OPSWAT.

客戶

# North Grid 滿足監管合規要求並停止 EMOTET MetaDefender Core

使用 Deep CDR 和多重掃描保護地方政府檔案上傳

North Grid

**關於North Grid：** North Grid 是一家領先的日本軟體公司，專門開發用於在線存儲和應用系統開發的軟體。他們提供量身定製的解決方案，例如 Proself 和 Proself Gateway Edition，專為滿足地方政府的獨特需求而設計。

**這是怎麼回事？** North Grid 的主要挑戰在於保護檔案上傳到其在日本銷售的雲存儲系統免受惡意檔案上傳。為了解決這個問題，他們與 OPSWAT，將深度內容威脅解除和重建（Deep CDR）和多重掃描技術整合到其旗艦產品 Proself 中。這種合作關係確保了日本地方政府及其網路的強大安全性。這是他們的故事。

**工業：**
網路安全

**位置：**
日本

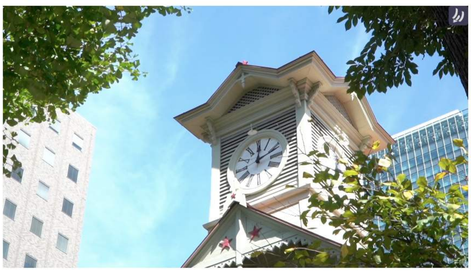
**大小：**
27 員工s

**使用的產品：**
MetaDefender Core

**關鍵技術：**
OPSWAT 使用8個防病毒引擎進行多重掃描
OPSWAT 深度 CDR

在札幌、日本的群山和現代摩天大樓中，North Grid 與惡意檔案上傳帶來的不斷上升的數位威脅作鬥爭。由於這些威脅，日本政府在總務省的指導下，積極探索能夠處理傳入檔案的解決方案，以阻止檔傳播的威脅。

North Grid 成立於 2003 年，一直處於解決檔案上傳安全挑戰和保護客戶免受檔案上傳威脅的最前沿。North Grid 的 Proself 和 Proself Gateway Edition 是開發本地和雲軟體解決方案的先驅，迎合了包括地方政府在內的廣泛行業，他們對網路安全的承諾體現在他們與 OPSWAT.



## 致力於保護數位基礎設施

憑藉其開創性的在線存儲建設軟體Proself，North Grid非常了解保護地方政府安全的必要性。我們最近採訪了 North Grid 的首席執行官 Toshiyuki Kikuchi，他詳細介紹了他們如何為熟衷於加強安全性的地方政府量身定製 Proself Gateway Edition。“我們的許多客戶都是地方政府，”菊池說，“對他們來說，Deep CDR 不僅僅是一種選擇;這是強制性的。雖然帶有八個病毒掃描引擎的多重掃描是可選的，但它提供了額外的保證層。

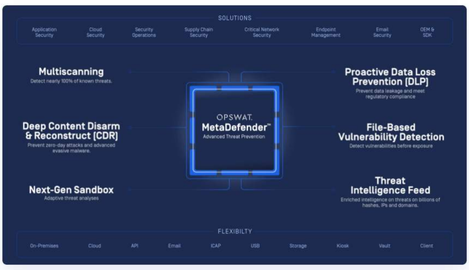
OPSWAT Deep CDR 不僅僅是另一個沙盒或防病毒掃描引擎。這是一項主動措施，用於處理和清理可能有害的檔。Kikuchi 詳細介紹了 North 如何處理安全檔案傳輸，他解釋說：“有必要在單獨的網絡之間交換檔案，我們發佈了一款專為此類環境設計的產品，稱為‘Proself Gateway Edition’，它允許在施加限制的同時進行檔交換。每個傳入的檔都經過徹底檢查，解除攻擊者使用的元素。結果是一個乾淨的、重建的檔，沒有隱藏的威脅，可供最終使用者使用。


日本政府總務省 致力於保護數位基礎設施，在 Deep CDR 中找到了安全性，通過添加多重掃描技術，組織可以刪除已知和未知的威脅、處理日語檔、使用基於預防的檔清理，並重新生成完全可用的檔。

## North Grid 如何使用 MetaDefender Core 到安全檔案上傳

North Grid 選擇了 OPSWAT MetaDefender 因為它全面高效的檔案上傳安全技術。菊池強調了使用 OPSWAT 在他們的產品中，“隨著 OPSWAT MetaDefender，我們的目標是創造一個安全措施像呼吸一樣自然的環境，而不會影響運營效率。

MetaDefender Core 通過結合基於預防和檢測的技術，以獨特的方式實現檔案上傳安全性。 多重 掃描技術通過利用多達 30 多個防病毒掃描引擎來檢測威脅，將人工智慧 （AI）、機器學習 （ML） 和廣泛的已知惡意軟體簽名資料庫相結合，確保無論威脅如何規避都能被檢測到。 深度內容威脅解除和重建 （CDR） 是 North Grid 許多客戶的強制性要求，可防止隱藏在檔中的威脅。




為了提供最大的安全覆蓋範圍，North Grid 開發了 Proself Mail Sanitize Edition，這是一款用於電子郵件的安全產品。整合 OPSWAT MetaDefender的 Deep CDR，它可以消除附件中的威脅，確保安全可靠的通信，免受網路釣魚企圖的影響。

“勒索軟體攻擊在日本激增，”Kikuchi 說：“為了解決這個問題，我們通過定期更新 VPN 韌體來增強 VPN 設備和電子郵件（常見的勒索軟體入口點）的安全性。此外，我們還提供“Proself Mail Sanitize Edition”，這是一種安全電子郵件產品。整合 OPSWAT MetaDefender的 Deep CDR，它可以清理電子郵件附件，使其成為我們勒索軟體防護策略中的關鍵工具。

犯罪分子正在不斷改進他們的方法，認識到這一點，North Grid 仍然致力於增加其防禦能力。Kikuchi 補充道：「攻擊者的策略在不斷變化，雖然培訓是必不可少的，但我們預見到未來會有更自動化、更高效的解決方案，比如 MetaDefender，將變得至關重要。

## 為關鍵網路量身定製的安全性

隨著政府將其安全措施與總務省制定的指導方針保持一致，對 Deep CDR 等綜合解決方案的需求變得顯而易見，尤其是對於 LGWAN（地方政府廣域網）系統。這些網路對本地管理功能至關重要，需要確保與更廣泛的互聯網進行安全通信的策略，從而降低電子郵件傳輸、檔案導入和潛在惡意軟體威脅的風險。

當 North Grid 在為當地政府開展專案時遇到 Emotet 病毒 時，這種對安全的承諾是顯而易見的。當傳統病毒掃描程式無法檢測到新出現的威脅時， MetaDefender的多重掃描功能識別了威脅，強調了分層安全措施的重要性。

“在為地方政府開發 Proself 時，我們遇到了Emotet病毒的爆發，該病毒通過附件傳播，”菊池解釋說，“收到這樣的檔後，我們立即使用 MetaDefender.令人印象深刻的是，八個掃描引擎中的兩個檢測到了病毒，展示了多重掃描的功效。值得注意的是，我們終端上的病毒掃描軟體在最初到達時未能識別出這種威脅。

在不妨礙運營效率的情況下平衡網路安全是走鋼絲的。然而，使用諸如 OPSWAT MetaDefender，North Grid相信建立一個無縫的環境，確保地方治理順利安全地運作。

隨著North Grid展望未來，其與 OPSWAT 仍然是其願景的核心：創造一個更好的數位世界，讓檔案上傳安全和效率共存，確保每個人都能擁有更安全的明天。

瞭解如何操作 OPSWAT的創新解決方案可以確保您的關鍵基礎設施安全，立即諮詢專家。

諮詢專家

標籤： MetaDefender Core，多重掃描技術，深度CDR技術



### 最新文章