CUSTOMER SUCCESS STORY

Global Energy Leader Unifies Multi-Vendor Security

Unifies a multi-vendor ecosystem under Tufin intelligent policy governance

Who they are: A global energy major operating across upstream, downstream, and renewables, with a five-vendor firewall estate, significant AWS and Azure footprints, and a large-scale Zscaler deployment serving its global workforce.

25K
Zscaler users under governed policy intelligence ✓

5
Firewall vendors governed consistently with cloud and SASE ✓

18mo
Pilot to enterprise scale, de-risked by proof ✓

INDUSTRY	ESTATE	ENFORCEMENT	TUFIN
Energy · Oil, Gas & Renewables	5-vendor firewall estate, AWS, Azure, Zscaler	Check Point · Palo Alto · Juniper · Cisco · Fortinet · Zscaler	Connectivity Graph · SecureTrack+ · Policy Intelligence

The Challenge

Few estates are as heterogeneous as a global energy major's. Check Point, Palo Alto, Juniper, Cisco, and Fortinet firewalls run alongside substantial AWS and Azure footprints, the result of decades of acquisition, regional autonomy, and successive technology cycles. Adding Zscaler for secure access raised the real question: not whether each platform could be managed, but whether anyone could reason about connectivity and risk consistently across all of them.

Why Now

Rather than commit blind, the organization ran a Zscaler pilot on Tufin to validate that one intelligent governance layer could genuinely model and govern connectivity across the firewall estate and the SASE edge together. The pilot took deployment risk out of the decision, and the deployment scaled to 25,000 users within eighteen months.

Strategic Goals

- Establish consistent policy governance across five firewall vendors, two public clouds, and the Zscaler edge
- Validate intelligent cross-estate connectivity analysis on production infrastructure before committing at scale
- Give security teams a reliable answer to connectivity questions that traverse multiple enforcement points
- Support continued cloud migration without fragmenting risk visibility

Why Tufin

› The Dynamic Network Connectivity Graph models real connectivity across all five firewall vendors, AWS, Azure, and Zscaler together, answering path and exposure questions no per-vendor tool can address

› Policy intelligence applies consistently regardless of which vendor enforces a given rule, so risk assessment does not vary by platform or by which engineer happens to be on shift

› A pilot-first path let the team validate intelligent governance on real infrastructure, converting an architectural bet into an evidenced decision

Solution Deployed

Tufin was first deployed against the Zscaler estate as a pilot, then scaled to 25,000 users. Zscaler is now a primary governed platform alongside a five-vendor firewall estate and AWS and Azure environments. The Dynamic Network Connectivity Graph maintains a live model of connectivity across the whole ecosystem, supporting continuous policy validation and intelligent recommendations wherever a change touches multiple enforcement points.

Business Outcomes

✓ **De-risked adoption, proven before scale**
A controlled pilot validated intelligent cross-estate governance on production infrastructure, so scaling to 25,000 users became an execution exercise rather than an architectural gamble.

✓ **Consistent governance across five vendors, cloud, and SASE**
Policy is reasoned about the same way whether enforced by Check Point, Palo Alto, Juniper, Cisco, Fortinet, AWS, Azure, or Zscaler, removing the per-vendor expertise tax and inconsistent risk assessment.

✓ **Connectivity questions answered across the whole estate**
The connectivity graph resolves path and exposure questions that traverse both traditional firewalls and the SASE edge, which no single-vendor tool can do.

✓ **Cloud migration without visibility debt**
AWS and Azure environments carry the same policy intelligence as the physical estate, so continued migration does not accumulate blind spots.

More Secure Together

The pilot answered the question that actually mattered: can one intelligent governance layer model and govern connectivity across a five-vendor firewall estate and a large Zscaler deployment at the same time? Proving it on real infrastructure turned a strategic bet into an evidenced decision, and made scaling to 25,000 users a matter of execution.

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, measure segmentation effectiveness, automate policy changes safely, and maintain continuous compliance 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.