# 看見每個裝置
# 看見每個連線

## 專為企業物聯網所設計的非侵入式安全防護

大部分企業都看不到自身環境中 40% 以上的設備。無論是否受到控管，對企業而言，辨識周遭的所有裝置並為自身做好防護都相當困難。Armis 能發掘您環境中的所有設備與相關風險、偵測威脅，並自動保護您的重要系統與資料，特別是未受控管的設備。

### 連網設備數量激增

未控管設備在工作場域正以前所未有的規模激增，這場數位轉型的規模甚至超過了個人電腦與智慧型手機革命的總和。未控管設備的品項包羅萬象，從傳統的筆記型電腦和智慧型手機，到智慧電視、監視攝影機、智慧燈具、數位助理、智慧空調系統、智慧家電、醫療裝置、製造設備等，全都含括在內。

每年進入企業的未控管設備數量都以 31% 左右的速率成長。2020 年，這些設備在企業中的數目預估會成為傳統電腦的 5 倍之多。雖然這些連線設備有助於達成更高的生產力，但同時也創造了更大的風險。

這些設備大部分都沒有防護、很難或無法升級，企業無法監看或管理。傳統的防火牆、網路安全及 EDR 端點防護解決方案皆無法因應，這一切都會為您的資安團隊帶來重大的問題。

### Armis 設備資安管理平台

Armis 是第一個無須安裝代理程式的企業級資安管理平台，可因應未控管設備及物聯網設備帶來的全新威脅型態。我們能找出所有受控管、未控管及物聯網設備（無論是連網或斷網），分析裝置行為並辨識風險或攻擊，進而保護您的關鍵業務資訊及系統。Armis 平台無須安裝代理程式，並能輕鬆與您既有的資安產品整合。

## Armis 平台

**全面性**
查找並分類您環境中的所有設備，無論設備是連網或斷網。

**非侵入式**
無須在裝置中安裝代理程式、無須設定，也無須將裝置停機。

**被動式**
不影響企業組織網路。
不會進行裝置掃描。

**無縫接軌**
數分鐘內即可在企業既有基礎架構下完成安裝。

Armis 被動式監控您的網路及空域（airspace）中的有線及無線流量，在不造成中斷的情況下辨識所有設備並瞭解每個設備的行為。接著資料會在我們的風險引擎（Risk Engine）中進行分析，這個引擎會運用來自 Armis 設備知識庫（Armis Device Knowledgebase）的設備檔案與特徵資訊，辨識每個設備、評估其風險、偵測威脅，並提供建議的補救方案

## 關鍵設備洞察

Armis 設備知識庫追蹤超過2億3000萬個設備，並持續增長中。

## 資產清單

可視性對所有組織的安全策略而言都是重要的基本要素，若您的組織需遵守 PCI DSS、HIPAA、NIST 或 CIS 關鍵安全控管等架構，您也會被要求維護環境中準確的軟硬體設備清單，這件事說起來簡單，做起來卻很難。

Armis 能查找並分類環境中所有受控管、未控管及物聯網設備，包括伺服器、筆記型電腦、智慧型手機、VoIP 電話、智慧電視、網路監視攝影機、智慧空調系統、醫療裝置、工控裝置等設備。Armis 甚至能辨識環境中使用 Wi-Fi、藍牙及其他物聯網協定的離線裝置—沒有任何其他資安產品能在不使用傳統硬體的前提下提供這項功能。

Armis 所生成的整合性設備清單包含各種關鍵資訊，如製造商、型號、序號、位置、使用者名稱、作業系統、已安裝應用程式，以及依時間先後進行的連線行為。

除了查找並分類設備外，Armis 還能根據弱點、已知攻擊模式以及每個設備在網路上所被觀察到的行為，自動計算設備的風險分數。這個風險分數能幫助您的資安團隊瞭解您的攻擊受面，並完成法規框架對漏洞辨識和重要性排序的合規要求。

## 風險管理

Armis 能做的不單是設備及風險辨識。Armis 威脅偵測引擎（Armis Threat Detection Engine）能持續監控網路中每個設備的行為，以及空域中的異常行為。結合設備知識庫，Armis 還能將每個設備的實時行為與下列項目進行比較：設備在網路上所被觀察到的行為，自動計算設備的風險分數。這個風險分數能幫助您的資安團隊瞭解您的攻擊受面，並完成法規框架對漏洞辨識和重要性排序的合規要求。

- 設備歷史行為記錄
- 環境中類似設備的行為
- 其他環境中類似設備的行為
- 常見攻擊方式
- 來自威脅情資的資訊

結合這些關鍵設備與行為洞察的分類，讓 Armis 處於辨識威脅、攻擊並採取相對行動的獨特地位。

## 偵測及回應

當 Armis 偵測到威脅時，會向您的資安團隊發出告警，並自動觸發防護行動以阻擋攻擊。藉由與交換器、無線區域網路控制器、既有安全防禦設備，如 Cisco、Palo Alto 防火牆，以及網路存取控管設備（Network Access Control，NAC），如 Cisco ISE、 Aruba ClearPass 等產品的整合，Armis 可限制存取或隔離可疑或惡意的裝置。這些自動防護將阻擋對所有設備的攻擊，無論是受控管或未控管，即使資安團隊忙於其他優先事項時，您也依然能高枕無憂。

## 無縫接軌的整合

Armis 無須部署其他代理程式或其他硬體，因此能在幾分鐘到數小時內完成建置，不只能與防火牆或 NAC 整合，也能與您的資安管理系統整合，如 SIEM、自動派工系統、資產管理資料庫等，讓這些系統及事件回應者能運用 Armis 所提供的豐富資訊。

## 關於 Armis

Armis 是全球第一個非侵入式的（agentless）、企業級的設備資安管理平台，可因應未控管和物聯網設備的新威脅。《Fortune》1000 大企業都信任 Armis 獨特的頻外（out-of-band）感測技術，可查找、分析所有受控管、未控管及 IoT 設備，從傳統設備，如筆記型電腦、智慧型手機，到新的未控管智能設備，如智慧電視、網絡攝影機、印表機、HVAC 系統、工業設備機器人、醫療設備等。Armis 會查找線上及離線的設備，持續分析端點行為以辨識風險和攻擊，並透過識別、隔離可疑或惡意設備，保護關鍵機敏資訊和系統。Armis 是總部位於加州 Palo Alto 的私人公司。

1.888.452.4011
armis.com