

Security Policy Change Automation for Business Agility & Compliance

Security and network operations teams face a multitude of challenges managing enterprise-wide security changes.

- Enforcing policies consistently across complex IT environments—multi-vendor, multi-technology platforms spanning physical networks and public and private cloud(s)
- Keeping pace with the growing volume of network security change requests
- Avoiding misconfigurations and re-work due to error-prone manual processes
- Maintaining security policy compliance including documentation for audits
- Supporting advanced firewalls and security policy management technologies such as NGFW capabilities and Security Groups
- Coping with the acute shortage of skilled network security personnel
- Responding quickly, and based on accurate data, to threats, vulnerabilities, and network topology changes
- Mitigating cybersecurity threats and the risks of new attack vectors
- Collaborating across teams to share security responsibility

SecureChange® – Automated & Orchestrated Network Security Change Management

SecureChange, part of the Tufin Orchestration Suite™, increases agility, visibility, and control for network security change processes. SecureChange automates provisioning, modification, and decommissioning tasks as well as custom workflows. It provides end-to-end policy management to reduce complexity and human error, eliminate blind spots, and lessen attack vectors. Make changes in minutes instead of days, while maintaining compliance.

- Greater agility with end-to-end automation and provisioning across heterogeneous and hybrid public and private cloud environments
- Transform network change management from repetitive, time-consuming, manual tasks to streamlined collaborative workflows
- Manage the entire firewall, network, and security group access lifecycle management
- Maintain continuous compliance with audit readiness based on fully documented and tamper-proof processes



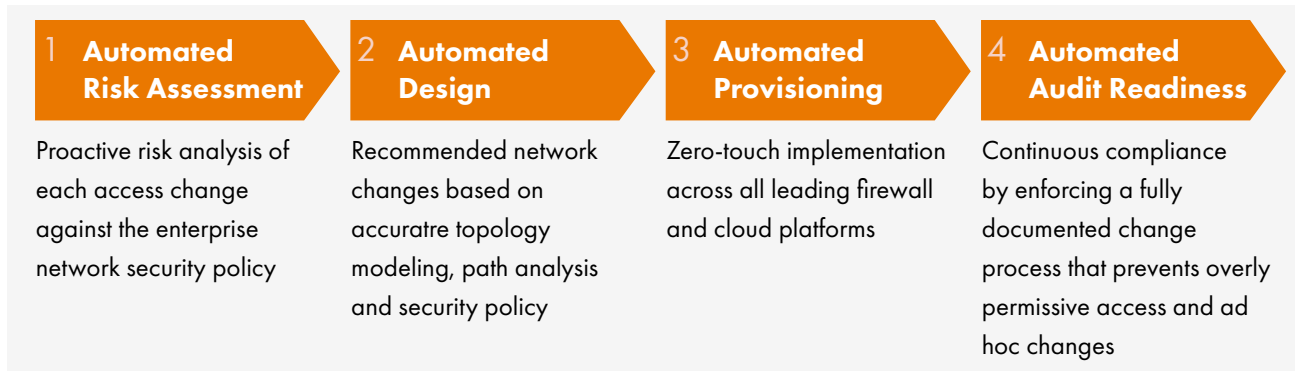
Highlights and Benefits:

- **Automate provisioning and end-to-end orchestration** for multivendor environments to reduce complexity and human error
- **Implement changes securely and accurately in minutes** instead of days
- **Perform proactive risk analysis** to avoid security policy and compliance violations
- **Leverage extensible, customizable workflows** for full integration into enterprise ITSM processes
- **Support all leading** enterprise firewall **vendors**, and public and private cloud platforms
- **Reduce time and effort required for audit readiness by up to 70%** through continuous compliance and automated audit trails

Agility & Efficiency Through Automated Workflows

SecureChange features nine workflow templates to jump-start automation. Each is designed around best practices and can be configured for specific use cases. SecureChange fully integrates with leading firewall solutions, ticketing systems, IPAM solutions, vulnerability scanners, and SIEM and SOAR platforms to manage the workflows across your security fabric. Open, function-rich APIs facilitate advanced workflow capabilities and integrate with custom portals and other external systems.

Risk-free Change Automation Workflow:



OOTB Integrations

Tufin's Workflow Integrator app allows users to build custom, code-free integrations between SecureChange and any REST API-based ITSM solutions. Select a workflow, configure the data exchange between the SecureChange server and third-party server, map data field values and prior or subsequent automated steps, and configure the trigger.

Productivity

An acute shortage of security professionals demands that enterprises mitigate risks and meet compliance more efficiently. SecureChange bolsters both security and productivity by automating daily security tasks, reducing human error, and minimizing remediation. Implement changes faster and do more with existing resources.

Maintain Continuous Compliance & Audit Readiness

Avoid the stress of audits through transparency and real-time reporting of compliance status against internal policies as well as industry regulations such as PCI DSS, HIPAA, GDPR, SOX, NERC CIP, and more.

- Out-of-the-box and customized workflows tailored to enterprise compliance and audit needs
- Automatic audit trail for all change requests including full accountability and audit-ready reports
- Automated access recertification to ensure rule-based adherence

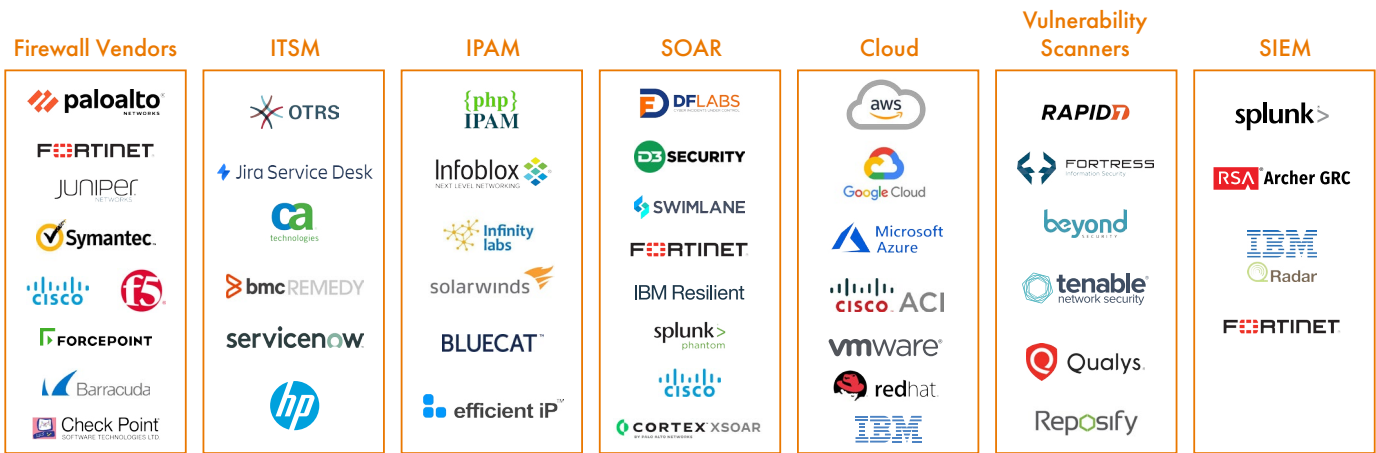
Proactive Risk Analysis

With SecureChange, security is built into network change processes. Tufin's Unified Security Policy (USP) defines segmentation and blocks unauthorized external and internal access. Risk assessment is automated through embedding in workflows and integrating with vulnerability scanner output.

Nine customizable workflows to automate security changes and management:

- Network Access Request
- Rule Decommissioning
- Server Decommissioning
- Group Modification
- Rule Modification
- Rule Recertification
- Clone Server Policy
- Access Request combined with Group Modification
- Generic workflow

Tufin's SecureChange enables users to control network security changes through process automation, proactive risk analysis, and remediation—all from a single console spanning physical networks and hybrid cloud platforms.



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 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.