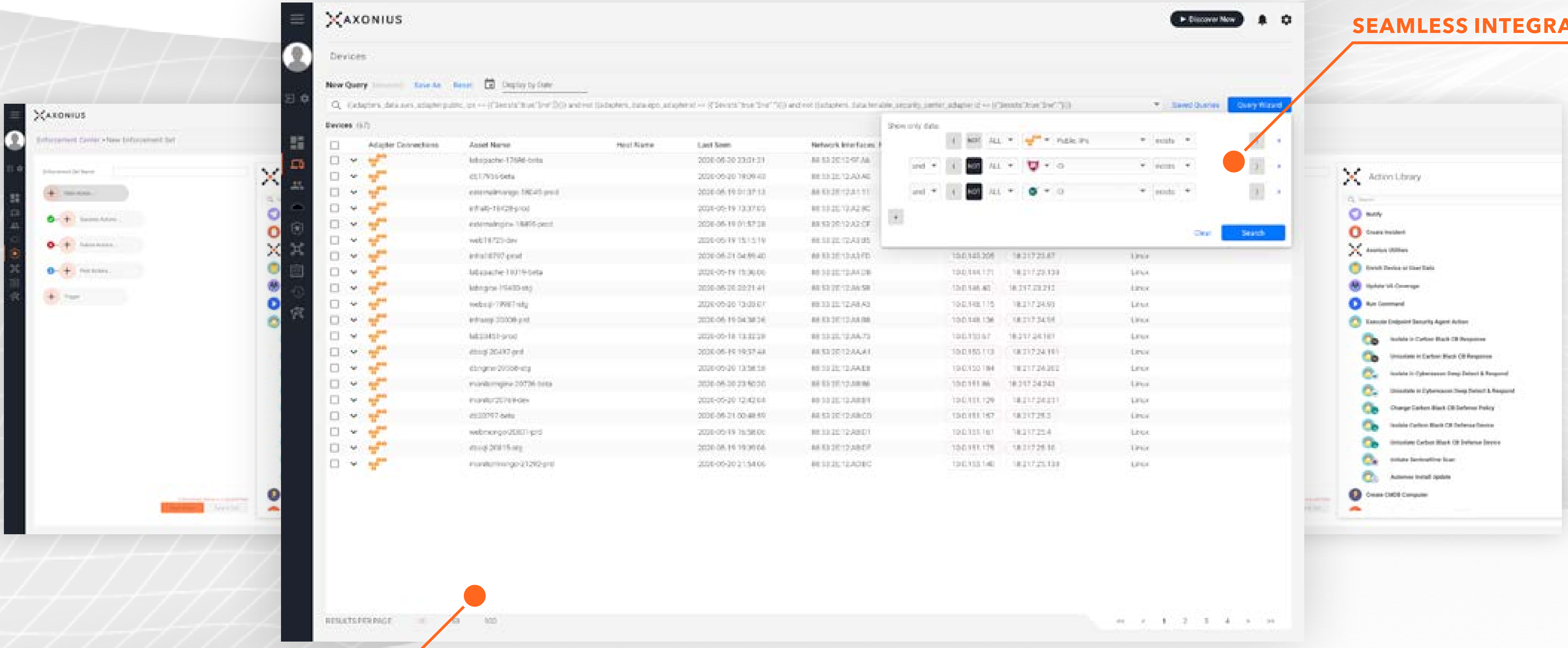
Cybersecurity Asset Management Platform

Axonius is the cybersecurity asset management platform that gives organizations a Comprehensive Asset Inventory. We uncover security coverage gaps, and automatically validate and enforce your security policies.

By seamlessly integrating with over 300 security and IT management solutions, Axonius deploys in hours (not weeks) to improve threat and vulnerability management, security operations, incident response, and overall security posture.



SEAMLESS INTEGRATION

COMPREHENSIVE ASSET INVENTORY

AXONIUS

> **There has never been a tool that does what Axonius does, allowing us to tie everything together using simple queries and then putting compliance on autopilot.**
>
> **– JEFFREY GARDNER**
> SENIOR DIRECTOR OF INFORMATION SECURITY, LANDMARK HEALTH

How it works.

DEPLOY AXONIUS

Axonius is an agentless single virtual appliance and can be deployed either on- premise or in cloud instances.

CONNECT ADAPTERS

Connect to the different solutions you already use with Adapters, pre-built integrations on the Axonius platform.

EXAMINE YOUR ASSETS

Axonius provides a fully unique list of devices and users so you can surface areas of risk and be alerted when policies aren't met.

Key Benefits

REDUCE MEAN TIME TO INVENTORY

Axonius correlates data from all sources to provide an up-to-date inventory of all unique assets. This single source of truth gives security teams a clear, consistent picture of their asset inventory without the need for constant manual audits.

AUTOMATE SECURITY POLICY ENFORCEMENT

The Axonius Security Policy Enforcement Center addresses assets that don't adhere to your security policies. Security enforcement sets can be customized for any condition to notify personnel, enrich data, or remediate incidents automatically.

SEAMLESS DEPLOYMENT AND MANAGEMENT

Axonius is agentless – no endpoint or network agent is needed. Even customers with more than a million devices and more than 50,000 employees still deploy Axonius as a single virtual appliance to get complete visibility into their assets.

Use Cases

ASSET INVENTORY MANAGEMENT

- Continuous discovery and management of all unique assets
- Fully characterized and aggregated data for each asset
- Single view across multicloud and virtual environments

UNMANAGED DEVICE IDENTIFICATION

- Find unmanaged devices, including IoT and connected medical devices
- Identify unauthorized devices on restricted network segments

SECURITY RISK MANAGEMENT

- Find vulnerable devices with missing or malfunctioning agents
- Find exploitable devices missing vulnerability scans and patches
- Identify rogue devices and software

SECURITY POLICY ENFORCEMENT

- Notify the right teams when assets don't meet policies
- Enrich device and user data with third party contextual data sources (i.e. Shodan, Censys, HaveIBeenPwned)
- Remediate machines via endpoint security agents or direct commands

Axonius is the cybersecurity asset management platform that lets IT and Security teams see devices for what they are in order to manage and secure all. **Interested in seeing what Axonius can do for your organization?**

LET'S TALK →

AXONIUS

THE CHALLENGE OF SaaS.

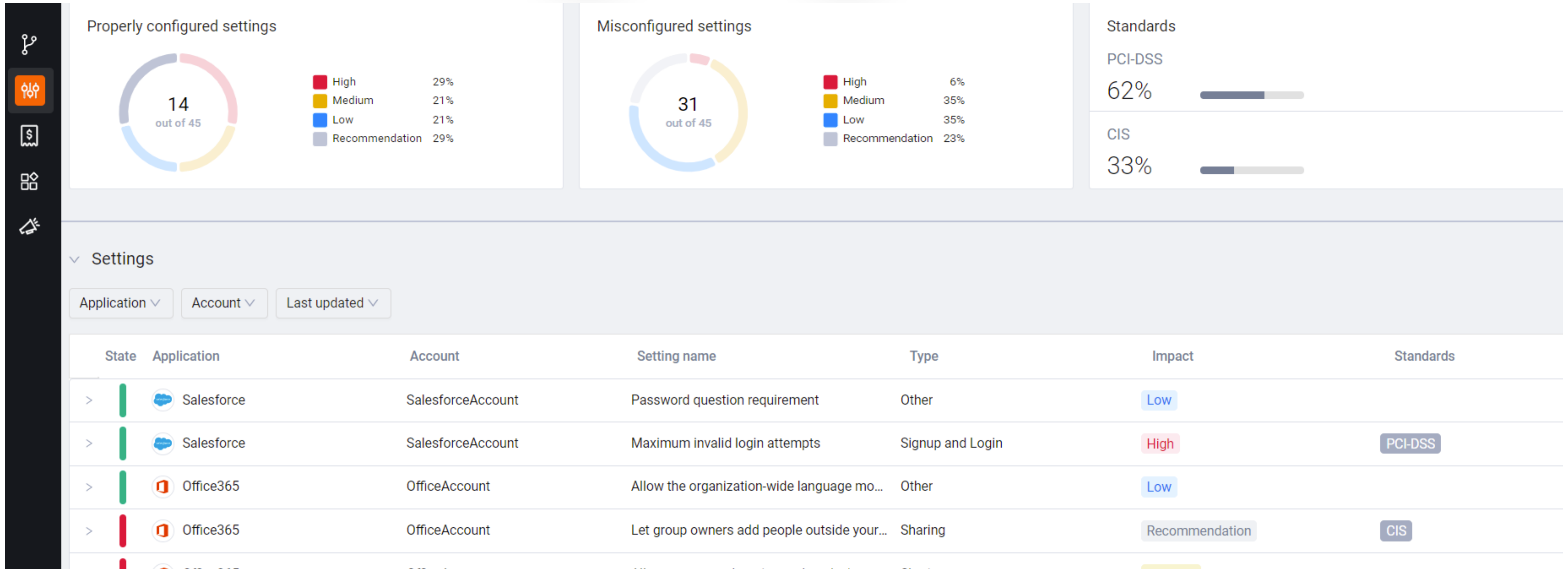
SaaS has benefitted all types of businesses, but the sprawl and interconnectivity of applications has become unwieldy. A typical company may have a CRM that is connected to company collaboration tools, an HR management platform that handles sensitive data and has integrations with many other platforms, and many more.

Compounding this challenge, **97% of SaaS apps are unmanaged** making it very difficult for IT, security, and finance teams to reduce security risk, manage SaaS licenses, and manage costs.

okta
salesforce
box

Axonius SaaS Management

Axonius SaaS Management connects to all layers of the SaaS application stack to reveal actionable insights and provide a comprehensive solution addressing both security and IT needs. Leveraging a rich library of API adapters, Axonius discovers all of your known and unknown SaaS applications, identifies misconfigurations and data security risks, and delivers insights for better IT management and cost optimization.



Properly configured settings

14 out of 45

🟥 High	29%
🟨 Medium	21%
🟦 Low	21%
⬜ Recommendation	29%

Misconfigured settings

31 out of 45

🟥 High	6%
🟨 Medium	35%
🟦 Low	35%
⬜ Recommendation	23%

Standards

PCI-DSS

62%

CIS

33%

Settings

Application ∨ Account ∨ Last updated ∨

State	Application	Account	Setting name	Type	Impact	Standards
🟩	Salesforce	SalesforceAccount	Password question requirement	Other	Low	
🟩	Salesforce	SalesforceAccount	Maximum invalid login attempts	Signup and Login	High	PCI-DSS
🟩	Office365	OfficeAccount	Allow the organization-wide language mo...	Other	Low	
🟥	Office365	OfficeAccount	Let group owners add people outside your...	Sharing	Recommendation	CIS

AXONIUS
SAAS MANAGEMENT

How it works.

CONNECT AND DISCOVER

Discover SaaS apps using pre-built API adapters an addtional discovery tools. Once connected, Axonius aggregates and correlates data to identify unknown and potentially unsanctioned SaaS apps and associated users.

SET POLICIES AND MONITOR DEVIATIONS

Monitor user access, permission levels, data sharing, and more across any SaaS application.

DETECT & AUTOMATE

Get alerted and take action whenever an app falls out of compliance or when new risks are found.

OPTIMIZE LICENSING & UTILIZATION

Leverage expense and utilization data to reduce cost by rightsizing licenses and removing redundant apps.

KEY CAPABILITIES

Security Operations

ASSESS THE LEVEL OF RISK POSED BY SAAS APPS

Understand what type of data is being sent out to other services, and the relative level of risk associated with certain SaaS apps

DISCOVER AND CLOSE SECURITY CONFIGURATION GAPS

Know when SaaS apps in use by your organization have disclosed vulnerabilities or misconfigurations that present security risks

IDENTIFY RISKY SAAS ACCOUNTS

Identify SaaS users that access apps outside of sanctioned SSO and authentication mechanisms.

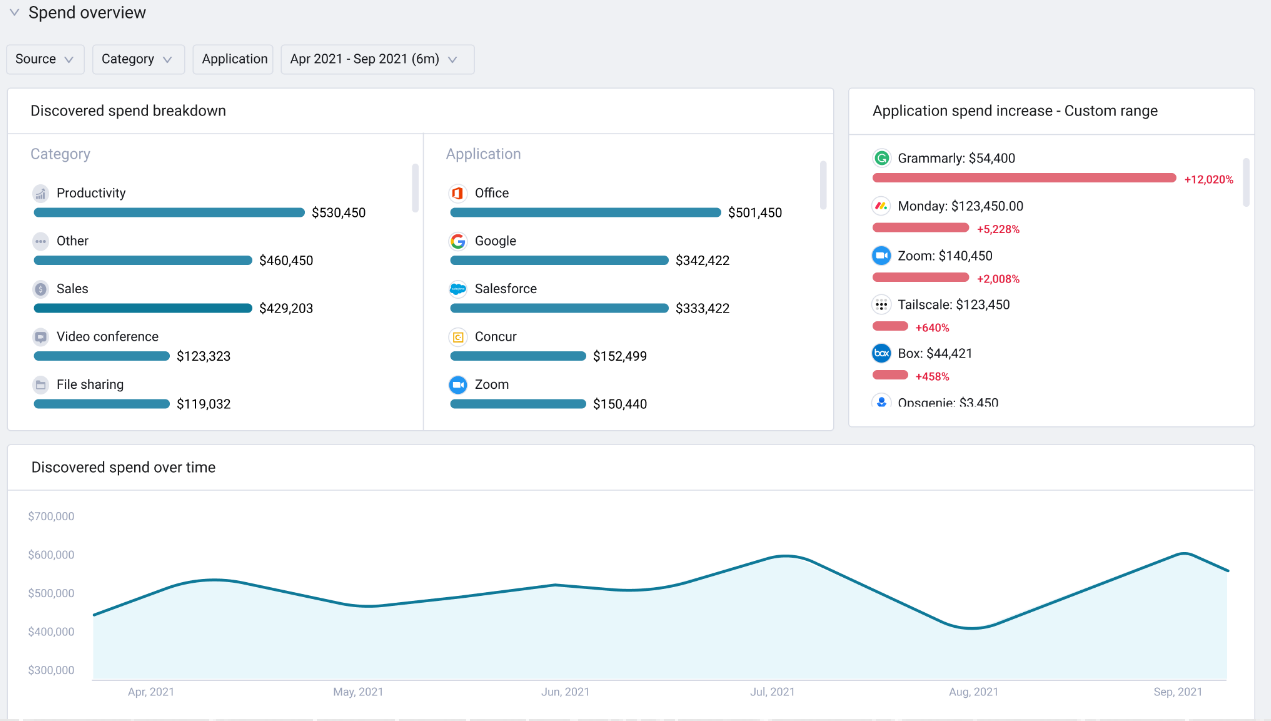
IT Management

DISCOVER AND ADDRESS MODERN DAY SHADOW IT

Identify and manage unsanctioned SaaS apps in use across your organization

CONTROL COSTS & OPTIMIZE SAAS LICENSING

Get an exact count of users with SaaS licenses to inform employee onboarding and offboarding, and reduce spend on underutilized and redundant SaaS apps



Spend overview

Source | Category | Application | Apr 2021 - Sep 2021 (6m)

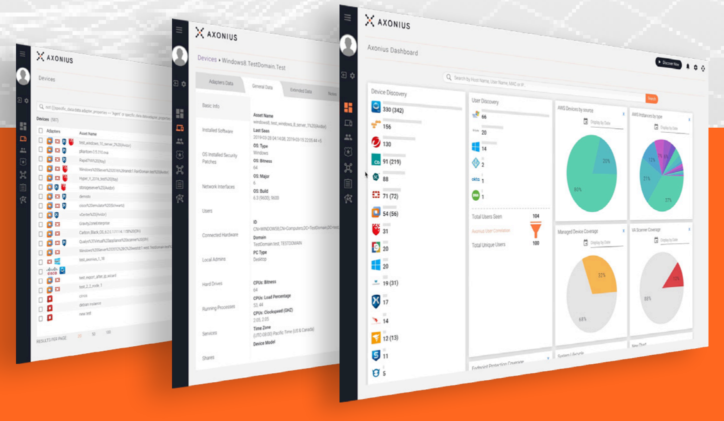
Discovered spend breakdown

Category		Application	
Productivity	$530,450	Office	$501,450
Other	$460,450	Google	$342,422
Sales	$429,203	Salesforce	$333,422
Video conference	$123,323	Concur	$152,499
File sharing	$119,032	Zoom	$150,440

Application spend increase - Custom range

Grammarly: $54,400	+12,020%
Monday: $123,450.00	+5,228%
Zoom: $140,450	+2,008%
Tailscale: $123,450	+640%
Box: $44,421	+458%
Opsgenie: $3,450	

Discovered spend over time



Axonius lets IT and security teams control complexity across devices, users, cloud assets, and applications. **Interested in seeing what Axonius can do for your organization?**

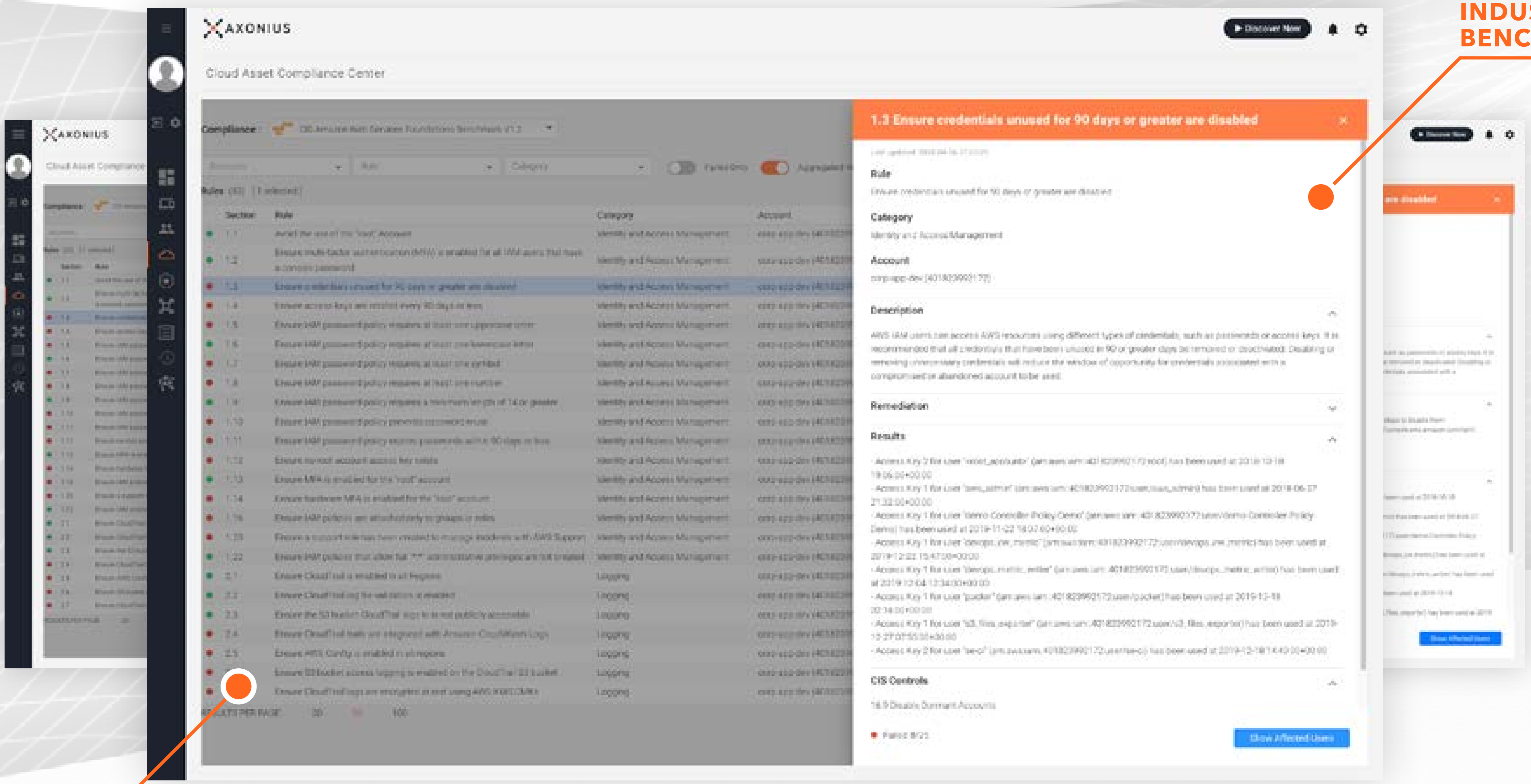
LET'S TALK →

docs.axonius.com | info@axonius.com

Axonius Cloud Asset Compliance

Axonius Cloud Asset Compliance continuously evaluates whether cloud assets adhere to or deviate from industry benchmarks and frameworks.

This add-on to the Axonius Cybersecurity Asset Management Platform strengthens cloud security posture by leveraging data from connected cloud IAAS provider accounts to automatically identify misconfigurations and policy lapses that introduce risk.



Cloud Asset Compliance Center

Compliance: CIS Amazon Web Services Foundations Benchmark V1.2

Failed Only Aggregated

Rules (43) (1 selected)

Section	Rule	Category	Account
1.1	Avoid the use of the "root" Account	Identity and Access Management	corp-app-dev (40182...
1.2	Ensure multi-factor authentication (MFA) is enabled for all IAM users that have a console password	Identity and Access Management	corp-app-dev (40182...
1.3	Ensure credentials unused for 90 days or greater are disabled	Identity and Access Management	corp-app-dev (40182...
1.4	Ensure access keys are rotated every 90 days or less	Identity and Access Management	corp-app-dev (40182...
1.5	Ensure IAM password policy requires at least one uppercase letter	Identity and Access Management	corp-app-dev (40182...
1.6	Ensure IAM password policy requires at least one lowercase letter	Identity and Access Management	corp-app-dev (40182...
1.7	Ensure IAM password policy requires at least one symbol	Identity and Access Management	corp-app-dev (40182...
1.8	Ensure IAM password policy requires at least one number	Identity and Access Management	corp-app-dev (40182...
1.9	Ensure IAM password policy requires a minimum length of 14 or greater	Identity and Access Management	corp-app-dev (40182...
1.10	Ensure IAM password policy prevents password reuse	Identity and Access Management	corp-app-dev (40182...
1.11	Ensure IAM password policy expires passwords within 90 days or less	Identity and Access Management	corp-app-dev (40182...
1.12	Ensure no root account access key exists	Identity and Access Management	corp-app-dev (40182...
1.13	Ensure MFA is enabled for the "root" account	Identity and Access Management	corp-app-dev (40182...
1.14	Ensure hardware MFA is enabled for the "root" account	Identity and Access Management	corp-app-dev (40182...
1.16	Ensure IAM policies are attached only to groups or roles	Identity and Access Management	corp-app-dev (40182...
1.20	Ensure a support role has been created to manage incidents with AWS Support	Identity and Access Management	corp-app-dev (40182...
1.22	Ensure IAM policies that allow full "*:*" administrative privileges are not created	Identity and Access Management	corp-app-dev (40182...
2.1	Ensure CloudTrail is enabled in all Regions	Logging	corp-app-dev (40182...
2.2	Ensure CloudTrail log file validation is enabled	Logging	corp-app-dev (40182...
2.3	Ensure the S3 bucket CloudTrail logs to is not publicly accessible	Logging	corp-app-dev (40182...
2.4	Ensure CloudTrail trails are integrated with Amazon CloudWatch Logs	Logging	corp-app-dev (40182...
2.5	Ensure AWS Config is enabled in all regions	Logging	corp-app-dev (40182...
2.6	Ensure S3 bucket access logging is enabled on the CloudTrail S3 bucket	Logging	corp-app-dev (40182...
2.7	Ensure CloudTrail logs are encrypted at rest using AWS KMS CMKs	Logging	corp-app-dev (40182...

RESULTS PER PAGE: 20 50 100

1.3 Ensure credentials unused for 90 days or greater are disabled

Rule
Ensure credentials unused for 90 days or greater are disabled

Category
Identity and Access Management

Account
corp-app-dev (401823992172)

Description
AWS IAM users can access AWS resources using different types of credentials, such as passwords or access keys. It is recommended that all credentials that have been unused in 90 or greater days be removed or deactivated. Disabling or removing unnecessary credentials will reduce the window of opportunity for credentials associated with a compromised or abandoned account to be used.

Remediation

Results
- Access Key 2 for user "root_accounts" (arn:aws:iam::401823992172:root) has been used at 2018-12-18 19:06:00+00:00
- Access Key 1 for user "aws_admin" (arn:aws:iam::401823992172:user/aws_admin) has been used at 2018-06-27 21:32:00+00:00
- Access Key 1 for user "Demo Controller Policy Demo" (arn:aws:iam::401823992172:user/Demo Controller Policy Demo) has been used at 2019-11-22 18:07:00+00:00
- Access Key 1 for user "devops_cw_metric" (arn:aws:iam::401823992172:user/devops_cw_metric) has been used at 2019-12-22 15:47:00+00:00
- Access Key 1 for user "devops_metric_writer" (arn:aws:iam::401823992172:user/devops_metric_writer) has been used at 2019-12-04 12:34:00+00:00
- Access Key 1 for user "packer" (arn:aws:iam::401823992172:user/packer) has been used at 2019-12-18 20:14:00+00:00
- Access Key 1 for user "s3_files_exporter" (arn:aws:iam::401823992172:user/s3_files_exporter) has been used at 2019-12-27 07:55:00+00:00
- Access Key 2 for user "se-ci" (arn:aws:iam::401823992172:user/se-ci) has been used at 2019-12-18 14:42:00+00:00

CIS Controls
16.9 Disable Dormant Accounts

● Failed 8/25

Show Affected Users

ADHERE TO INDUSTRY BENCHMARKS

IDENTIFY POLICY LAPSES

AXONIUS

AXONIUS CLOUD ASSET COMPLIANCE

How it works.

CONNECT CLOUD ADAPTERS

Cloud Asset Compliance simply leverages data from cloud adapters that have already been connected in the core platform.

GET RESULTS

Compliance mapping results are generated automatically and show affected users and assets, with detailed remediation instructions for each failed rule.

FILTER, REPORT, AND TAKE ACTION

Filter compliance results for specific accounts and rules, share results via email, and follow remediation instructions within Axonius to fix misconfigurations that have failed a rule.

Key Benefits

AUTOMATE CLOUD COMPLIANCE REPORTING

Understand how all of your cloud instances adhere to or deviate from industry benchmarks, like the CIS Cloud Benchmarks.

STREAMLINE REPORTING FOR MULTI-CLOUD ENVIRONMENTS

Gain a unified view into all cloud assets and report compliance metrics for any major cloud provider.

STRENGTHEN CLOUD SECURITY POSTURE

Identify all cloud instances and users potentially at risk, create triggered actions, and reference remediation instructions to fix misconfiguration issues any time a benchmark rule is failed.

Supported Frameworks

Axonius is an official CIS product vendor and has been awarded CIS Security Software Certification for the following CIS Benchmarks:

CIS AMAZON WEB SERVICES FOUNDATIONS BENCHMARK V1.2.0

Axonius checks whether AWS accounts adhere to or deviate from scored rules in the in the CIS Amazon Web Services Foundations Benchmark v1.2.0.

Categories include: Identity and Access Management, Logging, Monitoring, and Networking rules.

CIS MICROSOFT AZURE FOUNDATIONS BENCHMARK V1.1.0

Axonius continuously evaluates whether Microsoft Azure accounts adhere to or deviate from scored rules in the in the CIS Microsoft Azure Foundations Benchmark v1.1.0.

Categories include: Identity and Access Management, Security Center, Storage Accounts, Database Services, Configuring Log Profile, Monitoring Activity Log Alerts, Networking, Virtual Machines, App Service, and Other Security Considerations.

CIS ORACLE CLOUD INFRASTRUCTURE FOUNDATIONS BENCHMARK V1.0.0

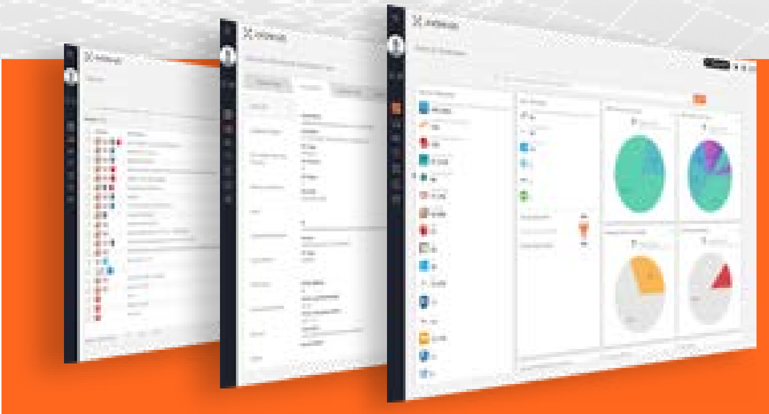
Axonius checks whether Oracle Cloud Infrastructure adheres to or deviates from scored rules in the CIS Oracle Cloud Infrastructure Foundations Benchmark v1.0.0.

Categories include: Identity and Access Management, Logging and Monitoring, and Networking rules.

CIS GOOGLE CLOUD PLATFORM FOUNDATIONS BENCHMARK V1.1.0

Axonius checks whether Google Cloud Platform adheres to or deviates from scored rules in the in the CIS Google Cloud Platform Foundation Benchmark version 1.1.0.

Categories include: Identity and Access Management, Networking rules, Virtual Machines, and Cloud SQL Database Services.



Axonius is the cybersecurity asset management platform that lets IT and Security teams see devices for what they are in order to manage and secure all. **Interested in seeing what Axonius can do for your organization?**

LET'S TALK →

docs.axonius.com | info@axonius.com