Cisco Secure Workload (formerly Tetration)

Contents

Cisco Secure Workload overview

Q. Briefly, what is the Cisco® Secure Workload platform?

A. Cisco Secure Workload is a hybrid-cloud workload protection platform designed to secure compute instances in both the on-premises data center and the public cloud. These compute instances could be virtual machines, bare-metal servers, or containers. It uses machine learning, behavior analysis, and algorithmic approaches to offer this holistic workload protection strategy. This approach allows customers to contain lateral movement by implementing effective microsegmentation, proactive identification of security incidents using behavior analysis, and reduction of the attack surface by identifying software-related vulnerabilities.

Q. From the customers' point of view, why would they need the Cisco Secure Workload platform?

A. Applications are critical entities to any organization, with the workloads supporting them deployed across a multicloud environment comprising the data center and one or more public clouds. One of the key challenges customers face is how to provide a secure infrastructure for applications without compromising agility. Even today, the majority of data centers are designed with traditional perimeter-only security, which is insufficient. A new approach is needed to address this challenge. Cisco Secure Workload addresses this challenge in a comprehensive way using a multidimensional workload protection approach.

Q. What is driving the need for workload protection?

A. With the evolution of modern application architectures, enterprise data centers are growing larger and much more complex, with hundreds or thousands of interdependent applications. This is leading to a continual rise in complexity due to increases in east-west traffic, application onboarding, virtualization, containerization, security threats, and cloud migrations.

Organizations have an imminent need to protect their critical application workloads with a new approach to minimize lateral movement, reduce the attack surface, and more quickly identify Indicators of Compromise (IoCs). Cisco Secure Workload, using big data technologies, is a comprehensive, single platform that provides a ready-to-use solution to address all these requirements at any scale.

Q. Can you explain Cisco Secure Workload capabilities in simple terms?

A. The Cisco Secure Workload platform offers a ready-to-use solution that enables network security teams, security operations teams, and application owners to:

- Gain complete visibility into application components, communications, and dependencies to enable implementation of a zero-trust model to protect their application assets.
- Automatically generate microsegmentation policy based on application behavior. It also provides a mechanism for including any existing security policy based on business requirements.
- Enforce this microsegmentation policy across all multicloud workloads consistently, to minimize lateral movement.
- Identify software vulnerabilities and exposures to reduce attack surface.
- Provide process behavior baselining and identify deviations for faster detection of any IoCs.

To achieve these capabilities, Cisco Secure Workload uses both agent-based and agentless approaches to collect telemetry data, understand workload context, and enforce a consistent, distributed zero-trust segmentation policy at scale. Secure Workload also integrates with Cisco AnyConnect® and Cisco ISE (Identity Services Engine) to bring user and endpoint context into the segmentation policy. This allows administrators to define policies in order to restrict application access based on the user, user group, user location, or other user-related attributes.

Overall, the Cisco Secure Workload microsegmentation approach helps contain lateral movement between workloads across any data center or cloud environment through zero-trust segmentation controls.

Q. How can customers find out more?

A. Go to www.cisco.com/go/secureworkload.

Architecture and use cases

Q. What is the software architecture for the Cisco Secure Workload platform?

A. Figure 1 shows the architecture.

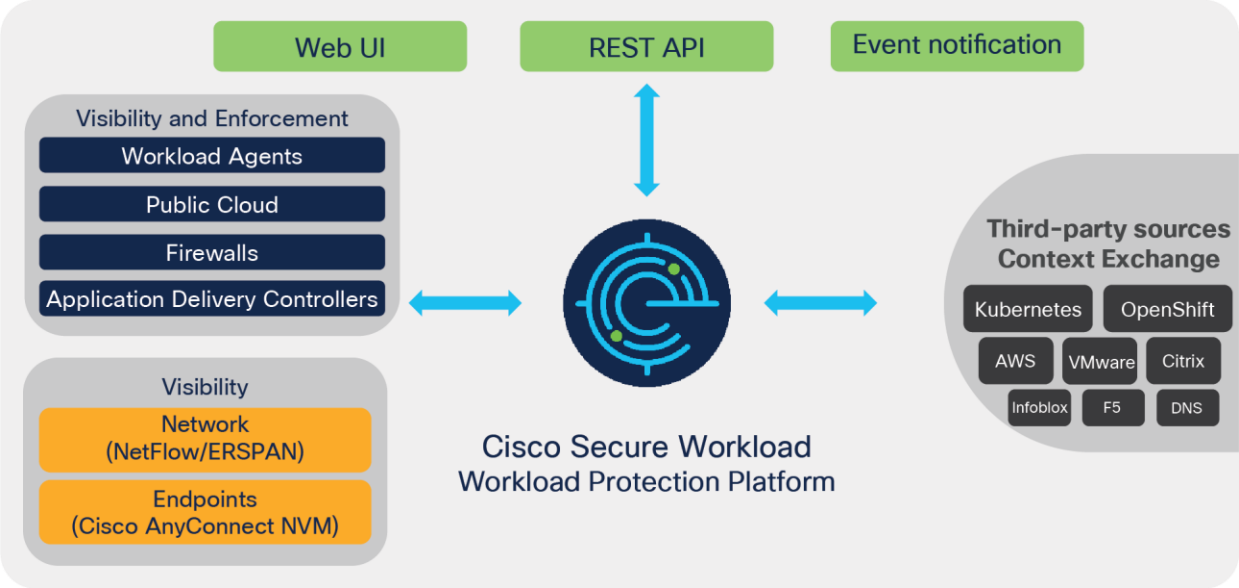

Figure 1.
Cisco Secure Workload architecture

Q. What are Secure Workload agents?

A. Secure Workload agents are installed on the server workloads (virtual machine, bare metal, or container host). Agents are available for major distributions of Linux, Microsoft Windows servers, Microsoft Windows desktops, and IBM AIX environments. These agents collect data from the workload, including all communication activities, process data, and software package details. They also provide an enforcement point for microsegmentation policy through direct control of the native operating system firewall.

Q. What are AWS connectors?

A. The AWS connector provides agentless workload security through integration with the customer's Amazon Web Services cloud environment. Capabilities offered include flow telemetry collection (VPC Flow Logs), labels and other metadata from EC2 workload instances, agentless policy enforcement (Security Groups), and ingest of workload metadata from Elastic Kubernetes Service (EKS). This delivers full visibility and a consistent segmentation approach for workloads deployed in an AWS environment without the requirement for agent deployment.

Q. What are Secure Workload Flow Ingest Connectors?

A. Deployed in a Secure Workload Ingest Virtual Appliance, Secure Workload supports a range of telemetry sources, including network data sources such as NetFlow/IPFIX, Application Delivery Controllers (ADCs) and firewalls (Cisco Adaptive Security Appliance [ASA]/Cisco Secure Firewall Firepower® Threat Defense [FTD]) along with endpoint data sources such as Cisco AnyConnect Network Visibility Module (NVM).

Q. What are NetFlow connectors?

A. The NetFlow connector is designed to generate Cisco Secure Workload telemetry data from NetFlow v9 or IPFIX records. NetFlow v9 and its standardized variant IPFIX provide flow information from a wide range of networking devices including routers and switches, Application Delivery Controllers (ADCs), and firewalls. NetFlow and IPFIX-enabled devices (flow exporters) perform local processing of packets to create a set of flow records that are then sent to the NetFlow connector as a collector instance.

Q. What are ERSPAN connectors?

A. These out-of-band sensors are designed to generate Cisco Secure Workload telemetry data using copies of network packet headers delivered from the network infrastructure through Encapsulated Remote SPAN (ERSPAN) configuration. These packet headers are delivered to ERSPAN sensors running in a virtual appliance as a truncated traffic stream. These ERSPAN sensors strip the ERSPAN header and process the original packet header data to generate Cisco Secure Workload telemetry data. This approach can be used to extend visibility into parts of the network where it's not feasible to deploy software agents.

Q. What are ADC connectors?

A. Through direct involvement in L4-L7 stateful forwarding of client-server connections, Application Delivery Controllers (ADCs) such as F5 BigIP or Citrix Netscaler can source IPFIX data to an ADC connector. As a source of Secure Workload flow telemetry, this ADC flow data also provides additional context for flow stitching, providing valuable context for operational visibility. ADCs also support enforcement of policy for workloads for which they are providing application services, extending both visibility and policy enforcement for specific parts of the network where it's not feasible to deploy an agent.

Q. What are Cisco ASA connectors?

A. Cisco ASA and FTD firewalls support NetFlow v9 in the form of NetFlow Secure Event Logging (NSEL). The ASA connector collects the NSEL data for processing as a Secure Workload flow telemetry source. NSEL provides a stateful, IP flow tracking method that exports state change and significant status events such as flow-create, flow-teardown, and flow-denied for all tracked flows. NSEL also generates periodic flow-update events to provide periodic byte counters over the duration of the flow, similar to traditional NetFlow.

Q. What are Cisco AnyConnect connectors?

A. The Cisco AnyConnect connector is designed to collect Network Visibility Module (NVM) telemetry from Cisco AnyConnect agents running on the endpoint devices such as laptops, desktops, and smart phones. This telemetry data is ingested into Secure Workload platform for two primary purposes:

1. To provide visibility into user activities and their communication with the business applications being protected
2. To extend the microsegmentation policy to include user and device context and, based on this, to allow or restrict access to the applications

Q. What are Cisco Identify Services Engine (ISE) connectors?

A. Cisco Secure Workload integrates with Cisco ISE through an ISE connector that subscribes to a real-time context feed from PxGrid. This context includes user and group information, endpoint profile, device posture, and Source Group Tags (SGTs) that allow for dynamic policy definition and enforcement with user/endpoint-specific rules to enhance and extend workload policy control.

Q. How do users access information from the Cisco Secure Workload platform?

A. Cisco Secure Workload enables user access through an easy-to-navigate and scalable web UI with programmatic access through an extensive set of Representational State Transfer (REST) APIs. In addition, Secure Workload provides a Kafka-based push notification to which northbound systems can subscribe to receive notifications about policy compliance deviations, flow anomalies, etc. Configurable alerting options also include syslog, email, Slack, Kinesis, and PagerDuty.

Q. Does this approach leverage big data and analytics?

A. Yes, it is big data analytics. Without using big data analytics, the speed and scale required to support workload security use cases cannot be achieved. We use these advanced technologies to address the use cases out of the box, thereby eliminating any need for advanced analytics capabilities to operationalize the platform. Big data focuses on the technology. We focus on the use case.

Q. What use cases are supported by the Cisco Secure Workload platform?

A. The platform supports the following use cases:

- **Application behavior insight:** Identify application components and their in-depth dependencies.
- **Automated microsegmentation policy generation:** Generate consistent microsegmentation policy based on application dependencies.
- **Automated policy enforcement:** Enable effective application segmentation using consistent policy enforcement in a heterogeneous environment to provide zero-trust control and restrict lateral movement.
- **Policy compliance:** Detect policy deviation in minutes and help ensure application policy compliance.
- **Process behavior baseline and deviation:** Collect the complete process inventory along with the process hash information, baseline the behavior, and identify deviations.
- **Software inventory and vulnerability detection:** Identify all the software packages and versions installed on the servers. Using the Common Vulnerabilities and Exposures (CVE) database and additional data feeds, detect if there are any associated vulnerabilities or exposures and take action to protect against active exploit.
- **Forensic analysis:** Detect anomalous or malicious workload behaviors as possible indicators of compromise with full granularity, for forensic analysis.

Q. What are the workload security use cases offered by Secure Workload beyond microsegmentation?

A. In addition to microsegmentation, Secure Workload offers multidimensional workload protection capabilities, which not only provide for reduction in workload attack surface, but also extend visibility to the operating system process level for deeper forensic monitoring. Explained further:

- **Server process baseline and behavior deviation:** Cisco Secure Workload collects and baselines the process details running on each of the servers. This information includes process ID, process parameters, the user associated with it, process start time, and process hash (signature) information. The platform maintains an up-to-date process hash verdict feed comprising known benign and flagged process hashes and compares process hashes across workloads to detect anomalies. You can search for servers running specific process or process hash information and get a tree-view snapshot of all the processes running on a server. The Cisco Secure Workload platform has algorithms available to track behavior pattern changes and find similarities to malware behavior patterns, for example, a privilege escalation followed by a shell code execution. Secure Workload raises security events for such behavior deviations. Security operations teams can customize those events, their severity, and associated actions by using simple-to-define rules. Using this information, security operations can quickly identify IoCs and take remediation steps to minimize the impact.
- **Software inventory and vulnerability detection:** The Cisco Secure Workload platform baselines the installed software packages, package version, patch level, and more for every workload. The platform maintains an up-to-date CVE data feed from multiple sources, including NIST and OS vendor data packs, which contain the latest vulnerability and exposure information. Using this, Secure Workload checks whether the software packages have known information security vulnerabilities. When a vulnerability is detected, complete details—including the severity and impact score—can be found. You can then quickly find all the servers with the same version of the package installed for patching and planning purposes. Security operations can predefine policies with specific actions, such as quarantining a host when servers have packages with certain vulnerabilities.

Product details

Q. The Cisco Secure Workload platform uses an allow-list security model with the ability to combine allow and block rules within a powerful policy model to deliver flexible segmentation outcomes. What is the difference between a block-list model and an allow-list model?

A. The block-list and allow-list models differ as follows:

- **Block-list:** I know you're a bad person by your name. You can't come in. Anyone I don't know can come in by default. This has been the traditional security model for many years.
- **Allow-list:** Nobody can come in unless I know their name and trust them.

Q. Why is an allow-list model better?

A. The allow-list model provides proactive protection based on a detailed policy that is modeled on specific application requirements to deliver least privilege access and restrict lateral movement within the environment. A zero-trust model requires an allow-list policy.

Q. Where is the microsegmentation policy enforced?

A. Microsegmentation policy should be enforced within or as close to the workload as possible to restrict lateral movement according to the defined policy. Secure Workload primarily enforces using the operating system firewall capabilities of the workload via an agent deployed to the workload operating system. These agents orchestrate the policy using IP sets and iptables in Linux-based servers (including Kubernetes nodes) and either Windows Filtering Platform (WFP) or Windows Advanced Firewall (WAF) security functions in Microsoft Windows servers. Policy is also consistently enforced through integrations with AWS for delivery through Security Groups (with or without agent deployment) and Cisco Secure Firewall through Access Control Policy (ACP) and Dynamic Objects. Policy may also be enforced in ADCs through native integration with F5 and Citrix or via third-party firewall infrastructure through orchestrator integration via Secure Workload's secure Kafka policy stream.

Q. Is the policy dynamically updated as the application environment changes?

A. Using rich contextual data, Cisco Secure Workload continuously tracks and updates the contextual status for every workload and endpoint within its inventory. Secure Workload policy is written in natural language form based on contextual inventory matching and automates the dynamic update of policy across all workloads on a continual basis. For example, if additional instances of a specific application component are added, Cisco Secure Workload will enforce the same policy automatically on those instances and update all related policy groups to adapt to the changes in workload population. Also, if the workload moves, policy moves with it; no additional action is required from administrators.

Q. Can the Cisco Secure Workload platform send notification when policy deviations are identified?

A. Yes. Cisco Secure Workload supports northbound notification through multiple mechanisms. These can be through Kafka, syslog, email, etc. Any northbound system can subscribe to those notifications and take additional actions. For example, a Security Incident and Event Management (SIEM) system could subscribe to those events and open tickets automatically.

Q. When a software vulnerability is found, can Cisco Secure Workload be used to take action?

A. Yes, administrators can define policies associated with a specific vulnerability or based on a vulnerability score. Secure Workload will automatically enforce the specified policy to all servers that meet the criteria or that communicate with the vulnerable systems.

Q. What is the impact of enabling telemetry capture on the server CPU?

A. Software sensors are built in with self-monitoring capabilities and offer a Service-Level Agreement (SLA) with configurable thresholds that restrict CPU and memory utilization to avoid any potential overconsumption of valuable server resources. If the sensor exceeds the CPU threshold, the agent will apply selective filters to data collection until the agent's CPU utilization returns to within the SLA threshold.

Q. What OS versions do the software sensors support?

A. Please see the Cisco Secure Workload Platform Information page for the full list of supported operating systems: www.cisco.com/c/en/us/products/security/tetration/platform-info.html.

Q. How much network traffic does Cisco Secure Workload telemetry generate?

A. Cisco Secure Workload collects only metadata, not the packet itself; therefore, the bandwidth requirement is very low. The agents can be selectively configured for high-fidelity flow (5-tuple) or conversation-only (4-tuple) collection to provide choice between rich per-flow detail, or conversation-only data that provides reduced detail with further reduced bandwidth overhead and increased data retention.

Q. Is the Secure Workload platform hardened?

A. Yes. Cisco Secure Workload platform internally uses zero-trust, SELinux controls, certification-based authentication, and encryption to ensure that all communication to the cluster and within the cluster is secure.

Q. Is this an "open" platform?

A. Cisco Secure Workload is very open.

- All policies can be exposed on the Cisco Secure Workload platform (JSON, XML, or YAML).
- REST APIs allow customers to query information through northbound systems.
- Kafka provides a streaming interface to publish information to multiple consumers. This "push interface" enables the northbound system to subscribe to notifications and provides a secure policy stream for consumption by third-party security orchestration systems.

Deployment options, licensing, and pricing

Q. What are the deployment options for the Cisco Secure Workload platform?

A. The Cisco Secure Workload platform provides flexible on-premises deployment and software-as-a-Service (SaaS) options. Three deployment options are available:

- Cisco Secure Workload SaaS: Cisco Secure Workload software runs in the cloud and can be consumed by customers as a software service offering. The customer does not need to deploy or maintain any platform hardware or manage Cisco Secure Workload software with this offer. This deployment model scales to tens of thousands of workloads.
- Cisco Secure Workload-M (small form factor): This deployment option consists of 6 servers and 2 Cisco Nexus 9300 switches. This platform supports up to 5000 workloads with detailed flow telemetry, or up to 10,000 workloads with conversation-only flow telemetry.
- Cisco Secure Workload platform (large form factor): This deployment option consists of 36 servers and 3 Cisco Nexus 9300 switches. This platform supports up to 25,000 workloads with detailed flow telemetry, or up to 50,000 workloads with conversation-only flow telemetry.

Q. How will I connect to Secure Workload SaaS?

A. Secure Workload architecture leverages secure, encrypted connections for data and control purposes between any on-premises or cloud-based workloads or infrastructure and the Secure Workload SaaS platform. Connections are always established northbound to the Secure Workload SaaS platform and support the use of proxy for outbound connectivity. No VPN is required.

Q. What are the components of Cisco Secure Workload pricing?

A. Cisco Secure Workload pricing consists of two components:

- **Software license:** This component is the software subscription license for the software. The customer can choose a 1-, 3-, or 5-year term with annual billing or a prepayment option. Software licensing options are consistent across Secure Workload SaaS and On-Premises deployments. There are two types of licenses:
  - **Workload license:** Based on the number of workload equivalents (virtual machines, bare-metal servers, container hosts, or virtual desktop [VDI] instances) from which the telemetry data is collected, analyzed, and policy enforced.
  - **Endpoint license:** Based on number of endpoint devices from which telemetry or context is collected through Cisco AnyConnect or Cisco ISE.
- **Hardware platform (applicable for the on-premises deployment option only):** This is a hardware-based appliance option to be deployed on-premises to deliver Secure Workload within the customer's data center environment.

Q. Who are the target customers, users, and buyers?

A. Cisco Secure Workload is targeted at security architects, security operations, and line-of-business managers in any size organization who are responsible for zero-trust architecture and delivery of microsegmentation. Microsegmentation is a high priority for many applications and security architect

teams, and effective microsegmentation and consistent enforcement of policy across on-premises data centers, container environments, and public clouds are essential.

Ecosystem

Q. Are Cisco Secure Workload and AppDynamics® complementary?

A. Yes. Cisco Secure Workload and AppDynamics complement each other. AppDynamics focuses on Application Performance Management (APM) and uses instruments within the application (Java, .Net, C#, etc.), monitoring of individual application transactions, and associated performance metrics. Cisco Secure Workload is a security platform that delivers zero-trust segmentation and other workload security capabilities through both agent-based and agentless approaches across a hybrid multicloud environment.

Q. What is the value of an ecosystem?

A. The Cisco Secure Workload platform provides actionable insights to a wide range of security use cases. Ecosystem partners can consume the policy recommendations from the platform and implement coarse-grained enforcement within the data center network or at the data center perimeter. They can also query the workload profile information from the Cisco Secure Workload platform through the REST API and implement their own logic.

Q. Which external platforms are part of the Cisco Secure Workload ecosystem?

A. Cisco Secure Workload has a broad set of ecosystem partners. These partners are classified into the following categories based on use cases:

- **Context exchanges:** VMware vCenter, Kubernetes, Openshift, ServiceNow, AWS resource tags, Infoblox, and DNS servers
- **Security orchestration:** Algosec, Tufin, and Skybox
- **Application delivery:** Citrix and F5

Full details about the ecosystem partner integrations can be found in our solution overview documents: www.cisco.com/c/en/us/products/data-center-analytics/Secure Workload-analytics/solution-overview-listing.html.

Solution deployment and services

Q. What is delivered to the customer site for on-premises deployments?

A.

- If the customer is deploying either a Cisco Secure Workload or a Cisco Secure Workload-M (SFF) solution, it is racked, stacked, and connected with base software loaded before it ships to the customer's facility. The customer needs to provide basic setup information about the environment and install the system software to complete the setup process.
- Cisco Secure Workload is built on Cisco Unified Computing System™ (Cisco UCS®) C-Series Rack Servers and incorporates Cisco Nexus 9300 switches for an integrated high-performance network.
- Cisco Services experts can assist the customer to integrate Cisco Secure Workload in their environment, support the development/discovery of segmentation policy for zero-trust enforcement, and enable deeper workload security.
- Cisco Solution Support for Cisco Secure Workload provides centralized support for both Cisco and solution partner technologies. One service combines software, hardware, and solution-level support to streamline the support experience for this multivendor solution.

Q. What Cisco services are available to support Cisco Secure Workload customers today?

A. The following Cisco services are available:

- Cisco Secure Workload includes solution support services to help organizations get the most value from the solution.
- The Cisco Secure Workload QuickStart Service is offered with the Cisco Secure Workload platform to help ensure that customers can successfully consume (adopt) the solution. Key deliverables include an as-built document, an operations runbook summarizing policies and endpoints, and transfer of knowledge to in-house staff to help staff understand the capabilities of the platform.
- Cisco Secure Workload customers also receive solution-focused expertise with centralized issue management and resolution among Cisco and solution partner products through Cisco Solution Support. Cisco Solution Support features and benefits include:
  - A primary point of accountability for resolving issues no matter where they reside, streamlining support from first call to resolution
  - A coordinated support framework with solution partner support teams, eliminating brokering support conversations
  - Solution-level expertise that results in faster time to resolution for complex issues
  - A single service for Cisco hardware, software, and solution-level support

Q. Does Cisco offer additional services for customers who would like access to Cisco Secure Workload expertise beyond the initial deployment?

A. Yes. Customers can engage with Cisco's Customer Experience (CX) team to help with deployment, optimization, and operations over the lifetime of their subscription.

Cisco Services experts have deep experience and cross-technology expertise in workload security and also collaborate with Cisco Secure Workload engineering teams.

Channels

Q. Who can sell the Cisco Secure Workload platform?

A. Any Cisco partner can sell Cisco Secure Workload. There is no specific Cisco Authorized Technology Partner (ATP) requirement.

Q. With what customers should partners position the Cisco Secure Workload platform?

A. Cisco Secure Workload provides value to a broad range of customers. Target verticals include, but are not restricted to, financial, healthcare, defense, intelligence, and other industries in which security and compliance are primary concerns.

How to buy

To view buying options and speak with a Cisco sales representative, visit https://www.cisco.com/c/en/us/buy.html.

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 C67-737402-10 12/21