CUSTOMER SUCCESS STORY

Banking Provider Reduces Audit Risk

Reduces audit risk across the Zscaler ecosystem

Who they are: A shared IT services provider for a network of cooperative banks in southern Europe, delivering core banking and network security services to its member institutions from a compact, Zscaler-led estate.

Zscaler
Governed as a primary platform, not an exception ✓

3
Enforcement platforms under one intelligent policy model ✓

1
Consistent governed process for every member bank ✓

INDUSTRY	ESTATE	ENFORCEMENT	TUFIN
Financial Services · Cooperative Banking IT	Zscaler-led, compact multi-vendor firewall footprint	Zscaler · Check Point · Cisco	Connectivity Graph · SecureChange+ · Policy Intelligence

The Challenge

As a shared services provider, this organization carries the security obligations of every member bank it serves. Change requests arrive from multiple institutions, each with its own risk posture and audit expectations, and each must be evidenced. The estate is deliberately compact and Zscaler-led, with a small number of Check Point and Cisco devices behind it. That shape is efficient, but it made firewall-centric tooling a poor fit: most of the policy surface carrying audit risk sat at the SASE edge, where conventional tools had least visibility.

Why Now

With Zscaler as the primary enforcement point, audit exposure concentrated exactly where governance was weakest. The provider needed policy intelligence and continuous validation that treated Zscaler as a first-class platform rather than an afterthought behind firewall management, and manual coordination across member institutions had become the limit on service delivery.

Strategic Goals

- Govern the Zscaler edge with the same rigour as firewall policy, since that is where audit risk concentrates
- Apply consistent policy validation across Zscaler, Check Point, and Cisco
- Give every member institution one governed, evidenced change process
- Remove manual coordination as the constraint on service delivery

Why Tufin

› Zscaler is governed as a designated primary platform, so the majority of the provider's audit-relevant policy surface is modelled natively rather than treated as an exception

› The Dynamic Network Connectivity Graph models connectivity across Zscaler, Check Point, and Cisco together, so risk is assessed on actual paths rather than per-platform configuration

› Continuous policy validation and intelligent recommendations help determine the right change for each member institution's risk posture, not merely execute what was requested

Solution Deployed

Tufin SecureChange+ governs the provider's Zscaler, Check Point, and Cisco estate, with Zscaler designated the primary platform in the policy model. Connectivity across all three is modelled continuously, so change requests from member institutions are validated against actual risk before execution and every action carries a traceable, evidenced record.

Business Outcomes

✓ **Audit risk governed where it actually sits**
The Zscaler edge, which carries most of the provider's policy surface, is modelled and validated continuously rather than governed indirectly through firewall tooling.

✓ **Consistent governance across a heterogeneous estate**
Zscaler, Check Point, and Cisco are assessed under one policy model, so risk evaluation does not vary by platform or by which member institution raised the request.

✓ **Evidenced service delivery for every member bank**
Each change carries a traceable record and a documented rationale, which matters when acting on behalf of multiple separately regulated institutions.

✓ **Coordination overhead removed from service delivery**
Routine access requests no longer require manual coordination between the provider and each member bank, freeing capacity for higher-value work.

More Secure Together

This estate inverts the usual assumption. Most of the policy surface, and most of the audit risk, lives at the Zscaler edge with only a handful of firewalls behind it. Governing Zscaler as a primary platform with full connectivity modelling, rather than as an add-on to firewall management, is what put audit risk under control on an architecture shaped this way.

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.