

defendpoint

腰馬合一，從特權帳號
控管捍衛企業資安

Avecto Defendpoint

Privilege management **in hours, not months**

數位資安 翁嘉宏



Session Outline

Today we will ...

defendpoint

思考 端點在整體資安扮演的角色

檢視 現有的防禦措施

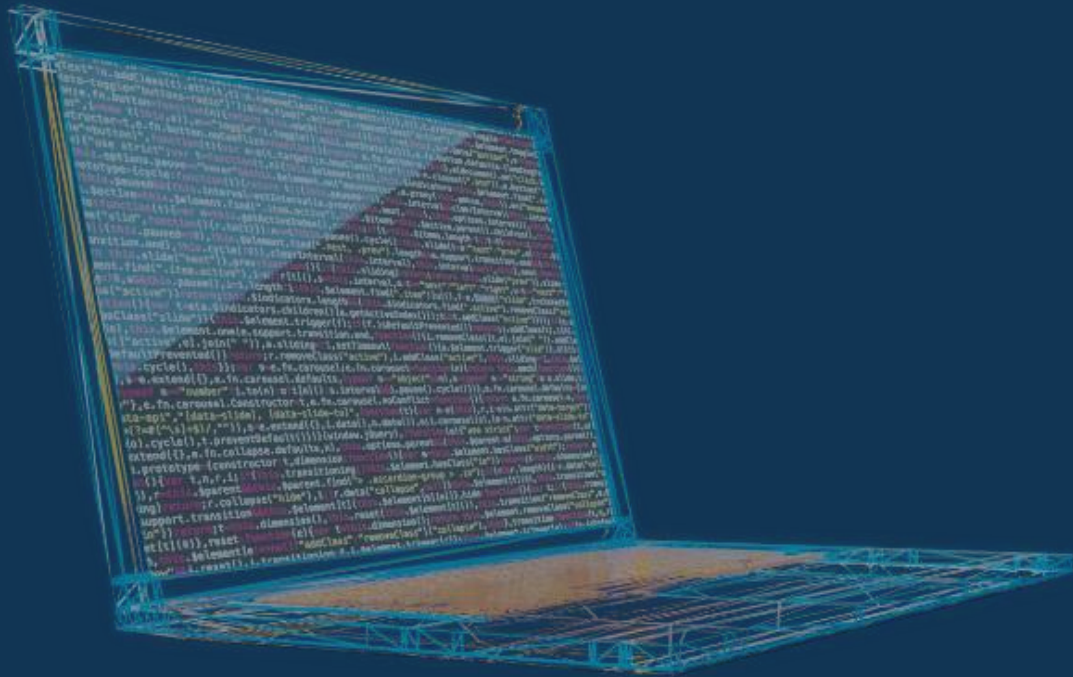
展示 不同的作法

討論 長治久安的策略

The Modern Endpoint

Why is it such a critical asset?

defendpoint



操作的便利性

常出差用戶

從端點發動的攻擊

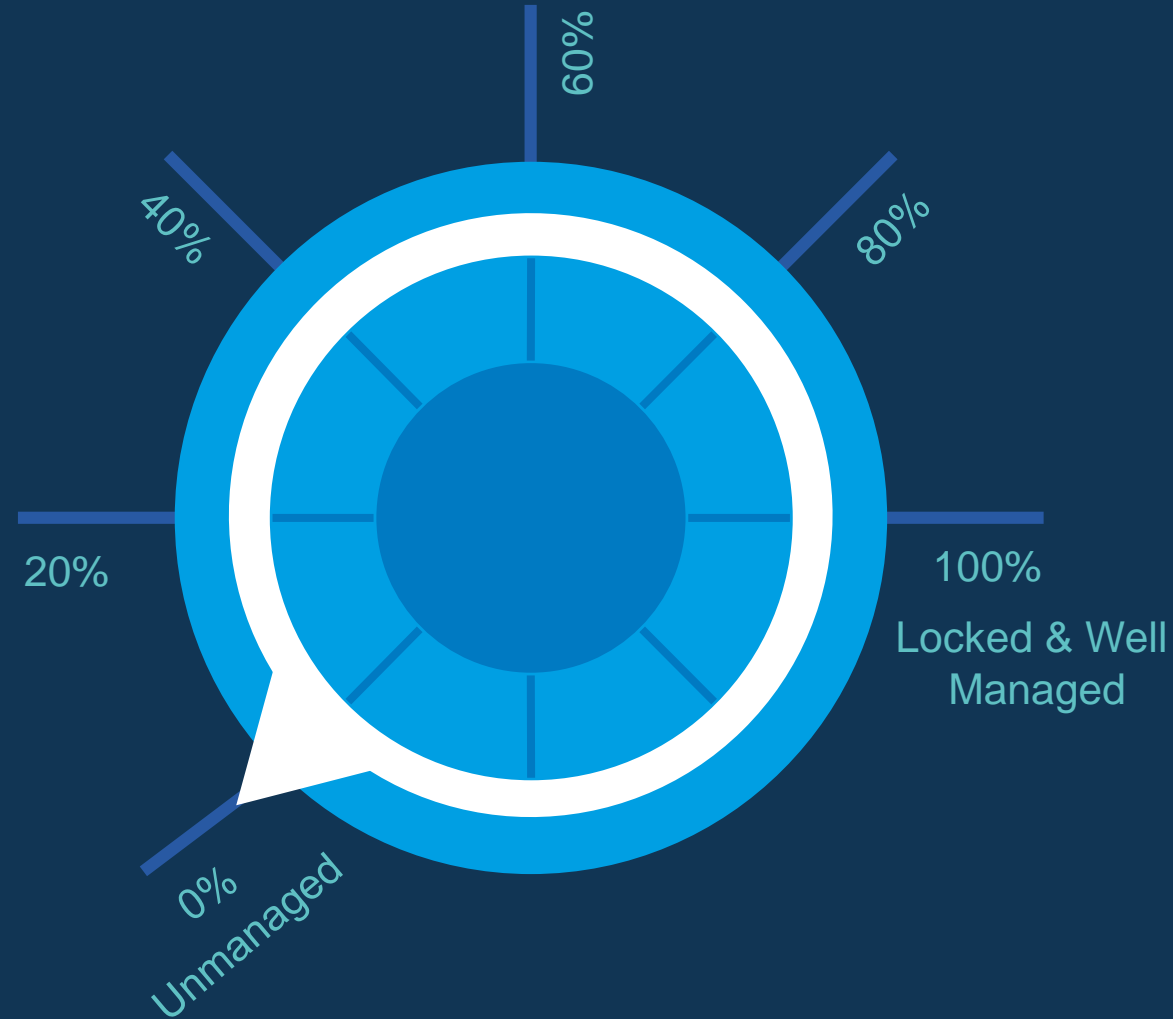
存取資料的入口

社交工程的重災區

Security Compromises

Why are the attackers winning?

- 導入安全性設定
- 定期安裝修補程式
- 保護昂貴的軟體, 或是高風險的行為
- 避免未知或是未允許的程式執行
- 使用最小權限作業



defendpoint

- 用戶希望自由的作業環境(就像自己的家用電腦)
- 系統的穩定和提供作業時間(UPTIME)是最重要的考量
- 用戶的生產力和效率必須維持
- 用戶需要彈性來執行新的和未被確認過的程式
- 用戶需要設定自己的作業環境和安裝軟體

Integrated Endpoint Protection

A proactive approach to security

defendpoint



Achieve Least Privilege



Whitelist the Good



Protect Trusted Apps

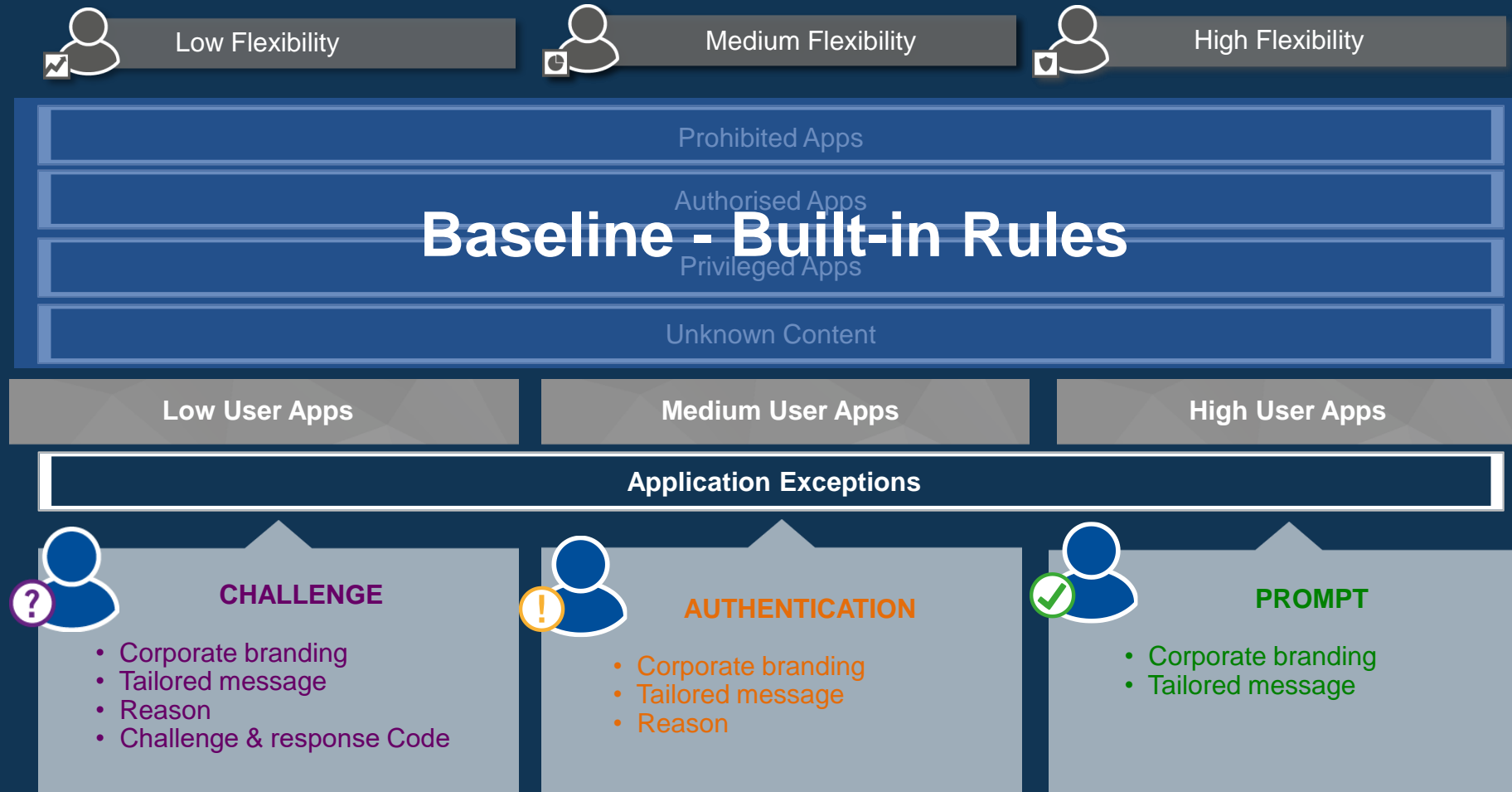


Gain Insights & Adapt

Quick Start

Policy overview

defendpoint



Quick Start

User roles

defendpoint

Low Flexibility Worker

數位資安管理政策

A Assistance Required defendpoint

即將執行的動作需要管理員權限，管理單位將記錄此事件，作為未來設定的依據，但不表示未來會持續允許。

Program Name	[PG_PROG_NAME]
Program Publisher	[PG_PROG_PUBLISHER]
Program Path	[PG_PROG_PATH]

Please provide a reason

Select a reason

Enter Response Code

To get a Response Code contact IT Support and quote the number shown on screen

4773 0992X → Code

OK Cancel

Medium Flexibility Worker

數位資安管控政策

A Reason Required defendpoint

即將執行的動作需要管理員權限，管理單位將記錄此事件，作為未來設定的依據，但不表示未來會持續允許。

Program Name	[PG_PROG_NAME]
Program Publisher	[PG_PROG_PUBLISHER]
Program Path	[PG_PROG_PATH]

Please select a reason

Select a reason

avecto-PC\avecto

Password

OK Cancel

High Flexibility Worker

數位資安管理政策

A Confirm Execution defendpoint

即將執行的動作需要管理員權限，管理單位將記錄此事件，作為未來設定的依據，但不表示未來會持續允許。

Program Name	[PG_PROG_NAME]
Program Publisher	[PG_PROG_PUBLISHER]
Program Path	[PG_PROG_PATH]

Yes No

Avecto Defendpoint: Customer Story : Successful Deployments

Putting theory into practice

Avecto's Deployment Methodology

Customer success stories

defendpoint

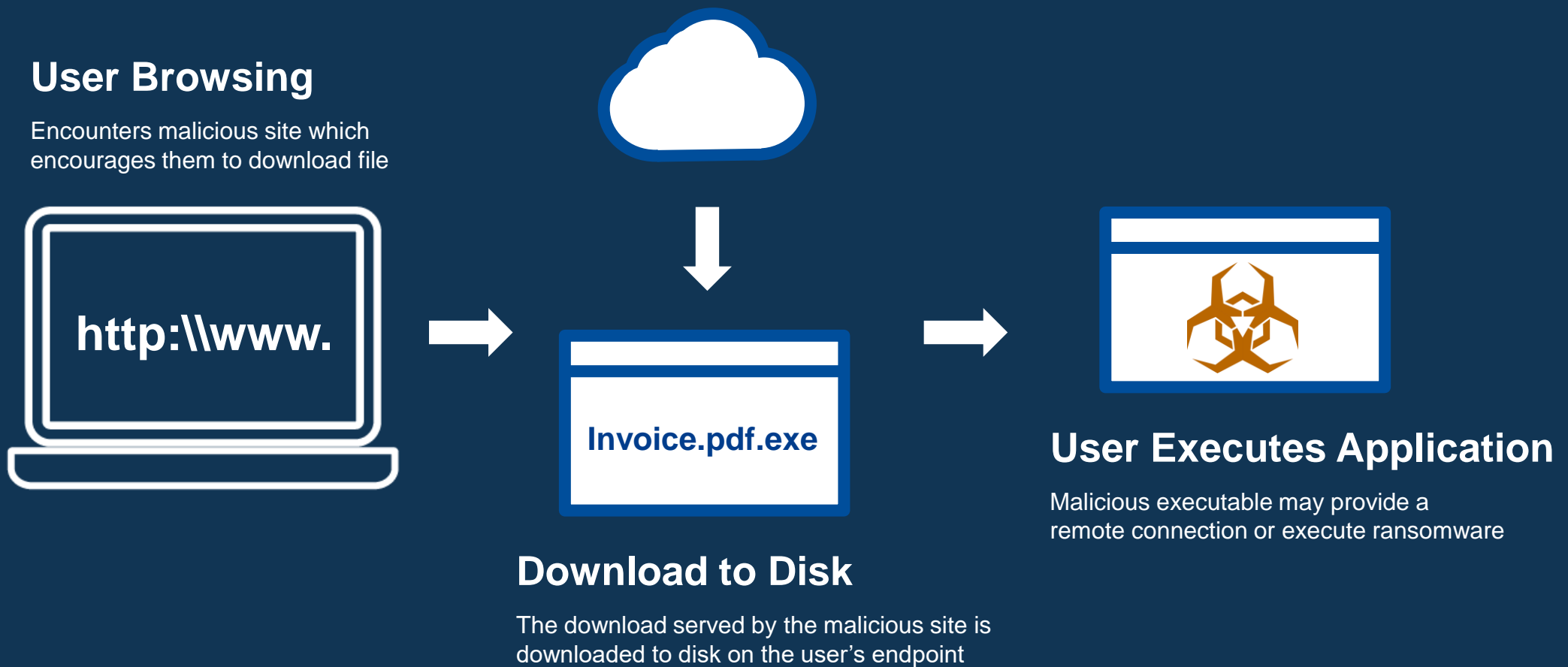
- - **Starting position:**
 - 20,000 machines 都用管理員權限在操作
 - 沒有任何應用程式管控措施
 - 用戶使用了錯誤的軟體版本
 - Helpdesk 平均每天收到 75 個電話
- - **After 6 months:**
 - 全部改用標準用戶登入
 - 稽核所有的程式操作紀錄, 即使是不使用特權的應用程式
- - **After 9 months:**
 - 全員進階到導入白名單控制機制
 - 沒有任何未知的程式可以被執行
 - 用戶都使用標準一致的軟體版本
 - Helpdesk 每天只收到1-2 電話



Traditional Malware

Example attack chain

defendpoint



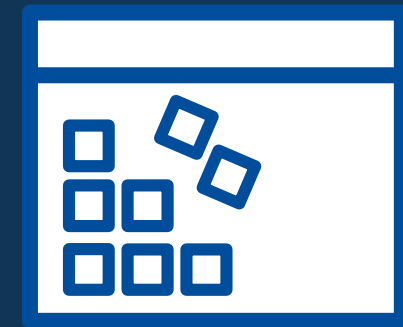
File-less Malware

Example attack chain

defendpoint

Phishing

Most common origin for attacks including ransomware and APTs



Malicious Content

Social Engineering & attacks against trusted apps



Persistence

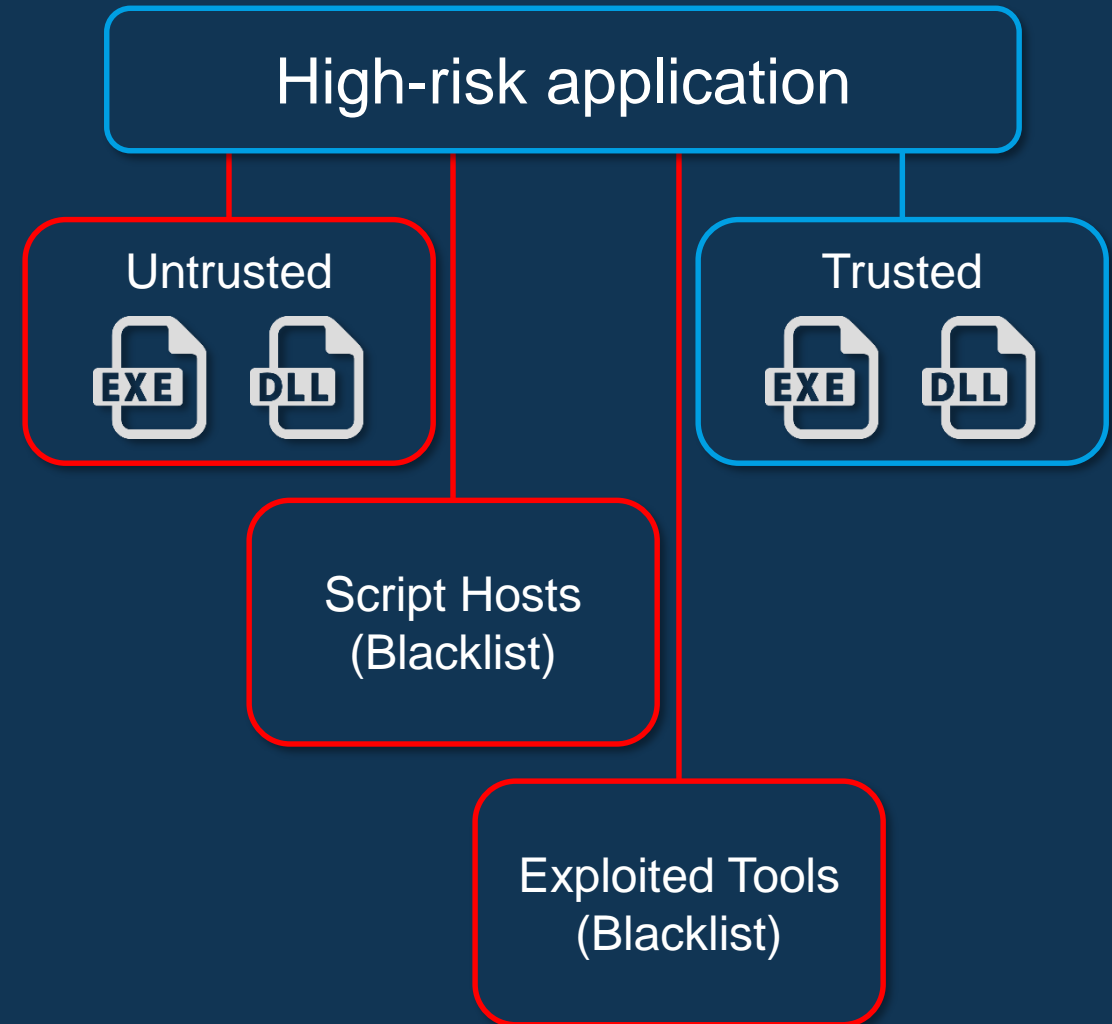
Establishes persistence mechanism to allow code to be re-launched after a restart

Trusted Application Protection (TAP)

defendpoint

Out-of-the-box protection of high-risk applications

- Targeted rules for highest risk applications
 - Web browsers 
 - Microsoft Office 
 - Adobe Reader 
- Blocks
 - All unknown & untrusted processes and DLLs
 - Native script hosts & commonly exploited tools
- Per-workstyle configuration
 - Lightweight, out-of-the box configuration
 - End-user warning messages
 - Auditing and reporting



Thank you

接下來的休息時間，
歡迎各位直接到後面的
攤位觀看會有DEMO。