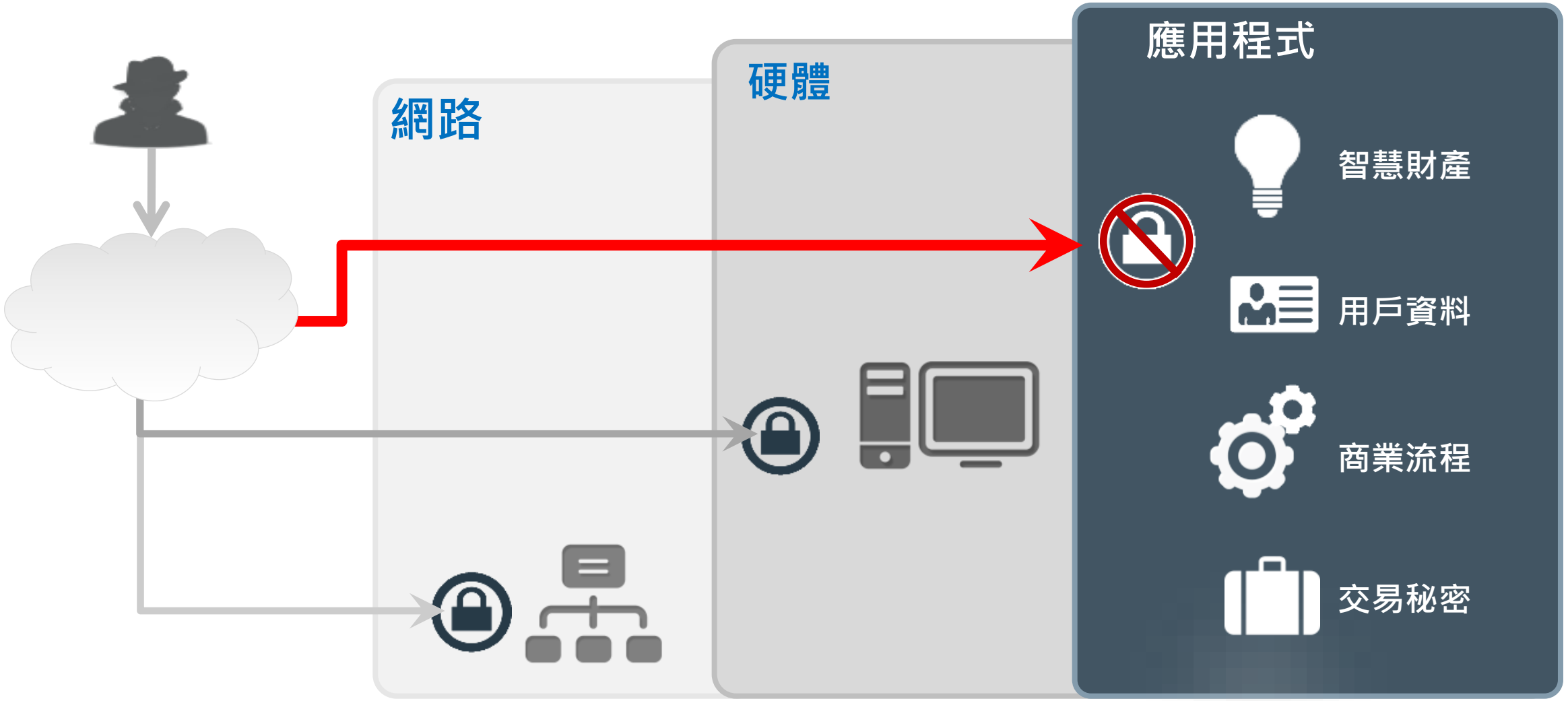
Hewlett Packard Enterprise

Web Server Protection (Web 伺服器防護)

Nicholas Hsiao

Dec., 2015

針對應用程式的網路犯罪活動



Hewlett Packard
Enterprise

80%

成功的攻擊是針對應用程式層

86%

的應用程式存在安全漏洞

<10%

IT 預算花費在應用程式安全上

$3.8m

資料外洩的平均成本

13%

自動具備有折衷的解決方案

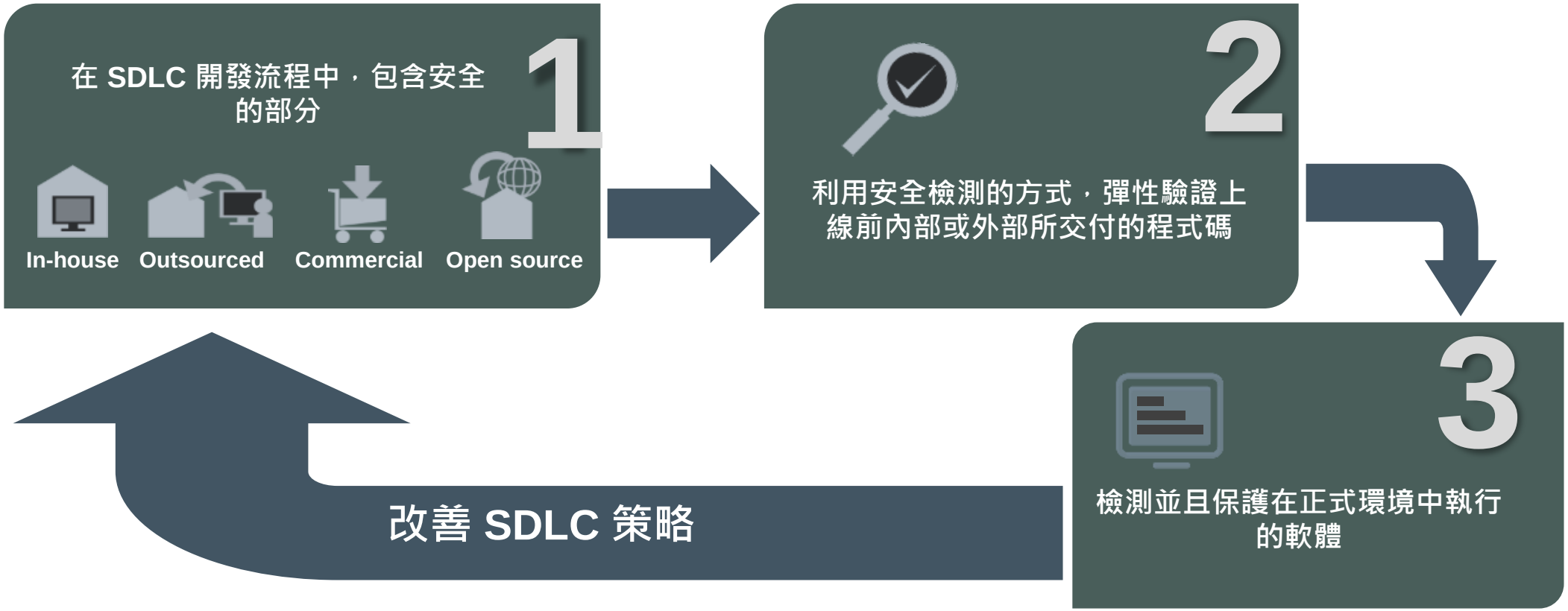
Sources: Gartner , Ponemon Institute, Annual Study: $U.S. Cost of a Data Breach, The Open Security Foundation

Hewlett Packard Enterprise

應用程式安全的挑戰

Hewlett Packard
Enterprise

正確的方法 > 系統性, 前瞻性

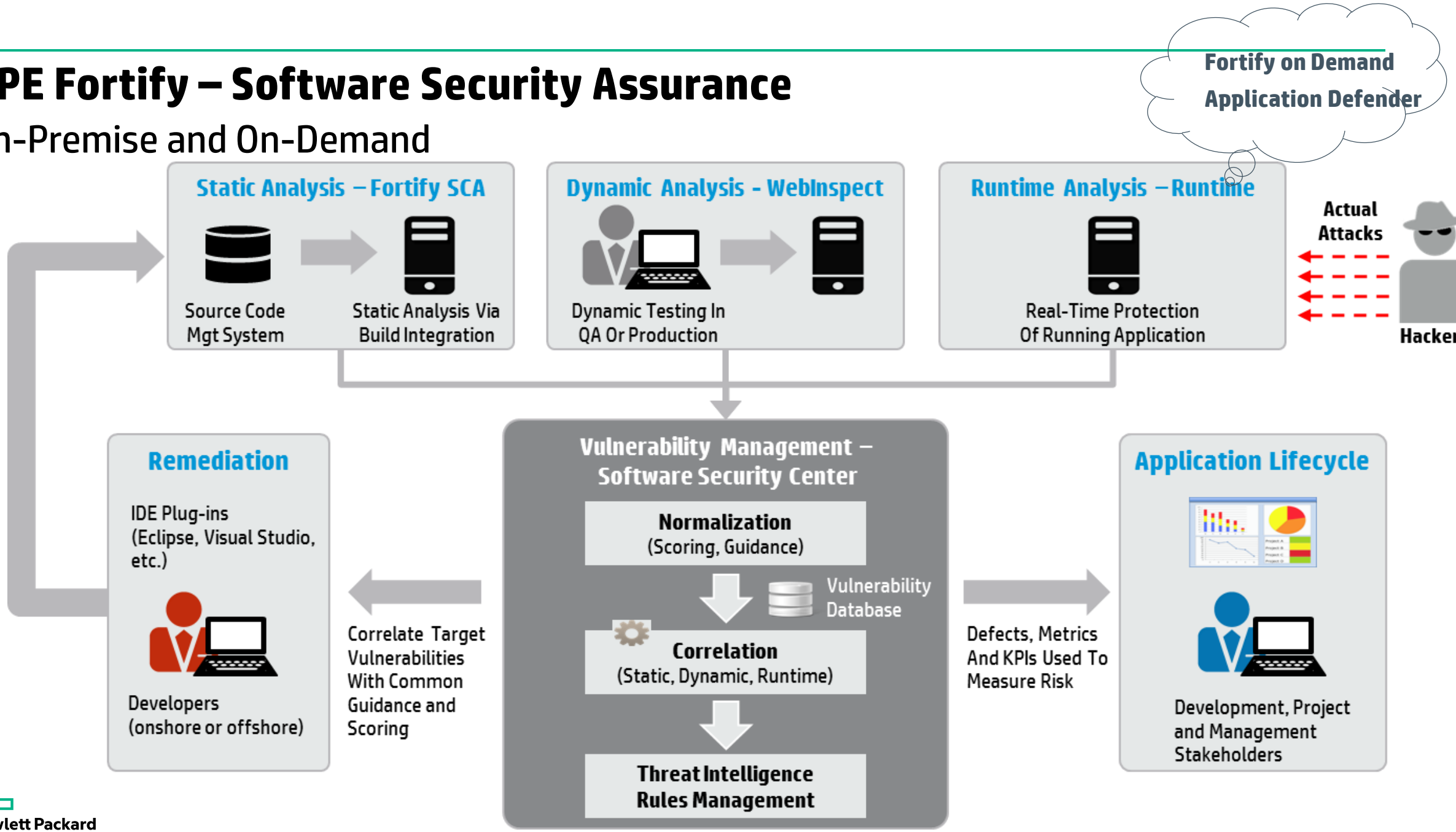


安全軟體保障 (SSA)

Hewlett Packard Enterprise

HPE Fortify – Software Security Assurance

On-Premise and On-Demand



Hewlett Packard Enterprise

Web Server Protection

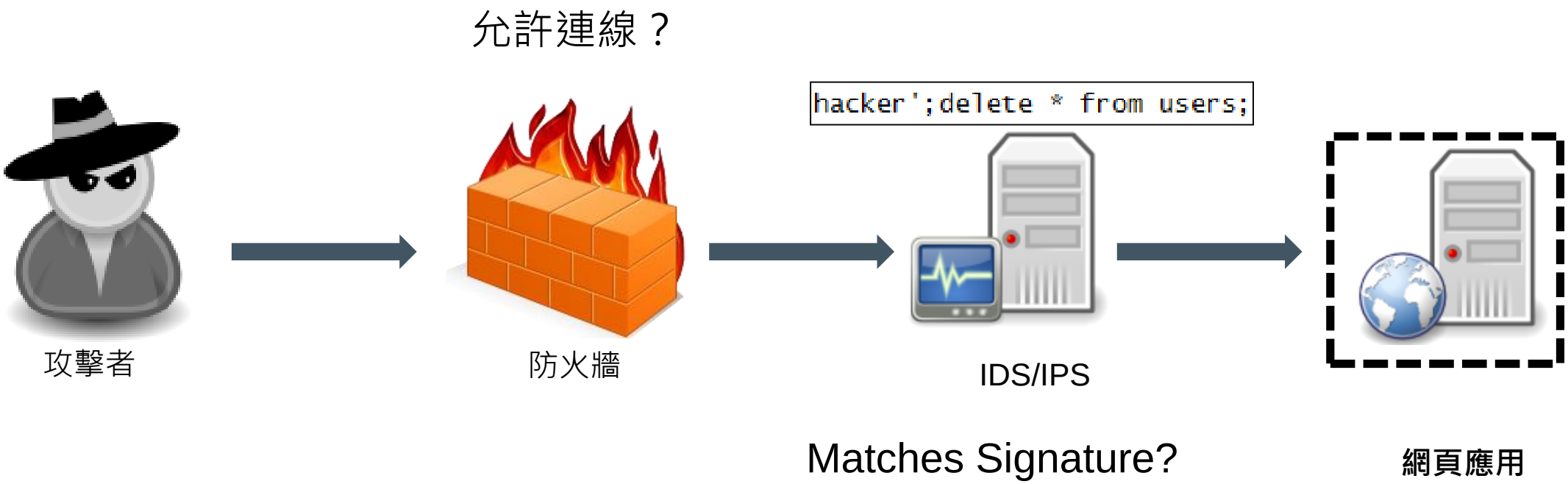
利用 IPS 或 TippingPoint 可以做什麼？

Filter Groups

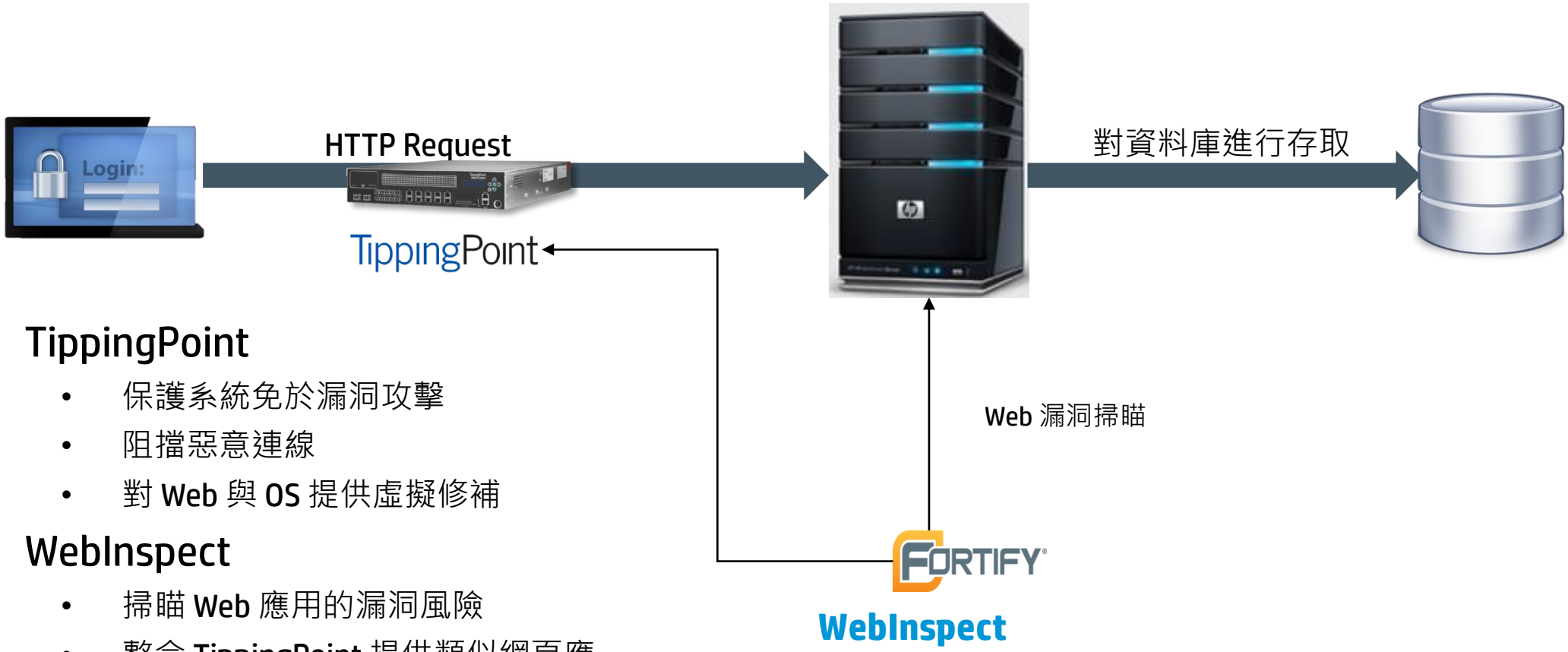
This table lists filter hits over the last 30 days, grouped by the filter's category.

Filter Group	Total Filters in Group	# Filters With Hits	Filter Hits: L
Backdoor	280	2	41
Cross Site Scripting (XSS)	66	9	1,621
DNS	51	3	52,027
HTTP (all)	3,257	145	361,502
HTTP (client)	1,692	12	13,679
HTTP (server)	1,655	135	348,890
Peer to Peer (P2P)	278	4	176,656
Phishing	29	1	2
PHP File Include	36	21	825
SCADA	44	1	3
SMB	144	4	43,117
SMTP	315	1	6
Spyware	205	2	17
SQL Injection	63	2	151,730
Zero Day Initiative	798	1	298

黑客/入侵者

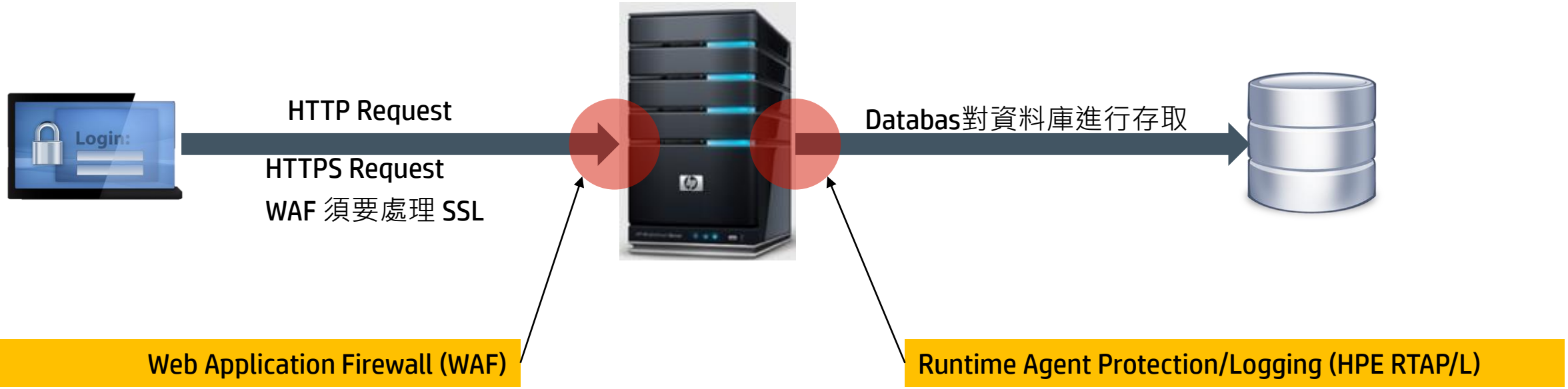

允許連線？
hacker';delete * from users;
攻擊者
防火牆
IDS/IPS
Matches Signature?
網頁應用
select * from users where username='evil' and password='hacker';delete * from users;
Attack!

對 Web 的防護方式 - I



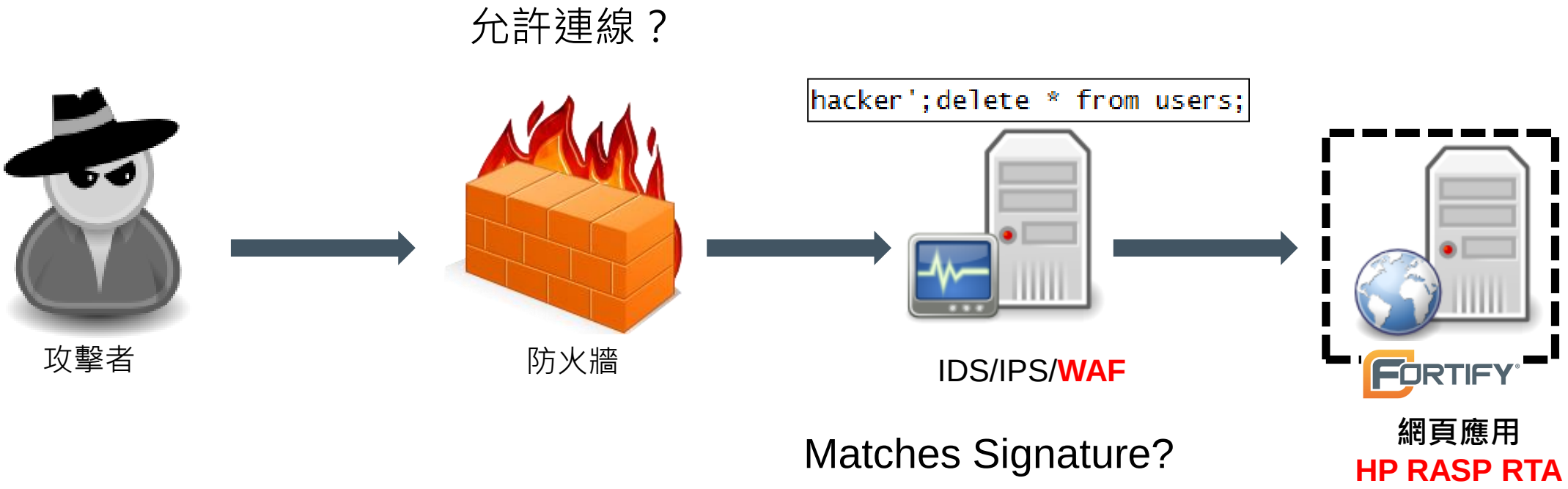
- TippingPoint
  - 保護系統免於漏洞攻擊
  - 阻擋惡意連線
  - 對 Web 與 OS 提供虛擬修補
- WebInspect
  - 掃瞄 Web 應用的漏洞風險
  - 整合 TippingPoint 提供類似網頁應用程式防護 (WAF) 的防護

對 Web 的防護方式 - II



WAF	RASP
網路層防護	應用層防護
需要另外處理 SSL	無需處理 SSL
僅能見到部分的 SQL 語法	可見到完整的 SQL 語法
無法取得應用程式內的使用者訊息	可從應用程式中取得使用者訊息
遲緩：網路	遲緩：應用
無法見到檔案存取狀態	可以關聯存取檔案名稱以即使用者訊息
無法偵測 Web 是否成為跳板主機	可檢查 Web 服務器是否開啟網路連線至其它系統

防護架構


允許連線？
hacker';delete * from users;
攻擊者
防火牆
IDS/IPS/WAF
Matches Signature?
網頁應用
HP RASP RTA
FORTIFY
select * from users where username='evil' and password='hacker';delete * from users;
Attack!

對 Web 攻擊進行偵測以及防護
風險管理 – RASP 技術提供資訊

HP Application Defender Event Details

Time: Jan 06, 2015 06:51:29.079 AM
Event ID: 8725e886-e24e-4f7f-8d1f-6e8005f66f20
Location: DelegatingStatement.java:206
* General
Category: SQL Injection
Event Severity: Critical
Target Path: /riches/ShowLocations.action
Action Taken: Monitor
Risk Group: Riches
Agent: windows7HP
Host IP: windows7HP.kornet
Hostname: windows7HP
* Request Details
User:
Session ID: 8A0A37816E304D52DDCCA91B49775019
Source IP: 210.216.53.202
Request Protocol: http
Request Method: POST
User Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/39.0.2171.95 Safari/537.36
Referer: http://118.33.120.184:8080/riches/FindLocations.action
Target Port: 8080

* Request Parameters:
-zip
-address ' or '1' = '1
-state
-type atm
-city

* Request Cookies:
-authType 0
-JSESSIONID 8A0A37816E304D52DDCCA91B49775019

* Request Header:
-x-bluecoat-via 8bc7350be8c88d2c
-referer
http://118.33.120.184:8080/riches/FindLocations.action
-content-length 58
-cookie authType=0; JSESSIONID=8A0A37816E304D52DDCCA91B49775019
-cache-control max-age=0
-accept-encoding gzip, deflate
-user-agent Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/39.0.2171.95 Safari/537.36
-origin http://118.33.120.184:8080
-accept text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
-host 118.33.120.184:8080
-accept-language en-US,en;q=0.8
-connection Keep-Alive
-content-type application/x-www-form-urlencoded

* Stack Traces
* Event Trigger
SELECT * FROM location WHERE branch = 'Yes' AND state = '' AND city = '' AND address = '' or '1' = '1'
* Location Stack Trace

org.apache.tomcat.dbcp.dbcp.DelegatingStatement executeQuery DelegatingStatement.java 206
com.fortify.samples.riches.model.LocationService findAtmByAddress LocationService.java 139
com.fortify.samples.riches.FindLocations execute FindLocations.java 32
sun.reflect.NativeMethodAccessorImpl invoke0
sun.reflect.NativeMethodAccessorImpl invoke NativeMethodAccessorImpl.java 57
sun.reflect.DelegatingMethodAccessorImpl invoke DelegatingMethodAccessorImpl.java 43

- Source Stack Trace

RTAP 防護

Java, .NET 應用程式可視化以及安全防護

1. Authorization Check Failure
2. Broken Link
3. Brute Force Login Attempt
4. Buffer Overflow
5. Command Injection
6. Cookie Security: HTTPOnly Not Set on Session Cookie
7. Cookie Tampering
8. Credit Card Fraud
9. Cross-Site Request Forgery
10. Cross-Site Scripting: Persistent
11. Cross-Site Scripting Attacks
12. Directory Listing
13. Discovery: Known Vulnerability Scanner Activities
14: Denial of Service: Hash Collision
15. Denial of Service: Parse Double
16. Denial of Service: Regular Expression
17. Forceful Browsing
18: Header Manipulation
19. Hidden Field Manipulation
20. HTTP Parameter Pollution
21: Insecure Randomness
22: JavaScript Hijacking
23: Leftover Debug Code
24.Link Spam: Persistent
25: Link Spam Attacks
26. Malformed Request: Missing Accept Header
27. Malformed Request: Missing Content=Type
28. Malformed Request: Use of Unsupported Method
29. Method Call Failure
30. Open Redirect
31. Poor Effor Handling: Unhandled Exception
32. Privacy Violation: Credit Card Number
33. Privacy Violation: Social Security Manager
34. Privilege Management: Unnecessary Permission
35. Probing
36. Probing: ColdFusion AJAX Debugging
37. Probling: Command Injection
38. SQL Injection
39. Session Fixation
40. Slow Method Call: Show Database position
41. Slow Method Call: Slow Database Query (Batch Processing)
42. Slow Method Call: Slow Database Query (Web Request)
43. System Information Leak
44. Value Shadowing
45. Value Shadowing
56. Getting Rid of Hard Coded XSS and issux.

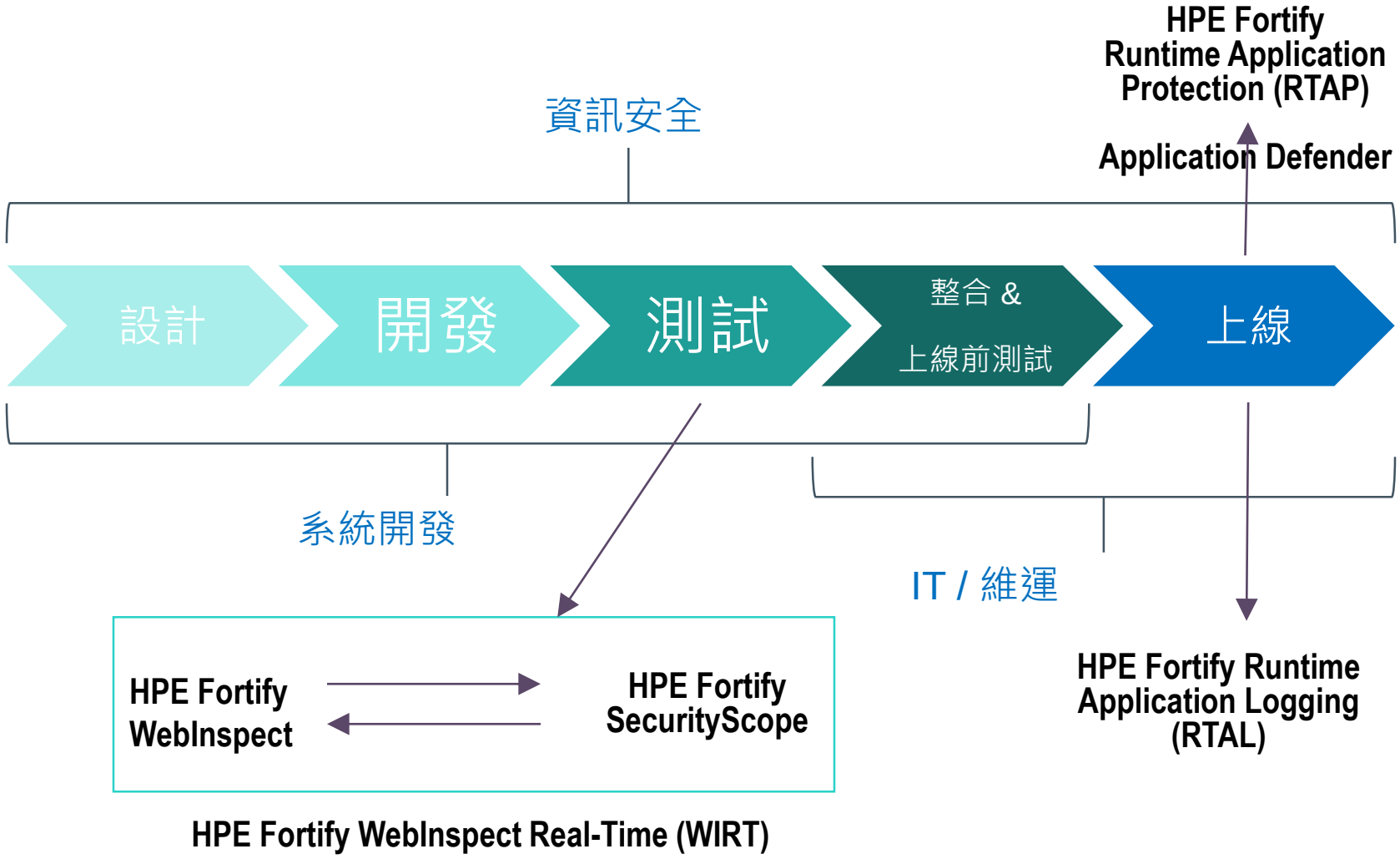
RTAL Logs 紀錄

Java, .NET 應用程式可視化以及安全防護

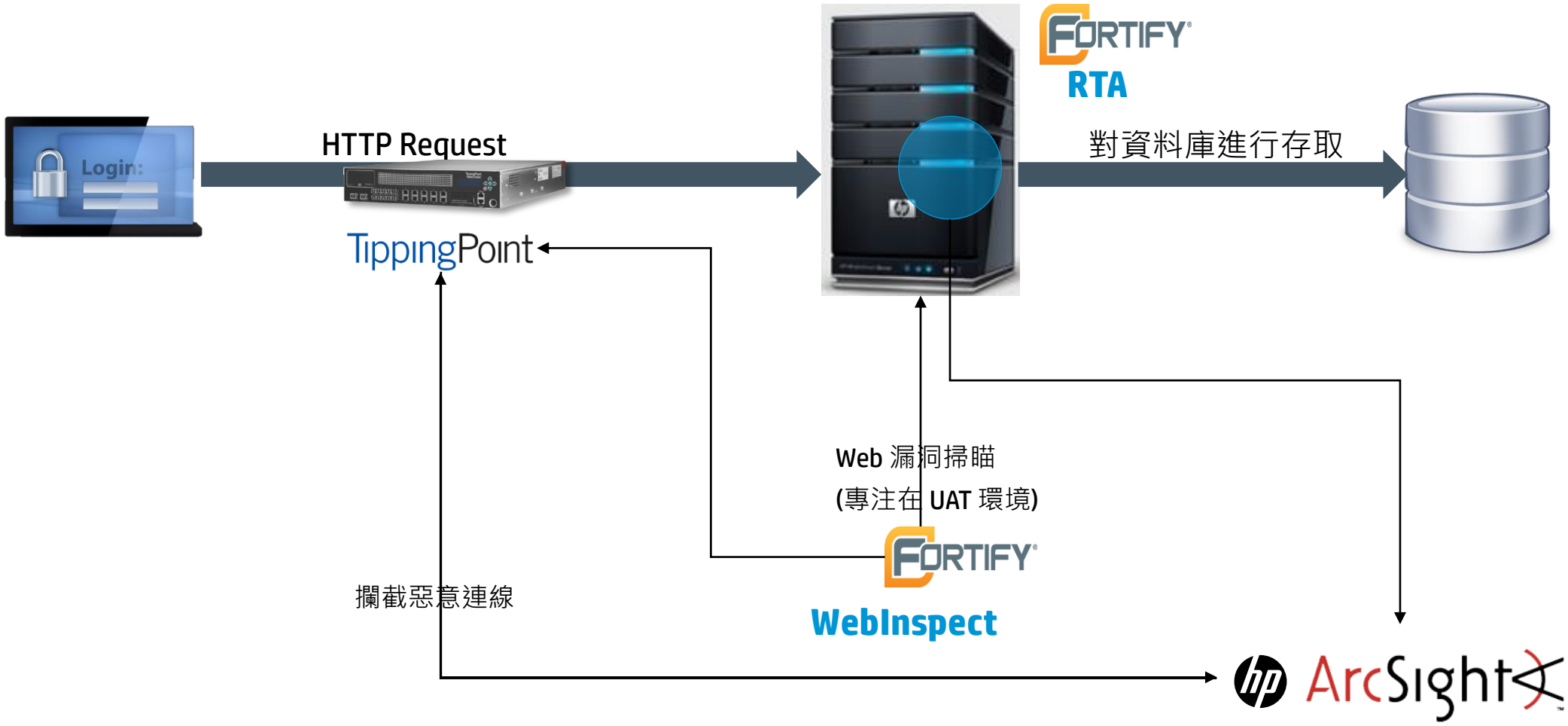
- HPE System Startup Message
- Web Application Start
- Web Application Stop
- HTTP Session Start
- HTTP Session Stop
- User Logon: Success
- User Logon: Failure
- User Logoff
- Database Query
- General Exception Created
- Security Exception Created (Java only) 1
- Crypto Exception Created (Java only)1
- File Create
- File Delete
- File Read
- File Write
- Network Socket Bind
- Network Socket Connect
- Network Socket Shutdown
- Network Socket Close
- Command Execution

- Windows Registry Create (.NET only)
- Windows Registry Read (.NET only)
- Windows Registry Write (.NET only)
- Windows Registry Delete (.NET only)
- Spring/Struts/Dotnet Validation Failure
- Unified Logging: JUL (Java only)
- Unified Logging: Log4j (Java only)
- Unified Logging: JCL (Java only)
- Unified Logging: Slf4j (Java only)
- Unified Logging: NLog (.NET only)
- Unified Logging: Log4Net (.NET only)
- Unified Logging: Enterprise Library(.NET only)
- User Management: Create User
- User Management: Delete User
- User Management: Change User Password
- User Management: Create Group
- User Management: Delete Group
- User Management: Add User to Group
- User Management: Remove User from Group
- Web AccessLog

相關解決方案

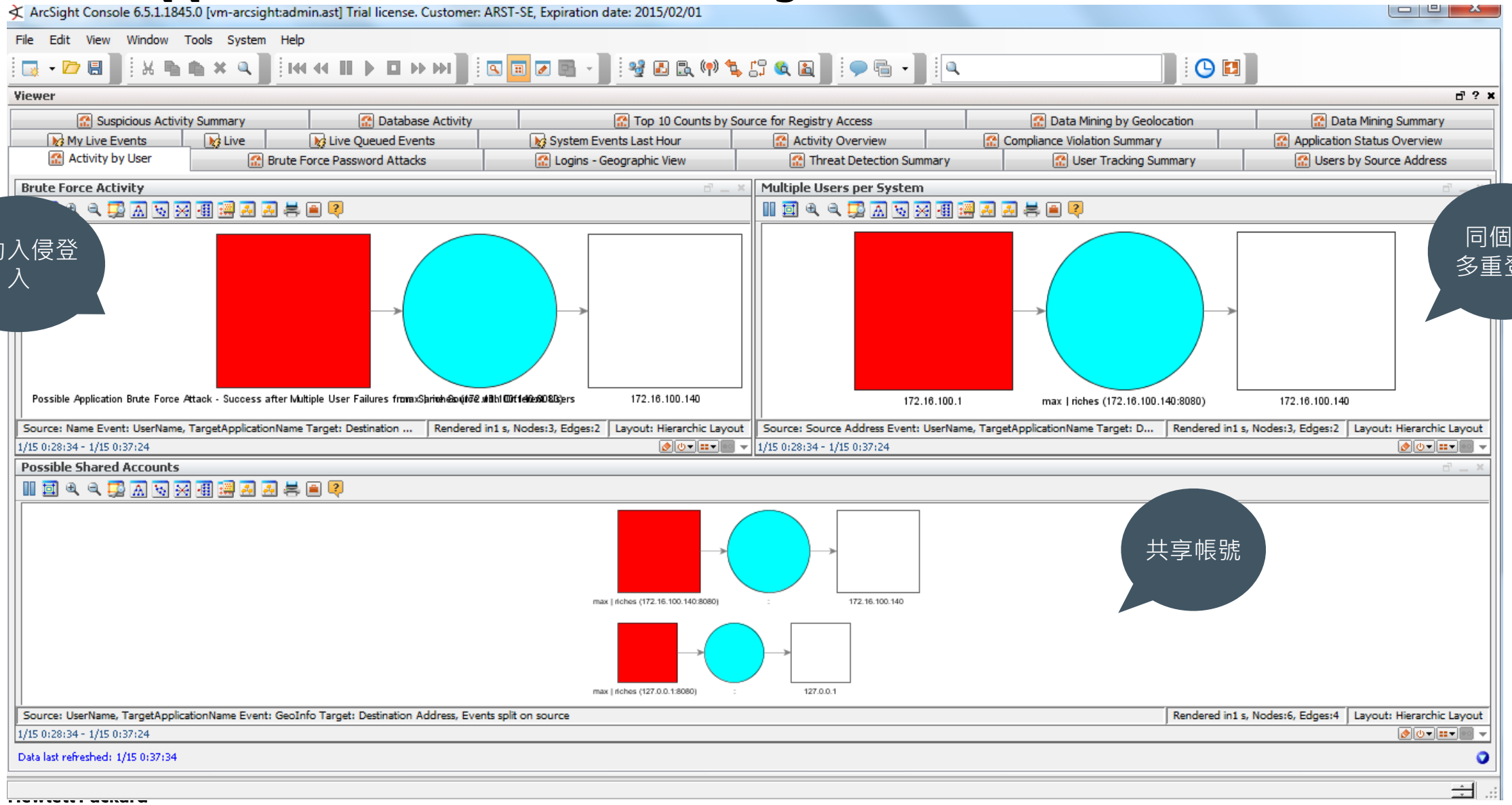

HPE Fortify
Runtime Application
Protection (RTAP)
Application Defender
資訊安全
設計
開發
測試
整合 &
上線前測試
上線
系統開發
IT / 維運
HPE Fortify
WebInspect
HPE Fortify
SecurityScope
HPE Fortify Runtime
Application Logging
(RTAL)
HPE Fortify WebInspect Real-Time (WIRT)

對 Web 的防護方式 - III

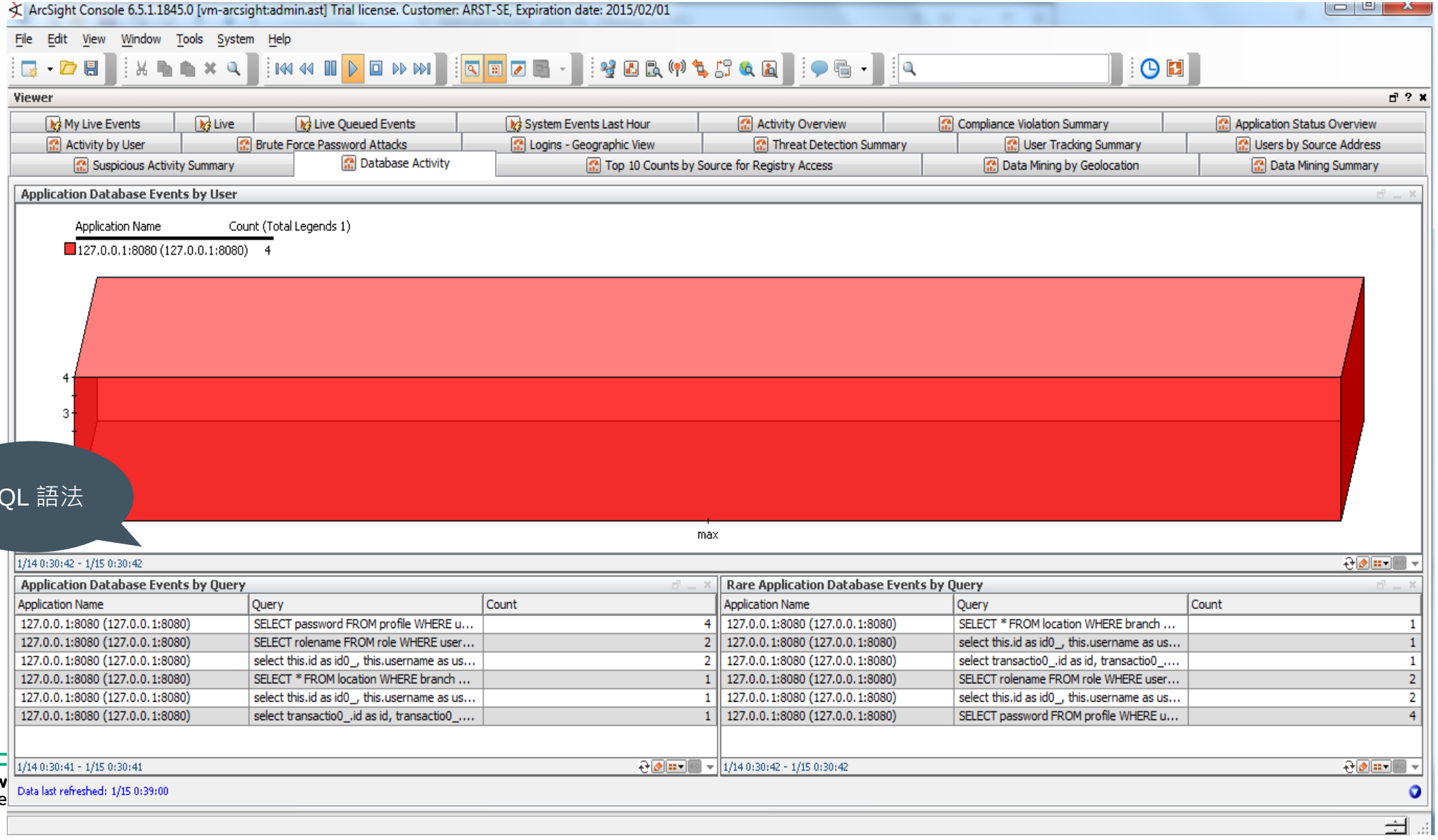


Hewlett Packard Enterprise

RTAL/AppView Web 上線監控 (ArcSight)



RTAL/AppView Web Online Monitoring (ArcSight)



SQL 語法

Web 的防護

Log
Command
Attack
HTPP/S Flow
Console

Fortify WebInspect

Fortify SCA

漏洞報告

AP 虛擬補丁

SSL

TippingPoint

Internet

SSC
黑白箱交叉分析

WAF (Optional)

RTAP/L

Web Server

阻擋連線

RepSM
Intelligence Data

ArcSight

正式環境監控人員

Hewlett Packard
Enterprise

Hewlett Packard
Enterprise

Thank you

Nicholas Hsiao
North Asia