IP FABRIC

AT YOUR
BREAKING POINT
WITH

GROWING ATTACK SURFACES?

Maintaining the status quo doesn't cut it anymore. Security tools don't provide sufficient context across the depth and breadth of the network to empower responders or agents to make the right decisions.

THE STATUS QUO

- Physical and virtual infrastructure is frequently deployed and either missing or not registered correctly in asset management or Systems of Record.
- Security, systems, and network teams' communication fail to converge on a shared understanding of risk.
- Blended threats use multiple attack vectors to pivot across networks and assets. The longer the dwell time, the greater the risk of further/deeper exploitation.
- Due to growth, unknown vulnerabilities and technical debt across the network are seen as Business as Usual.

52% of organizations conduct regular network security audits, while 19% confess to never conducting them.

Ponemon Institute via Hamilton Barnes

ACCEPTED BECAUSE

No shared view: Teams suffer from divergent views of the network and related zones or enclaves.

Missing context/gaps: Subject matter experts can't analyze the true picture end-to-end.

Lack of focus: Teams are busy firefighting issues and incidents, with no time to be strategic.

THE BREAKING POINT

VISIBILITY GAPS BECOME CRITICAL

IT leaders accept a level of obscurity in the network that would be unacceptable in other critical parts of the business.

The network is crucial for productivity and revenue in digitally-driven enterprises. When business continuity relies on the security and stability of the network, visibility gaps are not just less acceptable but constitute major risks with unquantifiable impact.

ONE TOO MANY BREACH CLOSE CALLS

A dynamic network is no excuse for gaps in redundancy or security. More than a stressful weekend of P1 calls, the long-lasting reputational damage of a security breach can destroy the trust in a business for years to come. Mandatory disclosure, increased fines, and increasing management-level legal accountability leave no more wiggle room.

ALERT FATIGUE BECOMES ALERT BURNOUT

Continuous alerts without context or any "why" provided, and insufficient calibration for severity or priority, waste your team's time and effort. As fatigue turns to burnout, expect slower times to resolution, interruptions to business continuity, and a talent exodus.

SECURE YOUR GROWING ATTACK SURFACE WITH AUTOMATED NETWORK ASSURANCE

Identify Rogue Devices / Configurations
IP Fabric finds hidden vulnerabilities, including surfacing rogue devices and undocumented firewall changes. Integrating network data into security operations is easy: use API requests to compare IP Fabric's insights with the CVE program to assess risks from discovered entities and their operating systems.

Perform Daily Security Audits
IP Fabric's 150+ customizable network intent checks allow you to set rules for your network that get validated with every discovery. Ensure that configuration and security policies are being applied, segmentation is operating as expected, and that the network as a whole is passing traffic as expected. Regain peace of mind + confidence.

Self-Serve Network Intelligence
Via API or pre-built integration, you can share key network intelligence with security teams or business leadership. Enrich ITSM tickets with end-to-end network paths or add critical context to alerts for rapid and targeted troubleshooting.

$4.88M
2024 global average cost of a data breach. +10% over last year. Highest total ever

IBM Cost of a Data Breach Report 2024

THE BENEFITS

- **REVEAL THE TRUTHS & VULNERABILITIES OF YOUR NETWORK.**
- **FOSTER TRUST & UNDERSTANDING BETWEEN TEAMS.**
- **PROTECT AND SECURE CRITICAL INFRASTRUCTURE PROACTIVELY.**

> *Red Hat's policy validation tool only displayed firewall rules, lacking the context needed for troubleshooting and contextualizing security issues. Their previous approach required manual processes, causing inefficiencies and team bottlenecks. By integrating IP Fabric's end-to-end path lookup, Red Hat added a self-service element, allowing teams to troubleshoot without relying on specific engineers or facing delays from missing information.*