Cisco Secure Workload Release Notes, Release 3.7.1.22

First Published: 2022-12-21

Last Modified: 2023-07-02

Introduction

The Cisco Secure Workload platform, formerly branded as Cisco Tetration, is designed to provide comprehensive workload security by establishing a micro perimeter around every workload across your on-premises and multi-cloud environment using firewalling and segmentation, compliance and vulnerability tracking, behavior-based anomaly detection, and workload isolation. The platform uses an advanced analytics and algorithmic approach to offer these capabilities.

This solution supports the following capabilities:

- Automatically generated micro-segmentation policies resulting from comprehensive analysis of application communication patterns and dependencies
- Dynamic label-based policy definition with a hierarchical policy model to deliver comprehensive controls across multiple user groups with role-based access control
- Consistent policy enforcement at scale through distributed control of native operating system firewalls and infrastructure elements like ADCs (Application Delivery Controllers) and physical or virtual firewalls
- Near real-time compliance monitoring of all communications to identify and alert against policy violation or potential compromise
- Workload behavior baselining and proactive anomaly detection
- Common vulnerability detection with dynamic mitigation and threat-based workload isolation

To support the analysis and various use cases within the Cisco Secure Workload platform, consistent telemetry (flow data) is required from across the environment. Cisco Secure Workload collects rich telemetry using software agents and other methods to support both existing and new installations in data center infrastructures.

This release supports the following telemetry sources:

- Secure Workload agents installed on virtual machine and bare-metal servers
- DaemonSets running on container host operating systems
- ERSPAN connectors that can generate Cisco Secure Workload telemetry from mirrored packets
- Telemetry ingestion from Application Delivery Controllers (ADCs) – F5 and Citrix
- NetFlow connectors that can generate Cisco Secure Workload telemetry based on NetFlow v9 or IPFIX records
- ASA connector for collection of NetFlow Secure Event Logging (NSEL) telemetry

- AWS connector for flow telemetry data generated using VPC flow log configurations
- Azure connector for flow telemetry data generated using NSG flow log configurations

In addition, this release also supports ingesting endpoint device posture, context and telemetry through integrations with-

- Cisco AnyConnect installed on endpoint devices such as laptops, desktops, and smartphones
- Cisco Identity Services Engine (ISE)

Secure Workload agents also act as a policy enforcement point for application segmentation. Using this approach, the Cisco Secure Workload platform enables consistent micro-segmentation across public, private, and on-premises deployments. Agents enforce policy using native operating system capabilities, thereby eliminating the need for the agent to be in the data path and providing a fail-safe option. Additional product documentation is listed in the Related Documentation section.

New and Changed Information

This section lists the new and enhanced features, and known behaviors in this release.

Compatibility Information

- Agent packages for Windows 8.1 have been removed as OS is no longer supported.

For detailed compatibility information, please refer to Platform Information on Cisco.com.

Known Behaviors

See the Cisco Secure Workload major release 3.7.1.5 release notes.

Important Notes

This section lists some important notes for the Cisco Secure Workload software:

- You must use the Google Chrome browser version 90.0.0 or later to access the web-based user interface.
- After setting up your DNS, browse to the URL of your Cisco Secure Workload cluster: https://<cluster.domain>
- When using the commission / decommission feature for Cisco Secure Workload virtual appliance environments, please observe the following usage guidelines:
  - This feature is meant to be used with the assistance of TAC and can cause unrecoverable damage if used incorrectly. No two VMs should ever be decommissioned at the same time, without explicit approval from TAC. The following combinations of VMs must never be decommissioned concurrently:
    - More than one orchestrator
    - More than one datanode
    - More than one namenode (namenode or secondaryNamenode)
    - More than one resourceManager
    - More than one happobat

- More than one mongodb (mongodb or mongoArbiter)
- Only one decommission/commission process can be executed at a time. Do not overlap the decommission/commission of different VMs at the same time.

Note Always contact TAC prior to using the esx_commission snapshot endpoint.

New Software, New Hardware and Deprecated Features

New Software Features

There are no new software features in this release.

New Hardware Features

There are no new hardware features in this release.

Deprecated Features

There are no deprecated features in this release.

Enhancements

- Software Agents now support Oracle Linux 9 on x86_64 architecture.
- Software Agents now support AlmaLinux 9 on x86_64architecture.
- Software Agents now support Rocky Linux 9 on x86_64architecture.
- Software Agents now support MSWindowsPro10forWorkstation and MSWindowsPro11forWorkstation
- --golden_image flag has been added for installer script-based Linux and AIX installations.
- Software Agent uninstall operation will now remove from disk all installation, runtime and log files and directories automatically.
- User can now instruct the Software Agent on Windows hosts to not program the *port scan prevention* filters when enforcement mode is WFP, by modifying the *enforcer_config* file.
- User can now directly download the secure connector RPM and generate token from the new Secure Connector page.

Changes in Behavior

There are no behavior changes in this release.

Verified Scalability Limits

The following tables provide the scalability limits for Cisco Secure Workload (39-RU), Cisco Secure Workload M (8-RU), and Cisco Secure Workload Cloud:

Table 1: Scalability Limits for Cisco Secure Workload (39-RU)

Configurable Option	Scale
Number of workloads	Up to 25,000 (VM or bare-metal). Up to 50,000 (2x) when all the sensors are in conversation mode.
Flow features per second	Up to 2 million.

Table 2: Scalability Limits for Cisco Secure Workload M (8-RU)

Configurable Option	Scale
Number of workloads	Up to 5,000 (VM or bare-metal). Up to 10,000 (2x) when all the sensors are in conversation mode.
Flow features per second	Up to 500,000.

Table 3: Scalability Limits for Cisco Secure Workload Virtual (VMWare ESXi)

Configurable Option	Scale
Number of workloads	Up to 1,000 (VM or bare-metal).
Flow features per second	Up to 70,000.

Note Supported scale is based on whichever parameter reaches the limit first.

Resolved and Open Bugs

The resolved and open bugs for this release are accessible through the Cisco Bug Search Tool. This web-based tool provides you with access to the Cisco bug tracking system, which maintains information about issues and vulnerabilities in this product and other Cisco hardware and software products.

Note You must have a Cisco.com account to log in and access the Cisco Bug Search Tool. If you do not have one, you can register for an account.

For more information about the Cisco Bug Search Tool, see the Bug Search Tool Help & FAQ.

Resolved Issues

The following table lists the resolved issues in this release. Click the Bug ID to access Cisco's Bug Search Tool to see additional information about that bug.

Identifier	Headline
CSCwc79283	Agent on RHEL hosts would repeatedly appear in Agent Restarted anomaly
CSCwf78123	[Linux] Continuous Policy deviation/Correction on newer platforms when iptables-legacy present.
CSCwc47484	Agent List Not Listed Correctly in Software Agents Agent List Page
CSCwc42706	Internal error in listing impacted Wrokloads when enabling enforcement.
CSCvz98522	Enforcement Compliance Alerts are not possible in a Federation
CSCwd07794	POST API to update the tags is not generating log entry in the change logs
CSCwd85126	On AIX lpars agent has a last check-in time but enforcement registration failed.
CSCwd00870	Netscaler external orchestrator Rest API failure when netscaler service group contains a space
CSCwb21189	Consumer and Provider Ports Mismatch
CSCwd24158	Iptables rules conflict between CSW rules and Openshift rules
CSCwc98940	Need vCenter external orchestrator snapshot retrieve status and timestamp for last known good attempt
CSCwd65352	Duplicate Windows agents reported post 3.7 cluster upgrade
CSCwb77220	Cannot view or download all conversations from ADM
CSCwc31985	Error decoding netflow datasets received from ACI with EOF errors
CSCwd60363	Agent will consume CPU beyond configured limits during connection issues to backend WSS service
CSCwc68679	Disabling the Forensic feature does not stop logging events into audit logs
CSCwc72280	Data Not Rendering in Tetration UI if User is Using IP Virtualization to Obtain Network Information
CSCwd14928	Inventory filter Query based upon the Package info breaks out the Inventory Filter Page.
CSCwd00625	Labels associated to a host IP will be replicated to all other IPs reported by this host
CSCwc31977	Constant errors in decoding netflow packets from Netflow Connector.
CSCwd28349	Windows: Agent registration fails when workload has only IPV6 addresses
CSCwd60335	Linux/AIX agents report hostname in FQDN on 3.7 when available
CSCwb80743	UI User Feedback Message Needed when Policy Compression Used

Open Issues

The following table lists the open issues in this release. Click an ID to access Cisco's Bug Search Tool to see additional information about that bug.

Identifier	Headline
CSCwd67224	AIX 7.x once enforcement is enabled, agent not able to connect to CSW Cluster due to fragmentation
CSCwf78123	[Linux] Continuous Policy deviation/Correction on newer platforms when iptables-legacy present.
CSCwd60340	Agent Installer Script Downloaded From 3.6 Release Will Not Download Sensor from 3.7 Release
CSCwb39541	Change error message on Investigate Traffic queries that are timing out.
CSCwb91717	Data for SW Status Upgrade chart for software agents in pending status is missing.
CSCwb80213	vNIC is hung up on a baremetal server (eNIC version on BM should be upgraded)
CSCwc63711	Missing permissions for Azure segmentation
CSCwd93604	Druid segment load queue could go high on 3.7
CSCwb42177	Live and Enforcement policy analysis - hover over the table for scopes column and text chopped off

Related Documentation

Document	Description
Cisco Secure Workload Cluster Deployment Guide	Describes the physical configuration, site preparation, and cabling of a single- and dual-rack installation for Cisco Secure Workload (39-RU) platform and Cisco Secure Workload M (8-RU). Cisco Tetration (Secure Workload) M5 Cluster Hardware Deployment Guide
Cisco Secure Workload Virtual Deployment Guide	Describes the deployment of Cisco Secure Workload virtual appliances (formerly known as Tetration-V). Cisco Secure Workload Virtual (Tetration-V) Deployment Guide
Cisco Secure Workload Platform Datasheet	Cisco Secure Workload Platform Datasheet
Secure Workload Documentation	Secure Workload Documentation
Latest Threat Data Sources	Cisco Secure Workload

Contact Cisco

If you cannot resolve an issue using the online resources listed above, contact Cisco TAC:

- Email Cisco TAC: tac@cisco.com
- Call Cisco TAC (North America): 1.408.526.7209 or 1.800.553.2447
- Call Cisco TAC (worldwide): Cisco Worldwide Support Contacts