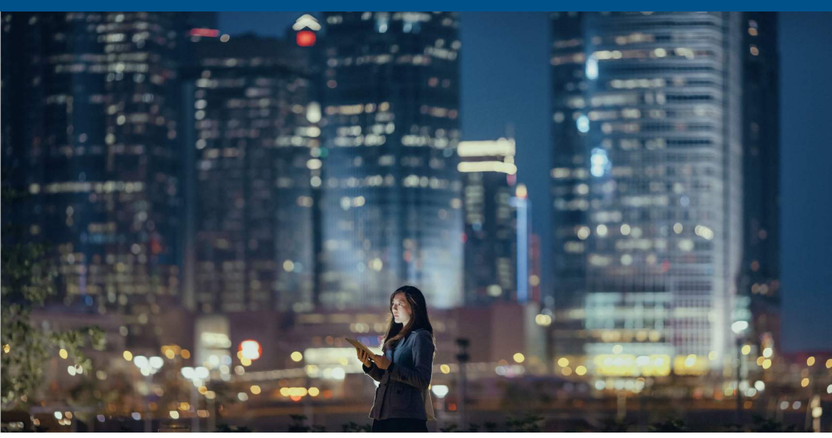
網路安全成為聯網生態系統普及化的首要考量

隨著先進科技的快速部署點燃更多商機，聯網生態系統的安全維護愈顯重要。網路安全是企業領導者最關注的核心。



70%
的受訪者表示，防範網路安全漏洞[1]是推動創新的驅動力之一。

59%
的受訪者表示是為了符合安全法規[2]。

科技變革帶來網路安全新挑戰

時代變遷加速跨應用程式的使用技術，網路安全可能帶來的影響包括：

物聯網 (IoT) 加速普及

預估至 2030 年，全球將有
500億台
物聯網裝置[3]。

這將提供給駭客無數易受攻擊的智慧裝置，藉此入侵重要產業，諸如運輸、醫療、國防或製造業。

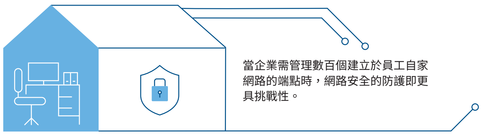
新世代行動網路

預計至 2021 年底，全球將有
2億9千萬台
使用 5G 網路的裝置[4]。

新世代的行動網路將制定全新的基礎架構，卻也產生新的網路安全漏洞。

遠端存取普及化

88%
的企業因受新冠肺炎疫情影響，鼓勵或要求員工在家上班[5]。



當企業需管理數百個建立於員工自家網路的端點時，網路安全的防護即更具挑戰性。

如何提升聯網生態系統的安全

清點數位資產

確認哪些是最重要的資料，位在何處，並評估資料外洩的後果。一旦企業提前意識到安全漏洞的隱憂，即可事先保護企業關鍵資料和 / 或評估資料外洩帶來的損害。

2019 年上半年度，受網路攻擊造成個資外洩達
4.1 億筆[6]

保護網路生態系統

針對供應鏈與整個企業系統提升防護，或至少了解有哪些弱點。

40%
的安全漏洞來自企業生態系統的弱點[7]。

偵測

利用端點偵測與回應 (XDR) 工具，自動偵測並製作潛在漏洞的詳盡清單。

60%
的管理者認為在自動化、機器學習、人工智慧與協同合作的投資，有助提升企業網路安全的防護[8]。

因應

擬定事件發生的反應機制，一旦資料外洩即能立即評估、迅速採取措施並清楚地溝通，才能降低損失、控制成本並保護品牌。

77%
的企業並未針對企業的網路安全擬定因應計劃[9]。

探索更多聯網生態系統的趨勢 UL.com/Insights

資料來源：
1– UL, Innovation survey, 2019.
2– UL, Security concerns escalate as IoT expands, 2019.
3– Statista, "IoT connected devices worldwide 2030," February 19, 2020.
4– Statista, "Forecast number of 5G connections worldwide by region from 2021 to 2025," 2019.
5– Gartner, HR Survey, March 19, 2020.
6– CyberRisk Analytics, "2019 MidYear QuickReview data Breach Report," August 2019.
7– Accenture, "2019 State of Cyber Resilience," 2019.
8– IBM, "2019 Ponemon Institute Study on the Cyber Resilient Organization," April 2019.
9– IBM, "2019 Ponemon Institute Study on the Cyber Resilient Organization," April 2019.

Empowering Trust®