

NC PROTECT™



USE NC PROTECT KNOWING THAT FEDRAMP CERTIFICATION IS NOT REQUIRED

Executive Summary

NC Protect from archTIS leverages Microsoft security investments to protect sensitive and classified information against data loss and insider threats. archTIS provides zero trust data-centric information security that is simple, fast and scalable across Microsoft 365 applications including Teams, SharePoint Online, Exchange, Office, and OneDrive, as well as SharePoint on-premises and Windows File Shares.

Key Benefits

- Scan and tag data or leverage MIP sensitivity labels in combination with other file and user attributes to dynamically adjust access and data protection.
- Control what users can see, how they can use and share information and with whom at the file, message and chat level using granular ABAC policies (e.g., security classification and nationality).
- Get unique security capabilities to: enforce secure read-only access, hide sensitive files from unauthorized users, apply dynamic personalized watermarks and alert on unauthorized access or internal data spills.
- Remove/redact sensitive or confidential information, such as keywords or phrases, in a document when viewed in its native application (Word, Excel, PowerPoint and PDF) or when the file is presented in the NC Protect secure reader for legal or security purposes.
- Integrate user activity and protection logs with Microsoft Sentinel for further analysis and downstream actions.

USE NC PROTECT KNOWING THAT FEDRAMP CERTIFICATION IS NOT REQUIRED

archTIS has confirmed with the FedRAMP Program Management Office (PMO) that our NC Protect product capabilities do not require FedRAMP certification as it is not a cloud service for the following reasons:

- NC Protect is an additional tool / proxy, not the cloud service itself, and integrates with Microsoft Information Protection and Azure to apply attribute-based policies established by and enabled by customer end users.
- NC Protect resides as layer on top of the security mechanisms provided by the application platform (e.g., O365 and Teams).
- NC Protect does not replace or compromise any of the Microsoft security stack it is deployed in.
- NC Protect executes within the customer's application environment (cloud, on-premises, etc.) with no multi-tenanted or externally hosted systems being used.

NC Protect for Microsoft 365 (cloud version)

The NC Protect for Microsoft 365 product status is that of a tool or proxy. NC Protect is not a cloud service based on NIST SP 800-145 cloud definition of rapid provisioning and elasticity, self-service, resource pooling like data storage and measured services.

NC Protect for SharePoint On-Premise

NC Protect is installed and configured, as an application alongside the Microsoft Office products by onsite system or server administrators. When using NC Protect as an on-premise installation, account for the capabilities of the tool in the system description of the SSP (System Security Plan) as being an available implemented service for end users.



archTIS.com | info@archtis.com

