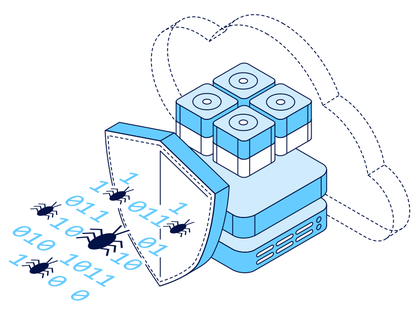
亞太和日本地區版本

2022年

勒索軟體趨勢報告

在 2022 年 1 月，一家獨立研究公司完成了一份針對 1,000 家公正 IT 導廠商的調查，內容是關於勒索軟體對他們環境的影響，以及他們的補救措施與未來應對策略。 受訪者包含以下四種人員：資訊安全長、安全性專業人員、備份管理員以及 IT 營運人員。 這些人員代表來自亞太和日本地區、歐洲、中東和非洲以及美洲 16 個不同國家/地區的各種規模的組織，包括來自亞太和日本地區的 200 人。

勒索軟體猖獗



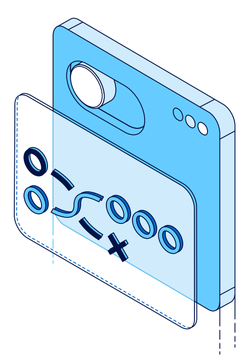
97%

的勒索軟體攻擊嘗試感染備份存放庫，其中 **73%**的攻擊嘗試得手了

52%

的營運資料遭到加密，但其中只有 **68%** 的資料可復原

贖金 ≠ 補救措施



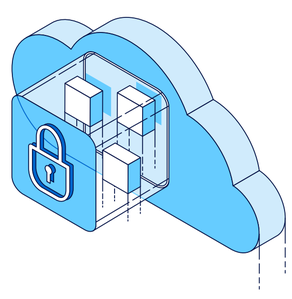
18%

的組織並未支付贖金就能復原資料

36%

的組織支付贖金後，仍然無法取回其資料

存活所需的技術



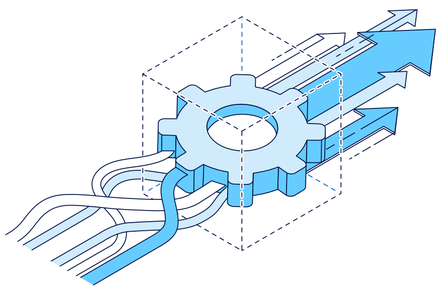
84%

的組織仰賴備份記錄或媒體可讀性來確保資料復原能力，這表示只有 **16%** 的組織會定期透過還原和測試功能來進行測試

41%

的組織在受到勒索軟體攻擊後，先將資料還原至隔離沙箱，再復原資料

組織調整



55%

的組織認為在備份與網路安全之間需要進行完整或重大的改造

29%

的網路團隊勒索軟體教戰手冊包含驗證或保證乾淨度要求

安全備份是您的最後一道防線

勒索軟體是一場災難，每次事件都要讓企業花費將近兩百萬美元 (美國)。Veeam® 公司認為面臨勒索軟體攻擊，安全備份是您的最後一道防線。 我們軟體的資安設計可杜絕綁定專屬硬體與您現有架構 (包含內部部署和雲端) 的情況，因為擁有可靠的備份可以決定停機、資料遺失和支付鉅額贖金的差異。

了解詳www.veeam.com/tc-tw

在此下載完整研究報告