tufin

SOLUTION BRIEF

Tufin SecureChange+

Automate and Orchestrate Network Change Across Multi-Vendor Networks

Executive Summary

When connectivity fails, or a new application needs access, the question network and application teams ask is simple: how does this traffic actually get from source to destination, and what is stopping it? Answering it requires seeing the entire path a specific flow takes across the real, multi-vendor network, including routers, switches, SD-WAN, NAT, cloud security groups, secure web gateways, microsegmentation controls, and firewalls, not the rules on a single device.

SecureChange+ gives network, security, and application teams that enterprise-wide view, and then acts on it. It traces the path to show exactly where traffic is allowed, where it is blocked, and why. When a change is required, it identifies every in-path device, designs the change, assesses risk, provisions it, and verifies the result end to end. Analysis and troubleshooting come first; governed automation follows from the same topology and policy model.

SecureChange+ includes all SecureTrack+ capabilities natively, so network-wide visibility, topology mapping, and path analysis are available out of the box rather than as an add-on or separate purchase.

Business Challenges

Network and security teams handle hundreds of access and change requests each week, across environments that span data center, campus, branch, WAN, SASE, and cloud. Manual investigation, scattered approvals, and inconsistent validation slow the business and introduce risk.

- Connectivity issues that take hours to isolate because no single tool sees the full path
- Lengthy, manual change design and approval cycles across multiple vendors and domains
- Limited visibility into the network impact of each change before it is deployed
- Difficulty validating compliance and risk ahead of deployment
- Lack of closed-loop verification and audit-ready documentation
- Homegrown scripts that break with every firmware upgrade or new platform
- Inefficient rule governance and incomplete change tracking

The result is slower response times, configuration errors, unnecessary change requests, and larger security gaps.

Enterprise-Wide, Multi-Vendor Network Context

Automation is only as good as the model behind it. SecureChange+ builds and maintains a live topology of devices, subnets, and clouds, so every query and every change reflect how the network actually behaves today rather than a static diagram. The TOS Discovery module finds unmanaged routers and switches, onboards them, and keeps that topology current automatically.

Network constructs modeled in the path

The topology model reflects how the network actually forwards traffic, not just where policy is enforced. It accounts for routing tables and interfaces, policy-based routing, NAT, IPSec connectivity, MPLS and EVPN/VXLAN participation, and Cisco ACI fabrics. It also covers AWS Transit Gateway and Cloud WAN, and VNet and VPC peering across Azure, AWS, and Google Cloud. Devices that are not directly monitored can be represented as generic devices with their interfaces and routes, so the path stays complete end to end.

Technology coverage across the network stack

- Routers and switches, including Cisco, Juniper, Arista, Huawei, and Aruba platforms
- SD-WAN and WAN edge, including Cisco Catalyst SD-WAN, Meraki, Arista VeloCloud, Versa Networks, and Aruba EdgeConnect
- Cloud and virtualized networking: AWS, Microsoft Azure, Google Cloud, and VMware NSX
- Secure web gateways and cloud proxies, including Zscaler and Symantec Blue Coat
- Microsegmentation and zero-trust access controls, including Illumio and Akamai Guardicore
- Firewalls and NGFWs, including Palo Alto Networks, Check Point, Fortinet, Cisco, Juniper, F5, and Forcepoint
- Load balancers, address translation, and other network-related controls and appliances, including devices onboarded through the Open Policy Model and Tufin Open Platform plugins

The complete, current list of supported devices and platforms, and the full topology model reference, are published at forum.tufin.com/support/kc.

SecureChange+ is built on Tufin's Open Policy Model, which normalizes routing, NAT, and policy data from every supported vendor into one consistent model.

Tufin maintains and extends that model as vendors change their data models and APIs, and as new technologies are added to the environment, so path analysis and automation keep working without the customer's own team rebuilding it.

Network Access Troubleshooting: Find the Root Cause Fast

When connectivity breaks, teams need to see exactly how traffic moves through the network, and where it is routed, filtered, or blocked. SecureChange+ traces the full path between any source and destination, hop by hop, across every device and control point along the way, so teams stop guessing and start diagnosing.

A single path query pinpoints whether traffic is blocked by:

- A missing or misconfigured route
- A NAT rule along the path
- A cloud security group or access policy
- A firewall or security policy rule
- An incomplete or out-of-date topology segment

Path analysis also confirms when a path already exists end to end and traffic is already permitted, so teams can rule out unnecessary change requests entirely, closing the ticket without touching a single device. Where a recent change is the likely cause, New Revision and Advanced Change reports correlate the failure with the specific configuration change that introduced it.

Teams can run this analysis from the topology map, through the API, or conversationally: TufinMate for IT, powered by TufinAI, lets engineers check access in natural language, view the devices on a path, generate topology reports, and open a change ticket directly from the chat.

From Insight to Action: Governed Change Automation

Understanding the problem is the first half. Once the root cause of an access issue is confirmed, or a new access request is approved, SecureChange+ carries the same path and policy context directly into a governed change workflow. The team moves from diagnosis to remediation without re-establishing context or handing off to another tool.

AUTOMATED CHANGE LIFECYCLE

When a change is required, SecureChange+:

- Identifies every in-path device automatically, using the same topology data as path analysis
- Evaluates risk against the Unified Security Policy and live vulnerability data before deployment
- Generates vendor-specific rule and object changes for every affected device
- Provisions the change to the target devices within the approved workflow
- Verifies the completed change end to end against the intended access outcome, and blocks progression until the result meets defined criteria
- Synchronizes with ServiceNow: a ticket opened in ServiceNow is closed with verified, documented results from SecureChange+. The same REST API integration extends to Jira and other API-driven ITSM platforms

Every request, whether it results in a change or is closed because access already exists, is fully documented. When an audit asks why a given network path is permitted, the record shows who requested it, when, under what business justification, and what was changed.

High-Impact Scenarios

Network Path Analysis and Troubleshooting. Trace traffic paths hop by hop across routers, switches, SD-WAN, NAT, cloud, and security controls. Identify where traffic is blocked and why, correlate failures with recent configuration changes, and export detailed reports for troubleshooting and compliance.

Network Mapping, Topology, and Discovery. Maintain a live map of devices, subnets, and clouds, with automatic discovery and onboarding of unmanaged routers and switches. Visualize dependencies, validate change impact, and keep the model accurate enough to drive automated design.

Automated Change Management. Automate the change lifecycle from target device selection through design, risk assessment, provisioning, and post-change verification. Closed-loop automation ensures every change is accurate, compliant, and fully documented.

ITSM-Led and Event-Driven Change Processes. Let requests originate where the business already works. SecureChange+ integrates with ServiceNow to synchronize tickets, approvals, tool outputs, and custom fields in both directions over REST APIs, and the same integration model extends to Jira and other API-driven ITSM platforms. The ITSM system stays the system of record; SecureChange+ does the analysis, design, provisioning, and verification behind it.

Rule Lifecycle Management. Automate governance from creation through recertification and removal. Identify expiring or unused rules, assign them to owners for review, and open tickets to certify, modify, or decommission them.

Rule and Group Management. Modify rules and network object groups through structured, validated workflows across supported devices, with built-in approval and documentation.

Continuous Compliance and Audit Readiness. Measure real-world network behavior against the Unified Security Policy, detect deviation from the intended segmentation model, and maintain audit-ready documentation and change history continuously rather than at audit time.

Application Connectivity and Exposure. Understand what is reachable from where across the whole environment, and what changed. Support segmentation, zero-trust, and exposure-reduction initiatives with evidence rather than assumption.

Orchestration, Integration and Extensibility

Workflow orchestration	Multi-step, customizable workflows with conditional logic and dynamic task routing, designed without custom code and applicable across multiple vendors and domains.
Deterministic and AI-assisted	Precise, repeatable workflows where exact control is required, alongside TufinAI capabilities for natural-language analysis and requests under the same governance and guardrails.
Centralized management	A single console for the platform lifecycle, with role-based access control, multi-domain administration, and a documented REST API that exposes platform functionality to external tools.
System integration	An extensive REST API underpins turnkey integration with ServiceNow and other API-driven ITSM platforms, vulnerability management, cloud and virtualization platforms, SIEM and logging, and identity sources, ingesting and acting on data from across the wider stack, with real-time change notification via syslog and SNMP.
Configuration and revision tracking	Continuous device monitoring with a full revision history of every policy and configuration change, automatic scheduled fetches to capture out-of-band changes, and change reports that correlate an access failure with the revision that caused it.
Works with existing tooling	Coexists with Ansible, Python, and vendor-native controllers already deployed. Extend and scale existing automation investments rather than replacing them.
Modular adoption	Capabilities adopted in stages: visibility and analysis first, then change design, then deployment, all on a common data model and control plane.

Why In-House Automation Doesn't Scale Across Vendors

Many teams first try to solve path visibility and change automation with their own scripts, built against individual vendor APIs. Each vendor has its own data model, its own API, and its own release cadence, so a script that works today breaks with the next firmware upgrade, the next SD-WAN rollout, or the next cloud platform added to the network. Maintaining that patchwork becomes an ongoing engineering burden rather than a one-time project.

Scaling past the easy use cases means either investing heavily in a permanent in-house engineering function, or adopting a platform that normalizes the environment once and maintains it. The Open Policy Model is that normalization layer: routing, NAT, and policy data from every supported vendor reduced to one consistent model that Tufin maintains as the environment changes.

One Tier, Full Capability

SecureChange+ includes all SecureTrack+ capabilities, including network mapping, topology visualization, discovery, and path analysis. Organizations do not need SecureTrack+ separately to get enterprise-wide path visibility and troubleshooting; every SecureChange+ deployment includes it from day one.

Why SecureChange+?

- **See the whole path:** enterprise-wide, multi-vendor visibility across routers, switches, SD-WAN, NAT, cloud, security groups, gateways, and firewalls
- **Resolve faster:** pinpoint where traffic is blocked and why, and rule out unnecessary change requests entirely
- **Accelerate change delivery:** automate target selection, design, risk assessment, and approvals to cut turnaround times
- **Reduce risk and errors:** validate compliance and security impact before every change, and verify the outcome after
- **Govern every change:** give external tools and requesters a governed, logged path to the network through an extensive documented API
- **Ensure continuous compliance:** complete documentation and audit-ready trails for every request, changed or not
- **Scale without rebuilding:** one normalized model maintained across vendors, alongside the automation tooling already in place

About Tufin

Tufin helps enterprises govern and secure connectivity across today's complex multi-vendor networks. As the leader in network security posture management, Tufin provides the trusted control layer organizations need to understand exposure, automate policy changes safely, and maintain continuous security posture across on-premises, cloud, SASE, microsegmentation, and hybrid environments. Built on customer-proven network automation playbooks and the industry's only Dynamic Network Connectivity Graph, Tufin is bringing Multi-Vendor Agentic Network Security to the enterprise - helping organizations move from visibility to governed, AI-driven action.

To learn more, visit www.tufin.com.