





## 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 policies

## 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.<sup>1</sup>

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 Conditional Access and Security



### LEVERAGE INTELLIGENT RULES

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 contextual enforcement rules 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.

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

## NC Protect Delivers Conditional Access 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

Locate all sensitive and confidential data (PII, PHI, HR, IP, etc.) to create an 'information footprint' of your sensitive data using a single set of rules for one or multiple on-premises and cloud environments.

### CLASSIFY

Once sensitive information is detected the file can be automatically classified based on the sensitivity of the content and pre-defined governance policies. You can also define which users can classify or reclassify data, unlike standard metadata that can be modified by anyone that has document access.

### RESTRICT

Based upon the business rules associated with its classification, access to files within a Yammer group can be restricted to a specific individual or set of group members, even if a wider audience has access to the rest of the Yammer feed where the item physically resides. With file level controls, users and administrators can reduce the number of Yammer groups needed to enable secure collaboration within a subset or group members. Managing access at the

file level is made possible by leveraging the data and user attributes rather than the data location.

### ENCRYPT

Data loss prevention is a critical issue for many organizations. In addition to securing a document based on its classification (metadata), NC Protect can further secure Yammer files using encryption to ensure only properly authorized and credentialed users will be able to access the content regardless of their Yammer group membership status. This additional security makes it safe to store highly confidential documents such as internal only, Board and HR documents. It also ensures access can be controlled for data shared with external parties even when it is removed from the Yammer group.

### PREVENT

To further extend the tracking process 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 Yammer and a member does not have proper access to that category of document, then the file can be hidden from the view of the

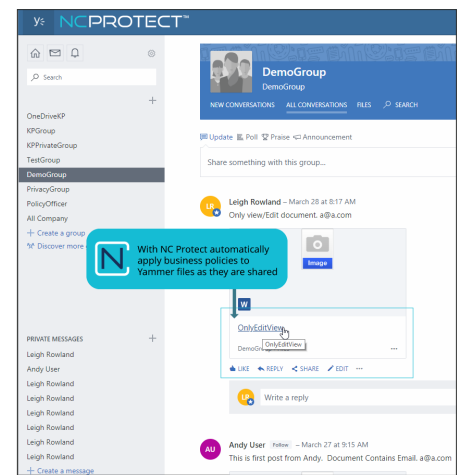
unauthorized individual. Users can also be prevented from printing, emailing via Exchange, saving or copying the contents of Microsoft Office documents and PDFs outside of the Yammer group.

### CONTROL

Using workflows, NC Protect can trigger access approval requests for policy officers or managers, or 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.

### REPORT

A dynamic Results Viewer provides centralized reporting and management of classified data. It reports 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. The list can be filtered based on flexible search conditions and exported to various formats for reporting or archiving purposes.



## ADVANTAGES OF INTELLIGENT, ITEM-LEVEL SECURITY

Nucleus Cyber's granular data-centric approach to security enables conditional access control down to the item-level using secure metadata and user attributes. Since access and usage rights can be applied to specific content or individual files (using classification), as compared with solutions that secure or encrypt at the app or location level, sensitive content can be safely stored, shared and collaborated on from any Yammer group regardless of user membership. In addition to better protecting your organization from an accidental breach, this approach also controls the proliferation of Yammer groups to support individual collaboration scenarios.



info@nucleuscyber.com | www.nucleuscyber.com