

2027

State of the Network Study

Strategic Initiatives to Drive Security and Resilience Across the Modern Network

Complex environments create a range of difficulties for network and security operations (NetSecOps). Despite ongoing challenges in balancing security and performance, most organizations continue working toward achieving both goals. Tooling, testing, and organizational approaches such as NetSecOps are important dimensions for achieving the best results.

Complexity raises the stakes for balancing network performance and security

Network and security teams face an ongoing and ever-changing set of operational challenges.



What Are the Top Cybersecurity Challenges?

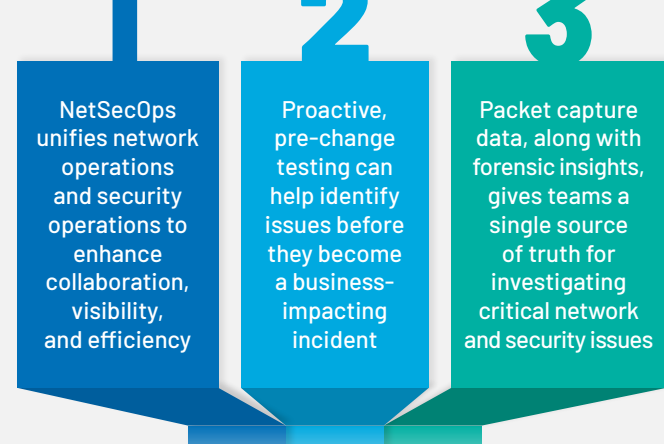


How does the challenge of balancing network performance with security requirements rank?

65% FIND BALANCING NETWORK PERFORMANCE WITH SECURITY REQUIREMENTS TO BE A SIGNIFICANT CHALLENGE

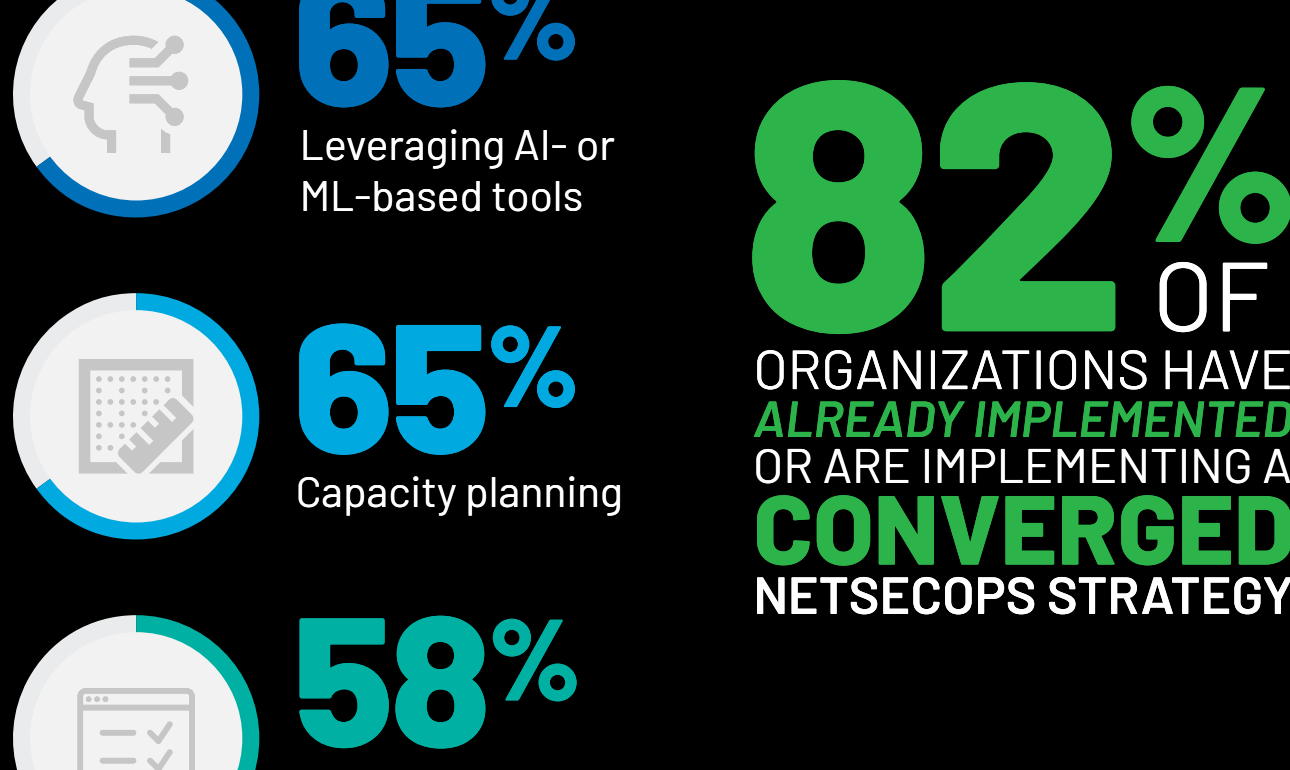
Convergence via NetSecOps and proactive resiliency testing can help alleviate these issues

There are a variety of avenues to alleviate these issues...



but 3 stand out.

To mitigate the impact of security measures on network performance, organizations reported:



Benefits from these practices include fewer issues, faster detections, and stronger security

The convergence of network operations and security operations into **NetSecOps** helps:

- Rationalize Tools
- Streamline Processes
- Faster Detection
- Better Security Outcomes

Proactive testing of new technologies, such as **PQC**, **AI security**, **SASE**, and **cloud networking**, can help avoid issues, leading to:

- Fewer Outages
- Improved Performance

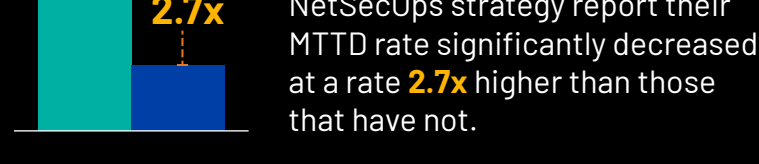
Correlating **PACKET-BASED ANALYTICS** with **FORENSIC INSIGHTS** helps:

- Streamline Investigations
- Improve Threat Hunting
- Reduce Mean Time to Restore

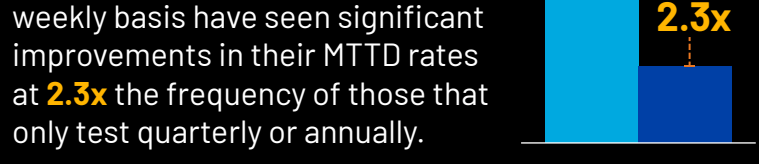
Impact on MTTD

Another key success story regarding reducing Mean Time to Detect (MTTD) is related to NetSecOps team convergence and proactive testing...

NetSecOps Impact:



Proactive Testing Impact:



Benefits from correlating packet analytics with forensic insights

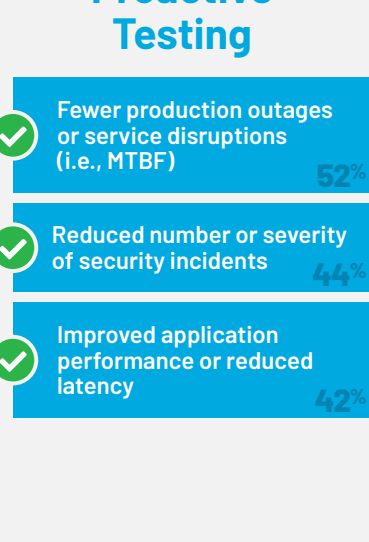
Of the many options that network and security teams have in terms of telemetry, one that is particularly useful is packet-level capture and analysis. Those with a NetSecOps framework, in particular, are choosing packet-level data for incident investigation and forensic analysis at rates **2.1x** higher than those without, indicating exceptional value for identifying and investigating critical network and security issues and incidents.

Top benefits of...

NetSecOps Convergence



Proactive Testing



Correlating Packet Analytics with Forensic Insights



Network and security teams are under pressure to act faster, collaborate more effectively, and improve outcomes across increasingly complex environments. This study reinforces the value of NetSecOps adoption, proactive resiliency testing, and broader use of packet data across multiple use cases. Together, these strategic initiatives help organizations enhance security, have fewer production outages or service disruptions, reduce the severity of security incidents, and shorten MTTD rates.

READ THE FULL REPORT AT stateofthenetwork.com



Research and analysis conducted in conjunction with:



sofn27-ig-ec-nse-se • 30195228 900 1026