Technology Partner Solution Brief

How to achieve 24/7 network security audit readiness

Overview

Failing a compliance audit can result in fines and penalties, reputational damage, loss of business opportunities, and even legal action. Beyond the audit, lack of compliance with industry standards often indicates a subpar security posture that increases the odds of a security incident wreaking havoc on the business.

Audit readiness is more difficult than ever before, largely due to the intricate, rapidly changing nature of today's networks.

Key challenges to cybersecurity audit readiness include:

- Hybrid network complexity.
- Multi-vendor environments.
- Fragmented visibility and processes.
- Bandwidth and resource constraints.
- Manual change management.
- Lack of policy hygiene and documentation.

The average cost of a data breach for organizations with high levels of noncompliance is $1.04 million greater than those with low levels of noncompliance.

[Source]

How to achieve 24/7 network security audit readiness

The best way to overcome these challenges is to implement a strong network security compliance program. A NetSec compliance program is the global set of policies, procedures, and practices designed to help the enterprise identify and manage risks while maintaining compliance with relevant regulatory requirements, industry standards, and internal obligations.

Because most enterprise networks are too large and intricate to handle on a per-vendor or per-device level, organizations need a solution that integrates with all existing infrastructure to make the hybrid network much easier to manage while achieving continuous compliance. Tufin makes audit readiness a practical reality while facilitating desired outcomes such as:

- Audit readiness in hours (rather than days, weeks, or months).
- Ideal state of continuous compliance.
- Reduced risk exposure.
- Faster, safer application delivery.
- Increased operational efficiency.

Here are the core areas NetSec teams must address to achieve 24/7 network security audit readiness.

Understand the current state of the network security policy and evaluate risk

The first step toward audit readiness is to take stock of the current state of the hybrid network and **develop a strong understanding of the organization's risk exposure and how many risky rules exist across the network.**

During this stage, the NetSec team will collaborate with the compliance team to determine how remediation efforts across both of these areas should be prioritized. This includes developing a vulnerability remediation plan to ensure that sensitive assets are not exposed to vulnerabilities. Proper segmentation is also a necessary practice for reducing your total attack surface and number of vulnerabilities. For example, an organization might segment their PCI zone from their network to confirm that they align to the standards set by the PCI-DSS council.

A large U.S. financial services company used Tufin to **automate cleanup and decommissioned 18,000 redundant rules in one day** while tightening network security.

[Source]

It's worth noting that, even though full audit readiness has yet to be achieved, it's still important to practice transparency on your compliance journey and keep key stakeholders in the loop. Report to leadership on progress toward hybrid network visibility and vulnerability remediation goals.

Tufin provides end-to-end network visibility and automation so NetSec teams can carry out this foundational phase of audit readiness with far less manual effort. The platform's security best practices report, for instance, runs out of the box with minimal configuration to perform analysis on the frequency and severity of risky rules across the network. Tufin can also integrate with vulnerability scanners (Tenable, Qualys, Rapid7, etc.) to diagnose if any critical assets (e.g., PCI databases) have a direct pathway to a known vulnerability, further increasing the likelihood of a breach. Combining vulnerability data with Tufin's subjective understanding of the network accessibility state can help your organization manage mitigation efforts and determine which risks are actually the highest priority.

Design and refine appropriate network access policies

Policies are the central component of a strong network security compliance program. Enterprises must define and enforce security policies that control who can talk to whom, and what can talk to what across the hybrid network.

To create effective policies that ensure compliance, **you will need to codify audit requirements related to network access and traffic flows.** This involves further collaboration between NetSec and compliance teams to define expected, permissible connectivity between zones, workloads, and applications. At the end of the day, you need to ensure that what defines risk for the compliance team means the same thing for the Net Sec team.

That's why you need a single place to design, refine, and manage network security policies — a Unified Security Policy (USP). Starting to develop a USP should go hand in hand with a rule cleanup plan to optimize firewall performance and ensure compliance. For example, regulatory requirements such as PCI DSS require regular cleanup of unused firewall rules and objects.

This will provide a necessary foundation for audit readiness and continuous compliance automation. A USP lists all security zones in your environment and identifies traffic that must be blocked or allowed between security zones. Key objectives and outcomes related to audit readiness include:

- Provide documented evidence of network compliance with policies while prioritizing the remediation of policy violations.
- Establish consistent, auditable policy exception designation management encompassing future re-evaluations.
- Track alerts of policy violations or unusual activities that could indicate unauthorized access to sensitive assets.

Tufin is the best way to practice USP management across on-premise, cloud-native, and hybrid cloud environments. The platform simplifies the translation of business requirements so teams know exactly what changes need to occur in order to become compliant. It also includes templates for compliance with regulatory standards so you don't have to start your USP from a blank state.

Ultimately, Tufin's centralized and automated network security policy management significantly boosts operational efficiency for security teams, resulting in improved resource utilization and tangible savings for the business

Three-year, risk-adjusted present value for the composite Tufin customer includes a **$5 million ROI tied to security policy management and audit cost savings.**

[Source]

Streamline change processes

When it comes to actually implementing policies you've designed and ensuring your entire rulebase remains compliant, it is necessary to establish effective change processes so you can:

1. **Reduce the likelihood of misconfigurations** (the top cause of cloud breaches).
2. **Facilitate network changes as part of the cleanup process.**
3. **Prevent noncompliant rules or access flows from being introduced to the network.**

Comprehensive change management ensures that every network change has a complete audit trail that captures its who, what, when, and why. This includes defining and codifying roles, responsibilities, and ownership as part of the change process, as well as documenting the business justification for change requests.

To meet these needs, NetSec must have a repeatable way to manage network changes and demonstrate enterprise-wide compliance without disrupting business agility. The way many teams currently manage changes (spreadsheets, Visio diagrams, emails) is too time- and resource-intensive, and can lead to missed SLAs, network downtime, and noncompliance incidents.

The composite Tufin customer sees a **94% efficiency improvement for network change analysis and implementation.**

Tufin's network change design automation maintains harmony among rules and policies across rapidly changing environments. The platform offers customizable compliance templates and access change workflows that can be used to automatically evaluate proposed changes (access requests, rule modifications, etc.) and associated risk. These repeatable, auditable, and policy-driven processes improve security for your organization while making it easier to achieve 24/7 audit readiness.

Establish continuous compliance operations

Everything up until this point has been done to lay the foundation for **continuous compliance operations — a comprehensive, searchable audit trail demonstrating the lifecycle of sensitive data and application access,** including a complete history of change requests.

Tufin facilitates proactive, integrated risk analysis to enforce and demonstrate compliance while preventing regulatory violations and associated fines. The platform includes everything you need to produce audit-ready network security reports; you can even give auditors read-only access to the Tufin Console where they can review compliance metrics and evidence themselves.

Another way in which Tufin drives continuous compliance operations is via its ability to fully automate remediation activities in response to risks classified as critical. For instance, if your vulnerability scanner delivers new threat intel, Tufin can automate the process of closing off access flow to critical assets. The tool can also automate rule recertification, send timely messages to owners about single-click recertification or initiation of processes to disable, modify or decommission a rule.

A large utility company in EMEA used Tufin's automation capabilities to enforce a consistent, fully documented change process and **cut down audit preparation to just one to two days.**

tufin

The stress-free path to audit readiness

Preparing for an audit doesn't have to be a nightmare. Tufin quickly transforms this process from a painstaking, labor-intensive activity that can take weeks into a largely automated, hands-off process that takes just a couple days.

To learn more about how Tufin can help your business move quickly while improving security posture and achieving continuous compliance, watch Stay Audit-Ready Anytime:

How to Boost Cyber Compliance Efficiency by 95%.

About Tufin

Tufin provides a single platform for network and cloud security teams to simplify the management of security policies across today's complex, multi-vendor hybrid networks. The platform gives some of the largest companies in the world the end-to-end visibility and automation tools necessary to swiftly provide new access, enable fast and secure application deployment, and ensure continuous compliance and audit readiness. Tufin's proven solutions help more than 2,000 customers across industries including healthcare, financial services, utilities, telecommunications and retail to quickly identify and mitigate network risks. For more information, please visit www.tufin.com.