



The Asset Management Resurgence: From Boring to Top of Mind

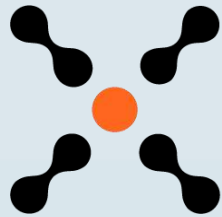
January 22, 2020



The Asset Management Resurgence: From Boring to Top of Mind



Today's web conference is generously sponsored by:



AXONIUS

<https://www.Axonius.com/>

Speakers



David Vaughn
C|CISO, LPT, GSNA, CISSP
ISSA



Nathan Burke
CMO
Axonius



Bryan Bethelmy
CISO
Mancon

Agenda

- Why the Bad Reputation?
- What Changed?
- Cybersecurity and Asset Management Overview

Why the Bad Reputation?



Traditional ITAM

- **Inventory**
 - Hardware
 - Software
 - Network Assets
- **License Management**
 - Making sure all devices are running licensed software
- **Lifecycle Management**
 - Procurement
 - Decommissioning
 - Updating Inventory

Asset Management: Unsexy



**ASSET MANAGEMENT:
THE TOYOTA CAMRY OF CYBERSECURITY**

The Asset Management Challenge



Jim Schwar

@jimiDFIR

Replying to [@MalwareJake](#)

CISO: How many windows hosts do we have?

AV Guy: 7864

Desktop Management: 6321

EDR Team: 6722

CMDB Team: 4848

SIEM Team: 9342

5:55 AM - 8 Feb 2018

540 Retweets 1,023 Likes

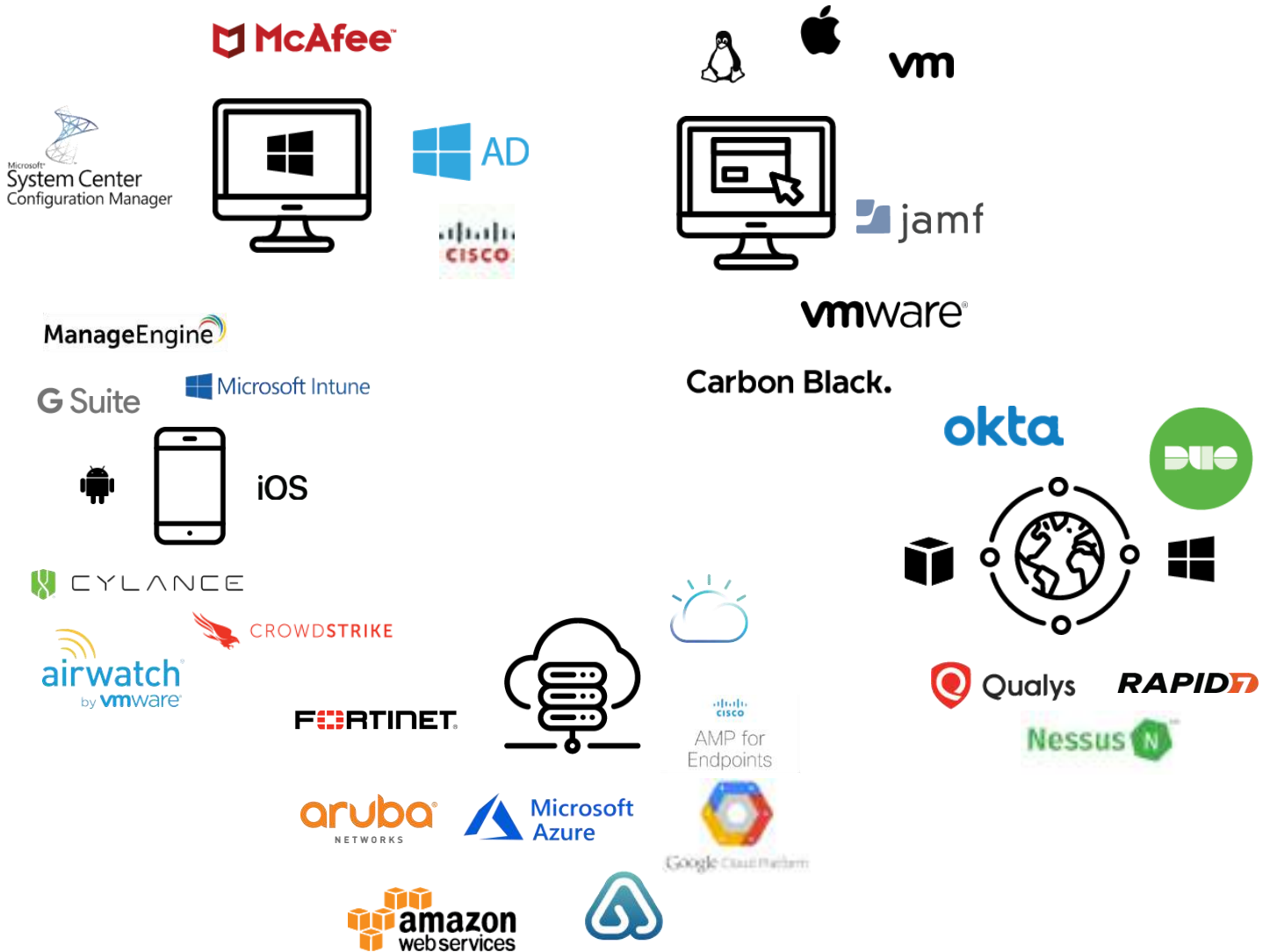


33

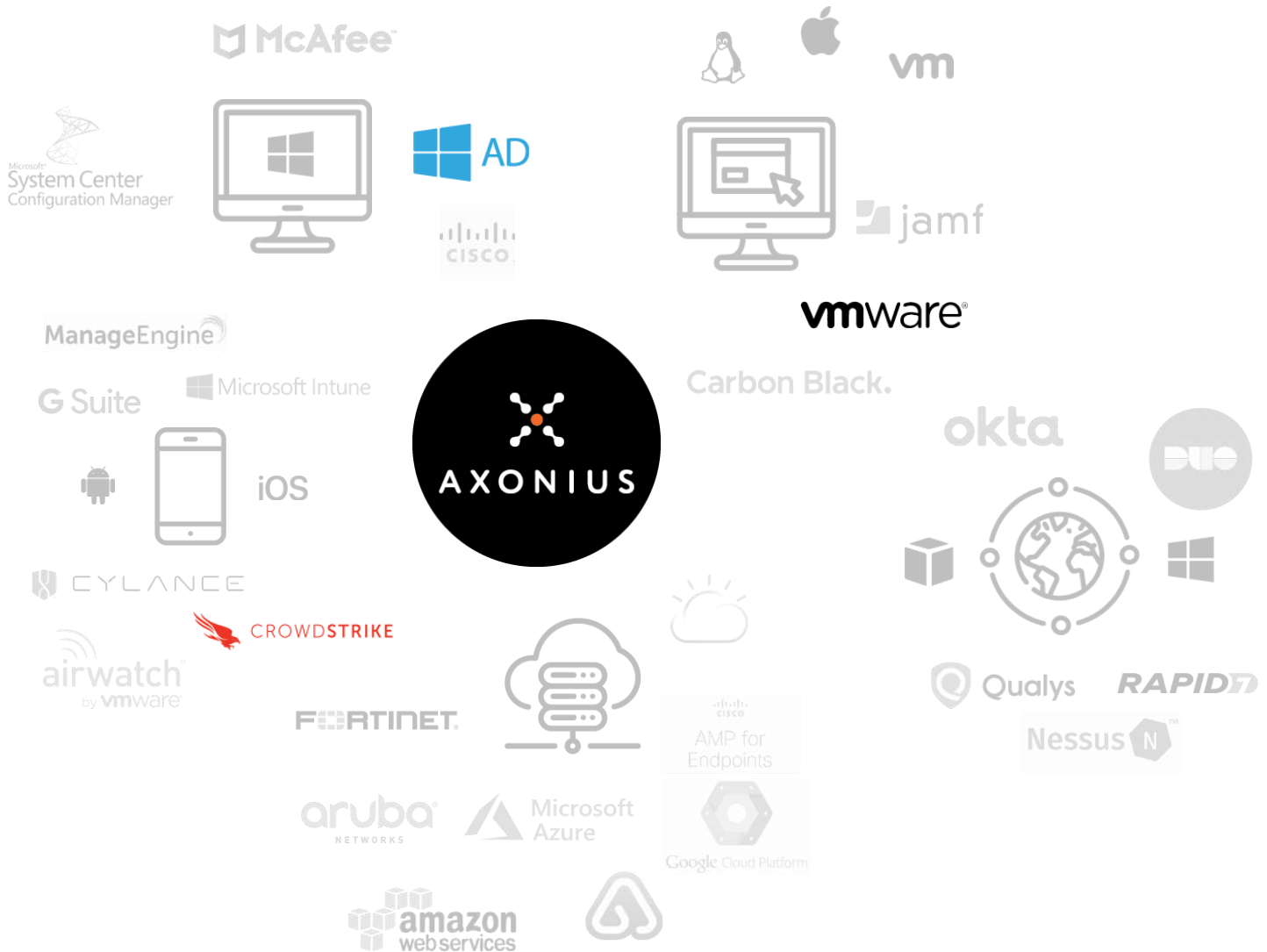
540

1.0K

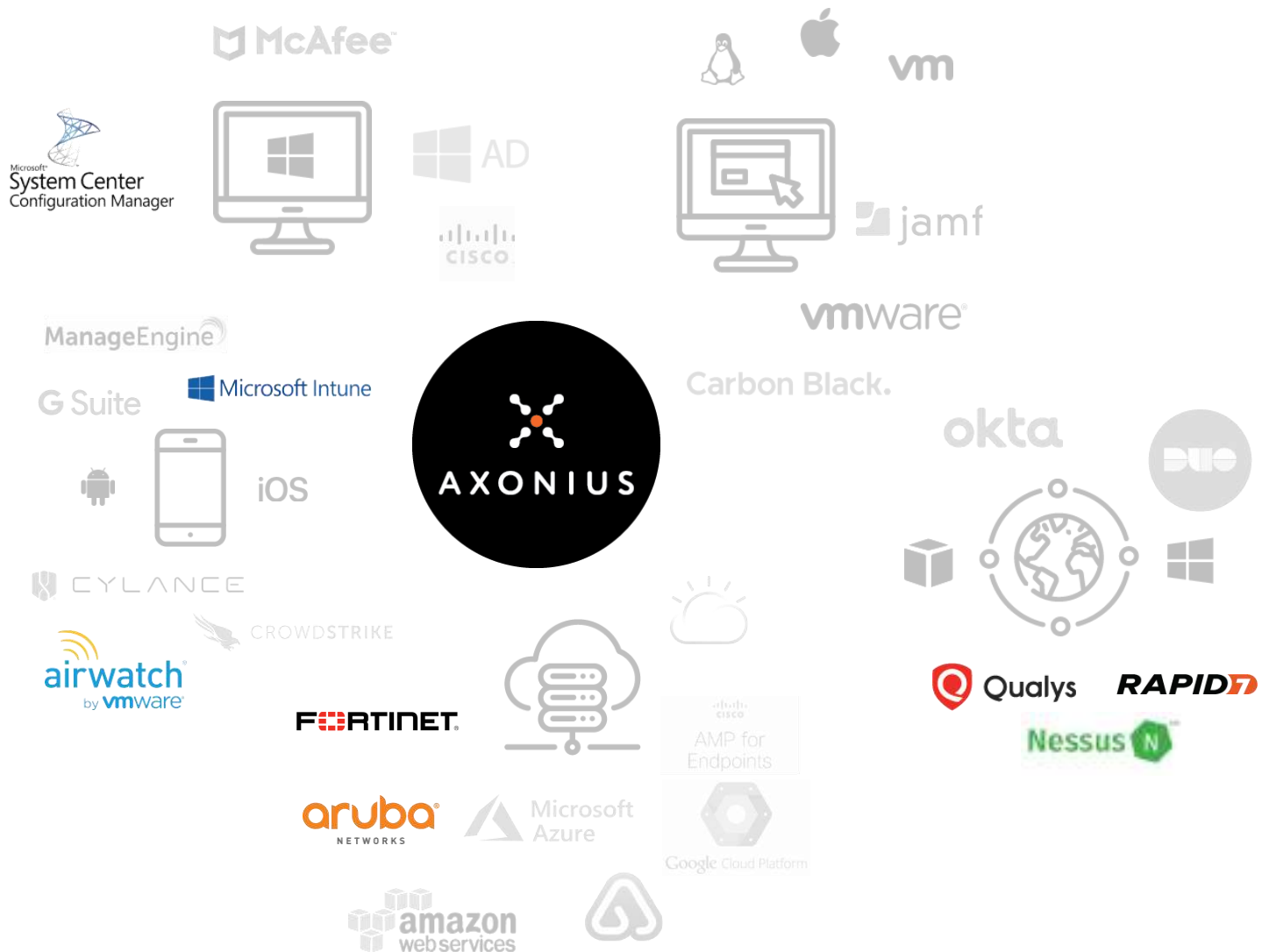
Why is Asset Management So Difficult?



Is your agent everywhere it should be?



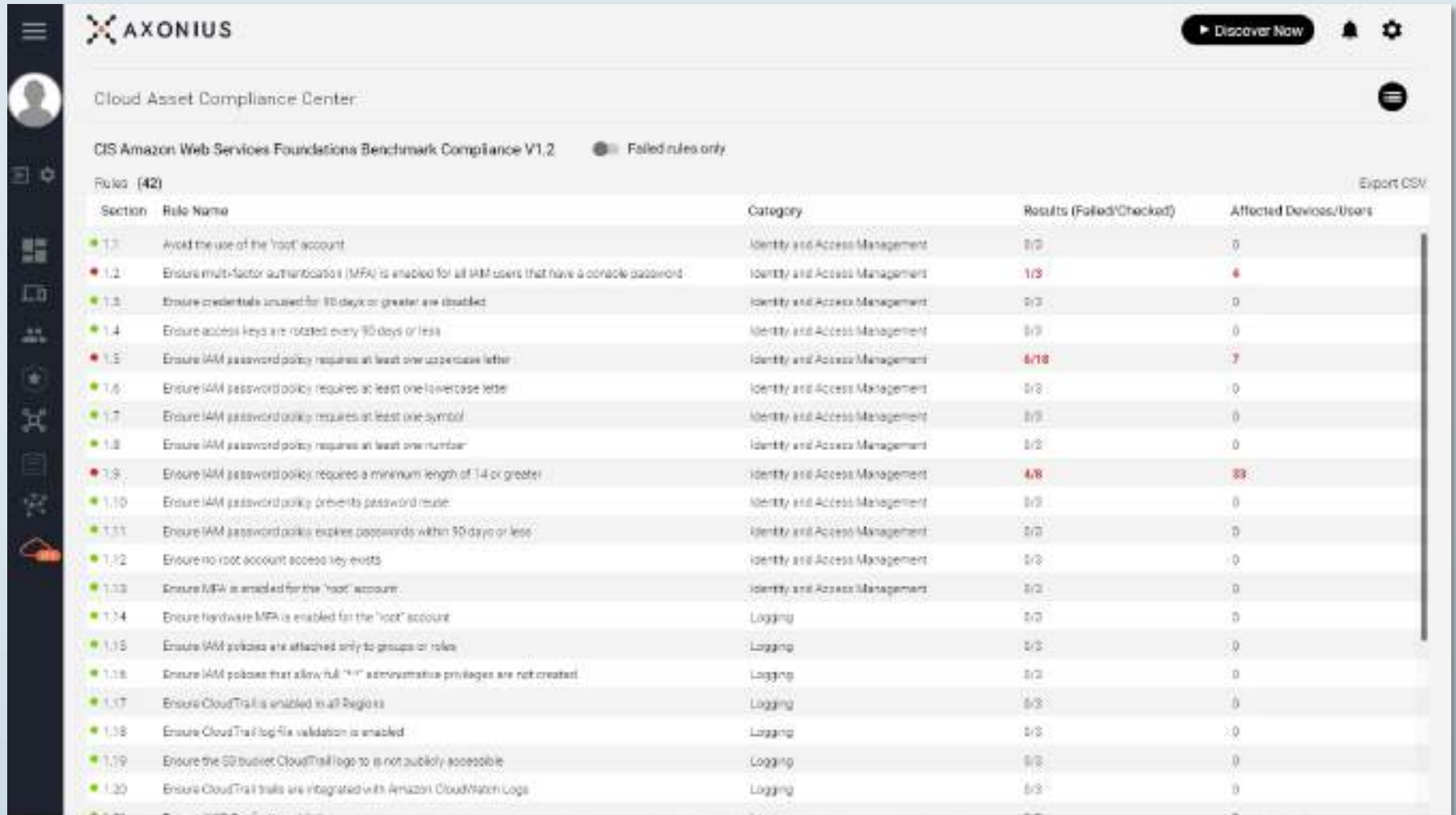
Which unmanaged devices are connected to privileged networks?



Are your cloud instances covered?



Cloud Asset Compliance



AXONIUS Discover Now

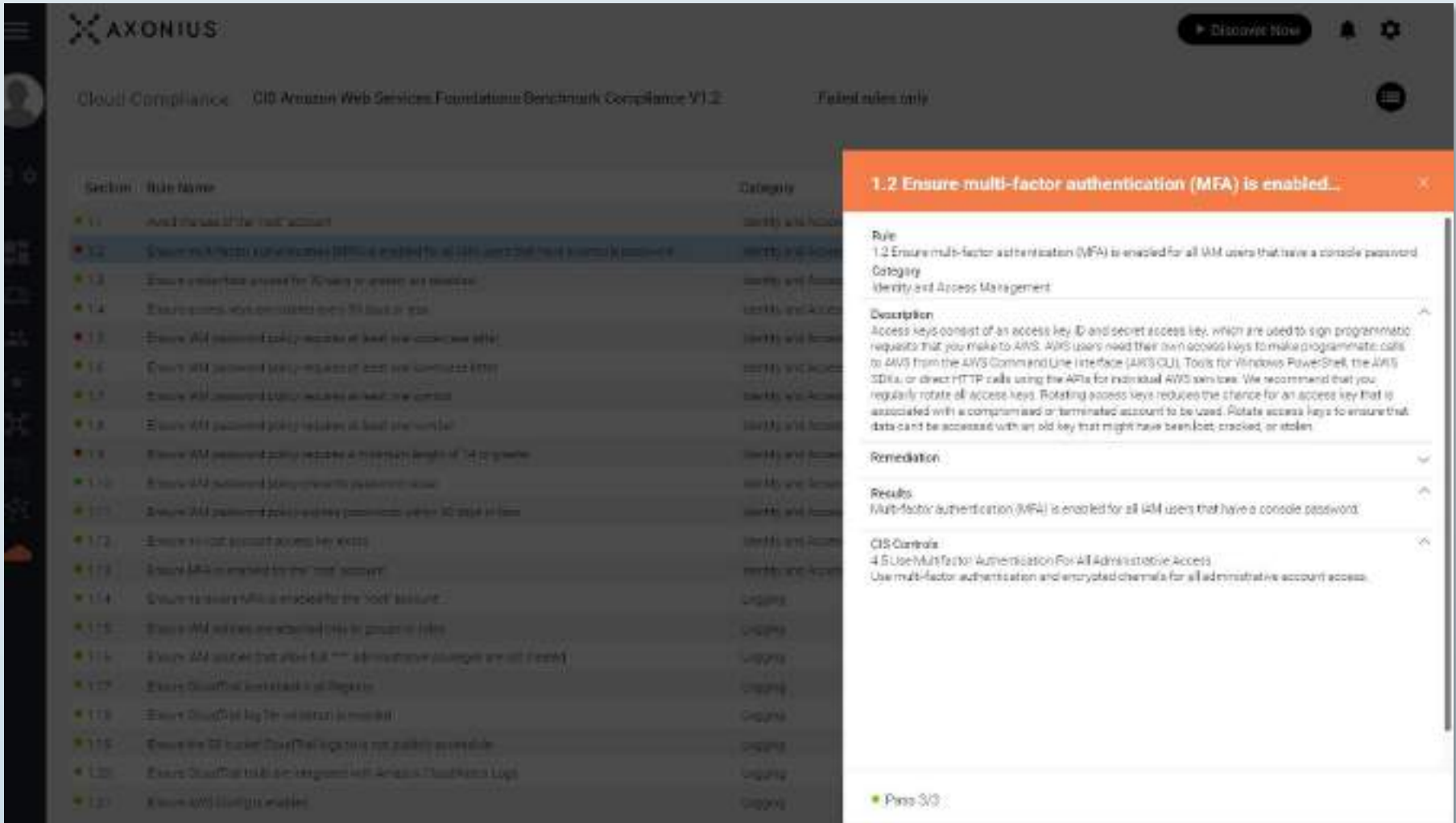
Cloud Asset Compliance Center

CIS Amazon Web Services Foundations Benchmark Compliance V1.2 ● Failed rules only

Rules (42) Export CSV

Section	Rule Name	Category	Results (Failed/Checked)	Affected Devices/Users
1.1	Avoid the use of the 'root' account	Identity and Access Management	0/0	0
1.2	Ensure multi-factor authentication (MFA) is enabled for all IAM users that have a console password	Identity and Access Management	1/0	4
1.3	Ensure credentials issued for 90 days or greater are disabled	Identity and Access Management	0/0	0
1.4	Ensure access keys are rotated every 90 days or less	Identity and Access Management	0/0	0
1.5	Ensure IAM password policy requires at least one uppercase letter	Identity and Access Management	6/10	7
1.6	Ensure IAM password policy requires at least one lowercase letter	Identity and Access Management	0/0	0
1.7	Ensure IAM password policy requires at least one symbol	Identity and Access Management	0/0	0
1.8	Ensure IAM password policy requires at least one number	Identity and Access Management	0/0	0
1.9	Ensure IAM password policy requires a minimum length of 14 or greater	Identity and Access Management	4/8	33
1.10	Ensure IAM password policy prohibits password reuse	Identity and Access Management	0/0	0
1.11	Ensure IAM password policy expires passwords within 90 days or less	Identity and Access Management	0/0	0
1.12	Ensure no root account access key exists	Identity and Access Management	0/0	0
1.13	Ensure MFA is enabled for the 'root' account	Identity and Access Management	0/0	0
1.14	Ensure hardware MFA is enabled for the 'root' account	Logging	0/0	0
1.15	Ensure IAM policies are attached only to groups or roles	Logging	0/0	0
1.16	Ensure IAM policies that allow full '*' administrative privileges are not created	Logging	0/0	0
1.17	Ensure CloudTrail is enabled in all Regions	Logging	0/0	0
1.18	Ensure CloudTrail log file validation is enabled	Logging	0/0	0
1.19	Ensure the S3 bucket CloudTrail logs to is not publicly accessible	Logging	0/0	0
1.20	Ensure CloudTrail trails are integrated with Amazon CloudWatch Logs	Logging	0/0	0

Cloud Asset Compliance



The screenshot displays the Axonius Cloud Compliance dashboard. The main view shows a list of rules under the heading "Failed rules only". A modal window is open, providing details for rule 1.2.

Section	Rule Name	Category
1.1	Ensure MFA is enabled for the root account	Identity and Access Management
1.2	Ensure multi-factor authentication (MFA) is enabled for all IAM users that have a console password	Identity and Access Management
1.3	Ensure console access for IAM users is disabled, not restricted	Identity and Access Management
1.4	Ensure console access is restricted to only the root account	Identity and Access Management
1.5	Ensure IAM password policy requires at least one uppercase letter	Identity and Access Management
1.6	Ensure IAM password policy requires at least one lowercase letter	Identity and Access Management
1.7	Ensure IAM password policy requires at least one symbol	Identity and Access Management
1.8	Ensure IAM password policy requires at least one number	Identity and Access Management
1.9	Ensure IAM password policy requires a minimum length of 14 characters	Identity and Access Management
1.10	Ensure IAM password policy requires no password reuse	Identity and Access Management
1.11	Ensure IAM password policy requires password expiry of 90 days or less	Identity and Access Management
1.12	Ensure root account access key exists	Identity and Access Management
1.13	Ensure MFA is enabled for the root account	Identity and Access Management
1.14	Ensure MFA is enabled for the root account	Identity and Access Management
1.15	Ensure IAM roles are restricted only to group or roles	Identity and Access Management
1.16	Ensure IAM users do not allow full *** administrative privileges are not needed	Identity and Access Management
1.17	Ensure CloudTrail logs are enabled in all Regions	Logging
1.18	Ensure CloudTrail logs for IAM actions is enabled	Logging
1.19	Ensure the S3 bucket CloudTrail logs is not publicly accessible	Logging
1.20	Ensure CloudTrail logs are integrated with Amazon CloudWatch Logs	Logging
1.21	Ensure AWS CloudTrail is enabled	Logging

1.2 Ensure multi-factor authentication (MFA) is enabled...	
Rule	1.2 Ensure multi-factor authentication (MFA) is enabled for all IAM users that have a console password
Category	Identity and Access Management
Description	Access keys consist of an access key ID and secret access key, which are used to sign programmatic requests that you make to AWS. AWS users need their own access keys to make programmatic calls to AWS from the AWS Command Line Interface (AWS CLI), Tools for Windows PowerShell, the AWS SDKs, or direct HTTP calls using the APIs for individual AWS services. We recommend that you regularly rotate all access keys. Rotating access keys reduces the chance for an access key that is associated with a compromised or terminated account to be used. Rotate access keys to ensure that data can't be accessed with an old key that might have been lost, cracked, or stolen.
Remediation	
Results	Multi-factor authentication (MFA) is enabled for all IAM users that have a console password.
CIS Controls	4.5 Use Multi-Factor Authentication For All Administrative Access Use multi-factor authentication and encrypted channels for all administrative account access.

Each tool answers some questions,
while begetting other questions that
it can't answer by itself.

6 Essential Questions About Every Asset



1. Is the asset “known” and managed?
2. Where is it?
3. What is it?
4. Is the core software up to date?
5. What additional software is installed?
6. Does it adhere to my security policy?



Modern asset management is the nexus for cybersecurity projects and decisions.

Modern asset management is the nexus for cybersecurity projects and decisions.

- Connect to all existing IT systems, bridging the siloed data sources.
- Correlate to create a unique entry for every asset, viewed from several perspectives.
- Remediate gaps and report on progress toward cybersecurity objectives.



ISSA

Information Systems Security Association
International

www.issa.org

QUESTIONS?