EXPRESS UNSTRUCTURED DATA RISK ASSESSMENT REPORT

Prepared for:

Acme

DOCUMENT CHANGE CONTROL

Version	Release Date	Summary of Changes	Addendum Number	Name
1.0	***April 2, 2015***	***1st draft***		***David Gibson***

Table of Contents

Contents

1. Executive Summary

Introduction:

On date, Varonis Professional Services performed a review of Acme's unstructured data and directory services environments to identify areas of potential exposure and opportunities for improvement. A sample of Acme's data stores and user repositories were assessed for risks in the areas of access controls and authorization processes, privileged and end user access monitoring, Active Directory structure, NTFS and sharing permissions structure, and data retention proficiency, in accordance with Varonis best practices and industry standards.

Background:

For unstructured data, the most fundamental preventive control is the access control lists. Access control lists (ACLs) permit their "listed" users some level of access (e.g. read, modify) to the folders and files they pertain to, and prevent others from accessing them. Access controls most typically:

- Are applied to data containers like folder and SharePoint sites, though files may have their own unique ACLs.
- Refer to groups of users that reside in a user-repository (e.g. Active Directory), though individual users may also be listed.
- Track permission level associated with each listed group or user object, such as read-only, modify, full control, etc.

Despite their importance, access controls are difficult to analyze and are most often maintained through time-consuming, error-prone manual processes. As a result, access control lists and the groups they refer to are frequently out of date or inconsistent, resulting in users with access to far more data than they require to perform their jobs. Without correctly set and well-maintained access controls, organizations risk data theft, loss, misuse, and abuse. Furthermore, these risks often increase over time as data grows and preventive controls fall further into disarray.

In many information systems preventive controls are augmented with detective controls that "detect" inappropriate or undesirable actions. Unfortunately, for unstructured data, access activity is rarely audited, tracked or analyzed. This means that not only do users have access to far more data than they require, but that they can also access data without leaving any trace of their activities, and without tripping any "alarm" when they access data inappropriately. With inadequate preventive controls and nonexistent detective controls, an organization's unstructured data is vulnerable to both insiders and outsiders (that have appropriated an insider's credentials), and the organization has little hope of preventing abuse, detecting abuse, or analyzing an incident's impact after the fact.

Additionally, without adequate controls and analytical capabilities, organizations struggle to answer fundamental questions about their data, such as:

- Who can and should have access to data?
- Who is using or abusing data?
- Who deleted data?
- Which data is sensitive or regulated?
- Who does data belong to, or who is the owner?
- Is data stored in the correct places?
- Is data archived or deleted appropriately?

This Varonis unstructured data risk assessment inspects key controls and capabilities pertaining to unstructured data, identifies areas of risk and controls deficiencies, and makes recommendations on where and how risk can be reduced.

Opinion:

- Acme is not able to assess risk associated with PCI data not being secured properly because it has neither the ability to identify unstructured data containing PCI data, nor adequate controls to assess that unstructured data is correctly accessible and used.
- On the file system, global access was found on 365,543 folders in the sample of Acme's environment. This represents nearly 50% percent of all folders in the sample, and these excessive permissions must be removed.
- Nearly 622 folders were detected with NTFS inheritance inconsistencies. Again, although this represents only .10% of all folders, broken NTFS inheritance is a serious condition which must be remediated.
- Stale general data was also detected in abundance across all of the sampled file servers. On 2 servers, more than 50% of the data was identified as stale. In total, 45,246 folders containing stale data were found. This data totals almost 2TB of storage space, or 66% of all data in the sample environment. Significant cost savings may be realized by deleting or archiving this unused data.

2. Assessment Scope

The following servers and user repositories were included in the scope of this assessment. Unless otherwise noted, the numbers provided represent a total or average of all in-scope resources. The scope of this assessment is limited to the file servers covered by the Varonis Data Governance Framework evaluation license.

FILE SERVERS

- Server 1
- Server 2

DOMAINS

- Domain 1

3. Capabilities Assessment

Grade	Capability
Full	Track and report on Active Directory changes (group membership, GPO, etc.)
Partial	Track and report Access control list changes
None	Track and report on file usage (creation, modifications, deletions, etc.)
None	Track and report on email usage (send, receive, send as, etc.)
None	Detect unusual file and email activity
Partial	Analyze potential access for file container objects
Partial	Analyze potential access for email container objects
None	Analyze user or group potential access across file containers
None	Analyze user or group potential access across email stores
Partial	Identify sensitive or regulated content
Partial	Identify stale, unused content

4. Summary findings and security vulnerabilities

The following is a summary of the results of the risk findings for the identified measurement. A detailed overview is included in Section 4.

Risk Level	Results	Description
High		Folders with Global Group Access Including Subfolders
High		Sensitive files with Global Access
High		Stale but enabled users AD accounts
High		Folders with Inconsistent (Broken) Permissions
Medium		Users with passwords that don’t expire
Medium		Folders with stale data
Medium		Looped nested groups within AD
Low		Folders with unique permissions
Low		Folders that are protected from inheritance
Low		Folders that have unresolved SIDs
Low		Security groups with no users in AD
Low		Folders where the user is assigned directly

4.1 High Risk

4.1.1 Folders with global group access

Description: Global access groups include groups such as Everyone, Domain Users, and Authenticated Users. These groups allow all or most users within a company to view or modify files. To achieve a least-privileged access model, it is critical to eliminate these groups wherever they are not absolutely needed, and further restrict access to only those who require access.

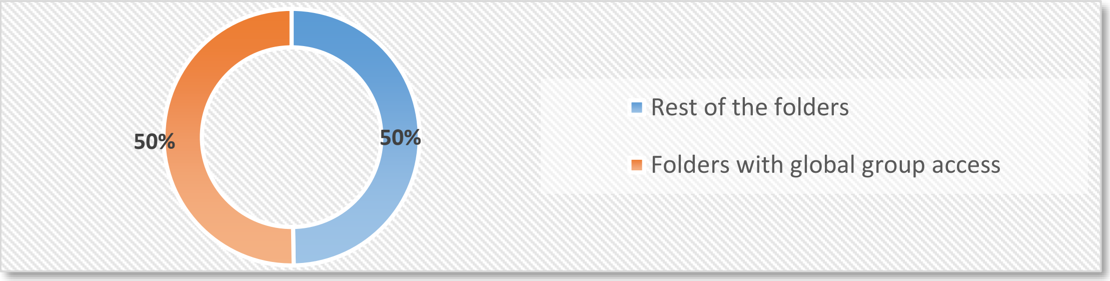
Risk of non-compliance: Failing to reduce or eliminate the use of global access groups will allow anyone within an organization to access data with these access controls. A common misconception is that most data breaches are due to complex hacking or exploits, from external sources. In reality, many data breaches come from within an organization. When users have access to data that they do not need, the likelihood of data leakage is high. Excessive user access through global groups is a key failure point for many security and compliance audits.

Performance range: 0-100%

Optimal range: 0%

Action items: Remove global access group permissions by utilizing the DatAdvantage to identify folders open to global group access, and their active users. Place active users in a new group, and replace the global access group with the new group on the ACL.

File System	*Results*	*Impact*
Folders with global group access	**2,365,523**	**High**



4.1.2 Folders with inconsistent permissions

Description: The NTFS permissions structure is highly flexible. Folders may be individually protected or may inherit some or all of their permissions from a parent folder. Data is frequently being moved between folders, domains, and servers and re-permissioned using bulk editing tools such as xcacls. Without careful inspection, these moves and changes can lead to inconsistencies in the NTFS inheritance structure. Inconsistent permissions must be identified and repaired prior to optimizing access controls.

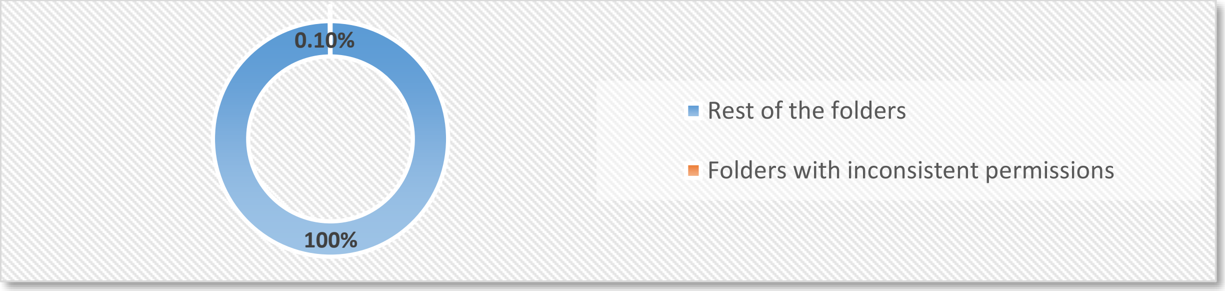
Risk of non-compliance: Failing to repair inconsistent permissions will lead an organization to believe they have successfully locked-down access to data, while the reality may be quite different. Inconsistent inheritance, a common by-product of inconsistent permissions, may expose important data to individuals who should not have access to that data. While organizations make significant investments in firewalls, IAM, IPS, DLP, and SIEM, none of these systems can prevent an insider from accessing over-exposed data. The first step in securing data is understanding who has permission to access that data, but inconsistencies in the NTFS inheritance structure can make this impossible.

Performance range: 0-100%

Optimal range: 0%

Action items: Repair inconsistent permissions by reestablishing NTFS inheritance on the portions of the file system where the inheritance structure has become inconsistent.

File System	*Results*	*Impact*
Folders with inconsistent permissions	**4622**	**High**



4.1.3 Sensitive files with global group access

Description: Many files contain critical information about employees, customers, projects, clients, or other business-sensitive content. Some of this content may be subject to industry regulation, such as C-SOX, PIPEDA, or PCI. When global access groups grant access to such data, there is significant risk to the business. These instances must be identified and remediated so that only the appropriate users retain access to this sensitive, regulated data.

Risk of non-compliance: While any data that is exposed to unneeded user access is problematic, data containing sensitive information requires particularly close attention. These sensitive files include custodial data such as credit card numbers, personally identifiable information (PII) such as social insurance numbers, and personal health information (PHI), as well as business intellectual property, including business plans and product designs. This data must remain tightly controlled, and any breach or leakage of this information may potentially damage the business.

Performance range: 0-100%

Optimal range: 0%

Action items: Acme has purchased Data Classification but has not configured it. Without Data Classification being configured it is impossible to determine risks associated with sensitive files. For this reason we highly recommend Acme configure Data Classification as soon as possible on all file servers in their environment. That includes but is not limited to their main network and their PCI network.

4.1.4 Stale enabled users

Description: "Stale enabled users" are user accounts which are not disabled, but have not been utilized to log in to the domain. When users, including both employees and contractors, leave a company, or applications are removed from production, the associated Directory Service accounts should be disabled and/or deleted. Stale enabled accounts should be identified and promptly disabled if not justified.

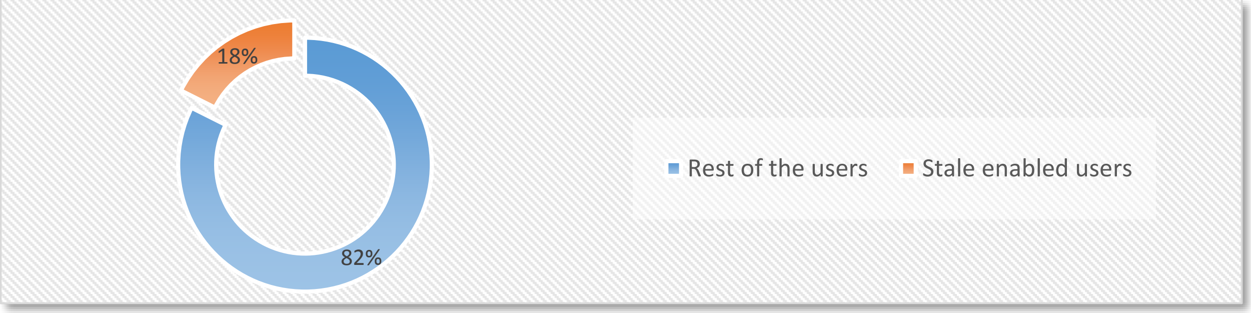
Risk of non-compliance: Stale enabled accounts still retain all of the access permissions they were granted while active. While active, they become a target for exploitation and malicious use. These accounts increase potential access to data, and may be used in attempts to leak data outside of an organization.

Performance range: 0-100%

Optimal range: 0%

Action items: Review stale enabled accounts to determine if they are necessary. Delete or disable accounts as needed.

File System	*Results*	*Impact*
Stale enabled users	**842**	**High**



4.2 Medium Risk

4.2.1 Folders with stale data / Amount of stale data

Description: The volume of electronic data that companies manage continues to grow exponentially. Much of this data becomes stale or unused immediately after it is created. Stale data represents little value to the business while it’s not being used, but still carries with it risk and potential financial impact if used inappropriately. Data that has not been accessed for a long period of time should be identified and archived, or deleted if no longer needed.

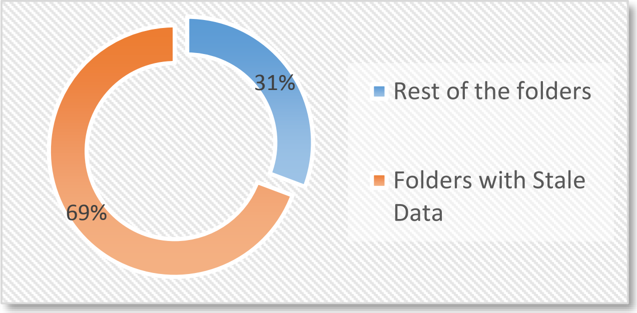
Risk of non-compliance: In addition to the increased risk of managing stale data, unused data is expensive to manage. Data which is kept beyond a pre-determined retention period can expose an organization to additional liability.

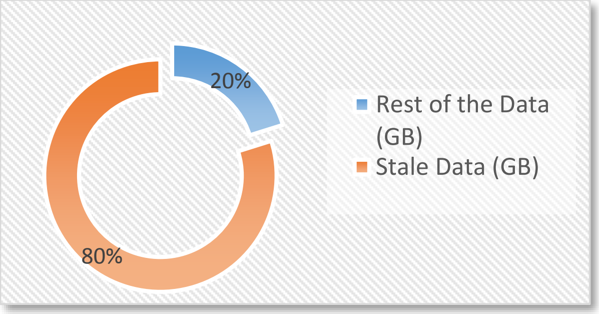
Performance range: 0-100%

Optimal range: 0%

Action items: Utilize DatAdvantage to identify stale data, and determine if the data can be moved, archived, or deleted.

File System	*Results*	*Impact*
Folders with Stale Data	**3,260,246**	**Medium**
Amount of Stale Data	**39,095 GB**	**Medium**





4.2.2 Users with non-expiring passwords

Description: Users with non-expiring passwords will never be prompted to change their password. A strong security policy should include changing of passwords at a predetermined interval. Accounts which maintain permanent passwords must be identified and corrected.

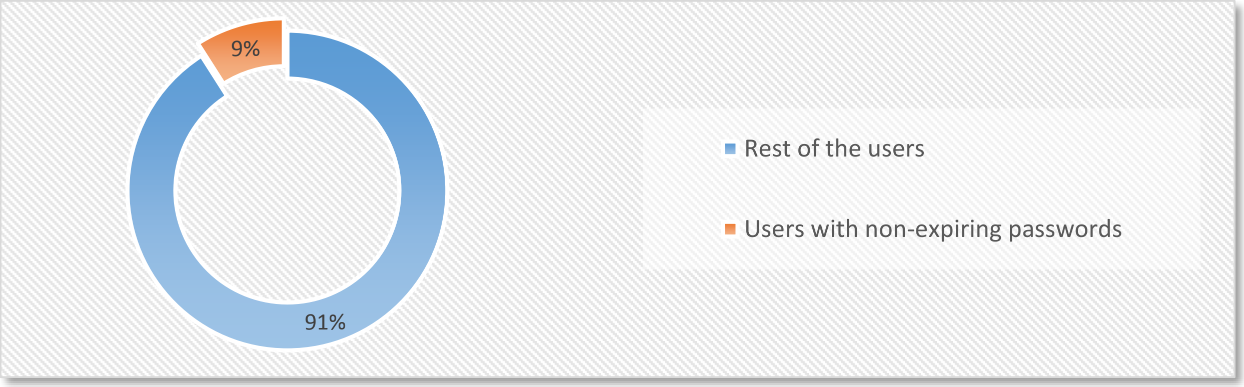
Risk of non-compliance: A non-expiring password allows anyone who has ever used the account to have access to the information available via that account. In many cases this need no longer exists. Additionally, should a list of hashed passwords be acquired in a security breach, a non-expiring password gives a potential hacker an unlimited amount of time to brute-force the encrypted password, making these accounts an attractive target for a malicious exploit.

Performance range: 0-100%

Optimal range: 0%

Action items: Update accounts to comply with a strong password policy, including regular password changes. Service accounts with non-expiring passwords should be kept to a minimum.

File System	*Results*	*Impact*
Users with non-expiring passwords	**432**	**Medium**



4.2.3 Looped nested groups

Description: Active Directory allows groups to be nested within groups. While useful in many cases, this functionality allows a group to be nested within a group, even if the nested group contains the parent group as a member, creating a cyclical condition (e.g. A contains B, B contains A). As many applications and scripts enumerate group membership recursively, looped nested groups can cause application crashes or unexpected behavior. Looped nested groups must be identified and the cyclical condition removed.

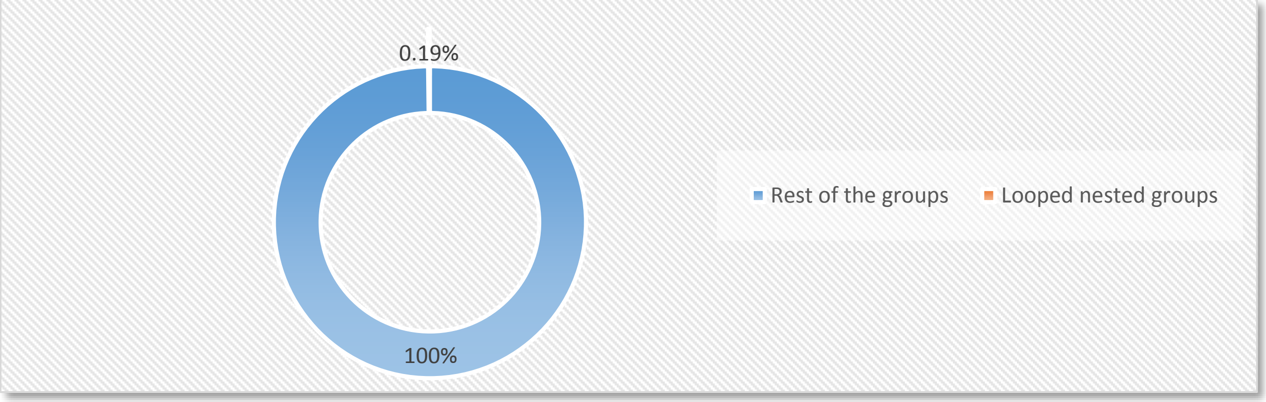
Risk of non-compliance: Although looped nested groups do not inhibit proper authentication within built-in Windows processes, many organizations utilize and rely on 3rd party applications and scripts. Looped nested groups may cause failures in these applications, causing them to fail to function, or to consume excessive processing resources.

Performance range: 0-100%

Optimal range: 0%

Action items: Utilize DatAdvantage to identify the looped nested groups, and remove the cyclical condition.

File System	*Results*	*Impact*
Looped nested groups	**4**	**Medium**



4.3 Low Risk

4.3.1 Folders with unique permissions (Not blocking inheritance)

Description: A folder with unique permissions inherits its ACL from a parent folder and has additional ACEs applied to it. Unlike folders that inherit all their permissions, or inherit none of their permissions (protected), these folders permissions are more complex to analyze and can cause confusion when trying to identify the effective permissions on these folders. In some cases, folders inadvertently become unique through the use of permission utilities or data migration tools. When large amounts of folders containing unique permissions are discovered, their inheritance structure should be reviewed, and if possible, reestablished.

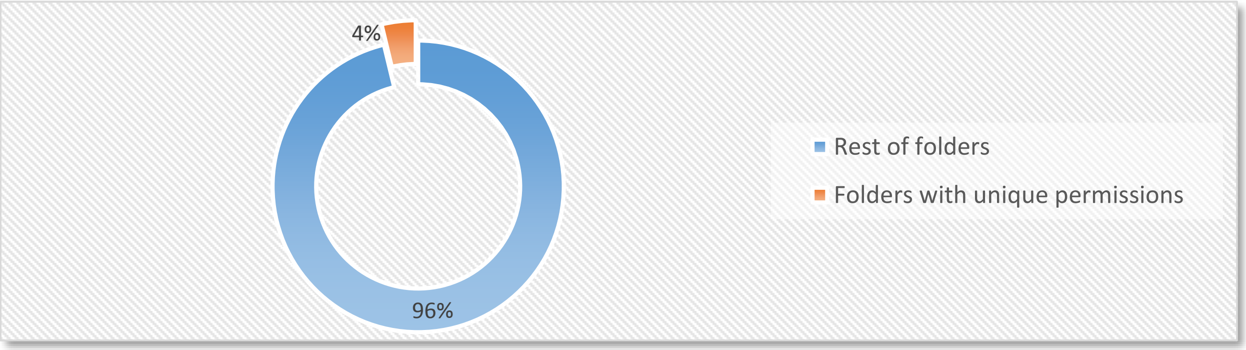
Risk of non-compliance: With the high risk of unauthorized access to data, effective management of access permissions is critical in ensuring that data is secured using a least-privileged access model. The more complexity that exists in a file system structure, the more risk there is for users to gain unintended access. While unique permissions are necessary in some cases, they should be used sparingly in order to simplify access management.

Performance range: 0-100%

Optimal range: < 10%

Action items: Review permissions structure to determine if folder uniqueness is required. If not, allow the folder to re-inherit parent permissions, replacing unique ACEs.

File System	*Results*	*Impact*
Folders with unique Permissions	**177,815**	**Low**



4.3.2 Protected folders

Description: Protected folders are NTFS folders which contain an explicitly defined ACL and will inherit no ACE's from their parent folders. Best practices for permissions management dictate the usage of protected folders at higher levels in the directory tree, propagating their permissions down through the subfolders via inheritance. A large number of protected folders relative to the total number of folders on the filesystem may indicate protected folders at varying and deep levels of the folder structure. Deeply nested protected folders are difficult to locate and control, making permissions management complex. When a high percentage of protected folders are found, the access management process should be reviewed and adjusted.

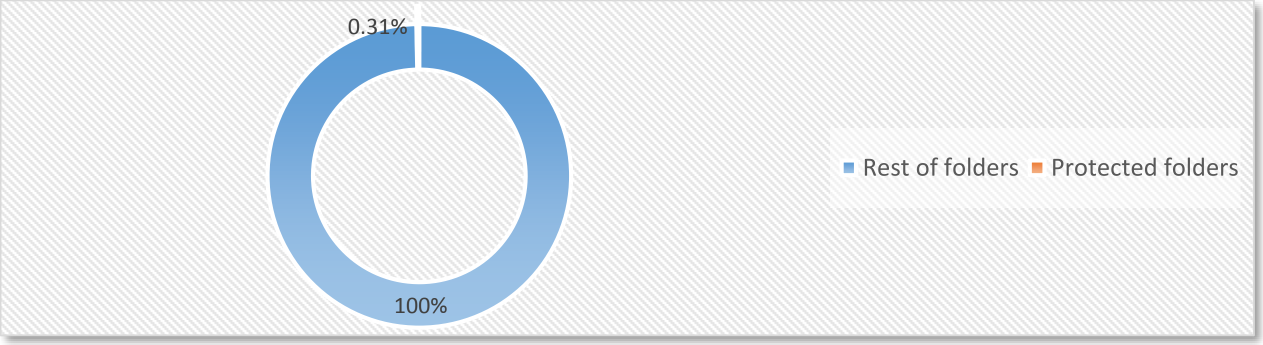
Risk of non-compliance: While protected folders are necessary to establish a starting point for an inheritance structure, when found at deeper levels of the file system, they may contain users and permissions which were not visible at the higher levels. This may lead an administrator to assume that permissions to a folder are configured correctly, when an underlying folder's permissions may not be. If these underlying folders contain sensitive data, this data may be exposed to individuals who should not have privileges to view the data in these folders, yet they do.

Performance range: 0-100%

Optimal range: < 5%

Action items: None.

File System	*Results*	*Impact*
Protected folders	**14,679**	**Low**



4.3.3 Folders with direct user ACEs

Description: Best practices for access management dictate that a user be placed within a group, and a group be permissioned on an ACL (access control list). However, users are sometimes given access to data by assigning their account permissions directly on the folder ACL. This is sometimes performed to provide a user with immediate access to that data. However, when the time arises to revoke a user's access, it becomes difficult to find all of the folders across the file system where access was granted to individual accounts. Should a user's account be deleted, these instances of direct permissions will become unresolved SIDs. Folders with user ACEs should be identified and those user accounts placed into appropriate groups.

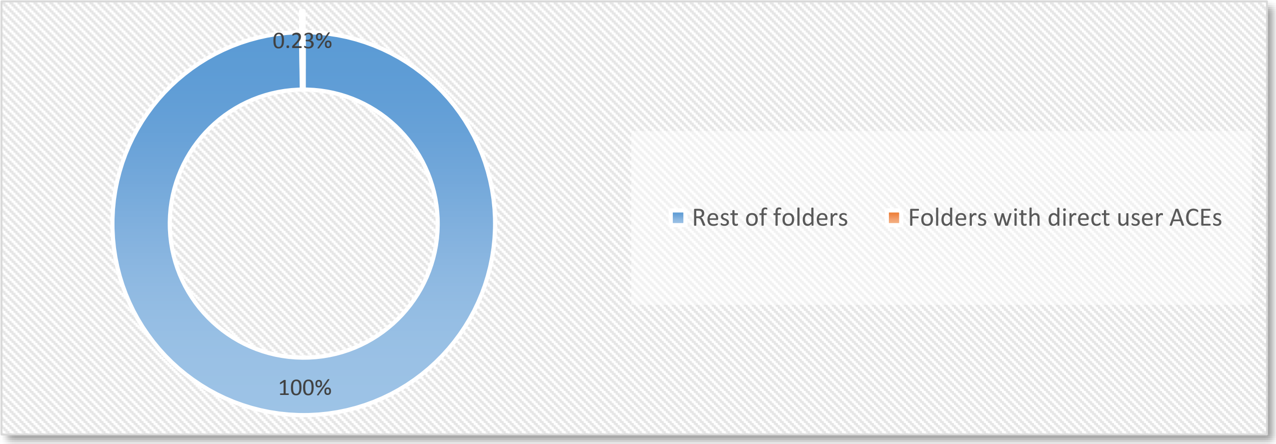
Risk of non-compliance: Users who are directly permissioned on an ACL obtain the same access as through a security group. While the account is enabled, these account privileges cannot be managed with Active Directory groups. Because every instance of user access through individual ACEs must be identified directly on the file system, these permissions are difficult to locate, and may create inappropriate access to data, including sensitive data.

Performance range: 0-100%

Optimal range: 0%

Action items: Utilize DatAdvantage to identify folders with direct user permissions. Place users into an appropriate group, and remove the user ACE from the ACL.

File System	*Results*	*Impact*
Folders with direct user ACEs	**10,724**	**Low**



4.3.4 Unresolved SIDs

Description: Unresolved SIDs (security identifiers) occur when a group or user ACE (access control entry) is permissioned directly on a folder, and that group or user's associated Active Directory account is deleted. The SID becomes orphaned, and remains on the ACL for the folder. Unresolved SIDs should be identified and removed in order to ensure a well-organized directory structure.

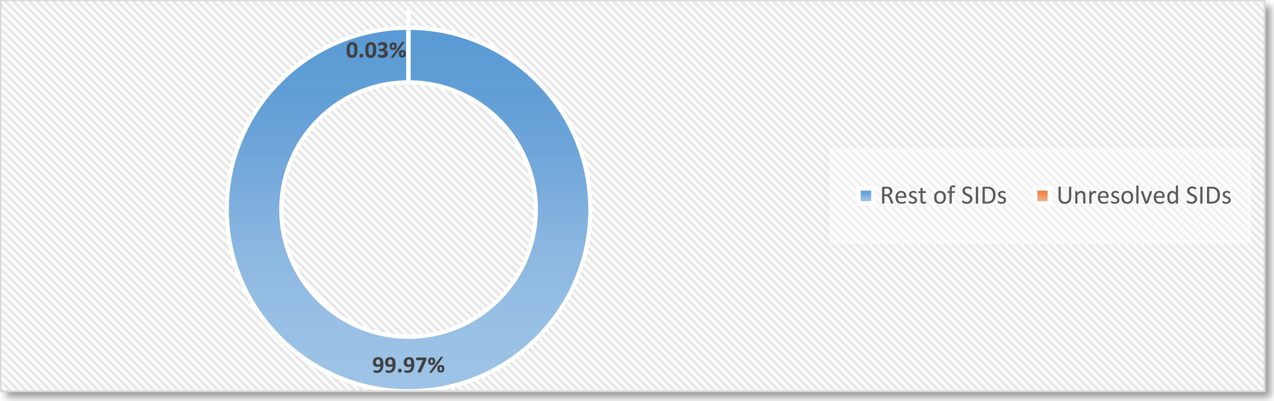
Risk of non-compliance: With the high risk of unauthorized access to data, effective management of access permissions is critical in ensuring that data is secured using a least-privileged access model. The more complexity that exists in a file system structure, the more risk there is for users to gain unintended access. Unresolved SIDs increase the complexity of the ACL and should be removed. Additionally, an unresolved SID with access to data provides a potential target for a token manipulation attack.

Performance range: 0-100%

Optimal range: 0%

Action items: Utilize DatAdvantage to identify folders with unresolved SIDs, and remove them from the ACL.

File System	*Results*	*Impact*
Folders with Unresolved SIDs	**5,846**	**Low**



4.3.5 Empty security groups

Description: Empty security groups are active directory groups containing no users. These groups clutter the active directory, and should be located and removed. Unnecessary resources, including empty security groups, should be identified and removed from any directory service where they are configured.

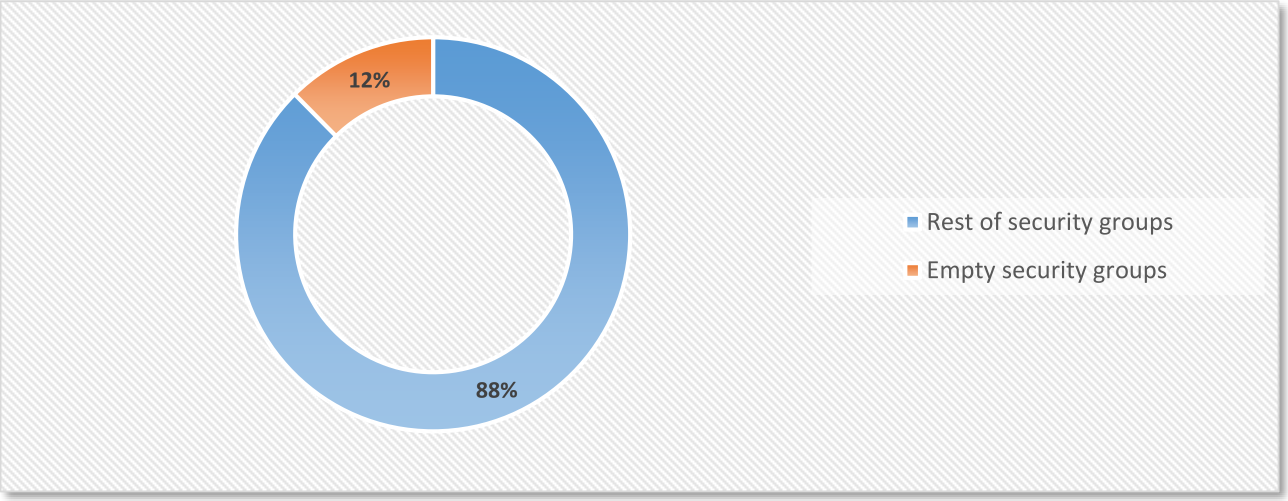
Risk of non-compliance: Although empty security groups are not actively granting access to data, any user that is placed into these groups would instantly be given access anywhere the group is permissioned on a file system. Reusing groups in this way can lead to unintentional access permissions for the user.

Performance range: 0-100%

Optimal range: 0%

Action items: Utilize DatAdvantage to identify empty security groups, and remove them.

File System	*Results*	*Impact*
Empty security groups	**267**	**Low**



4.4 No Risk/General Information

4.4.1 The items below are provided for informational purposes only and do not represent increased risk. They are included purely to provide the reader with the relevant statistics that were analyzed when creating this report.

File System	*Results*
Folders	**4,706522**
Files	**42,783,285**
Permissions	**23,229,590**
Size of folders	**48,969.55 GB**
Inherited folders	**4,528,707**
Groups	**2,152**
Users	**4,781**
Computer accounts	**8,906**
OUs	**3,363**
Disabled users	**633**
Folders without data owners	**4,706,522**

Unstructured Data Governance Best Practices Questionnaire

	YES	NO
Data Owners are defined in the environment	☐	☒
Users have unique accounts for Administrative and User level	☒	☐
IT Security Administrators have FULL NTFS access to all folders	☒	☐
Data security is managed through NTFS and not Share permissions	☒	☐
The only users who have FULL access to data are a small, select group of IT Admins	☒	☐
Permissions are inheriting starting 3 levels below the share	☒	☐
Each share or base group folder has 1 MODIFY and 1 READ group for access (1:1 access – folder ratio)	☐	☒
There is repeatable, documented process for access request provisioning	☒	☐
Business data owners determine who should have access to business data	☒	☐
There is repeatable, documented process for access recertification	☒	☐
There are no folders where global groups such as Everyone, Domain Users and Authenticated Users have access permissions higher than LIST permissions	☐	☒
Folders with sensitive data are known and access to them is restricted	☒	☐
Groups with high level access such as Domain Admins are recertified on regular basis	☒	☐

What regulatory requirements does your business need to comply with? (ie. C-SOX, PIPEDA, PCI)

PCI			

Recommendations

Varonis is the leading provider of software solutions for unstructured, human-generated enterprise data. Varonis recommends the following actions in order to fully secure and maintain unstructured data security. The following remediation, classification, reporting and recertification steps should be taken in order to properly control and govern unstructured data in your environment.

- Identify and remediate high risk areas through data classification, real-time alerting and DatAdvantage modeling and commit functions. Focus on areas with Global Group access (i.e. Everyone, Authenticated Users, Domain Users, etc…)
- Varonis Data Classification product is installed but has not been configured in the environment. Data Classification is the foundation for identifying high risk / PCI data. Without Data Classification configured Acme cannot assess their PCI data risk. As soon as possible, we recommend Acme configure Data Classification on all of their file servers and assess their PCI risk footprint.
- Automate data retention and migration with the use of the rules, scope and tiered storage in Data Transport Engine.
- Restructure NTFS permissions in order to simplify ACLs and create a least privileged model. Provide only Administrators with FULL NTFS control, creating a MODIFY and READ group for user access and enabling inheritance wherever possible.
- Identify and tag responsible business units and data owners for sets of data across the enterprise.
- Remove access for global groups such as Everyone, Domain Users and Authenticated Users.
- Change group based access model on base folders / shares to one read and one modify group.
- Automate the file share access provisioning process and perform regular audit and recertification of permissions on data sets.

- Enhance accessibility and collaboration with the addition of DatAnswers and DatAnywhere. Provide data owners and users the ability to easily search through data sets and find relevant documents and then easily share or sync those documents with their mobile devices or other users within their department.

Remediation Package Options

15 days Professional Services Consultation

- Process development
- Industry Best Practice
- Process Documentation

During the 15 day consultation, Varonis will provide information and guidance around industry best practices regarding security and permissions as well assistance with documentation and help develop process workflows for cleanup and remediation of issues identified in the risk assessment report.

50 Days Professional Services remediation

- Process development
- Best Practice
- Documentation
- Resolution of Inconsistent Permissions (Broken ACLs)
- Global Access Group Remediation
- Risk Reduction

During the 50 day remediation engagement, Varonis will provide information and guidance around industry best practices regarding security and permissions as well assistance with documentation and help develop process workflows for cleanup and remediation of issues identified in the risk assessment report. In addition, based on a sample scope of critical folders, Varonis will identify and resolve inconsistent permissions as well as find and remediate critical folders where global access groups are granted permission. Therefore, reducing risk on the selected sample scope.

100 Days Professional Services Remediation

- Process development
- Best Practice
- Resolution of Inconsistent Permissions (Broken ACLs)
- Global Access Group Remediation
- Permission restructuring
- Removal of legacy permission groups
- Creation of new permission groups
- Identifying and Assigning Data Owners to DataSet
- DP Rollout
- Documentation

During the 100 day remediation engagement, Varonis will provide information and guidance around industry best practices regarding security and permissions as well assistance with documentation and help develop process workflows for cleanup and remediation of issues identified in the risk assessment report. In addition, based on a sample scope of critical folders, Varonis will identify and resolve inconsistent permissions as well as find and remediate critical folders where global access groups are granted permission. This will therefore reduce risk on the selected sample scope. Varonis will restructure permissions in order to create a least privileged model by removing legacy groups that may have excessive permissions throughout the environment. This will be done by creating new permissions with a one-to-one relationship with folders. During the process, Varonis will include identifying and assigning data owners based on user activity or specific criteria. Identified Managed Folders will be synchronized to DataPrivilege which will pave the way for the DataPrivilege Rollout

Methodology

OVERVIEW:

Varonis offers a framework to map, monitor and analyze unstructured data stores. The Varonis DatAdvantage software solution aggregates user, permissions, data and access event information from directories and file servers. Sophisticated analytics applied to the collected information show detailed data use and determine rightful access based on business need.

DatAdvantage collects user and group information directly from Active Directory, LDAP, NIS, or other directory services, as well as the file system directory structure and access control lists, giving organizations a complete picture of their permissions structures. Varonis DatAdvantage also shows every user and group that can access data as well as every folder that can be accessed by any user or group. By combining the information on who can access the data with an audit trail detailing who is accessing the data and sophisticated bi-directional cluster analysis, Varonis DatAdvantage provides actionable intelligence on where excess file permissions and group memberships can be safely removed without affecting normal business processes.

With Varonis DatAdvantage, organizations achieve enterprise-wide data governance in a productive approach, through effective and efficient automated data controls. Varonis DatAdvantage ensures proper data use, proper permissions, and helps organizations meet legal, financial, intellectual property and data privacy requirements.

In order to complete this report, information was gathered both from DatAdvantage and from the customer contact assigned to the project. The results are provided based on a combination of these factors.

DATA COLLECTION:

Four streams of metadata were collected to compile the results of this assessment:

- User and group information - Collected from Active Directory using Varonis “AD Walk” job process.
- Permissions and file system information - Collected from file servers, using Varonis “File Walk” job process. Provides information such as which users and groups are listed on ACLs, access time stamps, file counts, and file sizes.
- Access activity - Collected using Varonis audit agents for Windows and SharePoint servers, “Fpolicy” for NetApp filers, and the “Common Event Enabler” for EMC Celerra, VNX, and Isilon devices. Provides data on which users access what data, when, and what actions they performed.

CUSTOMER FEEDBACK:

In order to properly complete this Assessment, customers have been asked to provide information that may not be available via data collection processes. This information will contribute to the assessment, by adding relevant information that cannot be gathered via DatAdvantage.