
Network security monitoring (NSM) is now an integral part of threat defense. Cisco recently commissioned the Enterprise Strategy Group (ESG) to evaluate the 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.

**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:
  - Detecting network traffic that indicates a security breach
  - Querying or hunting for suspicious behavior
  - Enabling continuous monitoring for risk management
  - Generating security alerts
  - Automating remediation tasks

At least 90% of cybersecurity professionals believe that:

- NSM depends upon collaboration between SecOps and NetOps
- NSM needs to include visibility into the cloud
- NSM is strengthened by insight into endpoints, servers, and other areas of the network

97% of respondents say investments in NSM will increase over the next two years.

- Companies will likely:
  - Increase use of data center automation and virtualization
  - Increase use of serverless infrastructure
  - Automate incident response
  - Integrate more tools to automate incident response

**Challenges**

- 73% of respondents say NSM is more difficult than it was two years ago.

Visibility is lacking in:

- The cloud
- Traffic from non-corporate devices
- Traffic between the organization and its business partners
- Traffic on the internal wireless network
- Networks residing in remote locations
- Public cloud traffic

- 1 in 4 respondents say they have difficulty detecting suspicious network behavior and identifying cyberattacks in progress.

- These capabilities are critical for preventing destructive data breaches.

**Future Strategies**

- 90% of respondents say investments in NSM will increase over the next two years. Companies will likely:
  - Incorporate new types of cloud infrastructure into NSM
  - Enable more collaboration between security and operations groups
  - Integrate more tools to automate incident response
  - Enable remote monitoring

Despite their efforts with NSM, 1 in 4 respondents say they have difficulty detecting suspicious network behavior and identifying cyberattacks in progress.

**How we can help**

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

To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. (1110R) 06/17