Qualys®

User Identity Risk

Lavish Jhamb

Senior Product Manager, Compliance Solutions

Why do we need to know User Identity?

User Identity

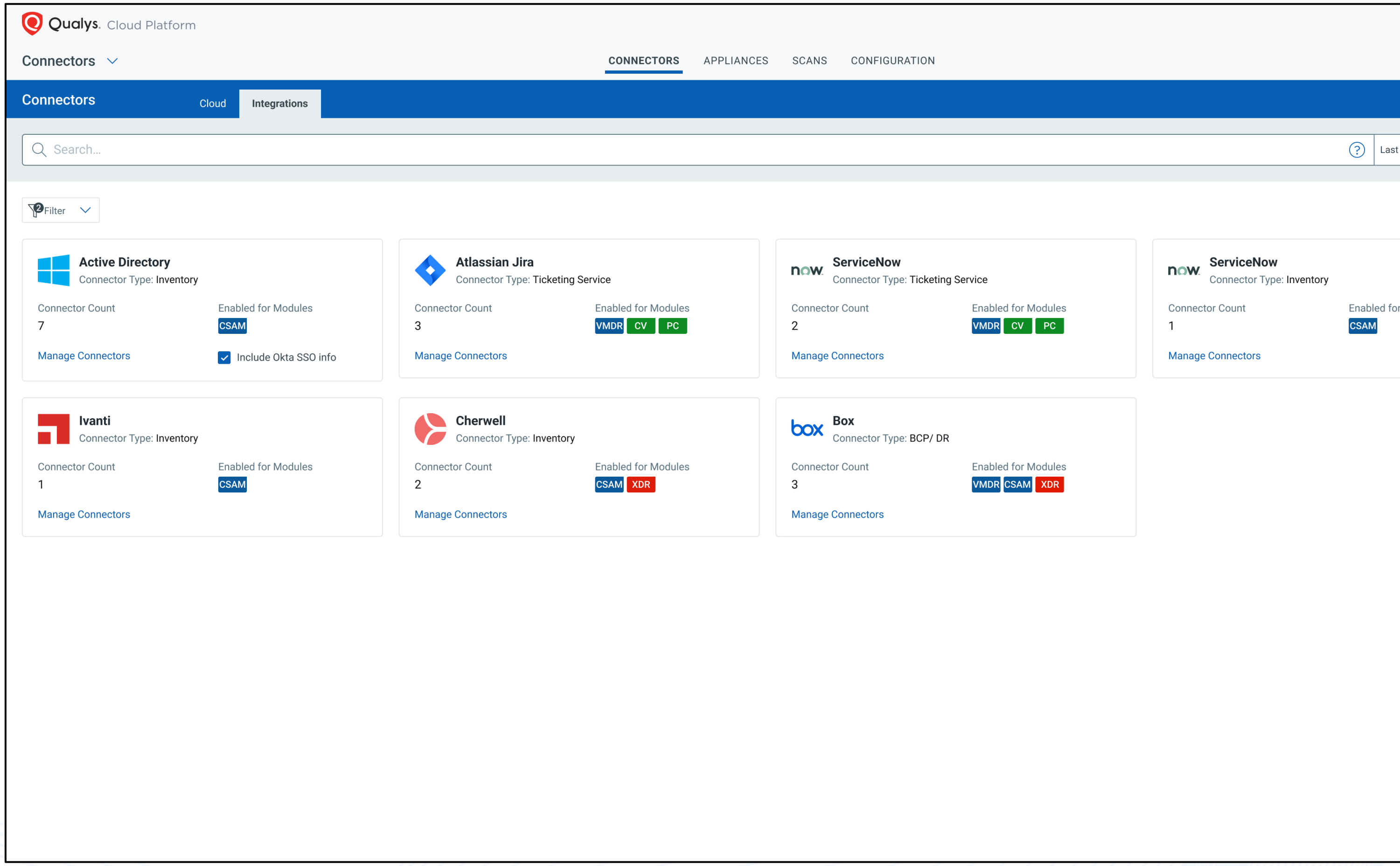
8/ 10	breaches that occur involved privileged credentials - Forrester report Source: Forrester report
57%	IT professionals do very little or no privileged account monitoring
> 40%	of organizations use MFA to secure their privileged accounts.
51%	fail to enact secure logins for privileged access accounts.
70%	of enterprises fail to discover all of the privileged accounts in their networks and 40% never bother to look in the first place
55%	fail to revoke permissions after a privileged employee is removed.
63%	don’t have security alerts in place for failed privileged access account login attempts

Source: Thycotic’s report

Source for User Inventory

Connector to fetch **user information**

- Active Directory
- Okta
- Azure



Active Directory
Connector Type: Inventory
Connector Count: 7
Enabled for Modules: CSAM
Manage Connectors
☑ Include Okta SSO info

Atlassian Jira
Connector Type: Ticketing Service
Connector Count: 3
Enabled for Modules: VMDR CV PC
Manage Connectors

ServiceNow
Connector Type: Ticketing Service
Connector Count: 2
Enabled for Modules: VMDR CV PC
Manage Connectors

ServiceNow
Connector Type: Inventory
Connector Count: 1
Enabled fo
CSAM
Manage Connectors

Ivanti
Connector Type: Inventory
Connector Count: 1
Enabled for Modules: CSAM
Manage Connectors

Cherwell
Connector Type: Inventory
Connector Count: 2
Enabled for Modules: CSAM XDR
Manage Connectors

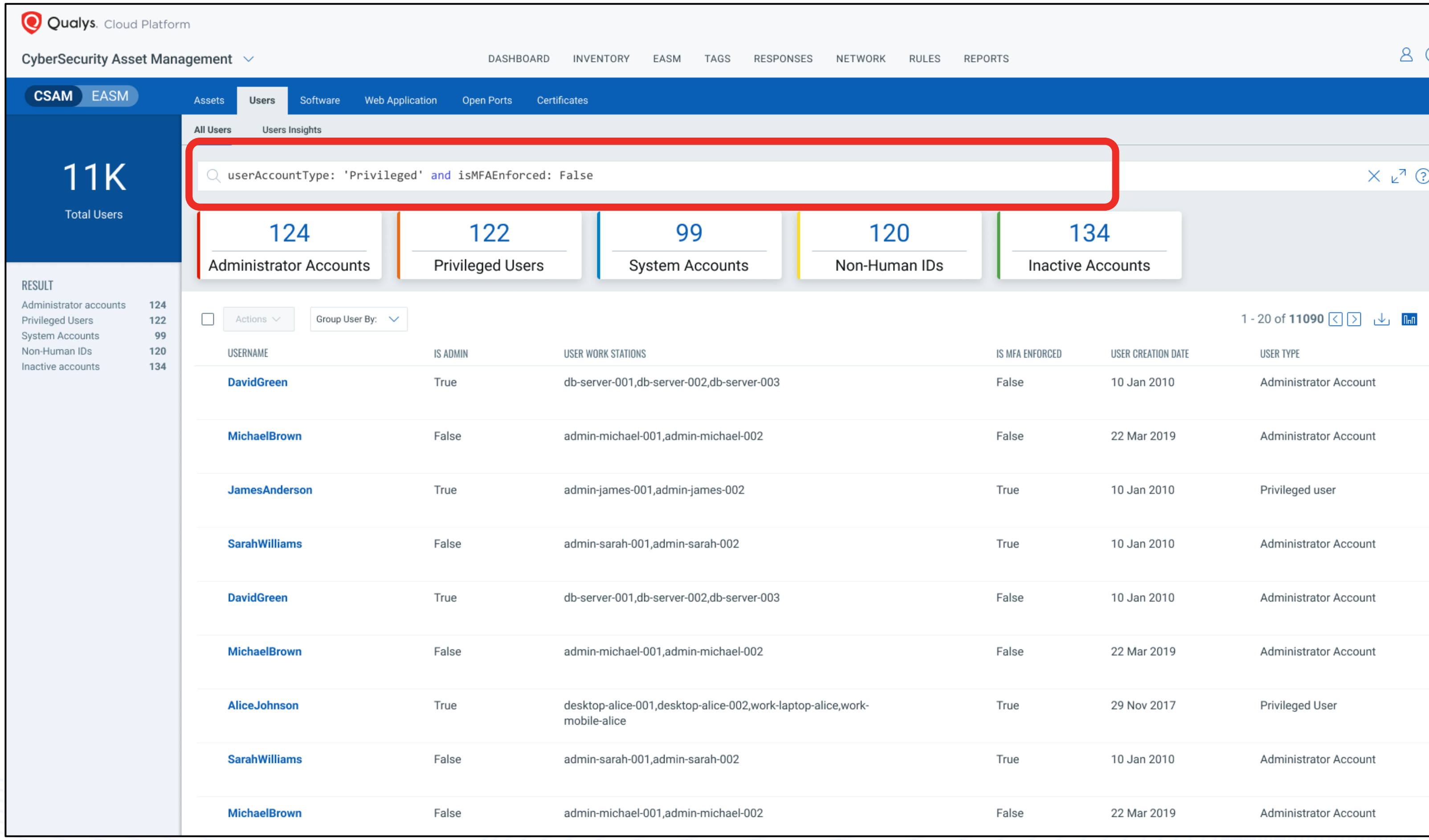
Box
Connector Type: BCP/ DR
Connector Count: 3
Enabled for Modules: VMDR CSAM XDR
Manage Connectors

User Inventory Includes Attributes and Entitlements

User inventory Domain users with comprehensive details

User Attributes Properties of domain users

User Entitlements Rights or privileges granted to users, determining what actions they can perform or what resources they can access within a system.



```
userAccountType: 'Privileged' and isMFAEnforced: False
```

11K Total Users

124	122	99	120	134
Administrator Accounts	Privileged Users	System Accounts	Non-Human IDs	Inactive Accounts

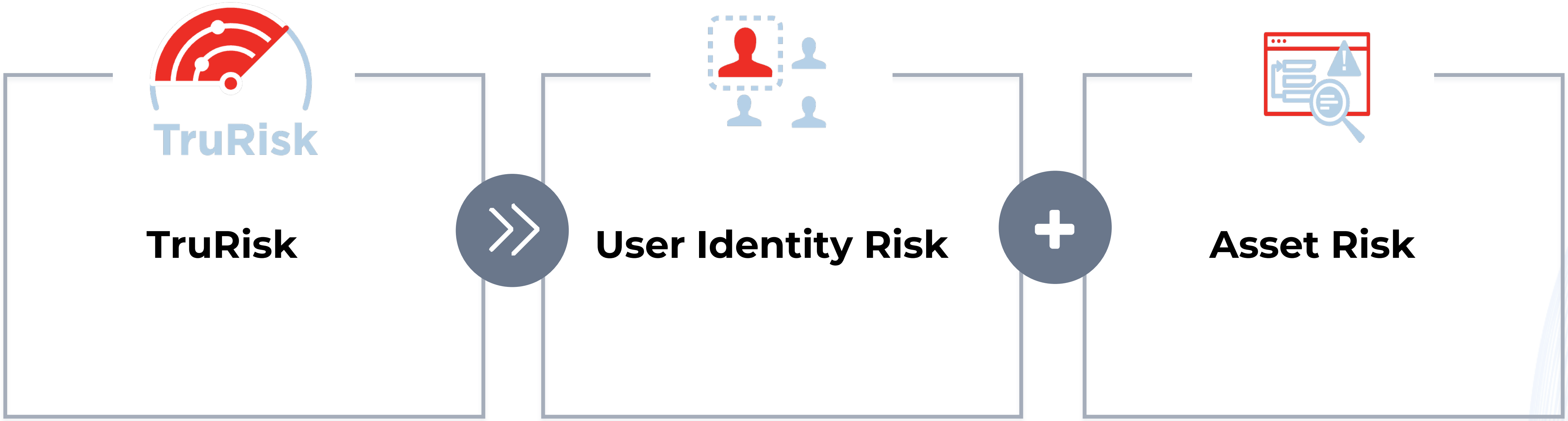
RESULT

Administrator accounts	124
Privileged Users	122
System Accounts	99
Non-Human IDs	120
Inactive accounts	134

USERNAME	IS ADMIN	USER WORK STATIONS	IS MFA ENFORCED	USER CREATION DATE	USER TYPE
DavidGreen	True	db-server-001,db-server-002,db-server-003	False	10 Jan 2010	Administrator Account
MichaelBrown	False	admin-michael-001,admin-michael-002	False	22 Mar 2019	Administrator Account
JamesAnderson	True	admin-james-001,admin-james-002	True	10 Jan 2010	Privileged user
SarahWilliams	False	admin-sarah-001,admin-sarah-002	True	10 Jan 2010	Administrator Account
DavidGreen	True	db-server-001,db-server-002,db-server-003	False	10 Jan 2010	Administrator Account
MichaelBrown	False	admin-michael-001,admin-michael-002	False	22 Mar 2019	Administrator Account
AliceJohnson	True	desktop-alice-001,desktop-alice-002,work-laptop-alice,work-mobile-alice	True	29 Nov 2017	Privileged User
SarahWilliams	False	admin-sarah-001,admin-sarah-002	True	10 Jan 2010	Administrator Account
MichaelBrown	False	admin-michael-001,admin-michael-002	False	22 Mar 2019	Administrator Account

Qualys. Get More Security

User Identity Attack Surface



TruRisk

User Identity Risk

Asset Risk

User Insights: Navigating Toxic Combinations

Top 5 user insights

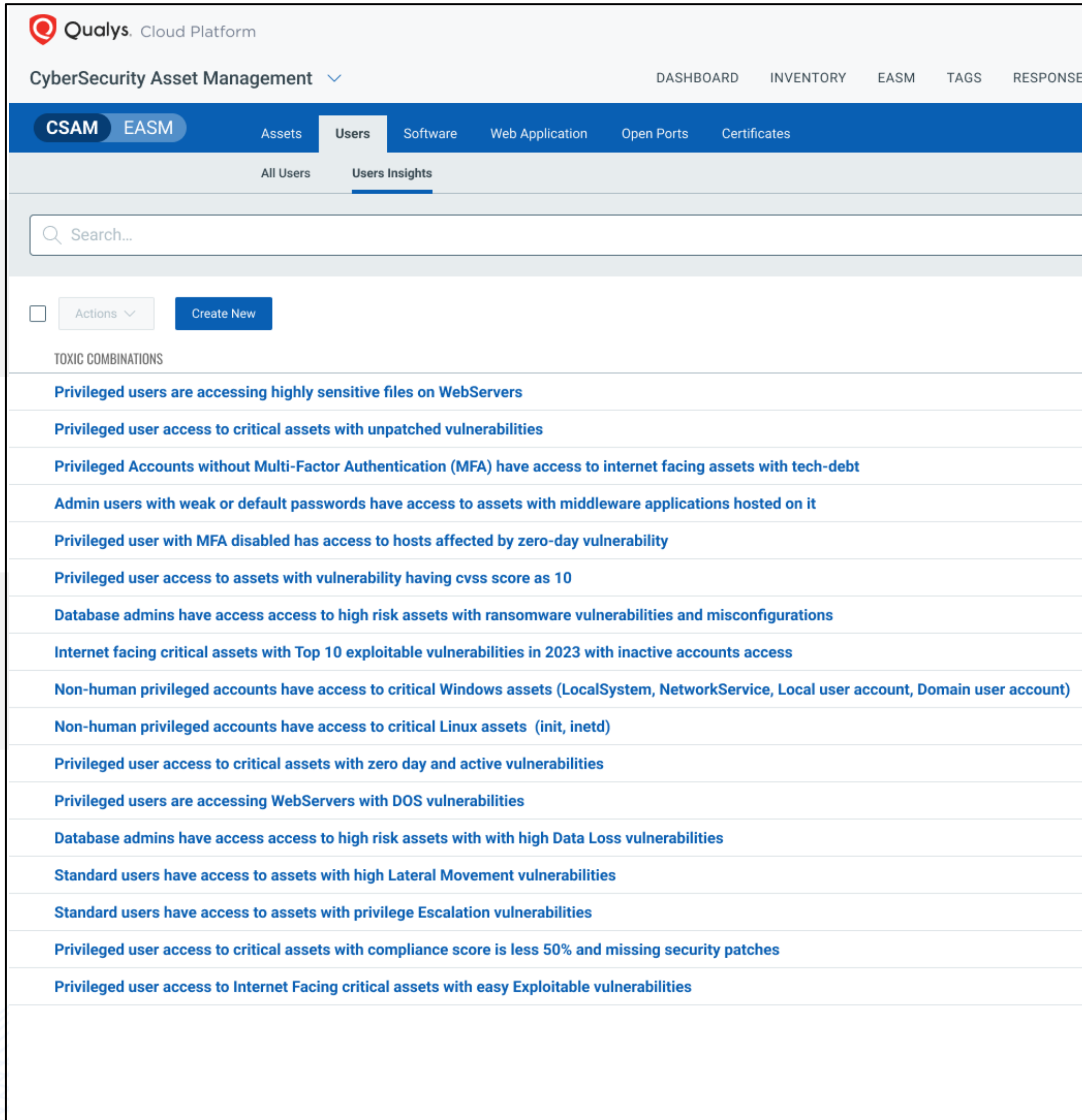
Privileged users are accessing highly sensitive files on Webservers

Privileged Accounts without Multi-Factor Authentication (MFA) have access to internet facing assets with tech-debt

Admin users with weak or default passwords have access to assets with middleware applications hosted on it

Privileged user with MFA disabled has access to hosts affected by zero-day vulnerability

Privileged user access to critical assets with unpatched vulnerabilities



TOXIC COMBINATIONS

- Privileged users are accessing highly sensitive files on WebServers
- Privileged user access to critical assets with unpatched vulnerabilities
- Privileged Accounts without Multi-Factor Authentication (MFA) have access to internet facing assets with tech-debt
- Admin users with weak or default passwords have access to assets with middleware applications hosted on it
- Privileged user with MFA disabled has access to hosts affected by zero-day vulnerability
- Privileged user access to assets with vulnerability having cvss score as 10
- Database admins have access access to high risk assets with ransomware vulnerabilities and misconfigurations
- Internet facing critical assets with Top 10 exploitable vulnerabilities in 2023 with inactive accounts access
- Non-human privileged accounts have access to critical Windows assets (LocalSystem, NetworkService, Local user account, Domain user account)
- Non-human privileged accounts have access to critical Linux assets (init, inetd)
- Privileged user access to critical assets with zero day and active vulnerabilities
- Privileged users are accessing WebServers with DOS vulnerabilities
- Database admins have access access to high risk assets with with high Data Loss vulnerabilities
- Standard users have access to assets with high Lateral Movement vulnerabilities
- Standard users have access to assets with privilege Escalation vulnerabilities
- Privileged user access to critical assets with compliance score is less 50% and missing security patches
- Privileged user access to Internet Facing critical assets with easy Exploitable vulnerabilities

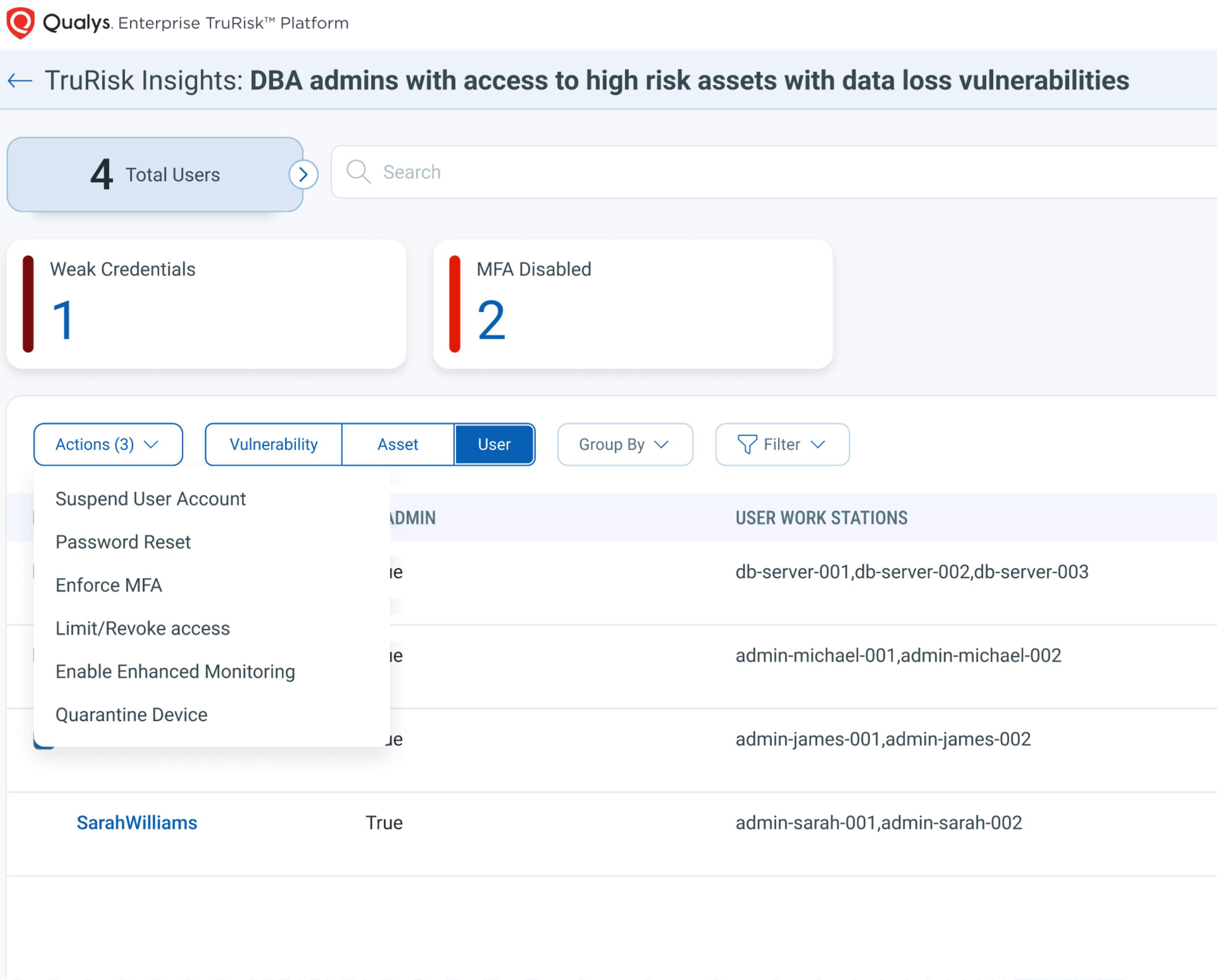
Eliminating User Risk

Default Response

Ability to take default response actions on users such as disable user, enforce MFA, etc.

Custom Response

Ability to take custom response actions on users leveraging scripting capability provided by Qualys Custom Assessment and Remediation (CAR)



Qualys. Enterprise TruRisk™ Platform

← TruRisk Insights: **DBA admins with access to high risk assets with data loss vulnerabilities**

4 Total Users

Search

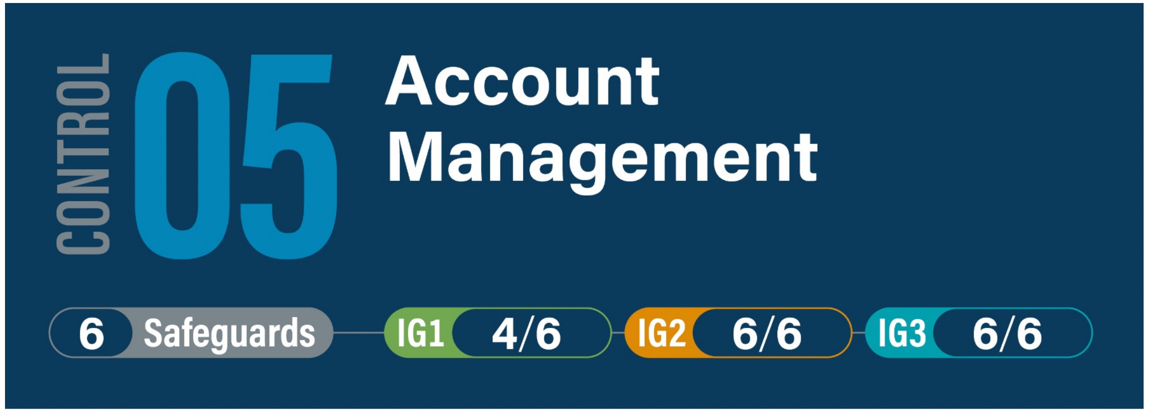
Weak Credentials
1

MFA Disabled
2

	ADMIN	USER WORK STATIONS
	ie	db-server-001,db-server-002,db-server-003
	ie	admin-michael-001,admin-michael-002
	ue	admin-james-001,admin-james-002
SarahWilliams	True	admin-sarah-001,admin-sarah-002

It's a Compliance Requirement Too!

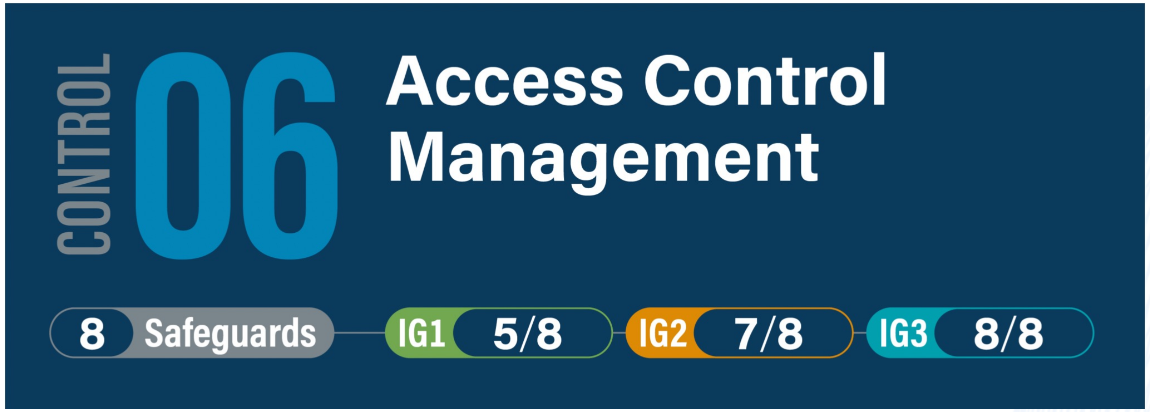
Top 18 **CIS** Critical Security Controls include



CONTROL 05

Account Management

6 Safeguards | IG1 4/6 | IG2 6/6 | IG3 6/6



CONTROL 06

Access Control Management

8 Safeguards | IG1 5/8 | IG2 7/8 | IG3 8/8

Qualys®