CASE STUDY

Global IT Services Leader Eliminates Internet-Facing Attack Surface with Tufin

94%
Internet-facing hosts eliminated globally

80%
Firewall rules removed
60,000+ rules eliminated

76%
Reduction in change ticket completion time

INDUSTRY
IT Services & Managed Services

REGION
Global (70+ countries)

COMPLIANCE
ISO 27001 · SOC 2 · FedRAMP

PLATFORM
Tufin Unified Control Plane

The Challenge

A leading global IT services provider delivers end-to-end technology solutions for governments, financial institutions, and global enterprises across 70+ countries. The product of a major merger, the organization inherited a vast, sprawling firewall estate, tens of thousands of rules accumulated over decades, a significant internet-facing attack surface, and change control processes that could not scale. A ransomware incident forced a strategic inflection point: the CISO expanded scope to cover all enterprise security and issued a clear mandate, bring every firewall under systematic, policy-driven management.

> ***"We had accumulated decades of complexity, thousands of rules that nobody owned, hosts exposed to the internet that should never have been, and change processes that failed too often and required too many people to run."***
>
> Network Security Lead, Leading Global IT Services Provider

Why Now

The organization had committed to migrating 90% of enterprise applications to the cloud, making network visibility and policy governance more critical than ever. With the CISO now accountable for all 3,000+ firewall devices, including a delivery network that had relied on a competing tool without full lifecycle automation, the organization ran a competitive evaluation and selected Tufin for its breadth of automation coverage and multi-vendor scalability.

Strategic Goals

- Eliminate excessive internet-facing attack surface across the global firewall estate
- Remove decades of stale, unused, and overly permissive firewall rules at scale
- Automate change control end-to-end, from request through to provisioning
- Establish ownership and governance for all IP addresses across the estate
- Achieve continuous, measurable security posture improvement globally

Solution Deployed

Tufin's unified control plane was deployed across the organization's global firewall estate, spanning thousands of devices across multiple vendors and geographies. The platform enabled systematic attack surface analysis across approximately 300,000 potential IP addresses, identifying ownership, flagging internet-facing exposure, and surfacing decades of stale and overly permissive rules for remediation. Change automation was deployed enterprise-wide, replacing manual workflows with end-to-end automation from request through to provisioning.

Results

• 94% of internet-facing hosts removed globally

Over 2,000 hosts eliminated from internet exposure; 17,000 unused internet-facing hosts identified and remediated, reducing the estate's external attack surface to a fraction of its original size.

• 80% reduction in firewall rules globally

60,000+ firewall rules removed and approximately 400 firewall pairs decommissioned, driving millions of dollars in hardware and software cost savings.

• 18,000 attack points eliminated

2,750 overly permissive "Any" protocol rules removed; ownership established for ~300,000 potential IP addresses, closing gaps accumulated over years of unchecked network growth.

• Change ticket completion 76% faster

End-to-end automation cut ticket completion time by 76% and improved first-time change success by 50%, with fewer resources required to run the process.

• Continuous security posture now achievable

With full ownership, visibility, and automation across the global estate, the organization shifted from reactive firefighting to proactive, continuously measurable security governance.

> ***"The numbers speak for themselves, 94% of internet-facing exposure eliminated, 60,000+ rules removed, and change processes running 76% faster. But the real outcome is control: we know what we own, we know what's exposed, and we can fix it safely at scale."***
>
> Chief Information Security Officer, Leading Global IT Services Provider

Why Tufin

• Only platform delivering a unified control plane capable of managing attack surface reduction, rule cleanup, and change automation at the scale of the organization's global firewall estate
• Automated identification and remediation of internet-facing exposure, eliminating the need for manual, device-by-device analysis across thousands of firewalls
• End-to-end change automation with first-time-right enforcement, cutting failed changes and freeing security teams from manual, error-prone workflows

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.