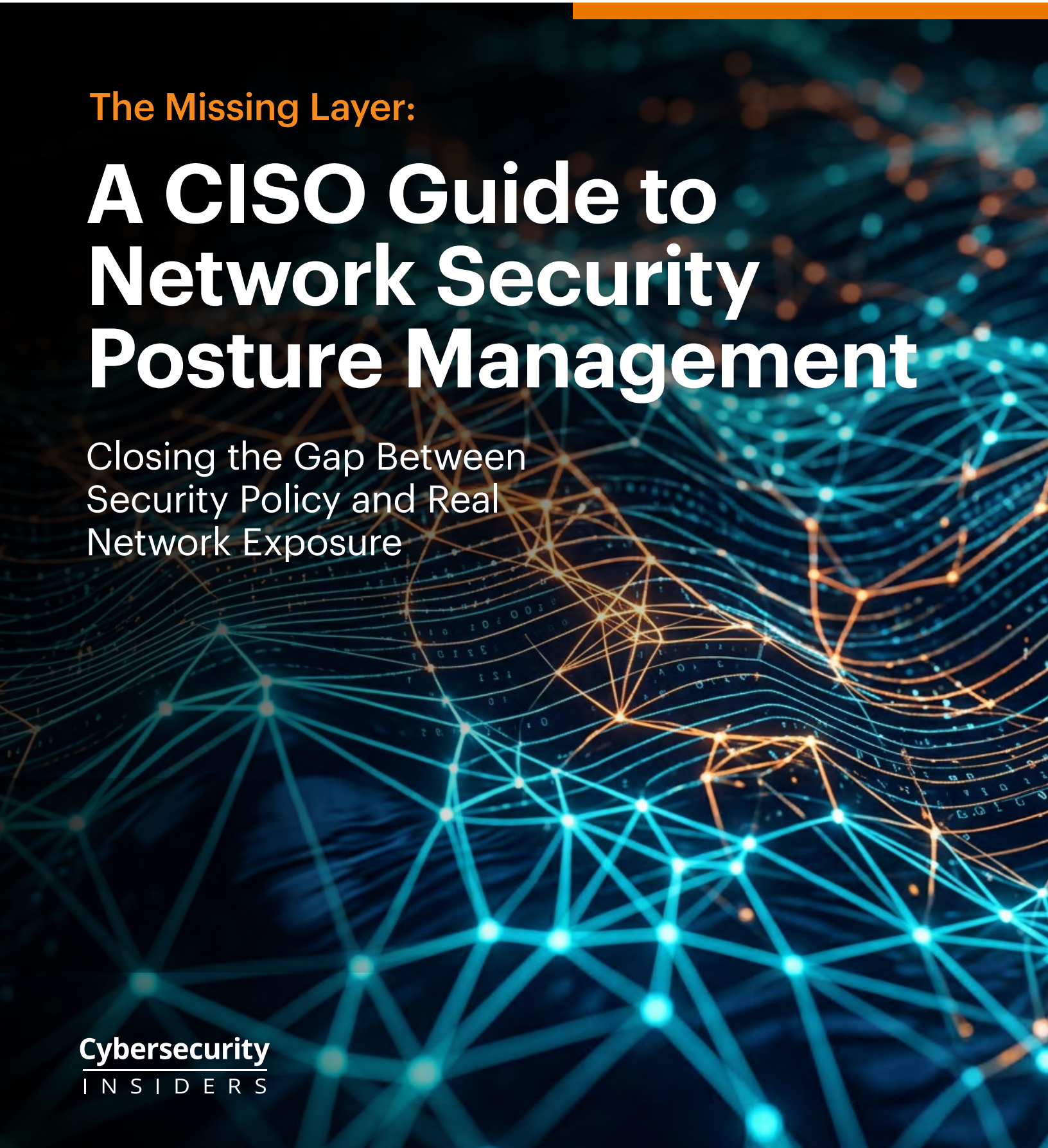
tufin

The Missing Layer:

A CISO Guide to Network Security Posture Management

Closing the Gap Between Security Policy and Real Network Exposure



Cybersecurity INSIDERS

tufin

Executive Summary

The network is the layer where security policy gaps become real exposure. If network posture is unknown, organizations cannot reliably prove which assets are reachable, whether segmentation is holding, or whether policy intent is actually being enforced.

Threat actors weaponize AI to compress the time between discovery and exploitation, and manual network validation cannot keep pace. Recent BCG research[1] found that 60% of companies may have faced AI-enabled attacks in the past year, while only 7% are using AI in defense. The network layer, where those attacks actually traverse, is where that gap matters most.

Cloud, identity, data, and application security have each adopted continuous posture management to tackle these challenges. **The network was the exception, until now.**

Network Security Posture Management (NSPM) is the discipline that closes this gap. If an organization cannot continuously validate the network, it cannot confidently prove that segmentation and exposure controls are working as intended. While other posture management tools look for misconfigurations, the goal of NSPM is threefold.

3 Principles of NSPM

1. **Continuously validate that network controls enforce intended policies:** Leadership should be able to verify that security policies are working as intended and hold teams accountable when they are not.

2. **Confirm that segmentation boundaries are holding across every vendor and environment:** Networks change constantly and segmentation guidelines that are not validated in real time quietly stop being segmentation at all.

3. **Identify which assets are reachable through live network paths:** Knowing which vulnerabilities lead to reachable critical assets is the difference between a minor incident and a breach.

This guide explains why the network has remained unvalidated despite decades of security investment, what NSPM must deliver, and how organizations can build toward continuous network validation in four concrete phases.

Source: Boston Consulting Group, "AI Is Raising the Stakes in Cybersecurity," December 2025. Survey of 500 senior leaders globally.

tufin

The Network Security Gap

Regardless of entry point, attackers must traverse the network to reach their objectives. Yet most organizations cannot answer a basic question on demand: what is reachable, and through which network paths?

In a 2026 survey of 600+ cybersecurity professionals conducted by Cybersecurity Insiders, only 11% said they could confidently report on east-west segmentation posture without advance notice. 58% said they could not. Confidence drops further across cloud networks (35% not confident), remote access environments (46%), and the internal segmentation boundaries where lateral movement actually occurs.

58%
cannot report
east-west segmentation posture on-demand.

– 2026 Cybersecurity Insiders Survey

That gap is widening. Attackers operate on the same clock, using AI to discover exposure and map lateral paths faster than periodic human review can catch them. The window between a control drifting out of policy and an attacker finding the opening is collapsing, and point-in-time validation cannot close it.

Every Security Domain Has Posture Management Except the Network

Every major security domain now has a posture discipline that continuously validates whether controls are configured correctly and exposure is understood. The network remains the exception, even though every other posture discipline ultimately depends on it.

Domain	What Posture Management Validates	Consequence When It Fails
Cloud/CSPM (Established)	Configuration drift, workload exposure, and cloud network exposure	Data exposure, compliance violations, workload compromise
Identity/ISPM (Maturing)	Privilege creep, entitlement sprawl, access policy drift	Unauthorized access, privilege escalation
Data/DSPM (Maturing)	Sensitive data discovery, access controls, and data exposure	Regulatory violations, uncontrolled data exposure
Application/ASPM (Maturing)	Application vulnerabilities, API exposure, and runtime risk	Application exploits, supply chain compromise
Network/NSPM (Gap)	Reachability, segmentation integrity, and control enforcement validation across network environments	Undetected lateral movement. Controls across all other domains ultimately depend on a network layer that may not be validated

If the network lacks its own posture discipline, the question becomes what such a discipline must actually deliver. The next section examines the core capabilities required to continuously validate network exposure and control enforcement across the entire control plane.

Why Network Posture Is So Hard to Prove

Network posture is difficult to prove, but not due to a lack of controls. Instead, it is the structural difficulty of proving how they work together. Seven structural constraints make continuous network validation difficult:

1 Distributed, multi-vendor architecture

Posture emerges from how firewalls, cloud-native security groups, SASE policies, and microsegmentation controls interact across five or more vendors. No single console shows the full picture.

2 Fragmented ownership

Network Security, CloudOps, platform teams, and data center operations each manage part of the environment. Exposure accumulates at the seams between teams.

3 Hybrid complexity

On-premises, multi-cloud, SASE/SSE, and legacy platforms each use different consoles and rule syntax. Exposure appears where environments interoperate. Forrester reports 39% of leaders say their organizations are losing control due to rising complexity.

4 Policy enforcement gap

Policy is defined at the organizational level; enforcement happens across many technologies. The translation between intent and implementation is where posture quietly falls apart.

5 Constant change

Deployments, migrations, and maintenance constantly reshape the network. AI-assisted tools now initiate changes without direct human review. The result is operational residue: temporary access that became permanent, application paths left open after migration, overlapping rules, and exceptions long past their business reason. It is exposure no audit can catch.

6 Operational bias toward availability

Network teams are measured on uptime and consistently choose permissive configurations over restrictive ones. Over time, the network becomes more "open" than leadership intended.

7 Legacy validation

Periodic audits and manual rule reviews produce snapshots that are outdated the moment they finish. Point-in-time review is not the same as posture management.

Of these seven, the policy enforcement gap matters most to CISOs: each control may look reasonable in isolation while the combined end-to-end posture still violates intended policy. Recent edge-device exploitation patterns illustrate the issue: the controls existed, but no one could continuously validate whether drift, reachability, and effective exposure matched policy intent.

tufin

From Policy Management to Posture Management

The network posture gap is not new. What has changed is the tempo: networks now change at machine speed, with less direct human oversight than ever before, while the cost of leaving the gap unresolved continues to rise.

Four converging pressures make it urgent to close now: In a 2026 survey of 600+ cybersecurity professionals conducted by Cybersecurity Insiders, 78% rate full network visibility as critical, yet few organizations can actually deliver it. Traditional tools show vulnerabilities and alerts but rarely reveal the network paths that connect them. As attackers increasingly use AI to map those paths faster than defenders can manually trace them, continuous modeling of real reachability becomes essential.

Machine-speed change and machine-speed attacks

Networks are changing faster than ever, as automation and AI-assisted tools take on a larger share of routine infrastructure and policy changes. At the same time, attackers use AI for exposure discovery, lateral-movement mapping, and drift exploitation, often faster than periodic human validation can detect them. Defenders need continuous, automated analysis on both fronts to keep pace with change and exposure alike.

Exploitability prioritization

Security teams face overwhelming volumes of vulnerability findings but lack visibility into which assets are actually reachable. Without network path context, remediation is often prioritized by severity rather than real exposure. As attackers accelerate their own discovery with AI-assisted tooling, that advantage becomes time-sensitive and defenders who still rely on periodic validation lose it.

Hybrid network complexity

Modern enterprises operate across on-premises infrastructure, multiple cloud environments, SASE platforms, and legacy networks, typically managed through a patchwork of tools from many different vendors. Security controls may function correctly within each vendor's platform but create exposure at the boundaries between them.

Regulatory accountability

Regulators and cyber insurers increasingly expect organizations to demonstrate that segmentation and exposure controls are continuously enforced rather than periodically reviewed. Recent updates to frameworks such as PCI DSS, NYDFS, and EU DORA have shifted from point-in-time assessment models toward explicit requirements for ongoing validation of network segmentation.

Traditional network security tools improved operational efficiency by automating changes, cleaning up rule bases, and managing individual platforms. NSPM operates at a different level. It verifies whether those controls actually enforce the intended security posture across the entire environment, not within a single network domain or a single vendor platform.

Policy management asks:

Can we manage and change rules efficiently?

Posture management asks:

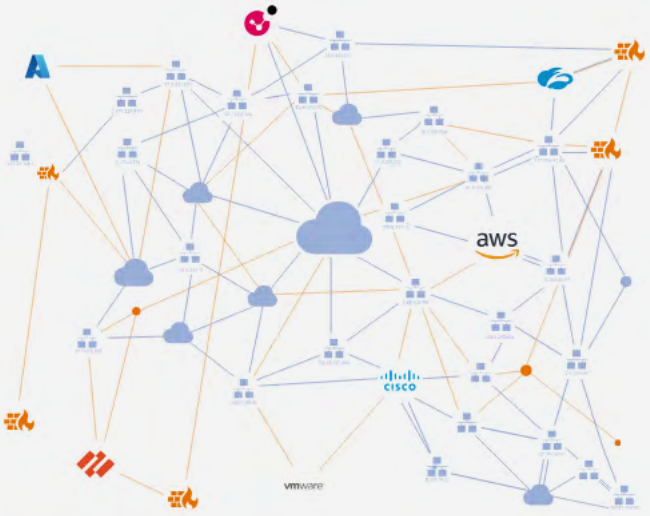
Do those controls actually create the posture we intend?

NSPM Requires a Control Plane for the Network

A posture-driven model requires something different: a unified control plane that operates above individual enforcement points. Important to note, the control plane connects existing controls; it does not replace them. It does so by normalizing policies across vendors into a common model, continuously analyzing how those policies interact, and providing a consistent way to validate and govern changes across the entire environment. Instead of asking whether a rule was configured correctly on a specific device, it answers whether the combined effect of all controls produces the intended security posture.

This distinction is what separates policy management from posture management.

With a control plane in place, posture becomes measurable, testable, and continuously validated. With dynamic connectivity and AI, networks can be easily modeled across the entire hybrid environment, policy drift can be detected as it occurs, and changes can be evaluated against intended outcomes before they reach production.



Dynamic Network Connectivity Graph

A live, accurate model of how connectivity actually works across a multi-vendor enterprise network. It shows who can talk to whom, what is actually reachable, where exposure exists, whether segmentation still holds, and whether the network still aligns with policy and security.

But the most immediate impact of that shift is in how organizations understand and prioritize risk. Without a control plane, vulnerability data and network exposure remain disconnected, forcing teams to prioritize based on severity alone. With continuous visibility into real connectivity, that gap closes.

Vulnerability + Exposure = Exploitability

Severity without exposure context produces alerts, not actionable risk. Vulnerability tools deliver the first half. NSPM delivers the second, transforming prioritization from severity scores to confirmed, reachability-based risk.

The network is also one of the few domains where defenders hold a structural analytical advantage: **reachability is determined by rules and configurations that can be traced before an attack occurs.**

That means defenders can adjust rules and tighten exposure before attackers discover the gaps, not after. As attackers accelerate their own discovery with AI-assisted tooling, that advantage becomes time-sensitive, and defenders who still rely on periodic validation lose it.

Only 8%
of organizations can automatically determine whether a critical vulnerability is actually reachable through the network.

– 2026 Cybersecurity Insiders Survey

tufin

What NSPM Delivers

Network Security Posture Management continuously validates that network controls enforce the organization's intended security posture across the entire environment. It answers the questions that matter: which paths exist, whether segmentation holds, and whether controls still behave as designed. The value of NSPM becomes most concrete in the operational problems security teams deal with every day. The scenarios below illustrate where continuous posture validation changes the outcome.

Network Exposure Visibility

NSPM provides a unified control plane that maps every reachable path across on-premises data centers, private and public cloud, edge and remote networks, and microsegmentation boundaries.

Attack Path Analysis

NSPM's digital twin models real reachability across the environment, allowing teams to identify and close high-risk attack paths before they are exploited.

Vulnerability Prioritization

NSPM overlays reachability analysis onto vulnerability findings, enabling teams to focus remediation on vulnerabilities that are actually exploitable.

Change Risk Reduction

NSPM simulates proposed changes before production and validates them against security policy and compliance mandates.

Rapid Exposure Containment

NSPM accelerates response by identifying affected assets, proposing containment changes, simulating their impact, and routing approved actions through operational workflows.

Continuous Compliance Evidence

NSPM supports continuous control validation and faster evidence generation across frameworks such as PCI DSS, SOX, HIPAA, and NERC CIP.

tufin

NSPM in Action

The operational challenges described in the previous section appear across many industries. The examples below illustrate how continuous network posture validation changes the outcome in real environments.

Healthcare: From 347 Critical Findings to 89 Confirmed Exposures

Using network reachability analysis to prioritize real risk

ENVIRONMENT:

A healthcare organization operates hundreds of networked medical devices (including X-ray systems, diagnostic equipment, and mobile clinical platforms) across a complex hybrid network where patient-care requirements make broad patching infeasible.

CHALLENGE:

Vulnerability scanners flagged 347 critical issues. The security team had no reliable way to determine which devices were actually reachable from untrusted zones. Manual remediation often took a week or more per device, leaving patient-facing systems potentially exposed during that time.

WHAT NSPM CHANGED:

Once the topology model was operational, automated reachability analysis revealed that only 89 of the 347 critical vulnerabilities were on assets actually reachable through live network paths. The remaining 258 were behind effective segmentation.

For the 89 confirmed exposures, NSPM generated containment policies, simulated each against the live topology, and isolated affected devices (including X-ray machines directly accessible from untrusted zones) within minutes, without interrupting patient care.

74%
reduction in critical remediation workload (347 to 89)

<1hr
Remediation time per device: from more than a week to under an hour

0
patient care disruption

Audit-ready HIPAA segmentation evidence generated automatically and continuously maintained

tufin

Making the Case

Business Outcomes

When organizations gain continuous evidence of network exposure and control effectiveness, several operational and business outcomes follow:

Improve exposure visibility:
Security teams gain a clear view of which assets are actually reachable and which network paths connect them. This visibility replaces fragmented console views with a unified, continuously validated topology of the environment.

Prioritize real risk:
Reachability analysis reveals which vulnerabilities are actually exploitable. Instead of prioritizing remediation based on severity scores alone, teams can focus effort on exposures that truly create risk.

Reduce remediation workload:
By distinguishing reachable vulnerabilities from those already contained by segmentation, organizations eliminate unnecessary emergency remediation and focus resources on the exposures that matter most.

Provide continuous compliance evidence:
Network segmentation and exposure controls can be validated continuously rather than reconstructed during audits. Evidence becomes available on demand across frameworks such as PCI DSS, HIPAA, SOX, and NERC CIP.

Increase confidence in security decisions:
CISOs and security teams gain evidence-based answers to critical questions about exposure, segmentation effectiveness, and control enforcement, replacing assumptions with continuous validation.

Reduce breach probability:
By identifying exploitable paths and validating control enforcement across the network layer, organizations reduce the likelihood that attackers can move laterally to reach critical assets.

From Posture Management to Board-Level Confidence

These outcomes typically emerge as organizations move from fragmented visibility toward a posture-driven operating model. The technical case for NSPM is straightforward. The harder conversation is explaining the risk and business value to the CFO, the board, or the risk committee.

The board-level question is no longer whether security investment is sufficient, but whether the organization can prove its core controls still enforce intended posture as environments grow more dynamic and more automation-driven. As more decisions are initiated by automated systems and as more of the network changes faster than any human can review, boards need evidence — not assurance — that the controls they have funded are still doing what they were funded to do. NSPM is how that evidence is generated and maintained.

What CISOs Are Now Expected to Prove

Boards, regulators, and cyber insurers now expect security leadership to demonstrate that segmentation, reachability, and exposure controls are continuously enforced and continuously verified, not validated only when an audit demands it.

What they actually can prove today.

Most organizations can produce point-in-time evidence: last quarter's audit report, last month's scan, last week's compliance attestation. Few can produce live evidence of how the network actually behaves right now.

What they cannot answer quickly.

When a board member asks, "Which assets are reachable from the internet at this moment, and which segmentation controls would slow lateral movement if a breach happened tomorrow?", most CISOs who are in the room cannot answer the question.

Where Is Your Organization Today?

Fragmented Weeks (Manual)	**Consolidated** Days (Coordinated)	**Posture-Driven** Minutes (Automated)
Platform-specific consoles. Manual path tracing. Retroactive compliance evidence.	Visibility across most environments but gaps at the edges. Faster but still manual audit prep.	Continuous modeling across every environment. Evidence always current.
"Which assets are reachable from the internet right now?"	*"Can you show segmentation posture across every environment?"*	No major posture questions lack an evidence-backed answer. Posture questions are answered from live data, not reconstructed after the fact.

60-Second Posture Self-Assessment: Four questions to place your organization on the maturity curve.

1. Can you analyze network connectivity across every environment today: on-premises, cloud, and edge or remote networks? (If no: Fragmented)
2. Are network changes validated against security policy intent before deployment? (If no: Fragmented)
3. Can you generate compliance evidence on demand without manual assembly? (If no: Consolidated at best)
4. Do you know which critical vulnerabilities are reachable through live network paths right now? (If no: Consolidated at best)

If every answer is yes, your organization is operating at a posture-driven level. If any answer is no, the maturity table above highlights the gaps, and the implementation roadmap in the next section shows where to begin.

tufin

Getting Started

Once an organization understands its current maturity level, the next question becomes practical: how to begin moving toward continuous posture validation. The four execution phases map directly to the Fragmented, Consolidated, and Posture-Driven maturity levels, providing a practical path from fragmented visibility to posture-driven operations.

PHASE 1 → PHASE 2 → PHASE 3 → PHASE 4

Establish Unified Visibility

Fragmented > Consolidated

Days to weeks

Led by: Network Security

- Connect enforcement points across on-premises firewalls, cloud security groups, SASE/SSE services, and data center infrastructure into a unified topology model.
- A complete asset inventory is not a prerequisite; the model reveals what is missing.

VALUE:
Reachability questions that took days become answerable in minutes.

Policy Governance and Drift Detection

Consolidated

Weeks to months

Led by: Network Security + SecOps

- Establish a normalized policy model that translates vendor-specific rule formats into a unified control framework.
- Enable automated drift detection and connect change management workflows for pre-deployment validation.
- Fully documented baselines are not required – the normalization process formalizes existing configurations as it goes.

VALUE:
Every network change is validated against policy before deployment. Beyond compliance, the normalization and drift detection capabilities established in this phase create the policy-aware foundation that any safe agent-assisted workflow depends on later.

Continuous Compliance Validation

Consolidated > Posture-Driven

Weeks (value immediate)

Led by: GRC

- Map regulatory frameworks (PCI DSS, SOX, HIPAA, NERC CIP) directly to network segmentation and access controls, reflecting the shift in recent framework updates toward stronger evidence of control effectiveness.
- Enable continuous evidence generation.
- Pre-built framework mappings accelerate deployment; organizations do not need to build compliance logic from scratch.

VALUE:
Audit preparation shifts from weeks of fire drills to on-demand evidence generation.

Exposure Context and Rapid Containment

Posture-Driven

Days (scanner), months (automation)

Led by: SecOps

- Connect vulnerability scanner data to the topology model.
- Enable reachability-based exploitability analysis and automated containment.
- Standard vulnerability scanner integrations allow reachability analysis to become operational within days, while full remediation automation can mature over time.

VALUE:
In one documented deployment, reachability analysis reduced critical remediation workload by 74%. Containment drops from weeks to under an hour.

Beyond Phase 4: The Agentic End State

Once topology, policy normalization, continuous validation, and exposure context are in place, the network posture foundation exists for something new: AI agents that operate against a trusted model of how the network actually behaves. Without that trusted model beneath it, AI can recommend changes that look technically valid but are operationally unsafe, miss exposure because it lacks end-to-end context, or create governance gaps the organization cannot explain.

The goal is trusted autonomy:
AI that operates inside boundaries the enterprise can govern and prove. Organizations that have built this foundation can safely introduce agent-assisted prioritization, recertification, and containment, and not as a replacement for human judgment, but as a way to keep pace with change velocity that manual review cannot match.

Measuring the Shift

Metric	Without NSPM	With NSPM
Path Analysis	Hours (manual)	In real time (automated)
Change Risk Analysis	Days/weeks	Pre-deployment (simulated)
Audit Preparation	Weeks (fire drills)	Continuous (always-on)
Vulnerability Prioritization	Severity-based remediation	Exploitability-based prioritization (74% workload reduction)

Organizations do not need to complete all four phases to realize meaningful value. As the healthcare case study demonstrates, Phase 1 visibility alone can transform how a security team understands and acts on its own environment.

tufin

Conclusion

The phases above resolve the tactical question of how to begin. The strategic question is harder. The gap between what security leaders prioritize and what their organizations can actually prove has become a defining security challenge. 78% of organizations rate full network visibility as critical, yet only 11% can deliver it on demand. That gap is structural and will widen as hybrid environments expand, attacker timelines compress, and regulators increasingly expect current evidence of control effectiveness.

Tools designed primarily for policy management and operational efficiency cannot answer the exposure questions modern security leadership is accountable for. Network posture is not about operational efficiency. It is about governance credibility.

Network Security Posture Management addresses that gap. It shifts network security from assumed posture to continuous proof, from severity-based prioritization to reachability-based risk, and from isolated tools to strategic control of exposure.

If an organization cannot continuously validate the network, it cannot confidently prove that segmentation, reachability, and exposure controls are functioning as intended. In that situation, every other posture discipline rests on an unverified foundation.

Next Steps

The first step is understanding your current posture maturity and where continuous validation is missing.

Organizations can begin by assessing exposure visibility across every environment, reviewing segmentation enforcement against stated policy, and identifying where evidence is reconstructed after the fact rather than generated continuously. From that baseline, the path toward posture-driven operations becomes a sequence of concrete gaps to close, and the practical way to measure progress against the four phases described in this guide.

Tufin's unified control plane and Dynamic Network Connectivity Graph were built to deliver this foundation across multi-vendor hybrid environments. Organizations evaluating NSPM platforms can use the maturity framework and implementation phases in this guide as a practical benchmark for any solution they consider.

To learn more or get a demo: Visit Tufin.com