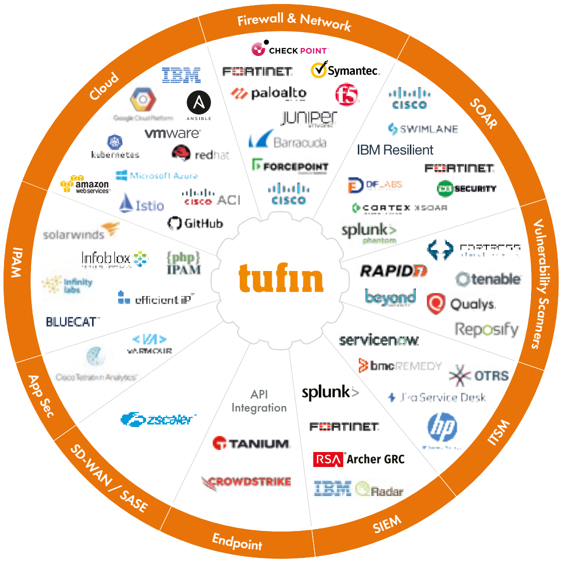
Technology Partner Solution Brief

Tufin Integrations: The Value of Leveraging Tufin's Ecosystem

Overview

Tufin's extensive partner ecosystem facilitates a cybersecurity mesh architecture, enabling customers to enhance risk decisions, network insights, and policy automation.

Tufin offers its customers an expansive partner ecosystem that spans IT, networking, security, and hybrid cloud to support a cyber security mesh architecture.



Tufin's ecosystem promotes collaboration and interoperability among IT and security capabilities, streamlining the integration of diverse technologies for improved cybersecurity management.

Key Benefits:

- **Enriched Topology View:** Third-party sources enhance Tufin's topology view, enabling informed policy and risk decisions.
- **A Single 'Source of Truth':** As the ‚source of truth' for network topology, Tufin enhances partner workflows, including vulnerability management and SOAR use cases.
- **Seamless ITSM Integration:** Tufin integrates into broadly deployed ITSM solutions, allowing customers to leverage their ticketing system for all IT requests.

5 Common Use Cases: Enhancing Cybersecurity with Tufin's Ecosystem

The following are five common use cases, representing just a selection from a larger pool of Tufin use cases and integrations.

- **Network security policy management and access control:** For better network security and access control.
- **Vulnerability Management:** For network insights and precise risk prioritization.
- **IP Address Management:** For Accurate IP addressing in dynamic environments.
- **ITSM:** For efficient change requests.
- **SOAR:** For contextualized network information.

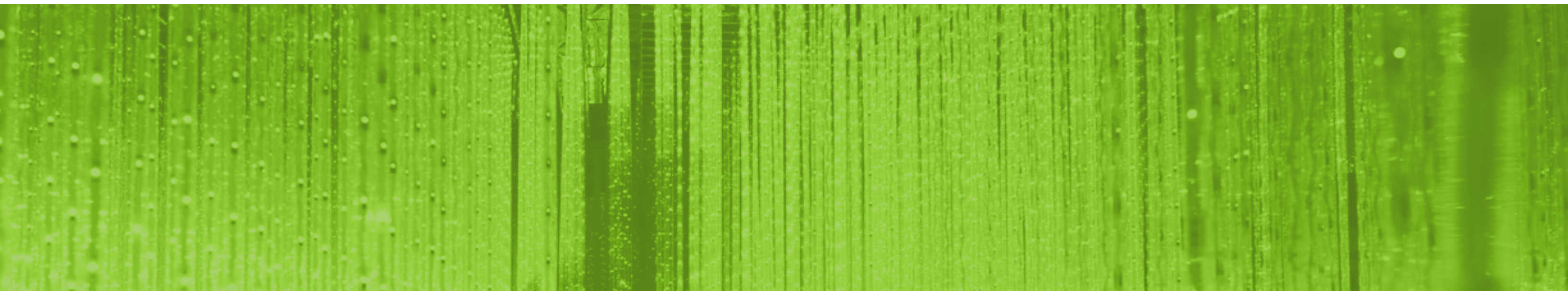
Use Case #1: Vulnerability Management

Tufin offers the broadest support in the industry for the leading firewall and networking vendors. With their support, Tufin builds the integrations natively into our solution.

Tufin enables best-in-class visibility and management of your multi-vendor network infrastructure, whether on-premise, on the edge, or in the cloud. This enables:

- End-to-end visibility & troubleshooting capability (you can only protect what you can see)
- Consistent Security Policy across hybrid/heterogeneous networks (which reduces the risk of breach and non-compliance)
- Meet SLAs and minimize risky change implementation(s) around multiple use-cases (access enablement, access decommissioning, policy optimization, and environment clean-up and hygiene)
- Audit preparations and (regulatory) compliance alignment

Tufin specializes in end-to-end network visibility, hybrid-cloud security policy management, continuous compliance automation, and audit readiness.



Use Case #2:
Vulnerability Management

The Tufin Vulnerability Mitigation App (VMA) (SecureTrack+):
Tufin's VMA ingests and analyzes vulnerability scan results, showing vulnerability management teams the vulnerabilities exposed to untrusted networks and most likely to be exploited by attackers.
It allows:

- Users to create new network rules to block access to vulnerable ports temporarily.
- New services for compensating controls to reduce vulnerabilities until a permanent solution is integrated.

Tufin applies network insights to existing vulnerability scan results to help enterprises prioritize vulnerabilities that expose the enterprise to the most significant contextualized risk.

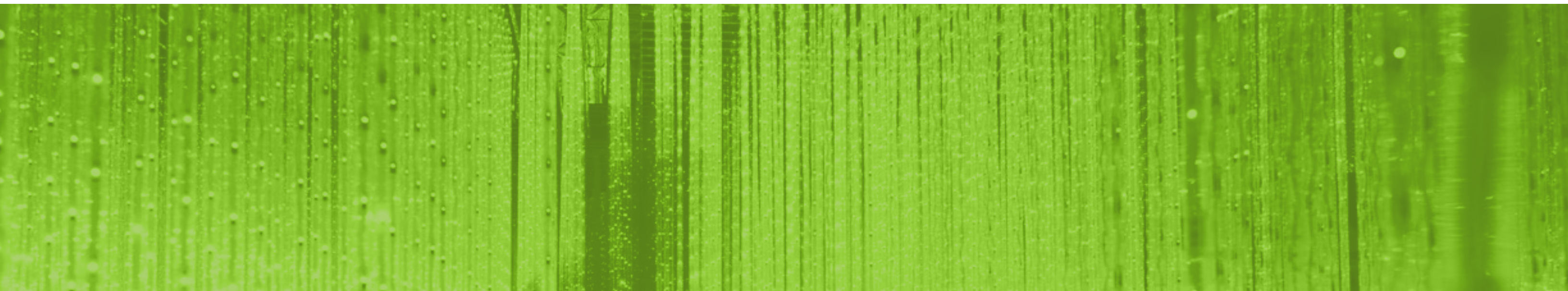
The VMA and Vulnerability-based Change Automation (VCA) natively support Qualys, Rapid7, and Tenable. Various use cases for other vulnerability vendors can be supported via PS.

Use Case #3:
IP Address Management (IPAM)

The IPAM Security Policy App (ISPA)
(SecureTrack+): Tufin's IPAM ingests IP zone information and automatically updates Tufin's zones, ensuring the appropriate USP zone requirements are applied when calculating rule compliance.

The ISPA natively supports PHP IPAM, EfficientIP, Infoblox, NetBox and BlueCat. Infoblox has also written its integration, which fulfills a similar use case. Various use cases for other vulnerability vendors can be supported via PS.

Tufin integrates with enterprise IPAM vendors to ensure your security policies are accurately evaluated against dynamic networks.



Use Case #4:
IT Service Management (ITSM)

Depending on the level of integration, the functionality may be one way (ITSM sends the request to SecureChange+ and receives no updates) or two way (ITSM sends the request to SecureChange and SecureChange+ sends the ITSM continuous updates on the status of the request).

ITSM integration is delivered through PS, often partially by leveraging the Workflow Integrator App.

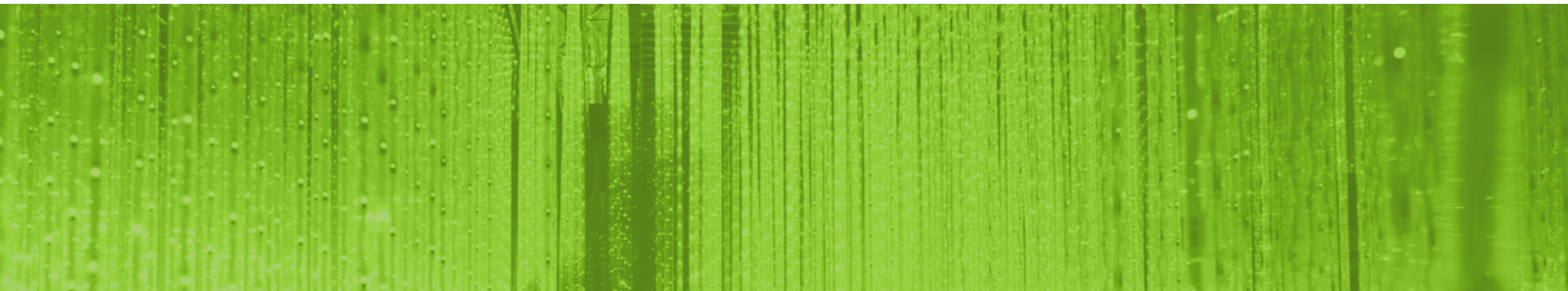
ITSM can be used as a front end to SecureChange+, allowing end users to have a seamless change request while the network team continues to realize the full benefits of SecureChange+.

Use Case #5:
Security Orchestration, Automation, and Response (SOAR)

Tufin’s SOAR:
Tufin’s network information contextualizes information from a SOAR alert and can achieve network containment of a potential incident by implementing blocking policies via SecureChange+ automation to prevent further damage while the incident is investigated

Tufin has out-of-the-box integrations with Splunk (Cisco) and Palo Alto Networks Cortex XSOAR — some PS required based on unique customer environments. The customer or PS will need to create the workflows (aka playbooks or runbooks) within the SOAR to trigger actions in Tufin when an alert is received.

Tufin extends a vast repository of network insight to the enterprise’s Security Operations team via SOAR to enable more accurate triage, escalation, and containment of security incidents.



Case Study: Swisscom Gains Control Of Its Firewall Operations With Tufin

The Challenge

Swisscom's security management realized that they were not in full control of their firewall operations after an external annual audit resulted in several high-risk findings. This prompted an immediate search for a solution that would address the following:

With Tufin, Swisscom has:

- Automated firewall auditing and management operations.
- Implemented real-time monitoring of all changes.
- Reduced time required to plan and implement security changes.
- Ensured compliance with regulatory requirements.
- Improved overall network security.
- Reduce the time required to plan and implement policy changes.
- Allow administrators to pinpoint the exact change that caused a network incident.
- Guarantee the correct implementation of all rule base changes throughout Swisscom's 150+ firewalls.

> "We already had tight processes in place, but the automation SecureTrack introduced provided us with an overall snapshot of the state of our firewalls that enables us to operate in a much more agile, proactive, and strategic manner. We accomplish more in less time, with full confidence that we are operating securely."
>
> - Michel Müller, Senior Network Security Engineer, Swisscom

Tufin specializes in end-to-end network visibility, hybrid-cloud security policy management, continuous compliance automation, and audit readiness. Tufin is a policy-centric solution for designing, provisioning, analyzing, and auditing enterprise security changes.