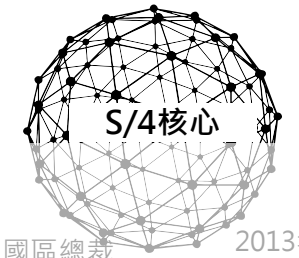
SAP S/4HANA 雲端資訊安全應用亮點

Ying-Jie Chen, Director, Presales
SAP Taiwan
January 16, 2018

SAP 雲方案整體架構



2016年12月，中國電信與SAP聯合簽訂戰略合作協定，發佈concur雲服務

2016年底SAP中國區總裁宣佈Ariba落地中國

2013年11月SAP宣佈與中數通完成了SaaS雲的HCM部署

2014年1月13日，SAP在上海建立首個Hybris雲資料服務中心，佈局大中華市場

SaaS

PaaS

IaaS

1 CONCUR 差旅管理

2 SAP Ariba 集團採購

3 SAP SuccessFactors 人力資源

4 SAP Hybris 管道行銷

SAP Cloud Applications

SAP BusinessObjects Cloud & SAP Digital Boardroom

ustomer and 3rd Party pplications

SAP Leonardo

SAP Cloud Platform

資訊安全

Ecosystem

API Business Hub

Marketplace

資訊安全 整合性 為業務服務 移動終端 客戶體驗協作 分析 機器學習 IoT服務

APIs

20億歐元投入

阿裡雲聯合生態合作

研究院成立專項團隊

智能資料集成 JAVA HTML 地理資料 API管理 動態報表 圖形文本 智能資產

SAP Cloud Platform

amazon web services

Microsoft Azure

雲平臺底層架構

面向客戶運營及業務場景的一站式運營、部署能力與方案

E2E雲基礎架構解決方案能力，與合作夥伴打包提供

2017年2月8日，SAP大中華區正式啟用中國本土資料中心，向客戶提供四款基於雲的解決方案。

2014年，SAP宣佈與大陸中數通共建雲服務體系，所有的服務安全、運營效率的保證都通過中國電信的資料中心服務體系來保證

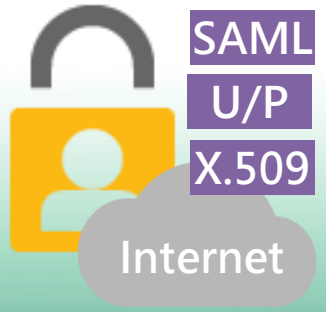
SAP Cloud Platform 公有雲平台
資安認證服務 Identity Provider

SAP Identity Authentication

- 認證生命週期管理的雲端版。
- Pay-per-Logon-Requests 每天每用戶計價。
- 依據 Tenant 隔離的用戶數據。
- 全網頁管理介面。
- 豐富的定製化與品牌頁面。
- 主要應用場景 : B2C 與 B2B。
- SAP CP 生產用戶默認的信賴 IdP。

“Bring Your Own Identity Provider”

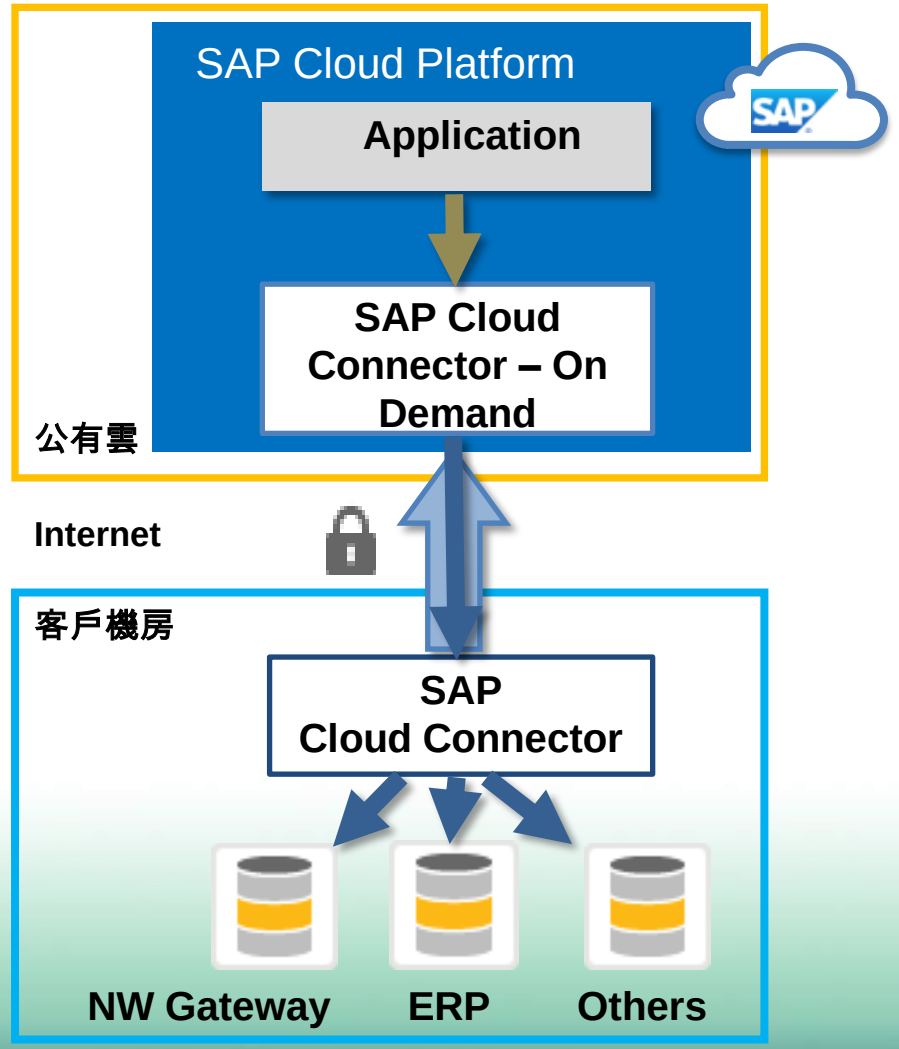
- 前提: 兼容於 SAML 2.0 協定。
- 主要應用場景 : B2E。
- 第三方整合的認證機制, 例如: Kerberos, X.509, …



“SAP ID Service”

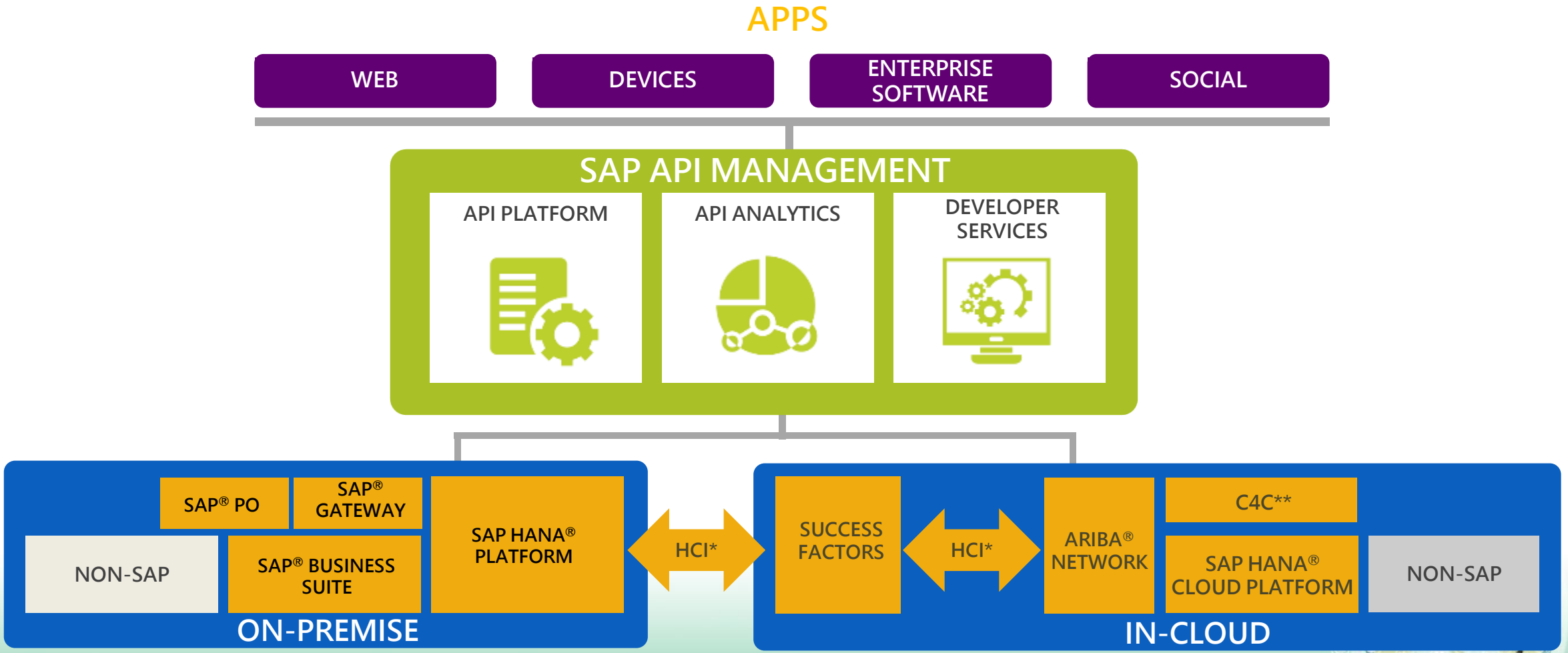
- SAP 發布於 Internet 上的公有雲 IdP。
- 免費服務, 類似 social IdPs 。
- 與 SCN 社群網站共用帳號。
- 只提供認證服務, 不包含用戶生命週期管理。
- SAP CP trial 帳號默認的 IdP 。

SAP Cloud Platform 公有雲平台
雲端安全連線服務 Cloud Connectivity Service



- 在 SAP Cloud Platform 與客戶機房系統之間, 建立安全的 VPN 通道 。
- 無須改動現有企業防火牆配置。
- 由機房內網啟動對公有雲的加密安全通道。
- 提供對客戶地端系統的安全訪問。
  - 詳細的 ACL 來管控雲端對地端資源的訪問權限。
  - 內建詳細的稽核歷史紀錄。
  - 採用基於 X.509 憑證的雲端與地端系統信賴關係。

SAP Cloud Platform 公有雲平台
API 管理服務 API Management Service



*SAP HANA® Cloud Integration

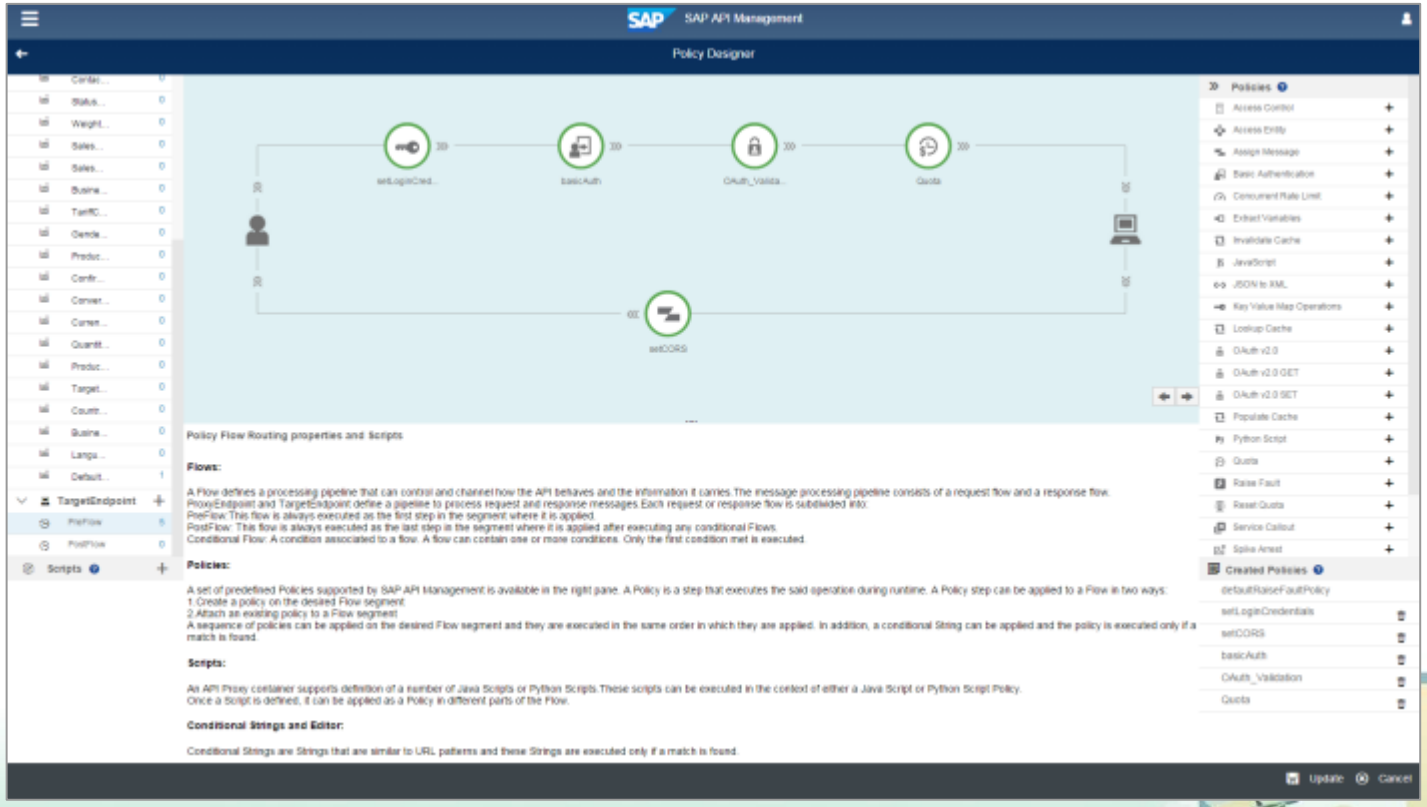
**SAP® Cloud for Customer

SAP Cloud Platform 公有雲平台
API 管理服務 API Management Service

入侵威脅保護

認證與授權

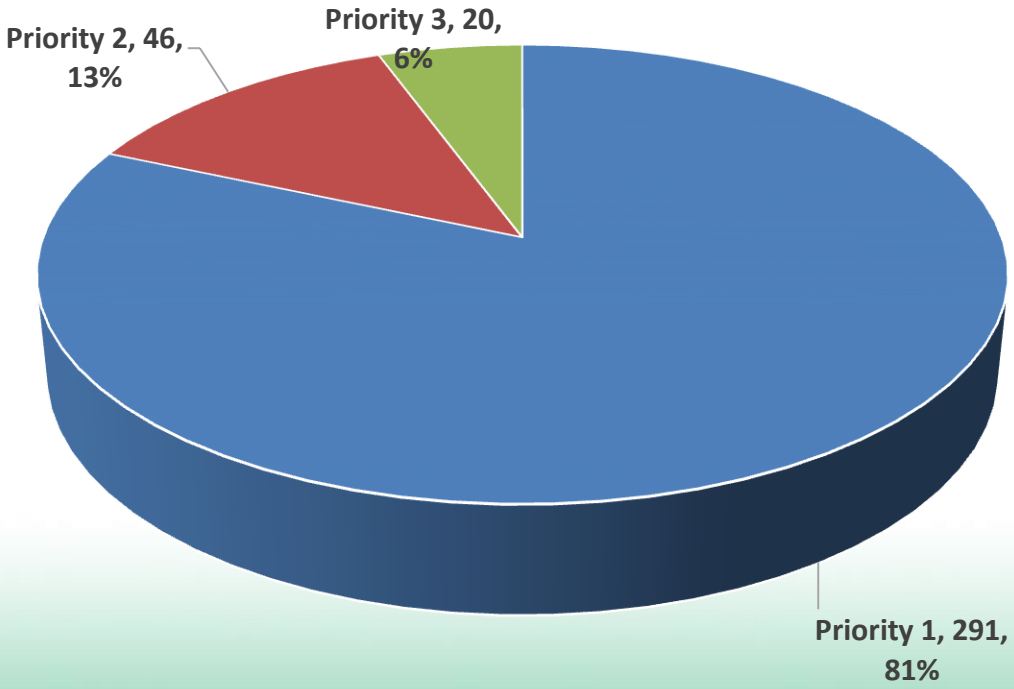
基於角色的訪問控制



客戶案例
SAP ERP ABAP OWASP Top-10 資安弱點掃描

在大型北美客戶 SAP ERP 生產系統實際操作, 在掃瞄
2,072 個客製化程式 (Y* & Z*) 後, 挖掘出 357 個資安弱點。

Vulnerabilities by priority



Statistics: Check	Prio 1	Prio 2	Prio 3
Total	300	46	20
Test Existence of a Program	1		
Program ... does not exist	1		
Security Analyses in Extended Program Check (SLIN)	291	46	20
Hard-coded user name	71		
Potential SQL injection (WHERE condition)	21		
Potential directory traversal	163		
Potential ABAP command injection	9		
Potential SQL injection (column names)		24	
Potential SQL injection (GROUP BY clause)			1
Potential SQL injection (table name when read performed)		20	
Potential SQL injection (table name when write performed)	12		
Potential directory traversal caused by non-secure parameters	1		
User-driven dynamic RFC function module call	8		
User-driven dynamic procedure call of program unit	3		
User-driven dynamic CALL TRANSACTION	3		
AUTHORITY-CHECK with explicitly specified user		2	
AUTHORITY-CHECK for SY-UNAME			17
Hard-coded system ID			2
Extended Program Check (SLIN)	8		
Program contains syntax errors	6		
The function module definition does not have a TFDIR entry	1		
Program source cannot be analyzed	1		

客戶案例
SAP ERP ABAP OWASP Top-10 資安弱點掃描

```
1  REPORT zslin_demo_sql_injection_2.
2
3  PARAMETERS: street  TYPE zemployees-street    LOWER CASE,
4              zipcode TYPE zemployees-zipcode   LOWER CASE,
5              city    TYPE zemployees-city      LOWER CASE,
6              phone   TYPE zemployees-phone_ext.
7  DATA: set_expr TYPE string,
8        user     TYPE xubname.
9
10 IF street IS NOT INITIAL.
11   set_expr = set_expr && ` STREET    = '` && street  && `'`.
12 ENDIF.
13 IF zipcode IS NOT INITIAL.
14   set_expr = set_expr && ` ZIPCODE   = '` && zipc
15 ENDIF.
16 IF city IS NOT INITIAL.
17   set_expr = set_expr && ` CITY
18 ENDIF.
19 IF phone IS NOT INITIAL.
20   set_expr = set_expr
21 ENDIF.
22
23 IF set_expr IS NOT
24   user = cl_abap_sy      _user_name( ).
25   UPDATE zemployees
26     SET (set_expr)
27    WHERE userid = user.
28 ENDIF.
29
```

Input for `street`:

```
 xyz' salary =
'1500
```

```
et_expr:
TREET = 'xyz'
salary = '1500'
```

Possible SQL injection (SET clause)

```
...
SET STREET = 'xyz'
    salary =
'1500'
```

開發生命週期資安端到端解決方案

動態應用安全測試	靜態應用安全測試
在執行中的應用找到弱點	在應用源碼中找到弱點
手動應用滲透測試	自動源碼掃描
自動應用弱點掃描	手動源碼掃描

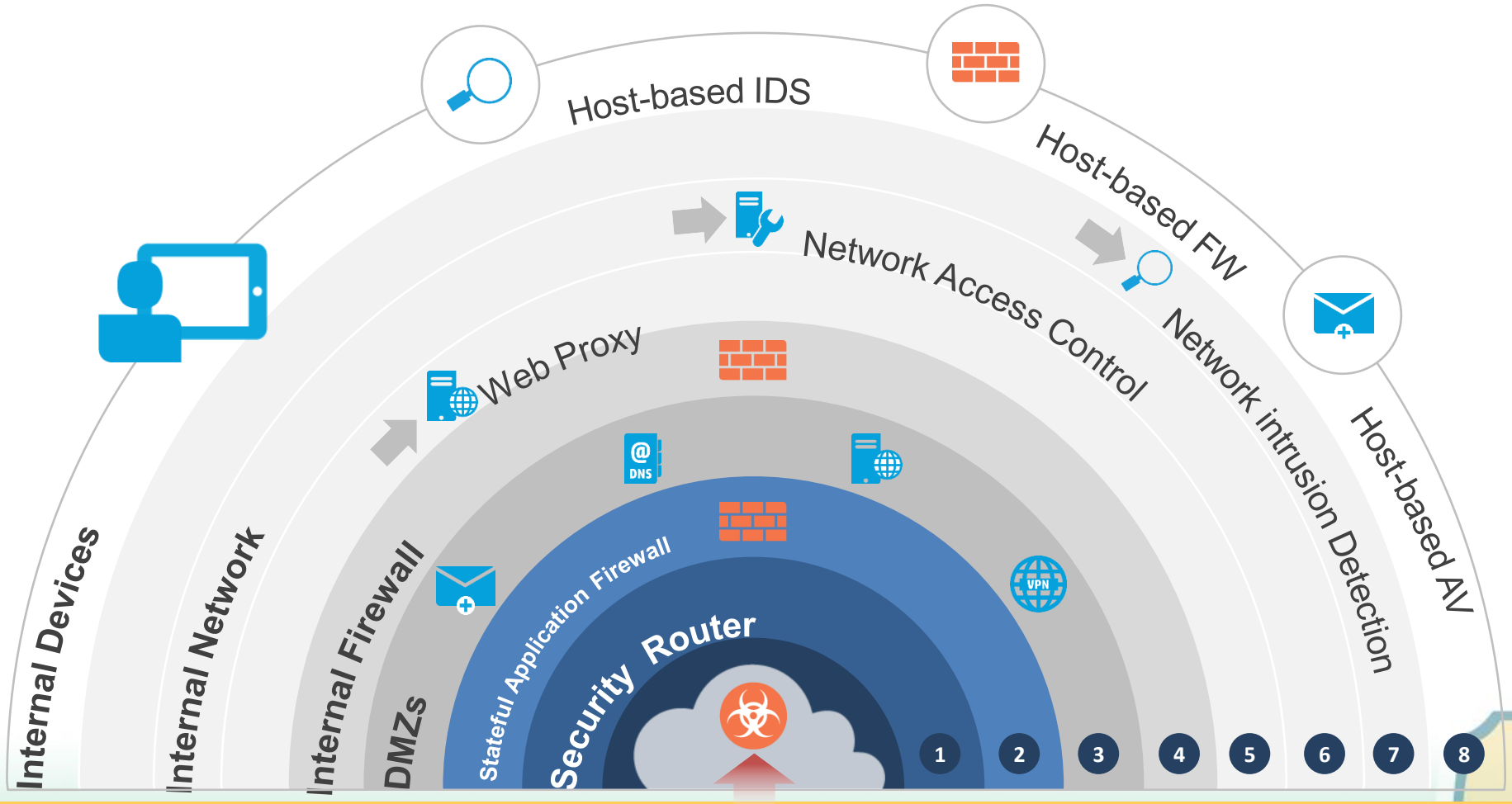
軟體開發資安治理、報表、稽核與分析管理平台

non-ABAP non-SAP	SAP Fortify by HPE / MicroFocus
ABAP	SAP NetWeaver Application Server, add-on for code vulnerability analysis (CVA)

SAP Fortify 與 CVA 整合

Finding security issues at design time instead of in production is easier and less expensive!

百密一疏, 魔鬼躲在 AP 裡



84% of breaches exploit vulnerabilities in the application layer 被利用的資安弱點發生在應用層, 但是對於在網路周邊與應用層的資訊安全投資比率為 23-1。

- Gartner Maverick Research: Stop Protecting Your Apps; It's Time for Apps to Protect Themselves (2014)

Thank you.

Contact information:

Ying-Jie Chen
Director, Presales, SAP Taiwan
Mobile : +886-921179040
Email : +886-921179040

Run Simple

SYSTEX A DATA COMPANY

© 2018 SAP SE or an SAP affiliate company. All rights reserved.