tufin The Security Policy Company.

Technology Partner Solution Brief

# Extend Your Network Security Policy Management to Cisco ACI

The Tufin Orchestration Suite™ for Cisco ACI enables organizations to centrally manage their ACI and non-ACI environments as one, directly from Tufin. With Tufin, organizations can now gain full visibility, automate contract and corresponding firewall rule changes, conduct path analysis, detect access violations, and more, for Cisco ACI infrastructure, and the rest of the hybrid environment.

## Gain comprehensive visibility, with accurate topology modeling of the Cisco ACI Fabric and the rest of your IT environment

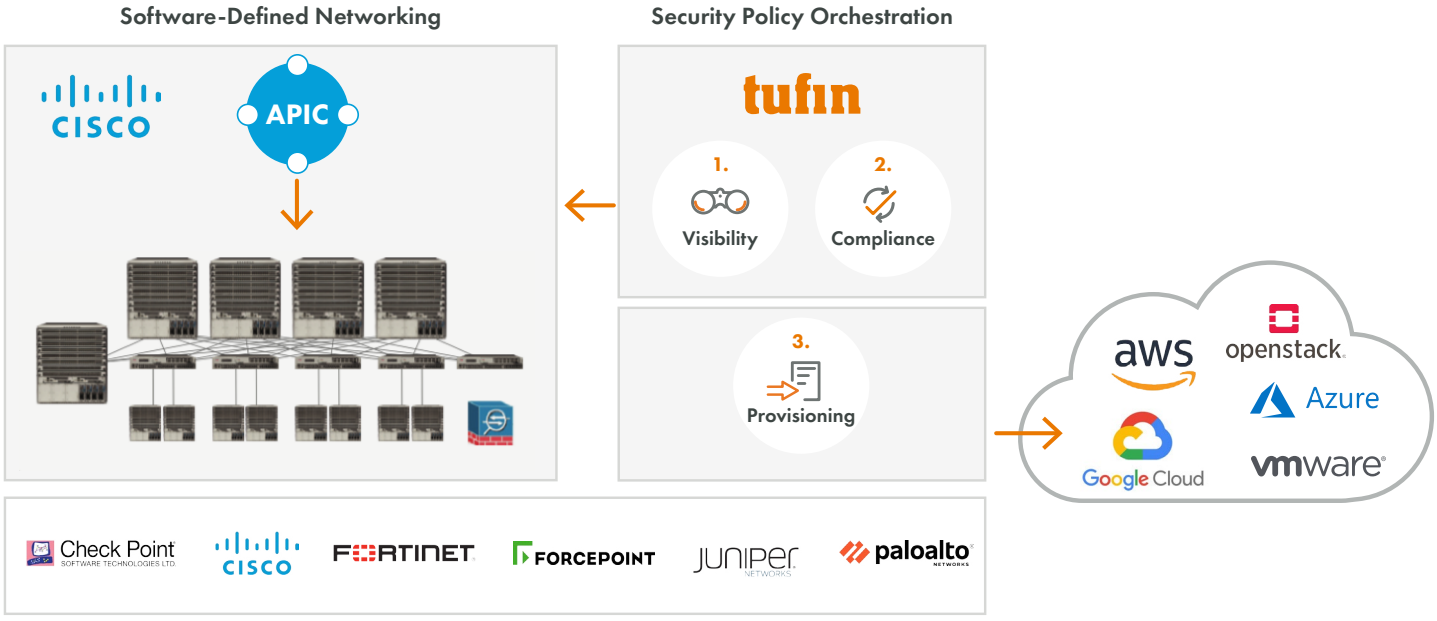
With end-to-end, real-time visibility into ACI objects and communications flows, as well as traffic traversing the ACI Fabric, users can monitor, detect, and remediate access issues within the ACI Fabric and across the hybrid environment.

## Apply consistent security policy and maintain compliance

Unify security policy management throughout your Cisco Application Centric Infrastructure (Cisco ACI) and the hybrid environment and eliminate security and compliance gaps. Tufin leverages security policy and third-party risk analysis data to analyze access changes, and detect anomalies and potential threats.

## Automate security policy changes for accelerated and secure app deployment

Automatically manage changes to ACI contracts, using Ansible, and corresponding firewall rules in the hybrid environment. Rapidly provision the right access for business apps deployed in the ACI Fabric and across the hybrid network, eliminating the risk of manual configuration errors.




Cisco Application-Centric Infrastructure with multi-vendor security policy orchestration from Tufin

# Visibility, automation, and compliance for Cisco ACI: Key Features

## End-to-end visibility within the ACI Fabric and across the hybrid environment

- Map out ACI objects (e.g. contracts, tenants, bridge domains, static/external EPGs, service graphs) as part of your overall hybrid environment
- Gain full visibility with accurate topology modeling of the Cisco ACI Fabric, and ingress/egress traffic traversing the ACI Fabric
- View a color-coded comparison between the new and old access revisions to easily visualize change revisions and differences
- Conduct path analysis between ACI objects (e.g. app profiles, contracts, tenants, bridge domains, EPGs) and non-ACI network objects to optimize and troubleshoot any access issues within the ACI Fabric, and between ACI to on-premise and cloud environments residing outside the ACI
- Map the selected access path or alert on unavailable traffic routes — view devices in the path, EPGs, and routing configurations inside and across the ACI Fabric. Path analysis is calculated across all network security devices throughout the hybrid environment, including the ACI Fabric. Based on the app's connectivity needs, rules that block traffic can also be changed.

## Segmentation policy management and automation

- Set and apply segmentation policies for business apps deployed in the ACI Fabric and across the hybrid environment
- Automatically manage access using customizable workflows and multiple Ansible playbooks
- Ensure accurate, optimized access changes – analyze L3 connectivity, service graphs, VRFs, contracts, and relevant EPGs, including network security devices outside the Cisco APIC
- Automate new contract creation between EPGs, as well as between EPGs and non-ACI assets (N/S traffic)
- Create/modify corresponding firewall rules across multi-vendor firewalls to enable access to non-ACI assets (e.g. on-premise database)
- Run Ansible templates and jobs directly from the Tufin app, for simple, automated and secure access changes
- Run proactive risk assessment against the security policy and vulnerability data, to ensure changes are not violating policies or introducing additional risks
- Configure specific conditions for the change, such as enable approvals within the Tufin app to be defined prior to executing an Ansible job
- ITSM integration provides unified change workflows, where opening a ticket in ITSM triggers a workflow within Tufin for automated change design and implementation

## Policy optimization & continuous compliance

- Automatically detect and alert on violations, misconfigurations, and out-of-band changes
- Provide actionable remediation information on detected risks
- Continuously optimize network access and troubleshoot connectivity
- Track and document rule changes (e.g. added contract, modified multi-vendor firewall rule)
- Automatically generate policy change reports (e.g. a contract was deleted from the policy) for audit and compliance purposes



DP20210405