型錄

NUCLEUS CYBER

NCPROTECT™

人工智慧導向的檔案分享資料安全

內容摘要

NC Protect™基於對檔案內容的即時分析以及用戶與檔案背景的比較來動態調整檔案保護，以確保用戶根據您的業務法規與政策檢查、使用與分享檔案。

NC Protect將安全性與加密套用於檔案分享內容，而無需人工管理的檔案夾分享與NTFS權限的負擔。

可以根據與檔案關聯的內容與 Metadata自動對資料進行分類與加密。組織不再需要依賴複雜的檔案夾層次結構，而是可以輕鬆地確保適當保護其敏感資料。

主要優點

- 集中、高經濟效率的政策法規遵循管理與防止資料丟失。
- 根據法規與公司政策監控與稽核內容。
- 根據敏感資料（包括PII，PHI，IP與其他因素）的存在、自動分類、限制對內容的存取與加密。
- 偵測潛在的違規行為並啟動工作流程以補救並最大程度地降低風險。
- 細緻安全性限制了使用安全Metadata 在項目級Item Level進行的存取。
- 儲存文件“指紋”，以便在通過電子郵件/社交方式分享檔案分享文件時套用策略規則。
- 稽核追蹤與舉證追蹤對敏感資料的存取，以確保透明性與究責。

非結構化大資料構成重大風險

數字說明了這一點，今天產生的資料有90%是非結構化的（客戶購買歷史、電話服務中心日誌、電子郵件、電子表格、文件、Web內容、部落格、Wiki等）。[1]資訊速度並沒有因為千萬億美元而放緩 每天建立的資料位元組 bytes。

許多組織已經轉向文件協同與管理平台，包括Microsoft SharePoint、Office 365、Dropbox與其他雲解決方案，以在此非結構化內容上進行儲存與協同。但是許多公司仍然擁有舊的檔案**分享**，其中仍儲存與存取了數TB的資料。有些人會將這些內容遷移到 SharePoint 之類的系統上。其他人將繼續在現有儲存庫中儲存與歸檔資訊。

如此關注新系統與雲，如何在舊檔案分享上管理存取與法規遵循？ 對於舊系統，同樣適用於新技術的資料隱私與安全問題也同樣重要。

確保檔案分享內容的資料法規遵循與安全性

NC Protect為協同系統與檔案分享提供集中、高經濟效率的策略法規遵循管理與資料丟失防護。它通過持續監控與稽核資料，確保資料法規遵循與安全性。

Windows Server File Shares上的文件違反法規與公司政策，以防止資料洩露，未經授權的存取與濫用。相同的規則也可以套用於SharePoint，Office 365，Dropbox等上的內容。

使用NC Protect管理法規遵循與安全性就像1-2-3一樣容易。

智慧型規則設計

NC Protect的策略管理器為美國與國際隱私策略（《隱私法案》，GLBA，COPPA）以及其他監管要求（包括HIPAA，FISMA，PCI DSS等）提供了數百個預先定義的檢查點。.

輕鬆定義與配置自定義檢查點，以匹配您組織的獨特隱私、機密性與安全性策略。

自動化合規

當NC Protect掃描並識別風險區域，偵測到特定的策略違規或機密內容時，會通過增加Metadata自動對標記的檔案進行分類。

安全的個人檔案

分類後，NC Protect中用戶定義的業務規則可以自動限制對檔案的存取，對其進行加密、追蹤文件鏈 Document's Chain 並防止其離開檔案分享。

[1] PC Magazine https://www.pcmag.com/news/364954/90-percent-of-the-big-data-we-generate-is-an-unstructured-me

使用NC Protect在文件級別保護內容

NC Protect使用Metadata導向的項級別安全性，根據敏感與/或不合規資訊來限制對內容的存取、加密、追蹤與阻止其通過電子郵件發送，從而為提供具備內容感知資料丟失保護（DLP）功能的 Windows Server檔案分享。除了SharePoint以外，還使用Windows Server檔案分享進行儲存與協同的組織可以在兩個平台上利用NC Protect的規則來集中管理策略、分類與控制。

分類 CLASSIFY

使用NC Protect，用戶可以輕鬆配置安全的Metadata並定義選擇值以適合任何業務需求。 授權用戶可以根據其內容對文件進行分類，這與標準Metadata不同，任何允許存取的人都可以對其進行修改。用戶可以定義文件的敏感度級別，例如 機密、私人或秘密，然後根據其選擇可以根據需要增加其他分類級別，包括選擇讀者 Audience、部門 Department 或專案 Project。

限制 RESTRICT

基於與其分類相關的業務規則，可以存取檔案分享中的文件或內容項目Content Item即使有更廣泛的讀者可以存取該專案實際居住的網站或圖書館，也只能將其限制為特定的個人或群體。有了檔案級權限，管理員可以減少建立的檔案夾位置數量（檔案夾位置擴散），以應對另一組協同用戶。 使用NC Protect管理檔案權限很容易，因為它們基於分類時增加的Metadata值。

加密 ENCRYPT

預防資料丟失對於許多組織而言都是至關重要的問題。 除了根據文件的分類（Metadata）保護文件安全之外，NC Protect還可以通過加密來進一步保護檔案分享內容。 這意味著只有具有適當資格的用戶才能讀取內容（無論在檔案**分享**內部還是外部），即使他們具有管理員權限，也可以安全地儲存董事會與HR檔案等機密檔案。它還可以確保只有憑證用戶才能存取任何使其脫離檔案系統的文件。

防止 PREVENT

為了進一步擴展追蹤過程，您還可以在NC Protect中定義規則，以防止敏感資訊或機密文件的分發或對風險用戶進行教育。例如，如果要將文件通過電子郵件發送給某個組，而列出的收件人對該文件類別沒有適當的存取權限，則只有在將個人從通訊組列表中刪除後才能發送電子郵件。 還可以防止用戶在檔案分享之外列印、保存或複制Microsoft Office文件的內容。

還可以定義分發規則，以實現通過電子郵件與第三方進行安全文件交換。可以使用Adobe證書（PKI）將檔案**分享**資產中的Office與PDF文件作為安全的只讀PDF電子郵件附件發送給外部收件人。

控制 CONTROL

通過使用工作流，NC Protect可以觸發工作流，以請求策略官員或管理員的批准，或請求用戶的解釋。可以製定完整的業務規則，以便您可以糾正法規遵循問題並向組織中的適當個人負責，以檢查內容並可能對其進行分類，更改其分類或對其進行加密。

報告 REPORT

動態結果檢查器可提供集中報告與分類資料管理。它按分類級別報告已發現的問題數量，並允許策略人員檢查結果並在需要時重新掃描，重新分類或重新申請權限。可以根據靈活的搜索條件過濾列表，並將其導出為各種格式以用於報告或存檔。

Metadata導向的項目級安全性的優勢

Nucleus Cyber的安全性細緻化方法使用安全的Metadata在項目級別限制了存取。 除了可以更好地保護組織免受意外破壞之外，此方法還可以控制Windows Server檔案分享上檔案夾的擴散。NC Protect會檢查內容的整個檔案夾以及項目中包含的資料，以根據策略管理器中內建的特定策略識別要保護的單個文件與檔案。 然後它通過安全的Metadata進行分類，並且如果需要可以限制對項目的存取與加密。

與在檔案夾級別進行安全保護或加密的解決方案相比，由於權限是在單一個檔案級別（使用分類）應用的，因此敏感內容可以從檔案分享中的任何檔案夾進行儲存、分享與協同。 它確保對檔案的存取僅限於按其分類定義具有權限的人員。