BOMGAR

BOMGAR DISCOVERY REPORT

This report is designed to give you important information about the privileged credentials regularly being used to access endpoints and systems on your network, including:

- **AD Domain Accounts**
- **Local Windows Accounts**
- **Service Accounts**

The first step in addressing security risks from privileged users such as insiders and third parties is a high level assessment of the privileged accounts on your network. The Bomgar Discovery Report provides key information on the scope of these privileged accounts, including not just the number of credentials but also password age.

Why This Data Is Important

The vast majority of data breaches today involve compromised or stolen credentials. Both hackers and malicious insiders regularly use legitimate privileged credentials to initiate breaches and move undetected in IT networks for weeks or months, quickly elevating access levels across systems to then exfiltrate data or spread malware. The risk related to the inappropriate or dangerous use of privileged credentials cannot be adequately addressed without understanding their scope in your network.

How To Use This Report

The data in this report is available for your organization to utilize in the effort to protect your organization from cyber threats. The Bomgar team is available as a resource when you are ready to take these actions:

- Ask questions about the data in this report
- Run a more in-depth discovery exercise utilizing automated, continuous discovery available with Bomgar Privileged Identity that protects privileged credentials at scale
- Evaluate Bomgar Privileged Identity as a solution to simplify the management of privileged credentials and reduce cyber breach risk

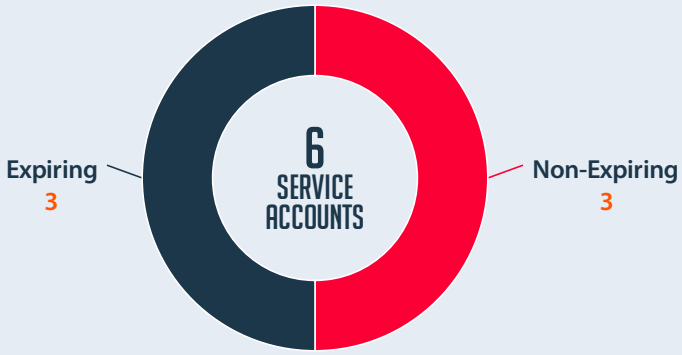
Learn more about how Bomgar Privileged Identity empowers you to proactively defend your organization from the ongoing threats of compromised privileged credentials.

View a Demo:
bomgar.com/privileged-identity/demo

Service Account Analysis

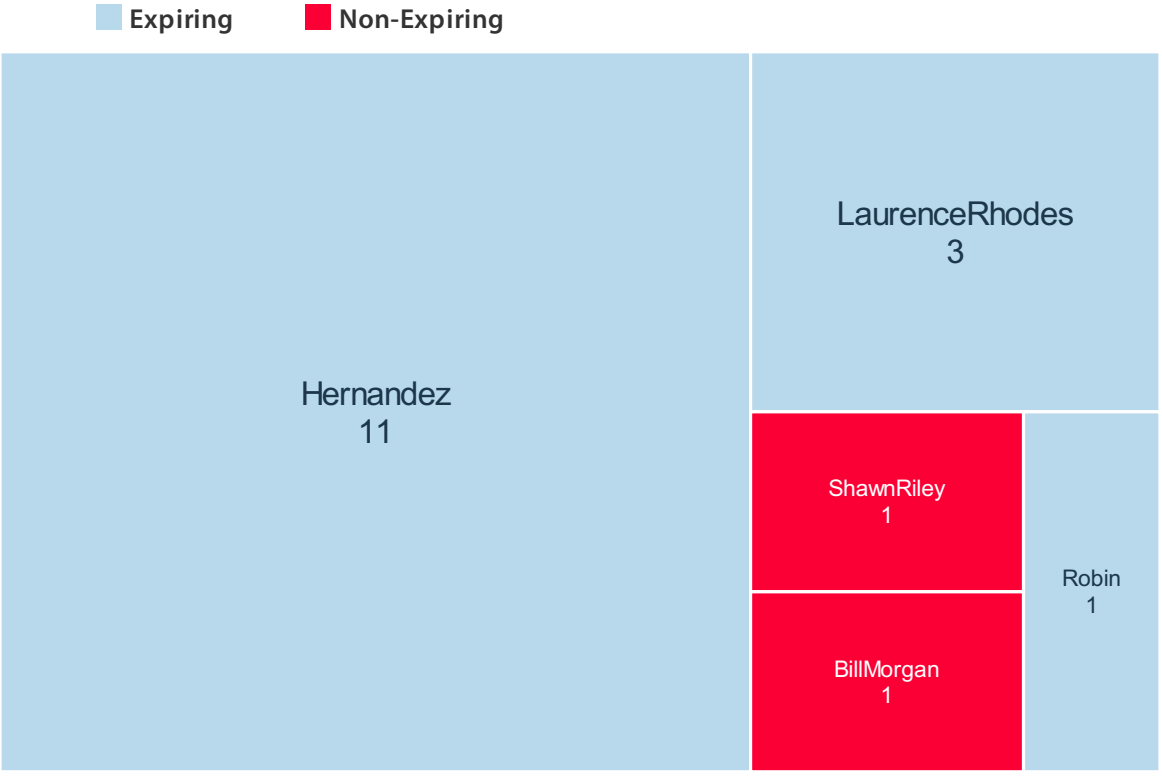
This data represents the total number of Service Accounts found during the Discovery process. A service account is a special account type that belongs to an application or service, instead of to an individual end user.

SERVICE ACCOUNTS SUMMARY



PASSWORD AGE – NON-EXPIRING SERVICE ACCOUNTS

TOP SERVICE ACCOUNTS BY NUMBER OF DEPENDENT APPLICATIONS



Key Takeaway

Service accounts present a unique security and usability threat, especially if the service accounts require privileged login credentials and have multiple dependencies across various systems and locations. Non-expiring service accounts increase the potential risk of attacks from threat actors. Bringing these accounts under management secures the credentials while managing the complexity of dependencies.

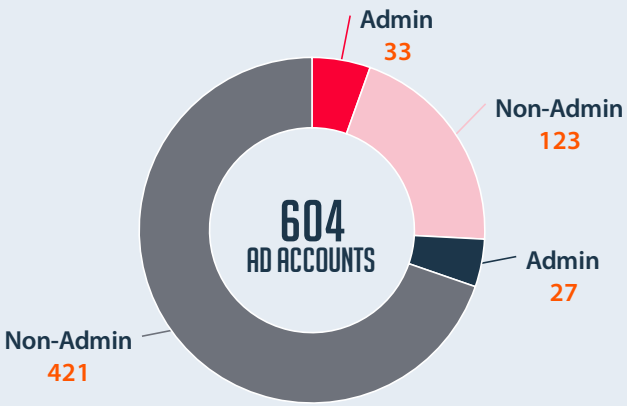
Active Directory Account Analysis

This data represents the total number of Active Directory accounts found during the Discovery process. These accounts are separated based on their status as an admin or non-admin account as well as whether they are set to expire or not expire based on their password policy.

ACTIVE DIRECTORY ACCOUNT SUMMARY

Non-Expiring Accounts 156

Expiring Accounts 448



PASSWORD AGE – NON-EXPIRING ACTIVE DIRECTORY ACCOUNTS

HIGH RISK AD ACCOUNTS

	ACCOUNT NAME	PASSWORD AGE (IF NON-EXPIRING)	# SERVICES CONTROLLED BY THIS ACCOUNT
1.	Hernandez	--	15
2.	Tammy	288	14
3.	BillMorgan	57	18
4.	HeatherSimmons	78	4
5.	KevinPrice	--	5

Key Takeaway

Non-expiring accounts are a security risk as they can be compromised and utilized by malicious actors who can then use the credentials in perpetuity, especially for admin accounts. If these privileged accounts with elevated credentials are compromised, they can be used very quickly to move laterally across your network and pivot into other areas of your network. In just a matter of hours, hackers can use them to initiate a breach and introduce malware or exfiltrate sensitive data.

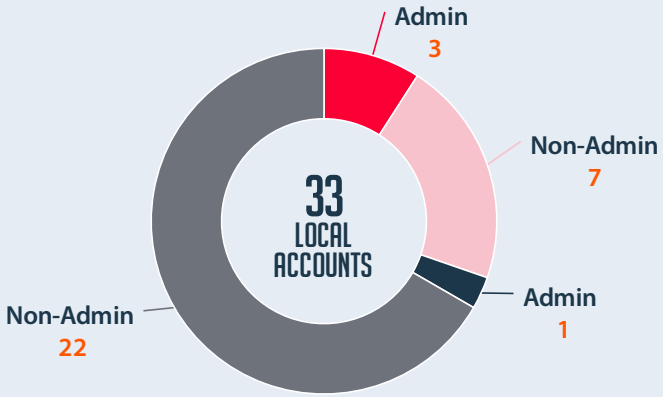
Local Account Analysis

This data represents the total number of Local Accounts found during the Discovery process. Local user accounts are stored locally on the server, and are assigned rights and permissions on a particular server only.

LOCAL ACCOUNT SUMMARY

Non-Expiring Accounts
10

Expiring Accounts
23



PASSWORD AGE – NON-EXPIRING LOCAL ACCOUNTS

Key Takeaway

Non-expiring passwords on Local Accounts can present a serious threat to an organization by providing a threat actor with the means necessary to compromise an organization's network, yet they are often overlooked and hard to report on in aggregate across the enterprise. As organizations are faced with a continuously changing environment of local accounts as new servers are added, bringing these local accounts under management proactively protects them.

Scan Summary

SERVICE ACCOUNTS SCAN SUMMARY

Service Accounts	6
Total Services	15
IIS App Pools	6
DCOM Components	6
COM+ Applications	2
Scheduled Tasks	0
Windows Services	1
Accounts with Non-Expiring Passwords	3
Non-Expiring Accounts with password age less than 30 days	2
Non-Expiring Accounts with password age 30-90 days	0
Non-Expiring Accounts with password age 90+ days	1

ACTIVE DIRECTORY ACCOUNTS SCAN SUMMARY

AD Accounts	604
Computers	19
Accounts with Non-Expiring Passwords	156
Admin Accounts	60
Admin Accounts with Non-Expiring Passwords	33
Non-Expiring Accounts with password age less than 30 days	152
Non-Expiring Accounts with password age 30-90 days	1
Non-Expiring Accounts with password age 90+ days	3

LOCAL ACCOUNTS SCAN SUMMARY

Local Accounts	33
Computers Scanned	14
Accounts with Non-Expiring Passwords	10
Admin Accounts	4
Admin Accounts with Non-Expiring Passwords	3
Non-Expiring Accounts with password age less than 30 days	9
Non-Expiring Accounts with password age 30-90 days	0
Non-Expiring Accounts with password age 90+ days	1

Key Takeaway

Failure to frequently change privileged account credentials can put your network at risk for attacks from insiders and external threats. Furthermore, privileged account passwords that remain unchanged for longer than 60 days can result in compliance failures for standards such as PCI, HIPAA, GDPR, and others.

Scan Exceptions

COMPUTER	MESSAGE
somecomputer1	Unable to discovery COM+ accounts on somecomputer1. Please ensure that the server can accept service control messages or some other technical sounding firewall related thing that you might have to do to make this process work in the expected manner.
somecomputer2	Unable to discovery COM+ accounts on somecomputer1. Please ensure that the server can accept service control messages or some other technical sounding firewall related thing that you might have to do to make this process work in the expected manner.
somecomputer2	Nothing really happended, this is a test fatal message.

Mitigating The Risk of Privileged Credentials

Controlling and effectively managing privileged credentials, such as the ones covered in this report, is a primary security priority for a companies across industries and geographies. Not only does a credential management solution protect your most sensitive and critical privileged accounts from hackers, it is often a requirement to meet a variety of industry compliance mandates such as PCI, HIPAA, NERC, or GDPR.

When evaluating credential management solutions for your organization, key considerations include:

SERVICE ACCOUNTS

How are service account credentials managed within the solution?

Can service account passwords be rotated automatically without disrupting their dependent applications or dependencies?

AUTOMATION

Does the tool continuously discover credentials? Automated discovery prevents credentials from falling through the cracks as your network changes on a daily basis.

SPEED AND SCALE

How many credentials can reasonably be stored?

How fast are passwords rotated? Most organizations have hundreds or thousands of privileged accounts, and the time it takes to continuously rotate is important.

Contact Bomgar today to learn more about how Bomgar Privileged Identity empowers you to proactively defend your organization from the ongoing threats of compromised privileged credentials.

VIEW A DEMO:

bomgar.com/privileged-identity/demo

CONTACT | INFO@BOMGAR.COM | 866-205-3650 (U.S.) | +44 (0)1628-480-210 (U.K./EMEA) | BOMGAR.COM