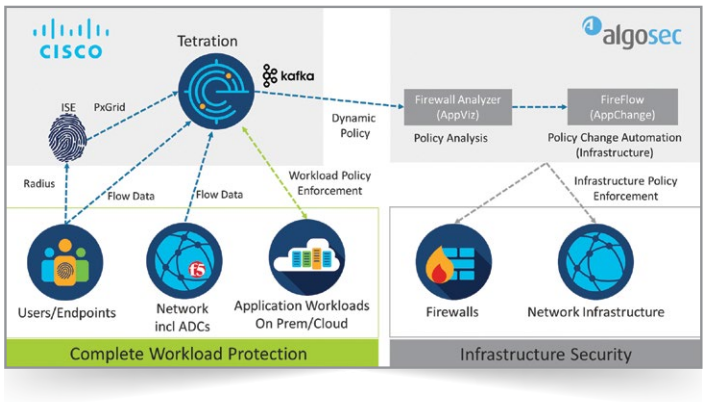
APPLICATION SEGMENTATION WITH CISCO SECURE WORKLOAD (TETRATION) AND ALGOSEC

Better Together: Cisco Secure Workload (Tetration) and AlgoSec

Cisco Secure Workload is an application workload security platform designed to secure your compute instances across any infrastructure and any cloud. Cisco Secure Workload extends security analytics and policy to multi-cloud apps. To achieve this, it uses behavior and attribute-driven micro-segmentation policy generation and enforcement. It enables trusted access through automated, exhaustive context from various systems to automatically adapt security policies. But, using Cisco Secure Workload alone, has some limits.

A Whole Network Approach

Cisco Secure Workload offers complete workload protection over users and endpoints, networks, including network ADCs, and application workloads, both on-premises and in the cloud. However, relying on Cisco Secure Workload alone does not enable infrastructure policy enforcement over your firewalls, SDN and cloud security controls



Enforcing Micro-segmentation Throughout Your Entire Network

Organizations need consistent segmentation policies, across application workloads and infrastructure. Cisco Secure Workload can help by publishing the segmentation policies over Kafka in real time. However, Cisco Secure Workload alone cannot enforce the policies on your security infrastructure. Cisco Secure Workload enforces micro-segmentation policies only within the native software and hardware sensors. The segmentation policies are not enforced on all on-premises, cloud and SDN technologies but only those that originate from Cisco Secure Workload. AlgoSec allows Cisco Secure Workload-enforced micro-segmentation policies to be applied beyond the native software and hardware sensors. AlgoSec extends the segmentation policy originating from Cisco Secure Workload

cisco Partner

Why Integrate AlgoSec with Cisco Secure Workload?

- Consistent security across your entire hybrid network, including multi-cloud and on-premises environments.
- Optimize and present Cisco Secure Workload-enforced policies to non-technical Business Application Owners, in an easy-to-understand business application view
- Expand native enforcement capabilities of Cisco Secure Workload beyond the native Secure Workload agent
- Leverage existing security technologies for micro-segmentation, to maximize current investment
- Extend implementation of micro-segmentation projects to legacy and appliance-based environments, as well as hybrid networks across the on-premises and public cloud environment.
- Implement defense-in-depth in your data center and cloud environments
- Make changes and secure your environment within minutes rather than days or weeks

to all supported on-premise, cloud, and SDN technologies. AlgoSec AppViz addon connects to the Secure Workload REST API and Kafka broker to collect enforced policies for the relevant applications and publishes the segmentation policies over Kafka in real time. AlgoSec AppViz collects all enforced policies, which will become application flows in AppViz. AlgoSec updates firewall rules or other infrastructure elements to enforce relative firewall elements.

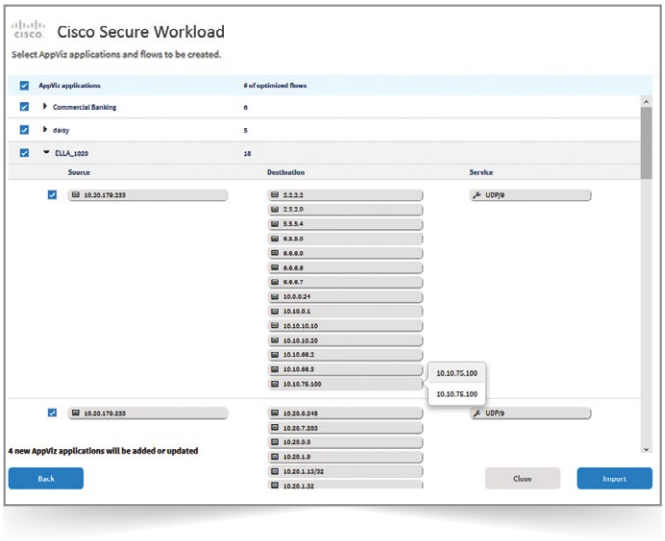
There are also instances where Cisco Secure Workload alone cannot enforce micro-segmentation policies on workloads. For such applications or application components, AlgoSec can orchestrate micro-segmentation policies as firewall rules.

Effectively Managing Risk, Vulnerabilities, and Compliance

A micro-segmentation project cannot be successful without managing risk, vulnerabilities and compliance in the context of affected business applications. A successful micro-segmentation strategy requires a clear understanding of what business applications map to which security rules.

By integrating Cisco Secure Workload with AlgoSec, AlgoSec AppViz addon discovers, identifies, and maps business applications, ensuring visibility of the network connectivity flows associated with each business application. This provides critical information regarding the firewalls and firewall rules supporting each connectivity flow.

As part of building and enforcing an organization's network segmentation policy, risk, vulnerabilities, and compliance should be managed in the context of impacted business applications. By using AlgoSec, you can prioritize vulnerability and patch management based on the affected business applications. You



can view aggregated information about the network security risks and vulnerabilities relevant to each business application.

AlgoSec is able to break down the applications identified by Cisco Secure Workload into their individual traffic flows. This makes the traffic flows readable, usable and easier to tie your business applications to security policies, as well as understand the entire traffic pathway. AlgoSec lets you understand the myriad maze of connectivity flows and discover the pathway to one single connectivity flow.

AlgoSec's AppViz provides a concise, human-readable view into business application connectivity, including:

- Automated application architecture
- Security governance zone overlay and diagram
- Optimized business application flows
- Automated mapping of business applications to downstream device changes.