生成式 AI 七大商業用例與資安風險

生成式 AI 使用案例在企業各層面差異甚鉅，一如它們帶來的資安風險。

文／Michael Hill　譯／Nica

生成式 AI 商業使用案例，隨著該項技術滲入各種產品、服務與科技而不斷成長。與此同時，不斷進化生成式 AI 能力造成的資安影響持續成為新聞頭條。近期對 500 位資深 IT 領導者進行的 Salesforce 調查報告揭露，還是有絕大多數（67%）調查對象在未來十八個月優先考慮將生成式 AI 用於商業營運。幾乎所有人都承認，需要額外措施處理資安問題，讓企業本身具備充份利用這項技術的能力。

大部份企業會購買（不是建構）生成式 AI，其中更多不是直接購買生成式 AI，而是透過綁在一起的整合性產物接受它。這讓資安領導者不得不花時間瞭解各種不同生成式 AI 在所處商業行為的使用案例，與其相關風險。

Forrester 新一份報告還揭露：最可能採用生成式 AI 的是業務部門、它們首要使用案例，以及隨這項技術漸成主流，資安威脅與風險團隊所需的防禦。

最可能的生成式 AI 七大商業使用案例

據 Forrester 保障生成式 AI 安全的報告指出，企業組織最可能的生成式 AI 使用案例有七個面向，與之相關的資安威脅與風險如下：

一、行銷：文字生成器讓行銷人員能瞬間產生行銷活動粗略草稿。Forrester 表示，此舉會導致資料外洩、資料滲透與競爭情報威脅。帶來的風險則是釋出前疏於勘誤釋出內容並進行處理，而衍生相關客戶/公關議題。

二、設計：影像生成工具激發設計師靈感，只要花點時間與努力就能成就想法雛型，Forrester 如此寫道。它們還可以整合到廣泛工作流程。這會導致模型投毒、資料篡改與資料完整性威脅。要考量的風險則是因資料完整性與生成內容潛在「版權 / IP」議題，而導致未依循設計約束與政策。

三、IT：程式設計師使用大型語言模型（LLM）尋找程式碼錯誤，並自動生成文件。這會導致資料滲透、資料外洩與資料完整性威脅，產生的文件可能冒險曝露公司正規不揭露的重要系統細節。

四、開發人員：TuringBots 有助於開發人員撰寫原型程式碼，執行複雜軟體系統。據 Forrester 所述，這會帶來程式碼安全性、資料篡改、勒索軟體與 IP 竊取問題。可能風險則是未依循 SDLC 資安實作的不安全程式碼、違反智慧財產權許可要求的程式碼，或生成式 AI 遭勒索產物系統危害。

五、資料科學家：生成式 AI 讓資料料學家可以在不危及個人資訊前提下，產生與共享訓練模型資料。此舉易導致資料投毒、資料反混淆（deobfuscation）與對抗式機器學習威脅。合成資料生成模型的相關風險則是逆向工程「允許對手識別使用資料的來源」。

六、銷售：AI 生成內容協助銷售團隊提出構想，

以周延的語言建立新內容。這會帶來資料篡改、資料滲透與監管單位合規性威脅。「銷售團隊生成與分發內容時，可能違反聯絡偏好設定。」

七、營運：內部營運利用生成式 AI 提升組織智慧。這將引發資料篡改、資料完整性與員工體驗的威脅。Forrester 指出，風險在於：用於決策制定程序的資料可遭篡改，從而導致錯誤結論與誤導施行措施。

供應鏈、第三方管理，對確保生成式 AI 安全很重要

Forrester 的生成式 AI 最可能的商業使用案例清單，雖然著眼於內部營運，但也敦促資安領導者不要忽視供應商與第三方風險因子。「有鑑於大部份企業組織發現生成式 AI 已整合在佈署的產品與服務上，資安領導者當務之急就是第三方風險管理。」他寫道。當公司企業購買內含生成式 AI 的產品或服務，就仰賴供應商保障解決方案的安全了。「微軟與 Google 將生成式 AI 綁定 Copilot 與 Workspace 這類服務時就負有責任，但其他供應商是從自有供應體系取得 AI 解決方案。資安單位，必須依上述使用案例為基礎，編制自有的一套供應商安全性與風險管理的提問。」