Cisco Secure Workload – Messaging And Positioning

- Cisco Secure Workload Messaging
- Cisco Secure Workload Champions page
- Latest Updates

Training

- **Youtube Series:**
    - Cisco Secure Workload Design & Implementation Series
    - General Topics
    - VDI Segmentation
    - Secure Firewall Integration
- **Cisco Learning Network:** Tetration Virtual Bootcamp

Demo and Test Drive

- **Demo Example:** Demo Example Link
- **Test drive or proof of performance:** Test Drive Link

Proof of Value

- **Templates, Presentation, Guide:** Proof of Value Documents
- **Proof of Value Request Form:** Request Form Link
- **BDM Deck:** BDM Deck Link
- **Technical Decision Maker (TDM):** TDM Link
- **Competitor Comparison:** Comparison Link
- **Proposal Template for Cisco Sales:** Proposal Template Link
- **RFP Submittal Questions and Answers:** RFP Questions Link

Key Differentiators and Strength of Cisco Secure Workload

1. Unified Solution for Micro-Segmentation

CSW offers agent-based and agentless microsegmentation for bare metal, virtual machines, and containers; located on-premise, in hybrid, or multi-cloud environments. All of this done through single platform and through single UI.

Agent Based covers: Windows 10, Windows 11, Windows Servers, Linux (RHEL, Oracle, Ubuntu, AWS Linux, Centos, Debian, SUSE, Alma and Rocky), RHEL and SUSE on IBM Power and IBM z/Systems, AIX, Solaris (Solaris 11.4 on x86_64 and SPARC architectures), Kubernetes, OpenShift, AKS, EKS, and GKE.

Agentless approach: through native integration with Cisco Secure Firewall, F5 and Citrix ADCs, Firewall Orchestrators (AlgoSec, Tufin and Skybox), Security Groups in AWS, NSGs in Azure, GCP built-in firewall.

2. NVIDIA Bluefield Data Processing Units (DPU)

Cisco Secure Workload and NVIDIA DPU integration allows the offloading of Secure Workload Agent functionality from hosts to Nvidia Bluefield DPUs. This integration will enhance application performance, scalability, and administrator productivity. The agent deployed on the DPUs gathers the flow telemetry and enforces the policy on the DPU to achieve microsegmentation.

3. Extensive labeling and robust orchestration ecosystem

CSW follows an automation-first approach, offering a range of integrations for workload inventory/metadata ingestion.

It supports 32 manual labels along with unlimited labels from orchestrators/automation.

Automated Context Ingestion through native integration with:

- ServiceNow
- Cisco ISE and Active Directory
- DNS Servers & Infoblox
- VMware vCenter
- Public cloud platforms: AWS, Azure, GCP
- Kubernetes environments: Managed K8s - AKS, EKS, OpenShift and unmanaged K8s

This allows us to construct logical groups for policy, which are dynamic and evolve with the ongoing change in the customer environment. In addition, CSW automatically discovers, and groups, workloads together based on their role within the application. There is no requirement for CMDB integration or manual effort from engineers to provide additional label information for server types. CSW analyzes live traffic flows across various applications, regardless of if they connected to the virtual or physical fabric allowing for a sizable and complex ADM with intra and inter dependencies and communications.

4. Flexible and Hierarchical Policy Model

Hierarchical Policy: Cisco Secure Workload allows breaking the policy into smaller subsets of rules such as "Shared Service Rules" and "App Specific Rules". Secure Workload allows you to build an Organizational Structure and customize it in a way that meets your organization needs. Using inventory Labels, we can break down an IP scheme of an organization into manageable blocks called scopes. Scopes are organized in a tree structure, with a Root Scope at the top of the tree which represents all IP addresses; both internal and external. Each leaf of the scope tree is tied to a query, with the queries typically being more broad at the higher levels of the tree and becoming more specific as you traverse down the tree structure until at the bottom of the tree we are matching workloads that are specific to an application. Scopes provide a hierarchy and structure to the inventory which will be useful for assigning policies and user roles for each of these blocks.

This allows user to create very broad policy to represent corporate policy by applying it at Root level. for example "Dev can't talk to Prod". At next level you can define one or more "Shared Services Rules" that are common across the organization or across a particular location or environment, such as DNS, Active Directory once in the higher level scope and have those policies applied across all workloads. while applying policy that is required specifically for the application to function at the lower-level application scopes.

With this scope hierarchy, policy can be applied at any level of the tree and will be collapsed into a single policy that will be applied on matching workloads.

CSW supports both Allow and Deny policy actions and it has unified view of all allow and deny rules on a per-application basis.

Others don't support hierarchal model and they are using whitelisting methodology, the absence of any rule to allow traffic implies traffic must not be allowed.

You may not feel the limitation of whitelisting methodology in beginning of deployment or while you are testing the micro segmentation solution in your environment. But we live in a nonideal world, exceptions and risk acceptance are part of any business, so we need to make sure that the micro segmentation solution supports all business cases that we currently have and what we may have in future. We should be able to allow and deny policies similar to way we are currently do on firewalls, also we should be able to use all possible attributes to build the required policies.

5. Host based microsegmentation leveraging OS native tools

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. Without the need to install proprietary host firewall that introduces the following risks:

- Proprietary host firewall is inline with traffic, making it a point of failure and may impact the running applications
- Proprietary host firewall can be running in Kernel space firewalling - Kernel Intrusive: The agent has a direct kernel hook
- Proprietary host firewall requires reboot with installation, uninstall and update
- Proprietary host firewall may cause kernel crash for compatibility issues or when OS is patched or updated

6. Intelligent Policy Generation

AI/ML powered intelligent policy generation: Unsupervised Machine Learning for application dependency mapping, while others leverage templates, manual configuration of groups and limited environment automated grouping, CSW can automatically discover ANY application exactly the way that a customer has deployed. This is because CSW leverages advanced machine learning techniques for discovery. This significantly improves the accuracy and granularity of the policy that CSW discovers over others. ADM has no hard dependency on manual tags and can look at the flows & workload behavior to intelligently identify workload groupings. ADM can be fine-tuned to generate coarse policies for ringfencing or fine policies to microsegment down to each unique workload.

ADM can be fine-tuned to:

- Generate coarse policies for ringfencing or fine policies
- Generate granular micro-segmentation policies unique to each workload
- Exclude conversations that match specific filters

7. Behavior Anomaly Detection

CSW supports process and network behavior anomaly detection, it builds baseline that provides insight into process identification, parameters, associated users, start times, and hash information. Then applies behavior analysis and statistical models incorporate with MITRE ATT&CK techniques to identify and track behavior pattern changes and determine exposure.

8. Native Vulnerability Scanning

CSW has native vulnerability scanning and it does not require any integrations with third-party vulnerability scanners, which allows build policies based on vulnerability CVE-IDs.

9. Native integration with Cisco Vulnerability management

Cisco Vulnerability Management uses proven data science techniques, including machine learning, natural language processing, and predictive modeling to assess, prioritize, and even predict risk. CSW allows to build a network-based policy based on Vulnerability Security Risk Score such as active internet breach, easily exploitable, fix available and malware exploitable, ...etc.

10. Virtual Patching

Secure Workload agents collects CVE data from workloads and push CVE information from Cisco Secure Workload to Cisco Secure Firewall Management Center to augment the threat protection capabilities of the firewalls to protect the workloads from known vulnerabilities and provide virtual patching as a compensating control using the IPS signatures on the firewall.

This feature may help user to automate IPS policy review task as CSW collects the existing vulnerabilities and Cisco FMC/Firewall/NGIPS will activate the required IPS signatures.