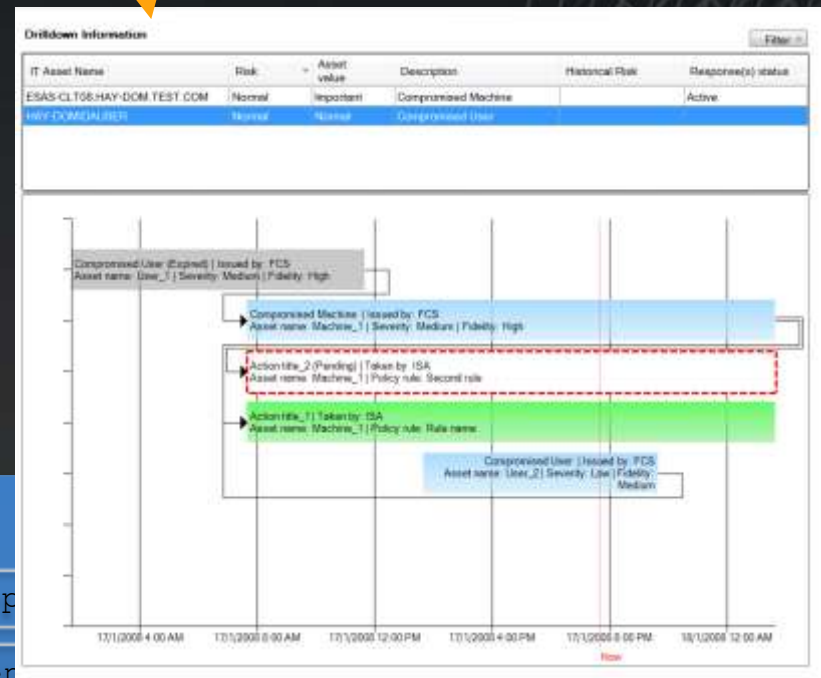


All Assets Security Risk: Low  
Declared on: 11/30/2007 3:38:54 PM

30 computers out of 678 (4%) are in medium risk  
12 computers out of 678 (1%) are in medium risk  
3 manual approvals require your attention

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 Exception

Security Assessment Check: Failed Remediation      Client

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

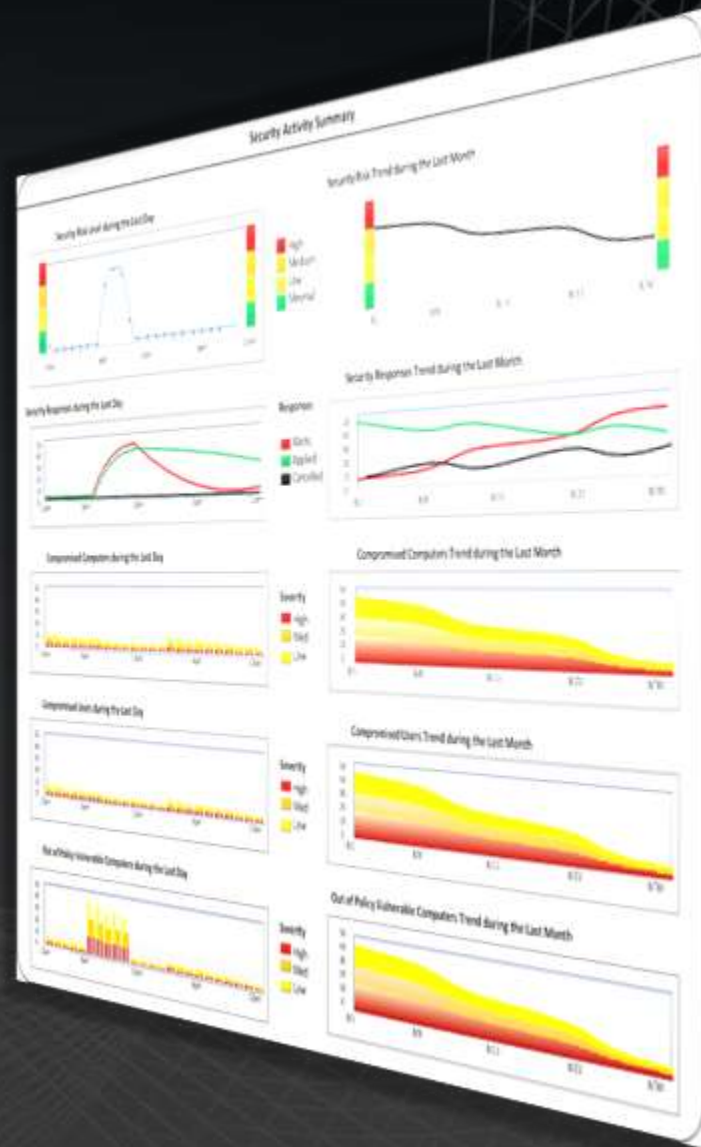
Get Public Folders

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*

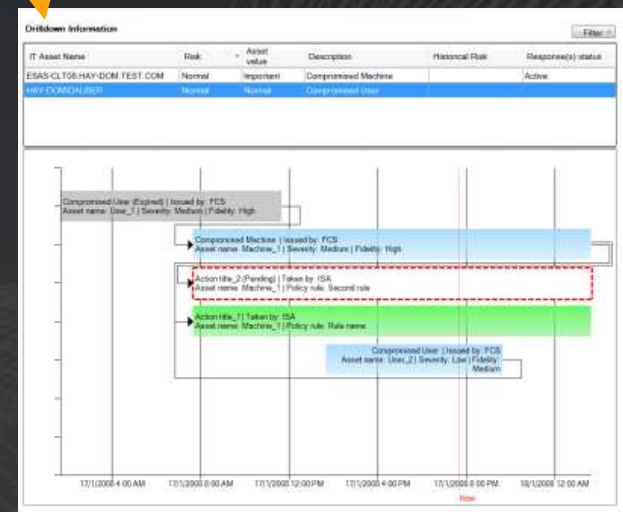
---

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

The screenshot displays the Windows Group Policy Editor interface. The left pane shows the navigation tree with 'System' > 'Device Installation' > 'Prevent installation of removable devices' selected. The main pane shows the policy details for '防止安裝卸除式裝置' (Prevent installation of removable devices). The policy is currently set to 'Not configured' (尚未設定). A red box highlights the policy name in the list on the right side of the main pane.

設定	狀態
允許系統管理員覆寫裝置安裝限制原則	尚未設定
允許使用符合這些裝置安裝類別的驅動程式安裝裝置	尚未設定
防止使用符合這些裝置安裝類別的驅動程式安裝裝置	尚未設定
因原則而無法安裝時顯示自訂訊息 (汽球內文)	尚未設定
因原則而無法安裝時顯示自訂訊息 (汽球標題)	尚未設定
允許安裝符合這些裝置識別碼的裝置	尚未設定
防止安裝符合下列任何裝置識別碼的裝置	尚未設定
<b>防止安裝卸除式裝置</b>	尚未設定
防止安裝未由其他原則設定描述的裝置	尚未設定

**防止安裝卸除式裝置**

顯示 內容

需求:  
必須是 Windows Vista 以上的版本

描述:  
防止安裝卸除式裝置。

如果您啟用這個設定，將不能安裝卸除式裝置，也不能更新現存卸除式裝置的驅動程式。

如果您停用或未設定這個設定，只要裝置安裝的其他原則設定允許，就可以安裝卸除式裝置，也可以更新現存的卸除式裝置。

注意：這個原則設定優先於其他任何允許安裝裝置的原則設定。如果這個原則設定防止安裝某個裝置，即使該裝置符合其他允許安裝該裝置的原則設定，仍然無法安裝或更新該裝置。

對這個原則來說，當連接裝置的驅動程式表示該裝置為卸除式時，該裝置會被視為卸除式。例如，某個「通用序列匯流排」(USB) 裝置由連接該裝置的 USB 集線器之驅動程式...

延伸 標準

# 行動裝置的原則檢查

The screenshot displays the Group Policy Editor interface for the 'Block Compromised Clients' policy. The left-hand navigation pane shows the tree structure, with 'Security State Assessment' > 'Device Control' selected. The right-hand pane shows the configuration for 'Security State Assessment: Device Control'. The policy is set to 'Verify that device configuration complies with following settings:'. Under the 'Removable storage devices' section, the 'Removable disk access' dropdown menu is open, showing options: 'No Restrictions (default)', 'Restrict read and write access', and 'Restrict only write access'. The 'No Restrictions (default)' option is currently selected. Other dropdowns for 'CD and DVD drive access', 'Floppy drive access', 'Tape drive access', and 'WPD device access' are all set to 'No Restrictions (default)'. At the bottom, there are two checkboxes: 'If this check fails, automatically configure assets to comply with these settings' and 'If this check fails, restrict network access for computers that do not comply', both of which are currently unchecked.

Block Compromised Clients

Select or clear policy units

- Network Inspection System
  - General
  - Authorized Software Management

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)**

CD and DVD drive access: **No Restrictions (default)**

Floppy drive access: **No Restrictions (default)**

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**

This check verifies that users are not configured to automatically logon without entering their credentials.

- Verify that the built-in Administrator account is not configured to automatically log on or stored in the local Administrators group
- If this check fails, restrict network access for computers that do not comply

**Guest account**

This check analyzes the state of the built-in Guest account to ensure that it is disabled or does not exist.

- Verify that the built-in Guest account is disabled or does not exist
- If this check fails, restrict network access for computers that do not comply

**Local administrators group**

This check verifies that the local Administrators group contains only members that are not expired.

- Verify that the local Administrators group contains only members that are not expired
- If this check fails, restrict network access for computers that do not comply

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**

# UAC的原則設定

The screenshot shows the 'Edit Policy: Block Compromised Clients' window. The left-hand navigation pane is expanded to 'User Account Control' under 'Security State Assessment'. The main pane displays the following configuration:

- Security State Assessment: User Account Control**
  - This check determines the configuration of User Account Control (UAC) on assets running operating systems that support UAC. You can force assets to comply with these settings by automatically reconfiguring UAC settings and 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:

Two blue callout boxes are overlaid on the screenshot:

- Top callout: 確認程式安裝時要提醒提升權限
- Bottom callout: 是否在未通知的情況下安裝Active X



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**<sup>®</sup>

*Your potential. Our passion.*<sup>™</sup>

© 2008 Microsoft Corporation. All rights reserved. Microsoft, Windows, Windows Vista and other product names are or may be registered trademarks and/or trademarks in the U.S. and/or other countries. The information herein is for informational purposes only and represents the current view of Microsoft Corporation as of the date of this presentation. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information provided after the date of this presentation. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS PRESENTATION.