tufin

White Paper

# The Six Cracks in Every Network Security Program

## and How to Close Them

© Tufin 2026

tufin

# The Six Cracks in Every Network Security Program and How to Close Them

White Paper • 2026 • Network Security Posture Management

## Executive Summary

Security teams don't lack tools, and they don't lack good intentions. What they lack is continuous proof that those intentions are actually being enforced. Walk into almost any network, big budget or small, mature program or scrappy one, and you'll find the same six cracks: rule sprawl, blind spots in visibility, manual changes, compliance burden, policy drift, and multi-vendor complexity.

**33%**
Fully segmented organizations

*In Cisco's 2025 segmentation survey of 1,000 large organizations, only 33% had fully implemented both macro- and microsegmentation, and 87% said their segmentation process needs improvement.[1] For most security leaders, that's a pretty accurate snapshot of where their own program stands today.*

Look closely at any of the six problems in this paper and you'll find the same root cause wearing a different hat: a gap between the policy an organization designed and what's actually enforced. Closing that gap continuously, not just scrambling at audit time, is what the rest of this paper is about. It's also exactly the problem Tufin Segmentation Intelligence and a new generation of purpose-built AI agents were built to solve.

01
**Rule Sprawl**
Increased risk and complexity

02
**Lack of Visibility**
Slow troubleshooting and poor decisions

03
**Manual Changes**
Delays, errors, and higher costs

04
**Compliance Burden**
Audit risk and operational overhead

05
**Policy Drift**
Inconsistent security and governance

06
**Multi-Vendor Complexity**
Operational inefficiency and inconsistency

tufin

SECTION 01

# Rule Sprawl & Lack of Visibility

CRACK 1 OF 6

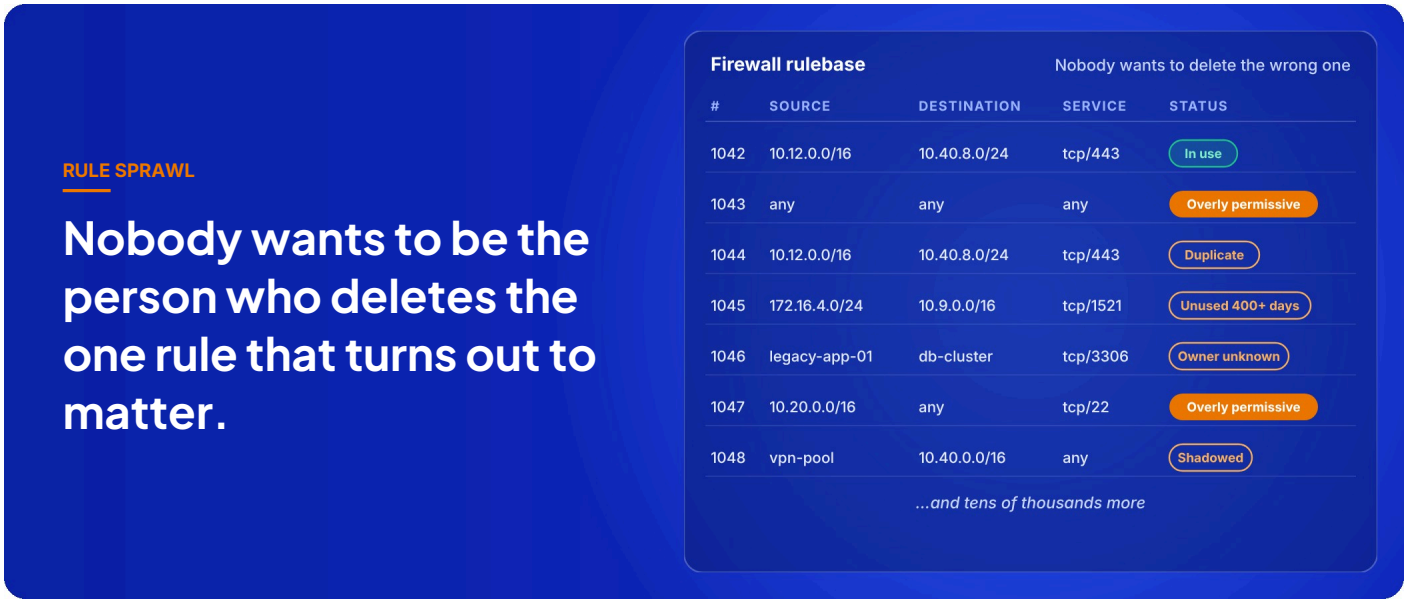
## Rule Sprawl

Firewall rules pile up for years, duplicated, outdated, and overly permissive, because nobody wants to be the person who deletes the one rule that turns out to matter.

BUSINESS IMPACT **Increased risk and complexity.**

In a mid-size enterprise, that ruleset can easily run into the tens of thousands of entries, most written for a business need that expired years ago. Every rule the team isn't quite sure about tends to just stay put, since removing the wrong one can take down a production application at the worst possible moment.

Over time the estate gets less secure and harder to reason about, even as more effort goes into managing it.




### What good looks like

Continuous rule-usage analysis and automated cleanup, not a once-a-year fire drill. Tufin identifies unused, redundant, and overly permissive rules and helps retire them safely.

tufin

CRACK 2 OF 6

# Lack of Visibility

Every vendor and every cloud comes with its own console, so security teams end up with no single place to see how traffic actually flows across the environment.

BUSINESS IMPACT **Slow troubleshooting and poor decisions.**

That fragmentation shows up fastest during an incident. An engineer chasing down unexpected traffic must log into several consoles, stitch logs together by hand, and reconstruct a path that should take seconds to trace.

The same blind spot makes it surprisingly hard to answer a simple question with any confidence: what can actually reach what, right now, across the whole hybrid estate?

**#1**

Exploitation is now the leading way into a breach

*Attackers have started to notice the same blind spot. Verizon's 2026 Data Breach Investigations Report found that vulnerability exploitation overtook stolen credentials as the leading way into a breach for the first time in the report's 19-year history, with edge devices and VPNs among the fastest-growing targets.[2]*




### What good looks like

One connectivity model spanning firewalls, cloud, SASE, and microsegmentation. Tufin keeps that model current by discovering and mapping devices, validating traffic paths, and closing monitoring gaps as the network changes.

tufin

SECTION 02

# Manual Changes & Compliance Burden

CRACK 3 OF 6

## Manual Changes

At plenty of organizations, network changes still run on email threads and spreadsheets, with deployment cycles measured in days or weeks and rules designed one vendor at a time.

BUSINESS IMPACT **Delays, errors, and higher costs.**

A single access request might touch a cloud security group, an on-premises firewall, a SASE policy, and a microsegmentation workload, each needing its own ticket, its own approver, its own manual check. The result isn't just slower delivery. It's inconsistent judgment: two engineers making the "same" change six months apart rarely make it the same way.

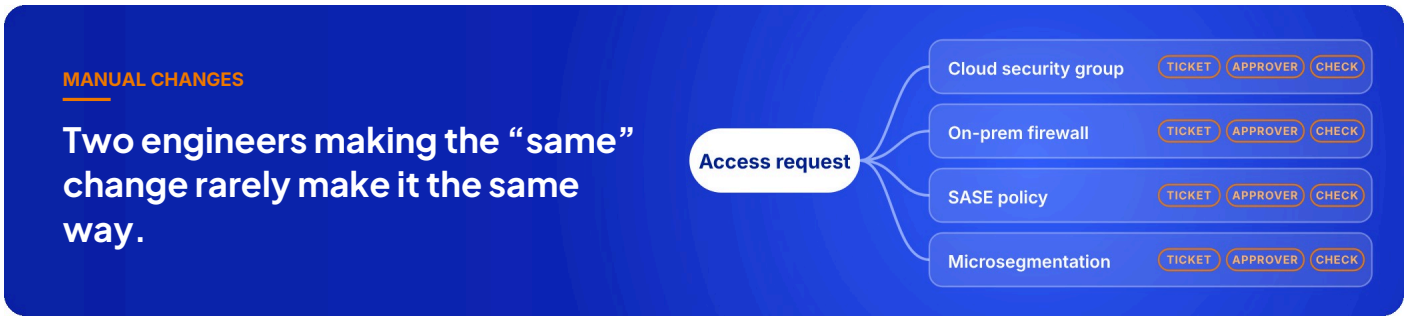
**$2M**

Median cost per hour of a high-impact outage[3]

**$600B**

Annual cost of unplanned downtime to the Global 2000[4]

*Network and IT-environment issues are behind more of that downtime than any other single cause. Manual, error-prone network changes are a direct contributor to that risk window.*




**What good looks like**

A defined access-change workflow, automation that only touches what it needs to, and a full audit trail behind every change.

tufin

CRACK 4 OF 6

# Compliance Burden

PCI DSS, NIST, SOX, and HIPAA all want proof that segmentation is enforced as designed, not just that it was designed on paper. Most teams still gather that proof by hand, in a mad scramble before every audit.

BUSINESS IMPACT **Audit risk and operational overhead.**

Passing one audit doesn't guarantee you'll pass the next. Segmentation that was compliant in January can quietly drift out of alignment by the time auditors come back in the fall, and most teams only find out when the auditor does. Without a continuous record to point to, the whole evidence-gathering slog gets repeated from scratch, every single cycle.

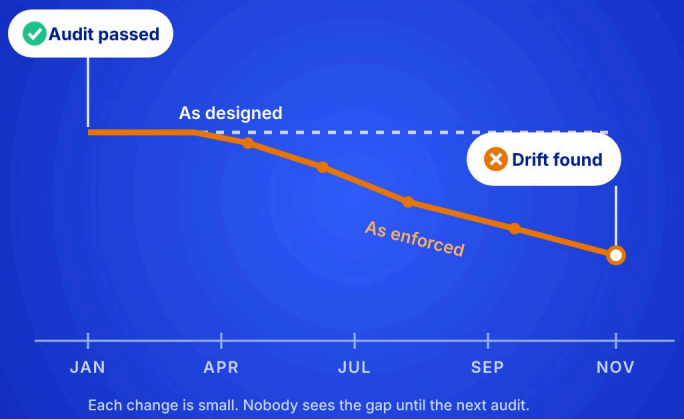
**4+**

Audits a year for most organizations

*It's also not getting any lighter. Now that SOC 2 has become table stakes rather than a differentiator, most organizations run four or more audits a year just to keep pace with client and regulatory expectations.*[5]

COMPLIANCE BURDEN

## Most teams only find out when the auditor does.




### What good looks like

An always-audit-ready posture, with reporting available whenever you need it. Tufin continuously validates segmentation and access against compliance frameworks and flags violations immediately, rather than waiting for the next review cycle.

tufin

SECTION 03

# Policy Drift & Multi-Vendor Complexity

CRACK 5 OF 6

## Policy Drift

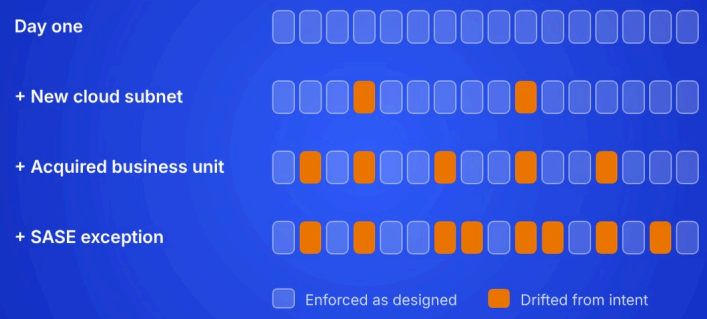
Defining segmentation intent is the easy part. Proving it stays enforced over time is where it gets hard. Cloud migrations, M&A, SASE rollouts: they all shift your posture continuously, and periodic audits simply can't keep up.

BUSINESS IMPACT **Inconsistent security and governance.**

A segmentation plan that was airtight on day one rarely stays that way. A cloud team spins up a new subnet. An acquired business unit gets bridged into the network. A SASE policy gets adjusted for a one-off exception. Each of those is an ordinary, reasonable change, and each one quietly nudges enforcement further from what was originally intended. None of it shows up until someone goes looking for it, and by then it's usually been true for months.

POLICY DRIFT

**Each ordinary change quietly nudges enforcement further from what was intended.**




### Tufin Segmentation Intelligence

This is exactly the gap Tufin Segmentation Intelligence was built to close: continuously measuring the difference between the segmentation an organization designed and what's actually enforced across the hybrid estate, so drift gets caught as it happens, not months later.

tufin

CRACK 6 OF 6

# Multi-Vendor Complexity

Palo Alto, Check Point, Cisco, Fortinet, and Juniper. Add AWS, Azure, and GCP for cloud, Versa and VeloCloud for SASE, and Illumio for microsegmentation, and each one comes with its own syntax, its own console, its own way of thinking about policy.

BUSINESS IMPACT **Operational inefficiency and inconsistency.**

A rule that's an explicit allow in one vendor's syntax might just be default behavior in another, and the same segmentation intent can take entirely different steps to implement depending on where it lands. Multiply that across vendors spanning on-prem, cloud, and SASE, and even a sharp team ends up spending more time translating policy than actually improving it.

**64%**

Would build on a single unified platform

*It's enough of a headache that, given a blank slate, most security leaders say they wouldn't choose it: 64% would build their security stack on a single unified platform if they were starting from scratch today, largely to escape exactly this kind of integration overhead.*[6]




**What good looks like**

One policy, expressed once, translated and enforced consistently across every vendor and every layer.

tufin

SECTION 04

# The Common Thread & What's Next

Every one of the six problems above is a symptom of the same root cause: organizations can define what they want their network to do, but they can't continuously prove it's actually happening.

That's the premise behind Tufin Segmentation Intelligence, and it's also the premise behind where Tufin is headed next. IT is increasingly run through agents and automation, and network change is starting to happen at machine speed while review and compliance processes are still built for human speed. Tufin's purpose-built AI agents are being built to close that gap.

### Posture Agent: coming in early 2027

Prioritizes vulnerabilities based on real connectivity exposure, attack paths, and critical assets rather than raw CVE severity.

- Real connectivity exposure, not raw CVE severity
- Attack paths mapped to critical assets
- The first of a new generation of Tufin AI agents

## More agents on the way

**Compliance Agent** | **Cleanup Agent** | **Topology Agent**

All four agents are coming in early 2027, with more planned after that. They aren't a separate initiative bolted onto the rest of this paper. Each one takes direct aim at a problem named above, and each is built on the same idea: closing the gap between intent and enforcement, continuously, instead of catching it after the fact.

*"Most security teams don't have a policy problem. They have a proof problem. When the network changes every day, enforcement has to be checked every day too, by agents that work inside the guardrails your team sets."*

Erez Tadmor, Global Field CTO, Tufin

tufin

SECTION 05

# Closing the Gap

None of the six problems in this paper are about under-investment. They're six specific, recurring operational breakdowns that show up in nearly every environment, no matter how much budget sits behind it. Tufin Orchestration Suite, Segmentation Intelligence, and Tufin's agentic layer exist to close the loop between defining policy and proving it holds, across every vendor, every environment, and every stage of the network's evolution.

**See how Tufin closes the gap between policy and enforcement**

Visit tufin.com to request a demo.

**Request a Demo**

## Works Cited


1. Cisco, The Segmentation Report: Cisco's 2025 Network Segmentation Survey, conducted by Vanson Bourne, October 2025. cisco.com

2. Verizon, 2026 Data Breach Investigations Report, May 2026. verizon.com/business/resources/reports/dbir

3. New Relic, 2025 Observability Forecast. Median cost of a high-impact outage of $2M per hour. newrelic.com

4. Splunk, "The Hidden Costs of Downtime 2026." Estimated $600B annual cost to the Global 2000; 43% of downtime events are network- or IT-environment-related. splunk.com

5. A-LIGN, 2025 Compliance Benchmark Report. Most organizations now conduct four or more audits annually. a-lign.com

6. Fortinet / Cybersecurity Insiders, 2026 Cloud Security Report: Closing the Cloud Complexity Gap, January 2026. 64% would choose a single-vendor platform if designing their security strategy from scratch. fortinet.com



**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, automate policy changes safely, and maintain continuous security posture 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.**