Technology Partner Solution Brief

How To Extend Network Security Into The Cloud

Overview

Enterprise networks have changed significantly in recent years. The cloud has introduced new flexibility — and complexity — that make network security look much different than it did a decade ago. As a result, NetSec teams now have to view their jobs in a fundamentally different way.

The cloud has caused an explosion in network tool and solution adoption, unprecedented speed and fluidity (that can lead to misconfigurations), a pressing need for NetSec to align with applications teams, and a new world of compliance that makes audit readiness more difficult.

This evolution equates to a new threat landscape, along with a host of new responsibilities that are a significant ask for security teams. That's why it is vital that NetSec pros are equipped with the right knowledge and tools to secure the hybrid network. Adequate preparation will allow them to fulfill their core objectives:

- Empower the business.
- Enable users to do their work.
- Protect sensitive and critical data.
- Monitor threats as they evolve.
- Ensure compliance and audit readiness.

More than a third (36%) of enterprise technology professionals don't feel fully equipped to manage hybrid network complexity, and only 8% feel extremely confident.

[Source]

How to extend network security into the cloud

Enterprises must accept that change is needed to help network security enable rapid progress across the business while increasing security and agility. Fortunately, this transformation will result in less stress and greater bandwidth for team members to focus on strategic, high-value work. Here are four ways NetSec can work smarter, not harder, to improve enterprise security and compliance.

Achieve consolidated, end-to-end visibility

The foundation for effective hybrid security lies in visibility. Without complete network visibility, the gaps between disparate technologies will inevitably create blind spots. This creates unmeasured risk and misconfigurations that can go undetected for long periods of time.

According to research from Enterprise Management Associates (EMA), only 34% of organizations believe they are successful in their approach to visibility, with architectural complexity, skill gaps, and limited visibility into the cloud named as top challenges. Many of these issues stem from the fragmented nature of large, multi-vendor hybrid cloud environments. Siloed tools — and teams — are not communicating as much as they should be.

To overcome these challenges, enterprises must think about visibility more holistically. **End-to-end visibility encompasses more than just network enforcement information — you need to leverage and integrate all of the tools in your security stack**. For example, when managing access requests and policy changes, being able to bring in data from your vulnerability management solution, your governance, risk, and compliance tools, etc. is critical to making the most informed decisions on how to keep the hybrid network secure while promoting business agility.

Tufin offers an all-in-one solution that unlocks end-to-end network visibility across the hybrid cloud, no matter the product or provider. Without a consolidated network visibility platform like Tufin, NetSec has to check a variety of tools and consoles just to gain a vague picture of whether or not security mechanisms are configured properly to effectively protect the organization — a major waste of time and resources.

Tufin allows NetSec teams to extend the same level of awareness and control they are used to having in traditional networks into the cloud. The platform provides the broadest possible coverage of your environment at scale, eliminating blind spots and enabling strong security governance. Its industry-leading topology map, for instance, offers dynamic visualizations of all network devices and zones for real-time analysis and troubleshooting.

> "Before, we were always focused on getting the proper rules in place and not being able to do anything else. We would have to look into every environment and which firewall goes where, which was difficult due to the complexity of our environment."
>
> – Technical lead forsecurity, financial services company
>
> *[Source: TEI of Tufin Report]

Increase speed while reducing risk of breach

For hybrid network security to operate at the speed of the cloud, the enterprise has to practice proactive network change management — real-time risk identification for every proposed network or cloud change and its impact on security posture.

Step 1:

The first step toward proactive change management is to review your access policy change processes to ensure that requested changes are being properly approved, implemented, and documented. For all requests, you should be able to answer essential questions such as:

- Is the requester documented, and are they authorized to make this change?
- Is the business reason for the change documented, including any impact on network devices and topologies?
- Were the approvals recorded before the change was implemented?
- Are the changes well documented in the change ticket, including any required remediation or cleanup?
- Is there documentation of risk analysis for each change, including prioritizing and aggregating risks?

Step 2:

Next, take inventory of all firewall and security group rules that are currently in place. Ideally you will use a global security policy, a single place to design and manage requirements for governing segments and traffic across your hybrid network. Ask questions such as:

- How many rules does the rulebase currently have compared to last year?
- Are there any redundant rules that should be removed?
- Are there any policy rules that are no longer used, including VPN or network environments?
- Are there any overly permissive rules (e.g., rules with more than 1,000 IP addresses allowed in the source or destination)?
- Are there any rules that violate our corporate compliance requirements (e.g., HIPAA, PCI DSS, SOC, etc.)?

Having completed these steps, you will be able to get started with policy-driven automation that allows changes to be implemented in minutes rather than days while removing the chance of human error resulting in misconfigurations — the #1 cause of security breaches in the cloud.

Tufin has everything you need to adopt an automated, policy-based approach to meet business demands and eliminate tradeoffs between agility and security. For example, the platform's Unified Security Policy (USP) Builder lists all security zones in your environment and identifies traffic that must be blocked or allowed between security zones.

Tufin also offers customizable templates and 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 reduce risk for your organization while making it easier to maintain continuous compliance.

The composite Tufin customer sees a **75% reduction in manual effort related to application connectivity management.**

*[Source: TEI of Tufin Report]

Maintain continuous compliance and audit readiness

The pinnacle of hybrid network security is to attain continuous compliance and audit readiness. This means the business is always ready to undergo and pass a third-party audit to verify that your network infrastructure, security controls, and practices comply with relevant security policies, industry standards, and regulatory requirements.

The truth is that effective, 24/7 compliance for the hybrid network is impossible to achieve without automation. Any manual, "snapshot in time" inventory of controls almost immediately becomes obsolete. This is a major reason why Flexera's 2022 State of the Cloud report found that compliance is a top cloud challenge for 76% of organizations.

The composite Tufin customer sees a **95% efficiency gain for audit preparation and reporting activities.**

*[Source: TEI of Tufin Report]

Tufin offers the most efficient path toward continuous compliance and audit readiness. The platform facilitates and automates essential activities, giving NetSec the ability to:

- Always see and understand the current state of hybrid network infrastructure and identify areas that don't comply with policies.
- Set up and issue real-time alerts for automated monitoring to ensure continuous compliance.
- Define a Unified Security Policy that works across even the most complex infrastructures (multi-vendor, multi-platform, multi-cloud, etc.) to simplify policy review and management.
- Identify compliance violations before they occur as part of an automated change process.
- Access and automate an audit trail of all changes and approvals which can be used to generate a variety of customizable reports for standards such as PCI DSS, NIST, SOX, NERC CIP, and more.

The fastest path to integrated hybrid network security

NetSec must adopt a new toolkit to successfully adapt to the new enterprise network. Tufin is the best way for security teams to achieve the desired results while working smarter and avoiding burnout. Our platform offers unified, end-to-end network visibility and unparalleled security automation across network and cloud environments. With the power of Tufin, your teams will be able to deploy apps faster, remediate issues more quickly, maximize efficiency, and stay audit-ready year round.

tufin The Security Policy Company.

WHERE NETWORK SECURITY MEETS THE CLOUD

6 Ways the Cloud Changes Everything About Enterprise Network Security.

To learn more about how cloud computing has altered the way enterprises approach security, download 6 Ways the Cloud Changes Everything About Enterprise Network Security.

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.