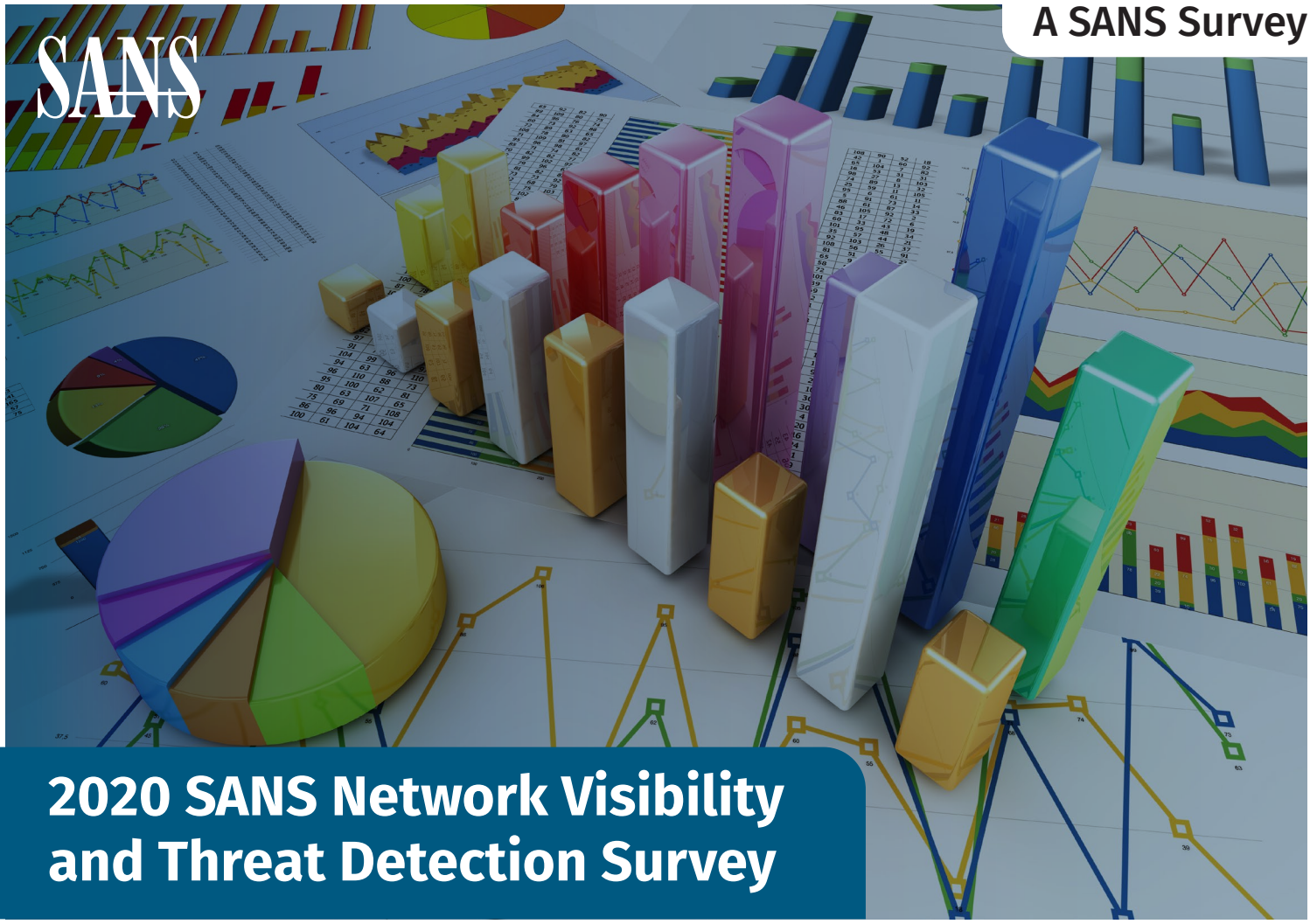
A SANS Survey



2020 SANS Network Visibility and Threat Detection Survey

Written by **Ian Reynolds**

April 2020

Sponsored by:

ExtraHop Networks

Analyst Program

Executive Summary

As organizations continue to move to the cloud, encrypt communications, adopt IoT and manage third-party vendors, the complexity of the network increases—impeding visibility, slowing operations and impacting security. This statement is reinforced by the data we collected in this SANS survey on network visibility. For example, of the participating organizations, 59% believe that lack of network visibility poses a high or very high risk to their operations, and 64% of respondents experienced at least one compromise over the past 12 months.

Historically, the perimeter security model put great value in understanding the data flowing into and out of the network (north–south traffic). In fact, a little more than half of respondents (52%) indicated a high degree of north–south visibility, achieved mainly through next-generation firewalls (NGFWs) with proxy solutions to control the flow.

With the shift to software-as-a-service (SaaS) and infrastructure-as-a-service (IaaS) comes a new challenge: how to monitor application and user activity across hybrid and multicloud environments, as evidenced by the fact that only 17% of respondents reported high visibility into traffic within their networks (east–west traffic).

As a solution, most organizations have adopted EDR and SIEM solutions. But those solutions have some weaknesses: Endpoints can be tampered with, log data can be too noisy and turned off, and as a result, organizations are missing critical data to find threats within the east–west corridor.

Building an equivalent capability to monitor and visualize east–west traffic, whether inside the perimeter or in the cloud, has been a challenge for most organizations. The use of data encryption and improvements in encryption security, such as the perfect forward secrecy (PFS) requirements within Transport Layer Security (TLS) v1.3, adds a further layer of complication. A full 82% of respondents reported encrypting 25% or more of the traffic in their network, with 79% using PFS.

As the data will show, lack of visibility creates blind spots for many organizations. Good visibility brings an improved situational awareness allowing for rapid identification and investigation of threats for faster resolution of internal performance issues and security breaches. Monitoring and analyzing network data assists as part of those crucial first steps in closing any visibility gap.

Key Findings

- **64%** suffered one or more compromises over the last 12 months.
- **59%** believed that a lack of network visibility poses a high or very high risk to the organization.
- **52%** had high visibility into traffic into and out of their network (north–south traffic).
- **17%** reported high visibility into their lateral communication inside their network (east–west traffic).

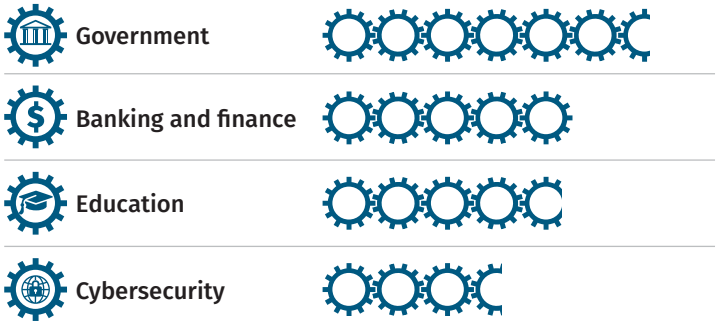
Respondents and Their Environments

The SANS Network Visibility and Threat Detection Survey gathered responses from 213 respondents representing a broad cross-section of organizations with at least 1,000 employees. This group provides a global sample of security professionals from organizations of differing sizes.

Demographics

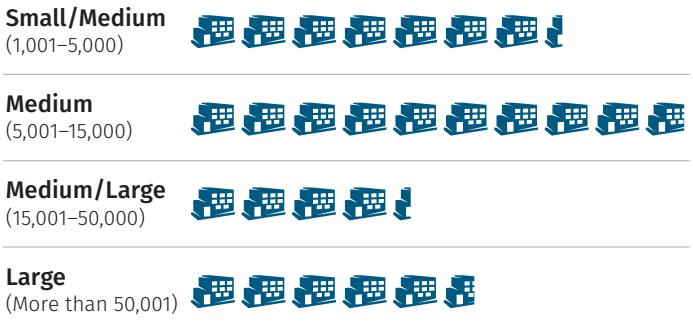
Figure 1 provides a snapshot of the survey respondents.

Top 4 Industries Represented



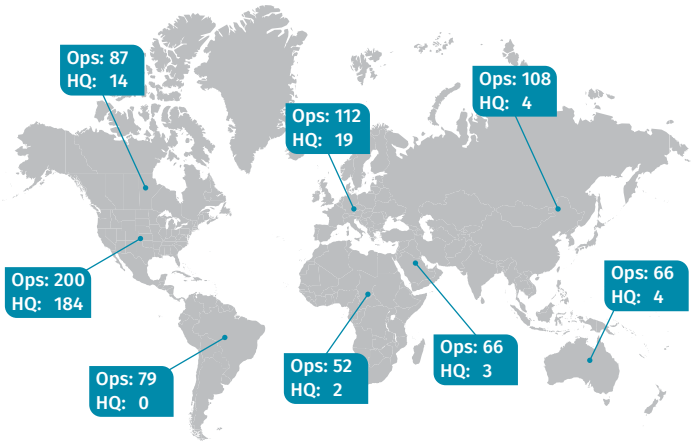
Each gear represents 5 respondents.

Organizational Size

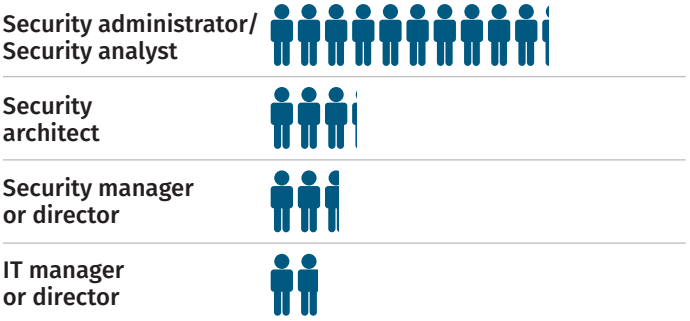


Each building represents 10 respondents.

Operations and Headquarters



Top 4 Roles Represented



Each person represents 10 respondents.

Figure 1. Key Demographic Information

Infrastructure

The infrastructure results, detailed in Table 1, show the majority of respondents have a typical mix of on-premises systems, both physical and virtual, alongside a strong representation of cloud-based systems. It is reassuring to see almost half of respondents (49%) consider IoT controls and sensors to be part of their infrastructure. Unfortunately, only 20% view them as a risk and security concern. As more organizations become aware of these often-overlooked devices, we expect that number to rise because such devices are often outside the standard management channels.

Table 1. Devices and Risk/Security Concerns

	Part of Infrastructure	Risk and Security Concern
On-premises—physical servers	93.4%	34.8%
On-premises—virtualized servers	92.5%	35.2%
Routers/Firewalls/Switches/Other network devices	92.5%	20.0%
Networked printers/Multifunction devices	91.7%	6.1%
Desktops (employer-owned)	90.8%	44.4%
Physical security systems (electronic access controls, surveillance systems)	85.5%	8.3%
Cloud-based servers or systems	82.0%	40.0%
Employer-owned mobile devices (tablets, laptops, notebooks/iPads, smartphones)	80.3%	25.7%
Employee-owned mobile devices (tablets, laptops, notebooks/iPads, smartphones)	64.5%	26.5%
IoT controls and sensors	49.1%	19.6%
On-premises—containers	46.9%	3.0%
Cloud-based containers	39.0%	9.6%
Point of sale (POS) devices	38.6%	7.4%
ICS and SCADA	35.1%	16.1%
Other	4.8%	3.5%

The data also highlights that respondents believed employee desktops (44%) pose the most significant cause for concern. Traditionally this judgment is a smart choice—humans are fallible—and we know attackers frequently target employee workstations as the initial point of entry. Cloud-based systems (40%), on-premises physical servers (35%) and virtual servers (35%) are perceived as the next riskiest groups.

Tools

The survey results also detailed which tools organizations currently use to measure and monitor network traffic. The reliance on commercial tooling was evident and was bolstered by open source tools and tools developed in-house. A substantial weighting toward IDS/IPS was apparent, with both network (92%) and host (70%) variants represented in first and fourth place, respectively. Next-generation firewalls (NGFWs), selected by 84%, secured second place. See Figure 2.

What tools or technologies do you currently utilize for network visibility?
Indicate only those that apply.

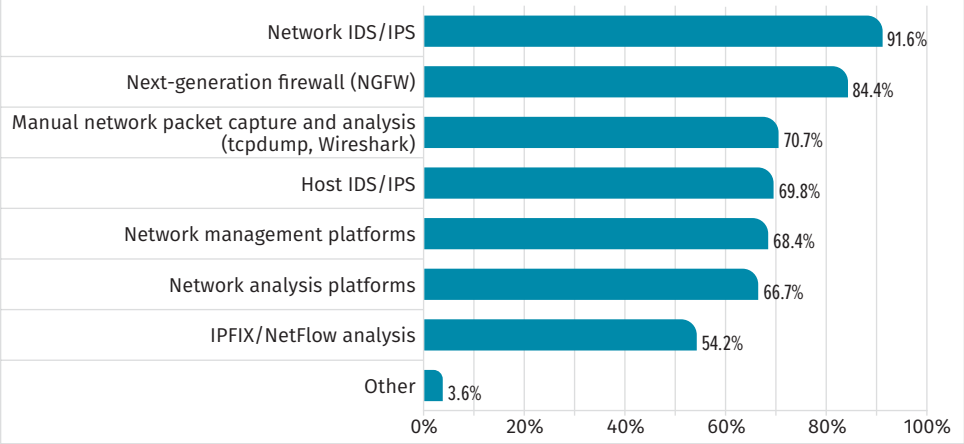


Figure 2. Tools in Use

Defining the Issues

With a better view of the infrastructure in use and the tool sets available, we can shift our focus to understanding the issues facing organizations today: complexity, visibility and threats.

Complexity

More than 93% of respondents indicated that they manage more than a thousand endpoints, and almost 90% manage between hundreds to thousands of servers. The complexity of the overall challenge is broad as well as deep. Bringing the correct solutions and tools to meet this challenge is a vital part of security operations. The majority of companies (51%) use tooling from more than 10 vendors, with 18% utilizing more than 20.

The majority (68%) expressed a desire to reduce the complexity of their systems by reducing the overall number of tools involved in their operations, as illustrated in Figure 3.

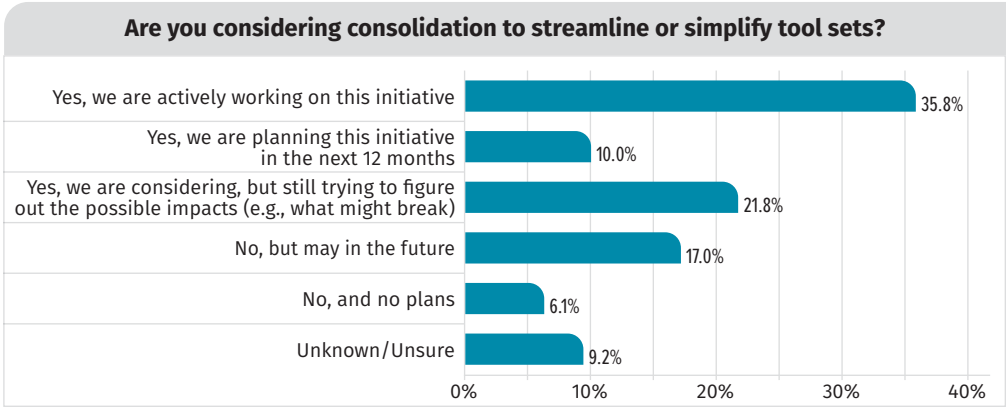


Figure 3. Tool Consolidation Plans

Visibility

As operations continue to evolve beyond traditional borders, utilizing IaaS, PaaS and SaaS in public or private cloud environments, solutions need to evolve as well to ensure we maintain visibility and control of organizational data. Only 38% of respondents had high or very high levels of confidence in their ability to discover all of the devices connecting to their networks, with just 6% expressing a very high level of confidence. That lack of confidence is tied to a perception of higher risk for most organizations (see Figure 4).

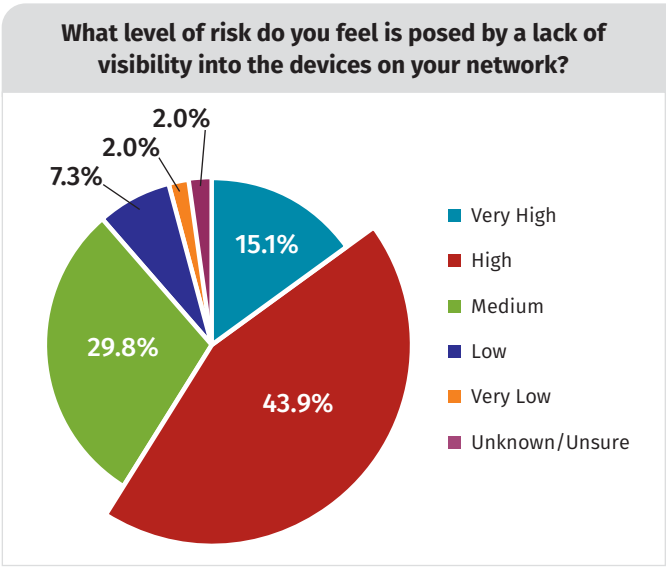


Figure 4. Visibility and Risk

While the majority of respondents (52%) claim high visibility into traffic entering and leaving their network (north–south traffic), only 17% claim the same level of visibility into traffic moving within their networks (east–west traffic). Improving the east–west visibility and keeping track of applications as they are deployed can play an important role in enhancing threat detection capabilities and making organizations feel more confident about their security posture. See the "Visibility and Threat Detection Challenges" section for more detail.

Threats

More than 64% of respondents reported suffering at least one successful attack within the last year (see Figure 5), with only 11% reporting a single attack and 6% reporting more than 100. While 36% reported no successful attack within the past year, that could be a sign of a high-performing security program, or unfortunately, it could be a sign of missed opportunity or lack of resources to detect a skilled attacker.

In the coming sections, we expand upon the importance network visibility plays in gaining a better understanding of the threat landscape and the signs of unwanted adversaries moving within the network. Without visibility, it is impossible to detect threats or secure networks effectively.

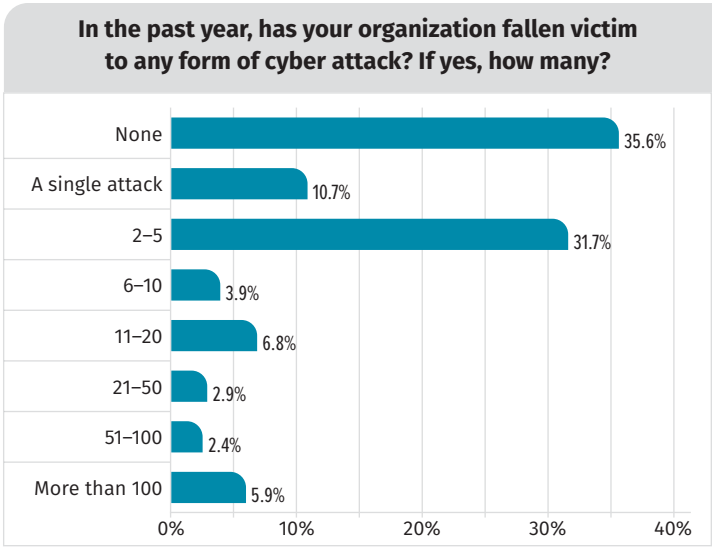


Figure 5. Cyber Attack History

Visibility and Threat Detection Challenges

Complexity definitely affects security by making it more difficult to streamline security practices. It is a daunting task to ensure that solutions from multiple vendors will communicate seamlessly. Where those solutions don't quite mesh, blind spots are introduced into the security landscape, making visibility, data collection and by extension threat detection, more difficult. In this section, we explore how the challenges to achieving visibility affect threat detection capabilities and network security.

Only 17% of respondents believed that they have high visibility into their east–west traffic, with 46% admitting they have low to no visibility. With a historical focus on perimeter, it is no surprise that more than 52% claim high visibility into north–south traffic. See Figure 6.

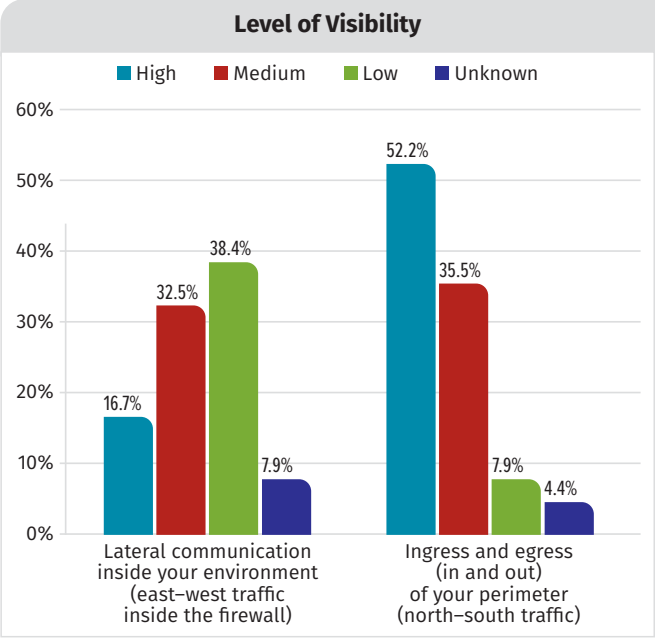


Figure 6. Organizational Traffic Visibility

A perimeter focus of their data leaves organizations with only a partial view of the network operations. This becomes an issue when investigating potential and actual intrusions using only the data captured within the SIEM. Across the enterprise, network data flowing between clients and applications can provide a far richer stream of transactional data. The behavior seen in network data can be looked at as the ground source of truth. And, while visibility into that traffic is lacking for most organizations, organizations that monitor their network data can gain much needed context from their east–west traffic and develop a more in-depth insight into their networks to detect and respond to threats on the network.

Takeaway

Having visibility of every device and how they are meant to behave on your network is crucial to understanding what constitutes normal traffic and what could be considered a deviation. Network data provides a rich source of information about the traffic moving across your network to find threats in the east-west corridor and troubleshoot application performance problems. Once you have an intelligent view of how the network should behave and what the user behaviors within it look like, you can monitor activities not fitting those patterns to detect and respond to threats.

Inhibitors to Network Visibility

As migration projects continue to move traditional workloads into the cloud, corporate environments shift outside of corporate data centers, requiring security teams to pivot appropriately to maintain control and visibility of the network.

Cloud adoption, coupled with an increasingly mobile workforce and modern working patterns, means the perimeter is dissolving and applications are moving to the edge. As remote access has evolved over the years, the requirements and options for flexible access to corporate data have increased. With the shift to cloud-based SaaS options, the challenge continues to evolve.

Takeaway

The move to the cloud is a top priority for most organizations. This explosion in cloud adoption creates new challenges for an organization's infrastructure and security teams. Visibility into workloads and behaviors in the cloud is critical to address the new challenges the cloud imposes. Network and security analysts must make a concerted effort to develop the current capabilities of their internal teams or partner with external vendors that can bring a more specific domain knowledge to bear on the problem.

Encryption

Organizations use encryption to enhance the security of their internal communications in transit or at rest (see Figure 7). Encryption guarantees the integrity and confidentiality of the data in transit and at rest. Encryption's purpose is to mitigate some of the problems arising from malicious or unauthorized data interception.

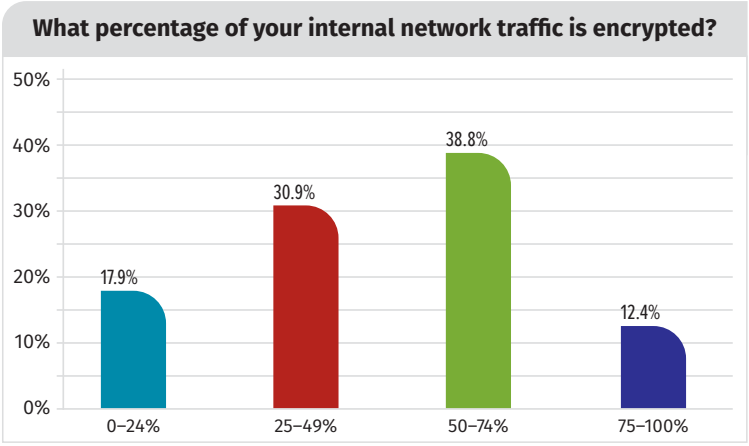


Figure 7. Use of Encryption

Encryption comes with a price, however, and that price is visibility. As shown in Figure 8, organizations are worried about how their encrypted traffic obscures visibility. Only 2% of respondents are not at all worried about encrypted traffic; most highlighted significant levels of concern over encryption making visibility more difficult.

With the use of enhanced encryption and perfect forward secrecy (PFS), visibility may be even more difficult to achieve. The largest percentage (41%) of respondents didn't know whether their organization has adopted PFS, while just 22% use PFS to encrypt 50% or more of their traffic. For these organizations, the challenge is being able to see inside traffic to know whether there is a malicious payload in that encrypted data.

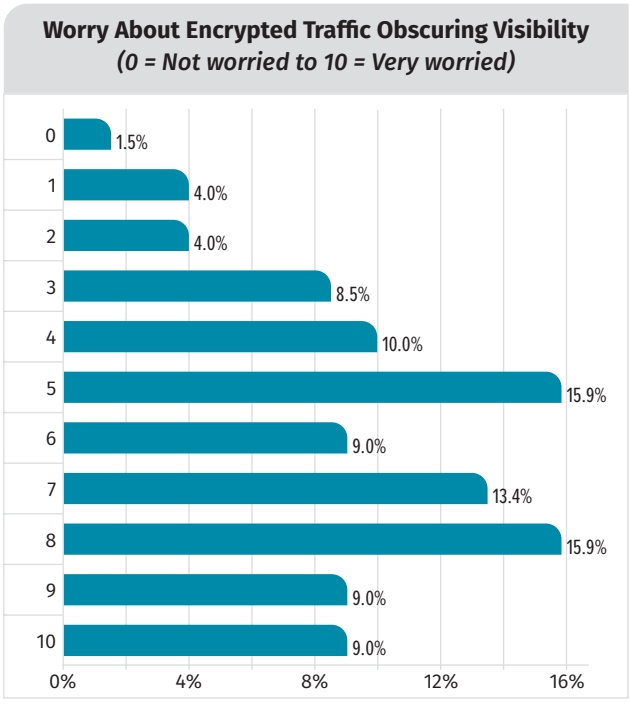


Figure 8. Concern About Encrypted Traffic

Decryption

It is still possible to understand the flow of data when that data remains encrypted. Tools will record which hosts are communicating and provide insight into the ports, protocols and traffic volume. Knowing which parties are communicating gives a valuable set of data points, even if the encryption raises further challenges in understanding the content.

With proper planning and architecture, an organization can maintain visibility where required and decrypt traffic as it enters the network, but the organization will need to take steps to ensure that encryption keys are actively secured for cases where the traffic needs to be inspected in detail or choose other methods. One method would be to use a corporate interception proxy. This approach enables security teams to record an unencrypted copy of the network transaction. Where interception is not an option, the application will need to be configured or adjusted to log the keys used for encryption and provide a way to match unique keys to traffic for later analysis.

Visibility of IoT and Unknown Devices

With 20% of organizations considering IoT devices to be a risk (see Table 1 on page 4), there needs to be a more potent network overview to enable better visibility of these devices. This problem lends itself to network observation. Using network data, organizations can identify IoT devices active on the network, classify their purpose and then monitor the IoT device activity for malicious activity. If this data is properly parsed, security teams could receive notifications in a network detection and response (NDR) tool or from the SIEM based on observed traffic patterns and behaviors. The same goes for rogue or unknown devices on the network. In either instance security teams are enabled to identify what the devices are and how and where they are in use.

Digging into the Network Data

Let's take a look at what types of network data the respondents considered important. We also explore some of the challenges raised by the collection and processing of the network data available within the organization.

Network Data Collection

In analyzing the survey responses about the collection of data, we see common sources usually directed to the SIEM for ingestion and processing. The less popular items such as certificate metadata, SMB/CIFS and database methods are underused in our opinion. Those data types uncover more detail about how organizations are using the applications and their data. See Table 2.

Table 2. Network Data Collected

Data Type	% Who Collect
Active Directory/LDAP login attempts	89.2%
DNS transactions	71.4%
DHCP transactions	64.0%
HTTP payloads	62.1%
IPFIX/NetFlow/Host-to-host connection data	60.1%
Certificate metadata	43.8%
SMB/CIFS methods	41.9%
Database methods	40.4%
Other	2.0%

Network teams often use network flow data, collected by 60% of respondents, to understand the top talkers across the network. This information helps teams understand the usage patterns and identify the heaviest users across the enterprise. Analysis of the flows brings a deeper understanding of how the systems and individuals interact. Network operations teams have the option to choose between taking samples of the data flows or collecting full flow data.

Takeaway

For an analyst sitting within a SOC, the ability to dig into this network data is a potential gold mine. The information drawn from this data allows analysts to build a clearer picture of which systems are communicating and can rapidly support or refute an investigation hypothesis. As organizations develop better methods to interrogate the data within the greater context of the network, the value of the network data increases.

When teams such as network or infrastructure operations collect and manage network data, it's not often shared with security teams, and vice versa, leading to friction when a problem arises. The teams need to ensure they nurture the relationships between their respective operations and security groups to allow for a more efficient information exchange. There are many areas where tools developed and supported within one silo can be of great use to others and ultimately reduce the time required to remediate. For example, network teams can often provide data reflecting the network design, firewall configurations and often have basic network flow visibility. This flow data may only be driven by sampling technology and may lack the fidelity required for in-depth investigation, but it still provides a reference point for what types of traffic are in use. Ultimately, if both network and security teams are using the same set of network data, they can quickly identify root cause and troubleshoot Layer 2 to Layer 7 problems with greater accuracy. If this data is also integrated with endpoints data, the teams can more efficiently utilize their SIEM.

Restrictions on analyzing the content of data, legal concerns about the potential liability of collection and the storage requirements also require consideration, especially in environments demanding protection of personally identifiable information (PII), such as healthcare. The network teams may already be collecting some of this data, and security teams can gain extra visibility by also using this data.

Inhibitors to Greater Use of Network Data

Visibility depends on the right teams in organizations having appropriate access to network data. Unfortunately, the same concerns raised in other recent SANS surveys[1] came to the forefront in terms of impediments to greater use of network data in security efforts. Figure 9 shows commonly voiced concerns that organizations need to address. Lack of staff (62%), lack of time—including having other issues with greater importance—(51%) and lack of appropriate skills in the existing staff (46%) were the leading concerns.

To combat these concerns, organizations can develop more efficient processes and drive automation efforts to remove repetitive work and rework from the analyst's daily task list. Organizations can select tools to close the gaps and integrate with existing workflows to ensure those tools do not become an additional burden to already stretched teams.

What, if any, impediments do you encounter that prevent you from making greater use of network data for security detection and investigation? ***Select all that apply.***

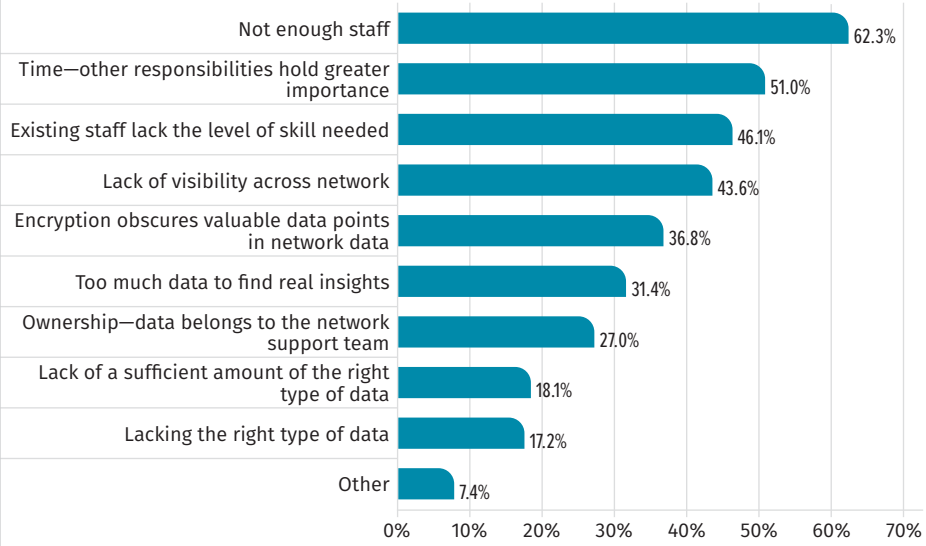


Figure 9. Impediments to Using Network Data

Takeaway

Organizations commonly express a desire for more staff to tackle daily challenges. To attain success, work on optimizing processes and incorporating automation to handle low level and repetitive tasks to make the best use of available staff. Choose tools that use machine learning to provide improved analytics for access to the right data in less time. This might assist in meeting staffing concerns and provide faster resolution of unexpected behaviors, threats and incidents.

[1] "SANS 2019 Incident Response (IR) Survey: It's Time for a Change," August 2019, www.sans.org/webcasts/integrated-incident-response-survey-110110, p. 10, Figure 9.

"Workforce Transformation: Challenges, Risks and Opportunities," December 2019, www.sans.org/reading-room/whitepapers/analyst/workforce-transformation-challenges-risks-opportunities-39340, p. 14, Figure 14.

"SANS 2019 Threat Hunting Survey: The Differing Needs of New and Experienced Hunters," October 2019, www.sans.org/webcasts/2019-threat-hunting-survey-differing-experienced-hunters-111010, p. 17, Figure 14.

Network Visibility Tooling

Earlier, we noted the tools respondents have in use at their organizations. Across the sample set, a significant number of respondents reported having network IDS/IPS and NGFWs, and a large number indicated using host IDS/IPS. We also asked survey participants to identify how they plan to use tools in the near future. As shown in Figure 10, 7% of respondents suggested that they may be looking to retire or replace NIDS/NIPS, with 9% considering the same for HIPS/HIDS. Another 7% are also considering replacing or retiring their NGFW platforms.

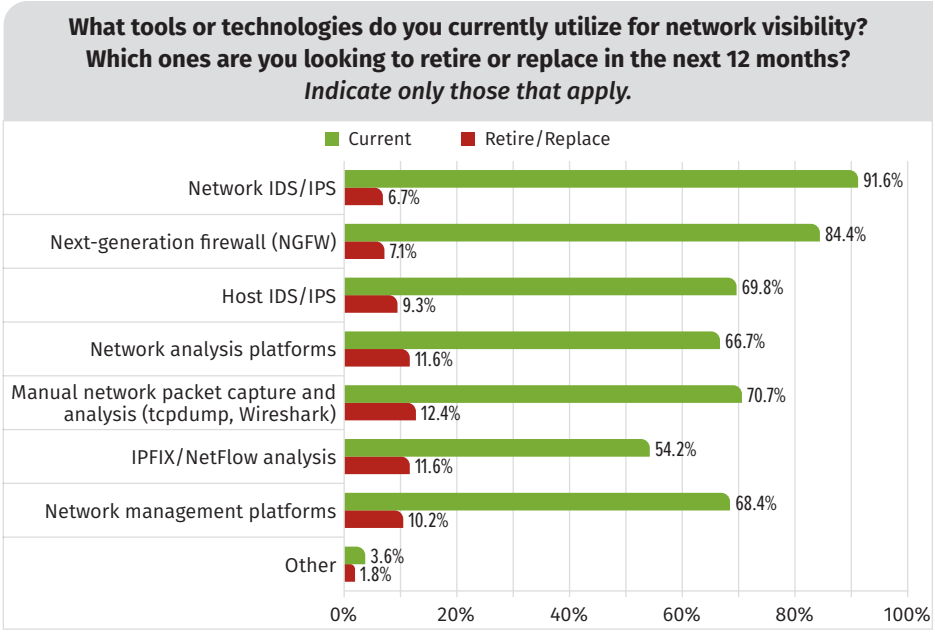


Figure 10. Tools in Use and Slated for Retirement/Replacement

It's hard to discern whether these plans reflect the increasing expansion of corporate boundaries and the continued shift from hard perimeters. If this is the case, a move from perimeter to data-centric protection would help ensure security of both data and assets. This shift drives the case for better visibility for data in transit—bringing challenges of both scale and transparency that will need to be addressed.

Action Step

Develop an understanding of the acceptable patterns for normal access to data. Use this to build an efficient auditing and monitoring strategy for entities accessing the data.

Organizations use a wide variety of tools to provide the data needed for visibility. The challenges have always been to determine what the most valuable data is, what the best tools for its collection are and how to correlate the results gathered from the network to develop the appropriate basis for information and action. With changing perimeters, these elements and related concerns may be driving organizations' plans to modify their current tooling across hybrid networks. For example, cloud service providers have started to offer virtual tap capabilities to make access to cloud traffic data easier. The following sections explore these challenges.

Data Capture: Using Full Packet

Most respondents (57%) reported that they only require full packet capture when the packets are associated with a detected threat, as illustrated in Figure 11. The reason may be because packet capture can be an expensive option and can bring challenges around storage, compliance and confidentiality. Because network traffic contains the raw data, possessing the traffic is only a few degrees removed from possessing the files.

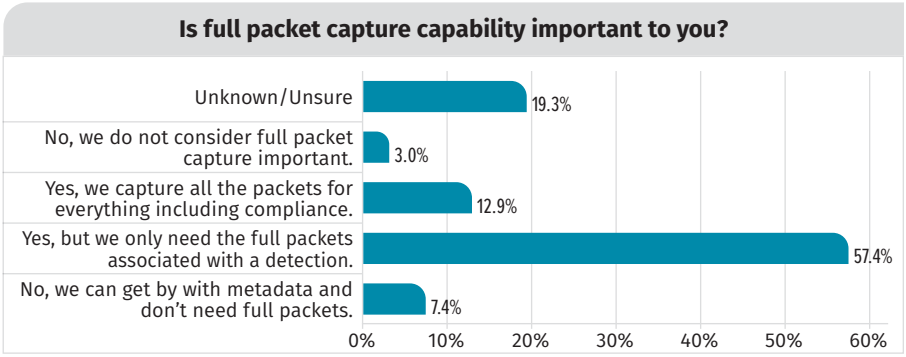


Figure 11. Importance of Full Packet Capture

File extraction is trivial across many standard protocols, so an attacker who is able to harvest network traffic is likely to gain access to the files being transmitted fairly easily. Encryption helps mitigate the risk of attackers successfully stealing sensitive data via network traffic, but it also reduces the security team's ability to deeply investigate threats and anomalies using network traffic. Decrypting traffic for investigation is an increasingly important step for security operations, but it has to be done the right way to avoid re-introducing risk.

Where traffic is captured for compliance, it may be to provide a record of conversations within financial institutions or organizations subject to similar levels of oversight. This traffic is usually only reviewed as part of a specific investigation.

Table 3. Tools/Services Used to Detect/Investigate Compromises

Tool/Service	% Who Use
Analyst investigation (SIEM or other)	73.2%
Anti-malware/Antivirus	63.8%
Automated alerts from SIEM	49.6%
Endpoint detection/EDR	42.5%
Intrusion detection or intrusion prevention systems (IDS/IPS)	37.8%
Next-generation firewall	31.5%
Threat hunting	25.2%
Sandbox/Detonation technologies	22.1%
Third-party notification	22.1%
Application whitelisting or blacklisting	20.5%
Security-as-a-Service (e.g., MSSP)	20.5%
Threat intelligence	18.1%
Web application firewall	18.1%
Extended system logging (Sysmon/Auditd)	17.3%
Network packet capture	17.3%
DLP or data monitoring	16.5%
User and entity behavior analytics (UEBA) anomaly detection	15.0%
IPFIX/NetFlow analysis	12.6%
Cloud service monitoring	11.0%
Network application layer transaction monitoring	6.3%
Other	6.3%
CASB	3.9%

Tools to Detect and Investigate

Respondents identified the tools they have available to detect and investigate potential compromises on their networks. Analyst investigation using SIEM was the top response, at 73%. Automated SIEM alerts (50%) were also high on the list. Anti-malware (64%), endpoint detection/EDR (43%) and IDS/IPS (38%) rounded out the top five tools. Table 3 details the remaining responses.

It is common for a SOC to use the SIEM to drive its responses. Even with a SIEM in place, organizations deal with a high degree of false positives. Network data offers a way to enhance the SIEM's effectiveness by providing data that is most important to alert on and validate the severity of potentially dangerous incidents.

The increased popularity of threat hunting within the last few years has allowed security teams to take a more proactive approach to detection. Network data is incredibly valuable to hunters attempting to validate their hunting hypotheses. Ensuring that hunt teams can efficiently query the collected data and that the data is indexed and available in the correct forms drives process efficiency in these teams.

Takeaway

If you want to make better use of network data, understanding how the data will be used is imperative. Decide whether the data will extend existing tooling, support a parallel process or a blend of these. Each choice may shape a different path to collection and processing of the network data.

Integration Needed

Having an interface that brings all the relevant data needed by an analyst to do their investigation is crucial. In practice, the promises of a single reference point, or single pane of glass, often involve too much compromise. While this single pane can work for a high-level overview, investigations generally require the ability to drill down into the available data to uncover the necessary level of detail on a detection.

Takeaway

Finding and understanding the data needed at any given time has always underpinned the success of a good analyst. Knowing where to find data to keep the investigation moving onward is vital for the success of the analyst and the overall security of the investigation.

Earlier, we highlighted that most respondents have both network and host IDS/IPS. This capability is a good starting point and reinforces the value we can gain from actions based on the network data. With IDS as a passive observation system, the visibility of network traffic can drive alerts, usually to a central management server or the SIEM. With the IPS options, the systems can actively block malicious traffic based on signature matches or anomaly detection. Historically, these products have relied on relatively coarse, static signatures to detect threats. Such signatures can still have value because many vulnerabilities go unpatched for years. However, these mechanisms cover an ever-smaller portion of threats.

Taking this a concept a step further would allow the enterprise to progress from the NIDS/HIDS model and make alert judgments based on a deeper understanding of the traffic content itself. The IDS model has evolved from the origins of signature matching and grown into a more mature feature set, which allows the detection of anomalous or unexpected behaviors in traffic. As new systems build better rulesets to understand normal traffic flow, they enable organizations to use machine learning and product-related innovations to scrutinize the transactions within the network payload. Further, these systems can look deeper into the traffic, analyzing the context of individual transactions and providing richer data to security staff. Together these benefits enable organizations to better understand the patterns of regular traffic and protocol usage, which can be cycled back to upgrading the models and rulesets in use.

In a 2019 Gartner paper,[2] the analysts revisited a modified term from one of Anton Chuvakin's prior blog posts.[3] Initially, in 2015, Chuvakin introduced the "SOC Nuclear Triad." In the later Gartner paper, this has now developed into the "SOC Visibility Triad." This triad, illustrated in Figure 12, reflects three powerful pillars that help modern SOCs identify and disrupt threats as they arise. The model also supports the importance of the network, given that this data is based on observation external to the hosts themselves and far less susceptible to malicious or external interference.

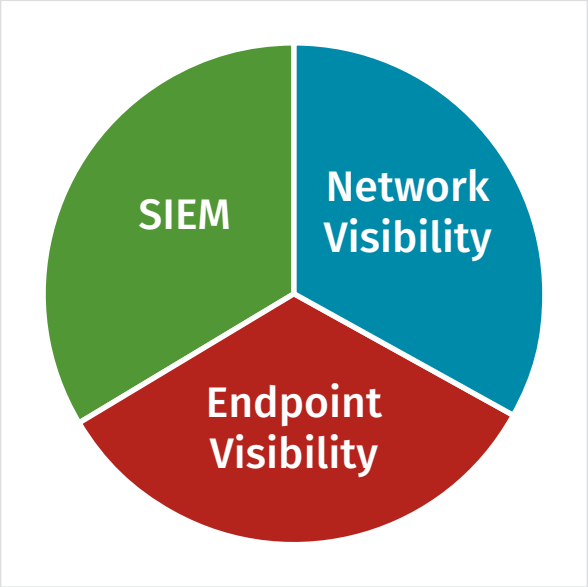


Figure 12. SOC Visibility Triad

As organizations evolve, the methods security teams use must also evolve at a similar pace to ensure that they do not fall behind. This evolution remains a crucial challenge, especially in older and more geographically dispersed organizations. If we add the burgeoning network of IoT devices into this mix, the first item on the CIS Controls list,[4] "Inventory of Authorized and Unauthorized Devices," becomes a daunting task.

[2] "Applying Network-Centric Approaches for Threat Detection and Response," March 2019, www.gartner.com/en/documents/3904768 [Registration required.]

[3] "Your SOC Nuclear Triad," August 2015, https://blogs.gartner.com/anton-chuvakin/2015/08/04/your-soc-nuclear-triad/

[4] www.cisecurity.org/controls/cis-controls-list/

Identifying and monitoring growing environments is where network visibility comes into its own. If properly managed and integrated, this practice has the potential to deliver considerable benefits to organizations both in the security space and in providing a clearer picture of the devices and activity on corporate networks.

Takeaway

Take steps to inventory all the devices connecting to your network. Without this knowledge, it is impossible to distinguish between normal and abnormal traffic.

Filling the Gaps in Network Visibility

Gaining network visibility within the enterprise is subject to numerous opportunities and challenges. With perimeter security, there are limited ingress/egress points, and this allows for easier traffic inspection. With the traditional perimeter disappearing, measuring traffic inside the organization is a broader challenge.

Traffic Flow: North–South vs. East–West Visibility

Most organizations have high confidence (52%) in their established visibility of the traditional north–south border. As explored earlier, this perimeter is becoming more and more porous as services and end users move outside of the traditional corporate office networks by choice or necessity. The network management systems originally intended to monitor corporate networks may struggle to maintain their relevance because the data flows may originate and terminate outside of the old perimeter.

Obtaining a clearer view of the east–west traffic allows the organization to regain some confidence. This picture should deliver an understanding of where critical applications and data are being accessed from and how they are being used. North–south visibility helps to identify intrusion attempts, whereas east–west visibility can identify attackers who have already successfully established a foothold inside the network. Within the traditional data center model, the need for mirrored ports and network taps to view traffic in detail has always been an architectural issue. Ideally, these would be present in the design at inception. Often, however, this is not the case. Monitoring requires deployment or retrofitting of network taps or the configuration of network SPAN ports. In the cloud, the implementation of the monitoring infrastructure is substantially easier, and CSPs offer options to replicate traffic with virtual taps, making the initial provision of the data easier.

Takeaway

The options to collect network flow data or full packet capture are present in the offerings of the major cloud vendors, although it is important to understand the pricing considerations that come with the more data intensive options.

The survey results reflect less confidence in the ability to meet these requirements, with only 16% of respondents reporting a high level of visibility for east–west traffic. There seems to be a common desire to close this gap. Matching technology capabilities to the business needs of the security groups can help accelerate the process.

Once an organization has the visibility it needs, the next step is finding the most efficient way to make the best use of the data available. Extracting information from the east–west traffic delivers a far more robust understanding of the daily patterns. This is especially relevant as the organizational landscape extends to the cloud providers. The patterns described by network source data reflect an accurate and current picture.

Takeaway

In the early phases of a compromise, most security teams rely on a mixture of data feeds to detect and eradicate the adversary. One of the most useful feeds for this hunt is the east–west network data, illustrating the lateral movement from host to host across the network. This dataset is invaluable to responders and threat hunters alike.

Traffic Flow: Lateral Movement

When it comes to investigating incidents, the choice of tools shows an interesting pattern. Traditional sources still play a major role for most respondents. At 73%, the analyst-driven SIEM investigation takes first place (see Table 3 on page 11). Given that endpoint detection remains a key factor across the board, it is no surprise anti-malware protection comes in a close second with 64%. Automated SIEM alerts and EDR detections follow up with 50% and 43%, respectively. This is nothing new, and the fact that network-driven sources are very low in the overall results reinforces the east–west visibility challenges outlined in the previous section. Thirty-eight percent report IDS/IPS as a source, 32% use a next-generation firewall and 17% use packet captures. Finally, 13% use network flow data, while 6% work with network application and transaction data. The potential for a faster and higher quality response is immense because, according to the survey responses, data sources reflecting east–west lateral movement are relatively underutilized.

Takeaway

Network data helps round out the investigation. Add data sources reflecting east–west traffic, such as IDS/FW data, packet capture analysis and network flow, and full-stream network traffic analysis. This data provides analysts with a more complete picture and helps them triage and classify incidents in a more efficient manner.

Expose the Abnormal

If an organization can automate the collection and interpretation of the network data, it can generate a pattern of normal behavior. There is a common risk: If we baseline without due care, bad traffic and unauthorized actions become part of the baseline.

When considering what other data can be collected, the payload data held within the network traffic shows why the traffic exists. The visibility of database methods, certificate data and Windows SMB/CIFS traffic drills down into a large part of the corporate traffic (see Table 4).

This data shows the true pattern of normal traffic. Understanding how the applications are being used on the network is often a goal that lies outside of the view available to the security team. Once the application data is available to the security team, it can be indexed and searched. This also adds to the data sets available for hunt teams to comb through.

Table 4. Additional Data Collection for Better Network Visibility

Tool/Service	% Who Want
Database methods	42.4%
Certificate metadata	35.5%
SMB/CIFS methods	34.0%
IPFIX/NetFlow/Host-to-host connection data	28.1%
HTTP payloads	24.6%
DNS transactions	23.2%
DHCP transactions	22.7%
Active Directory/LDAP login attempts	8.4%
Other	4.4%

Reactive and Proactive Monitoring

When used as a data source to support an investigation, network data is highly valuable and fills out the broader story. When tracing initial infections, lateral movement and data theft, network data is an invaluable reference source by first identifying the anomalous behavior and then providing the ability to drill down into affected packets. The restrictions that surfaced in the survey, especially around skill and staffing levels, outline a gap that is not going away. New methods to collect data, provide context and correlation, and query that data as part of an investigation offer a way to reduce the burden.

With the right focus on passively collecting the Layer 2 to Layer 7 data, there is an opportunity to turn this data into an active security source—a generator of incident notification and a true alert source. This does require analysts to learn difficult new skills; however, effective monitoring does provide intelligence to make their decision process more intuitive.

Moving from reactive to proactive monitoring allows organizations to actively utilize network data and provides the opportunity to gain insight from the encrypted traffic streams.

Working with Encrypted Traffic

As noted previously, 82% of respondents encrypt 25% or more of their internal network traffic. One difficulty in reviewing the network data is an absence of an efficient means to interrogate the encrypted data. Encryption requires extra steps to dig into the raw data. With good architectural planning or an analysis platform that can support decryption, the encrypted data can be extracted as and when required.

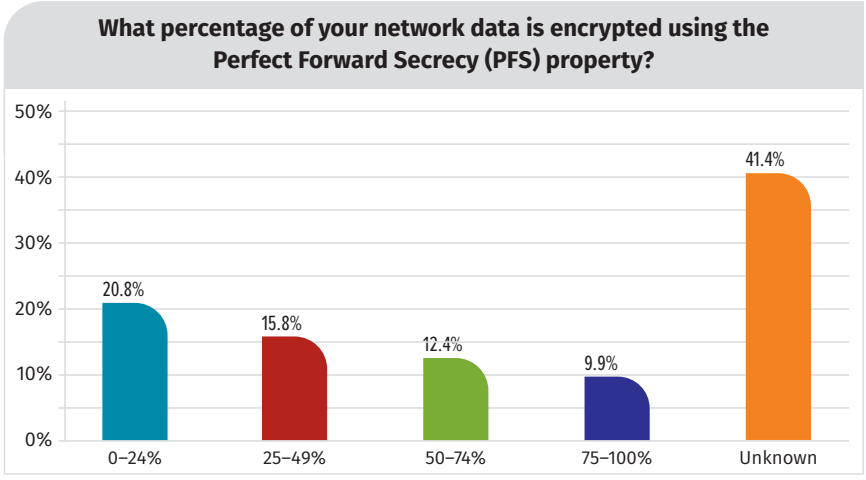


Figure 13. Use of PFS

Not all encryption is created equal. TLS 1.3 mandates PFS, which ensures that a unique encryption key is created for every encrypted session. This is a major step forward from prior options where the same server-side key could be used to decrypt all traffic captures from that server over a much longer period of time. However, PFS also breaks many passive decryption options and may necessitate either a man-in-the-middle appliance to terminate and decrypt these streams or a session-key forwarding capability in the analysis platform.

Where the encryption is negotiated with TLS, especially TLS 1.3 and PFS, it is essential to ensure that keys are recorded at the time of transmission and associated with the relevant network traffic. Figure 13 provides a breakdown of the usage of PFS in the respondents' networks.

If encryption keys are not captured and PFS is in use, any full packet capture of the encrypted data is unusable. Ensuring secure storage of encryption keys and auditing the use of these keys is critical to ensuring the continued secrecy of data both in storage and in use by the security team.

Action Step

Ensure that the solution used to record the encryption key and capture the encrypted traffic is securely architected. This presents a valuable repository of sensitive data and is a valuable target to external attackers and malicious insiders.

Automation and Analytics

For the capture and processing of network data to be successful and productive at scale, it is advisable to involve an automation and analytics platform that can take some of the load off the analyst team. This practice allows analysts to focus their skills on understanding the story that the data tells. Understanding that story is critical to recognizing an incident or discarding a false positive.

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.

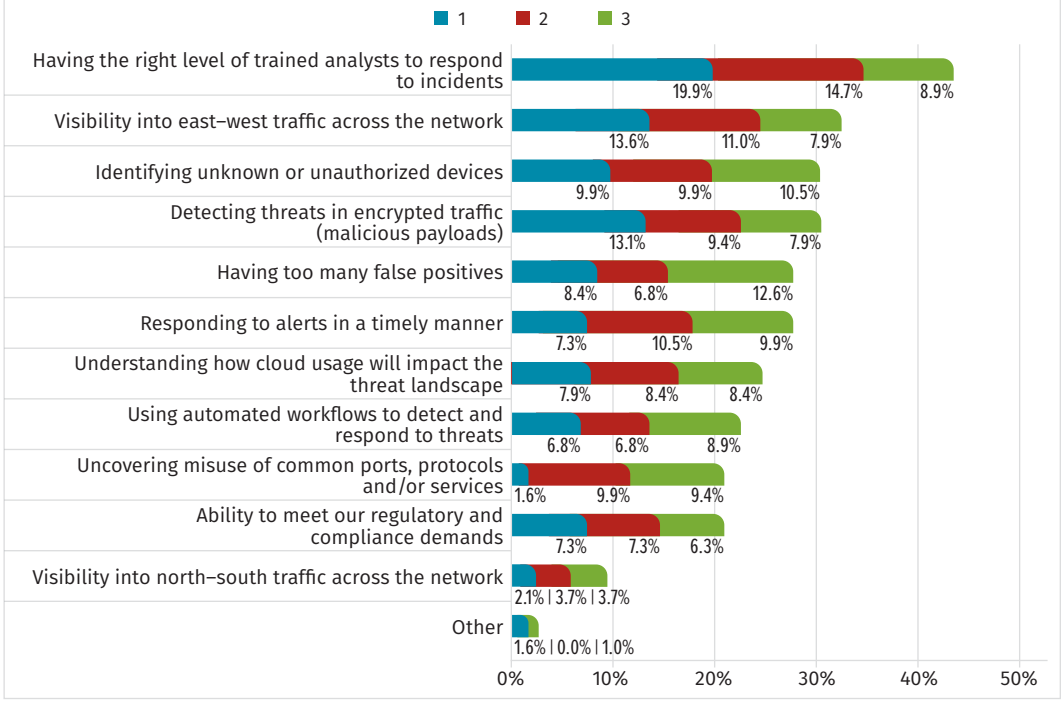


Figure 14. Challenges of Current Infrastructures

In a recurring theme, analyst skill (20%) and time (7%) again surface as key concerns, alongside better visibility into east–west traffic (14%), the ability to view encrypted data (13%) and identifying unknown or unauthorized devices (10%), as shown in Figure 14. Concerns around cloud adoption and compliance and regulatory requirements are also present. The scope of these issues will grow until the security tooling available reaches a maturity level, which frees the analysts from low-level collection tasks and allows them to concentrate on interpreting the data at their fingertips.

Automation can mitigate many of these problems. In fact, many organizations already automate visibility (68%) and detection (71%), with others planning to do so in the coming months, as illustrated in Figure 15.

Increasing automation in the areas of response and investigation look to be a goal for the coming year, with more than 50% reporting plans for such changes. When organizations embrace automation and apply it effectively, it delivers a consistent and noticeable advantage for the analysts. One obvious advantage of automation is freeing analysts from repetitive manual work, redirecting their attention to other more challenging or interesting cases that benefit the business.

Are you currently using automation for network visibility, detection, response or investigation within your network? If you are not currently using automation, do you have plans to do so within the next 12 months?

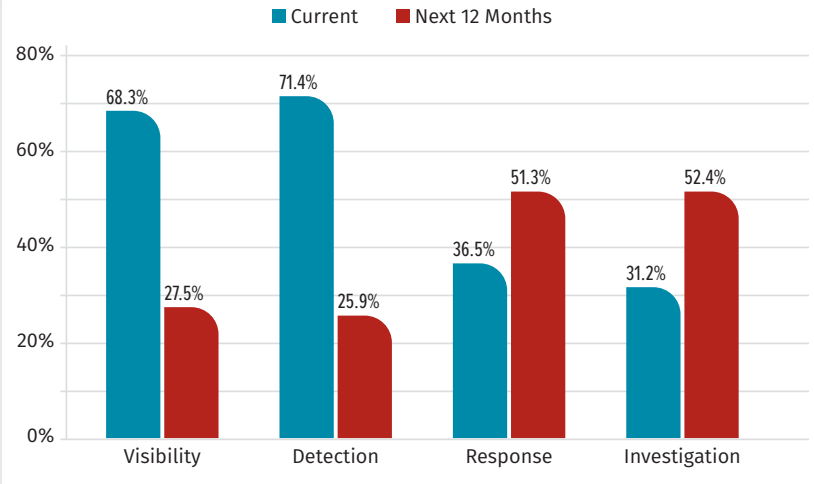


Figure 15. Use of Automation

Conclusion

There are untapped opportunities for organizations to mature in the methods they use to analyze network data. Investing time in understanding how and where those improvements can be delivered results in greater network visibility and threat detection capabilities.

Understanding the east–west traffic, securely decrypting and analyzing encrypted sessions, and identifying unknown devices on the network are all benefits of increased network visibility.

Capitalizing on these opportunities will bring real and measurable benefits. By building on existing foundations and working to develop more mature tool sets, the network data can reduce visibility gaps in both legacy and cloud environments.

The decision to build your own capability or buy a commercial offering is always a challenging one. If you have the internal capability, in staff, time and skills to collect, analyze and report on the available network data, building your own solution may be a valid choice.

Alternatively, it may be smarter to look outside and find a technical partner who can help relieve some of the internal challenges. They can help you find and process the right sources with the right priority and, subsequently, shorten the time required to deliver real gains in monitoring and response capabilities for the organization. Knowing where to look and how to interpret network data is more than half the battle. If you can make better use of the data you have without increasing resources, you will be one step ahead of the game. One aim of this survey was to understand where organizations are today. We challenge our readers to consider how best to use the available data to improve their organizations' security.

About the Author

Ian Reynolds, SANS SEC401: Security Essentials Bootcamp Style instructor, works with public sector bodies, corporate enterprises and businesses from a wide mix of verticals across the world. He runs his own consultancy and works with his clients to develop and improve security operations, threat hunting, incident response and forensic capabilities, helping them address business challenges along the way. Ian is a GIAC Advisory Board member and holds a variety of certifications, including the GSEC, GCED, GICSP, GCIA, GCIH, GCFE, GCFA, GNFA, GREM, GPEN, GXPN, CISSP and CISM, in addition to several vendor certifications.

Sponsor

SANS would like to thank this paper's sponsor:

ExtraHop