Cisco Secure Workload Release Notes, Release 3.8.1.1

First Published: 2023-05-19

Introduction

This document describes the features, caveats, and limitations for Cisco Secure Workload software, release 3.8.1.1.

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 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.
- GCP connector for flow telemetry data generated using GCP data sinks.

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

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.

The release notes are updated with latest information about restrictions and caveats. See the following website for the most recent version of this document:

http://www.cisco.com/c/en/us/support/data-center-analytics/tetration-analytics/tsd-products-support-series-home.html

The following table shows the history for this release:

Date	Release Information
May 19th, 2023	Cisco Secure Workload 3.8.1.1 is introduced.

New Software Features

Feature Name	Description
Ease-of-use	
Enhanced first time user onboarding experience	The onboarding experience is enhanced end-to-end from onboarding to installing software agents using the installer script or installer image method.
Migration automation	The migration of configurations from tenant to tenant is now fully automated to set up virtual appliances and connectors.
Secure Connector	The secure connector page is enhanced to display the metrics when the line protocol of a tunnel interface is down or comes up along with the event logs, offering more visibility into the stability of the tunnels.
Agent migration automation	You can now use the rehoming feature to move software agents from on-premises to SaaS or SaaS to on-premises.

Feature Name	Description
Policy usage reporting and compliance	You can now use the policy hit count as an indicator to: • find unused policies within a time range. • return hit count for a given policy within a time range, including the first and last count.
Label Management: Label-IP mapping	For each label usage, you can now add label-IP mapping in addition to adding label-key, label-filter, and filter-workspaces.
Traffic filtering and policy analysis by flow source type	You can now use sensor type to filter by source of flow and the flow search.
ADM Export	With the new ADM functionality, you can now download a high-resolution image of the graphical view of the policies.
Day 2 Operations	
Smart Licensing	Cisco Smart Licensing, a unified license management system that manages software licenses across Cisco products, is now available to register Secure Workload clusters, report the usage of licenses, and to track the compliance of Secure Workload on-premises cluster. You can also synchronize smart licenses manually or by scheduling the synchronization using the Smart Software Manager On-prem with the Smart Software Manager Portal.
Alert enhancements	You can now configure alert severity and alert threshold while configuring external orchestrator. You can also view the generated alert when an external orchestrator stops functioning or due to connection failure from the connector respectively at Secure Workload. For more information on how to enable and view Alert on External Orchestrator, see the *External Orchestrators* section in the Secure Workload user guide.
Generate a test alert	For review or testing purposes, use the Generate Test Alerts button to verify the connectivity with any publisher. While configuring the alerts, you can also configure the sample alert to send out alerts based on the alert type and the linked publisher. For more information on how to generate a test alert, see the *Generate a Test Alert on the Alert* section in the Secure Workload user guide.
Reporting capabilities	Reporting dashboard is introduced which is designed for executive personas, network administrators, and security analysts. This dashboard offers visual representations of critical workflow status, troubleshooting capabilities, and report creation functionalities.
Enhanced MITRE ATT&CK framework UI	The reporting dashboard includes a new card-layout for Security Summary to match the MITRE ATT&CK layout. The representation includes the tactics and their count.

Feature Name	Description
Extended telemetry buffering on the host agent	Software agents now offer extended network telemetry buffering on the host. The feature can be configured using the *Flow Disk Quota* or via the *Flow Time Window* in Agent Config Profile.
Password protection for the software agent (Windows) to disable and uninstall	Software agent on Windows can now be protected against stopping/disabling service and uninstallation. This feature can be switched on using the service protection configuration in Agent Config Profile page.
Uninstallation of agents reported to Secure Workload cluster	When you uninstall an agent, the information is communicated to the cluster, which in turn updates the Software Agent page with the information. You can also manually delete the agent from UI on the Software Agent page, or the user can enable automated cleanup or removal of the agent by turning on the cleanup period from agent config profiles. For more information, see the *Remove a Deep Visibility or Enforcement of Linux, Windows, AIX Agent on the Removing Software Agents* sections in the Secure Workload user guide.
Integration	
Enhancements for Secure Firewall Management Center integration	Network administrators can now push a specific set of rules associated with the workload to the corresponding Secure Firewall Management Center and Secure Firewall Threat Defense domains.
Virtual Patching of workloads using Secure Firewall Management Center	Network administrators can now push CVE information from Cisco Secure Workload to Cisco Secure Firewall Management Center to augment the threat protection capabilities of the firewalls to protect the workloads from known vulnerabilities and provide virtual patching as a compensating control using the IPS signatures on the firewall.
User Permissions for AD/LDAP Configuration on ISE connector	For onboarding an ISE and AnyConnect NVM connector, you can now configure LDAP on connectors with a standard domain user account. For more information, see the *LDAP Configuration* section in the Secure Workload user guide.
ISE Integration with ISE-PIC	ISE connector in Secure Workload now connects with ISE-PIC using the pxGRID to retrieve metadata, including ISE group name and ISE group type, from endpoints reported through ISE.
ISE integration: Ability to select/filter endpoints and their attributes being ingested from ISE PxGrid	You can now ignore ISE attributes while configuring the ISE connector if you do not want to ingest all contextual information of endpoints reported through ISE. When you configure the ISE connector, you can now filter ISE endpoints by entering multiple IPv4 or IPv6 subnets.

Feature Name	Description
Netflow connector to report list of Netflow sources	You can collect and report to the cluster, the list of netflow sources sending netflow to Netflow connectors.
AIX/UNIX enhancements for forensics, vulnerability and alerting	You now have only one tetration engine managing network visibility, and operating system process level visibility for deeper forensic monitoring and policy enforcement. Software agent on AIX, Linux and Solaris is represented only by csw-agent service.
Product Evolution	
Capture packets through the native OS API in Windows	Windows agent now uses ndiscap.sys (Microsoft in-built) driver and eventstTracing using Windows (ETW) framework to capture the network flows. The existing Secure Workload bundled Npcap version is no longer available on the host.
Support Network Visibility on Solaris 11.4 x86_64	Network visibility is supported on Solaris 11.4.
Containers	
Pre-built policy template for Kubernetes control plane traffic	Discovering and implementing policies on a Kubernetes cluster is now easier as policy templates are available for the Kubernetes environment (eks,aks,gke,openshift), where you can customize and add policies to suit the application requirements.
Support for K8s Service Object type Loadbalancer for Public Cloud	Supports the Kubernetes Service Object type Load balancer for AKS and EKS clusters.
ADM efficacy for Kubernetes or containerized workloads	A new topic for Policy Discovery Kubernetes Support is added where policy discovery uses the information on pods and services from Kubernetes configuration to create clusters for both pods and services. *Use for policy discovery clustering* from the external orchestrator page is removed.
Kubernetes - Windows worker node support	Software agents now capture and report host and pods' network telemetry on Kubernetes Windows worker nodes on AKS and vanilla Kubernetes clusters utilizing Windows worker nodes. **Note** Not applicable for GKE or EKS.
Cloud Native Workloads	
Differentiate between cloud and on-prem agentless workloads on the UI	Differentiate between a normal IP learned from flows versus an agentless cloud instance like EC2 on the UI.
Scaling	

Feature Name	Description
Enhanced scalability (75k) for SaaS and 39 RU appliance	• Single tenant in SaaS can support a maximum of 75K workloads (in conversation mode). • Single tenant or multi-tenant in 39 RU can support a maximum of 75K workloads (in conversation mode). • Single tenant or multi-tenant in 8 RU can support a maximum of 20K workloads (in conversation mode).
Hybrid Multicloud Workloads	
GCP Connector enhancements	GCP connector now supports new capabilities, it includes tag ingestion, VPC flow log ingestion and segmentation using GCP built-in firewall.
Enhanced security for AWS Connector	Support for AWS IAM role-based authentication is added in the AWS connector.
AWS Connector troubleshooting enhancements	A new Event Log tab is added that displays events for each AWS connector; the logs help to understand the significant events happening per AWS connector from different capabilities.
Upgrade the backend and UI for improved workflow	The AWS connector page is enhanced for an improved workflow. Some of the enhancements are: • The improved UI displays an overview of all the created configurations for each cloud connector. • Template generation and getting started are added in a separate view. • Assume Role registration/update/removal with its states and trigger actions are added. • Registration states are added at a glance on each configuration. • To reduce the real estate on the UI: • Assume Role workflow is added to Settings. • Resource selection is available in a tree-like structure to fetch resources at each level. • A separate Inventory tab is added, which shows inventory tables in the chosen Resource and Scope Context, this allows users to compare the differences between them. • Except for the Settings, filters are added to every view to help in Resource/Scope selections.
Azure Connector troubleshooting enhancements	A new Event Log tab is added, which display events for each Azure connector; the logs help to understand the significant events happening per Azure connector from different capabilities.
Data Backup and Restore	

Feature Name	Description
Detailed status and error messages of S3 bucket configuration checks	When you configure the data backup, you can now view the detailed status checks for the S3 bucket configuration.
Enhanced error reporting to debug backup failures	Error reporting is enhanced to display a tabular view of the checkpoints with additional filter options on the backup status page.

New Hardware Features

There are no new hardware features in this release.

Changes in Behavior

- Software Agent installer script has to be in sync with Secure Workload cluster version. For example, all requests originating from a 3.7.1.22 installer script will be rejected by the cluster running 3.8.1.1 version.
- Software Agent uninstallation now completely removes all the files.
- Software Agent on AIX, Linux and Solaris is represented by only one service *csw-agent.* There will be no more *tet-sensor*, *tet-enforcer* and *tet-main* distinct services.
- Software Agent runtime communications to cluster upgraded to use CiscoSSL 1.1.1s.7.2.463 version.
- Software Agent number of connections to Collectors is now reduced by a factor of two.
- Secure Firewall Management Center's external orchestrator migrated to Cisco Secure Firewall Connector.
- In Secure Firewall Management Center, domain to application scope mapping is no longer supported.
- Flow learned Inventories will no longer show up in **Scopes and Inventory** page. This will have no impact on policy discovery, policy analysis and enforcement. Scope and Inventory Filter will also stop showing any flow learned inventories and may give the impression that a filter/scope is empty; however, under the hood policy discovery/analysis/enforcement will work as expected by using the subnet match.

Deprecated Features

Feature	Feature Description
Flow table columns are deprecated	The following columns in the flow table are no longer available: • TCP Performance • Fwd TCP Bottleneck • Rev TCP Bottleneck • Fwd Congestion Window Reduced • Rev Congestion Window Reduced • Fwd MSS Changed • Fwd MSS Changed • Rev MSS Changed • Fwd TCP Rcv Window Zero? • Rev TCP Rcv Window Zero? • Fwd Fabric Path • Rev Fabric Path • Fwd Burst Indicator • Rev Burst Indicator • Fwd Max Burst Size (KB) • Fwd Rev Burst Size (KB) • Flow filters
Alert features are deprecated	Neighborhood and fabric alerts, and External Kafka (Data Tap) publisher are deprecated from this release.

Compatibility Information

For information about supported operating systems, external systems, and connectors for Secure Workload agents, see the Compatibility Matrix.

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 Virtual.

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 75,000 (3x) 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 20,000 (4x) 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 Issues

The resolved and open issues 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, register for an account.

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

Resolved Issues

Click the Identifier link to access Cisco’s Bug Search Tool to see additional information about the issue.

Identifier	Headline
CSCwe83822	Windows Agent Upgrade from 3.7.1.22 can fail MSI signature check.
CSCwf78123	[Linux] Continuous Policy deviation/Correction on newer platforms when iptables-legacy present.
CSCwe27066	Anyconnect connector - the controller crashed: Not able to export flow data.
CSCwf29111	Policy Analysis may incorrectly show rejected flows by Windows workload.
CSCwf29138	TetSen.exe process is faulting on Windows workloads.

Identifier	Headline
CSCwe83822	Windows Agent Upgrade from 3.7.1.22 can fail MSI signature check.
CSCwf18991	AIX: DHCP broken when Catch-all is DENY.
CSCwf03825	AIX agent installer does not recognize ipfilter version greater than ipfilter v5.3.0.7

Open Issues

Click the Identifier link to access Cisco's Bug Search Tool to see additional information about the issue.

Identifier	Headline
CSCwd67224	AIX 7.x once enforcement is enabled, agent not able to connect to CSW Cluster due to fragmentation.
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.
CSCwf37266	AIX enforcement rules do not properly match on subnets with leading zeros.

Related Documentation

Document	Description
Cisco Secure Workload M6 Cluster Deployment Guide	Cisco Secure Workload M6 Cluster Deployment Guide
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

Document	Description
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