What's New in Cisco Secure Workload Release 3.8.1.1

First Published: 2023-05-19

Last Modified: 2023-07-27

New Software, New Hardware and Deprecated Features

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.
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	

Feature Name	Description
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.
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.
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	

Feature Name	Description
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.
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	

Feature Name	Description
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	
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.

Feature Name	Description
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	
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.

Note Support for M4 is limited to release 3.8.1.1; there will be no support for M4 after release 3.8.1.1.

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.	