

Case Study

Multinational Bank Eliminates 12-Month Security Policy Review Backlog and Automates Continuous Compliance

A customer since 2017, this multinational financial services institution operates in retail, corporate, and investment banking segments. Based in Asia, it is in the top 20 banks in the world, based on total assets, and it operates across 137 offices in more than 40 countries.

NetSec team achieves continuous compliance across 137 offices

Challenge I: Gain visibility across 33 Firewalls from two vendors

The network security team required visibility into their security policies, as well as audit capabilities across 40 countries and 33 firewalls from both Palo Alto Networks and Check Point Software. Their existing network security policy management (NSPM) platform was falling short in its ability to automate workflows and track changes across a multi-vendor environment. There was urgency to solve these challenges and enable global policy enforcement, because they were in the midst of a merger with another company, which would only make their visibility and tracking challenges worse.

“We looked at a number of [automation] products, including the one that we had at the time. They always fell short around Palo Alto. The long-term view was not always there.”

— Manager, Network Security, Top 20 Global Bank

Challenge II: Automating Rule Recertification and Change Workflows

The company had defined a global security policy, but these 4000+ rules were being managed outside of their existing NSPM. This resulted in a 12-month backlog of rules that required review and recertification. They lacked an efficient way of making any changes to clean up legacy rules, and they were unable to automatically track any changes being made. So, to reduce workload, the team resorted to annual reviews, which was far from ideal, and the task remained monumental.



BUSINESS IMPACT

- Manages a global security policy across 33 firewalls, 40 countries and 137 international offices.
- Automated management of 4000+ rules, eliminating spreadsheets and manual processes.
- Eliminated 12-month rule recertification backlog and implemented automated daily rule reviews.
- Virtually eliminated manual audit prep and compliance reporting.

Challenge III: Eliminate Manual Tasks to Document and Prove Compliance

All rules and changes were being tracked through spreadsheets and emails. Therefore, demonstrating compliance with various regulations and security standards, such as NIST 800-53 and PCI-DSS, took a significant toll on a team that would have been better utilized on more strategic projects.

Why Tufin?

The bank took a hard look at its existing NSPM platforms and determined it was time for a change. They needed broader support for visibility into and control over their next-gen firewalls.

They also sought a vendor with a long-term vision and roadmap that was aligned to their network expansion plans. The netsec team understood Tufin's offerings would future proof their security policy orchestration, helping them to bridge gaps between on-premises and cloud teams as they expanded their networks.

Automation Maturity Across Hybrid and Multi-Cloud Networks

Tufin's advanced automation capabilities provided incentive for change. The team's long-term goal was to achieve zero-touch automation. They felt Tufin was best suited to deliver automation within massive, complex environments and that Tufin's roadmap aligned with their maturity plan – something other vendors could not offer.

// We were really keen to develop the USP [Unified Security Policy] and have no-touch automation... We can approve that request and then the rest is done by Tufin and the install on the firewall is done automatically... That was one of the key reasons why we felt Tufin would be a product that we could mature [with] along the way.

— Manager, Network Security, Top 20 Global Bank

The Results

Full Network Visibility Delivered “Instant Benefit”

With Tufin’s SecureTrack and SecureChange, the netsec team was able to review, approve and implement changes across their multiple firewall vendors—with full topology visibility and an audit trail. Upon deployment, they saw “instant benefit” with Palo Alto Networks firewall monitoring, something that was previously unavailable to them.

Automated Rule Review and Recertification

Within 12 months, the bank implemented automated rule review and recertification workflows with variable rule expiration timeframes. Using the Tufin dashboard, the team was able to perform daily rules reviews against their unified security policy, remediate or allow exceptions as warranted.

Continuous Compliance with Minimal Audit Preparation

Tufin automates policy enforcement against the company’s unified security policy by delivering impact assessment and provisioning automation that ensures continuous compliance. Automated enforcement and comprehensive reporting has dramatically reduced the amount of time required for the team to prepare for audits.

The Future: Zero-Touch Automation

The company has been keen to further develop its Unified Security Policy (USP) model on a path to zero-touch automation. They envision a process in which a user submits a request which is approved following a structured review process and “the rest is done by Tufin” to make changes to the firewall without additional human intervention. This degree of automation is expected to drive significant efficiencies for business users and security experts alike while preventing misconfiguration errors.



We liked [that our] Tufin installation could provide a full network view so that when a request came in, it would actually tell the user or administrator what firewalls needed to be changed”

— Manager, Network Security, Top 20 Global Bank

Full visibility entails gaining multiple layers of knowledge across your hybrid infrastructure.

These layers include...

1. Which security devices, workloads and apps are running both on-prem and in the cloud
2. What connections those devices or programs are allowing
3. History and ownership of access or security policy changes
4. If policies in force are in or out of compliance

Moved from annual
rule review cycle
to **daily rule
reviews**, vastly
improving
security posture.

About Tufin

Tufin (NYSE: TUFN) simplifies management of some of the largest, most complex networks in the world, consisting of thousands of firewall and network devices and emerging hybrid cloud infrastructures. Enterprises select the Tufin Orchestration Suite™ to increase agility in the face of ever-changing business demands while maintaining a robust security posture. The Suite reduces the attack surface and meets the need for greater visibility into secure and reliable application connectivity. With over 2,000 customers since its inception, Tufin's network security automation enables enterprises to implement changes in minutes instead of days, while improving their security posture and business agility.



TD20220427

Tufin, Unified Security Policy, Tufin Orchestration Suite and the Tufin logo are trademarks of Tufin. All other product names mentioned herein are trademarks or registered trademarks of their respective owners.

Copyright © Tufin 2022

