NCPROTECT™

ADVANCED INFORMATION PROTECTION FOR DROPBOX® & DROPBOX BUSINESS®

Executive Summary

The number and variety of collaboration channels and tools has increased dramatically. NC Protect provides data-centric security to protect your sensitive content regardless of where it is located - without impacting user collaboration.

NC Protect simplifies the enforcement of your information security policies with capabilities for discovering, classifying and protecting Dropbox content. Apply encryption and data usage rights to maintain control throughout the collaboration cycle.

Monitor access and usage of sensitive data with granular auditing and reporting that can be leveraged by other systems for analysis and breach response.

Key Benefits

- Automatically control sharing of files in Dropbox and adjust sharing rights according to compliance policies
- Identify and protect sensitive information being shared via Dropbox
- Adjust protection based on content sensitivity
- Only encrypt data when the scenario requires as per policy
- Hide sensitive content from unauthorized users
- Granular approach to security and protection mitigates risk down to the item level and security policies and DLP

GREAT FOR COLLABORATION, PROBLEMATIC FOR DATA SECURITY

The nature of collaboration is changing. Cloud collaboration tools like Dropbox make it easier than ever before to store files for easy access across all devices, and share and collaborate with both internal and external users.

However, the ability to secure sensitive content within platforms like Dropbox is problematic due to the ease of which users can share content with anyone. Reports show that accidental data leaks are on the rise and currently represent almost 25% of breaches from insider threats.[1]

It's clear that while adopting cloud collaboration tools makes it quick and easy to share files – they also greatly increasing the risk of information security lapses.

That is unless the right data-centric protections are in place.

Data-Centric Security and Compliance for Dropbox & Dropbox Business

NC Protect offers centralized, cost-effective policy compliance management and data loss prevention (DLP) for files in Dropbox and Dropbox Business. It ensures security by continuously monitoring and auditing files against regulatory and corporate policies to protect against data breaches, unauthorized access and sharing, and misuse.

Policies for encryption and usage rights can be automatically enforced based on the content sensitivity and collaboration scenario. It provides an unmatched level of data-centric protections without impacting productivity to facilitate secure collaboration and reduce the risk of Shadow IT.

PROTECT DROPBOX FILES WITH ATTRIBUTE-BASED ACCESS AND SECURITY

Leverage ABAC Policies

NC Protect's policy manager features hundreds of pre-defined policies for US and international data regulations (PII, FINSEC, HIPPA, and more) as well as the ability to define attribute-based access control (ABAC) and data protection policies to match collaboration needs. Easily define and configure custom rules to match your organization's unique intellectual property, confidentiality and security policies.

Automate Discovery & Compliance

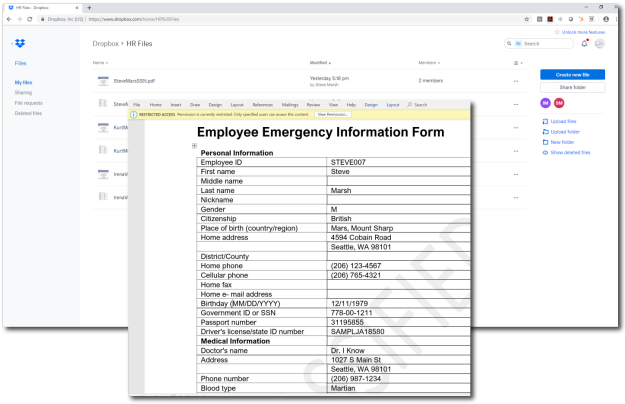
Scan files for policy violations and confidential content, once detected the file is automatically classified based on the sensitivity of the content and your pre-defined governance policies.

Secure Individual Files

Once classified, the pre-defined business and security rules in NC Protect can automatically restrict access to a file, control sharing, encrypt it, and track the document's chain of custody.

NC PROTECT DELIVERS GRANULAR CONTROL AT THE DOCUMENT LEVEL

NC Protect uses data-centric, item level security to restrict access to, control oversharing, encrypt, and track usage based upon the presence of sensitive and/or non-compliant information, offering content-aware data loss protection capabilities for Dropbox files. Organizations using Dropbox or Dropbox Business in addition to SharePoint, Teams, Yammer and Exchange for storage and collaboration can leverage NC Protect's rules across all platforms to centrally manage policies, classifications and controls.



DISCOVER & CLASSIFY

NC Protect scans and inspects files and any images inside them in Dropbox for sensitive or regulated data according to defined policies. Pattern matching is used to find recognizable data such as credit card numbers, medical record numbers, personally identifiable information, proprietary data, or custom taxonomy or keywords.

Once sensitive information is detected the file can be automatically classified by adding secure metadata based on the sensitivity of the content and pre-defined security and business policies. NC Protect ships with over 200 pre-configured scanning and classification policies and supports custom rules.

RESTRICT

Dynamically restrict access to and encrypt content based on the sensitivity of the content and business policies. Access permissions are automatically applied based on the content sensitivity, not the folder that it is stored in. Access to a file can be restricted to a specific individual or group, even if a wider audience has access to the rest of the folder where the item physically resides. The file(s) can be hidden from the folder view of the unauthorized individual.

ENCRYPT

NC Protect can further secure content by encrypting it to ensure only properly authorized and credentialed users will be able to access the content, even if they have administrative privileges. It ensures that the content can only be accessed by the appropriate people, even when it leaves Dropbox.

PREVENT

You can also define rules in NC Protect to prevent oversharing of sensitive information or confidential documents to minimize the risk of data loss. Users can also be prevented from printing, copying sharing or exporting content of Microsoft office documents and PDFs outside of Dropbox.

AUDIT & REPORT

NC Protect's dynamic Results Viewer provides centralized reporting and management of classified data. Report on the number of issues identified by classification level and allows policy officers to review the results and rescan, reclassify or reapply permissions if needed. Integrate user activity and protection logs with SIEM tools like Splunk or Microsoft Sentinel for further analysis and downstream actions.

[1] Dark Reading https://www.darkreading.com/vulnerabilities---threats/insider-threats/insider-dangers-are-hiding-in-collaboration-tools/d/d-id/1332155

ADVANTAGES OF DATA-CENTRIC SECURITY

NC Protect's granular data-centric approach to security enables conditional access control down to the item-level using secure metadata and user attributes. Since access and usage rights can be applied to specific content or individual files (using classification), as compared with solutions that secure or encrypt at the app or location level, sensitive content can be safely stored, shared and collaborated on from any Dropbox share regardless of native user sharing rights. In addition to better protecting your organization from an accidental breach, this approach also controls the proliferation of Dropbox locations to support individual collaboration scenarios.

archTIS

archtis.com | info@archtis.com Australia | United States | United Kingdom