HOJA DE DATOS

Identity Manager: Data Governance Edition

La gestión de datos le otorga el control del acceso a los datos confidenciales

Beneficios

- Encuentra y asigna los propietarios a los datos no estructurados.
- Ofrece en una "única consola" visibilidad de la información de uso de datos anteriormente faltante.
- Reduce la exposición a las infracciones de seguridad al permitir que los propietarios de datos determinen qué usuarios deben tener acceso a los datos confidenciales.
- Mejora la eficacia al reducir la carga del área de TI para cumplir con las solicitudes de acceso.
- Demuestra el cumplimiento a los auditores con informes de accesos de usuarios y confirmación.

Requisitos del sistema

Para obtener una lista completa de los requisitos del sistema, visite oneidentity.com/products/identity-manager-data-governance/.

Muchas empresas de hoy en día están en riesgo debido a una protección de datos inadecuada. Los responsables de la seguridad y el cumplimiento enfrentan mayores dificultades en cuanto a la protección de los datos confidenciales porque no tienen implementado un sistema de acceso adecuado. Como resultado, el cumplimiento es insuficiente, lo que pone a las empresas en riesgo.

Si bien los administradores del área de TI tienen permiso para otorgar acceso a datos específicos, a menudo lo hacen sin conocer las repercusiones de esto que, con frecuencia, genera el acceso no autorizado de personas dentro de la empresa, mientras se exponen otras cuentas a amenazas externas. Una mayor cantidad de controles internos garantiza que el acceso a los datos no estructurados permanezca en manos apropiadas para que la seguridad y las normas no se infrinjan. Identity Manager-Data Governance Edition, parte de las soluciones de One Identity, protege su empresa al otorgar control de acceso a los propietarios de empresas que saben quiénes deberían tener acceso a qué datos confidenciales, con la capacidad para analizar, aprobar y cumplir las solicitudes de acceso a los datos no estructurados para archivos, carpetas y recursos compartidos

ONE IDENTITY™

Figura 1. Mapa de calor: Los mapas de calor incluyen el índice de riesgo y las infracciones a las políticas de los datos actuales y una comparación histórica de los datos anteriores.

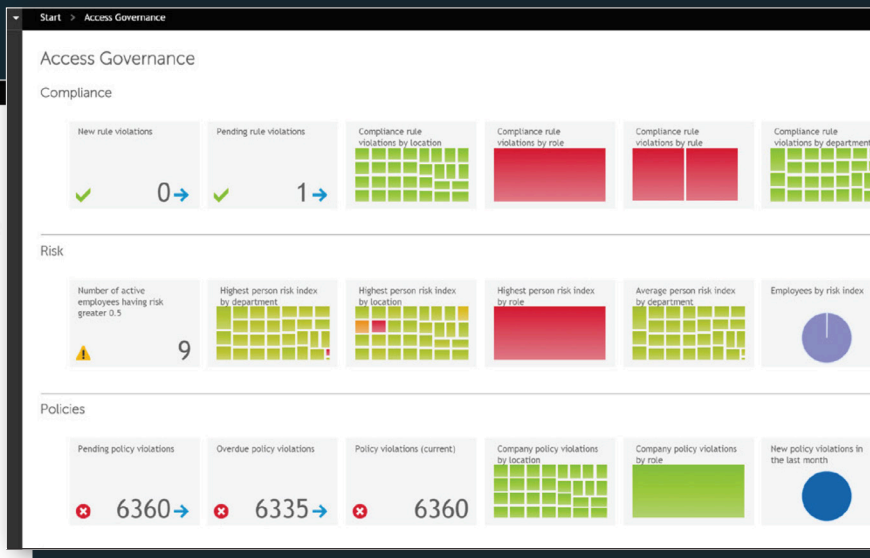

Figura 2. Datos gestionados: El propietario de los datos aprueba las solicitudes de acceso, informa, audita y administra el ciclo de vida de los datos gestionados.

en dispositivos NAS, NTFS y SharePoint. Identity Manager – Data Governance Edition ayuda a los propietarios de datos (no el área de TI) a determinar quién debería tener acceso, y automatiza el flujo de trabajo de solicitud y aprobación, para evitar que su empresa sea el próximo titular de seguridad y, al mismo tiempo, reducir la carga en el área de TI.

Características

Gestión de los servicios en la nube
Gestione los servicios en la nube y realice el informe de acceso con el soporte para Microsoft SharePoint Online y OneDrive.

Clasificación de datos
Clasifique los datos gestionados de manera manual. Los propietarios de empresas pueden colocar las clasificaciones en el portal web. Proporciona políticas rápidas y cálculos de los riesgos basados en la asignación del nivel de clasificación.

Acceso restringido
Defina políticas de acceso para su empresa, a fin de garantizar que solo los usuarios autorizados tengan acceso a los datos confidenciales no estructurados. Identity Manager – Data Governance Edition bloquea los datos confidenciales, como archivos, carpetas y recursos compartidos a través de dispositivos NAS, NTFS y SharePoint.

Asignación del propietario de los datos
Determine y asigne el propietario adecuado de los datos para todas las futuras solicitudes de acceso al evaluar los patrones de uso, y el acceso de escritura y lectura.

Auditoría simplificada
Identifique el acceso de los usuarios a recursos empresariales, como archivos, carpetas y recursos compartidos a través de dispositivos NAS, NTFS y SharePoint, para proporcionar información clave durante las preparaciones de auditoría.

Solicitudes de acceso automatizadas
Use flujos de trabajo integrados para dirigir automáticamente las solicitudes de acceso del portal de solicitudes al propietario de datos correspondiente. Las solicitudes aprobadas se completan automática y correctamente, sin ninguna carga para el área de TI.

Verificación de acceso
Garantice que solo los usuarios autorizados tengan acceso a los recursos específicos, incluidos aquellos que han abandonado la empresa o el departamento, o aquellos cuyos roles hayan cambiado. Identity Manager – Data Governance Edition le permite monitorear la actividad de los usuarios y recursos, así como configurar y programar un proceso de recertificación para los propietarios de datos a fin de verificar y certificar el acceso de los empleados.

Panel personalizado
Vea las tendencias, el acceso a los datos históricos y actuales, y estado de certificación en su panel personalizado con informes que pueden usarse para comprobar el cumplimiento con los auditores.

Acerca de One Identity

La familia de soluciones de administración de identidades y acceso (IAM) de One Identity ofrece IAM para el mundo real, incluidas las soluciones centradas en la empresa, modulares e integradas, además de listas para el futuro orientadas a la gestión de identidades, la administración del acceso y la administración de privilegios.

Obtenga más información en OneIdentity.com.

Datasheet-IdentityMgr-DataGovEd-US-CW-es_XL-WL-24725

ONE IDENTITY™