

CASE STUDY

Global IT infrastructure leader modernises a 1,000-firewall multi-vendor estate with Tufin

1,000

Firewalls under a single unified control plane ✓

£530K

Vendor platforms unified: Check Point, Fortinet, Juniper, Palo Alto ✓

40K+

End-to-end integration across change, cleanup & recertification ✓

INDUSTRY

Global IT Infrastructure & Services

ESTATE

~1,000 firewalls, multi-vendor

COMPLIANCE

NIST · ISO 27001/27002 · PCI-DSS · GDPR · SOC 2

PLATFORM

Tufin Unified Control Plane

The Challenge

A leading global IT infrastructure and services provider operates one of the largest multi-vendor firewall estates in the industry, supporting thousands of enterprise customers across Check Point, Fortinet, Juniper, and Palo Alto environments. After more than two years on an incumbent policy management platform, the team had lost confidence in its ability to keep up: usability gaps, weak topology and path analysis, brittle workflows, and limited ServiceNow integration meant engineers were spending more time fighting the tool than running clean policy.

The operational pain was specific. Engineers wanted to start every troubleshooting session from a simple question, "what rules apply to this device, and what is their impact?" The legacy platform could not answer that quickly. Cleanup, recertification, and decommissioning had all stalled, and the team needed a platform that matched how they actually worked.

"We were replacing a failed operating model, not buying a checklist of integrations. We wanted a platform that fit how our engineers actually work."

Senior Engineer, Global IT Infrastructure and Services Provider

Why Now

The organization launched a competitive replacement programme with a clear mandate from infrastructure and security leadership: select a platform that fits the operating model, integrates cleanly with ServiceNow, and scales across the full multi-vendor estate. The evaluation included a 14-requirement PoV after a 44-requirement RFP shortlist, backed by executive sponsorship from both technical and procurement leadership.

Strategic Goals

- Replace the legacy policy management platform across a 1,000-firewall multi-vendor estate without disrupting operations
- Restore engineer productivity through device-centric policy views, fast path analysis, and clean topology
- Anchor cleanup, recertification, modification, and decommissioning into ServiceNow-driven workflows
- Standardise change and policy hygiene across Check Point, Fortinet, Juniper, and Palo Alto
- Build a long-term automation foundation that scales with the estate and adapts to new vendors

Why Tufin

- Breadth of multi-vendor coverage across Check Point, Fortinet, Juniper, and Palo Alto, with topology, path analysis, and policy assessment unified in one control plane
- ServiceNow integration flexibility that mapped onto the customer's existing process model rather than forcing a generic workflow on the team
- Transparent technical engagement during the PoV: gaps named directly, workarounds and integration paths supplied, and a credible route to value at every step

Solution Deployed

Tufin's unified control plane is being rolled out across the multi-vendor firewall estate, with ServiceNow integration anchoring the four core workflows the team uses most: rule cleanup, recertification, modification, and decommissioning. Topology and path analysis are deployed in parallel to give engineers the device-centric view they need to troubleshoot quickly. Implementation is sequenced against the customer's existing change cadence.

Expected Outcomes

• Engineer time recovered

Device-centric views and clean topology accelerate day-to-day troubleshooting, replacing legacy-tool friction with an operating model that fits how the team works.

• End-to-end change automation in ServiceNow

Cleanup, recertification, modification, and decommissioning are anchored in the customer's existing process model, removing manual handoffs and rework.

• Continuous policy hygiene at scale

Risky and overly permissive rules across the 1,000-firewall multi-vendor estate are identified and remediated systematically, not during periodic audits.

• Multi-vendor standardisation

Change and policy governance are standardised across Check Point, Fortinet, Juniper, and Palo Alto, replacing point-tool variability with a single operating model.

• Automation foundation for what comes next

The unified control plane is positioned to extend to new use cases and vendors as the estate evolves.

"The buyer was replacing a failed operating model, not buying a checklist of integrations. Tufin built the evaluation around how our engineers actually work, and that is why the platform stuck."

Network Security Lead, Global IT Infrastructure and Services Provider

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.