Reporting Dashboard

Reporting Dashboard

Reporting dashboard, which is designed for Executives, Network Administrators, and Security Analysts, provides visual representations of critical workflow status, troubleshooting capabilities, and report creation functionalities. On the navigation pane, click **Reporting> Reporting Dashboard** to access the dashboard.

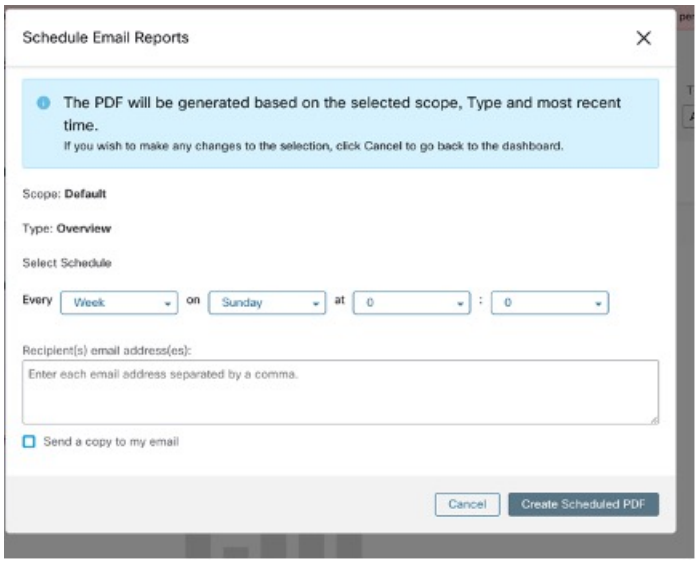
The sections below provide an overview of the reports, how to schedule and email the reports.

Schedule Email Reports

To generate a report, choose from either of the options:

- **Download**: After you generate a report, you can download and save a copy of the report for future reference.
- **Email**: If you choose the option to email reports, an email will be triggered to recipients with the attached report.
- **Schedule**: You have two options to choose from to schedule a report.
  - Daily
  - Weekly

    To schedule a report, enter the schedule details to trigger the report. Select Weekly or Daily, enetr the day and time, and the email addresses of the recipients. Click **Create Scheduled PDF** to save the details.



Note If the report scheduling fails, check the schedule for any incorrect email address or incorrectly entered date and time.

To access the report schedules that were generated earlier, choose **Generated Reports > Schedules**. If the report scheduling fails, check the schedule for any incorrect email address or incorrect date, time.

Note The maximum number of schedules that you can store in the scheduling dashboard is five.

Overview

The overview section provides real-time insights into the network flow information, security policies, system performances, and security threats. It enables security analysts and network administrators to make informed decisions and take measures to protect their data resources.

Segmentation Summary

Workspaces are the building blocks to discover, apply, and manage policies and enforcement within the cluster. You can define segmentation memberships by selecting the appropriate scope.

Segmentation summary captures the configuration details for every workspace, all policy-related activities, such as defining, analyzing, and enforcing policies for a particular scope in the workspace or workspaces that are associated with that scope.

The graph displays a summary of the various policies that are associated with the workspaces.

Figure 1: Segmentation Summary

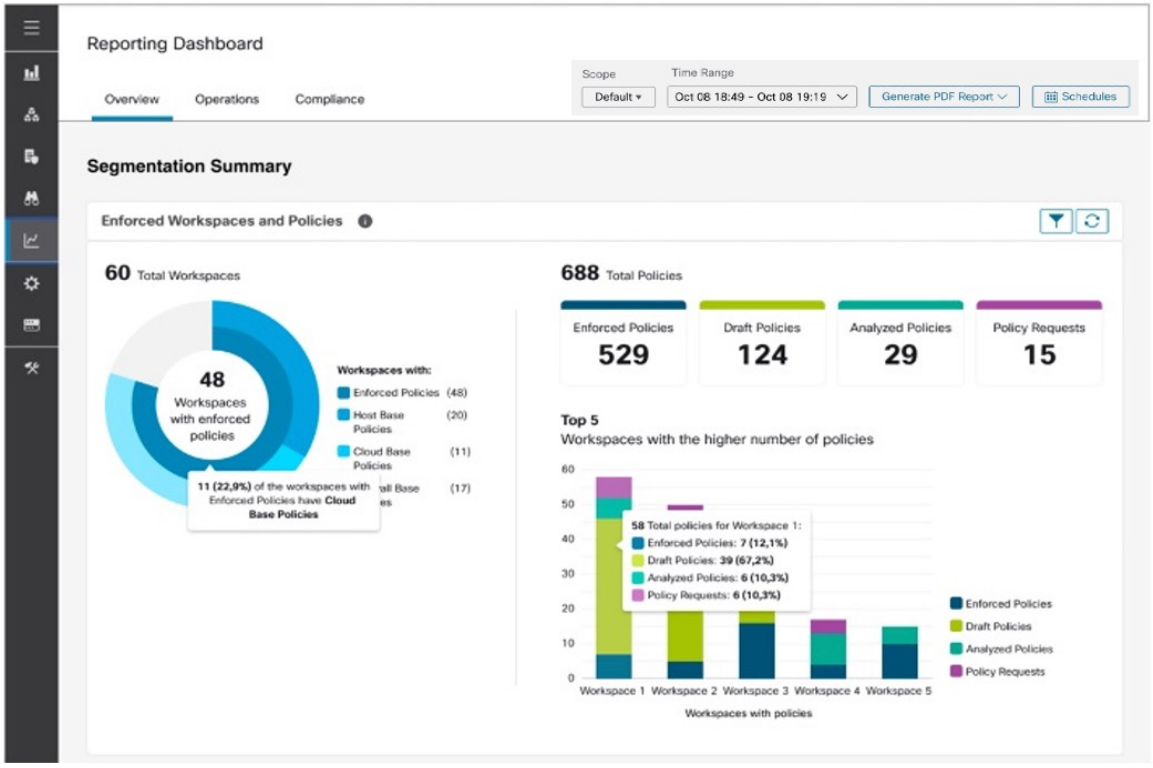
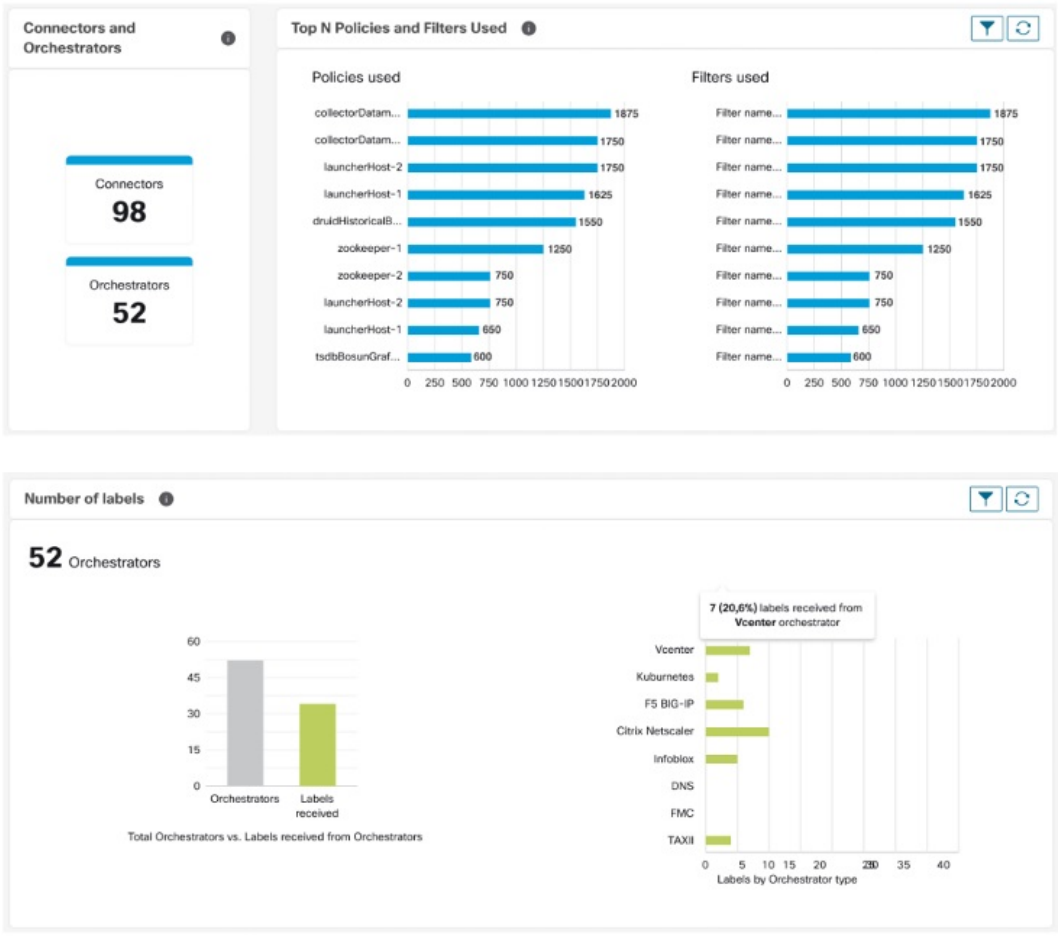


Figure 2: Connectors and Orchestrators

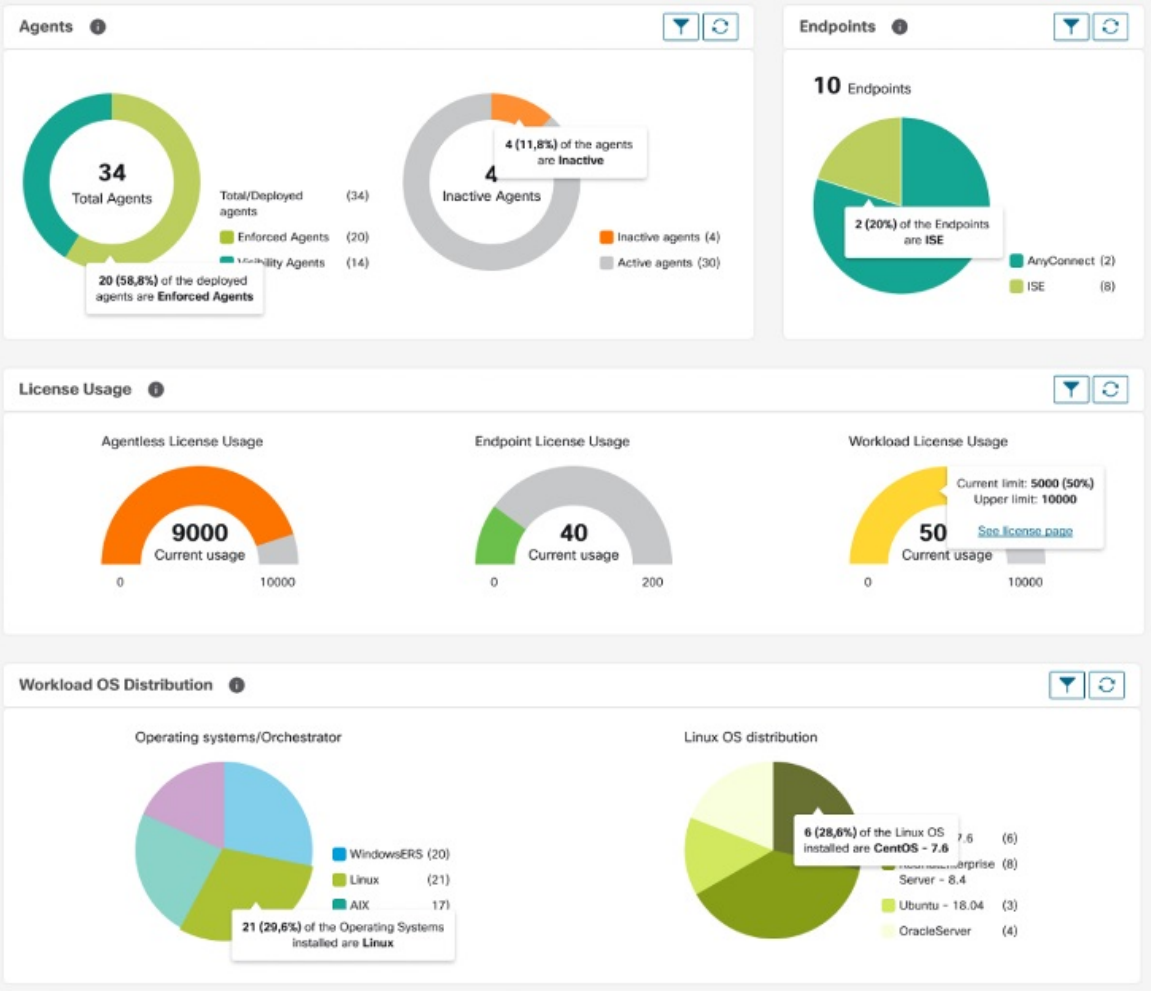


Workload Summary

The Workload summary provides the following details about the agents that are deployed on one or more servers and endpoints in the infrastructure:

- Agents monitor and collect network flow information.
- Agents enforce security policies with firewall rules on the installed hosts.
- Agents communicate the status of the workload.
- Agents receive updates on the security policies.

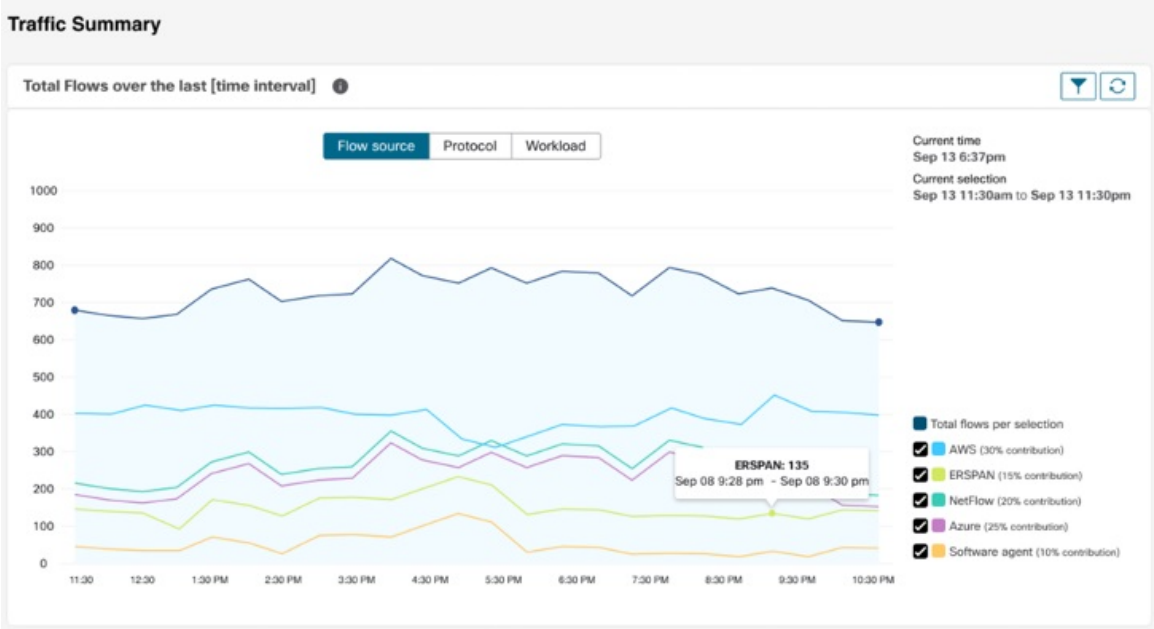
Figure 3: Workload Summary



Traffic Summary

Traffic summary captures the flow observations of each flow. Each observation in the flow source tracks the number of packets, bytes, and other metrics for the flows.

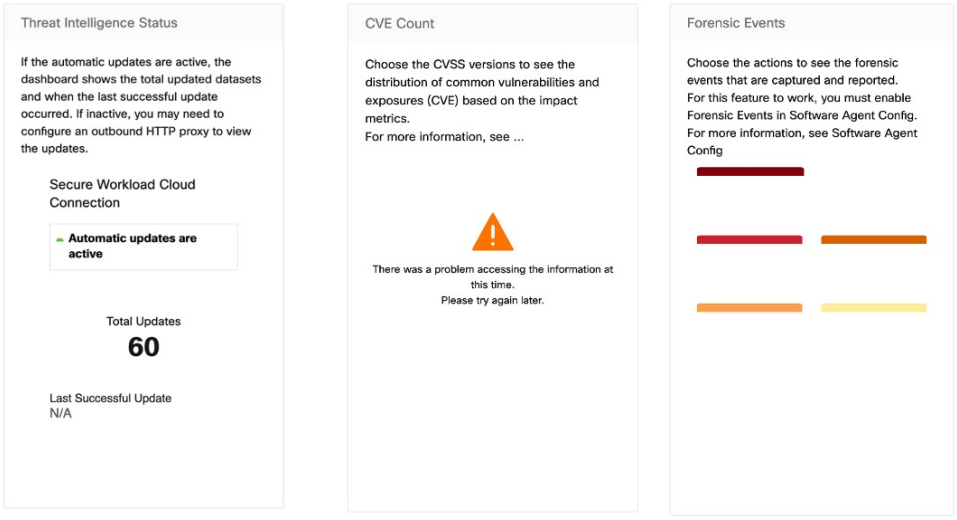
Figure 4: Traffic Summary



Security Summary

Security Summary provides Threat Intelligence Status (last time when the threat intelligence status updates were received are shown), count of CVEs, and distribution of Forensic events.

Figure 5: Security Summary

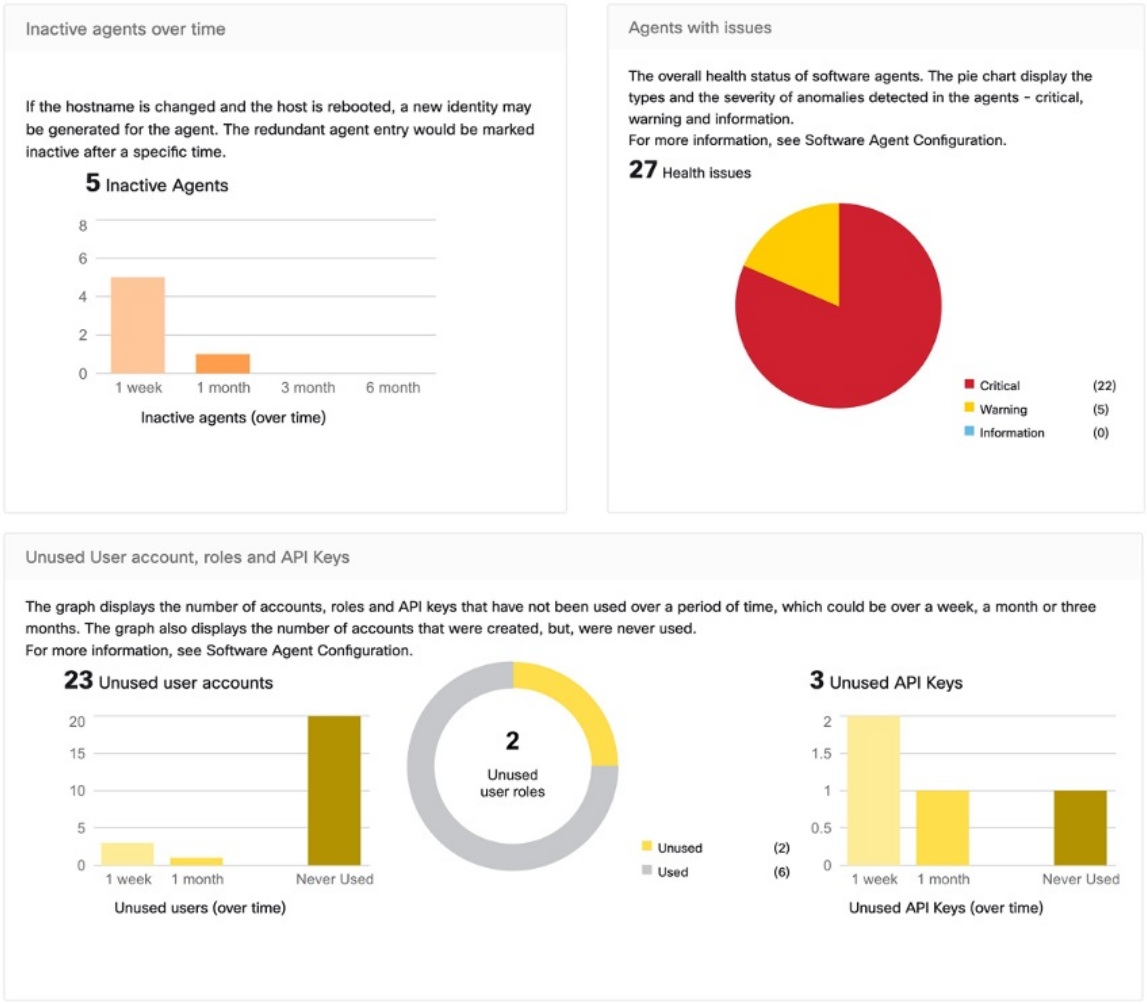


Operation

Workload Summary

Workload summary provides a view of the total agents that are deployed on one or more servers and endpoints in the network. The agents monitor and collect network flow information, enforce security policies with firewall rules on the installed hosts, communicate the status of the workload, and receive updates on the security policies.

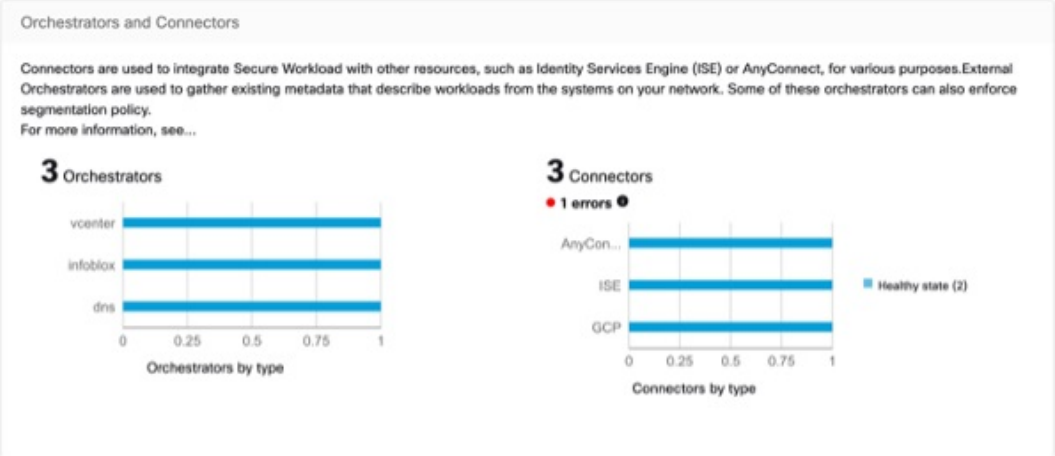
Figure 6: Workload Summary



Telemetry Summary

Many connectors that are deployed on the virtual appliance collects telemetry from various points in the network, these connectors must listen on specific ports on the appliance. Connectors can ingest flow logs if you have setup flow logs for your specific security groups. You can also use the telemetry data for visualization and segmentation policy generation.

Figure 7: Telemetry Summary



Cluster Summary

Site admins can access the cluster status page, but the actions can be carried out only by Customer Support users. It shows the status of all the physical servers in Cisco Secure Workload rack.

The processing and retention time for clusters refer to the duration for which data is stored and processed within a cluster. The specific processing and retention times depend on the requirements of the workload and the policies of the organization.

It is important to consider the processing time requirements when configuring the cluster, as this can impact the storage capacity and processing power that is needed to meet the workload's needs.

Retention time refers to the length of time that data is retained within a cluster. For some workloads, data may need to be retained for regulatory or compliance purposes, while for others it may be deleted once it has been processed. It is important to establish retention policies for the workload to ensure that data is retained for the appropriate length of time and then deleted securely to prevent unauthorized access.

Figure 8: Cluster Summary

Segmentation Summary

Segmentation or Application Workspaces are the building blocks for discovering, applying, and managing policy and enforcement within the cluster. The segmentation summary captures the configuration details for each of the Application Workspaces implemented, the no. of workspaces with and without enforcement, policies that have been enabled or disabled, workspaces that have up-to-date policies or out of sync, and with or without draft policies.

Figure 9: Segmentation Summary

Compliance

Workload Summary

Workload Summary provides a view of the total agents that are deployed on one or more servers and endpoints in the infrastructure. The agents monitor and collect network flow information, enforce security policies with firewall rules on the installed hosts, communicate the status of the workload and receive updates on the security policies.

Figure 10:

Security Summary

Configure your forensic events; once configured, all tactics are displayed without any rules under them, with a count of 0. Select one or more forensic rules to make the selection at the tactic level. Selecting a tactic selects

all the rules under it. Default MITRE ATT&CK rules are provided to alert techniques from the MITRE ATT&CK Framework.

Figure 11:

Workspaces with CVEs

Based on the scope that is selected and the scoring system (v2 or v3), the CVE count highlights the vulnerabilities (sorted by the scores) on workloads in the selected scopes. See the distribution of workspaces and the workloads with the highest number of critical CVEs.

Software packages on a workload could potentially be associated with known vulnerabilities (CVE). Common Vulnerability Scoring System (CVSS) is used for assessing the impact of a CVE. CVE can have CVSS v2 and CVSS v3 score. To compute the vulnerability score, consider CVSS v3 if it is available, else CVSS v2 is considered.

Vulnerability score for a workload is derived from scores of vulnerable software that is detected on that workload. The Workload Vulnerability Score is calculated based on the CVSS scores, the vendor data, and the security research team may adjust when the data is missing or inaccurate. Higher the severity of the most severe vulnerability, lower is the score.

Figure 12: