

NC PROTECT™ +



END TO END DATA LIFECYCLE SECURITY FOR MICROSOFT 365 & GCC HIGH

Executive Summary

Microsoft 365 is a powerful collaboration platform that allows users to create, access and share information from virtually anywhere. To keep data secure and ensure compliance, your strategies must evolve accordingly.

First, you need to identify and classify sensitive information. Second, your access and data protection policies must be strong enough to manage potential risks while remaining flexible enough to support a distributed global workforce and third-party users. Third, it is essential to ensure that these policies are enforceable and that the organization has the necessary resources to implement them.

While this may seem straightforward, it poses a significant challenge for IT and security teams when it comes to execution.

Discover, classify, and protect sensitive information with unparalleled precision with archTIS solutions.



END-TO-END DATA SECURITY SUITE

Microsoft Purview Information Protection (Purview) helps customers protect their sensitive data with labeling, encryption, and governance inside Microsoft 365 and GCC High. However, if your governance requirements are more complex, you may need to enhance Purview with fine-grained controls to meet strict government and industry compliance standards. This is where archTIS' Microsoft Information Security Association (MISA)-validated solutions add value.

archTIS solutions enhance Purview capabilities to:

- Provide deep discovery, accuracy, automation, and risk visibility.
- Enable attribute-based dynamic enforcement, secure access control, and real-time data protection for all your files.

The archTIS suite effectively bridges the gap between data discovery and policy enforcement with unmatched accuracy and precision. Moreover, it is fully integrated with Purview and your Microsoft 365 collaboration applications, as well as SharePoint Server, ensuring that you maximize your investment.

DISCOVER & CLASSIFY SENSITIVE DATA

Spirion Sensitive Data Platform (SDP) finds and classifies sensitive data with high accuracy across both structured and unstructured sources.

- Locate and Classify data based on its sensitivity or categorization.
- Augment Microsoft Purview sensitivity labels with additional labels to support multi-label classification and meet complex taxonomy needs.
- Use Spirion labels in combination with Purview sensitivity labels.

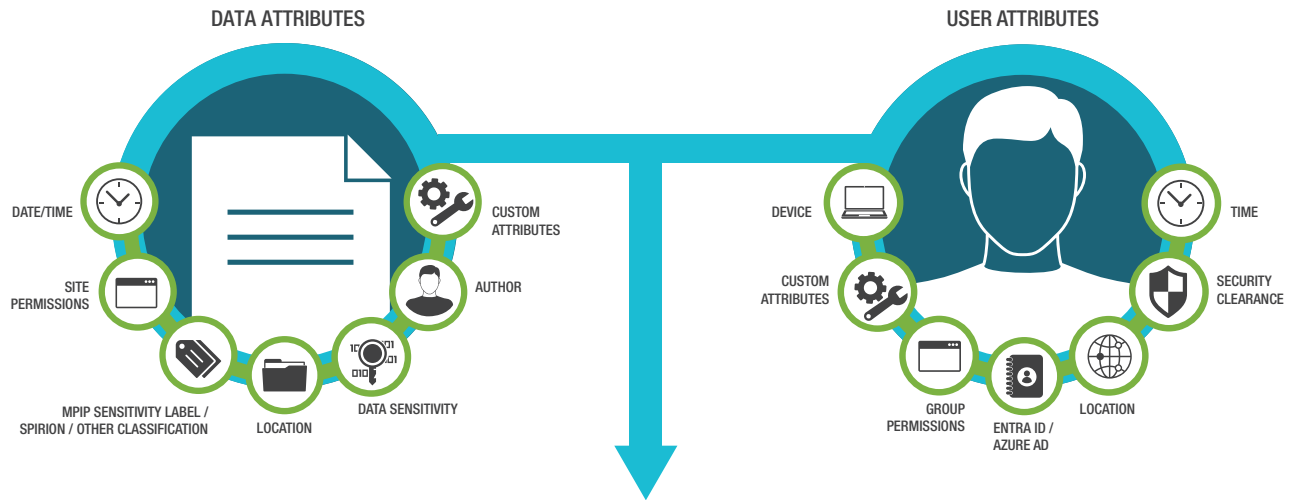
ENFORCE & GOVERN ACCESS & PROTECTION

NC Protect enforces dynamic, attribute-based access control and secure interaction policies on that data in SharePoint Online and Microsoft Teams.

- Utilize attribute-based access control (ABAC) policies that incorporate data and user attributes from Microsoft Purview, Entra ID, SharePoint properties, Spirion labels, and other sources to determine access rights and apply file protection in real time.
- Ensure fine-grained, dynamic access control and data protection policies so that only authorized users can access, edit, and share sensitive data in SharePoint Online and Microsoft Teams channels.
- Dynamically enforce secure read-only access, hides sensitive files from unauthorized users, and applies encryption and user-based security watermarks.
- Track access to and actions taken with protected sensitive data. Analyze logs and apply upstream actions in Microsoft Sentinel.

ENHANCING AND EXTENDING MICROSOFT PURVIEW WITH NC PROTECT + SPIRION SDP

Accurate Data Discovery & Classification +
Real Time, Attribute-based Access Control & Data Protection



Accurate Data Discovery & Automated Playbook Classification



Secure Office, CAD, PDF, Text and Image Files



Add multiple labels to a file to augment Purview labels



Apply Dynamic User-specific Security Watermarks



Create Unlimited Additional Classification Labels



Encrypt Files Dynamically using MPIP Rights Management



Use MPIP sensitivity labels & Spirion classification data in ABAC policies



Seamless integration with Microsoft Purview Information Protection & Entra ID



Dynamically Hide Files, Based on Content Sensitivity



Analyze User Activity Audits with Microsoft Sentinel



archtis.com | info@archtis.com
Australia | United States | United Kingdom
in t w y

