NETWITNESS

How-to

How to Evaluate Your Organization's Network Visibility Readiness

Table of Contents

Introduction

Most organizations believe they have network visibility. What they usually have is partial coverage and numerous assumptions.

The problem shows up during incidents. Teams can see alerts, but not the full story. They know something happened, but not where it started, how it spread, or what was actually impacted. There's a reason this keeps happening. **67%** of businesses say network blind spots are a top obstacle to their data protection efforts. Those blind spots are not edge cases. They sit inside hybrid networks, cloud workloads, internal traffic flows, and remote user connections that traditional monitoring was never designed to fully cover.

Network visibility readiness is the difference between reacting with confidence and guessing under pressure. It's not about how many tools you own. It's about whether your organization can consistently see, understand, and act on network activity across modern, distributed environments.

This guide explains how to evaluate that readiness without turning the exercise into a tool inventory or a maturity scorecard.

Source: https://www.auvik.com/franklyit/blog/network-visibility-guide/

What Network Visibility Means in Practice

Network visibility means having awareness of:

- Devices and endpoints connected to the network
- Applications and services in use
- Traffic flows between systems
- User behavior and access patterns
- Performance, availability, and anomalies

The term is often blurred with “observability.” As analysts at Gartner have noted, observability is largely an evolution of network visibility, not a fundamentally different capability.

What matters is the outcome. If your team cannot quickly answer who connected, what changed, where data moved, and why something looks abnormal, visibility is incomplete.

Why Network Visibility Readiness Matters Now

Modern networks are no longer bound by data centers or office walls. They span cloud platforms, SaaS applications, third-party services, and employee home networks.

The resulting visibility gap is well documented:

- **86%** of IT teams now support hybrid work across home and office networks, creating blind spots outside IT’s control.
- **67%** of organizations say network blind spots are a top barrier to protecting sensitive data.
- Only **33%** actively monitor internal network activity, leaving lateral movement largely unseen.
- **54%** of organizations lack sufficient visibility into supply chain cyber risk.

Visibility is widely recognized as essential yet rarely achieved end-to-end. Readiness is about closing that gap before an incident forces the issue.

Source: https://www.auvik.com/franklyit/blog/network-visibility-guide/

How to Evaluate Network Visibility Readiness

Evaluating network visibility readiness requires more than checking whether monitoring tools are deployed. The real question is whether your organization can reliably see, interpret, and act on network activity across modern, distributed environments.

The steps that follow are designed to help teams assess visibility in practical terms. Each step focuses on a specific aspect of readiness, from basic coverage to operational usability, and highlights where gaps most often emerge. The goal is not to achieve perfect visibility, but to identify the blind spots that slow investigation, increase risk, and weaken response.

Use these steps to evaluate what your organization can actually see today, where assumptions exist, and which gaps matter most to close.

Step 1: Evaluate Visibility Coverage Across Environments

Start by mapping where visibility exists and where it stops. This is not a tool list.
It's a coverage map.

On-Prem and Data Center

Ask:
- Is internal east-west traffic visible or assumed trusted?
- Are segmentation boundaries observable?
- Do you collect logs, flow data, or packet data consistently?

Cloud and Multi-Cloud

With most enterprises using multiple cloud providers:

- Are cloud flow logs enabled and analyzed?
- Can you see traffic between cloud workloads?
- Can activity be correlated across cloud and on-prem paths?

Remote and Distributed Access

- Do you have insight into last-mile performance issues?
- Can you distinguish user issues from ISP problems?
- Is remote access behavior visible beyond authentication events?

If you cannot clearly describe what traffic you cannot see, readiness is already compromised.

Step 2: Assess Telemetry Depth and Quality

Visibility depends on more than data volume. It depends on whether data explains behavior.

Evaluate:

- Can investigations reconstruct a user or attacker's path?
- Can normal administrative activity be distinguished from abuse?
- Can abnormal protocols or destinations be identified?

Logs without context, flows without correlation, and packets without scale all create false confidence. Readiness comes from the right mix, not more data by default.

Step 3: Examine Internal and East-West Visibility

Most breaches do not stay at the perimeter. They move laterally.
Yet internal traffic is still treated as implicitly trusted in many environments. If internal communication is invisible, attackers blend into normal activity.

Evaluate:

- Is traffic between internal systems monitored?
- Are lateral movement techniques detectable at the network level?
- Are internal flows correlated with identity and endpoint data?

If lateral movement is only detected through endpoints or after impact, visibility readiness is weak.

Step 4: Evaluate Visibility into Encrypted Traffic

Over 96% of network traffic is encrypted, and the majority of modern attacks use encrypted channels.

Readiness does not mean decrypting everything. It means:

- Extracting meaningful metadata from encrypted sessions
- Baselining normal encrypted traffic behavior
- Selectively decrypting high-risk traffic where justified

If encrypted traffic equals blind traffic, attackers already have freedom to move, communicate, and exfiltrate data without detection.

Step 5: Assess Cloud, SaaS, and API Visibility

Cloud and SaaS platforms expose visibility through APIs, not physical taps.

Ask:

- Are cloud-native logs and flow data integrated?
- Is SaaS usage visible beyond login events?
- Can API activity be monitored for misuse or misconfiguration?

Organizations that rely solely on traditional monitoring tools inevitably lose visibility as workloads move off-prem.

Step 6: Measure Operational Usability

The visibility that only a few experts understand is fragile.

Evaluate:

- Can Tier 1 and Tier 2 analysts investigate network issues confidently?
- Are investigation workflows consistent and repeatable?
- Is knowledge embedded in tools or locked in individuals?

If analysts spend more time hunting data than analyzing behavior, readiness is low.

Step 7: Test Visibility Under Real Conditions

Assumed visibility is not visibility.

Run realistic tests:

- Lateral movement simulations
- Credential misuse scenarios
- Partial outages or noisy traffic events

Measure:

- What was detected immediately?
- What is required for manual correlation?
- What went unseen?

These exercises expose gaps faster than audits or dashboards.

How Platforms Support Visibility Readiness

Organizations that improve readiness typically consolidate visibility instead of stacking point tools.

Security-focused platforms such as NetWitness correlate network, log, endpoint, and identity data to support investigation and response, not just alerting.

Tools enable visibility. Readiness depends on how well that visibility is operationalized.

Final Takeaway

Network visibility readiness determines whether an organization can see reality as it unfolds across its network, or only piece it together after the damage is done.

If your organization struggles to explain attack paths, identify internal movement, or understand remote user issues, visibility is likely fragmented.

The goal is not perfect visibility. It's enough clarity to reduce uncertainty quickly.

Evaluate coverage honestly. Test assumptions. Fix gaps deliberately.

Because when an incident hits, visibility is either your advantage or your liability.