NCPROTECT™

ADVANCED INFORMATION PROTECTION FOR YAMMER®

Executive Summary

The number and variety of collaboration channels and tools has increased dramatically. NC Protect dynamically adjusts access and protection of files within Microsoft Yammer to ensure that your organization's sensitive data is being used and shared according to your business regulations and policies.

NC Protect provides conditional access control without the overhead of complex user permissions and poorly applied at-rest encryption, ensuring that your information is protected at the right time across all collaboration scenarios. It can restrict usage and even hide data based on multiple attributes including data classification, user location, device and access rights, and automatically apply encryption when the data leaves the safety of your collaboration systems.

Key Benefits

- Automatically apply security and compliance policies to files in Yammer as they are created and shared
- Identify and protect sensitive information being shared via Yammer
- Adjust protection based on content and user context
- Only encrypt data when the scenario requires as per policy
- Hide sensitive content from unauthorized users
- Granular approach to security and protection mitigates risk down to the item level and security policiesand DLP

GREAT FOR COLLABORATION, PROBLEMATIC FOR DATA SECURITY

The nature of collaboration is changing. With social collaboration tools like Yammer we can now improve engagement across our entire organization making it easier than ever before to communicate with a wide audience, and share and collaborate on files.

However, the risk of accidentally sharing information too widely can increase with the introduction of social collaboration tools. Reports show that accidental data leaks are on the rise and currently represent almost 25% of breaches from insider threats. Couple that with the fact that employee collaboration messages are 144% more likely to contain confidential information.[1]

It's clear that while adopting social collaboration tools makes it easy to share files across the organization – they also greatly increasing the risk of information security lapses. That is unless the right data-centric protections are in place.

Data-Centric Security and Compliance for Yammer

NC Protect offers centralized, cost-effective policy compliance management and data loss prevention (DLP) for Yammer files. It ensures data compliance and security by continuously monitoring and auditing files against regulatory and corporate policies to protect against data breaches, unauthorized access and sharing, and misuse.

Policies for encryption and usage rights can be automatically enforced based on the content and context of the collaboration scenario. It provides an unmatched level of data-centric protections without impacting productivity to facilitate secure collaboration and reduce the risk of Shadow IT.

PROTECT YAMMER FILES WITH ATTRIBUTE-BASED ACCESS AND SECURITY

Leverage ABAC Policies

NC Protect's policy manager features hundreds of pre-defined policies for US and international data regulations (PII, FINSEC, HIPPA, and more) as well as the ability to define attribute-based access control (ABAC) and data protection policies to match collaboration needs. Easily define and configure custom rules to match your organization's unique intellectual property, confidentiality and security policies.

Automate Discovery & Compliance

Scan files for policy violations and confidential content, once detected the file is automatically classified based on the sensitivity of the content and your pre-defined governance policies.

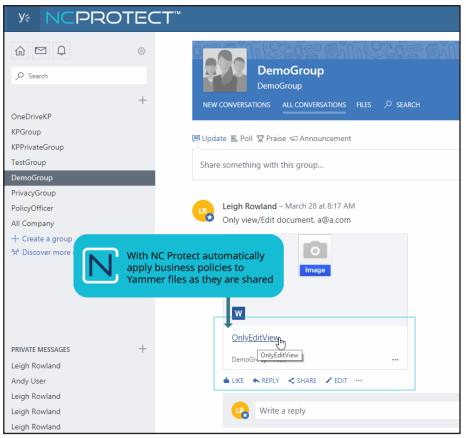
Secure Individual Files

Once classified, the pre-defined business and security rules in NC Protect can automatically restrict access to a file, encrypt it, track the document's chain of custody and prevent it from leaving Yammer.

[1] Dark Reading https://www.darkreading.com/vulnerabilities---threats/insider-threats/insider-dangers-are-hiding-in-collaboration-tools/d/d-id/1332155

NC PROTECT DELIVERS GRANULAR CONTROL AT THE DOCUMENT LEVEL

NC Protect uses data-centric, item level security to restrict access to, encrypt, track and prevent the sharing of content based upon the presence of sensitive and/or non-compliant information, offering content-aware data loss protection capabilities for Yammer files. Organizations using Yammer in addition to SharePoint, Teams and Exchange for storage and collaboration can leverage NC Protect's rules across all platforms to centrally manage policies, classifications and controls.



DISCOVER & CLASSIFY

NC Protect scans and inspects files in on-premises and cloud collaboration apps for sensitive or regulated data according to defined policies. When detect, it automatically classifies the file and applies information protection based on it's sensitivity and your policies. It can also leverage MIP sensitivity labels in combination with other file and user attributes to control access to and apply information protection.

RESTRICT

Utilize granular security to automatically restrict access to, sharing of and protection of content based on the business rules associated with the file's classification or MIP sensitivity label. Access to a file can be restricted to a specific individual or group, even if a wider audience has access to the rest of the site where the item physically resides. Managing access at the file level is made possible by leveraging the data and user attributes, rather than the data location.

ENCRYPT

NC Protect can further secure content by encrypting it to ensure only properly authorized and credentialed users will be able to access the content even if they have administrative privileges, making it safe to store confidential documents such as Board or HR documents. It also ensures access can be controlled for any data shared with external parties, even when it is removed from a site.

PREVENT

You can also define rules in NC Protect to prevent the distribution of sensitive information or confidential documents to minimize the risk of data loss. For example, if a file is added to a site and member does not have proper access to that category of document, then the file can be hidden from the view of the unauthorized individual. Users can also be prevented from printing, emailing via Exchange, saving or copying the contents of Microsoft Office documents and PDFs outside of Yammer.

CONTROL

Using workflows, NC Protect can trigger access approval requests for policy officers or managers or to request justifications from users. Complete business rules can be developed so that you can remediate compliance issues and task the proper individual(s) in the organization to review and potentially classify, alter the classification of, or encrypt the content.

UNIQUE DATA PROTECTION CAPABILITIES

NC Protect works natively with Microsoft collaboration and security products to augment native features to enforce secure read-only access, hide sensitive files from unauthorized users, trim

the application ribbon, apply dynamic personalized watermarks, and encrypt or restrict attachments sent through Exchange Email.

REDACTION

NC Protect can 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.

AUDIT & REPORT

A dynamic Results Viewer provides centralized reporting and management of classified data. Report on the number of issues identified by classification level and allows policy officers to review the results and rescan, reclassify or reapply permissions if needed. Integrate user activity and protection logs with SIEM tools like Splunk or Microsoft Sentinel for further analysis and downstream actions.

ADVANTAGES OF DYNAMIC, ATTRIBUTE BASED ACCESS AND CONTROL

archTIS' granular data-centric approach to security enforces a zero trust methodology through conditional, attribute-based access control at the item-level. Since access and information protection are applied to individual files, chats and messages, as compared with solutions that secure or encrypt at the app or location level, sensitive content can be safely stored, shared and collaborated on across Yammer and Microsoft 365 apps, regardless of user membership.

archTIS

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

Copyright 2021 archTIS Limited. All rights reserved. archTIS, the archTIS logo and NC Protect logo are trademarks of archTIS Limited. Microsoft is a registered trademark of Microsoft Corporation in the United States and/or other countries. All other product names mentioned herein are trademarks of their respective holders.