Business Challenge

Organizations that have adopted DevOps practices, or empowered cloud operations to operate outside the purview of security, now have deployed applications with connectivity that was never assessed by security or documented by networking. These deployed applications span the private or public cloud as well as the on-prem and are the primary drivers of network changes and are responsible for seeking access to various resources. Security teams now need comprehensive visibility over their entire network's connectivity matrix to streamline change management and control unnecessary or risky access. Remediating inadvertently introduced risky access is necessary to eliminate the opportunities for attackers to easily traverse the network from the cloud to the on-prem network, and vis-a-versa, to ensure security across the network without impeding the business.

To regain visibility of the hybrid cloud and mitigate the risk posed by risky access, enterprises are using application telemetry security solutions to identify dependencies and persist that data in network security policy management solutions. This integration enables security teams to understand and orchestrate the connectivity between the on-prem and hybrid cloud, and identify unused or non-compliant access against the enterprise's security policy for remediation.

Solution Benefits

- Comprehensive Application discovery
- Visualization of connectivity dependencies and services
- Highlight policy violations in the context of applications
- Efficient network automation ensuring business continuity
- Adhere to compliance and regulations during changes stemming from application migration

Solution: vArmour Application Controller and Tufin NSPM

The vArmour Application Controller seamlessly integrates with Tufin's Network Solution Policy Management (NSPM) solution Tufin Orchestration Suite™. Application Controller provides rich application discovery to visualize and track application connectivity dependencies, transfers computed application composition and detects policy violations to ensure access while maintaining compliance against the hybrid network access security policies that are outlined in Tufin Orchestration Suite. With vArmour and Tufin Orchestration Suite, security teams gain visibility over the existing connectivity and dependencies of applications, existing risks, and automated workflow-based remediation.

vArmour Application Controller allows you to choose the applications you want to protect and select the way in which you want to protect them. Application Controller utilizes vArmour Security Graph to are behaving as intended. The Security Graph is populated from existing and readily available telemetry data, increasing the value of the existing investments and providing shortened time-to-value.

The Tufin Orchestration Suite is a policy-centric solution for automatically analyzing risk, designing, provisioning and auditing network security changes. Tufin reduces the attack surface and minimizes

disruptions to critical applications. Its network security automation enables enterprises to implement security changes in minutes instead of days with continuous compliance and increased agility.

vArmour Application Controller + Tufin Orchestration Suite Integration

Application Controller visualizes and translates relationships into application identities and correlates existing policies to connectivity for import to Tufin's **SecureApp**. This enables developers to model their applications and stage changes required for deployment in **SecureTrack** to calculate compliance.

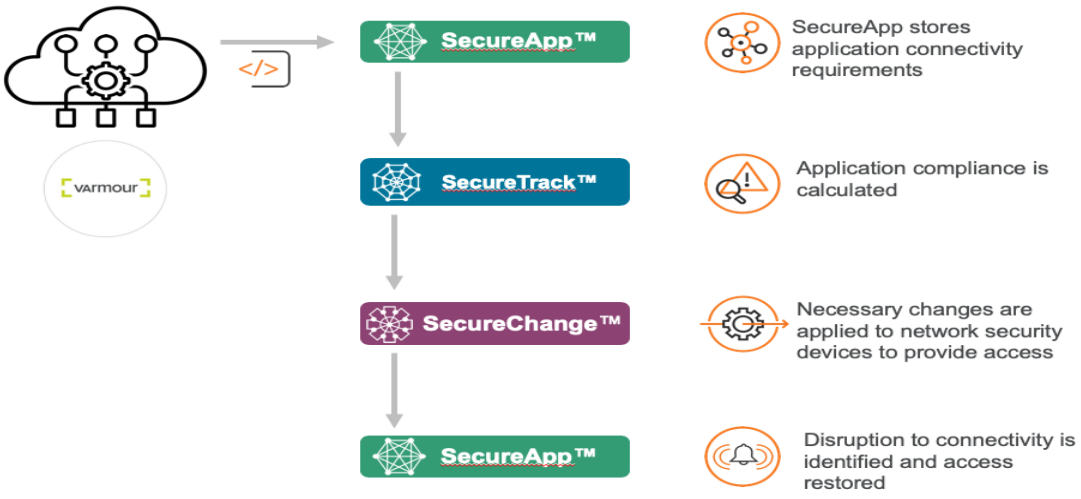
Application Controller transfers computed application composition into Tufin's **SecureChange** and applies any necessary changes to network security devices to provide access and maintain compliance. Specifically, Application Controller creates policy guardrails based on computed policy and Tufin's Unified Security Policy (USP). More, Application Controller detects policy violations by examining applications against Tufin USP policies and then creates USP policies based on observed application behavior to enforce compliance. Finally, after disruptions to connectivity have been identified by Application Controller, access is then restored in **SecureApp**.

Partner: vArmour
Partner Product: vArmour Application Controller
Benefits:

- **Auto-discovers** and visualizes applications and their relationships across diverse environments
- **Centralizes** all application communications, relationships and policies in Security Graph
- **Models** candidate policies between environments to align security intent with actual observed behavior
- **Computes** automatically intent-based security policies to assure policy compliance
- **Classifies** systems with advanced ML/AI by their behavior which enables inventory validation and improves the data quality within CMDBs
- **Leverages** rich sets of APIs to seamlessly integrate with external orchestration systems

How it Works

The diagram below demonstrates how the vArmour and Tufin work together to provide secure application connectivity, monitor policy and enforce compliance.



Benefits

The combined Tufin Orchestration Suite and vArmour Application Controller solution:

- Translates application relationships into application identities for Tufin's SecureApp
- Enables developers to model their actual application usage and stage changes required for deployment
- Leverages existing orchestration and change management workflows
- Creates USP policies based on observed application behavior to detect policy violations and to ensure continuous compliance

About vArmour

vArmour is the leader in centralized risk and control and empowers organizations to simplify security and compliance while reducing risk. Hundreds of companies worldwide rely on the vArmour Application Controller to consistently and effectively apply security controls across physical, virtual and cloud infrastructures, reducing the attack surface and maintaining continuous compliance. Learn more at www.varmour.com.

About Tufin

Tufin (NYSE: TUFN) simplifies management of some of the largest, most complex networks in the world, consisting of thousands of firewall and network devices and emerging hybrid cloud infrastructures. Enterprises select the company's Tufin Orchestration Suite™ to increase agility in the face of ever-changing business demands while maintaining a robust security posture. The Tufin Orchestration Suite reduces the attack surface and meets the need for greater visibility into secure and reliable application connectivity. With over 2000 customers since its inception, Tufin's network security automation enables enterprises to implement changes in minutes instead of days, while improving their security posture and business agility.