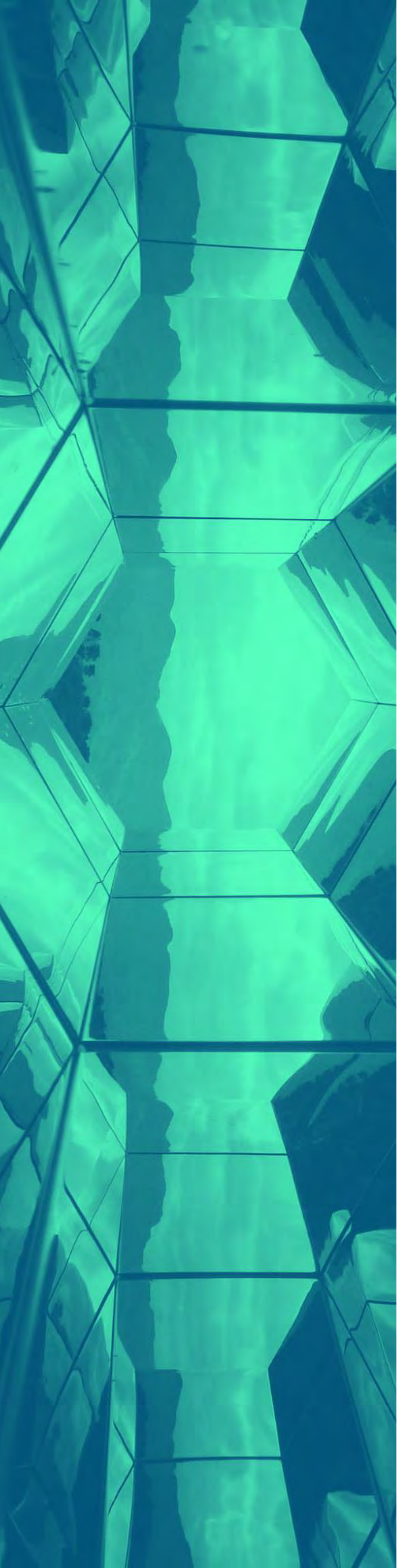
stealthbits

EXECUTIVE SUMMARY

CREDENTIAL AND DATA SECURITY ASSESSMENT

SAMPLE



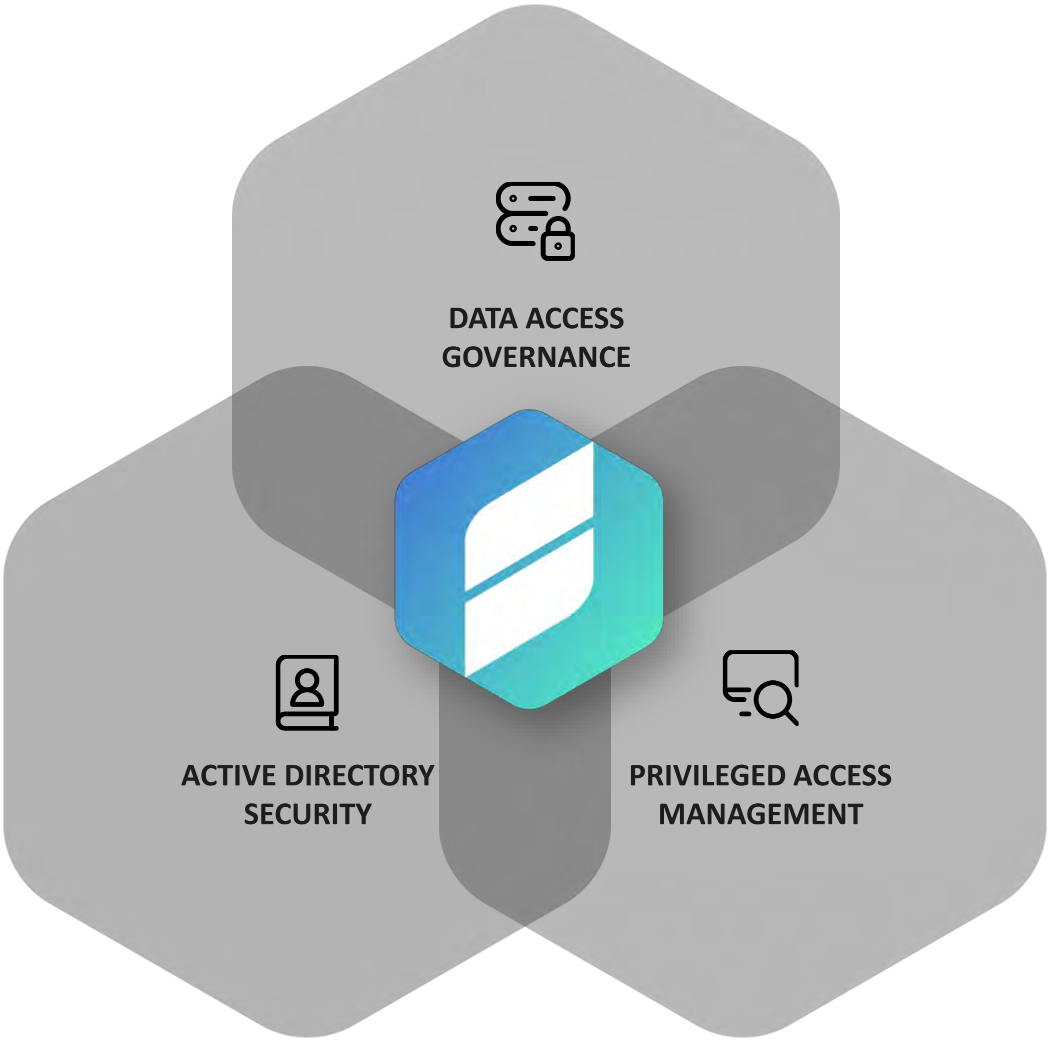
Stealthbits Technologies, Inc.

Credential and Data Security Assessment

Stealthbits' Credential and Data Security Assessment (CDSA)

Regardless of an attacker's entry point into an organization, they're always after the same two things – credentials and data. In response, Stealthbits helps organizations remove inappropriate data access, secure the credentials attackers seek to compromise and exploit, and detect, prevent, and mitigate advanced threats at the system, directory, and data layers of your environment.

To help shine a light on where you're most vulnerable, Stealthbits Technologies has engineered and conducted a comprehensive assessment of select data repositories, Active Directory, and Windows infrastructure. The analysis detailed in the pages to follow will provide clear insight into the security stature of your credentials and data.



DATA SECURITY

Data Access Governance (DAG) aims to provide understanding and oversight into data access, with the added context of data sensitivity, usage, and ownership as pivot-points for determining proper access rights (i.e. achieving a Least Privilege Access model).

In a recent study published by the SANS institute of 12 separate data breaches, it was determined that "only 14% of the information stolen by an adversary was needed by the owner of the compromised account." This fact clearly illustrates the need for tighter data access controls, as the overwhelming majority of the data stolen by attackers was practically handed to them.

Criteria Summary

- Open Access
- Sensitive Data
- Stale Data
- High-Risk Permissions

Assessment Scope

The following is a summarization of the scope of the assessment performed against chosen data repositories.

File Systems	273 Shares
SharePoint	1 Sites
Databases	24,788 Tables
Box	341 Collaborations
Dropbox	9 Shares
Exchange Mailboxes	13 Mailboxes
Exchange Public Folders	8 Folders
AWS S3	7 Buckets

# of Resources with Open Access

11,562

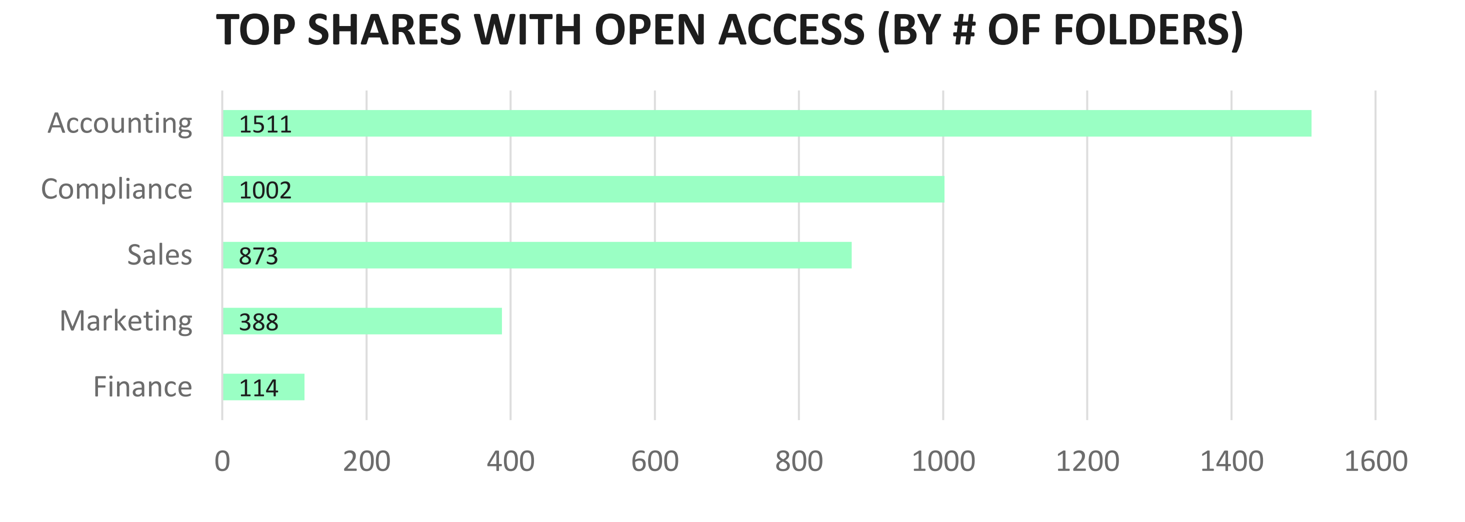
% of Resources with Open Access

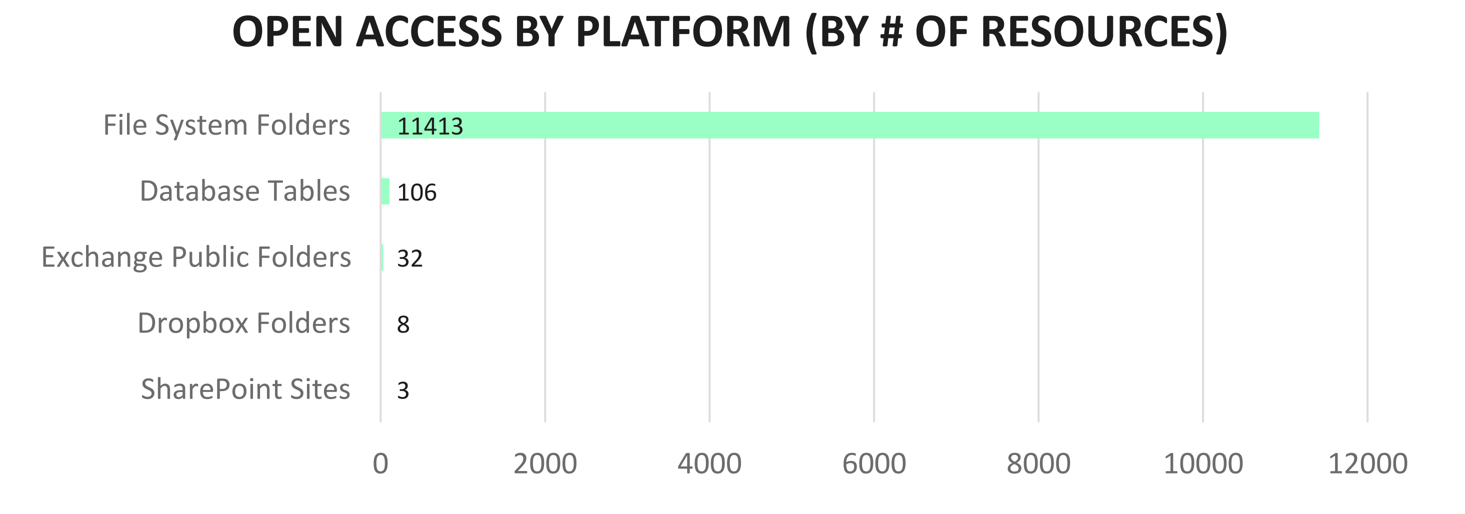
30.73%

CONDITION: Open Access

Open Access is a condition referring to the use of Global Security Groups (i.e. all-inclusive groups containing most or sometimes all users within an organization) being used to provide access to resources.

These groups (e.g. Everyone, Authenticated Users, Domain Users) should almost never be used to provide access to data resources, as it exposes organizations to significant risk of data breach, inappropriate data use, and even compliance failure.





CONDITION: Sensitive Data

Sensitive data (e.g. data containing personally identifiable information about employees or customers, trade secrets and other private business information, health information, etc.) can exist in virtually any file, anywhere within an organization.

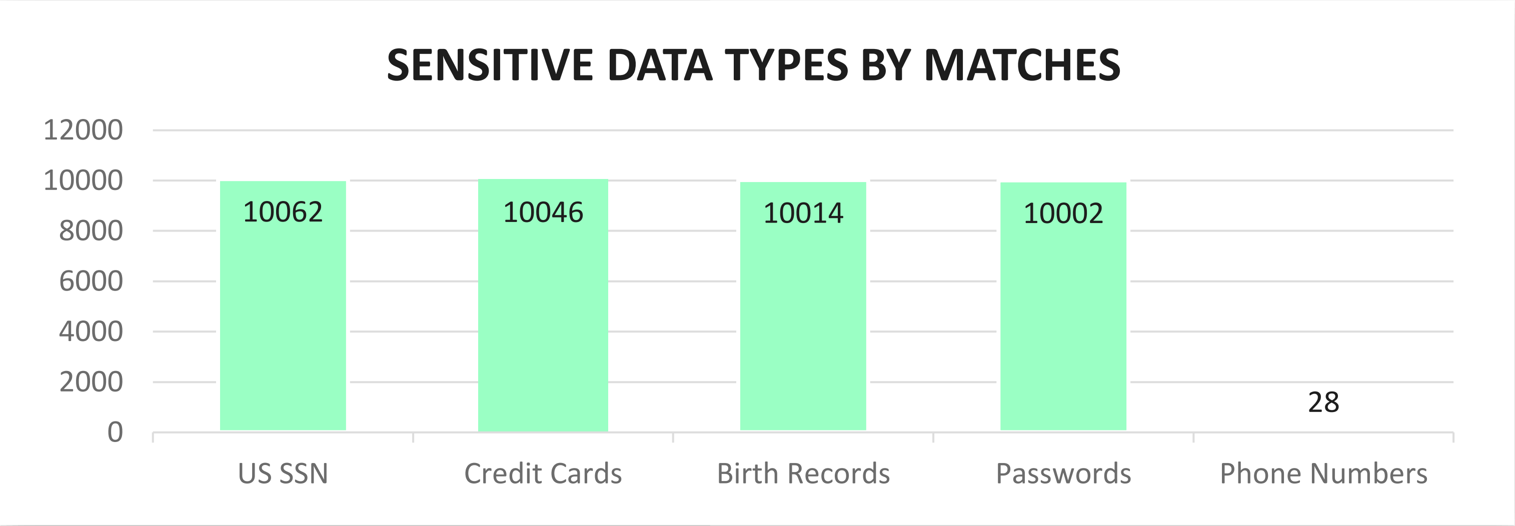
Understanding where this data exists, in what quantity, and how it has been secured is a necessity for security and compliance, and should be remediated in accordance with Least Privilege Access principles.

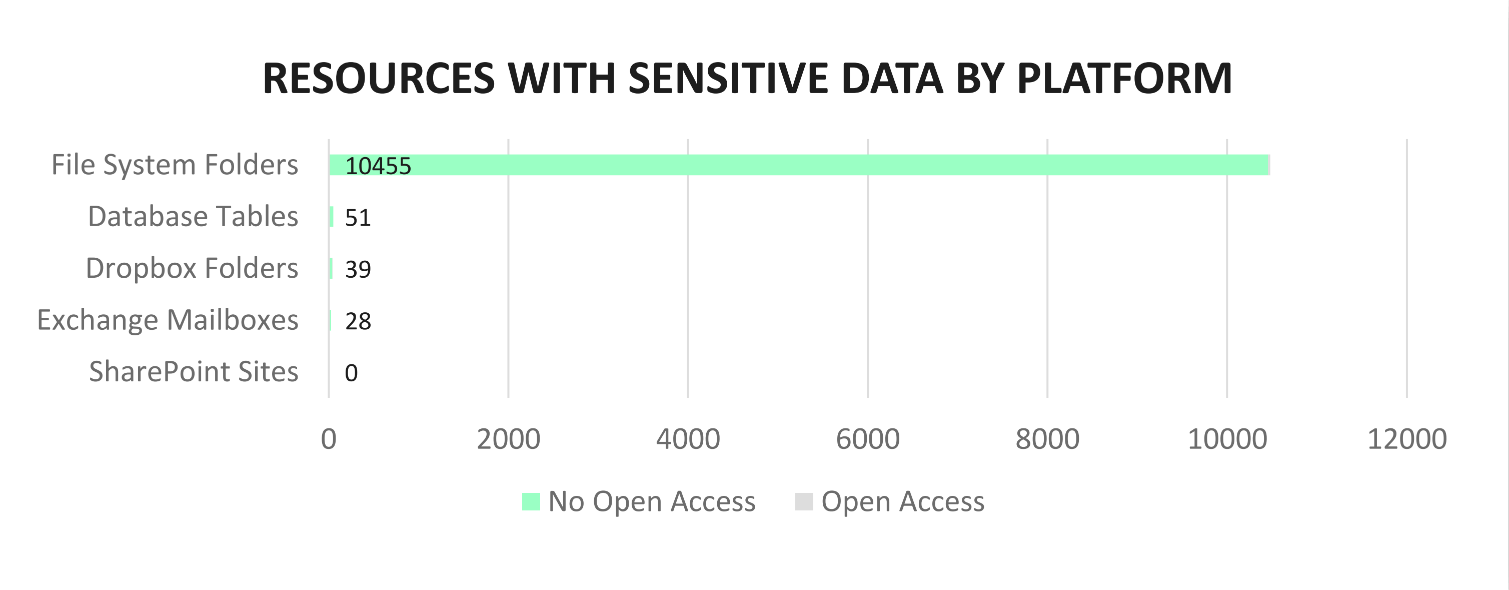
# of Resources with Sensitive Data

10,603

# of Sensitive Data Matches

40,672





CONDITION: Stale Data

Recent studies estimate that over 40% of corporate data is not only stale, but hasn't been accessed in over three years.

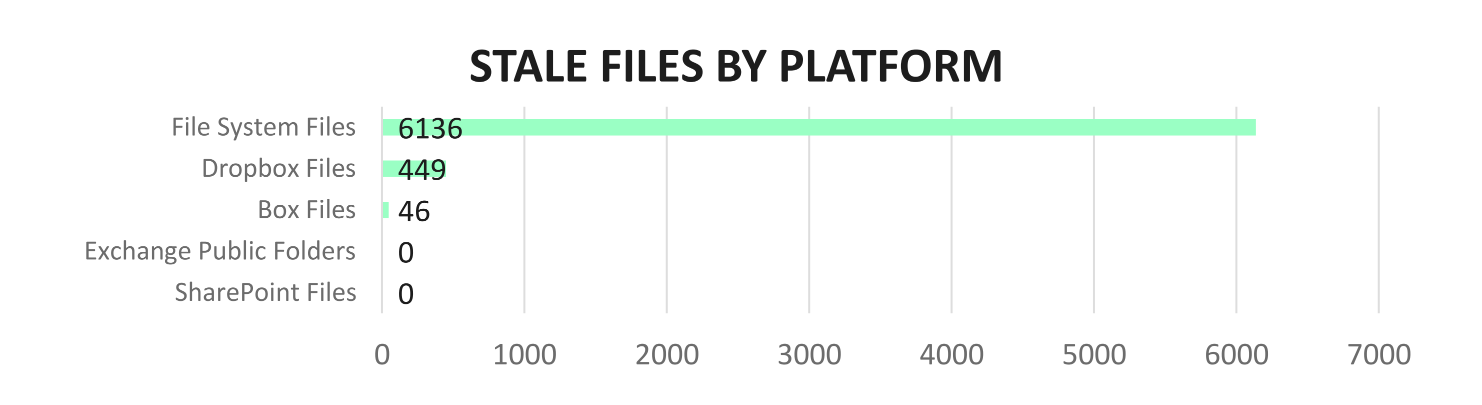
Understanding and proactively addressing stale data presents real opportunities for both risk reduction and cost savings, as less data to manage makes it easier to secure and reduces the necessity for spending on new storage and the overhead costs associated with it.

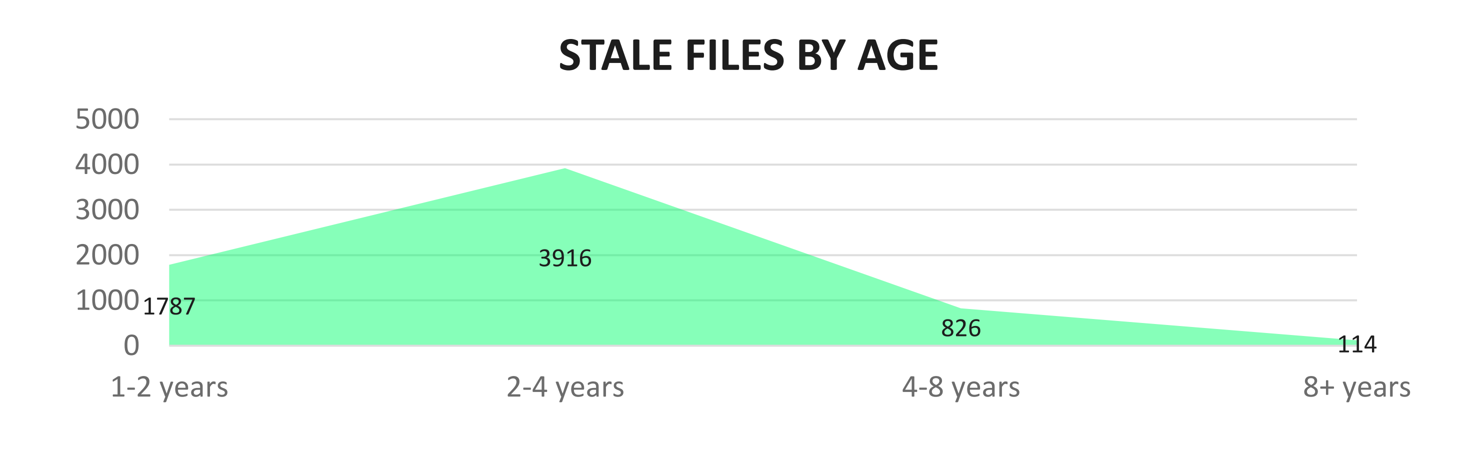
With additional context around stale data that is also sensitive and potentially subject to longer retention periods as a result of compliance mandates, stale, sensitive data can be easily moved to more secure locations or taken offline completely to drastically reduce the risk of otherwise highly avoidable data loss.

Organizations that invest in effective archival strategies are often able to realize substantial storage cost savings, reallocating funds to other critical projects and priorities.

% | Size of all Data that is Stale

89.35% | 10.32 GB





ACTIVE DIRECTORY SECURITY

Active Directory holds the keys to the kingdom.

As the authentication and authorization hub of almost every organization’s IT infrastructure, AD is a focal point in virtually every breach scenario. Attackers know that if they can own AD, they can own everything connected to it as well. As a result, Active Directory needs to be clean, understood, configured properly, monitored closely, and controlled tightly if organizations are to protect AD from otherwise inevitable attack.

Criteria Summary

- Weak Passwords
- Sensitive Groups
- Toxic AD Objects
- Object Permissions

Assessment Scope

The following is a summarization of the scope of the assessment performed against Active Directory.

Microsoft Active Directory	Azure Active Directory
Number of Domains 1	**Number of Domains** 1
Number of Users 9,985	**Number of Users** 1,087
Number of Groups 11,016	**Number of Groups** 73
Number of Computers 8,982	
Number of OUs 1,040	
Number of Permissions 8,099,223	

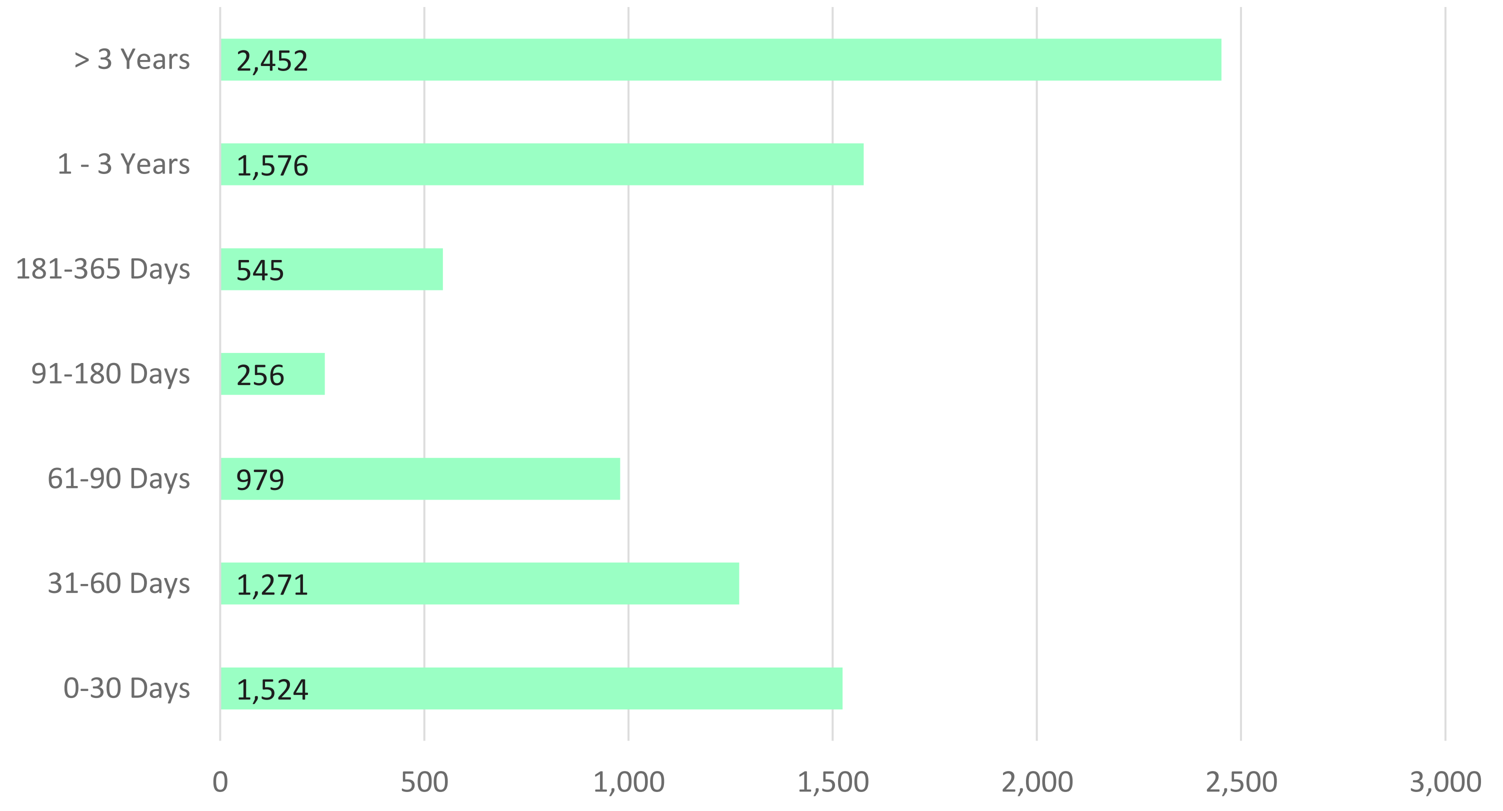
# (%) of Users with Weak Passwords	**263 (2.63%)**
# (%) of Users with Weak Passwords in History	**452 (4.53%)**
# (%) of Users with Common Passwords	**2,700 (27.04%)**
# (%) of Users with Non-Expiring Passwords	**2,405 (24.09%)**
# (%) of Accounts with Reversible or Weak Encryption	**297 (2.97%)**
# of Passwords Exposed via Group Policy Preferences	**1**

CONDITION: Weak Passwords

Password strength is an important component of any organization's overall information security strategy.

Identifying users leveraging passwords contained in publically available password dictionaries and organizationally-defined unapproved password lists allows security personnel to proactively identify accounts most susceptible to successful brute force or password guessing attacks. Leveraging strong passwords across all accounts effectively mitigates risk for the organization as a whole.

PASSWORD AGE DISTRIBUTION



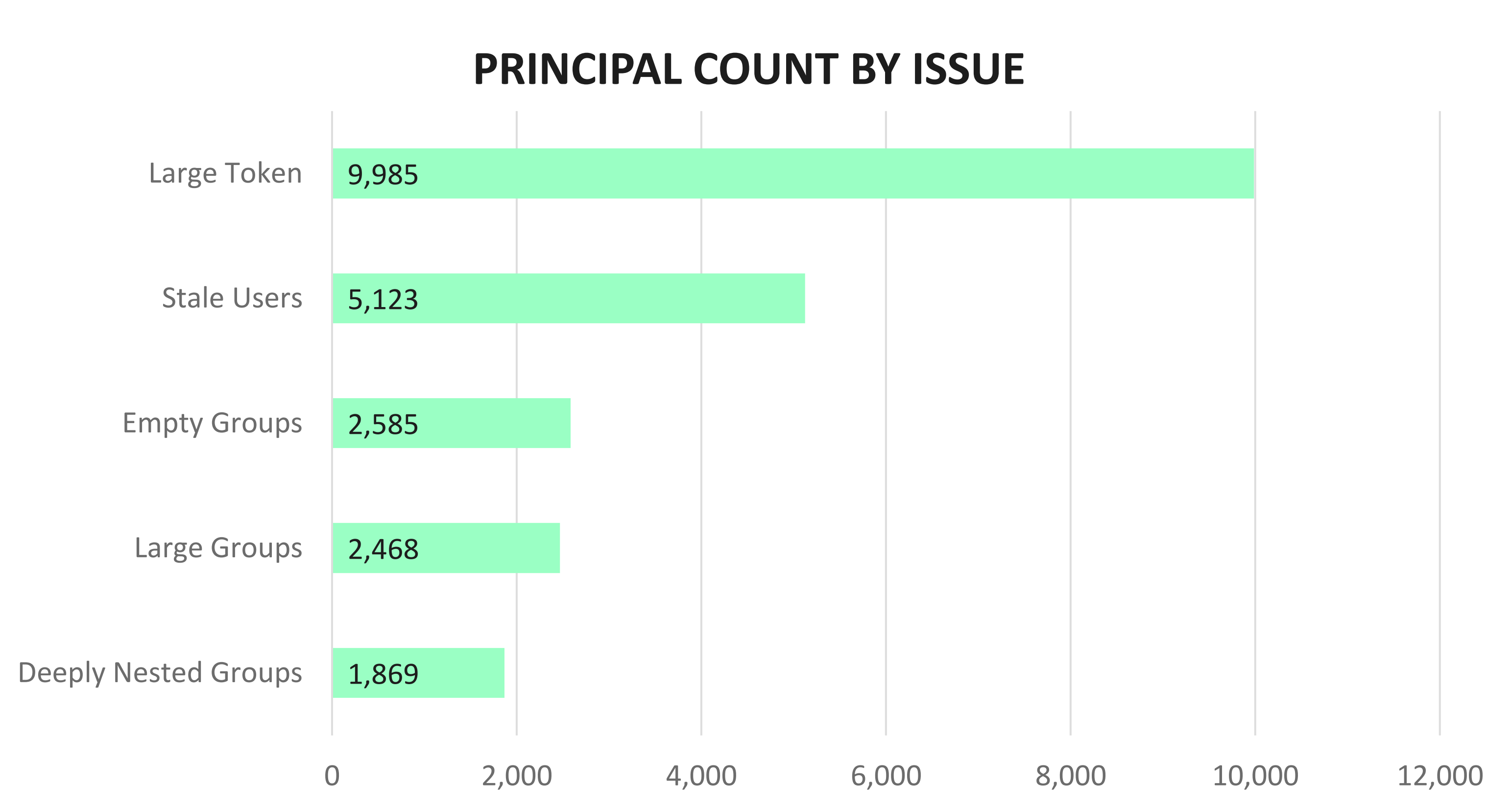
CONDITION: AD Object Toxicity

Most Active Directory environments have undergone significant transitions and transformations over time due to events like mergers, acquisitions, divestitures, migrations, and upgrades. Additionally, many organizations have adopted differing philosophies of how Active Directory should be managed and secured over the years, resulting in a plethora of "toxic" conditions and configurations that put Active Directory at risk of compromise or even catastrophic outage.

Clearing away the clutter of stale objects makes administering and securing Active Directory easier, and understanding how AD itself has been secured also shines a light on where attention is needed most to thwart modern cyber attacks.

Active Directory Object Permissions (# of Users)	
Reset Password Rights	116
Group Membership Change Rights	147
Domain Replication Rights	34

Stale Objects by Count (enabled/disabled)	
Users	1,403/3,720
Computers	2,847/253
Groups	1,580/1,321

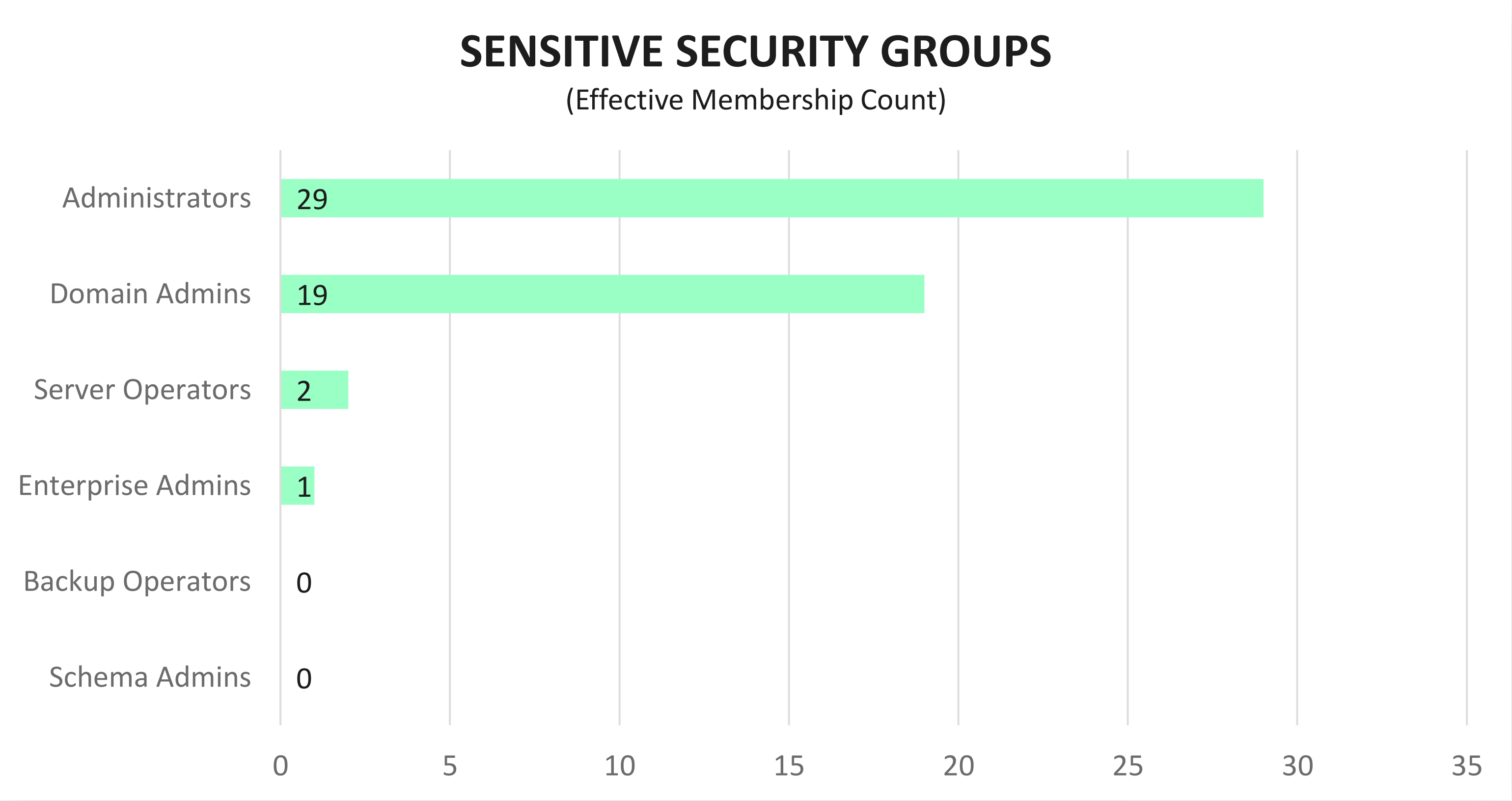


CONDITION: Sensitive Security Group Membership

Members of Sensitive Security Groups like Domain, Enterprise, and Schema Administrators have the highest levels of privilege within an Active Directory environment. If stolen by an attacker or abused by an internal bad actor, the critical changes these accounts can make can have devastating effects on the security of Active Directory and everything connected to it.

Administrative access through sensitive security groups should be provisioned on a least-privilege basis. In order to achieve this model successfully, it is advisable to remove all stale, disabled, and expired accounts, institute strong password security on all accounts in scope, perform regular certifications of sensitive security group membership, and alert on any changes to these groups the instant they occur.

Privileged Access Summary	
# Users with Privileged Access Rights	**29**
Password Never Expires (user count)	**15**
Oldest Password Age (in days)	**6,351**



WINDOWS SECURITY

Despite significant investments in perimeter and endpoint security, breach typically begins at the desktop and server layers of an organization’s IT infrastructure and spreads due to the overabundance of privileged access rights on each system, as well as the misconfigurations and vulnerabilities attackers are able to exploit as a result. Privileged access is at the root of successful breach and needs to controlled — even eliminated — in order to effectively reduce an organization’s attack surface.

CRITERIA SUMMARY

- Administrative Access
- Service Accounts
- Ticket and Credential Management

ASSESSMENT SCOPE

THE FOLLOWING IS A SUMMARIZATION OF THE SCOPE OF THE ASSESSMENT PERFORMED AGAINST WINDOWS SYSTEMS.

Number of Servers:	700
Number of Desktops:	4
Operating Systems:	Windows Server 2012 R2 Datacenter Windows Server 2012 R2 Standard Windows Server 2016 Datacenter Windows Server 2016 Standard Windows Server 2008 R2 Enterprise

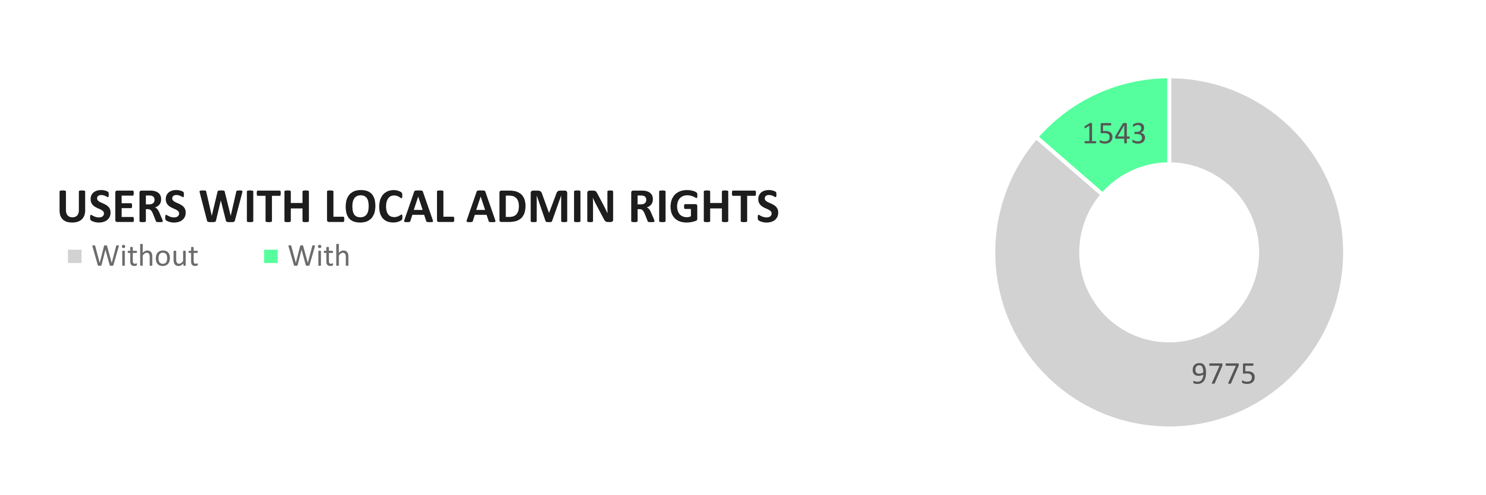
Top 10 Systems by Local Admin Count

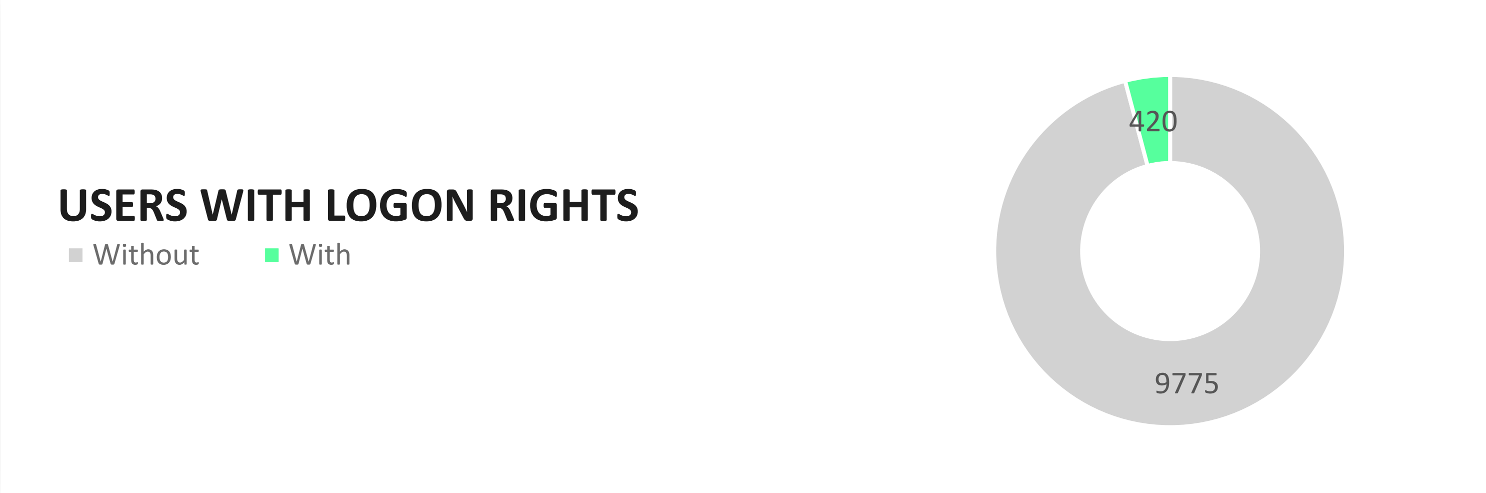
GCQAVM47	**54**
GCIMPSRV05	**48**
GCNYSRV22	**47**
GCORPSRV55	**45**
VM120	**43**
TOMT-W2K12-5	**43**
DEV_OUTLOOK-22	**42**
GCMBXSRV	**42**
GCH32-NY	**42**
DC01	**41**

CONDITION: Local Admin Rights

Excessive privileged access rights across Windows desktop and server infrastructure allow attackers to more easily compromise credentials and systems, move laterally and vertically, and ultimately obtain complete control over Active Directory and everything connected to it.

Foundation-level security starts with limiting Local Admin and equivalent rights to the lowest levels possible. With a strong foundation to build off of, investments in complementary technologies like Antivirus, Endpoint Protection, and patch management produce greater ROI through increased effectiveness.


USERS WITH LOCAL ADMIN RIGHTS


USERS WITH LOGON RIGHTS

CONDITION: Service Accounts and Windows Vulnerabilities

Misconfigured security settings, missing patches, and overexposed service accounts are just a few ways in which attackers circumvent security controls, locate and steal privileged credentials, and elude detection.

Ensuring critical security settings are configured properly across all systems significantly limits an attacker's options after initial system compromise. With fewer attack tactics, techniques, and procedures at their disposal, they're forced to leverage more overt options, increasing their likelihood of detection.

SERVICE ACCOUNTS

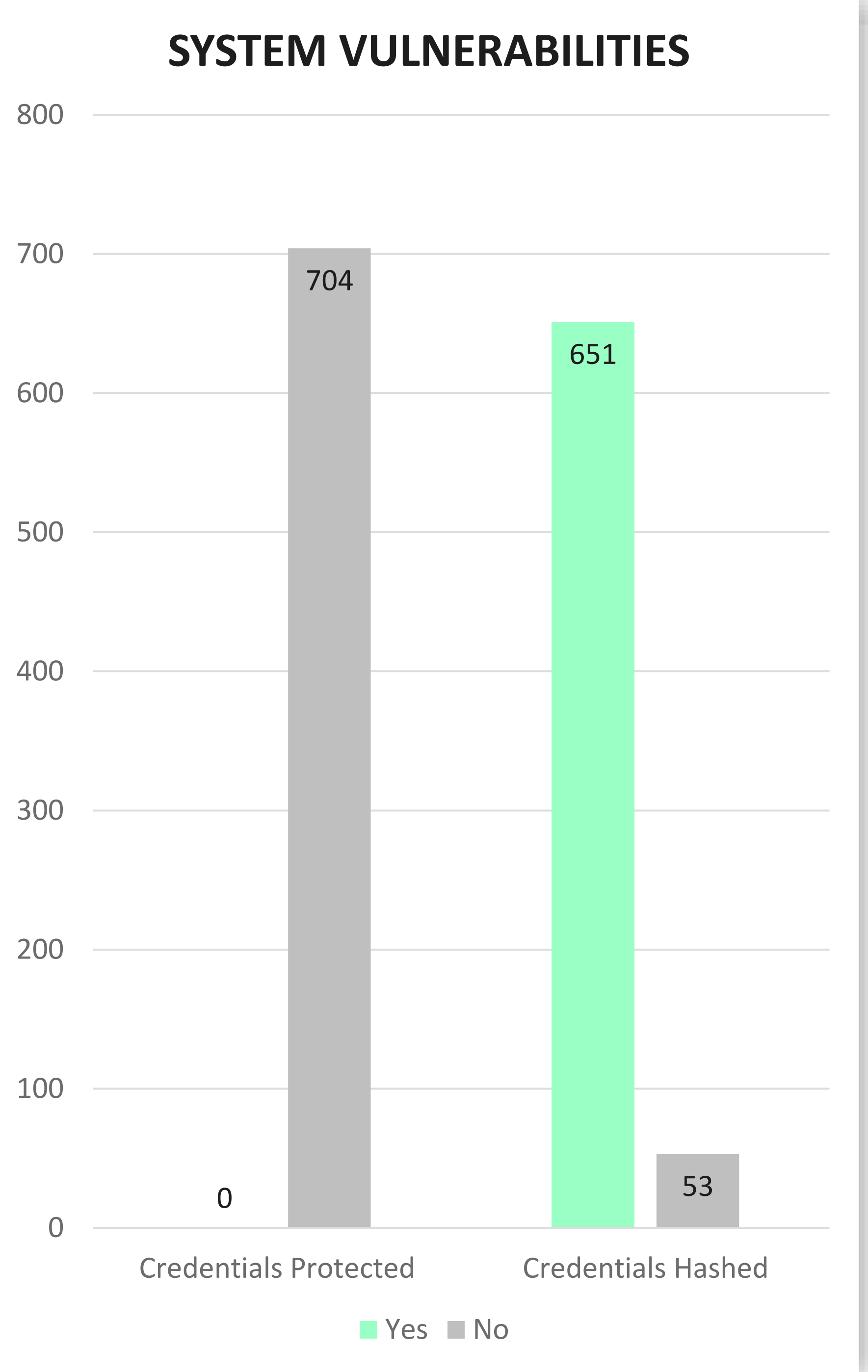
# Domain Users (Services & SPNs)	**50**
Average Password Age (days)	**515**
Oldest Password (days)	**1,412**

SECURITY CONFIGURATIONS

LSA Protection (enabled | disabled)	**0|704 Systems**
WDigest (enabled | disabled)	**651|53 Systems**

POTENTIAL SUSPICIOUS ACTIVITY

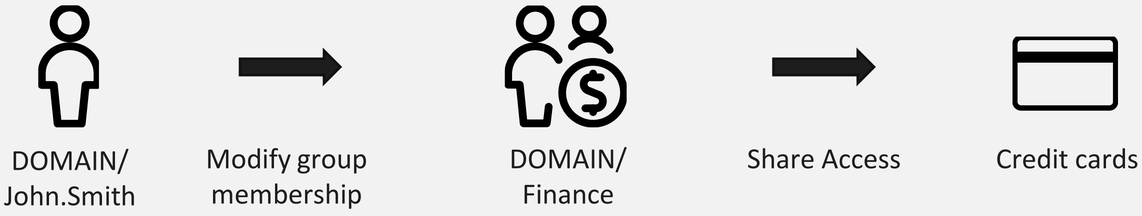
Suspicious PowerShell Commands	**Found on 27 Systems**



CONDITION: Shadow Access Rights

Security professionals struggle to keep up with and defend their organizations against the wide variety of tactics, techniques, and procedures (TTPs) attackers can choose from to infiltrate networks, elude detection, compromise credentials, and escalate privileges. While some risks are simple to identify, others lurk beneath the surface and exist due to the right – albeit toxic – combination of permissions and conditions. These risks are often the scariest, because only the attackers know they exist and how to exploit them.

Leveraging weaknesses in data, Active Directory, and Windows permissions and security, attackers are able to gain access to your privileged accounts and sensitive data in highly clever ways.



DOMAIN/ John.Smith → Modify group membership → DOMAIN/ Finance → Share Access → Credit cards

# Users with Active Directory Shadow Access

15

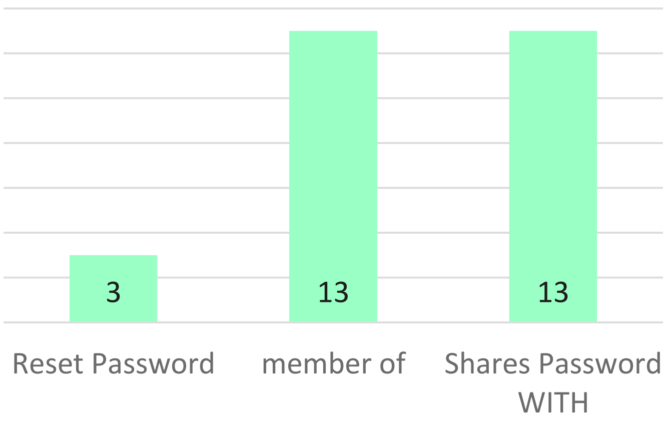
# Users with Sensitive Data Shadow Access

25

Average # of Steps

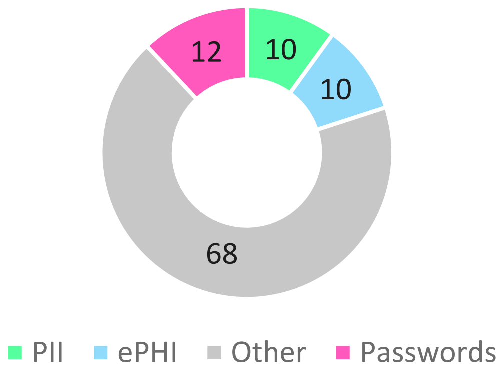
2

EXPLOITABLE PERMISSIONS



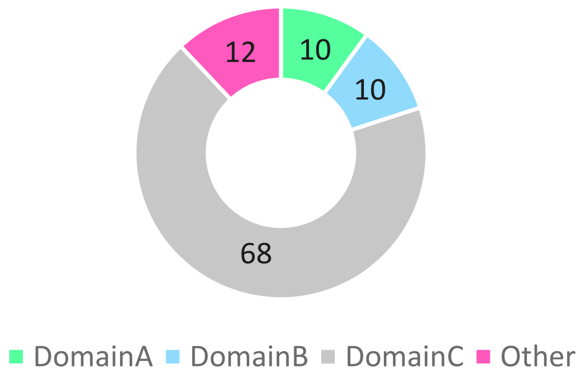
SENSITIVE DATA SHADOW ACCESS

(# of Users by Data Type)



ACTIVE DIRECTORY SHADOW ACCESS

(# of Users by Domain)



FILE SYSTEMS

- HIGH 26 files containing sensitive data are accessible via Open Access
- MEDIUM 95.98% of all data scanned has not been modified in 365 days or more
- MEDIUM There are 129 instances of user objects being used to provide access directly to data
- LOW There are 13393 instances of broken inheritance identified across the scanned file shares
- **NO FINDINGS** There are 0 different security groups being used to grant access to sensitive data

SHAREPOINT

- **NO FINDINGS** 0 files containing sensitive data are accessible via Open Access
- **NO FINDINGS** 0 files containing sensitive data are accessible by users outside of your organization
- **NO FINDINGS** 0% of all data scanned has not been modified in 365 days or more
- **NO FINDINGS** There are 0 instances of user objects being used to provide access directly to data
- **NO FINDINGS** There are 0 instances of broken inheritance identified across the scanned site collections

BOX

- MEDIUM 12.33% of all data scanned has not been modified in 365 days or more

DROPBOX

- HIGH 1 files containing sensitive data are accessible via anonymous access links
- MEDIUM 91.63% of all data scanned has not been modified in 365 days or more
- LOW There are 10 instances of inactive access to a shared folder

EXCHANGE

- **NO FINDINGS** 0 files containing sensitive data are accessible via Open Access
- **NO FINDINGS** 0% of files in Public Folders haven’t been modified in 365 days or more
- **MEDIUM** There are 101 different users with membership to Exchange Administration groups
- **LOW** 32 different security groups are being used to grant access to sensitive data
- **NO FINDINGS** 0 orphaned mailboxes
- **LOW** 13 mailboxes are associated with stale Active Directory accounts

DATABASES

- **HIGH** 26 tables containing sensitive data are accessible via the Public role
- **HIGH** 5 SQL Server instances with default naming for the SA account
- **NO FINDINGS** 0 SQL Server instances where insecure encryption practices are leveraged
- **HIGH** 2 SQL Server instances with XP_CMDShell enabled
- **NO FINDINGS** 0 Oracle databases with accessible data dictionaries
- **MEDIUM** 2 instances of user objects being used to provide access directly to data (tables)
- **MEDIUM** 2 SQL Server Services running as administrator
- **HIGH** 22 Oracle databases that allow remote clients to authenticate using non-secure protocols
- **HIGH** 12 SQL logons that leverage weak or shared passwords (both Oracle and SQL)
- **LOW** 2 Oracle database instances that have short, simple, common, or obvious SID values

ACTIVE DIRECTORY

- **NO FINDINGS** 0 service accounts have a password age of over 365 days
- **HIGH** 21 non-administrative user accounts have the ability to replicate directory objects
- **HIGH** 1 plaintext passwords are being stored in the SYSVOL share of your Domain Controllers
- **MEDIUM** 116 different non-administrative users can reset the passwords of accounts other than their own
- **LOW** The average token size across the entire user population is 1,474
- **LOW** 51.31% of all User objects, 34.51% of all Computer objects, and 26.33% of all Groups are considered stale

WINDOWS OS

- **MEDIUM** 7.84% of systems do not have LSA protection enabled
- **MEDIUM** 15.45% of all users have Local Admin rights to at least one system in your environment
- **LOW** 0.72% of systems have WDigest enabled

Glossary

Group policy preferences

Group Policy preferences enable administrators to configure, deploy, and manage greater numbers of operating system and application settings.
https://msdn.microsoft.com/en-us/library/cc512161(v=vs.85).aspx

Least privilege access

The principal of least privilege dictates that a user only be granted the privileges necessary to perform their function.
https://en.wikipedia.org/wiki/Principle_of_least_privilege

LSA protection

The LSA, which includes the Local Security Authority Server Service (LSASS) process, validates users for local and remote sign-ins and enforces local security policies. The Windows 8.1 operating system provides additional protection for the LSA to prevent reading memory and code injection by non-protected processes. This provides added security for the credentials that the LSA stores and manages.
https://docs.microsoft.com/en-us/windows-server/security/credentials-protection-and-management/configuring-additional-lsa-protection

Open access

Open Access occurs when global security groups or other well-known security principals like Everyone, Domain Users, and Authenticated Users are used to provide access to data.

Sensitive data

Sensitive data, in the context of this assessment, can mean any data subject to a mandated compliance standard, data that could cause material harm to an individual or business if revealed, or data that if lost could cause damage or distress to an individual or business.

Shadow Admins

Shadow Admins are non-privileged accounts that that can perform privileged operations due to unapparent permission configurations. For example, because a user can reset the password of a privileged account, they are thus a privileged account as well.

SMBv1

Server Message Block (SMB) is a legacy, vulnerable protocol used primarily for sharing files, printer services, and communication between computers on a network.
https://blog.stealthbits.com/what-is-smbv1-and-why-you-should-disable-it

Stale data

In the context of this assessment, stale data is any file that has not been modified within the past 365 days.

Token size

The number of security groups a user belongs to dictates the size of their Kerberos token. If above a certain size, a user will be unable to authenticate to network resources, preventing them from performing various job functions.
https://support.microsoft.com/en-us/help/327825/problems-with-kerberos-authentication-when-a-user-belongs-to-many-grou

WDigest

The Digest Authentication protocol is designed for use with Hypertext Transfer Protocol (HTTP) and Simple Authentication Security Layer (SASL) exchanges. These exchanges require that parties that seek to authenticate must demonstrate their knowledge of secret keys.
https://technet.microsoft.com/pt-pt/library/cc778868(v=ws.10).aspx

Weak passwords

In the context of this assessment, weak passwords are those that leverage passwords contained in publicly-available password dictionaries or organizationally-defined unapproved password lists, regardless of whether their password meets complexity requirements.

Notes

PRODUCT PORTFOLIO

STEALTHBITS' CREDENTIAL & DATA SECURITY SUITE

StealthAUDIT

Reporting & Governance

Limit access to data, systems, and applications

StealthINTERCEPT

Monitoring & Control

Monitor and enforce security and operational policy

SbPAM

Privileged Access Management

Task-based Administrative Access and Delegation

StealthDEFEND

Threat Detection & Response

ML-driven threat analytics, alerting, and response

StealthRECOVER

Rollback & Recovery

Rollback of undesired changes and recovery of deleted objects

PATH TO SUCCESS

Finding the right tools for your use case

DISCOVER...

Data Footprint – Obtain a complete view of where data exists

🟩

Sensitive Data – Discover where sensitive data lives

🟩

Open Access – Discover and remediate open access to sensitive data

🟩 🟪

Privileged Accounts/Access – Identify which accounts provide privileged access to systems and data *(PAM)*

🟩 🟦

Security Configurations – Discover data, directory, and system vulnerabilities that expose you to undue risk *(ITSM)*

🟩

ALERT...

Ransomware – Alert on and respond to activity patterns indicative of Ransomware *(SIEM)*

🟪

Threats (UBA) – Alert on anomalous behavior and automate downstream actions to contain threats *(SIEM)*

🟪

Authentication-based Attacks – Detect attempts to compromise account credentials, move laterally, and elevate privileges *(SIEM)*

🟪

High-Risk Changes – Alert on and block unintentional and malicious changes that put data at risk *(SIEM, ITSM)*

🟪 🟩 🟧

REMEDIATE..

Overprovisioned/Open Access – Remove over-permissive access and unnecessary “standing privileges” to enforce Least Privilege Access

🟩 🟦

Stale & Redundant Groups – Clean up no longer needed groups and access

🟩 🟥 🟪

Object Complexity – Clean up users, computers, weak passwords, conflicting policies, and more

🟩 🟥 🟪

Stale Data – Reclaim valuable storage and reduce threat surface through identification, deletion and/or reallocation of stale content

🟩

Weak Password – Enforce password policy to eradicate weak, unapproved and easy guessed passwords

🟧

AUTOMATE

Privileged Access Management – Delegate privileged access rights based on the task to be performed)

🟦

Ownership Identification – Automatically identify, assign, and manage data ownership *(IAM)*

🟩

Entitlement Reviews – Automate reviews of data access rights on desired schedules or ad hoc *(IAM)*

🟩

Self-Service Access Requests – Route new access requests to data owners for expedited review *(IAM)*

🟩

Data Classification & Tagging – Tag and classify content based on sensitivity or internal criteria *(DLP)*

🟩

🟩 stealthAUDIT 🟪 stealthDEFEND 🟧 stealthINTERCEPT 🟥 stealthRECOVER 🟦 sbPAM stealthbits

THANK YOU