

NC PROTECT™

ENHANCED MICROSOFT INFORMATION SECURITY FOR GOVERNMENT & DEFENSE

FINE-GRAIN, DYNAMIC POLICY-BASED DATA SECURITY FOR MICROSOFT 365, GCC, GCC HIGH & SHAREPOINT SERVER

NC Protect allows Government, Defense and Defense Industry to:

- Secure interagency and multinational collaboration in the Microsoft suite with fine-grain access and protection based on file and user attributes attribute (e.g., security classification, clearance level, department, nationality).
- Enforce secure read-only viewing of sensitive/classified information, including user-based dynamic security watermarks.
- Apply visual markings, including headers, footer and CUI Designation Indicator labels.
- Redact sensitive or confidential information, such as keywords or phrases, when viewed in Word, Excel, PowerPoint and PDF files or in the NC Protect secure reader.
- Apply multiple labels to individual files and leverage them to dynamically apply access and security controls.
- Dynamically enforce internal Information Barriers and restrict guest access to country specific sensitive information within SharePoint.

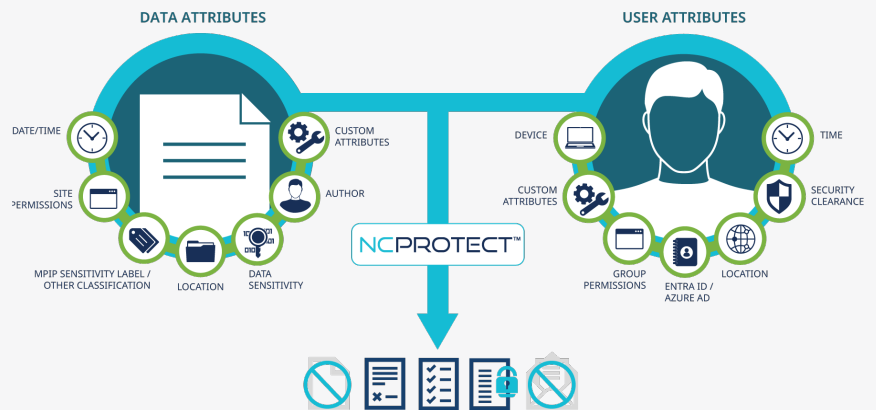
DATA-CENTRIC ZERO TRUST ACCESS AND INFORMATION PROTECTION POWERED BY ABAC

Empower your organization to take advantage of all the productivity and collaboration the Microsoft suite offers while meeting global information security and export controls regulations.

archTIS' zero trust attribute-based access control (ABAC) powered information security solutions for the public sector enhance native security capabilities to empower secure collaboration within your agency with other agencies, defense, multinational coalitions and supply chain partners.

NC Protect from archTIS leverages Microsoft security investments to protect sensitive and classified information against data loss and insider threats. archTIS provides data-centric policy-based information security that is simple, fast and dynamic across Microsoft 365, GCC and GCC High applications including SharePoint Online, Exchange and Office, SharePoint on-premises and Windows file shares.

CONDITIONAL ACCESS AND DATA PROTECTION BASED ON



Real Time, Contextual Access Control Determines:

If access to a file is approved or denied based on the policy and attributes

What a user sees when viewing and searching for files

Whether a user can open, edit, copy or download a file

If a file is encrypted when saved, copied, or emailed

If a dynamic watermark should be applied to a file

If a file can only be viewed in a secure application



Microsoft Partner

ENSURE SECURE AND CONSISTENT SECURITY AND COMPLIANCE

ON-PREMISES

Easily support your access, security and privacy requirements for SharePoint Server and Windows file share content with granular, ABAC-enabled access and data protection policies to ensure only the right users have access to the right information at the right time.

HYBRID

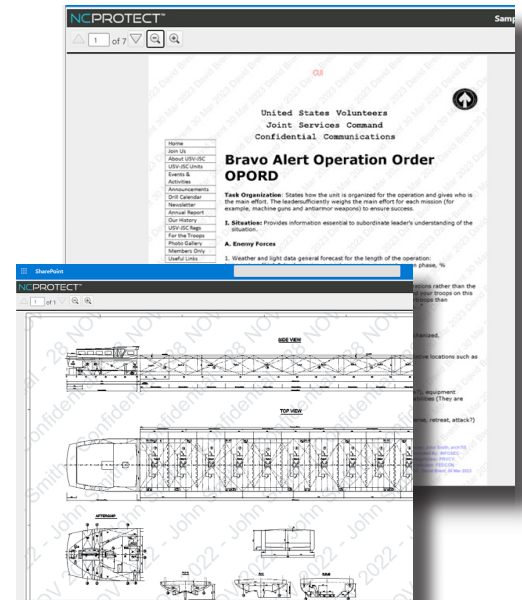
For agencies transitioning to the cloud or planning to support a long-term hybrid strategy, archTIS simplifies security and compliance with centralized policy management and tagging to ensure consistent protection across your collaboration tools no matter where they live – Cloud, hybrid or on-premises.

CLOUD

Manage access to and protect M365 and GCC High application data with granular ABAC policies to ensure secure collaboration of files and messages. archTIS solutions enforce compliance with federal, state, or international regulations, including ITAR, CMMC and NIST.

GET UNIQUE CAPABILITIES FOR FINE-GRAIN SECURITY AND ACCESS CONTROL

- **Tag data with multiple labels and use Microsoft Purview (MPIP) sensitivity labels or other classifications** in combination with file and user attributes to dynamically adjust access and data protection.
- **Control file access, usage and sharing** based on user attributes, including security classification, clearance level, department, nationality, etc.
- **Gain unique security capabilities** to enforce secure read-only access, hide sensitive files, and apply dynamic user-based watermarks.
- **Encrypt or restrict attachments based on sensitivity** sent through Exchange email.
- **Add CUI Headers, Footers and CUI Designation Indicator labels** (Owner Name, Controlled By, Category, Distribution/Limited Dissemination Control, POC) as a persistent watermark.
- **Remove/redact sensitive or confidential information** (keywords or phrases) in documents when viewed in its native application (Word, Excel, PowerPoint and PDF) or in the NC Protect Secure Reader.
- **Integrate user activity and protection logs** with Microsoft Sentinel for further analysis and downstream actions.



ENSURE COMPLIANCE WITH DATA SECURITY REQUIREMENTS

Extending a Zero Trust approach used for system and application access to file access and sharing with NC Protect ensures compliance with a number of domestic and international information security regulations.

- NIST 800-171
- NIST 800-53
- CMMC
- Controlled Unclassified Information (CUI)
- Defense Federal Acquisition Regulation Supplement (DFARS)
- Defence Industry Security Program (DISP)
- Export Administration Regulations (EAR)
- Cybersecurity Executive Order for Zero Trust Architecture
- FISMA
- Federal Contract Information (FCI)
- Global Privacy Acts (GDPR, Regional Privacy Acts)
- International Traffic in Arms Regulations (ITAR)
- Other Defense and Export Controls



archTIS.com | info@archtis.com Australia | United States | United Kingdom

