NCPROTECT™

PROTECCIÓN AVANZADA DE LA INFORMACIÓN PARA MICROSOFT 365 & SHAREPOINT®

Resumen ejecutivo

NC Protect™ ajusta dinámicamente y en tiempo real la protección de archivos basándose en el análisis de los atributos del contenido y los atributos del usuario para garantizar que los usuarios vean, usen y compartan archivos de acuerdo con las regulaciones y las políticas de seguridad de su negocio.

NC Protect protege los archivos en tránsito sin la sobrecarga de los permisos de usuario complejos o las limitaciones del cifrado en reposo, lo que garantiza que los datos estén protegidos en el momento en que se utilizan o comparten. Restringe el uso y visualización de datos basada en la clasificación del archivo y la ubicación actual del usuario, el dispositivo y los derechos de acceso, encriptando automáticamente los archivos cuando los datos salen de la seguridad de la información corporativa.

Beneficios clave

- Ajuste el acceso y la protección en función del archivo y los atributos del usuario en tiempo real
- Aplica automáticamente políticas del negocio a los archivos a medida que se mueven entre personas y ubicaciones
- Recorte las reglas del menú en las aplicaciones de Microsoft 365 según el contexto del usuario o el contenido del archivo
- Agregue marcas de agua personalizadas y específicas del usuario a documentos de Word, PowerPoint, Excel y PDF
- Proporcione acceso seguro de solo lectura a través de un visor de archivos sin huella
- Aplique cifrado de archivos específico del usuario y DLP

EXCELENTE PARA LA COLABORACIÓN, PROBLEMÁTICO PARA LA SEGURIDAD DE LOS DATOS

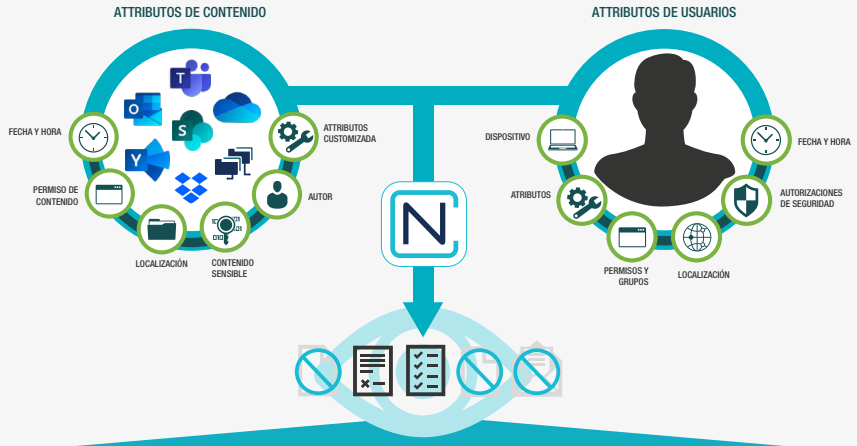
Con las aplicaciones de colaboración modernas, los usuarios pueden acceder a los datos desde una alarmante variedad de ubicaciones. Entre Azure, Office 365 y otras plataformas en la nube, las empresas están adoptando nuevas tecnologías más rápido que nunca y la metodología de prevención de pérdida de datos debe mantenerse al día. La política de protección de datos debe ser lo suficientemente firme para adaptarse a la adopción de nuevos servicios en la nube, y lo suficientemente flexible para permitir que sus usuarios trabajen cuando, donde y como quieran.

SEGURIDAD Y CUMPLIMIENTO SIMPLES, RÁPIDAS Y ESCALABLES PARA APLICACIONES MICROSOFT

NC Protect proporciona seguridad avanzada centrada en datos para las aplicaciones de Microsoft 365, incluidos los correos electrónicos de Office 365, SharePoint Online y locales, OneDrive, Teams, Yammer y Exchange. La plataforma permite a las empresas buscar, clasificar y proteger automáticamente datos no estructurados y determinar cómo se puede acceder a ellos con control granular en entornos de nube, locales e híbridos.

NC Protect funciona de forma nativa con los productos de Microsoft y mejora la seguridad para restringir el uso de la funcionalidad de Microsoft, incluidos los elementos del usuario, interfaz, métodos para ver archivos y cifrado o restricción de archivos adjuntos enviados a través del correo electrónico de Exchange. No requiere ninguna aplicación adicional del lado del cliente, lo que reduce la sobrecarga de TI y los riesgos involucrados en la implementación de nuevos servicios en la nube o políticas BYOD, NC Protect ofrece protección de información avanzada que es simple, rápida y escalable.

ACCESO CONDICIONAL Y PROTECCIÓN DE DATOS



En tiempo real, Determiné el control del acceso contextual:

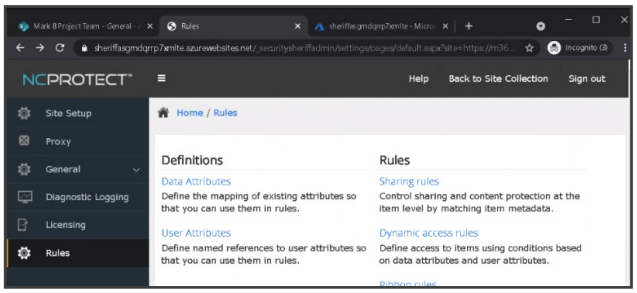
Lo que ve un usuario al ver y buscar archivos	Qué usuario puede, abrir, editar, copiar o bajar archivos	Qué usuario puede, abrir, editar, copiar o bajar archivos	Que un archivo es encriptado cuando se guarda, copia o envía por mail	Que un archivo solo pueda verse en una aplicación segura	Que acciones están habilitadas en la interfaz del usuario de Microsoft

SEGURIDAD Y CUMPLIMIENTO SIMPLES, RÁPIDAS Y ESCALABLES PARA APLICACIONES MICROSOFT

NC Protect aumenta la seguridad de las aplicaciones nativas en las soluciones de Office 365 y SharePoint utilizando los datos de identidad únicos que se crean a lo largo del tiempo.

Usando metadatos, etiquetas de confidencialidad MIP y atributos como nombre de archivo, autoría y sellos de fecha, así como un contexto más transitorio como ubicación IP, dispositivo, fecha y hora, NC Protect aplica control de acceso condicional basado en atributos (ABAC) y derechos de uso. para admitir todas las reglas comerciales y permitir una colaboración segura.

NC Protect toma sus políticas de seguridad de datos y las hace cumplir para todos y cada uno de los usuarios y dispositivos, de manera completamente transparente para el usuario final.



DESCUBRE Y CLASIFICA

NC Protect escanea e inspecciona archivos en aplicaciones de colaboración locales y en la nube en busca de datos confidenciales o regulados de acuerdo con políticas definidas. Cuando lo detecta, clasifica automáticamente el archivo y aplica la protección de la información según su confidencialidad y sus políticas. También puede aprovechar las etiquetas de confidencialidad de MIP en combinación con otros atributos de usuario y archivo para controlar el acceso y aplicar la protección de la información.

RESTRINGE

Utilice seguridad granular para restringir automáticamente el acceso, el uso compartido y la protección del contenido según las reglas asociadas con la clasificación del archivo o la etiqueta de confidencialidad de MIP. El acceso a un archivo se puede restringir a un individuo o grupo específico, incluso si una audiencia más amplia tiene acceso al resto del sitio donde el elemento físicamente reside. La gestión del acceso a nivel de archivo es posible aprovechando los datos y los atributos del usuario, en lugar de la ubicación de los datos.

CIFRADO

NC Protect puede proteger aún más el contenido cifrándolo para garantizar que solo los usuarios debidamente autorizados y acreditados puedan acceder al contenido incluso si tienen privilegios administrativos, lo que hace que sea seguro almacenar documentos confidenciales como: documentos del directorio, o de recursos humanos. También garantiza que se pueda controlar el acceso a los datos compartidos con terceros, incluso cuando se eliminan de un sitio.

PREVENCIÓN

También puede definir reglas en NC Protect para evitar la distribución de información sensible o documentos confidenciales para minimizar el riesgo de pérdida de datos. Por ejemplo, si se agrega un archivo a un sitio y el miembro no tiene el acceso adecuado a esa categoría de documento, el archivo se puede ocultar a la vista de la persona no autorizada. También se puede evitar que los usuarios impriman, envíen correos electrónicos a través de Exchange, guarden o copien el contenido de los documentos de Microsoft Office y archivos PDF fuera de Office 365, SharePoint o OneDrive.

CONTROL

Mediante flujos de trabajo, NC Protect puede activar solicitudes de aprobación de acceso para funcionarios o administradores de políticas o para solicitar justificaciones a los usuarios. Se pueden desarrollar reglas comerciales completas para que pueda remediar los problemas de cumplimiento y encargar a las personas adecuadas en la organización que revisen y potencialmente clasifiquen, alteren la clasificación o cifren el contenido.

CAPACIDADES ÚNICAS PARA PROTECCIÓN DE DATOS

NC Protect funciona de forma nativa con los productos de seguridad y colaboración de Microsoft para aumentar las funciones nativas para hacer cumplir el acceso seguro de solo lectura, ocultar archivos confidenciales de usuarios no autorizados, recortar el menú de la aplicación, aplique marcas de agua personalizadas dinámicas y cifre o restrinja los archivos adjuntos enviados a través del correo electrónico de Exchange.

REDACCIÓN

NC Protect puede eliminar/redactar información sensible o confidencial, como palabras clave o frases, en un documento cuando se ve en su aplicación nativa (Word, Excel, PowerPoint y PDF) o cuando el archivo se presenta en el lector seguro de NC Protect por motivos legales o de seguridad.

AUDITORIA Y REPORTERIA

Un visor de resultados dinámico proporciona informes y gestión centralizados de datos clasificados. Informar sobre la cantidad de problemas identificados por nivel de clasificación y permite a los oficiales de políticas revisar los resultados y volver a escanear, reclasificar o volver a aplicar los permisos si es necesario. Integre la actividad del usuario y los registros de protección con herramientas SIEM como Splunk o Microsoft Sentinel para análisis adicionales y acciones posteriores.

VENTAJAS DEL ACCESO Y CONTROL DINAMICO BASADO EN ATRIBUTOS

El enfoque de seguridad centrado en datos granulares de archTIS permite el control de acceso condicional hasta el nivel de artículo utilizando tanto datos como atributos de usuario. Dado que la protección del acceso y la información se aplica a archivos, chats y mensajes individuales, en comparación con las soluciones que protegen o cifran en el nivel de la aplicación o la ubicación, el contenido confidencial se puede almacenar, compartir y colaborar de forma segura en Teams y otras aplicaciones de Office 365, independientemente de membresía de usuario. Este enfoque también controla la proliferación de equipos para admitir escenarios de colaboración individuales.

archTIS

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