CISCO
SECURE

Data sheet
Cisco public

Cisco Secure Workload for Workload Protection

October 2020

The bridge to possible

Contents

Cisco Secure Workload (formerly Tetration) seamlessly delivers a zero-trust approach to securing your application workloads across any cloud and on-premises data center environments by reducing the attack surface, preventing lateral movement, identifying workload behavior anomalies, and remediating threats quickly.

Product overview

Traditionally in IT, we've 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.

Apps are distributed. They're deployed both on-premises and in the cloud, or across multiple clouds, and critical workloads are no longer tidily kept in the data center where they can be protected by a perimeter firewall. In some ways, there is no more 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" that surrounds each and every workload, allowing you to protect what matters most to you—your applications and your data.

With Cisco Secure Workload, you can **secure your environments by creating firewalls at the workload level across your entire infrastructure**, whether applications are deployed on bare-metal servers, virtual machines, or containers. Secure Workload helps you to **deliver zero-trust application security, reduce risk**, and **maintain compliance** with:

- Automatically generated microsegmentation policies through comprehensive analysis of application communication patterns and dependencies
- Dynamic attribute-based policy definition with a hierarchical policy model to deliver comprehensive controls across multiple user groups with role-based access control
- Consistent policy enforcement at scale through distributed control of native host firewalls and infrastructure, including ADCs (application delivery controllers) and firewalls
- Near real-time compliance monitoring of all communications to identify and alert against policy violation or potential compromise
- Workload behavior baselining and proactive anomaly detection
- Common vulnerability detection with dynamic mitigation and threat-based quarantine

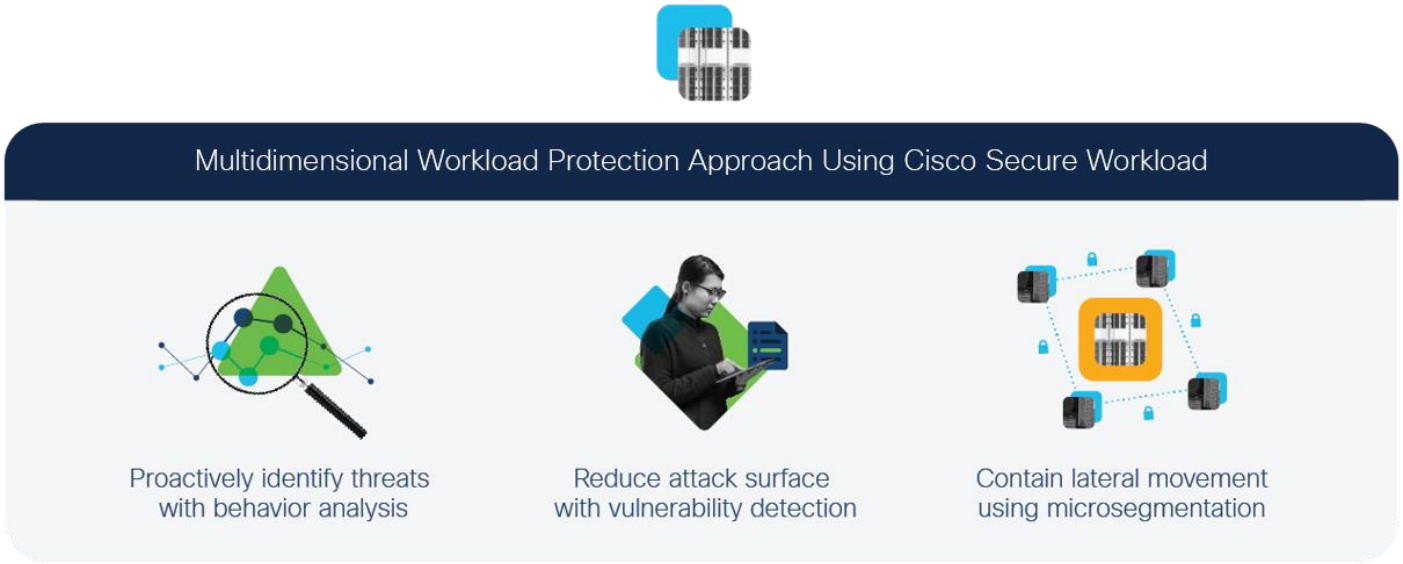

Figure 1. Cisco Secure Workload workload protection approach

Secure applications through microsegmentation

Cisco Secure Workload provides your team with automated microsegmentation policy recommendations and then helps you enforce those policies consistently at scale across all your environments. This model significantly **reduces your attack surface**, **increases operational efficiency** through automation, and **enables a zero-trust model.**

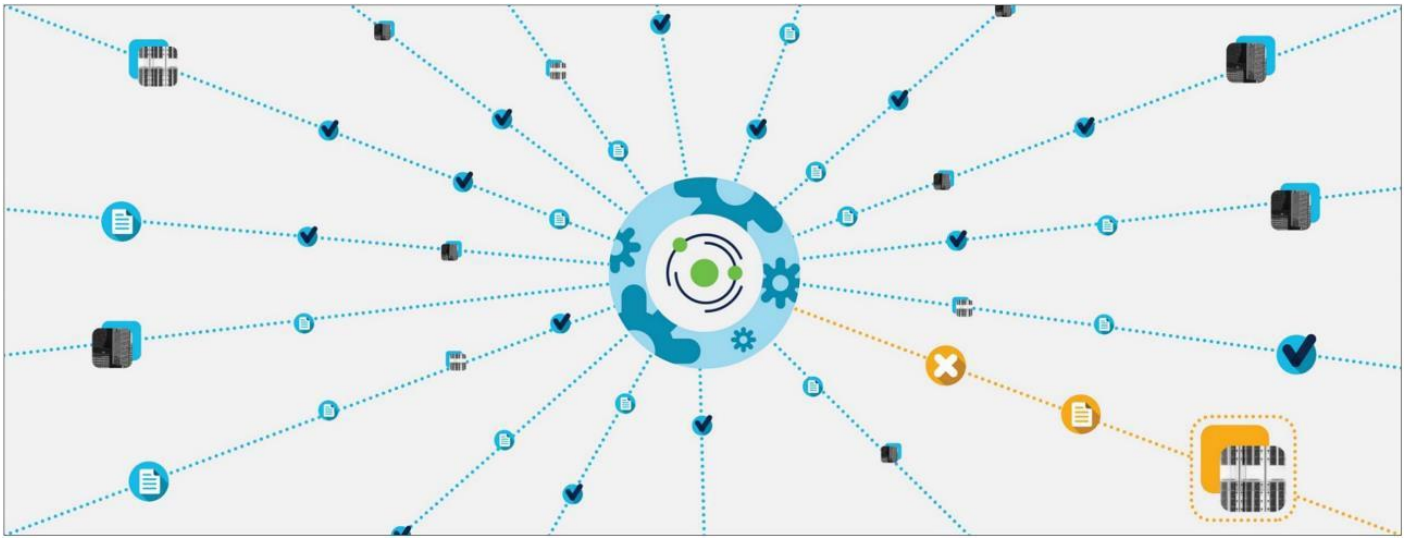

Figure 2. Secure applications using microsegmentation across any cloud

Flexible metadata-enriched policy definition

With the changing nature of application environments and the infrastructures across which they are deployed, a flexible, dynamic policy model is essential. Whether distributed across multiple clouds or operating on the same network segment, individual workloads have discrete policy requirements based on a rich set of attributes that define the application and environment, location, regulatory context, and much more.

To achieve this, Secure Workload maintains a context-rich inventory of every workload and endpoint along with associated metadata through integration with existing systems of record including Configuration Management Database (CMDB), IP Address Management (IPAM), orchestration platforms, access control, and authentication systems.

Secure Workload's natural policy definition language provides users with the ability to author and enforce dynamic policy intent to meet any demand, whether to ensure restricted user or endpoint access to a critical application, or to deliver against regulatory compliance or InfoSec mandates.

The policy is continually updated with the changing environment, which ensures up-to-the-minute policy delivery at each point of enforcement.

	Action	Consumer	Provider	Services
Regulatory Policy	Deny	Untrusted	Highly Sensitive	Any
Security Policy	Deny	Prod Workloads	Non-Prod Workloads	Any
Network Policy	Allow	Trusted Management	Mission Critical Retail	SSH
	Allow	Prod Workloads	Approved DNS	DNS

Figure 3. Flexible metadata-based policy definition

Automated microsegmentation policy recommendation

Using the Cisco Secure Workload platform, you can **automatically generate highly specific microsegmentation policies** based on complete visibility of application communications, running processes and their dependencies. It deterministically merges the autogenerated policy with the user-defined metadata-enriched policy allowing for a detailed policy visualization. Secure Workload empowers the user to review, test, and refine the policy to deliver an accurate and detailed policy set that can be deployed and enforced with confidence.

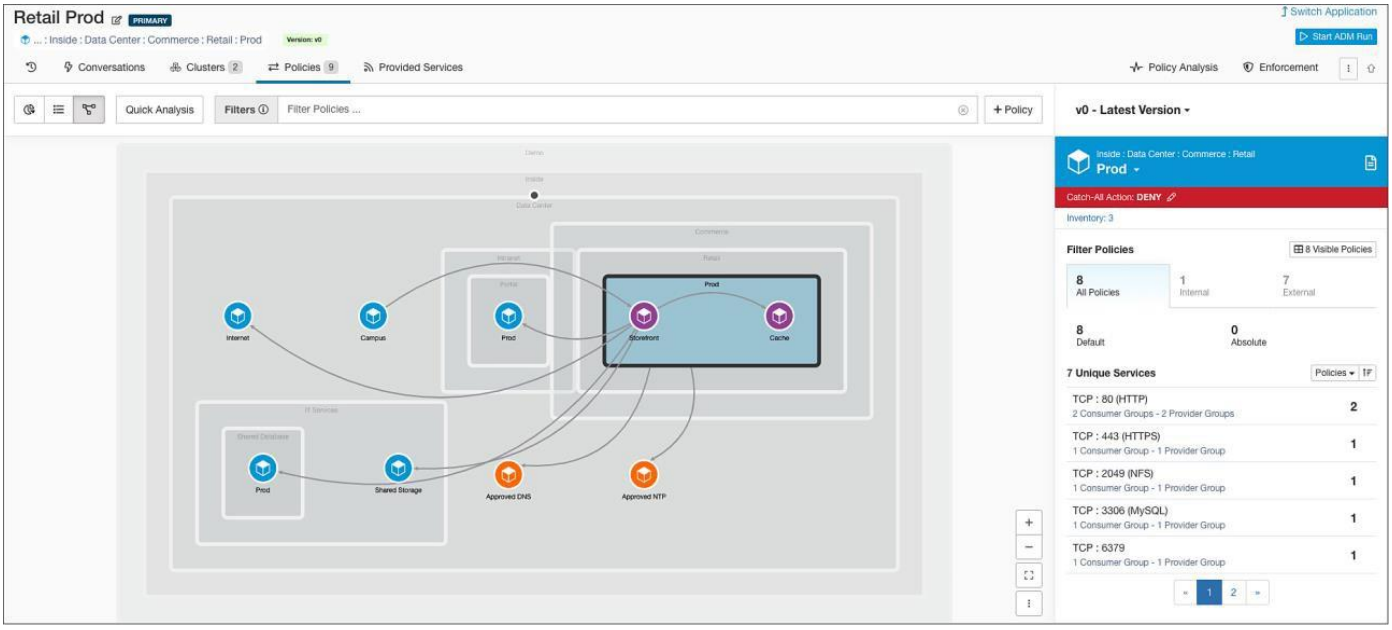

Figure 4. Automated microsegmentation policy recommendation based on application behavior

Application owners empowered with control

With Secure Workload, security no longer needs to be seen as an inhibitor to innovation because you are able to empower the application owners. Leveraging a hierarchical policy model and role-based access control (RBAC), application teams can deliver dynamic policy enforcement while operating within the bounds of the organizational policy requirements.

Figure 5. Application owners empowered with policy control

Policy flexibility can be achieved by using workload tag assignment through integration with orchestration platforms covering virtual machine and container-based workloads. Continuous Integration/Continuous Deployment (CI/CD) workflows are automated through API-driven policy sets, while maintaining end-to-end consistency across organizational boundaries.

Secure Workload's dynamic policy model also provides the ability for automated policy response such as for a quarantine or hardening action that may be triggered directly or by third-party integration via an API.

Automated policy enforcement at scale

Whether your environment consists of 100 workloads 100,000, Secure Workload is built for scale, providing fully automated enforcement of a dynamic allow-list policy to every workload. A discrete policy set is custom computed for each workload, distributed via the Secure Workload software agent, and programmed for enforcement by the native operating system firewall (either iptables or Windows Advanced Firewall).

The generated policy intent is also streamed across a secure Kafka broker for further enforcement in the infrastructure and delivered to ADCs through direct integration to ensure consistent policy enforcement to all workloads across the data center, and cloud.

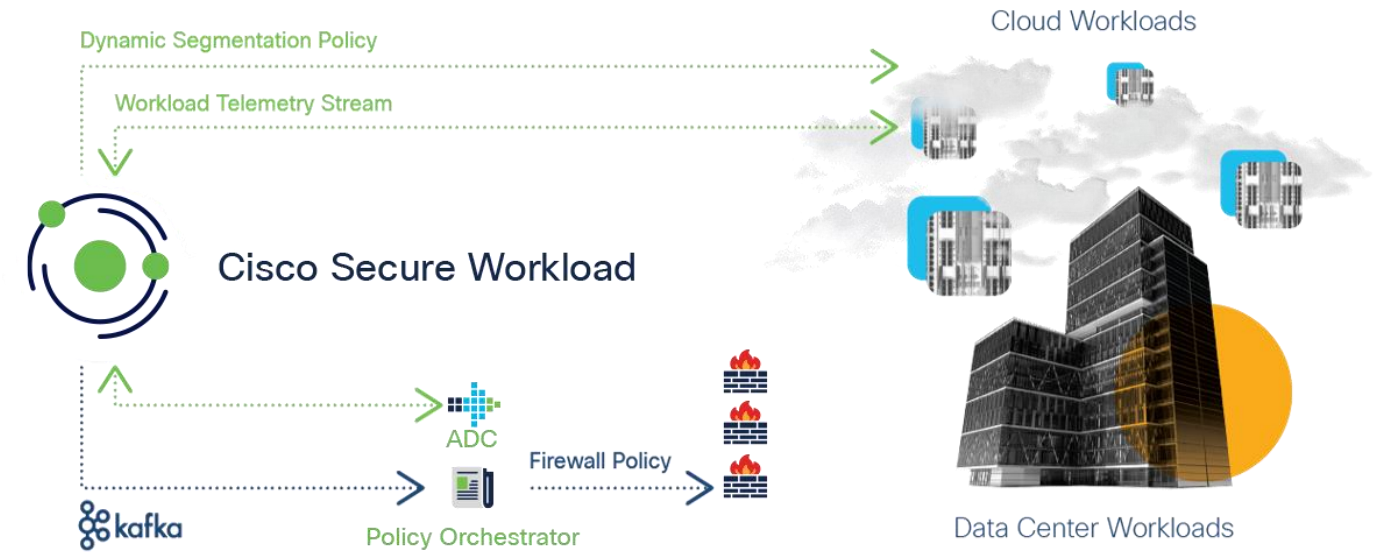

Figure 6. Policy enforcement across a multicloud infrastructure to enable consistent segmentation

Visibility and compliance in near real time

Secure Workload provides ongoing visibility of all communication activity with near real-time policy compliance assessment to quickly alert you to any policy violation. Flow records are retained for forensic record of all communications with analysis of flow disposition to identify the specific policy match. Whether responding to a breach or adapting to changes in application behavior, you will have a complete and up-to-date record of all communications to assist with rapid response and remediation efforts.

Reduce risks and maintain compliance

Cisco Secure Workload helps you reduce overall risks and maintain compliance by automatically identifying application behavior deviations and invoking appropriate workflows for policy updates. Analytics-based insights enable you to gain a unique perspective on your environment's operations and serve as a catalyst to increase efficiency and security.

Workload behavior baseline and anomaly detection

Secure Workload **continually monitors and baselines running processes on every server**, capturing detailed context for each process and its associated libraries. Process and library hashes are assessed against a threat data feed to identify malicious code execution and detect variation from known good processes.

Workloads are monitored for behavioral indicators of compromise through a configurable set of forensic event indicators. These forensic indicators include operating system event detections as well as a tailored set of MITRE ATT&CK techniques, identifying and alerting to anomalous behavior.

Security operations teams can customize these events, their severity, and associated actions using simple-to- define rules. In this way, security operations can quickly identify indicators of compromise and take remediation steps to minimize the impact.

Forensic event records provide a snapshot of the relevant process and metadata captured within the event to assist with exploit analysis.

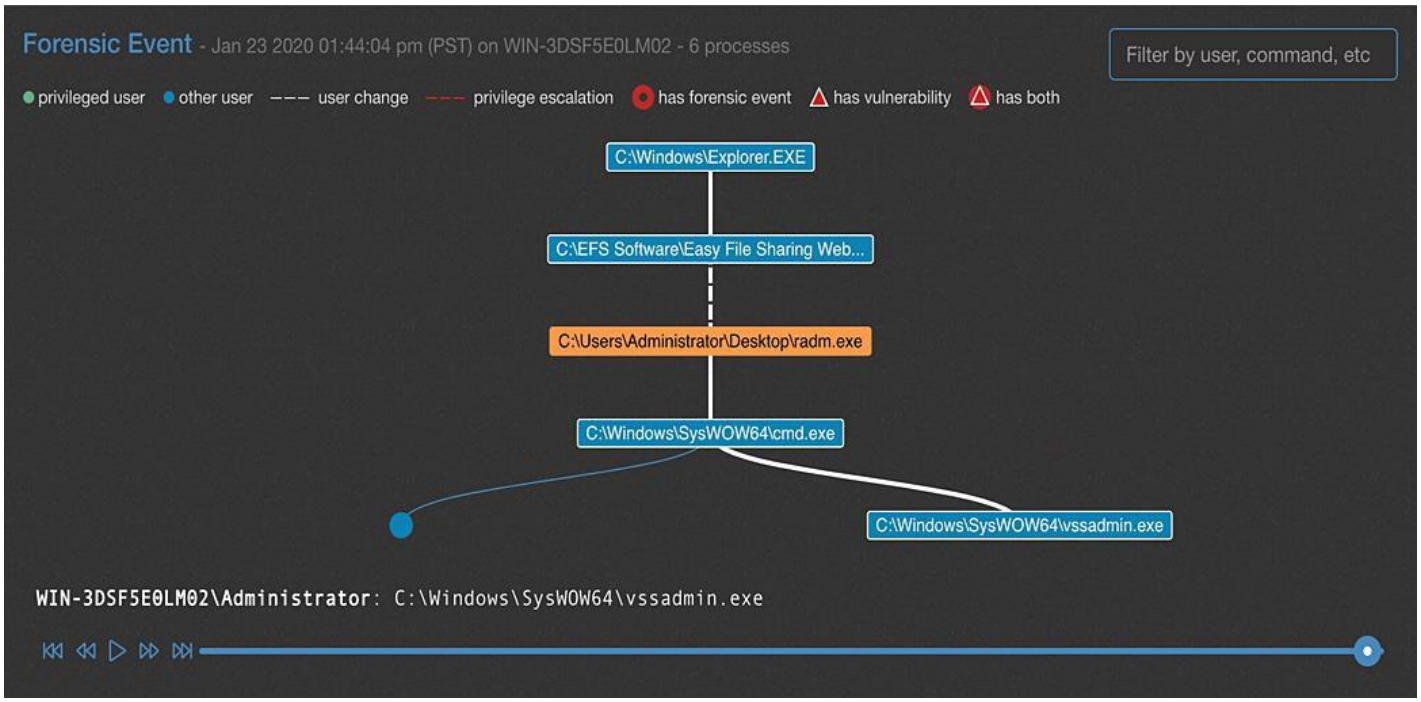

Figure 7. Forensic event

Proactive software vulnerability detection

The Cisco Secure Workload platform discovers the installed software packages and versions on your servers to report on known information security vulnerabilities by matching installed software versions against a vulnerability data feed that incorporates multiple sources, including National Institute of Standards and Technology (NIST) vulnerability database and vendor-specific updates.

Secure Workload allows you to quickly identify vulnerable workloads, enabling dynamic policy to be provisioned to protect these vulnerable machines from exploit or apply effective quarantine policy until the necessary patches are applied.

Figure 8. Software vulnerability detection and exposure details

Composite security dashboard for increased visibility

It is highly critical for security operations teams to understand both their security posture as a whole as well as the individual elements that are contributing to the current posture. This provides actionable data to further harden and remediate the environment against a potential breach.

Secure Workload's security dashboard **provides you with a composite security score** based on:

- Vulnerabilities associated with your software packages
- Process hash consistency and process behavior
- Workload attack surface assessment
- Segmentation policy compliance

The dashboard also helps you identify where to focus for improvement by providing the score breakdown for each of these elements.

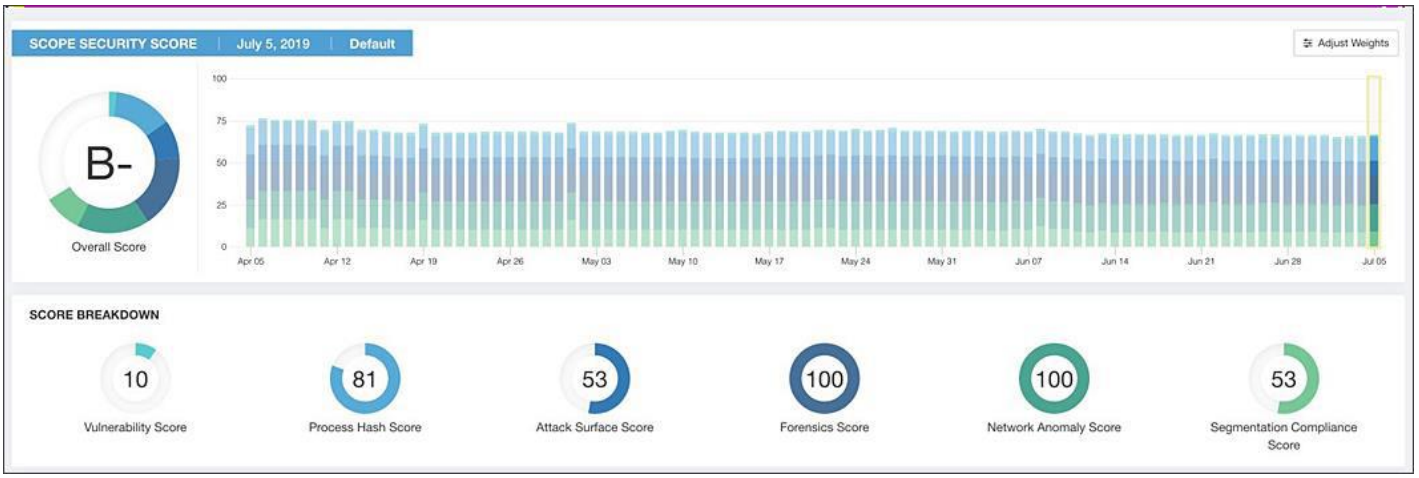

Figure 9. Security dashboard with composite security score

Features and benefits

Table 1 lays out the key features of the Cisco Secure Workload workload protection features and their benefits.

Table 1. Key features and benefits

Feature	Benefit
Zero-trust model using microsegmentation	• Make implementing microsegmentation within your environment a reality. • Secure Workload's automated approach helps accelerate deployment of microsegmentation. • Secure hybrid multicloud workloads and contain lateral movement using microsegmentation.
Extend policy definitions based on additional context	• Eliminate time-consuming manual creation of resource lists to segment applications. • Define microsegmentation default and absolute policies using meta-data tags (annotations). • Quickly develop consistent policies for applications using real-time annotations: ◦ Associate rich business context with the servers. ◦ Define policies based on users and user groups that need access.
Detect policy noncompliance events	• Track application policy compliance in real time. • Enable alerts for compliance events that can then be integrated with Security Incident and Event Management (SIEM) systems for investigation and remediation.
Software vulnerability tracking	• Get a baseline software inventory and the version information installed on servers. • Quickly identify if any of the package versions have known vulnerabilities or exposures, along with the severity. • Get an accurate inventory of all the servers that have the vulnerable package. • Tie this information to a policy that designates a specific action, such as quarantining a specific server.
Behavior-based workload anomaly detection	• Baseline the behavior or the workloads based on communication activities and processes on the workloads. • Proactively detect anomalous behavior and identify indicators of compromise. • Enable alerts for such events to be integrated with your SIEM systems for further security incident handling.
Rich context for users and endpoint devices	• Integrate with Cisco® Identity Services Engine (ISE) and Cisco AnyConnect® to get the user context, endpoint device posture, and other endpoint information. • Define policies to secure your applications and workloads from compromised endpoints or user information.

Cisco Secure Workload Platform details

Information regarding the deployment options, supported scale, supported operating systems, licensing, and ordering information can be found in the platform datasheet:

https://www.cisco.com/c/en/us/products/collateral/data-center-analytics/Secure Workload-analytics/datasheet-c78-737256.html?cachemode=refresh.

Cisco Secure Workload Software licensing terms

Secure Workload software-as-a-service (SaaS) deployment:

SaaS subscription is governed by the Secure Workload SaaS Offer Description (https://www.cisco.com/c/dam/en_us/about/doing_business/legal/OfferDescriptions/cisco_Secure Workload_saas_offer_description.pdf) and the Cisco Universal Cloud Agreement located at https://www.cisco.com/go/uca (or similar terms existing between you and Cisco) (the "Agreement"), and any software that you install is licensed under the Cisco End User License Agreement located at https://www.cisco.com/go/eula (the "EULA").

On-premises deployment models:

In addition to being subject to the Cisco EULA (see https://www.cisco.com/go/eula), Cisco Secure Workload software is subject to Cisco Supplemental End User License Agreement terms (SEULA; see https://www.cisco.com/c/dam/en_us/about/doing_business/legal/docs/cisco-Secure Workload.pdf).

Put Cisco Expertise to work 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 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.

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/c/en/us/products/security/Secure Workload/index.html or contact your local Cisco account representative.

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**.