Secure Workload

(formerly Tetration)

Cisco Partner

https://cs.co/1page

Cisco Secure Workload delivers a zero-trust approach using segmentation to secure application workloads for a SaaS (multicloud) and on-premises data center environments by reducing the attack surface, preventing lateral movement, identifying workload behavior anomalies, and remediating threats quickly.

Benefits:

Implement a zero-trust based model: By using advanced algorithms, Secure Workload generates a granular segmentation policy for each application.

Contain lateral movement: The platform provides consistent microsegmentation through workload operating system capabilities across the multicloud infrastructure.

Identify workload behavior deviation: Behavior of the workloads can be determined by baselining the processes that are running on the server and identifying any deviations in behavior from those baselines.

Detect vulnerabilities: Identify installed software packages, versions etc. Using this, check whether any of the package has known vulnerability listed in CVE database.

Compliance and auditability: Monitor application components and detect any segmentation policy compliance deviations in minutes and trigger a notification.

Cisco Secure Firewall integration: Leverage a true defense-in-depth strategy with unified segmentation policies. Secure Workload can enforce coarse macro policies to Secure Firewall to enhance the security posture of the network.

Endpoint visibility with Cisco ISE and AnyConnect: Extend the zero-trust model to endpoints by defining least-privilege based on dynamic user or device information.

Forensic analysis: Detect anomalous or malicious workload behaviors as possible indicators of compromise with full granularity, for forensic analysis.

Mentored Install Network Training (MINT)**:** Provides partners access to Digital Solution Integrators (**DSI**) who can lead mentored proof of value and install engagements for technologies across the portfolio including Secure Workload.

Components:

Secure Workload-SaaS: *Cloud*

- Offers workload protection features without any on-premises hardware
- Delivers faster onboarding to realize the benefits of the platform quickly

Secure Workload (L): *On-prem*

- Supports up to 25,000 workloads (VM/bare-metal) per cluster

Secure Workload (M): *On-prem*

- Supports up to 5,000 workloads (VM/bare-metal) per cluster

Use Cases:

Application behavior insight: Identify application components and their in-depth dependencies.

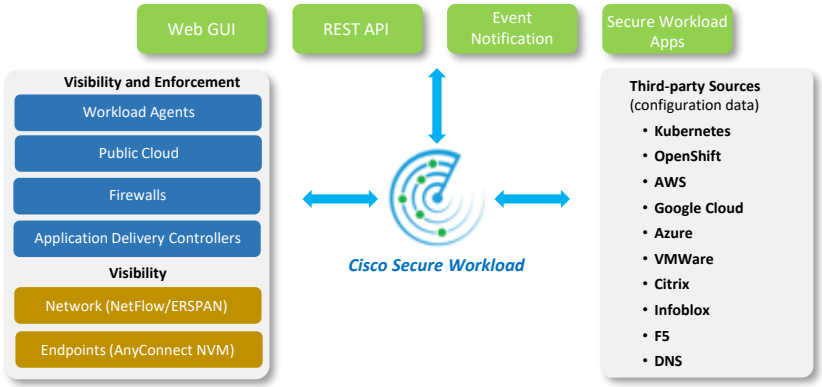
Automated policy Enforcement: Enable effective application segmentation using consistent policy enforcement in a heterogeneous environment to provide zero-trust control and restrict lateral movement.

Process behavior baseline and deviation: Collect the complete process inventory along with the process hash information, baseline the behavior, and identify deviations.

Detect vulnerabilities: Baseline installed software packages, package version, and patch level. Using this data, the platform checks whether any software packages have known information-security vulnerabilities.

Forensic analysis: Detect anomalous or malicious workload behaviors as possible indicators of compromise with full granularity, for forensic analysis.

Policy Compliance: Detect policy deviation in minutes and help ensure application policy compliance.



Resources:

SalesConnect
Order Guide
Data Sheet
User Guide
FAQ
At-a-Glance
Agent Support Matrix
YouTube Channel
Public page

Example SKU: ***T1-TETRATION***