Extreme™
Customer-Driven Networking

Data Sheet

## 重點提要

### 符合業務需求

- 讓您的業務需求透過關聯導向的政策（Policy）來驅動網路
- 主動防範未經授權的使用者、遭入侵的端點與其他高風險的系統免於網路存取風險，達到保護企業資料的目的
- 安全地推動重要計畫，像是自攜設備與物聯網
- 有效地兼顧使用者、承包商與訪客所需的安全性與可用性
- 從網路邊緣到資料中心，導入一致的政策（Policy）
- 運用使用者數量計價模式，讓價格符合您的商業需求

### 存取安全性

- 依據關聯式身分識別資訊提供動態的角色網路存取控制
- 支援整合第三方解決方案，像是 NGFW、SIEM、CMDB、內部安全性與EMM / MDM
- 主動確保訪客存取與自攜設備上線的安全
- 內建的裝置分類可使用內建與外部歸類技術，支援整合 agent-based 和 anentless 的安全狀態評估服務
- 安全的物聯網網路存取

# Extreme 身份認證存取控制管理系統

運用端點安全性確保您的網路邊際安全無虞。

有鑑於大多數資料外洩事件都發生在端點裝置上，您需要一套細膩的使用者與物聯網裝置控制機制，並在整個網路與多雲端環境中施行一致的安全政策（Policy）。我們的存取控制解決方案讓您從簡單易用、操作彈性的中央控制面板，深入探究並掌控整個有線與無線網路的所有端點。

無論是自攜設備還是物聯網裝置，都能透過 Extreme 身份認證存取控制管理系統確保網路安全，防範各種外部威脅。它能讓您集中管理並定義精細政策（Policy），以符合法規遵循規範、地區設定，同時驗證目標原則並將之套用到使用者與裝置上。

## 精細政策（Policy）控制與深入能見度，確保您的網路安全

Extreme 身份認證存取控制管理系統讓您針對網路允許的端點使用者、型號、使用時機與使用地點套用精細控制。您可以依據裝置的安全防禦工事導入即時原則，以確保自攜設備、訪客存取與物聯網的安全。Extreme 身份認證存取控制管理系統將端點屬性進行比對，例如使用者、時間、位置、漏洞或存取類型，以建立全面性的關聯式身分識別。角色型身分識別則會跟著使用者移動，無論使用者從哪裡以哪種方式連線到網路，都能維持一致的識別資訊。這些識別資訊可用來實施高安全強度的存取原則。

## 簡便又安全無比的操作程序，讓訪客與物聯網裝置輕鬆上線運作

無須 IT 人員操作，我們的身分識別感知解決方案能夠自動管理訪客帳戶的到期日、帳戶有效性與時間控制。運用完善的自訂、品牌與協力商核准功能，讓訪客與自攜設備輕鬆又安全地上線運作

內建的裝置，使用不同的內部與外部歸類技術，可確保只有符合貴公司原則的裝置才能存取您的網路。使用者可以登入自己的 Yahoo 或 Salesforce 帳戶以完成訪客註冊手續。

## 運用進階報表與警示功能取得整個網路的能見度

Extreme 身份認證存取控制管理系統內建簡單易懂的控制面板，讓您輕鬆監控網路上的問題。此功能可讓您針對驗證、訪客存取、上線作業、裝置分類與驗證，乃至於終端系統運作狀況自訂進階報告與警示，完成設定後即可自動發送這類報表與警示給您。