tufin The Security Policy Company. + cisco SECURE X

Technology Partner Solution Brief

Accelerate and automate incident response (IR) based on real-time network visibility and policy intelligence

Highlights

- Enhanced visibility into detailed network security intelligence
- Execute automated playbooks (e.g. block access) based on real-time network data
- Application-driven automation enables the translation of app security requirements into network changes

The Tufin Orchestration Suite™ integration for Cisco SecureX provides critical network security context and automated response capabilities to quickly address network threats in real-time.

Security practitioners are constantly inundated with information overload from various network and infrastructure components. The information assessment consists of collecting, analyzing, and measuring risks to the network from diverse dashboards, threat intelligence sources, device feeds, and other sources. The team will be in a perpetual catch-up mode without a focused approach to threat response that relies on collaboration, correlation, collection, threat assessment, and response.

The integration between Tufin and Cisco SecureX provides security analysts with accurate, up-to-date network topology and security policy information, to help make fast and detail risk assessments and execute automated network access changes to immediately mitigate threats, without impeding business continuity.

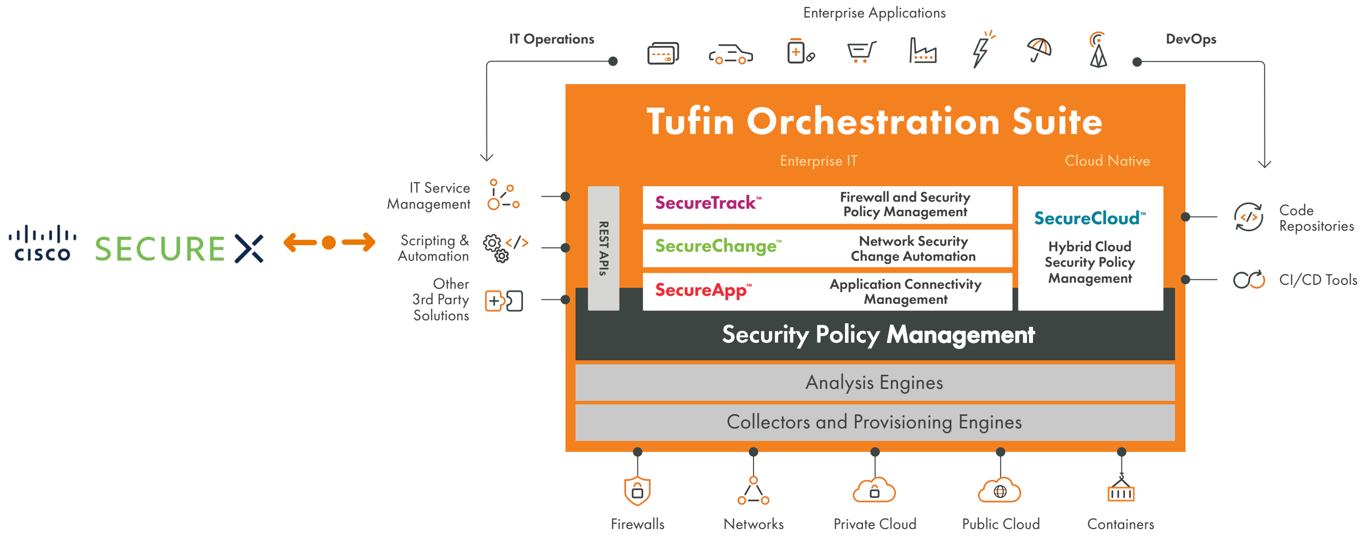
Cisco SecureX

Cisco SecureX is a cross-product, cross-vendor security platform that combines threat intelligence, defensive and response, and orchestration capabilities from multiple Cisco and third-party security and networking products. SecureX uses the APIs of these products in a coordinated fashion to bring security operations teams unprecedented simplicity, visibility, and efficiency. It is designed to empower teams – to increase collaboration, visibility, and automation, in order to streamline operations, and simplify security. It's a culmination of many years of listening to our customers and partners, and trying to find ways to make their jobs less complex. A critical component of that goal is integration – not just of our technology, but also allowing organizations to closely align their SecOps, NetOps, and ITOps teams, so they can more cohesively protect assets, and enable business.

Tufin Orchestration Suite

Tufin Orchestration Suite takes a policy-centric approach to security by providing visibility and security policy automation across heterogeneous and hybrid IT environments. It enables end-to-end change automation for network and application connectivity, and orchestrates a unified policy baseline across the next generation network. The result is that organizations can make changes in minutes, reduce the attack surface, and provide continuous compliance with internal and external industry regulations. The ultimate effect is greater business continuity, improved agility, and reduced exposure to cybersecurity risk and non-compliance.

Tufin in Cisco Ecosystem Exchange   Get your Tufin Cisco SecureX integration playbooks



✓ Visibility ✓ Automation ✓ Orchestration ✓ Compliance

Efficient analysis, actionable data

Network access information is critical in any security practitioner's playbook. The joint solution provides network and services connectivity information, such as access routes, device inventory, impact radius measurement, network path analysis, critical app and app dependency context when a potential security incident involves one or more applications, and more.

This information, combined with the threat intelligence from other Cisco security products, such as firewalls, ASA, Cisco ACI, routers, and switches, provides analysts with a detailed perspective of the exposure, and helps them evaluate the impact of an attack.

In addition to expediting time-consuming investigation, the integration provides established playbooks based on real-time network data for automated remediation and rapid response. Playbook actions, like server decommissioning, can be initiated with a complete record of the change, and a comprehensive audit trail.

Risk-free incident response

With Tufin's visibility into the entire network topology, analysts and incident responders can block a host, port, or service by simply submitting a change request with a source and destination. Tufin then automatically designs and provisions the required change on the appropriate network devices to ensure effective containment. Tufin provides immediate containment or isolation of potentially malicious internal or external hosts, without the need to specify the appropriate network enforcement point.

When the change is made through Tufin, existing compliance guidelines are followed and all changes are audited, ensuring that no additional risk is introduced because of the change. To increase agility, Tufin users can create a dedicated change workflow specifically for incident response, ensuring an efficient response, while maintaining compliance with an established change control process.

The Tufin solution provides responders with critical network information which is accurate, up to date, and actionable. Multi-vendor support enables visibility and control across a heterogeneous environment, serving as a single source of truth for the entire network. Incorporating Tufin into the incident response process significantly reduces the time to triage an alert, and the mean time to respond (MTTR) to an incident.