OPSWAT.

使用案例

檔案無毒化：
預防已知和未知的威脅

OPSWAT深度內容威脅解除和重建技術 (Deep CDR)，也稱為檔案無毒化，透過消除檔案中可能存在的惡意內容和中和惡意軟體，積極預防包含已知和未知威脅的檔案威脅。

僅依靠基於偵測的反病毒引擎並不總是足夠的。對於零信任的方法，使用者需要有Deep CDR這樣基於預防的技術。OPSWAT Deep CDR具有四種模式，分別設計用於不同的使用案例。

使用案例

使用案例1：

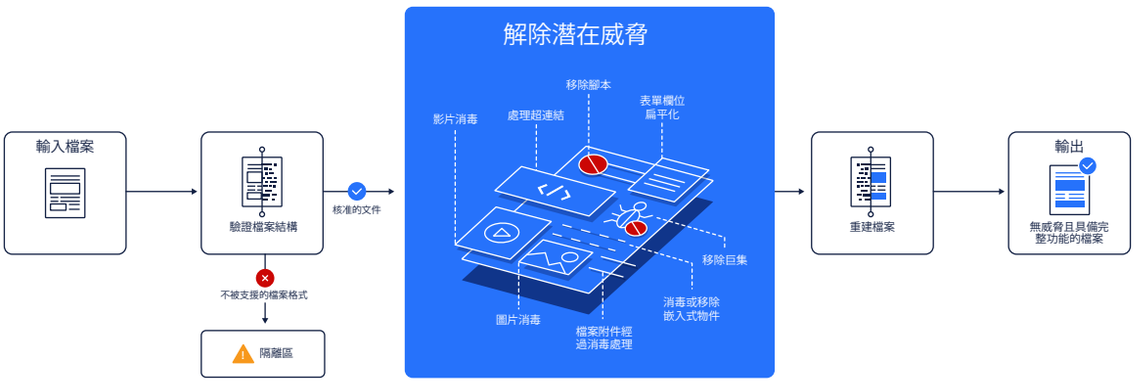
保護使用者免受惡意檔案侵害，同時維持工作流程

深度內容威脅解除和重建模式

深度CDR可在毫秒內提供經過消毒的檔案，讓網路管理員在保持工作流程的同時保護使用者免受惡意檔案的侵害。

深度CDR可移除所有動態內容，例如超連結、嵌入式媒體、腳本、巨集等，而不會影響檔案文字內容的完整性（重建）。

這是Deep CDR最受歡迎的使用案例，其中所有檔案都會經過消毒。



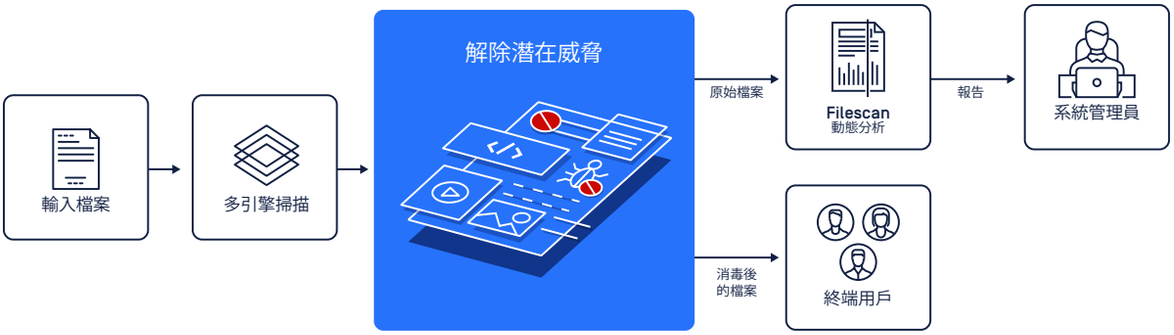
使用案例2:

消毒檔案並分析原始檔案

深度CDR離線分析模式

在您部署的多個防惡意軟體引擎進行掃描後，Deep CDR將對檔案進行消毒，然後再交付給最終用戶，這樣用戶就可以受到保護，防止惡意人士利用惡意軟體和零日攻擊進行攻擊。

此外，對於想要調查是否以及如何受到攻擊的團隊，我們的新一代沙箱FileScan可以分析原始檔案，為您的安全團隊提供深入的洞察力，以了解任何潛在的惡意活動。同時，通過分析原始檔案，您的安全團隊可以看到Deep CDR防止逃避惡意軟體的價值和效能。這個過程是在離線模式下進行的，不會中斷您的工作流程。



在某些情況下，重建檔案並不是一個最佳選擇：

- 基於不可否認的需求，包括法律或監管的限制，有時無法對檔案進行重建。
- 因財務數據的證明要求或法律限制（例如，證據數據和法律文件）而需要保持證據的鏈式鑑定
- 需要保持數據完整性
- 需要維護數位簽章

對於需要未修改檔案的組織，您可以在以下模式使用Deep CDR。

使用案例3:

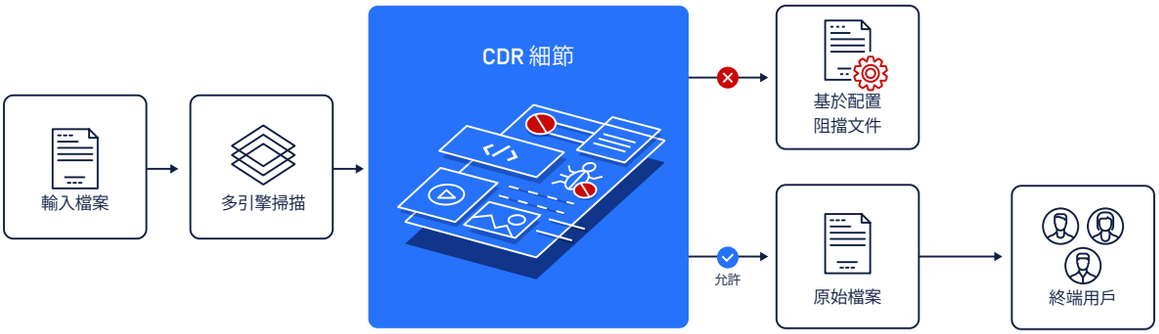
基於配置分析和封鎖檔案

Deep CDR 基於規則的阻斷模式

此模式允許您分析原始檔案並報告不符合公司政策的檔案。

此模式允許您分析原始檔案並報告不符合公司政策的檔案。在檔案通過多個防毒引擎掃描後，Deep CDR提供檔案的健康檢查，而無需對其進行消毒和重建。您可以設置引擎配置規則，以僅報告和封鎖具有特定類型的內嵌物件（例如巨集、超連結、腳本等）的特定類型的檔案。例如，如果您不允許PDF文檔中使用JavaScript。

通過全面的分析報告，您可以獲得對內容的可視性，降低惡意軟體和零日攻擊的風險，而不必修改檔案。



使用案例4:

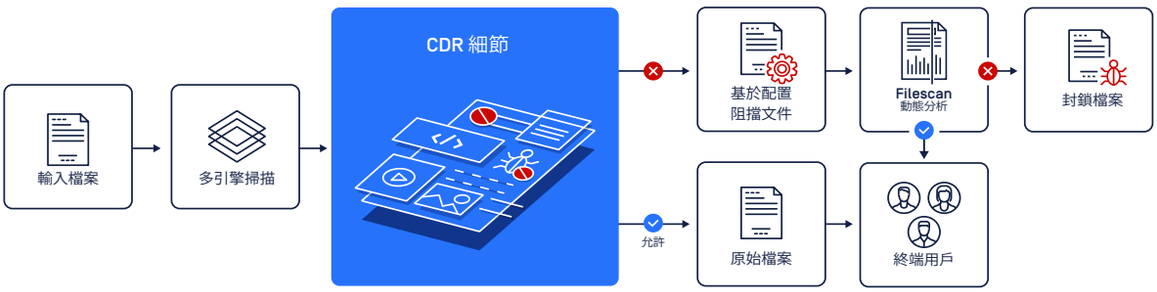
進一步調查不合規、被封鎖的檔案

Deep CDR規則基礎阻斷和內聯分析模式

為了進一步調查不符合規範的被封鎖檔案，您可以將Deep CDR基於規則的封鎖模式與FileScan內嵌分析結合起來，以判定是否可以釋放該檔案給最終使用者。FileScan允許安全分析人員安全地分析潛在有害的惡意軟體，而不會使目標系統面臨風險。如果該檔案被認為可以安全使用，則會提供給最終使用者。如果在過程中發現任何惡意嵌入式對象，則該檔案仍然會被封鎖。

如果某些嵌入式對象（例如巨集）是您的工作流程的一部分，則FileScan動態分析使團隊可以確保它們只刪除惡意檔案，從而最小化對生產力的影響。

此用例適用於希望最大程度減少資訊流中斷，同時仍然保持最高安全性水平的團隊。



OPSWAT.

Protecting the World's Critical Infrastructure

Published March 2023