Cisco Secure Workload Platform

April 2024

© 2025 Cisco and/or its affiliates. All rights reserved.

Contents

© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco Secure Workload (formerly Tetration) seamlessly delivers zero trust microsegmentation across any location, any infrastructure and any form factor workload from a single console. With comprehensive visibility into every workload interaction and powerful AI/ML driven policy lifecycle automation, Secure Workload reduces the attack surface, prevents lateral movement, identifies workload behavior anomalies, helps rapidly remediate threats, and continuously monitors compliance.

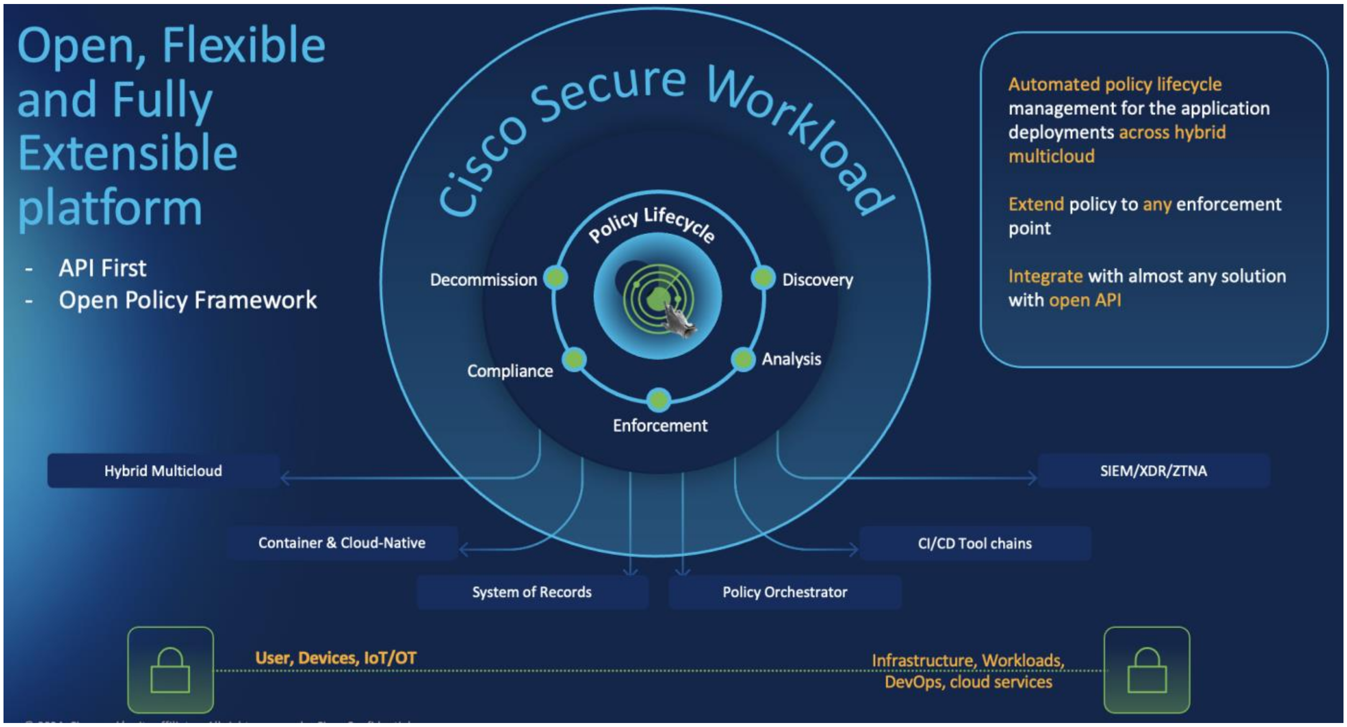
Product overview

Traditionally in IT, we have had an infrastructure-centric view of the universe. Our most valuable data was contained in the data center, so our job was to let good traffic in and keep bad actors out. And our tool of choice was the firewall.

In today's organizations, the center of gravity has shifted decidedly in favor of applications. Applications are critical to how you engage with customers, run your operations, and get paid. But the constant proliferation and dynamic nature of these applications have led to an unprecedented security challenge for IT professionals.

Applications have evolved by adopting cloud and cloud native technologies and are distributed across both on-premises and in the cloud, or across multiple clouds. The critical workloads are becoming ephemeral and no longer tidily kept in the data center where they can be protected by a perimeter firewall. In some ways, there is no more a perimeter. To respond to this app-centric world, you need a security solution that can bring security closer to the applications using a "new firewall or micro-perimeter" that surrounds each and every workload, allowing you to protect what matters to you—your applications and data.

With Secure Workload, you can secure your applications by creating micro-perimeters at the workload level across your entire infrastructure consistently, whether these are deployed on bare-metal servers, virtual machines, or containers.



Open, Flexible and Fully Extensible platform

- API First
- Open Policy Framework

Automated policy lifecycle management for the application deployments across hybrid multicloud

Extend policy to any enforcement point

Integrate with almost any solution with open API

Top 5 Secure Workload use cases

Secure Workload delivers zero-trust microsegmentation to protect applications, reduce risk, and maintain compliance. Below are top 5 use cases of Secure workload.

- SDN and Multi cloud adoption - Automatically generated microsegmentation policies through comprehensive analysis of application communication patterns and dependencies helps in adoption of SDN and multi cloud environment securely. Dynamic attribute-based policy definition with a hierarchical policy model to deliver comprehensive controls across multiple user groups with role-based access control enhances the security posture of multi cloud environment.
- Contain lateral movement - Advanced persistent threats use lateral movement to spread the exploits across workloads resulting in larger blast radius. Secure workload's whitelist policy approach and ability to detect anomalous behavior protects workloads from such malicious lateral movement and reduces blast radius.
- Reduce Attack Surface - Secure Workload provides visibility into not only network traffic but also packages installed, associated vulnerabilities, open and unused ports on the workload. It has built in policies to detect anomaly based on MITRE att@ck framework (TTPs) and ability to configure policies based on vulnerability scores which reduces the attack surface significantly.
- Compliance - The hierarchical inheritance of policy in Secure Workload simplifies the deployment of InfoSec and enterprise-wide compliance policies. It monitors the policy compliance in near real-time and alert against policy violation or potential compromise.
- Secure ephemeral workload - The applications are being modernized with cloud native and micro services architecture changing the form factor of workloads to more dynamic short-lived containers to adapt to the scale up and scale down requirements. Securing these ephemeral workloads is challenging. Secure Workload delivers same level of visibility and enforcement capabilities for any container environment.

Features and benefits

Table 1 lists the main features and benefits of Cisco Secure Workload.

Table 1. Secure Workload primary features and benefits

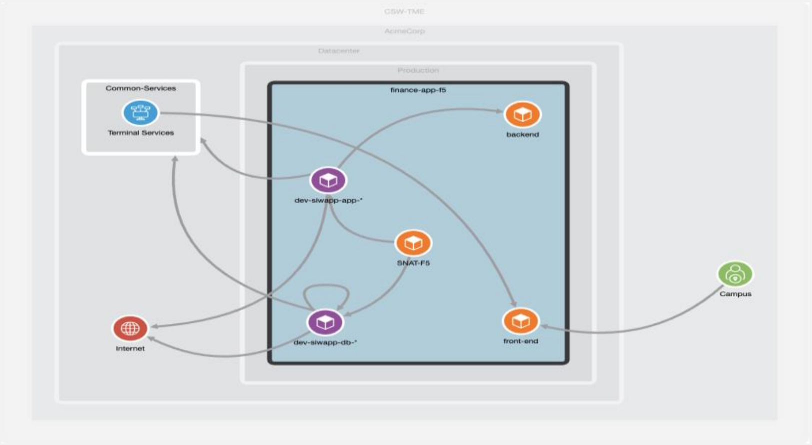
Feature	Benefit
Visibility	• Agents on workloads collects rich network telemetry and sends to CSW tenant. This telemetry is beyond just port and protocols giving more in depth visibility into network packets • The agents on workloads also collect the information about installed packages, open vulnerabilities, open unused ports and the process tree for complete visibility. This helps improve the workload security posture • For agentless environment the network telemetry is collected through ingest appliance and connectors such as NetFLow, ERSPAN, IP-FIX, Firewall, Load balancers. In the public cloud environment, the network flow logs (vpc flow logs) are used. The DPU based telemetry integration can be used alternatively wherever DPU hardware is available. • The Secure workload ingests contexts of the flow using different integrations. Existing labels/tags

© 2025 Cisco and/or its affiliates. All rights reserved.

<table>
<tr><th>Feature</th><th>Benefit</th></tr>
<tr><td></td><td>
and user information is discovered and used through Edge appliances and connectors such as ISE, ServiceNow, Identity and Cloud connectors. In case of cloud connectors all inventory, Services and tags are discovered over REST API.

- The Secure workload delivers a complete insights and visibility into traffic between containers in K8s and Openshift clusters.
- The Enterprise network and infrastructure is visualized in a scope tree with hierarchy. Each scope is a collection of workloads with similar labels. This provides visibility into how the enterprise network is architected.
</td></tr>
<tr><td><b>Zero Trust Microsegmentation policy life cycle</b></td><td>

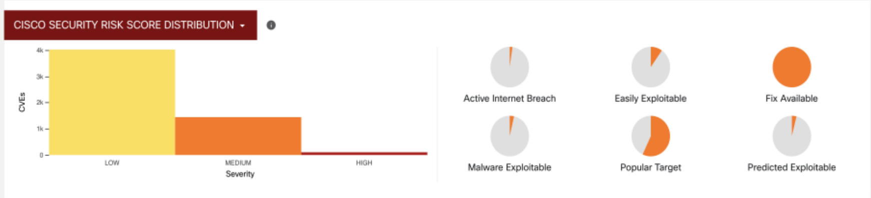
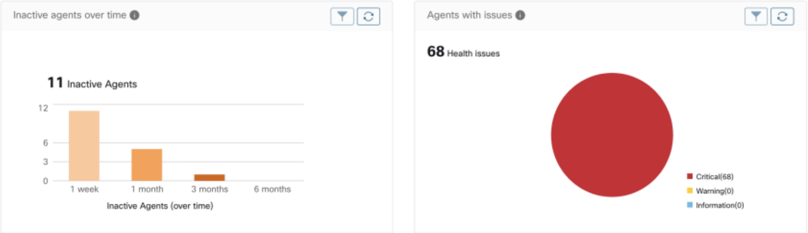
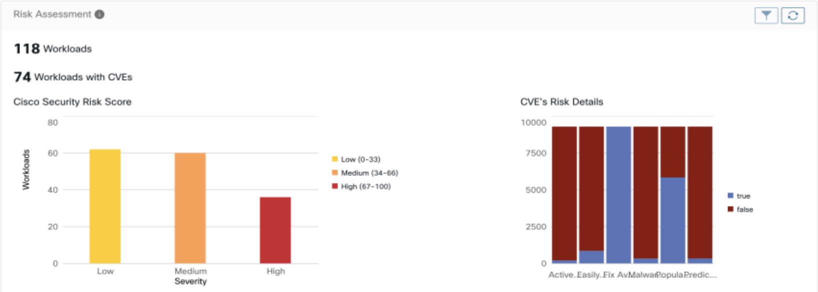
- **Absolute policies**-The InfoSec enterprise-wide policies are defined at the root scope level. These absolute policies are inherited to all child scopes in the hierarchy. These policies overwrite all other low-level policies.
- **Policy discovery**-Secure Workload utilizes AI/ML technology to analyze and baseline the workload behaviors, groups them into clusters and recommends the Microsegmentation policies.
- **Policy Analysis**-The discovered policies are analyzed to check for any unexpected escape and rejected flows. A quick analysis can also be done to check certain flows.
- **Policy Enforcement**-Analyzed policies are enforced by agents on hosts or in agentless way on different policy enforcement points such as firewalls, cloud native tools, load balancers etc.
- **Policy Decommissioning**-The policy insights like hit count, usage pattern and last used information provides details about policy usage and recommended for removal.
- **Advanced Policies**-The other type of policies includes FQDN, Vulnerability score, process, user and group-based policies. Generally, these are static policies and configured at the application scope level. Eliminate time-consuming manual creation of resource lists to segment applications.



</td></tr>
<tr><td><b>Enforcements</b></td><td>

- Agent based enforcements, utilizes OS level filtering capabilities to configure the policy rules - Windows utilize windows filtering platform, Linux use IP Filters.
- Agentless enforcement utilizes other enforcement points. For example, for cloud workloads cloud native security groups, firewalls, NSGs are used. For on-premises workloads, Cisco firewall
</td></tr>
</table>

© 2025 Cisco and/or its affiliates. All rights reserved.

Feature	Benefit
	integration is used and Integrations with F5, NetScaler is used for enforcement. • The latest DPU technology in servers is also leveraged to enforce the policies for all the virtual workloads running on physical host.
Vulnerability dashboard	• Secure workload agent collects all the package information of the workload and the vulnerabilities associated. • The intelligence about CVEs is integrated with secure workload from Cisco Vulnerability management based on 6 parameters. • The dashboard provides an overview of vulnerabilities present in the environment with filtering capability based on workloads, packages and CVEs.  CISCO SECURITY RISK SCORE DISTRIBUTION CVEs 4k 3k 2k 1k 0 LOW MEDIUM HIGH Severity Active Internet Breach Easily Exploitable Fix Available Malware Exploitable Popular Target Predicted Exploitable
Reporting dashboard	The new reporting dashboard has three persona-based reporting sections. • **Overview**-This provides the summary of segmentation, workloads, Traffic and license usage. • **Operation**-This section of reporting provides details such as agents summary and versions, agent issues and inactive agents, Top consumer and provider, cluster and telemetry summary:  Inactive agents over time 11 Inactive Agents 12 6 3 0 1 week 1 month 3 months 6 months Inactive Agents (over time) Agents with issues 68 Health issues Critical(68) Warning(0) Information(0) • **Compliance**-This section focuses on security-based reporting and gives workload risk assessment with CVEs risk scores, MITRE framework alerts summary:  Risk Assessment 118 Workloads 74 Workloads with CVEs Cisco Security Risk Score Workloads 80 60 40 20 0 Low Medium High Severity Low (0-33) Medium (34-66) High (67-100) CVE's Risk Details 10000 7500 5000 2500 0 Active. Easily. Fix Av Malwar Popula Predic... true false

© 2025 Cisco and/or its affiliates. All rights reserved.

Deployment models and scale

Cisco Secure Workload offers both Software-as-a-Service (SaaS) and on-premises options allowing customers to choose the model that meets their business needs.

For on-premises deployments, customers can choose a hardware-based appliance model (small or large form factors). The platform selection will depend on scalability considerations including the number of workloads in the environment and the desired fidelity level of flow telemetry.

When configured for conversation-only flow telemetry across all workloads, each platform can scale vertically up to two times the default platform scale with detailed flow telemetry enabled. In addition, Secure Workload may be scaled horizontally to meet the demands of very large, geographically distributed enterprise environments through federation capability.

Secure Workload also offers Disaster Recovery (DR) capability, delivered through continuous backup and restore functionality that allows customers to restore data and operations to a standby cluster in case of major failure or disaster.

Cisco Secure Workload SaaS option

With the Secure Workload SaaS option, customers can get the benefits of workload protection capabilities without having to deploy and maintain the platform on-premises. With this option, Secure Workload software runs in the cloud, managed and operated by Cisco. The customer is responsible for purchasing the required software subscription licenses and deploying software agents on workloads. The SaaS for Secure workload can now be accessed from Cisco Security Cloud Control (SCC), which provides unified management across multiple cisco products for provisioning, user access and roles management.

This deployment option is well suited for SaaS-only or SaaS-first customers because it offers scale flexibility. You can start small and grow as your demand grows. Other benefits of the SaaS option include:

- Significant reduction in TCO (Total Cost of Ownership).
- Faster time to value.

Table 2 shows the verified and supported scale for the SaaS option.

Table 2. Cisco Secure Workload SaaS Scale

Platform characteristics	Specification
Maximum number of IP Addresses that can be labeled per tenant (CMDB only)	6,000 / 100 licenses (SaaS only)
Maximum number of subnets that can be labeled per tenant (CMDB only)	120 / 100 licenses (SaaS only)
Number of flow events that can be processed per second	5000 flows per second / 100 licenses

Cisco Secure Workload-M (small form factor) option

Table 3 shows the verified and supported scale.

Table 3. Cisco Secure Workload-M platform scale

© 2025 Cisco and/or its affiliates. All rights reserved.

Platform characteristics	Specification
Number of concurrent workloads (virtual machine or bare metal or container host) from which telemetry data can be analyzed	Up to 10,000 workloads in detailed mode. Up to 20,000 workloads in conversation mode.
Number of flow events that can be processed per second	Up to 500,000 flows per second
Number of Tenants	7
Number of Child Scopes per Tenant	1000
Total number of Child Scopes across tenants	7000
Number of Workspaces per Tenant	1000
Total number of Workspaces across tenants	5000
Number of Inventory Filters per Tenant	1000
Total Number of Inventory Filters across Tenants	7000
Number of Roles per Child Scope	6
Maximum number of IP Addresses that can be labeled across all root scopes	500,000
Maximum number of subnets that can be labeled across all root scopes	50,000

Table 4 shows the power and cooling requirements for the Secure Workload-M platform.

© 2025 Cisco and/or its affiliates. All rights reserved.

Table 4. Power and cooling specifications for Cisco Secure Workload-M

Platform requirements	Secure Workload M5 Appliance	Secure Workload M6 Appliance
Max power	5.5 kW	6 kW
Maximum cooling requirement	13,500 BTUs per hour	14,171 BTUs per hour
Rack specification	Cisco R42612 Rack Data Sheet.	

Cisco Secure Workload (large form factor) platform option

Table 5 shows the verified and supported scale.

Table 5. Cisco Secure Workload large platform scale

Platform characteristics	Specification
Number of concurrent workloads (virtual machine or bare metal or container host) from which telemetry data can be analyzed	Up to 37,500 workloads in detailed mode. Up to 75,000 workloads in conversation-mode.
Number of flow events that can be processed per second	Up to 2 million flows per second
Number of Tenants	35
Number of Child Scopes per Tenant	5000
Total number of Child Scopes across tenants	35000
Number of Workspaces per Tenant	3500
Total number of Workspaces across tenants	20000
Number of Inventory Filters per Tenant	5000
Total Number of Inventory Filters across Tenants	35000
Number of Roles per Child Scope	6
Maximum number of IP Addresses that can be labeled across all root scopes	1,500,000

© 2025 Cisco and/or its affiliates. All rights reserved.

Platform characteristics	Specification
Maximum number of subnets that can be labeled across all root scopes	200,000

Table 6 shows the power and cooling requirements for the Secure Workload platform.

Table 6. Power and cooling specifications for large form factor

Platform requirements	Secure Workload M5 Appliance	Secure Workload M6 Appliance
Peak power single-rack option*	22.5 kW	31.8 kW
Maximum cooling requirements single-rack option*	50,000 BTUs per hour	72117 BTUs per hour
Total weight single-rack option	1800 lb (800 kg)	1800 lb (800 kg)
Power Distribution Unit (PDU) and power supply single-rack option	4 x 3-phase PDUs (current and voltage ratings vary by geography)	4 x 3-phase PDUs (current and voltage ratings vary by geography)
Peak power dual-rack option	11.25 kW per rack (22.5 kW total)	15.9 kW
Maximum cooling requirement dual-rack option	25,000 BTUs per hour per rack	36.059 BTUs per hour per rack
Total weight for dual-rack option	900 lb per rack (400 kg per rack)	900 lb per rack (400 kg per rack)
PDU and power supply dual-rack option	4 x single-phase PDUs per rack (current and voltage ratings vary by geography)	4 x single-phase PDUs per rack (current and voltage ratings vary by geography)
Rack specification	Cisco R42612 Rack Data Sheet.	

© 2025 Cisco and/or its affiliates. All rights reserved.

Data backup and recovery

The primary use case of the Data Backup and Recovery feature is to restore a cluster during an outage, to another cluster either at the same site or another site.

Table 7. Data Backup and Recovery Full backup mode and Lean mode comparison

Platform Characteristics	Full backup mode	Lean Mode
Platforms supported	• Cisco Secure Workload (large form factor) platform option. • Cisco Secure Workload-M (small form factor).	Same as Full backup mode.
Supported Storage Type	• Backup and Restore is supported from a customer managed object store with S3 interface that is compatible with S3V4 API since bulk of the data copied is immutable, flat and especially suited for object stores. • DBR can work with a physical data store that's racked up right next to the cluster or a cloud storage such as AWS S3 in the cloud or anywhere that can be reached with an IP address.	Same as Full backup mode.
Data Backed up	All back-ups will be a point-in-time synchronous back up across all data stores. The following data is packaged as objects and backed up: A full backup copies every object in a checkpoint, even if it is already copied and the object has not changed.	Lean Data Mode can be enabled to exclude the non-configuration data from being backed up. All data except the following is backed up: • Flow database. • Data required for automatic policy discovery. • Enforcement policies. • Data to help with forensics such as file hashes, data leak models. • Data related to attack surface analysis. • CVE databases.
Storage Limits	200TB of storage is recommended.	1 TB is sufficient as this does not back up the flows.

© 2025 Cisco and/or its affiliates. All rights reserved.

Licensing requirements

In order to activate Data Backup and Recovery, a license entitlement in the form of an activation key is required for the primary (active cluster). The activation key can be obtained by emailing ciscosecureworkload-licensing-support@cisco.com along with the cluster identification information.

© 2025 Cisco and/or its affiliates. All rights reserved.

Software licensing

Cisco Secure Workload software is licensed based on the number of workload equivalents or devices (endpoints) depending on the agent or sensor type being used. Telemetry data can be collected using agents, supported by other supported sensors or collectors, in any combination. Policy enforcement is enabled through agents with enforcement capability with infrastructure enforcement delivered through Cisco Secure Firewall Integration, Application Delivery Controllers (ADCs), and Security Groups in public cloud infrastructure or orchestrated via streamed Kafka policy. Workload is defined as a virtual machine, bare-metal server, or container host and includes server and desktop operating systems.

There are two primary license types for Secure Workload (including SaaS and On-Premises deployment options):

- **Secure Workload protection license**: This license provides workload protection capabilities, including telemetry data collection, application insight, forensics, software vulnerability detections, policy recommendation, policy simulation, policy enforcement, and compliance tracking functions.
- **Secure Workload endpoint license**: This license provides the comprehensive telemetry data collection from a Cisco AnyConnect client installed in the endpoints (laptops, desktops, smartphones, etc), using an NVM module. This provides insights into user, device, group, process ID, process hierarchy, and OS as well as the domain names accessed from the endpoint. Additionally, this license provides rich context from user devices for any endpoint device managed through Cisco ISE via PxGrid integration. Customers must purchase the endpoint visibility license if they want to use the platform's capability to collect, analyze, and define policies and provide visibility into endpoint device activities. This license can be independent of the workload protection licenses. This does not include any other licenses required to enable AnyConnect NVM or Cisco ISE (those licenses need to be purchased separately).

If a customer has multiple Secure Workload clusters, software licenses can be pooled across those clusters.

If a customer has Secure Workload SaaS licenses, they cannot be ported over to an on-premises license option or vice versa.

Licensing terms

Secure Workload SaaS deployment

The SaaS subscription is governed by the Cisco Secure Workload as a Service Offer Description and the Cisco General terms (Eg, the End User License Agreement) (The Agreement).

On-premises deployment option

The on-premises licenses and subscriptions are governed by the Cisco Secure Workload Offer Description and the Cisco General Terms or similar terms existing between You and Cisco (e.g., the End User License Agreement)(the "Agreement").

Support and compatibility

For detailed operating system support and compatibility information for Cisco Secure Workload, see Platform Support Information at Compatibility matrix.

© 2025 Cisco and/or its affiliates. All rights reserved.

Ordering information

Table 8 provides subscription software bundle part numbers used for the Cisco Secure Workload SaaS deployment option.

Table 8. Software bundle for Cisco Secure Workload SaaS option.

Bundle part number	Part numbers included in bundle	Description
C1-TAAS-SW-K9		Cisco Secure Workload bundle part number that includes the software subscription license for SaaS option.
	C1-TAAS-WP-FND-K9	Bundle part number for the Cisco Secure Workload protection subscription license. Minimum quantity is 100 and increments of 1 after that.
	C1-TAAS-ENDPT-K9	Cisco Secure Workload endpoint visibility software subscription license for endpoints. Choose a quantity between 1000 and 999,999. For example, a quantity of 5000 will provide license price for up to 5000 endpoint devices tracked through Cisco AnyConnect or Cisco ISE.

Also note the following additional information about the software subscription license part number:

- You can select a 1-year, 3-year, or 5-year subscription term.
- The subscription price includes software support.
- You can select the annual billing option or a monthly or quarterly option, or prepay for the entire term.
- You can add more workload instance licenses through subscription modification.
- This software subscription license can be used only with a Cisco Secure Workload SaaS deployment.

Table 9 provides hardware and software bundle part numbers for the Cisco Secure Workload-M platform option.

Table 9. Hardware and subscription software bundle for Cisco Secure Workload-M option.

Bundle part number	Part numbers included in bundle	Description
C1-TETRATION-M		Cisco Secure Workload bundle part number that includes the hardware and software subscription license.
	TA-CL-8U-M5-K9	Secure Workload Gen2 8RU Cluster.
	TA-CL-8U-M6-K9	Cisco Secure Workload Gen3 8RU Cluster.
	C1-TA-SW-K9	Bundle part number for the Cisco Secure Workload software subscription license; see Table 9 for details.

Table 10 provides hardware and software bundle part numbers for the Cisco Secure Workload platform option.

Table 10. Hardware and subscription software bundle for Cisco Secure Workload option.

© 2025 Cisco and/or its affiliates. All rights reserved.

Bundle part number	Part numbers included in bundle	Description
C1-TETRATION		Cisco Secure Workload bundle part number that includes the hardware and software subscription license.
	TA-CL-39U-M5-K9	Secure Workload Gen2 39RU Cluster.
	TA-CL-39U-M6-K9	Cisco Secure Workload Gen3 39RU Cluster.
	C1-TA-SW-K9	Bundle part number for the Cisco Secure Workload software subscription license; see Table 9 for details.

Table 11 provides the software bundle part number for the Cisco Secure Workload software subscription license.

Table 11. Subscription software license for Cisco Secure Workload on-premises deployment options.

Bundle part number	Part numbers included in bundle	Description
C1-TA-SW-K9		Bundle part number for the Cisco Secure Workload software subscription license
	C1-TA-CWP-K9	Cisco Secure Workload on-premises subscription license for workload protection. Minimum quantity is 100 and increments of 1 after that. This license combines previous base and enforcement capabilities. For example, a quantity of 500 will provide the license for up to 500 workloads.
	C1-TA-ENDPT-K9	Cisco Secure Workload endpoint visibility software subscription license is ordered in increments of 1 endpoint. Minimum quantity required is 1000. For example, a quantity of 1505 will provide license price for 1505 endpoint devices tracked through Cisco AnyConnect or Cisco ISE.

Also note the following additional information about the software subscription license part numbers:

- You can select a 1-year, 3-year, or 5-year subscription term.
- The subscription price includes software support.
- The subscription tier is selected automatically based on the quantity entered.
- You can select the annual billing option or prepay for the entire term.
- You can add more workload instance licenses through subscription modification.
- This software subscription license can be used with both forms of Cisco Secure Workload hardware clusters.

Your license for Cisco Secure Workload endpoint software does not include AnyConnect or AnyConnect NVM licenses. You are responsible for acquiring those licenses separately.

Cisco expertise to accelerate adoption

Cisco provides professional and support services from Advisory, Implementation and Optimization to ongoing Solution Support, to help organizations get the most value from the Cisco Secure Workload platform. Cisco Services experts help integrate the platform into your production data center environment, define use cases

© 2025 Cisco and/or its affiliates. All rights reserved.

relevant to your business objectives, tune machine learning, and validate policies and compliance to improve application and operation performance. Cisco Solution Support for Cisco Secure Workload provides hardware, software, and solution-level support. We offer a selection of custom and fixed-price, fixed-scope services for Cisco Secure Workload that help you experience faster time to value, comprehensive adoption in your environment, optimized policies and application performance, and solution wide support.

Cisco environmental sustainability

Information about Cisco's environmental sustainability policies and initiatives for our products, solutions, operations, and extended operations or supply chain is provided in the "Environment Sustainability" section of Cisco's Corporate Social Responsibility (CSR) Report.

Reference links to information about key environmental sustainability topics (mentioned in the "Environment Sustainability" section of the CSR Report) are provided in the following table:

Sustainability topic	Reference
Information on product material content laws and regulations	Materials
Information on electronic waste laws and regulations, including products, batteries, and packaging	WEEE compliance

Cisco makes the packaging data available for informational purposes only. It may not reflect the most current legal developments, and Cisco does not represent, warrant, or guarantee that it is complete, accurate, or up to date. This information is subject to change without notice.

© 2025 Cisco and/or its affiliates. All rights reserved.

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.

For more information

For more information about the Cisco Secure Workload platform, please visit https://www.cisco.com/go/Secureworkload or contact your local Cisco account representative.

© 2025 Cisco and/or its affiliates. All rights reserved.