Get Started with Cisco Secure Workload

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 that is required for business purposes.
- Identify anomalies on 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.

Workloads and IP Addresses in Secure Workload

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

Note To view the End User License Agreement and Supplemental End User License Agreement for your product, see End User License Agreement and Supplemental End User License Agreements.

- Supported Web Browsers, on page 1
- Quick Start Wizard, on page 2
- Get Started with Segmentation and Microsegmentation, on page 2

Supported Web Browsers

Secure Workload supports the following web browsers:

- Google Chrome
- Microsoft Edge

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 Secure Workload.

General Process for Implementing Microsegmentation

The intent of segmentation and microsegmentation is to allow only the traffic that is required for business purposes and to block all other traffic.

Procedure

Step 1 Ensure that Secure Workload supports the platforms and versions that your workloads are running on, and the systems that provide essential information to your policies. See Secure Workload Compatibility Matrix.

Step 2 Install agents on workloads.

Agents gather flow data and other information that is required that is for Secure Workload to group workloads and determine appropriate policies. The agents also enforce approved policies. For more information, 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 of each workload and provide other key information about each workload.

You need this information to group workloads, apply appropriate policies, and understand the policies that Secure Workload suggests. Labels are the foundation of maintaining groups that simplify policy management. For more information, see Workload Labels and Importing Custom Labels.

Step 4 Create a scope tree based on your workload 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. The hierarchical view enables you to create a policy once and apply it automatically to every workload on that branch of the tree. The view also lets you delegate responsibility for certain applications (or parts of your network) to people who have the expertise needed to determine the correct policies for those workloads.

You can query workloads and group them into scopes 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 a parent scope for the Application = Email-app scope by using the query Environment = Production. The Production scope includes the production Email-app and all other workloads labeled with Environment = Production.

For more information, see Scopes and Inventory.

If you have not yet created any scopes, you can use the Quick Start wizard to create a scope tree. For more information, see Quick Start Wizard, on page 2.

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

The workspace is where you manage policies for the workloads in that scope. For more information, see Workspaces.

Step 6 Manually create policies that apply 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. Policies can be absolute, meaning that they cannot be overridden by more specific policies, or default, where they can be overridden by more specific policies.

For more information, see Manually Create Policies.

Secure Workload has policy templates that make policy creation easier. For more information, see Policy Templates.

You can enforce manually created policies without waiting for the policies to be discovered. For more information, see Enforce Policies.

Step 7 Automatically discover policies based on existing traffic patterns.

Secure Workload analyzes traffic between workloads, groups workloads based on their behavior, and suggests a set of policies that are intended to allow the traffic that your organization needs, so you can block all other traffic.

Analysis of more data flow over a longer time period leads to more accurate policy suggestions.

You can discover policies iteratively. (There is more information about this later in this procedure.)

a. Discover policies for a branch of your scope tree.

If you are just getting started, you can have temporary set of policies in place and provide protection against future threats.

b. Discover policies for single scopes.

Typically, you will do this for scopes at or near the bottom of your scope tree. These scopes usually include workloads for a single application.

For more information, see Automatic Policy Discovery and Discover Policies for One Scope or for a Branch of the Scope Tree.

Step 8 Review and analyze your policies.

Examine your policies carefully to ensure that they have the effects you expect and that there are no unintended side effects.

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

a) Review the policies and clusters that Secure Workload has suggested.

(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. For more information, see Grouping Workloads: Clusters and Inventory Filters.)

For more information, see Review Automatically Discovered Policies.

b) Analyze your policies to see how they affect actual traffic on your network.

Use policy analysis and other tools in Secure Workload to confirm that your policies allow the traffic your organization needs in order to conduct business. For more information, see Live Analysis. and Policy Visual Representation.

As you analyze the results of your policies, keep the following points in mind:

- Policies in workspaces for higher scopes of a branch might affect the workloads of lower scopes of the branch. For more information, see Policy Inheritance and the Scope Tree.
- Microsegmentation creates a miniature firewall around each workload. In order for a connection to be successful, both consumer and provider of the transaction must have policies allowing the traffic. If both workloads are not in the same scope, creating these policies may require extra steps. For more information, see When Consumer and Provider Are in Different Scopes: Policy Options.

Step 9 Iteratively discover policies as needed.

More traffic flow produces more accurate policy suggestions. For example, for a monthly report even three weeks worth of data may not capture all essential traffic. Continue to discover policies and review and analyze new policy suggestions. Each discovery run suggests policies based on the current traffic flows.

You can also iteratively discover polices to capture changes in policy discovery settings and approved clusters. For more information, see Iteratively Revise Policies.

Before you re-run automatic policy discovery, ensure that you approve policies and clusters that you want to retain.

Each time you re-discover policies, you must review and analyze them.

Step 10 When you are ready, 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 enforce those policies.

You can iteratively enforce policies; for example, you might initially enforce just the manually created policies in scopes near the top of your tree, then over time, enforce discovered policies in scopes lower in the tree.

For more information, see Enforce Policies.

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

Procedure

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 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

Procedure

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

Procedure

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 in Secure Workload 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.

What to do next

Related Information:

- Workload Labels
- Scopes and Inventory
- Deploy Software Agents
- Manage Policies Lifecycle in Secure Workload
- Secure Workload Quick Start Guide