Privileged Access Management
Filling The Gaps

Discovery, Certification and Remediation of Privileged Accounts

Understanding the Complexities of Privileged Access

An IT server is built on an Operating System that is managed and maintained by administrators with varying degrees of access, whether the root for UNIX, local administrator for Windows or other sub-systems that have their own privileged service accounts.

The same server may require middleware and other installed applications that in turn require a database and web server with service accounts that may be managed by other IT teams with different roles and responsibilities.

With three operational groups leveraging different service accounts, there will be overlap with the web and database teams leveraging root/administrator accounts from time to time.

Add in the applications, developers and teams that manage them, and there are now upwards of five teams with four groups of service accounts.

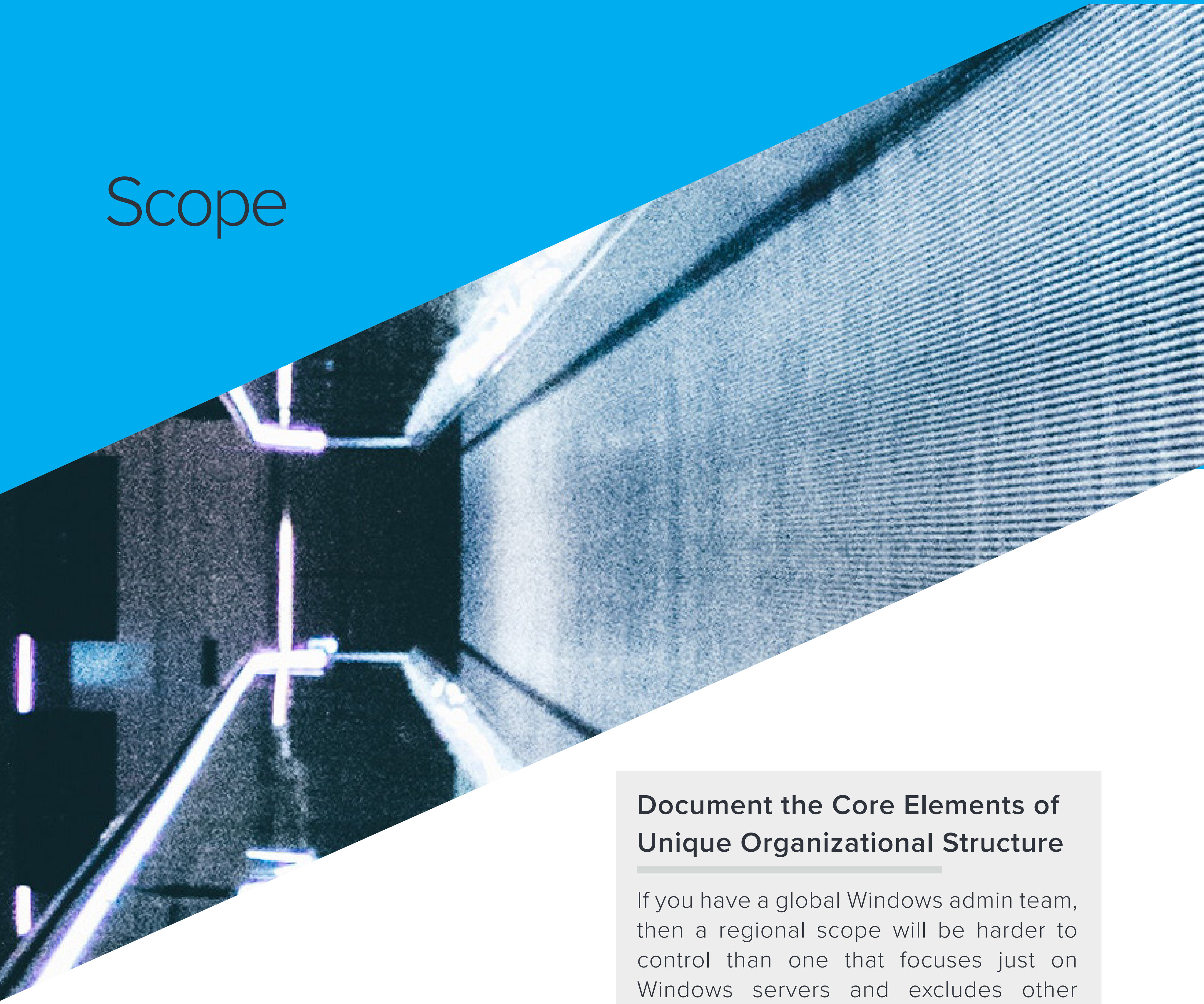
When overlaying the various internal compliance processes required to manage and maintain the systems, such as change control or trouble ticketing systems that may be over-ridden in the event of catastrophic failures, understanding permissions and access can get even more complicated.

What is the right vaulting solution?

Even with the understanding that privileged access is complex, knowing which accounts to password vault and where to escalate and record sessions require multiple foundational workstreams -- and that's all before an organization can onboard a single privileged account.

A successful and compliant end state should pull together the required reporting, analysis and certification on an ongoing basis, ensuring unmanaged accounts are identified, access is pruned regularly and an ongoing measure of key risk indicators is available to IT management for review. And that's just the start.

Scope



First, define the program's scope. For the program to be effective, there must be a complete understanding of the relationship between the various IT assets impacted by the change. Therefore, a comprehensive implementation involves systems, accounts, applications and processes that span the entire enterprise.

The goal is to leverage privileged accounts with the proper controls in place. This begins with defining priorities based on risk or ease of implementation and limiting the scope to one geography or business unit.

Document the Core Elements of Unique Organizational Structure

If you have a global Windows admin team, then a regional scope will be harder to control than one that focuses just on Windows servers and excludes other platforms. Similarly, be careful that you understand everything in your scope and don't exclude anything which can't reasonably be separated out.

If, for instance, you have very heavy systems account usage by applications, then excluding application use of privilege may make it impossible to deliver truly effective PAM. Indeed, the very first stage in your project, even before you have started to build out your PAM control infrastructure should be to document the these core elements within your scope.

Discovery and Inventory

Privileged account management can be complex. Access can be assigned in a specific location but have a direct impact on other areas of the infrastructure – so, for your first workflow, it is very important to have a solution that can locate and identify all of the privileged accounts across the enterprise.

Secondly, creating a relationship to what applications are tied to helps create a full implementation roadmap, as collections can be based on application usage or located on the servers where the accounts are found. In some cases, the accounts may be managed completely independent of the systems they provide access to. Having a solution that can provide a visual and contextual picture around these complex scenarios is critical.

Data Sources

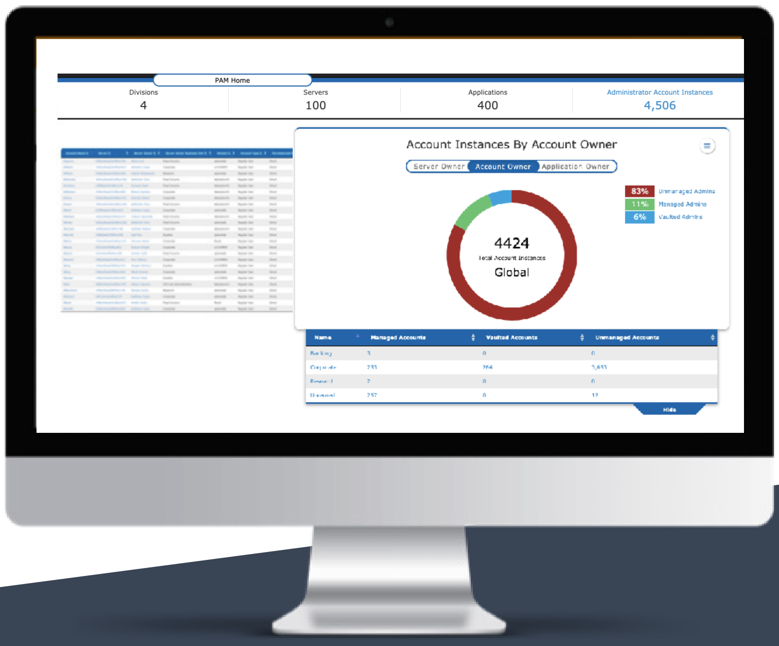
To get a complete picture of privileged accounts, IT organizations need applications that can cross platforms and gather data from disparate sources. This includes in-depth scans of servers, database access and other repositories of unstructured data. To accurately classify the use cases for each account, additional feeds are required from Active Directory (AD), LDAP, SIEM, CMDB's as well as Human Resources. It's at this point where IT organizations can organize or "bucket" the accounts to understand how they are being used.

Account Reach

Account reach is best quantified by instances that include every machine that an account has privileged access to and every which way they have access to it. This analysis defines the true reach of each account. If a privileged account has access to three hosts, this should be viewed as three unique instances. If the same host has access to 500 hosts, then they must be viewed as 500 unique instances.

The solution should include and incorporate these four components in an automated fashion:

1. Enumerate all groups to find effective memberships.
2. Map every account to every server.
3. Map every application to every server.
4. Identify administrator instances on a per account and per server basis.



Name	Managed Accounts	Vaulted Accounts	Unmanaged Accounts
Banking	3	0	0
Corporate	233	264	3,653
Research	2	0	0
Unowned	257	0	12

Ownership and Use Case

The most basic governance principle for those IT organizations looking to manage privileged access is ownership. Having a known owner of the data, organizations can catalogue who should have user rights to the information — and moving forward, the owner will be the authoritative source on how the accounts are being used, whether or not they are required and how they can be pruned as a part of recertification or other identity and access management (IAM) initiatives.

Automating Ownership

Attempting an ownership analysis exercise manually is nearly impossible. Automating the process is key, as no two IT environments are the same.

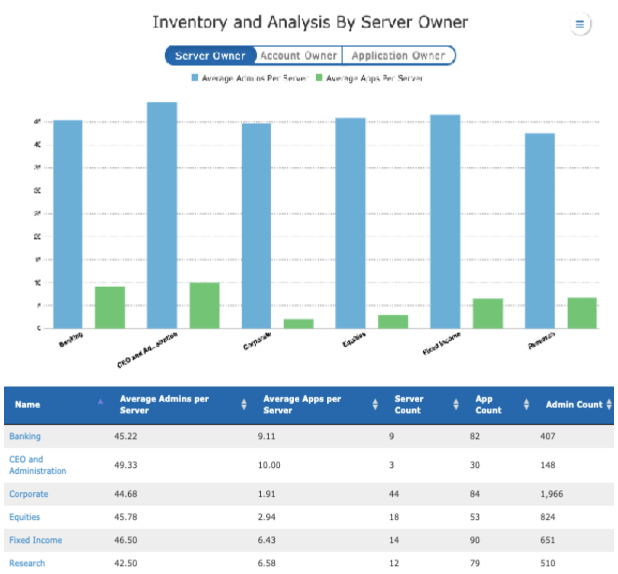
These ownership methodologies are naming convention, manager of majority users, Account / Server / Application meta data, associated AD group owner, as well as other existing ownership repositories. The solution must contain all the necessary data collection capabilities, algorithms for different methodologies along with a way to review, document, and pass along required information. Once an owner is identified, access to her personal meta-data will assist in organizing the accounts. For instance, ownership can be mapped to a business unit allowing privileged accounts to consequently be organized by business unit.

Understanding the individual use case helps to handle and prioritize accounts to remediate or improve controls. Define a set of criteria to determine what constitutes each use case. This can include naming convention matching, organizational unit (OU) location, managed by fields and other external feeds.

Understanding Use Case

The information required to do this analysis comes from a variety of disparate data sources – and based on the use case, the methodology can be vastly different. Understanding use case can also help drive the ownership analysis configurations. For example, when accounts contain username_adm, one could ascertain that the account is an alternate administrative account owned by username. Or, perhaps an account called App_X4T5 can reference an entry in your CMDB showcasing the owner of a certain application identified by code X4T5.

There may be a single account called SVCbackup that is a member of the local administrators group. This account may be sprawled across nearly every server across the organization and impacts nearly every application hosted on those servers. In your CMDB, you may have documented server owners, so do you simply choose one since the account has local admin access on the chosen server? No. Instead, this account should be owned by the Infrastructure team that owns the backup functions.



Name	Average Admins per Server	Average Apps per Server	Server Count	App Count	Admin Count
Banking	45.22	9.11	9	82	407
CEO and Administration	49.33	10.00	3	30	148
Corporate	44.68	1.91	44	84	1,966
Equities	45.78	2.94	18	53	824
Fixed Income	46.50	6.43	14	90	651
Research	42.50	6.58	12	79	510

Report on Security Issues

Once the discovery of all privileged access is compiled, ownership is catalogued and the use case is understood, IT can begin to measure the degree of risk and discover where the true security issues lie.

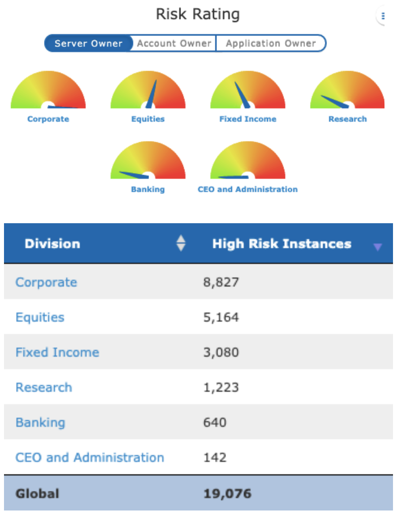
Risk ratings provide a measure of concern and establish the guidelines for the remediation. Risk dashboards should identify each account and the associated risk by applying business intelligence and an array of metrics:

1. Account Reach
2. Use Case
3. Application Criticality
4. Stale Data vs. Active Data
5. Business Unit Ownership

A comprehensive solution will deliver an enterprise-level view into the risk levels broken down into High, Medium, and Low that are associated with regular users with administrative access as well as their respective business units. This level of visibility enables project administrators to remediate the assets that pose the biggest risk to the organization.

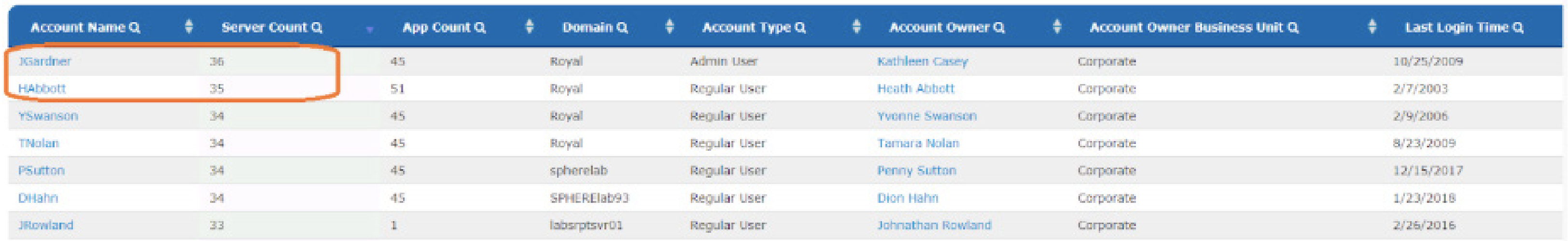
Using Account Reach to Prioritize Remediation

Once the source systems have been scanned and there is an inventory of privileged accounts, IT should focus initially on the accounts that have the highest reach. These examples show accounts that are local administrator on 35 or more hosts, and more importantly there are a set of accounts that provide admin access to over 100 applications.

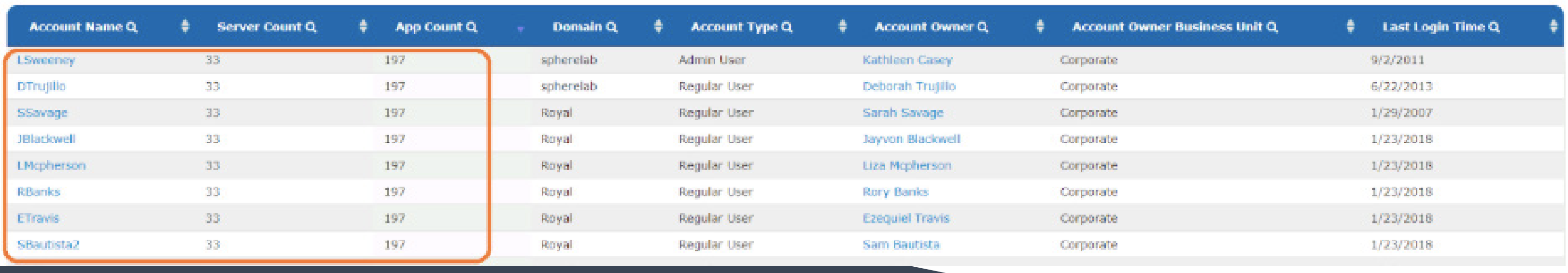


Division	High Risk Instances
Corporate	8,827
Equities	5,164
Fixed Income	3,080
Research	1,223
Banking	640
CEO and Administration	142
Global	**19,076**

These are ideal places to start remediating risk that put organizations on the path to better privileged account management. Armed with the broad analysis of account type, use case, ownership and business area provides the actionable intelligence for management to effect change across the enterprise.



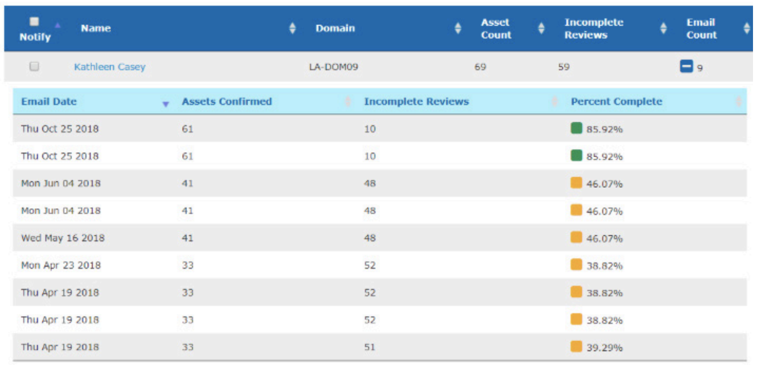
Account Name	Server Count	App Count	Domain	Account Type	Account Owner	Account Owner Business Unit	Last Login Time
JGardner	36	45	Royal	Admin User	Kathleen Casey	Corporate	10/25/2009
HAbbott	35	51	Royal	Regular User	Heath Abbott	Corporate	2/7/2003
YSwanson	34	45	Royal	Regular User	Yvonne Swanson	Corporate	2/9/2006
TNolan	34	45	Royal	Regular User	Tamara Nolan	Corporate	8/23/2009
PSutton	34	45	spherelab	Regular User	Penny Sutton	Corporate	12/15/2017
DHahn	34	45	SPHEREIab93	Regular User	Dion Hahn	Corporate	1/23/2018
JRowland	33	1	labsrptsvr01	Regular User	Johnathan Rowland	Corporate	2/26/2016



Account Name	Server Count	App Count	Domain	Account Type	Account Owner	Account Owner Business Unit	Last Login Time
LSweeney	33	197	spherelab	Admin User	Kathleen Casey	Corporate	9/2/2011
DTrujillo	33	197	spherelab	Regular User	Deborah Trujillo	Corporate	6/22/2013
SSavage	33	197	Royal	Regular User	Sarah Savage	Corporate	1/29/2007
JBlackwell	33	197	Royal	Regular User	Jayvon Blackwell	Corporate	1/23/2018
LMcpherson	33	197	Royal	Regular User	Liza Mcpherson	Corporate	1/23/2018
RBanks	33	197	Royal	Regular User	Rory Banks	Corporate	1/23/2018
ETravis	33	197	Royal	Regular User	Ezequiel Travis	Corporate	1/23/2018
SBautista2	33	197	Royal	Regular User	Sam Bautista	Corporate	1/23/2018

Certification

As only asset owners (account/server/application) know which accounts should be onboarded into a password vaulting solution, as well as who requires access and what they need access to, certifying accounts is equally as important as identifying ownership.

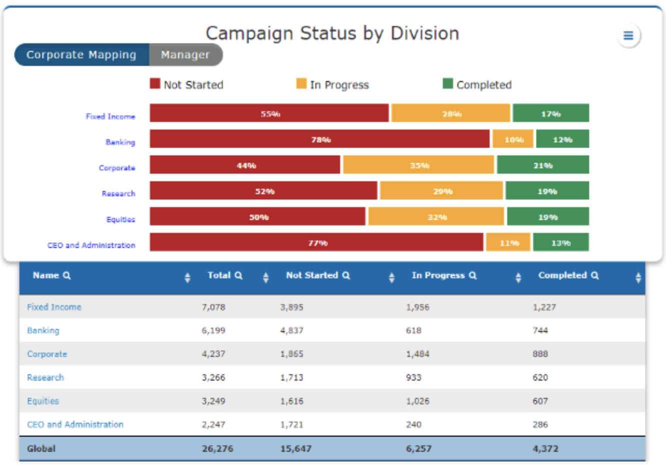


□ Notify	Name	Domain	Asset Count	Incomplete Reviews	Email Count
□	Kathleen Casey	LA-DOM09	69	59	9

Email Date	Assets Confirmed	Incomplete Reviews	Percent Complete
Thu Oct 25 2018	61	10	🟩 85.92%
Thu Oct 25 2018	61	10	🟩 85.92%
Mon Jun 04 2018	41	48	🟧 46.07%
Mon Jun 04 2018	41	48	🟧 46.07%
Wed May 16 2018	41	48	🟧 46.07%
Mon Apr 23 2018	33	52	🟧 38.82%
Thu Apr 19 2018	33	52	🟧 38.82%
Thu Apr 19 2018	33	52	🟧 38.82%
Thu Apr 19 2018	33	51	🟧 39.29%

What to Certify

To start validating ownership, simply ask the question, “Are you the owner?” as it is a critical first step before moving onto more detailed questions. If the individual is not the owner, it is inherent that the solution provides a mechanism to propose a new owner or supply additional information of value to the project team. Again, some accounts may no longer be needed.



Name	Total	Not Started	In Progress	Completed
Fixed Income	7,078	3,895	1,956	1,227
Banking	6,199	4,837	618	744
Corporate	4,237	1,865	1,484	888
Research	3,266	1,713	933	620
Equities	3,249	1,616	1,026	607
CEO and Administration	2,247	1,721	240	286
Global	**26,276**	**15,647**	**6,257**	**4,372**

Manage Results - Automation is key!

Historically, certifying accounts is incredibly tedious, error prone and, in the end, not very effective, in terms of tracking actual progress. Given large IT organizations can have hundreds of thousands of users and numerous accounts associated with them, automating the certification process is key to a successful recertification campaign. The software should not only track results, it should be able to collect feedback and provide the built-in mechanisms to share results with others in IT as well as the lines of business, if necessary.

Equally important is having the ability to measure and report on the areas of the business that are participating and making progress as well as the data owners and business units that are unresponsive or slow to respond, as auditors and compliance groups need a proof-of-completion as a part of their regular audit requirements.

Prune Access

With the visibility and ability to report on access and ownership, remediating unnecessary accounts is the next step. Remediating stale and unused accounts from the systems has an immediate reduction in risk with little or no impact to the end-users.

This will require identifying each account’s most recent log-on date per endpoint, its stale date, while removing the accounts on each endpoint that are defined as stale.

For a workflow application to be effective it should integrate with a change management solution. In three basic steps, this requires identifying any accounts that are unnecessary, submitting a change request to remove access, then removing the privileges and access from the endpoint.

Onboard to PAM

Here's where you begin to close the loop on longer-term PAM governance. At this point of the program, you will require a remediation plan encompassing an interview process, training and hand holding.

Your solution will take you through several activity workflows:

1. Workshop with internal developers to understand how authentication and privileged access is currently managed.
2. Create a standard communication and interview process for each asset.
3. Create formal training sessions for users after remediation.
4. Create and agree on processes and procedures for remediating and onboarding accounts to your PAM solution.

Next, you will work closely with application owners through your next set of activities:

1. Interview critical application owners and understand the full privileged access requirements of their application, encompassing:

   (a) accounts that require access;
   (b) the machines they need access to; and
   (c) the password management of the account.

2. Review the onboarding process with the owners.
3. Ensure owners make necessary access changes as required.

Accounts that have been certified by asset owners and reviewed to ensure proper access can now be onboarded. Here's what to keep in mind next:

1. Application service accounts will be onboarded into your password and session management system via their approved methods after the application owner interview.
2. Infrastructure access accounts will be onboarded either by:

   (a) Creating new local accounts to be onboarded into the system following a standard naming convention; or
   (b) Onboarding existing accounts where the use case of the account is approved.

3. Passwords will be rotated where applicable.

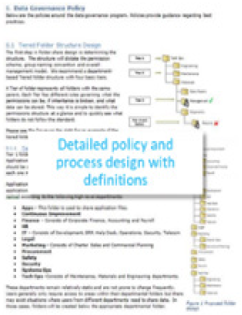
Target Operating Model

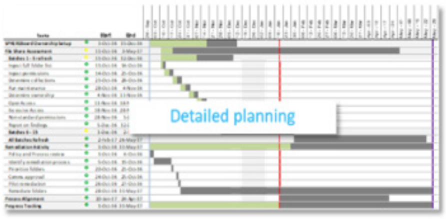
A target operating model establishes what a remediated environment should look like in its end state with the necessary policies, processes and controls in place for managing the environment on an ongoing basis. This includes existing control standards, staffing levels, existing or planned technologies, in addition to any regulatory or compliance standards.

A fully managed PAM environment will identify the current and future requirements around privileged access and create a set of policies and processes for the ongoing management of privileged access.

In order to discover, inventory, certify and remediate privileged accounts as needed, it is critical that any workflow application can report and provide analytics to the lines of business.

Recommended policies


Detailed policy and process design with definitions


Detailed planning

Enabling a fully managed end state for your privileged access.

When filling the gaps in PAM, consider this 10-step checklist:

1.

Align your scope to your organizational structure. You'll want to document all the core elements unique to your organization's use cases.

2.

Inventory your environment. Develop a picture of your systems, accounts, users and operational processes. This will inform the structure for access within your PAM control.

3.

Identify ownership. This analysis can include name convention matching, OU location, managed by fields and other external feeds.

4.

Measure risk and identify security issues. Ensure your solution assigns risk ratings based on access and use case. Remediate the assets that have the biggest impact on overall risk to the organization.

5.

Leverage automation for ownership outreach allowing potential owners to certify account access without manual analysis.

6.

Prune unused stale accounts from the target systems with little end user impact to start immediately reducing risk.

7.

Integrate with trouble ticket, change control and major incident systems to provide automation for many common processes.

8.

Understand your operational frameworks when evaluating access and processes for inclusion in your PAM system. Not every existing process or access criteria should be onboarded.

9.

Close the loop on longer-term PAM governance with ongoing remediation and account onboarding. Establish your target operating model.

10.

Know your controls and requirements. Monitoring and reporting are essential secondary controls for PAM and some regulated industries may even require session monitoring or advanced analytics.

About SPHERE

SPHERE Technology Solutions is an award-winning, woman-owned cybersecurity business focusing on improving security and enhancing compliance. SPHERE puts the controls in place to secure your most sensitive data, create the right governance processes for your systems and assets, and make sure companies are compliant with the alphabet soup of regulations surrounding their respective industries. For more information, please visit www.sphereco.com.

CONTACT US

50 Harrison St
Suite 308
Hoboken, NJ 07030

☎ +1 (201) 659-6204

✉ sales@sphereco.com

www.sphereco.com