Get Started

Cisco Secure Workload Overview

Today's networks include applications running in a hybrid multicloud environment that uses bare-metal, virtualization, and cloud-based and container-based workloads. The key challenge in such an environment is improving application and data security without compromising on agility. Cisco Secure Workload provides comprehensive workload protection by bringing security closer to applications and tailoring the security posture that is based on the application behavior. Secure Workload achieves this tailoring by using advanced machine learning and behavior analysis techniques. It provides a ready-to-use solution to support the following security use cases:

- Implement a zero-trust model with microsegmentation policies that allow only traffic required for business purposes.
- Identify anomalies on the workloads using behavioral baselining and analysis.
- Detect Common Vulnerabilities and Exposures in the software packages that are installed on the servers.
- Recommend quarantining of servers if vulnerabilities persist after enforcing policies and blocking communication.

About Workloads

In Cisco Secure Workload, a workload is an IP address; hosts that have software agents installed are called workloads and hosts that do not have an agent installed on them are called IP addresses.

Quick Start Wizard

An optional wizard can guide you through creating the first branch of your scope tree, which is a first step toward generating and enforcing policies for an application you choose. The wizard introduces the concepts and benefits of labels and scopes.

The following user roles can access the wizard:

- Site administrator
- Technical support
- Root scope owner

To access the wizard, do any one of the following:

- Sign in to Cisco Secure Workload.
- Click the link in the blue banner. The blue banner appears at the top of all pages.
- Choose **Overview** from the main menu.

Note You cannot access the wizard if scopes are already defined in **Organize** > **Scopes and Inventory**. Delete the existing scopes to access the wizard.

Get Started with Segmentation and Microsegmentation

Use the high-level procedures given here to set up segmentation and microsegmentation policies using Cisco Secure Workload.

General Process for Implementing Microsegmentation

The intent of segmentation and microsegmentation is to allow only the traffic your organization needs in order to conduct business, and block all other traffic.

Step 1 Meet requirements.

Verify that Secure Workload supports the platforms and versions that your workloads are running on, and the systems that provide essential information that informs your policies.

See https://www.cisco.com/go/secure-workload/requirements/agents.

Step 2 Install agents on workloads.

Agents gather flow data and other information that you and Secure Workload will use to group workloads and determine appropriate policies. Later, when you are ready, these agents will enforce the policies you approve. For details, including links to lists of supported platforms and requirements, see Deploying Software Agents.

Step 3 Gather or upload labels that describe your workloads.

Labels let you easily understand the purpose and other key information about each workload.

You will need this information in order to group workloads, apply appropriate policies, and understand the policies that Secure Workload suggests. Labels are the foundation for self-maintaining groups that simplify policy management over time. For details, see Workload Labels and Importing Custom Labels.

Step 4 Create a scope tree based on your workloads’ labels.

The logical groups of workloads that labels help you create are called “scopes”, and a well-chosen set of labels helps you create a hierarchical map of your network called a scope tree. This hierarchical view of the workloads on your network is key to efficiently creating and maintaining policies. It lets you create a policy once and apply it automatically to every workload on that branch of the tree. It also lets you delegate responsibility for certain applications (or parts of your network) to the people who have the expertise needed to determine the correct policies for those workloads.

You will group workloads into scopes based on queries based on their labels. For example, you can create a scope called “Email-app” that includes all of the workloads that have the labels “Application = Email-app” and “Environment = Production”. You can create the parent scope of this scope using the query “Environment = Production”. The Production scope will include your production Emailapp and all other workloads that are labeled with “Environment = Production”.

For details, see Scopes and Inventory.

Step 5 Create a workspace for each scope for which you want to apply policies.

The workspace is where you manage policies for all of the workloads in that scope. For details, see Workspaces.

Step 6 Manually create policies that apply broadly across your network.

For example, you might want to allow access from all internal workloads to your NTP server, and deny all external traffic, or deny access from all non-internal hosts unless explicitly permitted. You can create absolute policies that cannot be overridden by more granularly applied policies, and default policies that can be overridden if a more specific policy exists. You will typically create these policies in the workspaces associated with scopes nearer the top of your tree.

See Manually Create Policies.

Step 7 Automatically discover policies for scopes lower in your scope tree.

Secure Workload analyzes traffic between workloads to group workloads based on their behavior and suggest a set of policies based on existing traffic patterns.

More flow data over a longer time period generally creates more accurate policy suggestions.

You can discover policies iteratively (see below.)

For details, see Automatic Policy Discovery and subtopics.

Step 8 Review and analyze the policies that Secure Workload has suggested.

- Review the suggested policies and clusters to see if they make sense based on the labels associated with each workload.
- Use policy analysis and other tools in Secure Workload to confirm that the suggested policies allow the traffic your organization needs in order to conduct business. For example, see Live Analysis. and Policy Visual Representation.
- Understand clustering of workloads within a scope.

  Clusters are groups of workloads within a scope that are closely related and may warrant policies that are more tailored than policies targeted at the entire scope. See Grouping Workloads: Clusters and Inventory Filters and subtopics.
- Consider the impact of inheritance.

  As you analyze the results of your policies, keep in mind that policies in workspaces that belong to scopes above each scope in the hierarchy may affect workloads in lower scopes on the same branch. See Policy Inheritance and the Scope Tree.

Work with subject-matter experts in your organization to understand the needs of the organization and the appropriateness of suggested policies.

For details, see Review and Analyze Policies and subtopics.

Step 9 Iteratively discover policies as needed.

Because more traffic flow data produces more accurate policy suggestions (for example, if you have a report that runs monthly, even three weeks worth of data may not capture all essential traffic), you can continue to discover policies and review and analyze any newly discovered policy suggestions. Each discovery run suggests policies based on the current existing traffic flows.

Before you re-run automatic policy discovery, you can approve any policies that you do not want to be overwritten.

See Re-Running Automatic Policy Discovery.

Step 10 When you are ready, approve and enforce policies.

After you have determined that the policies associated with a workspace (and hence, the associated scope) are appropriate and will block unwanted traffic while not interrupting essential services, you can approve and enforce those policies.

You can iteratively enforce policies; for example, you might initially enforce just the manually created policies, then over time, enforce discovered policies that you have reviewed and approved.

For details, see Enforce Policies.

Set Up Microsegmentation for Workloads Running on Bare Metal or Virtual Machines

Step 1 Gather the IP addresses of workloads on your network.

For each workload, you will also want the application name, application owner, environment (production or non-production), and other information such as geographical region that will determine the policies to be applied..

If you do not have a Configuration Management Database (CMDB), you can collect this information in a spreadsheet.

To get started, choose a single application that you can focus on.

Step 2 Install agents on supported bare-metal-based or virtual workloads.

For more information, see Deploying Software Agents.

Step 3 Upload labels that describe these workloads.

For more information, see Workload Labels and Importing Custom Labels.

Optionally, you can run the quick start wizard to create labels and the first branch of your scope tree for your chosen application; after you run the wizard, you can skip to creating policies. For more information about the wizard, see Quick Start Wizard.

Step 4 If needed, create or update your scope tree based on your labels.

For more information, see Scopes and Inventory.

Step 5 Create a workspace for each scope for which you want to apply policies.

For more information, see Workspaces.

Step 6 Create manual policies that apply across your network.

For more information, see Manually Create Policies.

Step 7 For more information on platform-specific policies, see Platform-Specific Policies.

Step 8 Automatically discover policies in workspaces associated with lower-level scopes.

For more information, see Automatic Policy Discovery and subtopics.

Step 9 Review and analyze the suggested policies.

For more information, see Review and Analyze Policies and subtopics.

Step 10 Iteratively discover policies as needed.

For more information, see Iteratively Revise Policies and subtopics.

Step 11 When you are ready, enforce the policies.

You can enforce policies when you are satisfied with the behavior of the policies in each workspace.

You must enforce policies both in the workspace and in the agent configuration.

For more information, see Enforce Policies.

Set Up Microsegmentation for Cloud-Based Workloads

Step 1 Install agents on your cloud-based workloads, if required.

Cloud connectors provide VPC/VNet level granularity in policy discovery and enforcement. Install agents on supported platforms if you require policy discovery and enforcement at a more granular level.

Install agents based on the operating system on which your cloud service is running. For more information, see Deploying Software Agents.

Step 2 Set up cloud connectors to gather labels and flow data.

For more information, see:

- AWS Connector.
- Azure Connector.
- GCP Connector

Step 3 Create workspaces for the scopes created by the connector.

For more information, see Workspaces.

Step 4 Automatically discover policies.

Discover policies for each VPC/VNet-defined scope, and if applicable, for more granular scopes.

For more information, see Automatic Policy Discovery.

Step 5 Review and analyze the suggested policies.

See Review and Analyze Policies and subtopics.

Step 6 Iteratively discover policies as needed.

See Iteratively Revise Policies and subtopics.

Step 7 Approve and enforce policies for each scope.

You must enable enforcement in the applicable workspace and in the connector for each VPC or VNet, and for any agents installed on individual workloads.

- For more information, see Enforce Policies and subtopics.
- For more information on:
  - AWS-based workloads, see Best Practices When Enforcing Segmentation Policy for AWS Inventory.
  - Azure-based workloads, see Best Practices When Enforcing Segmentation Policy for Azure Inventory.
  - GCP-based workloads, see Best Practices When Enforcing Segmentation Policy for GCP Inventory.

Set Up Microsegmentation for Kubernetes-Based Workloads

Step 1 Install agents on Kubernetes-based workloads. Ensure that you check the requirements and prerequisites.

For more information, see Kubernetes/Openshift Agents - Deep Visibility and Enforcement.

Agents are automatically installed on all future workloads managed by the applicable Kubernetes service.

Step 2 Gather labels for your Kubernetes-based workloads.

For more information on:

- Plain-vanilla Kubernetes and OpenSource workloads, see External Orchestrators and Kubernetes/OpenShift.
- Elastic Kubernetes Services (EKS) Running on Amazon Web Services (AWS), see AWS Connector and Managed Kubernetes Services Running on AWS (EKS).
- Azure Kubernetes Services (AKS), see Azure Connector and Managed Kubernetes Services Running on Azure (AKS)
- Google Kubernetes Engine (GKE) running on Google Cloud Platform (GCP), see Managed Kubernetes Services Running on GCP (GKE).

Step 3 Create or update your scope tree based on your labels.

For more information, see Scopes and Inventory.

Step 4 Create a workspace for each scope for which you want to apply policies.

For more information, see Workspaces.

Step 5 Automatically discover policies for each low-level scope.

For more information, see Automatic Policy Discovery.

Step 6 For more information on applicable additional options, see Platform-Specific Policies.

Step 7 Review and analyze the suggested policies.

For more information, see Review and Analyze Policies.

Step 8 Iteratively discover, review, and analyze policies as needed.

For more information, see Iteratively Revise Policies.

Step 9 When you are ready, approve and enforce policies for each scope.

You must enable policy enforcement in the workspace and for the agents.

For more information, see Enforce Policies and Enforcement on Containers.

Deploying Software Agents

Related Topics

Workload Labels
Scopes and Inventory
Deploying Software Agents
Secure Workload Quick Start Guide
Segmentation