SECURING THE EDGE:
MASTERING DATA SECURITY IN DEFENSE

GET DATA-CENTRIC PROTECTION WITH ARCHTIS NC PROTECT AND MICROSOFT PURVIEW INFORMATION PROTECTION

archTIS

CONTENTS

HOW CAN ORGANIZATIONS MEET MODERN ACCESS DEMANDS WITHOUT SACRIFICING SECURITY?

Static data classification and access control settings are no longer enough for complex security needs

All organizations need to navigate some form of data sharing, and the risks associated with it. But the defense industry presents a heightened set of stakes, challenges, and requirements. For defense and Defense Industrial Base (DIB) organizations, it is unavoidable that classified or Controlled Unclassified Information (CUI) will need to be shared within the organization and with third parties. Unfortunately, these interactions come with the risk of data leaks. Breaches of classified or sensitive information not only carry serious consequences for those involved, including substantial fines, loss of contracts, or even prison time, but they also have a broader impact on national security and trust. Recent high-profile leaks in the defense sector underscore this issue.

- Classified U.S. intel on Israel's response to Iran was leaked on the Telegram messaging app, prompting an FBI investigation.[1]
- A U.S. National Guardsman leaked hundreds of classified documents on Discord, including intelligence about Russia's actions in Ukraine and U.S. spy intel on its allies.[2]
- In the UK, the personal data of 1,182 UK Special Forces soldiers who had recently been promoted from corporal to sergeant was leaked from someone inside the Ministry of Defence and subsequently shared in WhatsApp.[3]

Organizations in the defense industry need a more comprehensive way to protect sensitive information without disrupting operations.

Implement fine-grained, dynamic, data-centric security customizable to your specific requirements

Level up your data security with archTIS NC Protect. NC Protect integrates seamlessly with both Microsoft 365 and GCC High, and it builds on the capabilities of Microsoft Purview Information Protection, Microsoft Entra ID, and Microsoft Sentinel to dynamically classify and protect every file, no matter where it lives or travels. A data-centric approach focuses on securing every individual piece of data, not just the applications or cloud networks that host them.

Upgrade to attribute-based access controls

Move beyond role-based access controls to comprehensive, context-specific access security.

LEARN MORE

Classify, secure, and visually mark CUI

Meet multiple CUI regulations simultaneously with simple, clear, and customizable data labeling.

LEARN MORE

Extend full protection to non-Microsoft file types

Apply the same data labeling and access controls to PDFs, CAD files, images, and more.

LEARN MORE

UPGRADE TO ATTRIBUTE-BASED ACCESS CONTROLS

Role-based access controls don't provide the granularity needed to protect sensitive data in a constantly changing environment

Traditional role-based access controls (RBAC) and data sensitivity labels do provide some level of protection, but they lack the detail and contextual awareness that DIBs require. The static settings make them cumbersome to manage and potentially inaccurate in situations where uses and access needs are changing rapidly. Attribute-based access control (ABAC) is the next evolution of RBAC, offering far more granularity and context-based access decisions. ABAC considers multiple factors related to both the data and the prospective user to determine who should have access to what and when, enabling organizations to meet strict compliance requirements without disrupting operations or overwhelming IT teams.

NC Protect's ABAC policies take into account information from Microsoft Purview Information Protection, Microsoft Entra ID, and other third-party sources along with a user's nationality, clearance level, location, and more to determine what files a user can access, edit, and share at any given time. NC Protect also goes a step further by applying user-specific watermarks for greater data awareness, accountability, and tracking.

ABAC IN ACTION

The Australian Department of Defence is safeguarding access to mission-critical data in SharePoint with NC Protect

For the Australian Department of Defence, collaboration and data sharing are critical to their operations in the field. Brigadier General Warren Gould shared the impact that implementing NC Protect has had on their operations.

> "With NC Protect, we can increase our collaboration by automatically controlling access to classified information. Before NC Protect, we had to lock everything down so very few users could access content to the extent that it inhibited our ability to collaborate with our coalition partners in theatre."
>
> **– Brigadier General Warren Gould, Director General Systems and Integration, Australian Department of Defence**

CLASSIFY, SECURE, AND VISUALLY MARK CUI

Comply with complex regulations with customizable and dynamic labeling capabilities

There are a *lot* of policies that dictate how CUI and export-controlled data should be handled. NIST 00-171, DFARS 7012, International Traffic in Arms Regulations (ITAR), Export Administration Regulations (EAR), and Cybersecurity Maturity Model Certification (CMMC 2.0) are all potential regulations that may apply based on context. And overlapping requirements may dictate that multiple watermarks, labels, or other controls be applied simultaneously.

NC Protect offers a comprehensive solution to compliance by embedding CUI Designation Indicator markings along with headers/footers directly into documents. These visual markings include user-specific information such as the owner, controlling entity, category, distribution controls, and point of contact, ensuring continuous protection. When documents are accessed through Microsoft 365 or the NC Protect Secure Reader, these labels remain visible as persistent watermarks. By augmenting Microsoft Purview Information Protection labeling with multi-label classification and unlimited security labels, NC Protect meets complex categorization needs, no matter which regulations you are complying with.

Expanding on Microsoft Purview Information Protection's sensitivity labels

Microsoft Purview Information Protection provides essential sensitivity labels for data classification and protection. NC Protect enhances these capabilities with ABAC and dynamic protection features, offering a comprehensive solution for safeguarding sensitive information and ensuring compliance in a wider variety of uses cases.

EXTEND FULL PROTECTION TO NON-MICROSOFT FILE TYPES

Consistently apply the same robust data labeling and access controls to PDFs, CAD files, images, and more

Office-based files like Word, PowerPoint, and Excel aren't the only file types organizations use to conduct operations. CAD files, which are critical for designing models and architecture plans, are particularly challenging to protect using traditional security tools. The complexity of managing and protecting these files can be overwhelming, leaving organizations vulnerable to accidental sharing or malicious actions that could compromise their competitive advantage.

NC Protect enables you to extend the same Microsoft Purview Information Protection sensitivity labels, persistent watermarks, and dynamic access and sharing policies to these file types as well. With features like dynamic encryption, user-specific watermarks, CUI visual markings, and real-time tracking of user actions, NC Protect not only enhances data security but also ensures compliance with defense regulations. This empowers DIB organizations to confidently protect Defense-regulated information and intellectual property and maintain their competitive edge in the market. No matter what form your data takes, you can still secure it the same way you secure your Microsoft files.

CASE STUDY

CUI COMPLIANCE IN SHAREPOINT FOR A DEFENSE SUPPLY CHAIN MANUFACTURER

Situation

A global manufacturer of aircraft accessories needed a simpler way to identify and restrict access to the CUI they handled in their SharePoint on-premises environment as part of their work with the Department of Defense in order to meet strict data-handling regulations. The risk of noncompliance, even accidental, could have devastating consequences for the business.

Challenge

Multiple military contracts and offices outside of the U.S. meant that there were many applicable regulations they needed to follow. Managing the data access manually to meet these compliance requirements was simply not feasible.

Result

With NC Protect, the customer was able to automatically identify and classify documents according to their CUI level and manage access to meet their compliance requirements without overextending their budget or their security team.

Solution

NC Protect was able to provide the data labeling and fine-grained protection needed across all file types within the customer's budget. This included the ability to:

- Scan and classify files based on keywords that map to CUI Levels 1, 2, 3, or "no CUI".
- Restrict access to specific CUI levels based on user location and nationality.
- Require documents in restricted groups to be opened in the archTIS secure viewer to prevent unauthorized actions like printing or downloading.
- Automatically apply dynamic watermarks based on the user, date, and CUI level.

THE DEFENSE INDUSTRY IS DYNAMIC, YOUR DATA PROTECTION SHOULD BE TOO

NC Protect empowers your organization to take control of data security. With seamless integration with your existing Microsoft infrastructure, NC Protect provides a user-friendly experience without compromising on security. Get the fine-grained, data-centric protection you need to land contracts with confidence, knowing that your data is secure, compliant, and accessible only to those who need it.

NCPROTECT™

Find us on the Microsoft commercial marketplace

LEARN MORE

Book a demo

BOOK NOW

Learn more on our website

VISIT SITE

[1] FBI says it's investigating unauthorized release of documents on Israel's possible attack plans | AP News, 2024
[2] Pentagon secrets leaker Jack Teixeira is sentenced to 15 years in prison | NPR, 2024
[3] UK Special Forces soldiers' personal data was floating around WhatsApp in a leaked Army spreadsheet | The Register, 2021

archTIS

Member of
Microsoft Intelligent Security Association

Microsoft Security

Copyright © 2024 archTIS Limited and Microsoft Corporation. All rights reserved.