NUCLEUS CYBER

CUSTOMERS TRUST US TO PROTECT BUSINESS CRITICAL DATA

See how NC Protect helps secure data and meet compliance goals in your industry

FINANCIAL SERVICES

CLIENT

Top Global Financial Services Institution

Protecting:
- Material, non-public information concerning a publicly-traded company
- Monitor chats for inappropriate content

Challenge:
Set up Information Barriers (ISE Rule 810) between internal communities to control the flow of confidential information between internal business units to avoid improper use or disclosure of non-public information.

RESULTS

Solution:
- NC Protect leverages Active Directory profiles to identify registered reps and monitor their internal chat messages.
- Tags any non-compliant posts and files which require a compliance review.
- Monitors all employee chats for inappropriate content and flags violations.

Result:
NC Protect allows the institution to comply with both SEC guidelines and internal company social guidelines.

INSURANCE

CLIENT

Top Global Insurance Company

Protecting:
- Sensitive Data: customer PII, financials, contracts, M&A

Challenge:
Need to identify and classify all information across the enterprise by level of sensitivity.

RESULTS

Solution:
- NC Protect scans the company's documents to dynamically identify and classify content as Public, Internal or Confidential based on their business policies.
- It dynamically restricts file access and sharing based on the content and user context.

Result:
The insurer is able to minimize data loss and control access to sensitive information using NC Protect.

INSURANCE / LEGAL

CLIENT

Specialist Insurance Company

Protecting:
- Court ordered confidential documents for settlements

Challenge:
The claims processing department has limited people who are authorized to see settlement documents.

RESULTS

Solution:
- Classify settlement docs and provide conditional access to pre-approved claims processors.

Result:
The insurer is able to remain in court compliance and ensure confidentiality of settlements with NC Protect.

ENERGY / UTILITIES

CLIENT

Energy Power Management

Protecting:
- Sensitive company data

Challenge:
- Required confidential data to be secured by legal entity/business unit and needed to secure access at the document level.
- Needed to report on how information is accessed and secured.

RESULTS

Solution:
- Dynamically determines content access based on employee role and sensitivity of the document.
- Robust, highly configurable rules engine automated complex business needs and access policies.
- Eliminated the need for employees to know the rules and policies for content access.
- Light weight and easily to deploy across SharePoint records management project.

Result:
"Our business requires secure access of sensitive information so we can acquire, develop, construct, operate, improve and divest power generation assets for our many investors. NC Protect was exactly what we needed to solve both our technical and business requirements."

HEALTHCARE

CLIENT

Healthcare Insurer

Protecting:
- Discovery of protected healthcare information (PHI) and HIPAA regulated information

Challenge:
Need to identify and classify all PHI and HIPAA related information in SharePoint across the enterprise.

RESULTS

Solution:
- NC Protect scans the company's documents to detect files with PHI/HIPAA content and classify content based on its contents and level of sensitivity.
- It dynamically restricts file access and sharing based on the classification and user context.
- Tracks user access to PHI and actions taken with it to provide an audit trail for compliance auditing and breach investigation.

Result:
The healthcare insurer is able to comply with HIPAA and privacy regulations, and control access to the data using NC Protect.

MANUFACTURING

CLIENT

Multinational Technology Company

Protecting:
- Intellectual property (IP) and trade secrets

Challenge:
Concerned about IP theft by malicious employees for economic gain or nation-state espionage, and privilege abuse.

RESULTS

Solution:
- NC Protect conditional access eliminates elevated admin privileges in Active Directory and SharePoint.
- Prevents IP and other sensitive files from being downloaded, copied, printed or emailed.
- Provides an audit trail of access and actions taken with restricted file.
- Apply dynamic watermarks to secure viewer hindering the ability to photograph the screen with a mobile device.

Result:
NC Protect ensures IP can only be access by authorized users, prevents data theft by limiting what users can do with files and eliminates privileged user access to files greatly reducing the company's risk of IP theft.

HIGHER EDUCATION

CLIENT

Large Polytechnic University

Protecting:
- Board documents

Challenge:
Limit privileged user access to Board information in SharePoint and Exchange.

RESULTS

Solution:
- NC Protect's dynamic access rules deny administrators admittance to sensitive information that by self-assignment and/or SharePoint and Exchange defaults would have otherwise granted.
- It dynamically restricts file access and sharing based on the content and user context.

Result:
NC Protect ensures that only approved board members can access materials, and prevents administrators from being able to read them - without hindering collaboration between the University's board members and authorized contributors.

PROPERTY MANAGEMENT

CLIENT

Real Estate / Property Management Company

Protecting:
- Quarterly Financial Reports

Challenge:
Protecting Quarterly Financial Reports, while providing adequate permissions for editors and view only stakeholders.

RESULTS

Solution:
- Identify Quarterly Reports and encrypt content with NC Protect proprietary encryption.
- Allow Edit Permissions, with no add-on required, via Zero Footprint Reader and provide read-only copy of document for those with View permissions.
- Permissions driven by Active Directory for immediate permissions granting/revoking when ID is updated.
- Read only versions highly secured as a watermarked image conversion displayed in-browser vs in the native editor.

Result:
With NC Protect, the firm is able to identify and dynamically secure Quarterly Financial reports without impacting authorized users' ability to edit and/view documents securely.

GOVERNMENT / MILITARY

CLIENT

Government Military

Protecting:
- Strategic military documents

Challenge:
Need to secure top secret military documents across 40 active military theaters

RESULTS

Solution:
- NC Protect applies conditional security based on pre-existing document classifications to limit access and sharing.
- Provides an audit report of who has accessed a document and under what conditions.

Result:
NC Protect ensures highly classified military information remains secure and in the right hands, while leveraging this ministry's existing technology investments.

GOVERNMENT HEALTH

CLIENT

Government Health Ministry

Protecting:
- Protected Healthcare Information (PHI)

Challenge:
Concerned about employees uploading files containing PHI into SharePoint without classifying them as such.

RESULTS

Solution:
- NC Protect scans content at the time of upload for PHI and automatically classifies it accordingly, if found.

Result:
With NC Protect, the government health ministry is able to automatically detect and classify documents with PHI at the time of upload into SharePoint.

TRIBAL GOVERNMENT

CLIENT

Tribal Government Community

Protecting:
- Member/Citizen personal information, from health records to criminal records.

Challenge:
Provide an automated method of identifying and protecting personal information, identified by a combination of name and or ID number.

RESULTS

Solution:
- NC Protect leverages a secured SharePoint List to identify tribe members personal information via name, address and ID numbers.
- It then applies unique permissions to content to relevant government entities and tribe member as a result of identification.

Result:
With NC Protect, Tribe Member information is automatically identified and access is restricted to only government entities and the specific tribe member identified. No manual processes or manual interaction is required.