OPSWAT.

DATASHEET

MetaAccess®

端點存取控管

若員工的筆記本型電腦使用過期或配置錯誤的防毒軟體，可能讓企業網路受到漏洞和惡意軟體攻擊。具有遠程設備的企業也需要依資安政策合規要求進行控管和可視化。

MetaAccess 能在您使用 Salesforce、Microsoft 365 等雲端應用服務前，先確保您的設備符合資安政策，同時在單一介面中提供企業整體的可見性。

可見性，管控性，合規性

自帶設備 (BYOD) 的大量使用讓企業的資安風險也隨之增加。設備密碼是否受保護？是否安裝防毒軟體？檔案是否有加密？設備是否中毒？

MetaAccess中控台提供企業整體的可見性，進而解決設備存取網路和雲端應用服務的管理問題。靈活的控管方式，可對整個生態系統進行政策修改，以阻擋單一設備。API 則提供設備對雲端應用服務的安全存取控管，並能直接整合到企業現有和舊有的安全解決方案中。

MetaAccess為存取網路和雲端應用服務的每台設備提供安全性、可見性和管控性。

效益

滿足合規要求
定義、執行資安政策；產出稽核文件和報告

創造整合綜效
將威脅檢測、漏洞偵測、稽核、合規性和事件回應等不同面向的解決方案整合到單一監控平台

防止資料外洩
端點存取控制可將惡意軟體感染風險和法規罰款可能性降至最低

低維護成本
自我修復功能(Self-remediation)可指引用戶自行解決問題

彈性部署
企業可視業務規模使用依需求付費的授權 (pay-as-you-grow licensing)

OPSWAT.

MetaAccess

產品特色

對已安裝應用程式、缺少或過期的OS patch進行端點**漏洞偵測**。

提供零時差攻擊等**威脅檢測**，並結合**30種以上的防毒引擎**和重複感染分析。

針對**5,000個以上應用程式**進行合規性檢查。

在CD、USB和行動電話等**可攜式媒體**被掃描完畢前，會阻擋用戶存取。

身份識別提供者(Identity provider)可與OKTA、Centrify等SSO服務進行開箱即用(out-of-the-box)整合。

單一、輕型的Agent可收集所有安全風險、**降低授權成本**、簡化整合需要並提升效能。

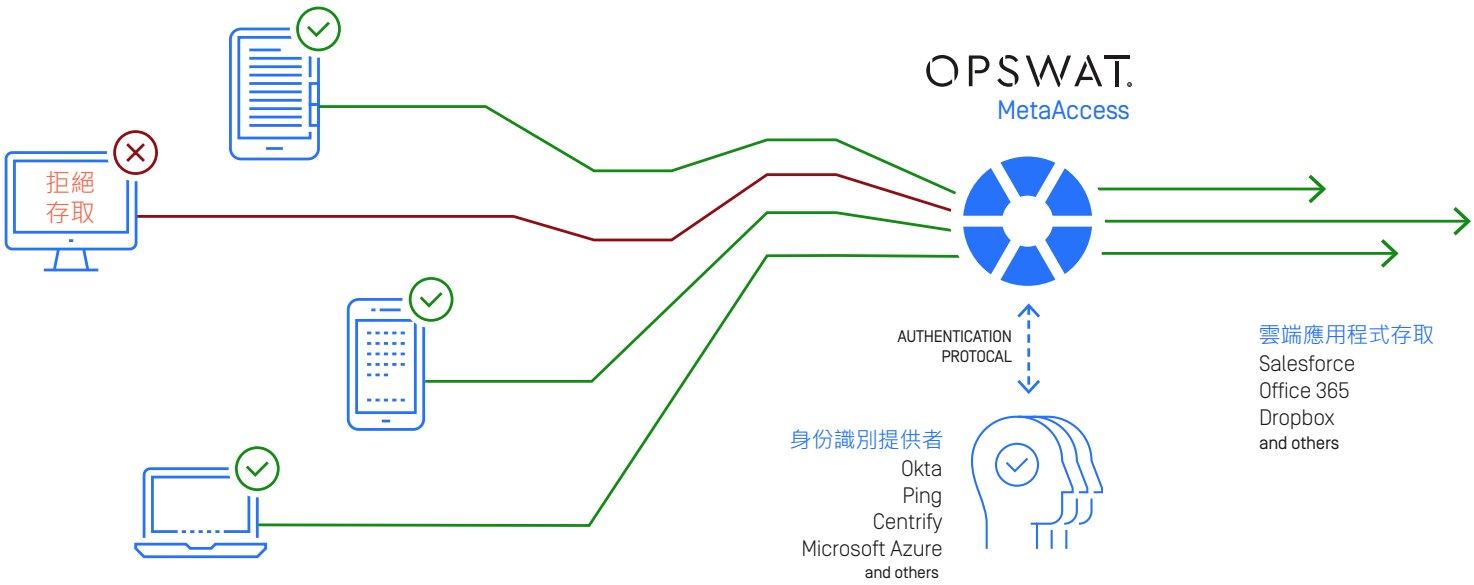
功能

- 細部執行組織政策
- 遠端診斷
- 可自行維護
- 可選電子郵件通知的事件Log輸出
- 支援 REST API，可整合到既有解決方案和客製化報告中

規格

用戶作業系統支援最小化

- **Windows**
  Windows 7, Windows Server 2008
- **Linux**
  - **Debian-based Linux v4 (15.4.x) Ubuntu 16/Mint 18/Debian 8**
  - **Red Hat-based Linux v4 (15.6.x) CentOS 7.14/Red Hat Enterprise 7/OpenSuse 11.4/Suse Enterprise 12.x/Fedora 27**
- **MacOS**
  OSX 10.9
- **iOS**
  iOS 8.3
- **Android**
  Android 5.1



OPSWAT.
Trust no file. Trust no device.