Building Custom Views

AiVRIC Analytics & Compliance

Purpose

AiVRIC's **custom views** allow users to tailor analytics, dashboards, and compliance results to specific cloud providers, regions, scans, and risk scopes. This ensures teams can focus on **relevant data** without losing visibility into the broader environment.

Custom views are available across **Overview**, **Compliance**, and **Findings** workflows.

Custom Views in the Overview Dashboard

Default View Behavior

By default, the **Overview** dashboard displays:

- **All connected cloud providers**
- All active resources
- All findings (unless explicitly muted)

This provides a **global posture view** across AWS, Azure, GCP, Kubernetes, GitHub, and other supported providers.

Filtering by Cloud Provider

Users can narrow the Overview dashboard to **a single cloud provider at a time**.

How it works:

1. Navigate to **Analytics → Overview**
2. Open the **Provider** dropdown at the top of the page
3. Select a specific provider (e.g., Amazon Web Services)

4. The dashboard refreshes to show:
    - Only resources associated with the selected provider
    - Provider-specific failed findings by severity
    - Provider-specific passing vs. failing checks
    - Updated totals reflecting only that provider

This enables focused analysis such as:

- AWS-only security posture reviews
- Azure-only remediation planning
- Kubernetes or GitHub risk isolation

Mutelists & View Customization

AiVRIC supports **Mutelists** to suppress known or accepted findings.

Key behaviors:

- Mutelists are applied **globally** to dashboards
- Muted findings are hidden when:
    - “Exclude muted findings” is enabled
- Mutelist changes take effect on the **next scan**

Use mutelists to:

- Reduce noise from accepted risks
- Align dashboards with organizational risk tolerance
- Customize views for executive vs. engineering audiences

Custom Views in the Compliance Dashboard

The **Compliance** dashboard supports additional dimensions of filtering beyond provider selection.

Filtering by Compliance Scan

AiVRIC allows users to review results from:

- The most recent scan
- Any prior completed scan

Use cases:

- Compare compliance posture over time
- Validate remediation progress
- Support audit lookbacks or evidence reviews

How it works:

1. Navigate to **Analytics → Compliance**
2. Use the scan selector dropdown
3. Choose a completed scan (date and time displayed)
4. The compliance dashboard updates to reflect:
    - The selected scan's results
    - Framework scores at that point in time
    - Passing vs. failing requirements from that scan

Filtering by Region

Compliance results can also be filtered by **cloud region**.

How it works:

1. Within the Compliance dashboard, open **Filters**
2. Select one or more regions (e.g., us-east-1, eu-west-1)
3. Compliance scores and requirement counts update dynamically

This enables:

- Region-specific compliance assessments
- Regulatory or data residency validation
- Narrowed audit scope reviews

Combining Scan + Region Filters

Filters can be **combined**, allowing users to answer questions such as:

- “What was our AWS CIS compliance in us-east-1 last quarter?”
- “How did remediation affect our FedRAMP posture since the previous scan?”
- “Are specific regions lagging behind in compliance maturity?”

Best Practices for Building Custom Views

For Security Teams

- Filter by provider to isolate attack surface
- Exclude muted findings to focus remediation work
- Use historical scans to validate improvements

For Compliance Teams

- Filter by framework and region for audit prep
- Use prior scans to demonstrate continuous compliance
- Narrow scope to reduce noise during assessments

For Executives & Leadership

- Use provider-level views for high-level risk summaries
- Rely on muted findings to ensure dashboards reflect accepted risk posture
- Review trends using older scans for strategic decisions

Summary

AiVRIC's custom views enable users to:

- Switch seamlessly between global and provider-specific perspectives
- Focus on the right data for the right audience
- Reduce noise while maintaining visibility
- Support compliance, audit, and executive reporting workflows

By combining **provider selection, mutelists, scan selection, and region filters**, teams can create **precise, repeatable views** that align with operational, compliance, and leadership needs.