VIAVI

16TH ANNUAL 2024/25

State of the Network

Enterprise networks are evolving, shifting from traditional network monitoring to observability

To Monitor Is Good; To Observe, Divine

Network Monitoring is vital, but rapidly evolving hybrid environments require more. Network Observability goes deeper, integrating and correlating data from multiple sources for efficient root cause analysis.

Top Drivers to Make the Observability Transition

Many respondents say observability is delivering benefits beyond their expectations:

- **83%** have seen unexpected security benefits enabled by better visibility
- **82%** have seen product teams' ability to innovate, improved by increased efficiency
- **78%** have said their ability to maintain compliance has been enhanced

Those with an observability strategy were 3.5x more likely to see a significant reduction in MTTD

Trimming the Monitoring Toolchest

Despite the necessity of diverse monitoring and management tools for complex IT setups, overloading can hinder efficiency. Streamlining tools boosts productivity and cuts costs.

Small enterprises use an average of **4-6 TOOLS**

Medium enterprises use an average of **7-10 TOOLS**

Large enterprises use an average of **11-15 TOOLS**

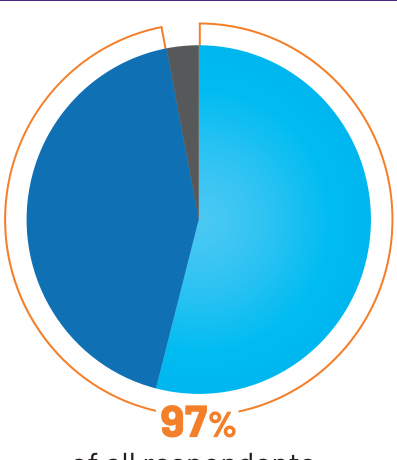
13.7 HOURS average for 11 or more solutions

FEWER TOOLS CLEARLY TRANSLATES TO LOWER MTTR

5.7 HOURS average for 10 or fewer solutions

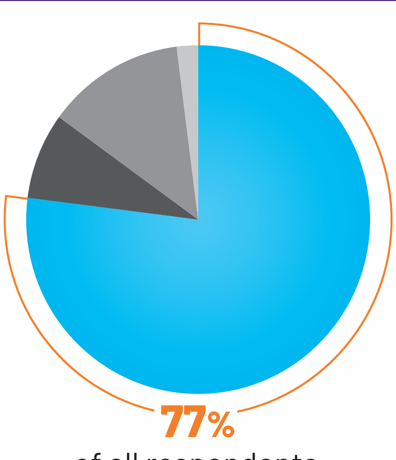
Vaulting the Hybrid Hurdles

80% of respondents face substantial visibility challenges within their cloud and hybrid environments



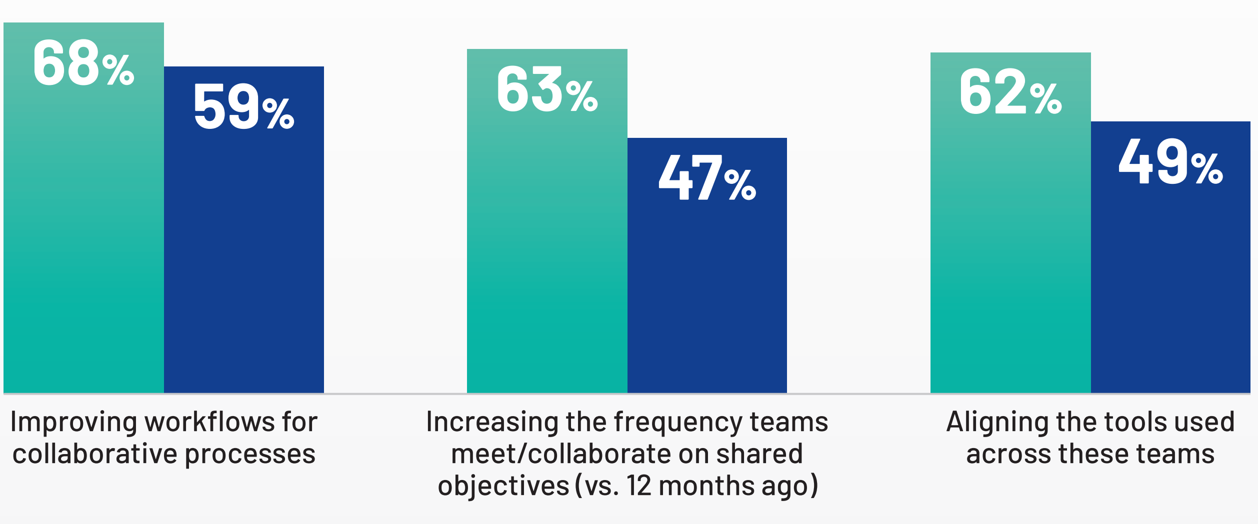
97% of all respondents view packet capture in the cloud as either **somewhat** or **extremely important**

Packet and flow data are still vital to achieving **complete network visibility**



77% of all respondents have an identified **need for technologies that capture flow data**

Observability enhances NetOps/SecOps Collaboration in Hybrid Environments



Integrating Threat Exposure and Attack Surface Management Across Hybrid Environments

Observability and Continuous Threat Exposure Management (CTEM), both enhance security by integrating and contextualizing data, providing the visibility needed to reduce the attack surface and respond to evolving threats.

TOP FIVE CHALLENGES IN CYBERSECURITY TODAY

- Increased attack surface due to the rising use of multi-cloud services and remote workers
- Regulatory compliance taking precedence over best practice implementation
- Cybersecurity teams that are too focused on incidents, impeding overall posture improvements
- Managing the volume of security alerts
- Insufficient vulnerability assessment capabilities

Concerns with threat exposure management show a direct correlation to planned investments

88% of organizations see threat exposure management as important or critical

87% are planning increased investments in exposure management

Organizations consistently recognize the value of CTEM, ranking it **third** among cybersecurity strategies. Investments in vulnerability assessment and CTEM are prioritized by organizations of all sizes.

Implementing network observability, tools consolidation, and CTEM strategies boosts collaboration, operational efficiency, and user experience while reducing costs and the attack surface.

READ THE FULL REPORT AT
stateofthenetwork.com

Enterprise Strategy Group™ by TechTarget

VIAVI

sotn2425-ig-ec-nse-ae | 30194163 900 0624