Cisco Secure Workload

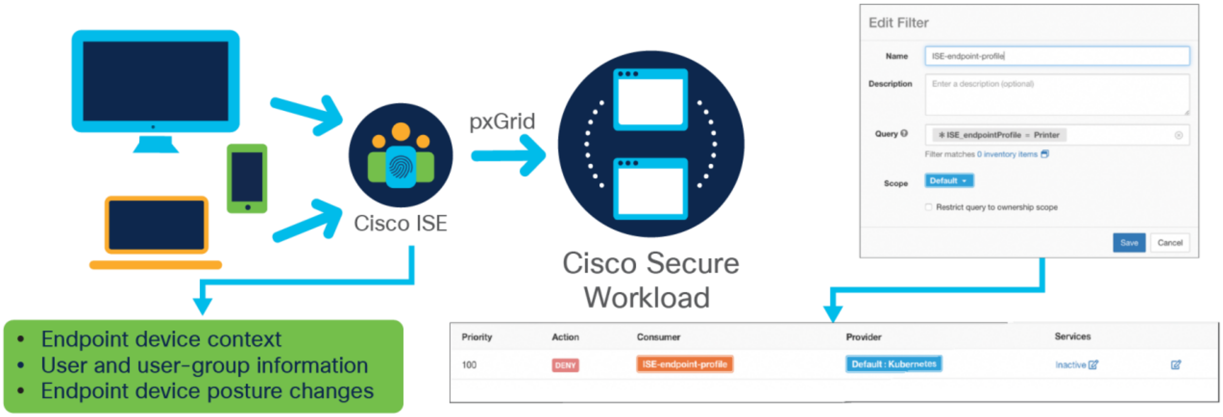
(formerly Tetration and Cisco ISE Integration Use Cases and Benefits)

Contents

Extend microsegmentation to include workforce and endpoint-device contexts with Cisco Secure Workload and Cisco ISE

Q. What if you could better secure your applications by dynamically extending microsegmentation policies based on workforce context and endpoint device postures?

A. Cisco Secure Workload integrates with Cisco Identity Services Engine (ISE) to gain the real-time context regarding both the workforce (for example: Who is logged into a device?) and the endpoint devices (for example: Is the device a printer? Is the device compromised?). Cisco Secure Workload allows users to predefine policies to allow, deny, or restrict access to applications based on this information. It then dynamically renders the policy in real-time to take necessary actions.



- Endpoint device context
- User and user-group information
- Endpoint device posture changes

Name	ISE-endpoint-profile
Description	Enter a description (optional)
Query	✱ ISE_endpointProfile = Printer Filter matches 0 inventory items
Scope	Default ▾
	□ Restrict query to ownership scope

Priority	Action	Consumer	Provider	Services
100	DENY	ISE-endpoint-profile	Default : Kubernetes	Inactive

Figure 1.
Cisco Secure Workload™ and Cisco Identity Services Engine (ISE) integration

Benefits

- Enhance your application workload security with workforce and endpoint-device contexts
- Dynamically adapt security policies based on changes in device postures
- Simplify the orchestration of policies across any infrastructure and any cloud

Trends and challenges

Today, enterprise applications span across on-premises infrastructures and public clouds. Eighty percent of enterprises use multiple public clouds. On the user and endpoint device side, there is a major transformation in how and from where applications are being accessed. In the past, users accessed applications only from a desktop or assigned laptop devices. With the exponential growth of endpoint devices and adoption of IoT by enterprises, a plethora of these devices connect to applications in data centers either to access data or send telemetry. For the first time, IoT has displaced cloud as the second most popular digital transformation initiative within organizations. This means that any of these devices can be exploited to gain access into the data center and move laterally compromising data and security. In order to defend against such modern threats, enterprises need to take a different approach to security. The result of such an approach would be a defense in-depth through an adaptive security based on endpoint-device and user contexts.

Overview

There is a notion that microsegementation can only be used to limit east-west traffic, that is, communication between various application components in a data center. What if you could enrich microsegmentation policies with user and endpoint-device contexts?

Enterprises today primarily use single-layer access control mechanisms using active directory, network access control, or other means to restrict user and endpoint device access to applications and data. Is this model sufficient for securing applications? If so, why are we still seeing so many security breaches where critical customer data is compromised, leading to data loss and privacy issues? Security is one of the top concerns when undertaking an IoT initiative, which means we need to think about multilayer defense in depth to better protect our applications and data.

Cisco Secure Workload, by integrating with Cisco ISE, is able to offer better security for your applications and data by dynamically rendering policies based on user and user-group information and endpoint-device context. Security owners can extend microsegmentation policy definitions based on these contexts. These policies are enforced on the application workloads themselves (virtual machines, bare-metal servers, containers, etc.), offering an infrastructure-agnostic solution for implementing segmentation. Using this approach, Cisco Secure Workload can extend microsegmentation beyond containing east-west traffic and, at the same time, add another layer of security to restrict access to applications and data.

How it works

Cisco Secure Workload is an application workload security platform designed to secure your compute instances across any infrastructure and any cloud. It uses behavior- and attribute-driven policy and policy enforcement in multicloud environments to achieve this. It enables trusted access through automated, exhaustive context from various systems to automatically adapt security policies.

Cisco ISE provides highly secure network access to users and endpoint devices. It helps you gain visibility into what is happening in your network, such as who is connected, which applications are installed and running on the endpoint devices, and much more. It also shares vital contextual data, such as user and endpoint device identities, threats, and posture changes with integrated solutions such as Cisco Secure Workload, so that threats can be identified, contained, and remediated faster.

Cisco Secure Workload platform gets the contextual data from Cisco ISE in real time through a notification interface called pxGrid. Whenever a new device connects to Cisco ISE, it shares the following information with Cisco Secure Workload:

- Endpoint profile
- Device posture
- Source group tag information

The user can predefine policies based on any of these attributes.

- Example of a policy based on the device type (defined by its endpoint profile: An HVAC control system cannot connect to anything but the HVAC application.
- Example of a policy based on the device posture: A user using a jail-broken iPhone cannot access any compliance-related applications.
- Example of source group tag information: Only users or devices in a particular group can access a database.

Cisco Secure Workload dynamically determines the endpoint information and updates the policy accordingly. This policy is then enforced on the workload itself, using ipsets/iptables for Linux servers and Windows Firewall for Windows servers. There are three primary benefits for using this approach

- Brings security as close to the application as possible (What better place than the server where the application is running?)
- Scales well – as the policy is distributed
- Offers consistent segmentation across any infrastructure and any cloud

Cisco Capital

Flexible payment solutions to help you achieve your objectives

Cisco Capital makes it easier to get the right technology to achieve your objectives, enable business transformation and help you stay competitive. We can help you reduce the total cost of ownership, conserve capital, and accelerate growth. In more than 100 countries, our flexible payment solutions can help you acquire hardware, software, services and complementary third-party equipment in easy, predictable payments. Learn more.

The Cisco Advantage

With your workforce on the go, workloads in many clouds, and devices outside of your control, knowing who and what to trust is the big IT security challenge.

Cisco, with its integration security portfolio, is uniquely positioned to address this problem.

Cisco makes it easier and safer to grant and restrict access by establishing trust-and software-defined perimeters based on dynamic contexts, not just static credentials or network topologies.

Call to action

Start securing your application workloads today

Secure access for your applications with an automated adaptive policy. Only Cisco can establish trust for users and devices anywhere, IoT in campus and branches, and hybrid workloads in on-premises and multicloud infrastructures. To learn more, visit www.cisco.com/go/Secure Workload, then contact your Cisco sales representative or Cisco authorized channel partner.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.

Printed in USA C22-742897-01 02/21