

# NCENCRYPT™

## DATA ENCRYPTION & KEY MANAGEMENT FOR MICROSOFT 365 & SHAREPOINT SERVER®

### Executive Summary

Ensure that your organization's business-critical data protection meets applicable regulatory and business requirements.

NC Protect adds granular access and protection controls to business-critical content in Microsoft applications by applying attribute-based access control (ABAC) and data protection policies that you define.

While dynamic classification and access control are NC Protect's first line of defense, when paired with Azure RMS or NC Encrypt, if a document that contains sensitive information is identified that requires encryption, it can encrypt the content immediately – limiting the audience to only credentialed users.

### Key Benefits

- Enables compliance with GDPR, CCPA, HIPAA and other privacy regulations with encryption, access control.
- Adds compliance without user impact by utilizing your existing Microsoft applications and user processes.
- Supports BYOK with connectors to third party key management platforms so customers can easily leverage existing encryption investments.
- Centrally controlled and granular security policies alleviate dependency on user behavior.
- Quick and easy to configure and maintain from within the centrally hosted NC Protect administration portal.

### WHY USE ENCRYPTION TO IMPROVE DATA SECURITY?

Encryption of sensitive data in Microsoft 365 (M365) applications and SharePoint on-premises is important for data security and compliance - especially with the surge in the remote workforce and number of collaboration channels available today.

There are several points to keep in mind about the security and encryption of your M365 and SharePoint documents and files; especially highly sensitive or regulated enterprise data such as personally identifiable information (PII), protected health information (PHI), intellectual property (IP), M&A and Board documents, as well as Defense and supply chain information:

- Encryption ensures that your sensitive data stays protected in case it is leaked or shared accidentally.
- The ability to identify and encrypt sensitive data is mandatory for certain compliance regulations (e.g., HIPAA/PHI, GDPR/PII).
- You should have dynamic fail-safe processes in place to encrypt highly sensitive, regulated or classified files shared via email.
- Data classification should be leveraged to set proper access permissions and encrypt sensitive or regulated data.

### DATA ENCRYPTION YOUR WAY

Dynamically encrypt Microsoft 365 data in SharePoint Online, Teams and OneDrive, as well as SharePoint Server on-premises to keep it protected no matter where it is stored or travels: in use, in motion and at rest.

NC Protect provides flexible options to encrypt your data and manage encryption keys:

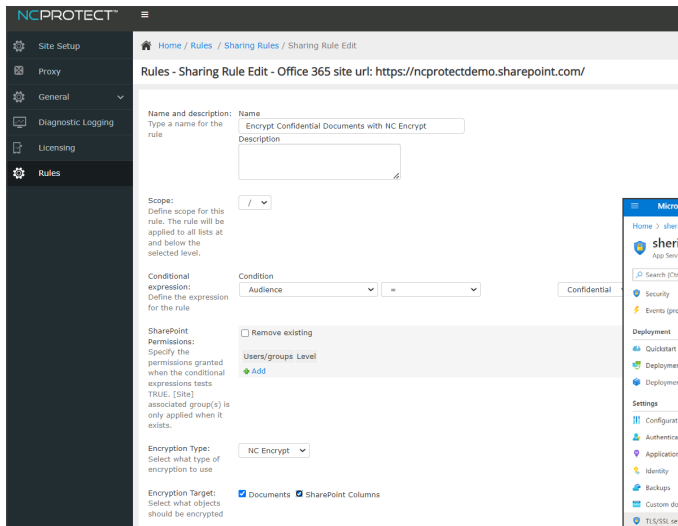
- Out of the box NC Protect adds additional protection capabilities to the standard Microsoft Purview Information Protection (MIP) and RMS controls that you may already own. Combining these Microsoft controls with NC Protect allows you to apply real-time protection of sensitive and business-critical data using NC Protect's ABAC policies to dynamically apply encryption and other data protections based on file and user context.
- Available as an add on module to NC Protect, NC Encrypt provides encryption capabilities for organizations that do not have RMS, have third party key management in place or require independent key management. NC Encrypt combines encryption with the access permission policies from NC Protect to provide a more effective way to centrally set your security posture. With NC Encrypt, you manage encryption keys and security policies out-of-the-box or via connectors to leading HSM key management platforms, including Thales CipherTrust.

## FLEXIBLE ENCRYPTION OPTIONS

NC Encrypt provides encryption capabilities out-of-the-box for organizations using NC Protect that prefer to manage their own encryption keys. NC Encrypt provides additional encryption and decryption capabilities using a company's own master key. Alternatively, a default AES-256 based encryption key can be dynamically created to get you started.

From the moment that you install NC Encrypt, your documents are secured immediately by the system generated encryption key. At any time in the future, you can switch to Bring Your Own Key (BYOK) via the NC Protect administration portal.

NC Encrypt's automatic key generation, key management and transfer to production procedures ensure that change control procedures, validation and testing phases are fully transparent and documented, while your data remains protected and encrypted.



Above left: Easily build encryption into data protection policies in NC Protect's central policy manager.

## KEY CAPABILITIES

### Encrypt Files & SharePoint Columns

- Encrypt individual files in supported applications and SharePoint columns.

### Bring Your Own Key (BYOK) Support

- Supply and manage your own keys or use NC Encrypt's dynamically created keys.
- Manage and automate key rotation.
- Provides connectors for third party key management platforms.

### Strong Encryption

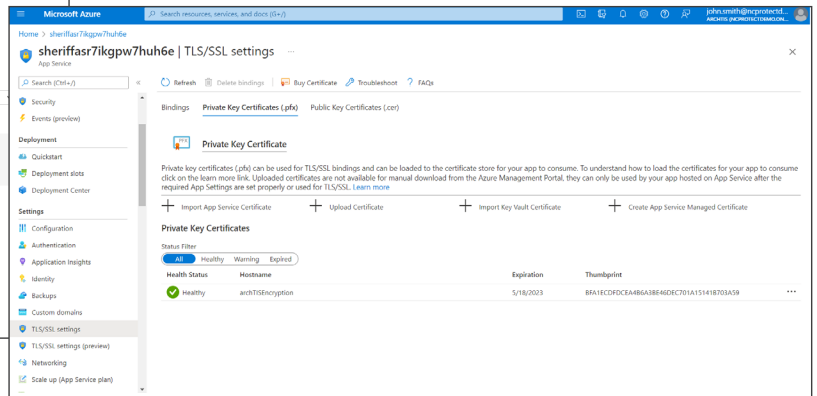
- Uses secure AES-256 bit encryption that is FIPS 140-2 compatible.

### Centrally Manage Encryption and Access

- Control encryption and access policies across all M365 apps, SharePoint Online, SharePoint Server and/or hybrid environments from the NC Protect administration portal.

### Reporting & Auditing

- Real-time activity logging and reporting tracks permitted and denied access requests, and actions taken with authorized files.



Above right: Use the dynamically created keys in NC Encrypt or supply and manage your own keys.

## SUPPORTS ENCRYPTION ACROSS THESE APPLICATIONS



SharePoint Online & On-Premises



Microsoft Teams



OneDrive



Exchange



Office 365