預測 #9

資安事件的數量將增加100倍，
避免、偵測與減緩資安威脅
最為可靠的方法是自動化。

預測 #9

當今企業每天都面臨著巨量的資安事件。這樣的情況使得即時優先存取與問題排除成為特殊挑戰，因為每個資安事件都需要進行個別評估，再加以採取措施或忽略。

《2018年Oracle與KPMG雲端威脅報告》中，受訪者提出的首要挑戰，是對資安事件的遠端遙測進行規模分析。McAfee的《2019雲端採用與風險報告》（Cloud Adoption and Risk Report）也進一步強調此點，表示企業組織平均只會在一億個事件中發現一個威脅。那麼資安團隊如何在這些諸多干擾中辨認出真正的威脅呢？

到2025年，惡意流量將利用AI隱藏在大量常規和合法的人為流量之中。惡意使用者將運用非線性（通常以AI為基礎的）科技，為殭屍網路行為模式注入隨機性，來發動數量前所未有、極度難以偵測的資安攻擊。

我們預測，未來企業組織也必須運用基於雲端的AI技術，來協助防禦這些威脅。抵禦高度自動化攻擊者網路之最有效的方式，是讓企業將資安事件的大規模分析轉交給橫跨整個企業IT範圍的數個智慧型AI驅動分析平台。

我們期望到2025年，許多企業都採用核心到邊緣的安全模型，以確保顧客的數據從基礎設施的核心到雲端的邊緣都能獲得安全保障。

延伸閱讀

電子書：Cloud Security for Dummies（雲端資安手冊懶人包）

IPaper：Cloud Essentials: Secure and Manage Hybrid Clouds（雲端基礎教學：保護與管理混合式雲端）

評估工具：Take the Cloud Security Assessment（進行雲端安全評估）

試用 Oracle 雲端平台 →