BeyondTrust

Privileged Access Discovery Report

This report is designed to give you a high-level overview of privileged activity information about the systems scanned on your network, including:

- Privileged accounts
- Password age
- SSH keys
- Services running with user accounts
- User accounts with administrative rights
- Remote access tools installed on your systems

The first step in addressing security risks related to privileged activity such as potential credential compromise or malicious activity from inside or outside of your organization (insiders and third parties) is an assessment of the privileged accounts on your network.

SCAN DATE

Mar. 23, 2022

In this Discovery Report:

YOUR RESULTS

01

Privileged Accounts Analysis

The data in this report is available for your organization to use in the effort of protecting your infrastructure from cyber threats.

Total Number of Accounts

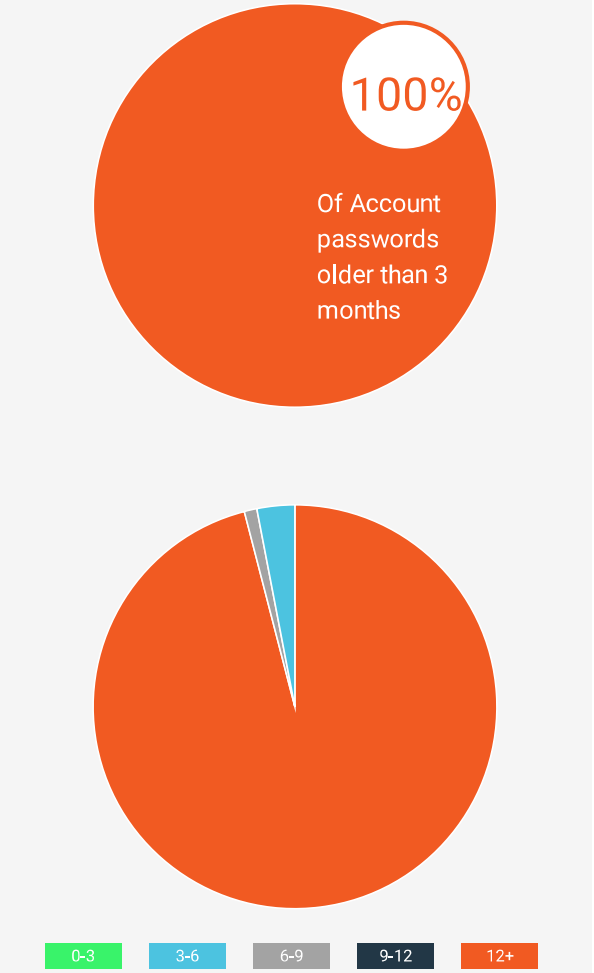
1,299	Total accounts
99	Administrative Accounts
26	Targets

Password Age

Of the 99 administrative accounts:

0	0-3 months with no password change
3	3-6 months with no password change
1	6-9 months with no password change
0	9-12 months with no password change
95	>12+ months with no password change

100% of account passwords are older than 3 months



01

Password Age Breakdown

Of the scanned accounts, the following password age breakdown was discovered:

	Windows/Mac		Unix/Linux		Total
	Admin	Non-Admin	Root	Non-Root	1,299
0-3 Months	0	0	0	0	0
3-6 Months	1	2	2	355	360
6-9 Months	0	0	1	5	6
9-12 Months	0	0	0	20	20
>12+ Months	1	6	94	812	913

Password Age Key Takeaway

Stale or aging passwords represent a security risk as they are sought after by malicious actors to gain access to your critical environments. Passwords should be rotated on a regular basis to mitigate the risk of abuse or misuse.

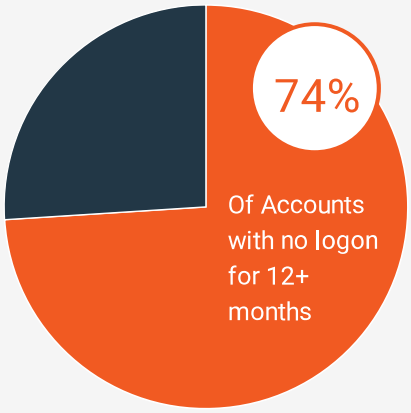
Learn more about: Password Rotation

01

Account Logon Analysis

99 Administrative Accounts

74 >12+ months with no logon



Of the scanned accounts, the following logon breakdown was discovered:

	Windows/Mac		Unix/Linux		Total
	Admin	Non-Admin	Root	Non-Root	1,299
0-3 Months	0	0	0	0	0
3-6 Months	0	0	23	24	47
6-9 Months	0	0	1	9	10
9-12 Months	1	0	0	0	1
>12+ Months	1	8	73	1,159	1,241

Account Logon Analysis
Key Takeaway

An account that has not been logged onto for an extended period may be an unneeded account. Every privileged account represents an attack vector, so it is advisable to assess whether these accounts are necessary or not. For accounts that must remain in your system, adaptive access control (a 'Just-in-Time') approach is recommended.

Learn more about: Just-in-Time Access Control

01

SSH Keys Analysis

7	Total SSH Public Keys
87	Accounts with SSH public keys attached
87	Accounts with >1 public key assigned
38	Accounts sharing a public key

SSH Keys Analysis

Key Takeaway

Traditional methods of SSH key management are very labor intensive, so it is easy to see why many organizations do not properly rotate their keys. Between the lack of rotation and the sharing of keys, organizations lose accountability over their systems, which could lead to those systems being vulnerable to exploits. We recommend storing private keys like any other privileged credential.

Learn more about: Simplified SSH Key Management

01

Service Account Analysis

1 Total service accounts

0 With expiring passwords

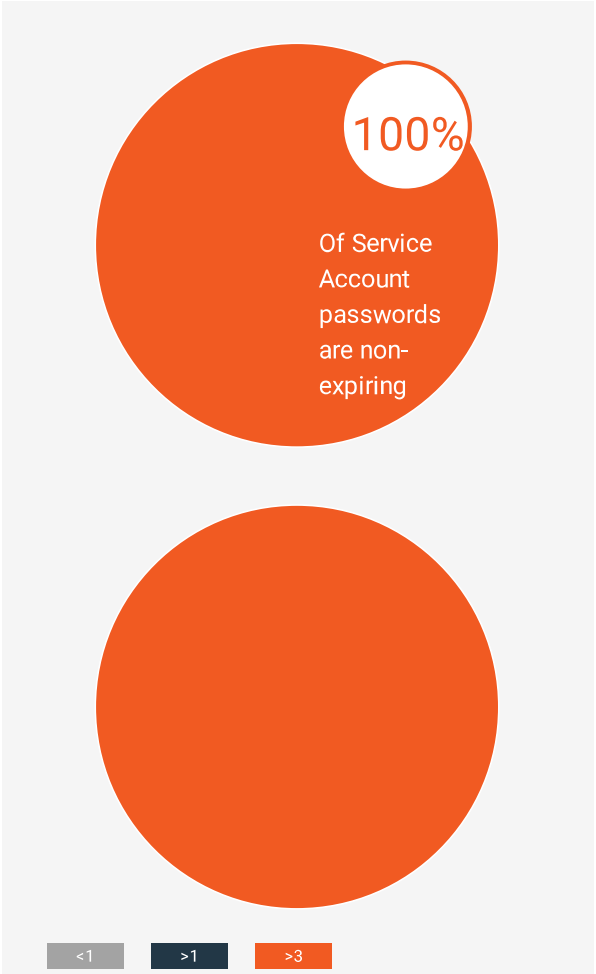
1 With non-expiring passwords

Of the 1 non-expiring service accounts:

1 With password >3 months old

0 With passwords >1 month old

VIEW A DEMO
Password Safe



Service Account Analysis
Key Takeaway

A service account is a special account type that belongs to an application or service, instead of an individual end user. All service accounts can present a security and usability threat if not properly managed. However, non-expiring passwords can be more susceptible to attacks from threat actors.

Learn more about: Service Account Management Best Practices

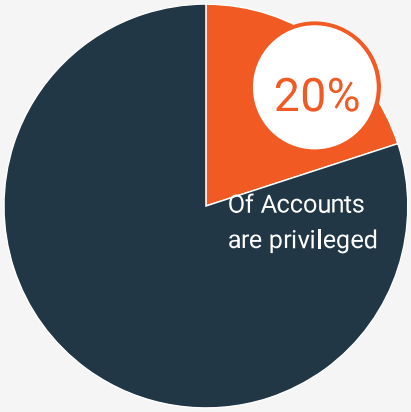
02

User Accounts Analysis

Windows / Mac

User Accounts with Administrative Rights

10	User accounts
2	Running with administrative rights



VIEW A DEMO
PM for Windows & Mac

User Accounts Analysis

Key Takeaway

With 20% of users having local admin rights, your organization is at high risk for a data breach. According to the Microsoft Vulnerabilities Report, Microsoft vulnerabilities have skyrocketed 48% in 2020 and "Privilege Escalation" was the number one category for vulernabilities.

Read the full report: Microsoft Vulnerabilities Report

03

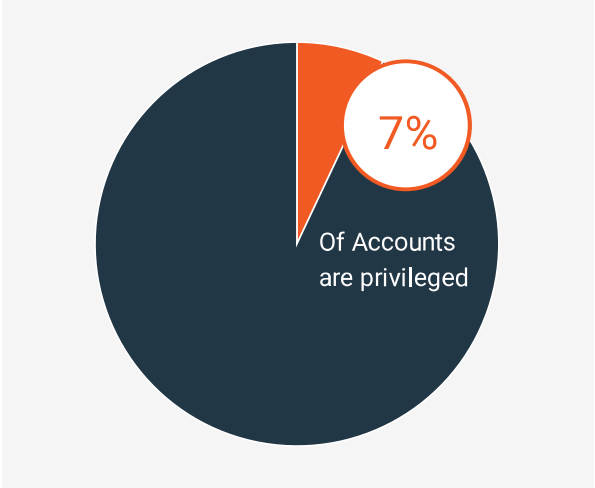
User Accounts Analysis

Unix / Linux

User Accounts with Root Privileges

1,289 User accounts

97 Running with root privileges



VIEW A DEMO
PM for Unix & Linux

With 96% of the world's web servers running Linux, solid security, root privilege management and heightended visibility are critical for larger enterprises, particularly in banking, finance, online retail, and manufacturing, especially those offering a SaaS solution.

Before 2020, most ransomware targeted Windows devices. But the pandemic accelerated digital transformation, creating a massive boom in the remote workforce and adoption of cloud applications.

04

Remote Access Tools Analysis

Remote access tools and pathways are increasingly being exploited by threat actors as backdoors into IT environments. You must closely consider how remote access tools impact the security, flexibility, reliability, and the reputation of your organization.

The following solutions have been found in the systems scanned:

VIEW A DEMO
Remote Support

RDP
Learn More

We noticed you are using RDP. It is behind the technology curve in comparison to most of the leading remote support products available. This is both from a feature and security perspective - which may be fine for small organizations on a single LAN but global organizations are exposed to risks of data breaches.

VNC
Learn More

We have noticed you are using VNC. While many organizations use VNC simply because it is free, however, it is behind the technology curve in comparison to most of the leading remote support products available. This is both from a feature and security perspective.

See all recommended solutions

Schedule a demo today!

Contact BeyondTrust

Reach out to our highly trained advisors about reviewing the results of your scan, discussing your privileged access management goals or anything else you need to know!

BeyondTrust

BeyondTrust is the worldwide leader in Privileged Access Management (PAM), empowering organizations to secure and manage their entire universe of privileges. Our integrated products and platform offer the industry's most advanced PAM solution, enabling organizations to quickly shrink their attack surface across traditional, cloud and hybrid environments.

The BeyondTrust Universal Privilege Management approach securesand protects privileges across passwords, endpoints, and access, giving organizations the visibility and control they need to reduce risk, achieve compliance, and boost operational performance. Our products enable the right level of privileges for just the time needed, creating a frictionless experience for users that enhances productivity.

With a heritage of innovation and a staunch commitment to customers, BeyondTrust solutions are easy to deploy, manage, and scale as businesses evolve. We are trusted by 20,000 customers, including 70 percent of the Fortune 500, and a global partner network.

beyondtrust.com