DATASHEET

NUCLEUS CYBER

NCPROTECT™

DATA DISCOVERY, PROTECTION & AUDITING 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 apply security and compliance policies to files in Dropbox as they are created and shared
- Identify and protect sensitive information including PII, PHI, IP, etc stored in Dropbox
- Adjust protection based on content and user context
- Only encrypt data when the scenario requires as per policy
- Granular approach to security and protection mitigates risk down to the item level and security policies

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 and context of the 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 Sensitive Files with Flexible Information Security

LEVERAGE INTELLIGENT RULES

NC Protect's policy manager features hundreds of pre-defined policies for US and international data regulations (PII, FINSEC, HIPAA, and more) as well as the ability to define contextual enforcement rules 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

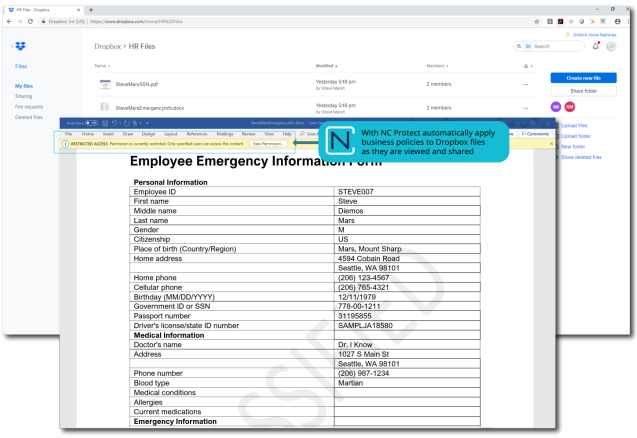
Once classified, the pre-defined business and security rules in NC Protect can automatically restrict access to a file, encrypt it, track the document's chain of custody and prevent it from leaving Dropbox.

[1] McKinsey https://www.mckinsey.com/business-functions/risk/our-insights/insider-threat-the-human-element-of-cyberrisk

* All NC Protect capabilities refered to as 'Dropbox' apply to both Dropbox and Dropbox Business

NC Protect Delivers Security and Control Beneath the Application Layer

NC Protect uses data-centric, item level security to restrict access to, encrypt, track and prevent the sharing of content 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

Locate all sensitive and confidential data (PII, PHI, HR, IP, etc.) to create an 'information footprint' of your sensitive data using a single set of rules for one or multiple on-premises and cloud environments.

CLASSIFY

Once sensitive information is detected the file can be automatically classified based on the sensitivity of the content and pre-defined governance policies. You can also define which users can classify or reclassify data, unlike standard metadata that can be modified by anyone that has document access.

RESTRICT

Based upon the business rules associated with its classification, access to files within Dropbox can be restricted to a specific individual or group of users, even if a wider audience has access to the rest of the Dropbox. With file level controls, users and administrators can reduce the number of Dropbox locations needed to enable secure collaboration within a subset or group members.

ENCRYPT

Data loss prevention is a critical issue for many organizations. In addition to securing a document based on its classification (metadata), NC Protect can further secure Dropbox files using encryption to ensure only properly authorized and credentialed users will be able to access the content regardless of their Dropbox access rights.

This additional security makes it safe to store highly confidential documents such as internal only, Board and HR documents. It also ensures access can be controlled for data shared with external parties even when it is removed from the Dropbox share.

PREVENT

To further extend the tracking process you can also define rules in NC Protect to prevent the distribution of sensitive information or confidential documents to minimize the risk of data loss. For example, if a file is added to Dropbox and a member does not have proper access to that category of document, then the unauthorized user's ability to view or edit the file can be controlled.

Users can also be prevented from printing, emailing via Exchange, saving or copying the contents of Microsoft Office documents and PDFs outside of Dropbox.

CONTROL

Using workflows, NC Protect can trigger access approval requests for policy officers or managers, or request justifications from users. Complete business rules can be developed so that you can remediate compliance issues and task the proper individual(s) in the organization to review and potentially classify, alter the classification of, or encrypt the content.

REPORT

A dynamic Results Viewer provides centralized reporting and management of classified data. It reports 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. The list can be filtered based on flexible search conditions and exported to various formats for reporting or archiving purposes.

ADVANTAGES OF INTELLIGENT, ITEM-LEVEL SECURITY

Nucleus Cyber'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.

NUCLEUS CYBER

info@nucleuscyber.com | www.nucleuscyber.com