

Network Security Monitoring:

Practices, Challenges, and Plans

Network security monitoring (NSM) is now an integral part of threat defense. Cisco recently commissioned the Enterprise Strategy Group (ESG) to evaluate the current state of NSM to uncover key statistics on today's most prominent cybersecurity practices, challenges, and plans.

Here's how IT and Security professionals view today's state of network security.

NETWORK SECURITY MONITORING

Current State

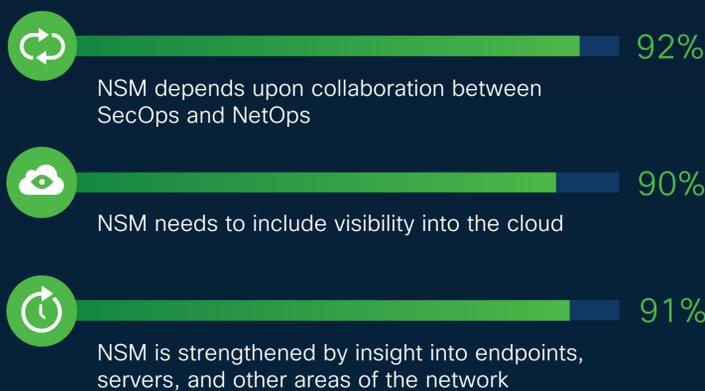
97%

of respondents say network security monitoring is an important or critical function. Why? Because of the many important use cases and goals it supports:



What NSM needs to be effective

At least 90% of cybersecurity professionals believe that:



NETWORK SECURITY MONITORING

Challenges

73%

of respondents say NSM is more difficult than it was two years ago.

Biggest external challenges:

an increase in malware volume and sophistication



more network traffic

Biggest internal challenge:

network blind spots

Visibility is lacking in:

- User behavior
- Traffic from non-corporate devices
- Traffic between the organization and its business partners

- Public cloud traffic
- Networks residing in remote locations
- Traffic on the internal wireless network

NETWORK SECURITY MONITORING

Future Strategies

90%

of respondents say investments in NSM will increase over the next two years. Companies will likely:



Despite their efforts with NSM,

1 in 4 survey respondents



say they have difficulty detecting suspicious network behavior and identifying cyberattacks in progress.



These capabilities are critical for preventing destructive data breaches.

How we can help

Whether you are just getting started, or already have NSM technologies in place, Cisco can help you extract maximum value from your infrastructure. With Cisco Stealthwatch, you can obtain the end-to-end network visibility you need to effectively monitor and remediate security issues around the clock.

Find out more at cisco.com/go/stealthwatch, or contact stealthwatch@cisco.com.

Read the [full ESG report](#).

