

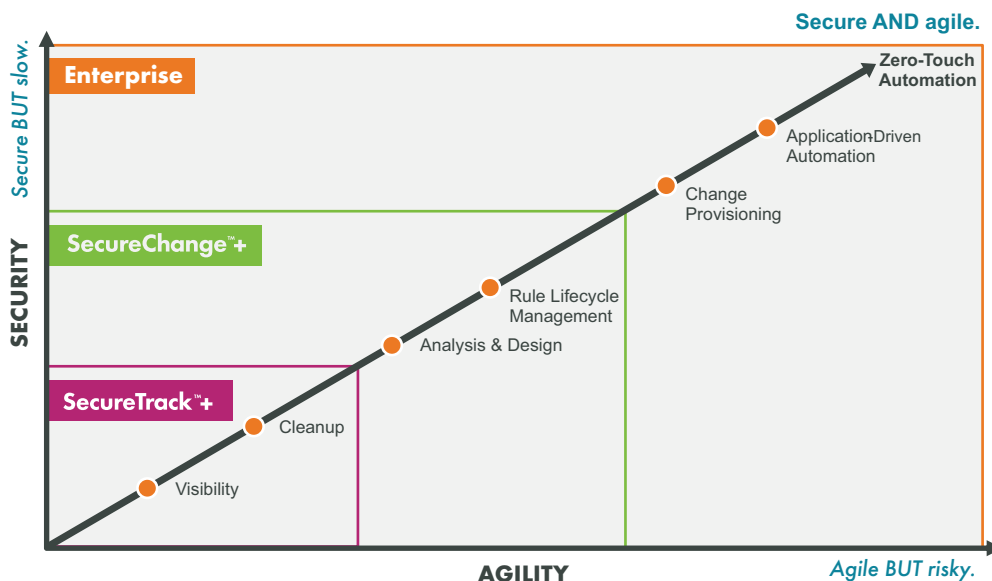
Complete Your Journey to Zero-Touch, Application-Based Security Policy Automation

Overview

Tufin provides solutions for each stage of your development towards achieving policy-based, holistic network security management. Our vision is to help you gain visibility and control over your entire hybrid, multi-cloud network with zero-touch, application-driven security policy automation.

Tufin Enterprise is the ultimate destination on this journey. It elevates your network security program to a highly evolved state, in which, network and cloud security processes are integrated, policy is managed and implemented via zero-touch automation, and everything is administered via a central control plane that delivers unmatched scalability and extensibility. Tufin Enterprise delivers:

- Rapid design and implementation of changes across your hybrid enterprise network
- Policy-based, unified network security from on-prem to cloud
- Visibility into and control over application connectivity, dependencies and access policies
- Security policy validation integrated into your CI/CD process, so your DevOps teams can meet audit obligations



Change Provisioning

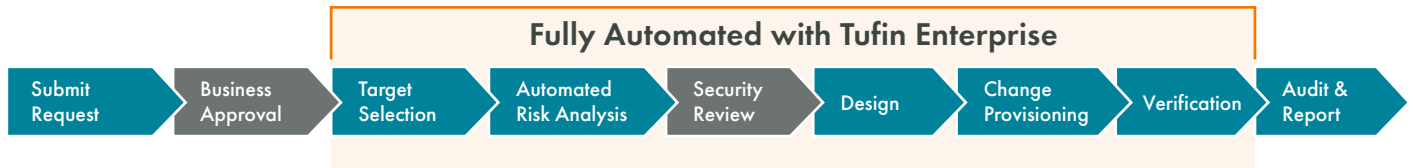
Large enterprise networks, often contain a complex collection of security controls across devices and cloud resources from several different vendors. Pushing network access changes to your hybrid infrastructure is likely a large effort involving many people who specialize in specific network device technologies. This manual approach is time consuming, error-prone, and results in increased cyber risk and noncompliance with corporate policy and regulations.



Key Features

- SecureTrack+ & SecureChange+ functionality
- Zero-touch, app-driven network change automation, including provisioning
- Cloud-native security policy management and compliance monitoring
- Integrated with CI/CD pipelines and DevOps processes
- Application connectivity management
- High availability with highly redundant, multi-node clusters
- Premium 24/7 follow-the-sun support

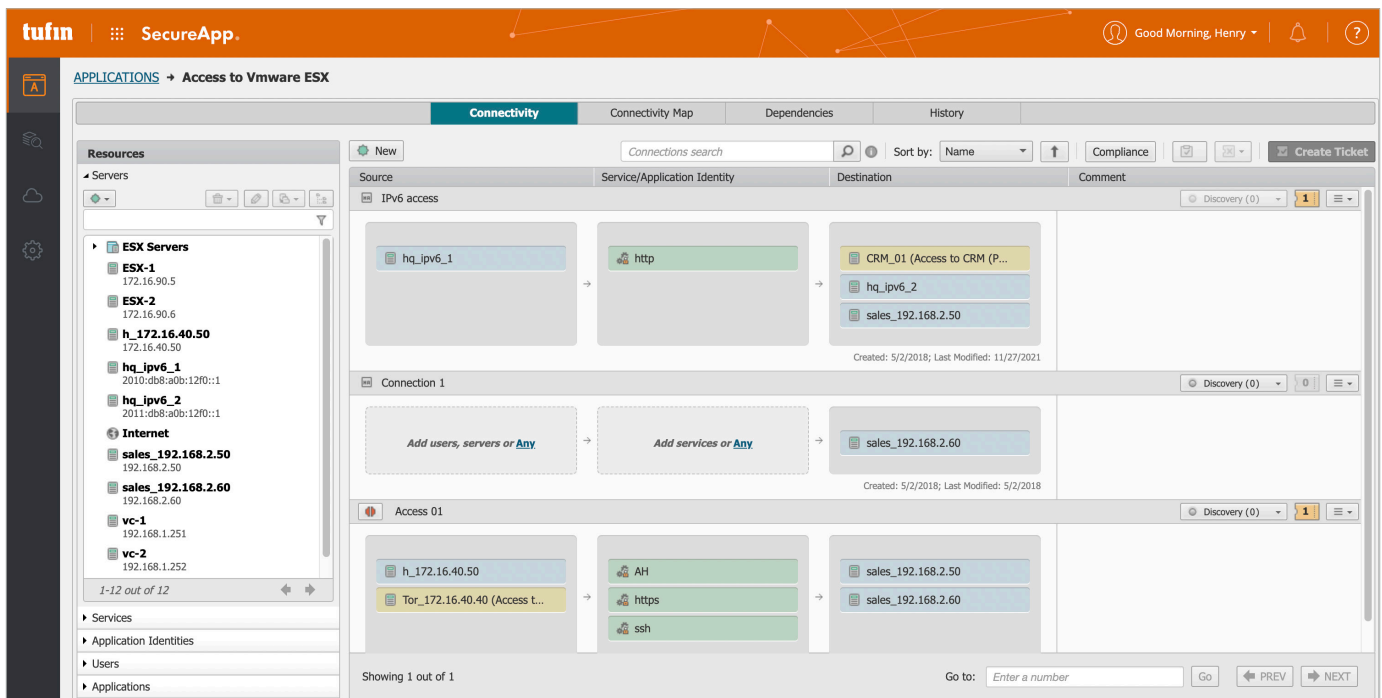
With Tufin Enterprise, security configuration changes designed in SecureChange+ can be provisioned to the relevant firewall and cloud platforms. With Tufin Enterprise it is possible to automate the entire network change process, from request, through target selection, risk and impact assessment, all the way to implementation.



Application Connectivity Management

Implementing security policies based on application needs is usually a joint effort between security and application teams. Both teams need to constantly communicate connectivity requirements and ensure they align with security access policies, which can lead to bottlenecks, until the application is deployed securely.

The SecureApp module provides an intuitive user interface and real-time visibility into and control over all apps and traffic flows. Application owners can easily manage application-critical connectivity based on their understanding of access requirements, with only minimal required knowledge of network topology or firewall and router policies. Tufin automatically translates access requirements into security policy changes on the relevant firewalls via a process that is fully transparent to both security and application teams. This is just another way Tufin enables multi-team collaboration and maintains a state of continuous compliance.



Application Connectivity Mapping

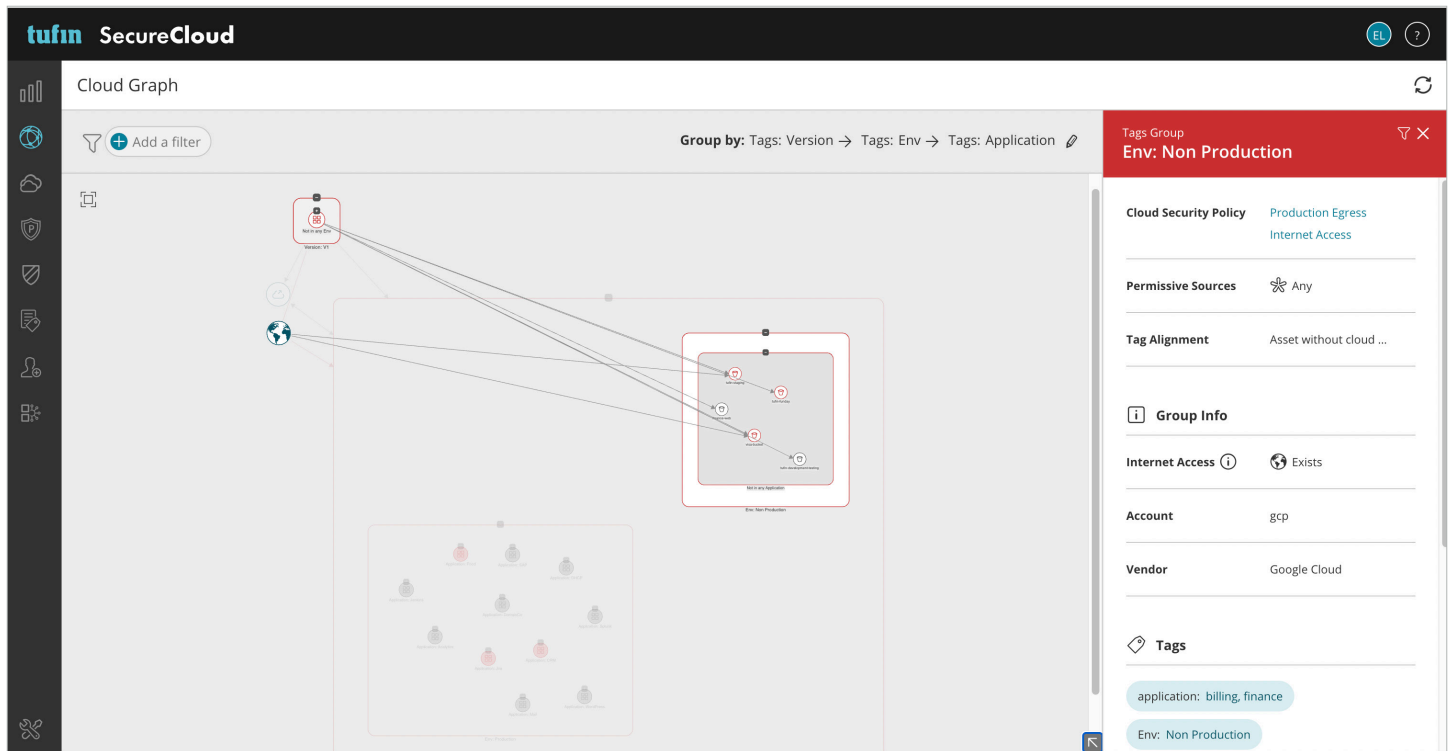
Security Policy Management for Cloud-Native Environments

The SecureCloud module is an agentless SaaS solution that extends security policy management, compliance monitoring and security guardrails to your public cloud deployments. It will automatically discover and visualize all workloads and security groups, providing an application-centric topology view of all deployed assets, configurations and security settings. It provides a unique tag-based security policy for managing microsegmentation across public cloud environments, to ensure least privilege and maintain a strong security posture.

Managing security in the cloud is often only part of the challenge. As workloads and applications migrate to the cloud, some applications need access to the on-premises environment. Even cloud-native applications often require access to resources protected behind traditional network security devices. Tufin Enterprise bridges this gap, streamlining access change processes from cloud to on-premises.

DevOps Doesn't Have to Change How They Work

Tufin's SecureCloud module can integrate into your CI/CD pipeline, acting as a gatekeeper to ensure code deployment complies with the organization's network security policy. It connects to Cloud Formation and Terraform, and monitors whether any security group changes are being deployed through the CI/CD pipeline. It automates the detection, alerting and remediation of security risks, throughout the build, test, deploy and operate lifecycle, and ensures your DevOps team is always audit-ready.



Cloud Segmentation Mapping and Management

High Availability with highly redundant, multi-node clusters

Tufin has built-in support to run in high availability mode, using a redundancy mechanism, in which your data is kept up to date on three server nodes (or more) simultaneously. Tufin's High Availability provides both redundancy and load-sharing within the cluster. This ensures business continuity and proper load distribution during peak times.

Premium 24/7 follow-the-sun support

Tufin's premium level support offers round-the-clock call handling, troubleshooting and problem resolution via dedicated support engineers.

This leads to faster completion times, by addressing customer needs without regard to geographic location or current time.