



SAP S/4HANA 雲端資訊安全應用亮點

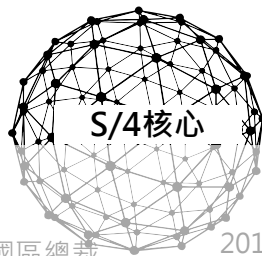
Ying-Jie Chen, Director, Presales

SAP Taiwan

January 16, 2018



SAP 雲方案整體架構

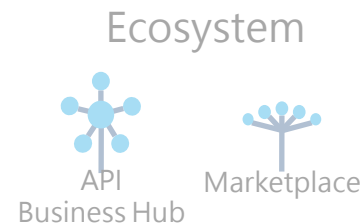


2016年12月，中國電信與SAP聯合簽訂戰略合作協定，發佈concur雲服務

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

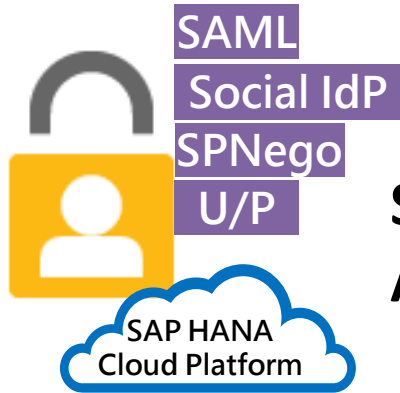


- 20億歐元投入
- 阿裡雲聯合生態合作
- 研究院成立專項團隊
- SAP Cloud Platform

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



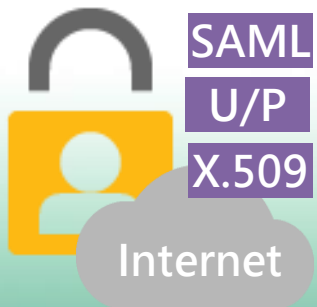
SAP Identity Authentication

- 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, ...



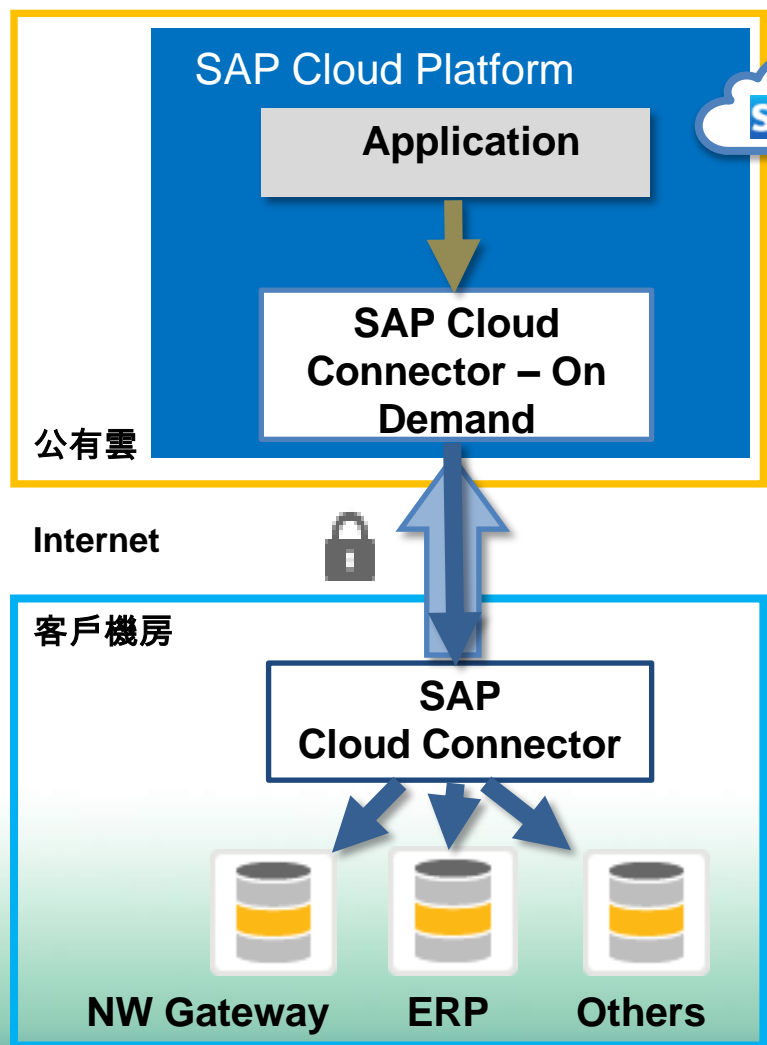
“SAP ID Service”

- 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

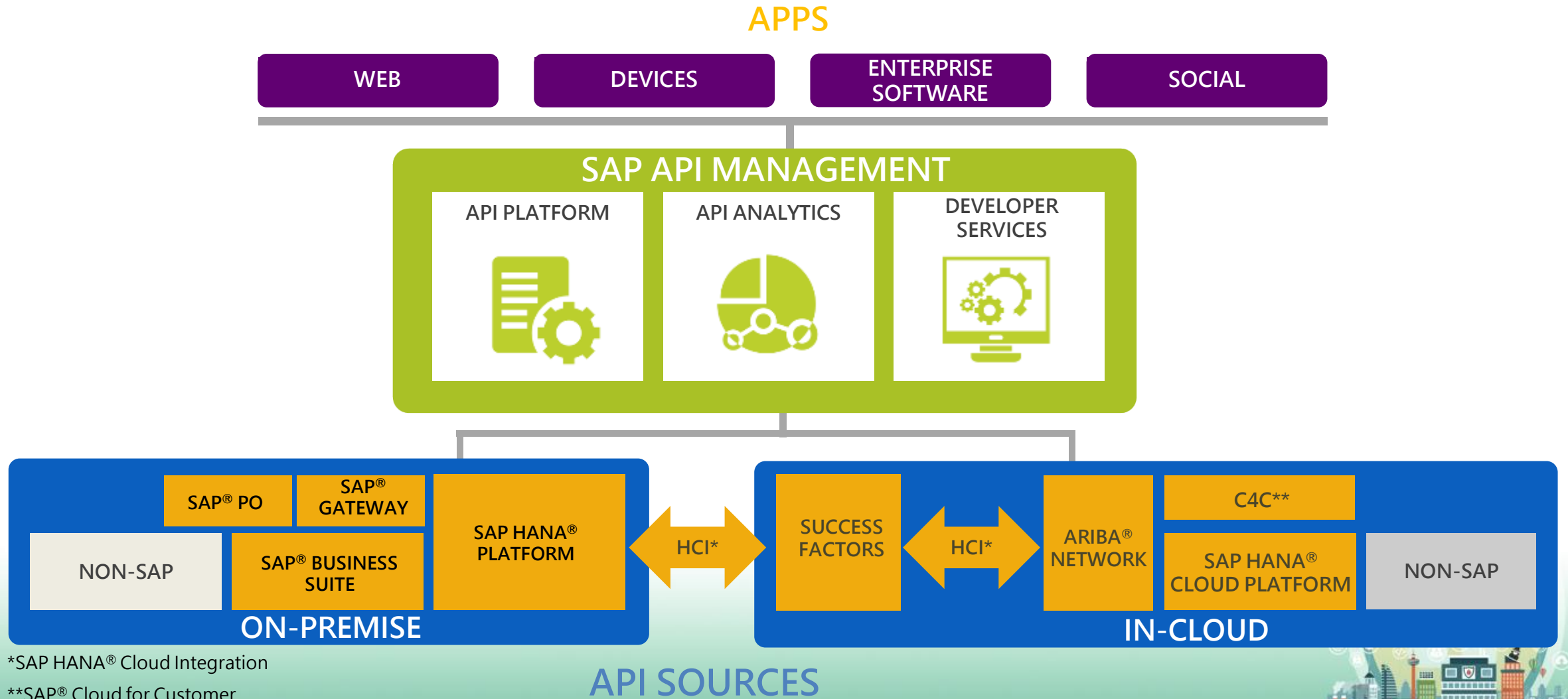


- 在 SAP Cloud Platform 與客戶機房系統之間，建立安全的 VPN 通道。
- 無須改動現有企業防火牆配置。
- 由機房內網啟動對公有雲的加密安全通道。
- 提供對客戶地端系統的安全訪問。
 - 詳細的 ACL 來管控雲端對地端資源的訪問權限。
 - 內建詳細的稽核歷史紀錄。
 - 採用基於 X.509 憑證的雲端與地端系統信賴關係。



SAP Cloud Platform 公有雲平台

API 管理服務 API Management Service



*SAP HANA® Cloud Integration

**SAP® Cloud for Customer

API SOURCES



SAP Cloud Platform 公有雲平台

API 管理服務 API Management Service



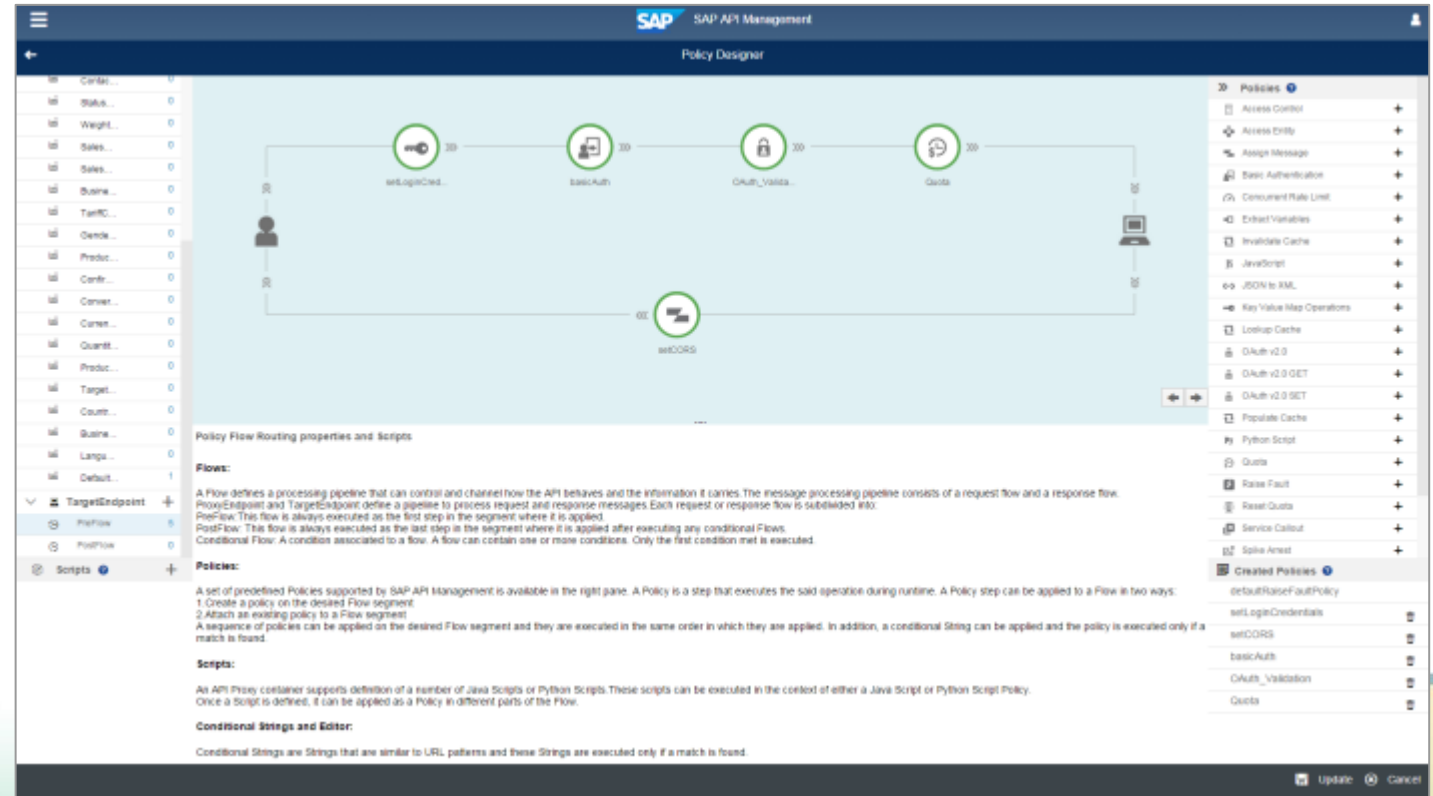
入侵威脅保護



認證與授權



基於角色的訪問控制

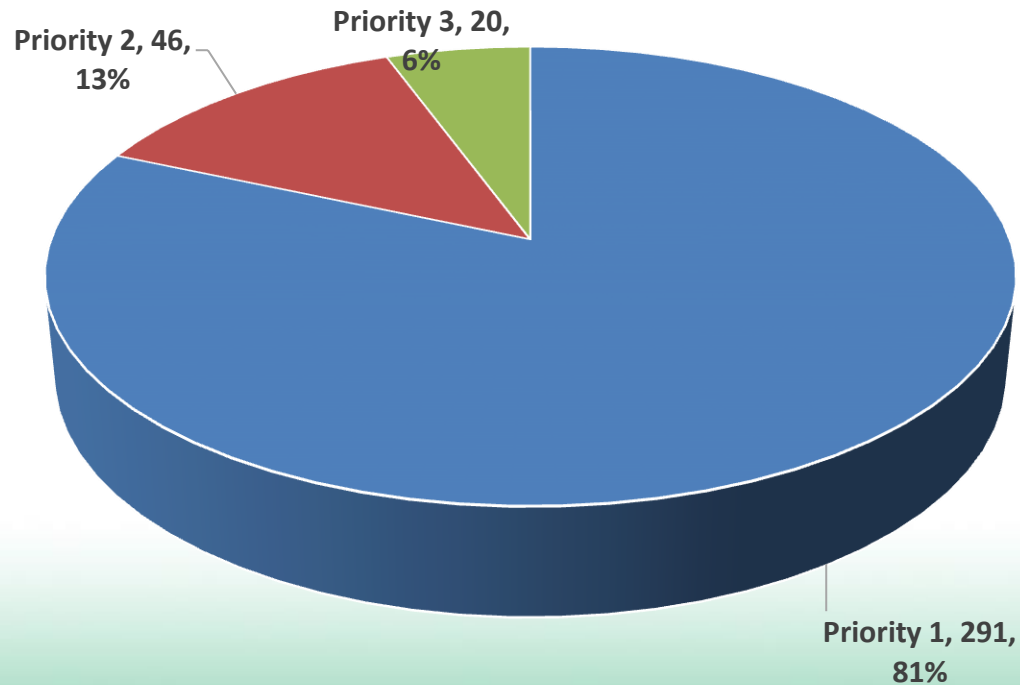


客戶案例

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, 在掃描 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
8  DATA: set_expr TYPE string,
9        user     TYPE kubname.
10
11 IF street IS NOT INITIAL.
12   set_expr = set_expr && ' STREET = ' && street && ' '.
13 ENDIF.
14 IF zipcode IS NOT INITIAL.
15   set_expr = set_expr && ' ZIPCODE = ' && zipcode && ' '.
16 ENDIF.
17 IF city IS NOT INITIAL.
18   set_expr = set_expr && ' CITY = ' && city && ' '.
19 ENDIF.
20 IF phone IS NOT INITIAL.
21   set_expr = set_expr && ' PHONE = ' && phone && ' '.
22 ENDIF.
23 IF set_expr IS NOT INITIAL.
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

Possible SQL injection (SET clause)

set_expr:
STREET = 'xyz'
salary = '1500'

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



開發生命週期資安端到端解決方案



non-ABAP non-SAP | **SAP Fortify** by HPE / MicroFocus

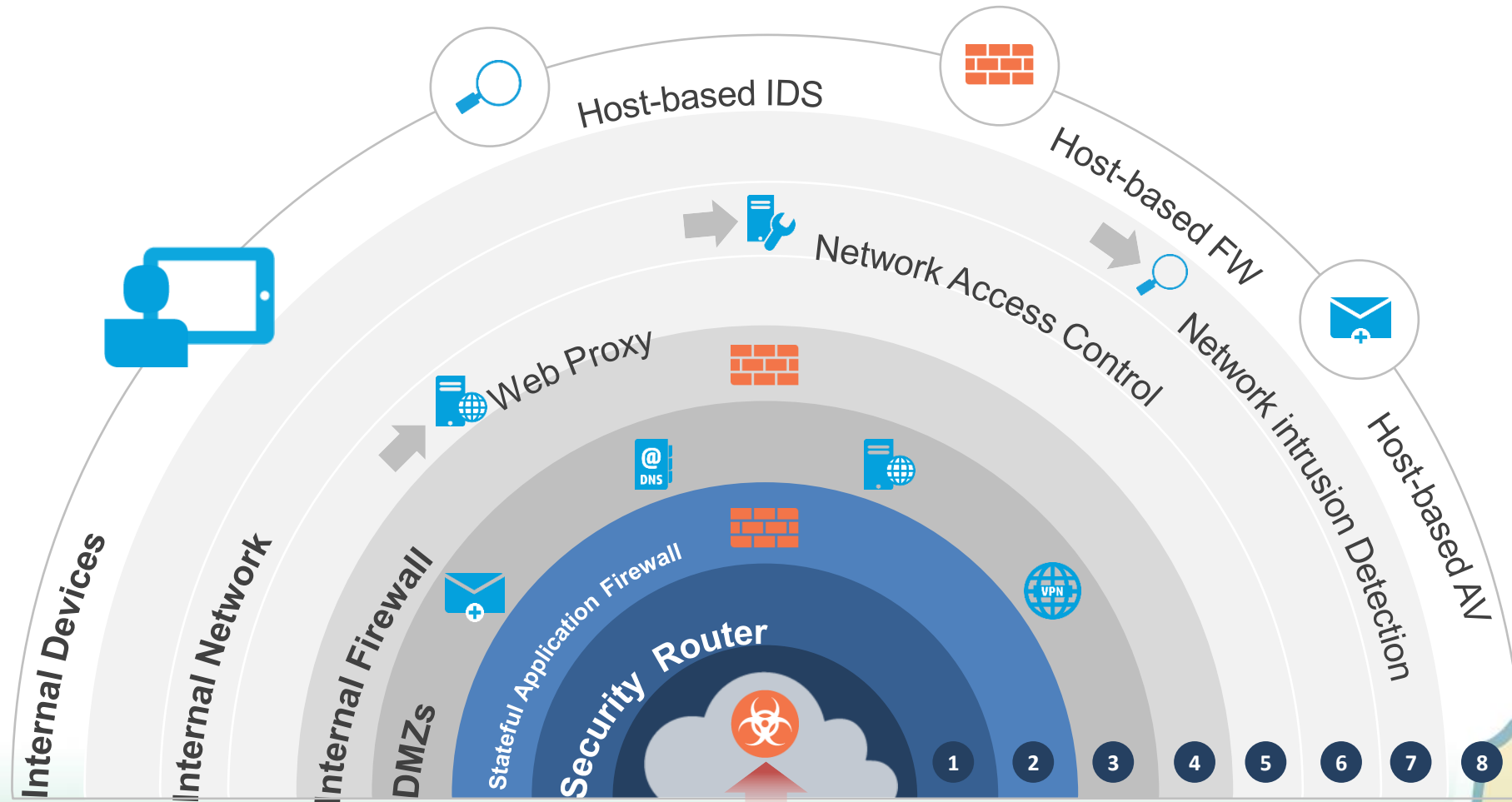
ABAP | SAP NetWeaver Application Server, add-on for code vulnerability analysis (**CVA**)

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



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

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE or an SAP affiliate company.

The information contained herein may be changed without prior notice. Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors. National product specifications may vary.

These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

In particular, SAP SE or its affiliated companies have no obligation to pursue any course of business outlined in this document or any related presentation, or to develop or release any functionality mentioned therein. This document, or any related presentation, and SAP SE's or its affiliated companies' strategy and possible future developments, products, and/or platform directions and functionality are all subject to change and may be changed by SAP SE or its affiliated companies at any time for any reason without notice. The information in this document is not a commitment, promise, or legal obligation to deliver any material, code, or functionality. All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, and they should not be relied upon in making purchasing decisions.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. All other product and service names mentioned are the trademarks of their respective companies.

See <http://global.sap.com/corporate-en/legal/copyright/index.epx> for additional trademark information and notices.

