tufin

SOLUTION BRIEF

Accelerated Device Onboarding with Unified Policy Management

Eliminate Onboarding Delays Across Your Hybrid Network

Modern hybrid networks evolve faster than most security teams can keep up with. New firewalls, cloud platforms, SASE services, and microsegmentation tools introduce their own policy models and management consoles, creating inconsistency, blind spots, and operational drag. Organizations need a way to enforce security policy once and apply it everywhere. Tufin's Open Policy Model (OPM) delivers that foundation. As a vendor-agnostic and extensible framework, OPM ensures rapid onboarding of new devices while maintaining a unified, scalable policy enforcement across the entire hybrid environment. With OPM, enterprises achieve complete visibility, faster automation, and consistent policy enforcement as their environment grows.

What is Tufin OPM?

Tufin's Open Policy Model (OPM) is a flexible abstraction layer that unifies diverse network security technologies under a single, vendor-agnostic policy framework. Instead of adapting security workflows to each firewall, cloud platform, or segmentation tool, OPM normalizes them, allowing Tufin to support any device quickly and consistently. Once a new device or platform is integrated through an OPM connector, it immediately inherits all of Tufin's core capabilities, including visibility, change design, policy validation, compliance checks, and lifecycle management. No custom development, no hardware upgrades, and no platform-specific engineering are required. With OPM, Tufin can deliver support for new devices and platforms faster than traditional security vendors. And as new features roll out, such as enhanced compliance validation or change tracking, every OPM-connected device receives them automatically. No delays. No capability and version gaps across vendors or environments.

Tufin OPM Capabilities

Capability	Description
Rapid Onboarding Device	Bring new platforms, cloud, on-premises, SASE, or microsegmentation, under centralized control in weeks, not months, accelerating time-to-value.
Unified Policy Enforcement	Enforce business-driven security policies consistently across your hybrid environment to reduce risk and eliminate configuration drift.
Full Network Visibility	Gain real-time insight into traffic flows, zones, and dependencies across vendors, enabling faster troubleshooting and smarter segmentation decisions.
Change Automation	Automate access requests and policy changes with built-in risk checks and audit trails, shortening change cycles while improving accuracy.
Continuous Compliance	Maintain ongoing alignment with segmentation and zero-trust requirements, with audit-ready controls that adapt as your environment evolves.
Scalable by Design	Extend security policy control as your infrastructure grows, without re-architecting or adding operational overhead.

How It Works

When a new platform is onboarded through Tufin OPM, it is immediately normalized into Tufin's topology, policy, and change workflows. This ensures every device, whether Huawei firewalls, Versa SD-WAN, or cloud-native controls in Azure, is managed with the same consistency, accuracy, and security across your on-premises, cloud, and hybrid environments. Once integrated, all Tufin capabilities work automatically for that platform. Access-path simulation, rule revision history, risk analysis, and change automation require no manual configuration or device-level customization. Teams gain instant visibility and control, accelerate change delivery, and eliminate the operational overhead typically associated with supporting new technologies. Tufin OPM already supports dozens of technologies across firewalls, SD-WAN, cloud, SASE, and microsegmentation, including:

Your Network Will Keep Evolving. Will Your Security?

If growth, device or platform sprawl are outpacing your security processes, OPM delivers the visibility, automated policy consistency and enforcement to stay ahead of potential security risks, not react to it.

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.