Dynamic data defense made simple

Expand your data protection capabilities to better defend against foreign and domestic threats with archTIS and Microsoft

archTIS

Microsoft Security

Contents

Protecting national interests starts with secure collaboration

Sensitive and classified information is increasingly at risk of a breach

Organizations in the Defense Industrial Base need to protect national interests and their sensitive information. But with multiple supply chain partners in different geographical locations, sensitive data being shared across information sharing channels becomes more vulnerable to attack – both inside and outside the organization. To meet strict security and compliance requirements, the need for a comprehensive solution that secures all collaboration pathways while also enforcing regulatory compliance is critical.

- 62% of breaches involve employee or contractor negligence.*
- The average cost of an insider or contractor breach is over $300,000 per incident.*
- The cost related to insider breach averages $4.58M per year per organization.*

Enable simple, fast, and dynamic security and compliance across all of your Microsoft Apps

Gain real-time protection

Proactively protect against insider threats with real-time data protection and unique capabilities.

Read More

Enforce data access and protection policies

Ensure need-to-know principles with granular attribute-based access control policies to better protect sensitive data.

Read More

Control shared content, anywhere

Monitor and control collaboration across your Microsoft 365 applications with dynamic protection policies.

Read More

Gain real-time protection

Maintain full control over sensitive and classified information with fine-grain data protection

The way we work has changed, and so have the ways we share data. While new tools and methods for sharing important information have made collaboration more efficient, it has also made it more difficult to maintain full control over our data. But when it comes to national defense, letting any amount of critical data slip through the cracks isn't an option.

NC Protect leverages Microsoft Purview Information Protection sensitivity labels in combination with other file and user attributes to dynamically adjust access using attribute-based access control (ABAC) and data protection policies. Access and security are automatically adjusted based on a real-time comparison of user attributes (nationality, clearance level, organization, location, time, and so on), file content, and sensitivity level to ensure that users access, use, and share files according to organizational regulations and policies. Gain fine-grain, data-centric access control and unique data protection capabilities to secure internal and guest collaboration across your Microsoft 365 applications and enforce data handling requirements in CMMC, NIST, ITAR, EAR, and Zero Trust mandates.

Discover the combined power of NC Protect and Microsoft Purview Information Protection

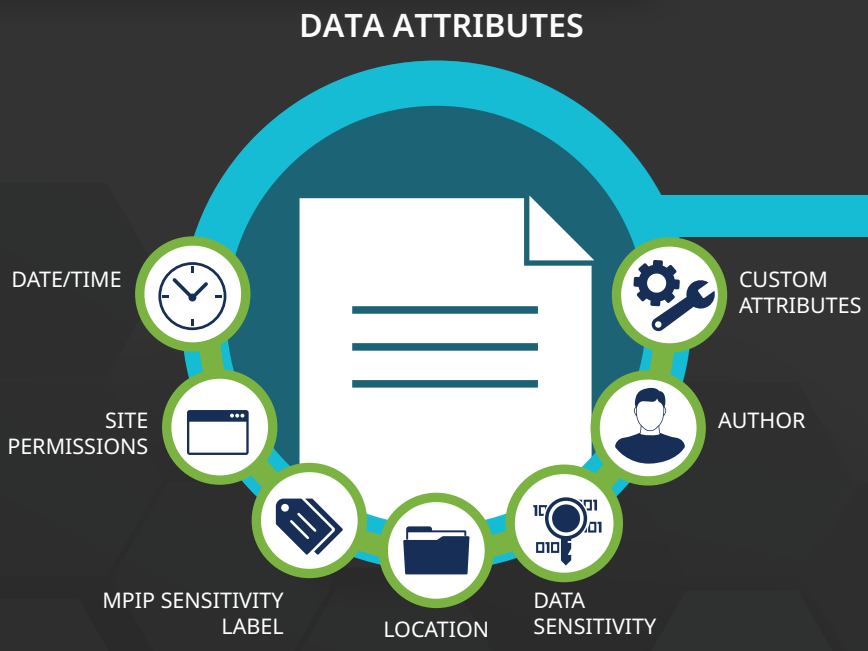
NC Protect from archTIS leverages key Microsoft Purview Information Protection capabilities to provide data-centric security that is underpinned by a zero trust ABAC methodology for collaboration in Microsoft 365 applications, including Teams, SharePoint, Exhange, OneDrive, and Office, as well as SharePoint on-premises and Windows file shares. By combining Microsoft Purview Information Protection sensitivity labels with NC Protect's dynamic attribute-based policies, you will gain expanded protection and control over information access, collaboration, and sharing.

Enforce data access and protection policies

Implement secure ABAC policies to protect critical data from unauthorized users

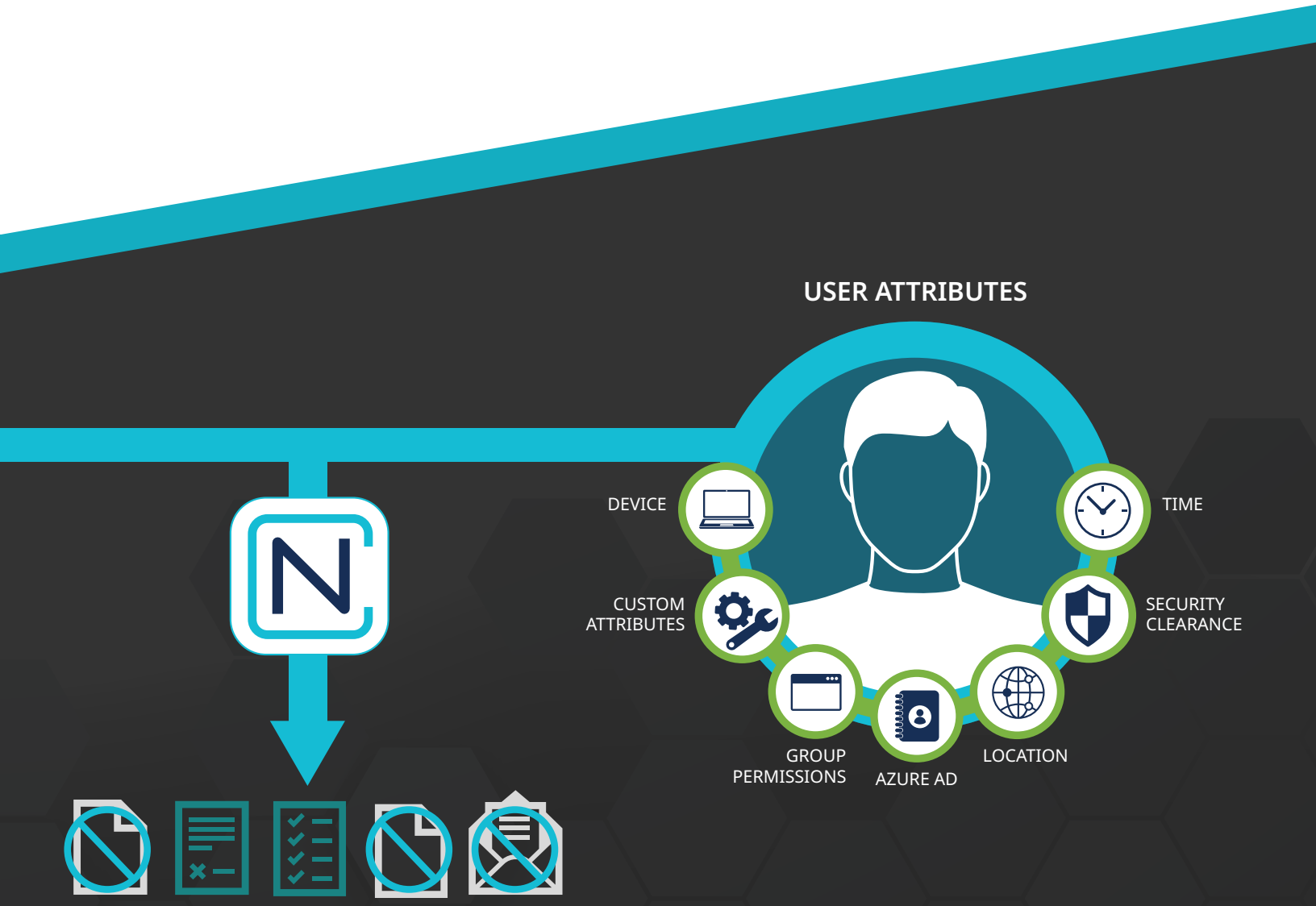
Organizations today, especially in the defense industry, must enforce protection policies that are firm enough to accommodate the adoption of new cloud services, yet flexible enough to allow users to work when, where, and how they need. Further, organizations also require the ability to ensure that employees and partners with access to classified information use and share it properly to avoid it falling into the wrong hands.

Apply real-time, attribute-based access and sharing control



With NC Protect, extend ABAC-powered conditional access, usage, and sharing policies for internal and guest users across your Microsoft 365 applications for granular information protection. Scan and tag data or leverage Microsoft Purview Information Protection sensitivity labels in combination with other file and user attributes to dynamically adjust access and data protection.

Gain unique security capabilities that allow you to enforce secure read-only access; apply dynamic, personalized watermarks; redact sensitive information; trim the application ribbon to restrict actions; and audit access. Integrate NC Protect's user activity and protection logs with Microsoft Sentinel for further analysis and downstream actions.

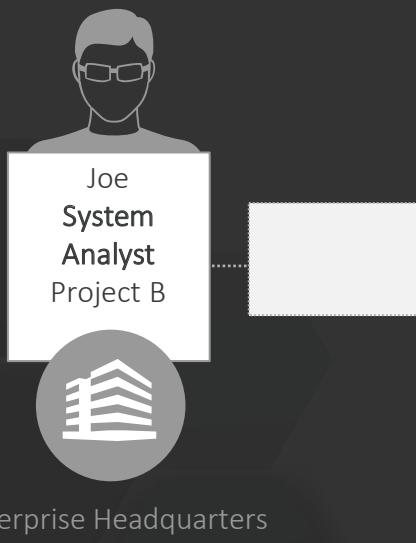


Control shared content, anywhere

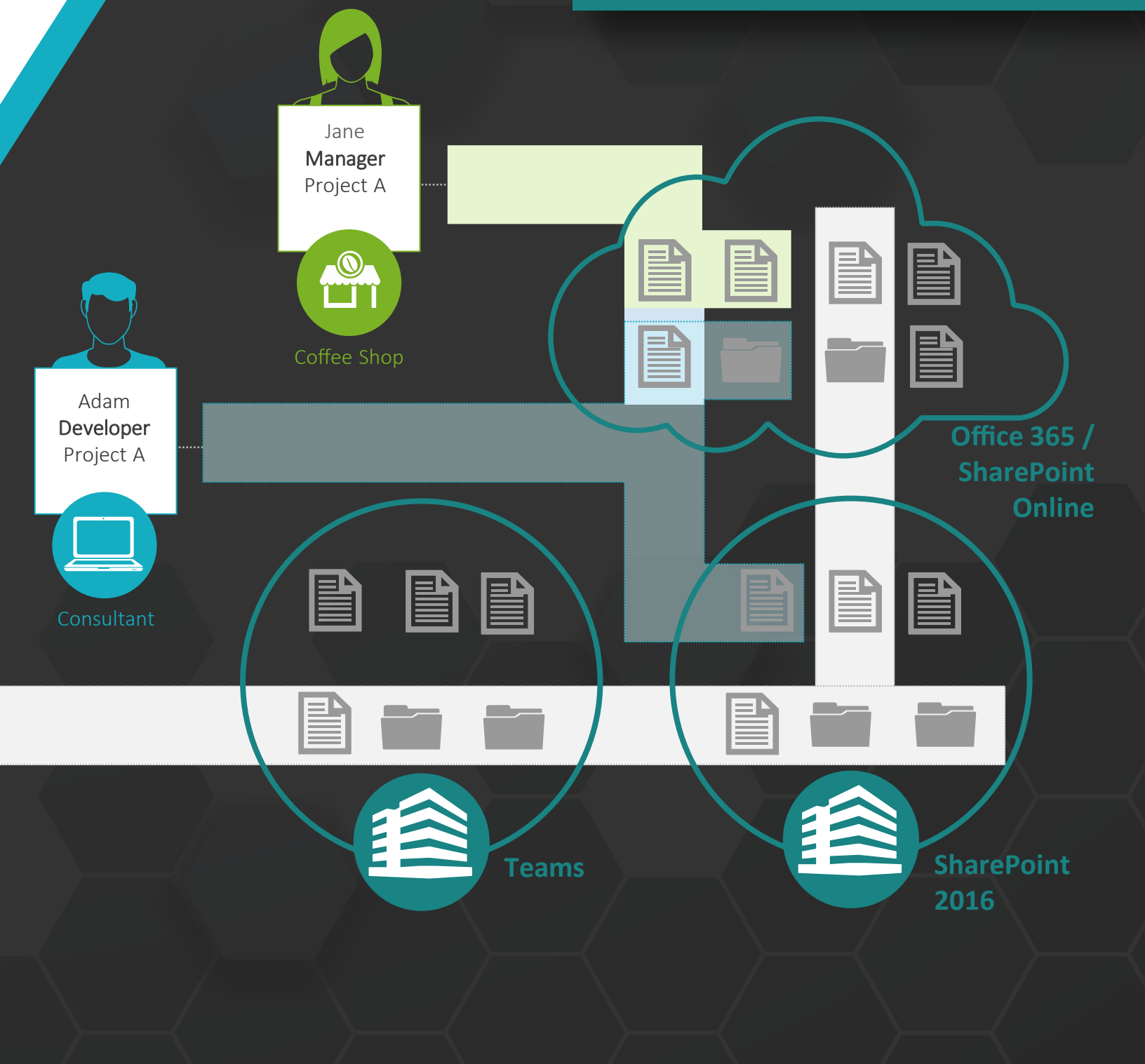
Expand protection and control over information access, collaboration, and data sharing

With modern collaboration apps, users can access data from an alarming variety of locations. And while digital file sharing and collaboration across channels is both efficient and necessary to ensure success in the defense industry, rapid adoption of new technologies has made it difficult for traditional data defenses to keep up.

NC Protect allows you to dynamically apply the same fine-grain access and data protection policies used across your M365 applications to your files and chats in Teams, and encrypt attachments and email sent through Exchange, helping seamlessly enforce consistent security across all collaboration channels. Easily apply access controls and data protection to sensitive files and control guest access by segmenting access to country-specific information (such as ITAR/EAR) using granular ABAC policies.



Enable dynamic security across channels



Case study: Defense supply chain manufacturer – ITAR and CUI compliance

Situation

Organizations in the Defense Industrial Base (DIB) form an important part of the supply chain for government and defense. As a result, they store and collaborate on highly sensitive data known as Controlled Unclassified Information (CUI) that is subject to a variety of regulations. With several military contracts and non-US–based offices, this DIB with locations in the US and UK has many regulations that they need to follow to ensure CUI is handled properly for ITAR compliance.

Challenge

Since there are fewer controls over CUI as compared to classified information, loss of CUI is one of the most significant risks to national security – making its protection critical. Managing CUI compliance manually would be extremely difficult, so the DIB sought a solution to help automate the identification and classification of CUI in their SharePoint systems and help restrict access to it.

Result

The DIB chose NC Protect because it fit their requirements and budget with its ability to scan files in SharePoint for CUI and automatically classify them according to their CUI level and restrict access based on user location and the document's CUI designation. The DIB can now collaborate with full confidence knowing that CUI is automatically identified, properly classified, and restricted based on the CUI and ITAR compliance guidelines.

Solution

NC Protect for Microsoft 365 and SharePoint creates a simpler way to identify, manage, and restrict sensitive information by leveraging your pre-existing Microsoft security investments so that your organization can operate and collaborate with confidence. With NC Protect, you can:

- Ensure compliance with CUI information handling requirements (ITAR, EAR, NIST, CMMC).
- Scan and identify files with CUI and classify them according to the CUI level and ITAR compliance guidelines.
- Restrict who in the organization can access documents containing CUI by classification and geolocation.
- Control the type of access allowed: full or read-only.
- Apply a secure digital watermark with the current date, user, and CUI level.

Read the full case study

Simple. Fast. Dynamic.

With NC Protect, leverage your existing Microsoft security investments to protect sensitive and classified information using data-centric security that is simple, fast, and dynamic. NC Protect applies and enforces dynamic, policy-driven access controls that leverage both user and data attributes to ensure your employees and partners can access, share, and collaborate on sensitive and classified information – securely.

Combat data loss and stop insider threats with the combined power of archTIS and Microsoft.

*Ponemon 2020 Cost of Insider Threats | Ponemon Institute

Ready to get started?

Visit our website

Find us on the

Microsoft Commercial Marketplace

Azure Government Marketplace


archTIS