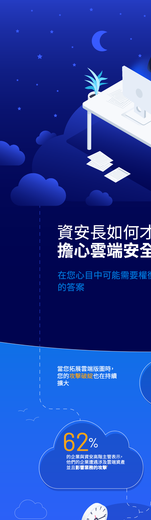
tenable



資安長如何才能不再擔心雲端安全並高枕無憂

在您心目中可能需要權衡的最重問題的答案

當您拓展雲端版圖時，您的[攻擊面](#)也在持續擴大

92%

的高階主管表示，**在過去12個月當中**，他們已注意遭遇過影響嚴重的網路攻擊或入侵事件

62%

的主要資安決策者主管表示，**他們內部**有意或非主意地成為**主要**影響嚴重的攻擊



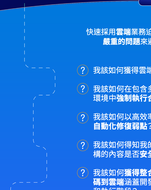


74%

受訪中被問到未來兩年的企業投資方向時，76%的安全主管都為雲端基礎架構平台

$900 億美元

相較於 2021 年，IDC 預測 2022 年的雲端基礎架構支出將成長高達 31.7%，達到 900 億美元



快速採用**雲端**架構迫使您難以克服這些**龐雜的問題**來避免資料外洩：

- 我該如何獲得雲端環境的**完整能見度**？
- 我該如何在包含多個控制點的雲端環境中**強制執行合規性與監管工作**？
- 我該如何以高效率且有成效的方式**自動化修復錯誤**？
- 我該如何得知我的開發人員正在建構的內容是**安全**？
- 我該如何**獲得整合式安全性**，從**程式碼到雲端**，並跟開發人員的建構程序和執行階段？



簡言之，您要如何在整個雲端基礎架構中找到弱點並加以修復？

您必須**適應並延伸**企業的弱點管理功能，**深入並進一步**運用在雲端堆疊和建構程序。

方法

利用提供下列功能的全方位解決方案：



全面檢視您所有的資產和雲端作用中的工作負載，以及檢視其**弱點和設定錯誤**



偵測、預防及強制執行合規要求



直接並快速修復 IaC（基礎架構即程式碼）佈建基礎架構



整合安全性，延伸回建構程序和生產環境

高枕無憂 tenable.cs cloud security



透過端對端、回應和修復，您即可擁有**完整能見度**和**掌控度**，從程式碼到雲端保護您的整個雲端基礎架構。



電子書

按一下以下載

[資料來源]「調查之外」三方供給公司代表網路安全決策者進行調查，該調查在線包含 [Tenable Cloud Security](#) 的2021年3月執行。

[資料來源] IDC 全球雲端支援基礎架構組織：回應雲端雲端架構 2020 年第 4 季。

Hi! How are you looking for a solution to help manage cloud entitlements and cloud risks?

版權所有 2022 TENABLE, INC. 保留所有權利。TENABLE、TENABLE.IO 和 NESSUS 為 TENABLE, INC. 的註冊商標。TENABLE.SC、LUMIN、INDEGY、LUMIN LEGEND、ASSURE 和 THE CYBER EXPOSURE COMPANY 為 TENABLE, INC. 的商標。所有其他產品或服務為其各自所有者的商標。