Analyst Program

Network Visibility: Detecting the Threat from Within

Sponsored by: ExtraHop

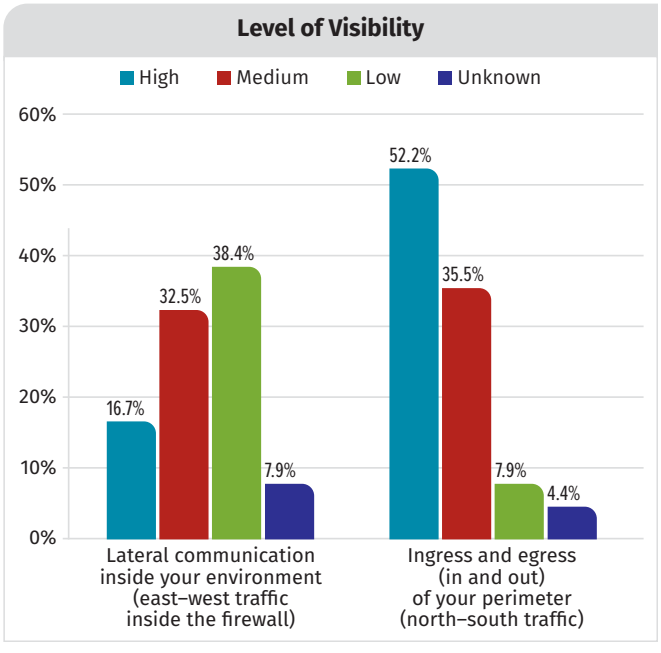
Traditionally, perimeters were well established and backed by security models that placed great value on boundary visibility—data flowing both in and out of organization (north–south traffic) as well as well-defined internal boundaries, such as the DMZ. Today, that model is challenged by the move from physical network architectures to logical ones, including VPN and SD-WAN.

Knowing your internal assets is fundamental to security hygiene. Data from the 2020 SANS Network Visibility and Threat Detection Survey indicate that for those organizations that suffered at least one cyberattack in the past 12 months, analyst intervention using SIEM or other tools is the leading method to detect and/or investigate the compromise for the majority of respondents (73%). Endpoint involvement figured high in the tools used as well, with 64% relying on anti-malware/antivirus and 43% using endpoint detection/EDR.

Replacing a physical, perimeter-based network architecture with a logical one (VPN, SD-WAN) requires that security teams account for connecting a wider variety of endpoints, not all of which are standardized in their approach to connectivity. The network remains the common denominator to achieving visibility across multiple endpoints. This is where the 2020 SANS Network Visibility and Threat Detection Survey indicates that network visibility may be lagging.

Visibility Levels Differ

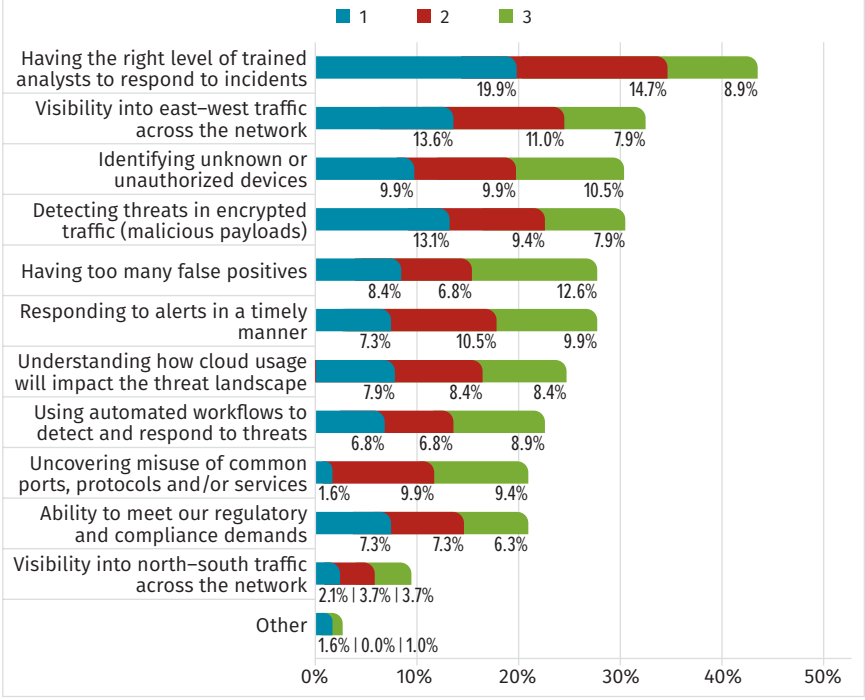
A little more than half of respondents (52%) indicated a high degree of north–south visibility, which they achieve mainly through next-generation firewalls (NGFWs) with proxy solutions to control the flow. Contrast this with the fact that only 17% of respondents reported high visibility into traffic within their networks (east–west traffic), while 46% reported low to no visibility.



The ranking of the greatest challenges that respondents face, given their current network infrastructure, indirectly supports the following courses of action:

- Provide better visibility into east–west traffic to identify those devices that could pose potential threats.
- Look for solutions that enable visibility into protected/encrypted traffic to see whether a threat has been realized.
- Make sure the right level of trained analysts is available to respond to incidents.

Which of the following reflects the greatest challenges you face, given the capabilities of your current network infrastructure?
Rank your top three challenges, with 1 being the most challenging.



Enhancing East–West Visibility

Building an equivalent capability to monitor and visualize east–west traffic, whether inside the perimeter or in the cloud, can be a challenge. Survey results suggest areas where organizations might target their efforts:

- **Improve discovery of devices connected to your network.** Only 38% are highly confident that they can discover all devices connected to their network. And even then, this may be optimistic, given that 37% reported that encryption obscures valuable data points in network data.
- **Understand normal behavior for new types of devices. Information can be readily extracted from network data, based on internet protocols.** Analysts, however, need to know what the extracted information means. The collection of additional data elements, such as database and certificate metadata, may require additional training for analysts.
- **Identify approaches to mitigate the complications afforded by the use of data encryption.** Improvements in encryption security, such as the perfect forward secrecy (PFS) requirements within Transport Layer Security (TLS) v1.3, add another layer of complication. A full 82% of respondents reported encrypting 25% or more of the traffic in their network, with at least 38% using PFS to encrypt 25% or more of their traffic. As the use of PFS increases, organizations will need to have systems in place to examine such messages to ensure north–south security.
- **Extend the use of automation for all aspects of visibility, detection, response or investigation within your network.** Most respondents (71%) use automation for detection, with more than 50% planning an increase in automation for response and investigation. With regard to visibility, 68% currently rely on automation for visibility, and another 28% plan to adopt its use in the next 12 months.

In closing, network data remains a major source to achieve visibility and insight into the internal functioning of your network, bringing improved situational awareness that allows rapid identification and investigation of threats. Monitoring and analyzing east–west network data, as well as north–south traffic, should be considered an essential first step in closing the visibility gap and improving overall threat detection.

2020 Network Visibility Survey

Webcast

Listen to the survey results webcast at
www.sans.org/webcasts/113445

Read the related whitepaper at
www.sans.org/reading-room/whitepapers/analyst/2020-network-visibility-threat-detection-survey-39490

Sponsored by:
ExtraHop