Corporate network visibility in 2020

ptsecurity.com

We surveyed information security experts to learn their opinions on:

Respondents included 231 infosec pros

01 Visibility of their corporate networks

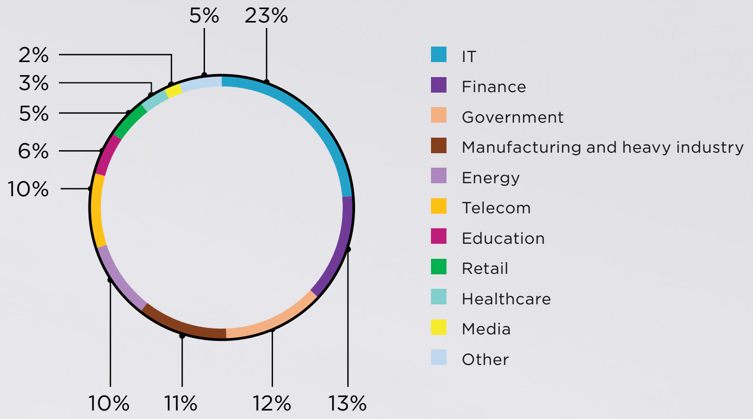
02 Expectations for traffic analysis

03 Perceived trade-offs of encrypting internal traffic

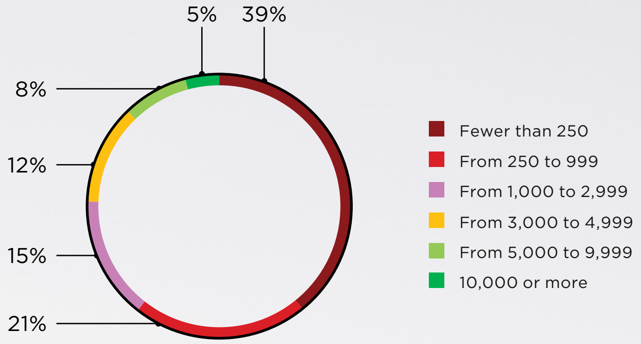
The anonymous survey, with responses from 231 specialists in Belarus, Russia, and Kazakhstan was conducted from August 27 to September 14.

Who participated in the survey

What is your company's industry?



How many employees does your company have?



On the whole, we found that responses did not tend to vary significantly based on a company's size or industry.

Summary: What we learned

01 The surveyed infosec experts assess the visibility of external traffic as on par with that of internal traffic at their companies.

02 Over the last year, only 8 percent of respondents have detected attacker lateral movement and only 17 percent detected the use of hacking tools. This is likely because most of the surveyed experts do not have appropriate detection tools in place at their companies.

03 When asked to choose between encrypting traffic or improving visibility into the internal network, 64 percent of respondents prefer the latter.

04 According to respondents, the most important tasks for traffic analysis tools are to detect attacks inside the network (88%) and on the perimeter (86%), detect network anomalies (71%), and monitor compliance with security standards (71%). These are typical functions performed by network traffic analysis (NTA) (or network detection and response, NDR).[1]

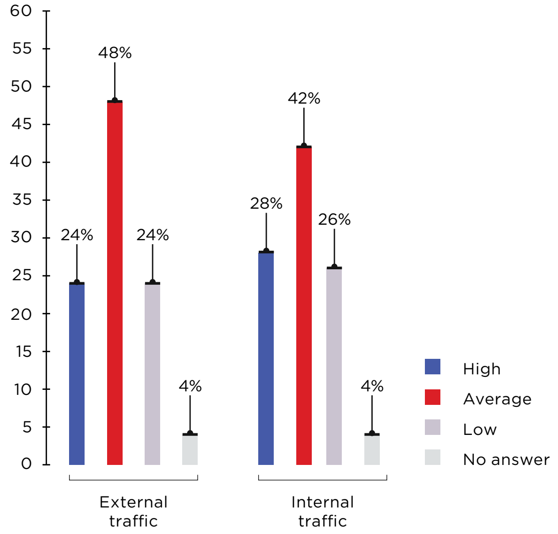
05 Traffic decryption and retrospective analysis are considered lower-priority tasks, winning the enthusiasm of 29 and 27 percent of experts, respectively.

[1] **NTA performs analysis of traffic both on the perimeter and inside infrastructure.** NTA solutions automatically detect attacks based on a large number of signs, including use of hacking tools and exfiltration of data to an attacker server. They store information about network interactions; some also store raw traffic. Such data can be useful for tracking attacker movements and investigating incidents.

Traffic visibility

Our survey demonstrates that most companies lack traffic analysis tools, not all network segments are covered, or visibility is hampered by data encryption. "Low" or "average" visibility into external traffic is a complaint of 72 percent of respondents; 68 percent have the same opinion regarding the visibility of internal traffic.

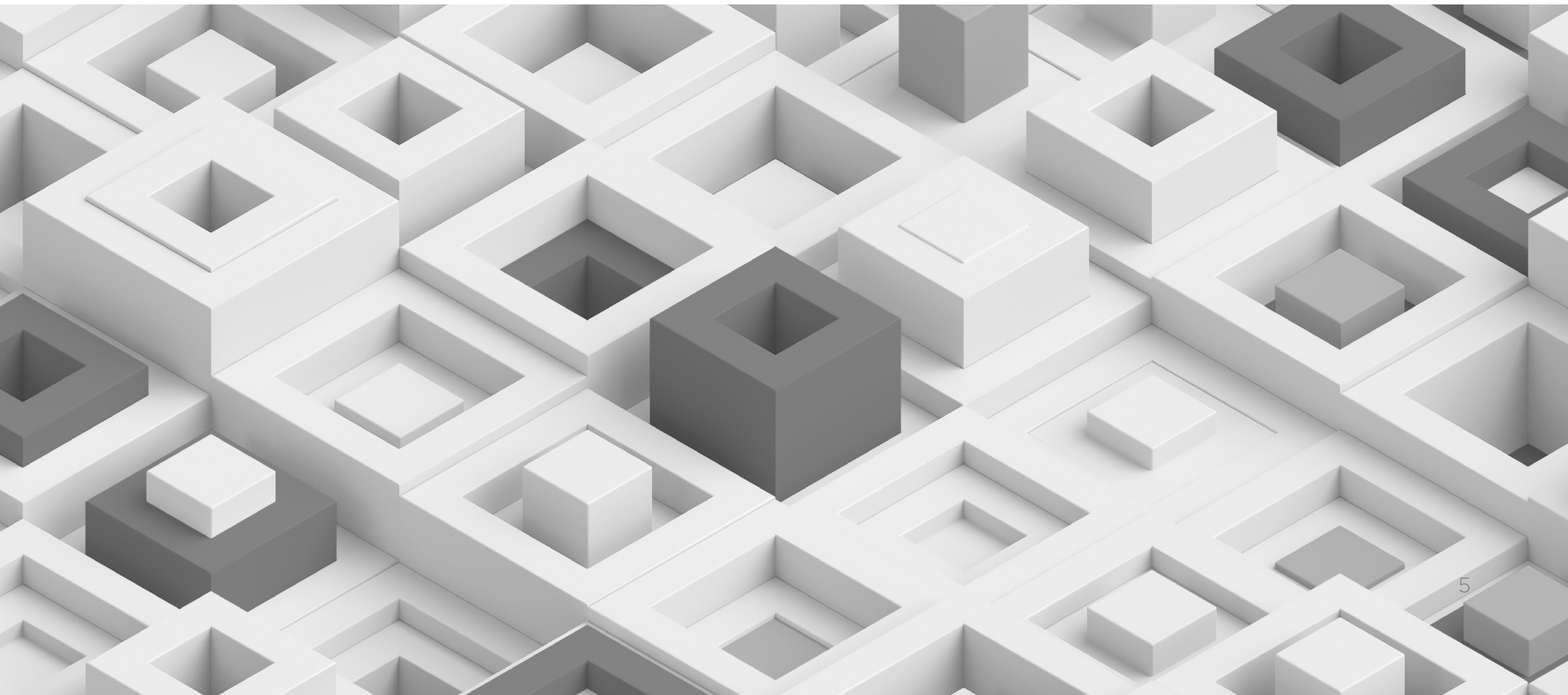
How do you assess the level of traffic visibility at your company?



Traffic visibility by industry

IT and financial companies turn out to be the most satisfied with the visibility of external traffic: 42 percent and 38 percent of these respondents, respectively, assess the visibility level as high. Industrial companies are on the other end of the spectrum: 36 percent of experts consider external traffic opaque.

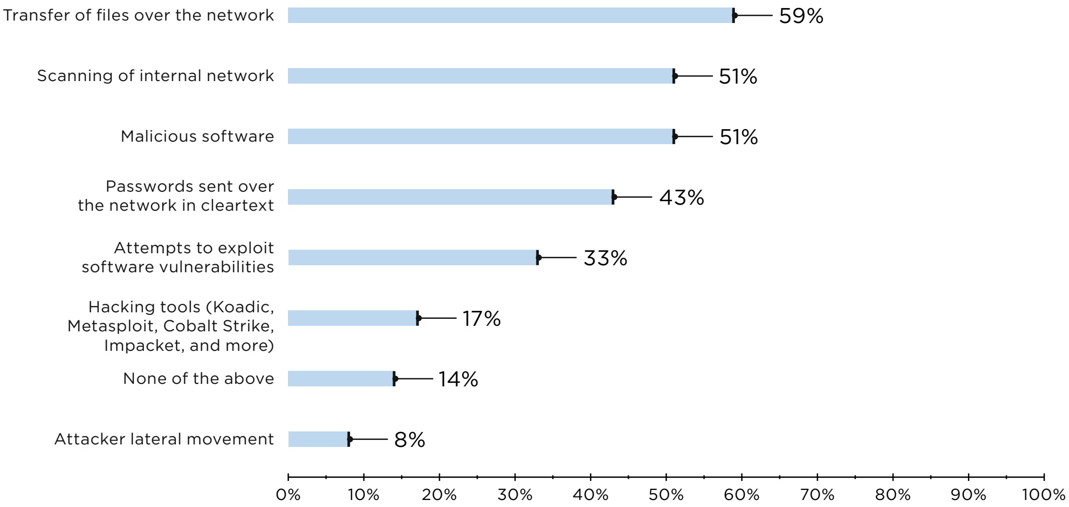
The situation is similar with internal networks. Almost half of IT companies (47%) claim high visibility, while slightly more than half of respondents at industrial companies (52%) assess visibility as low.



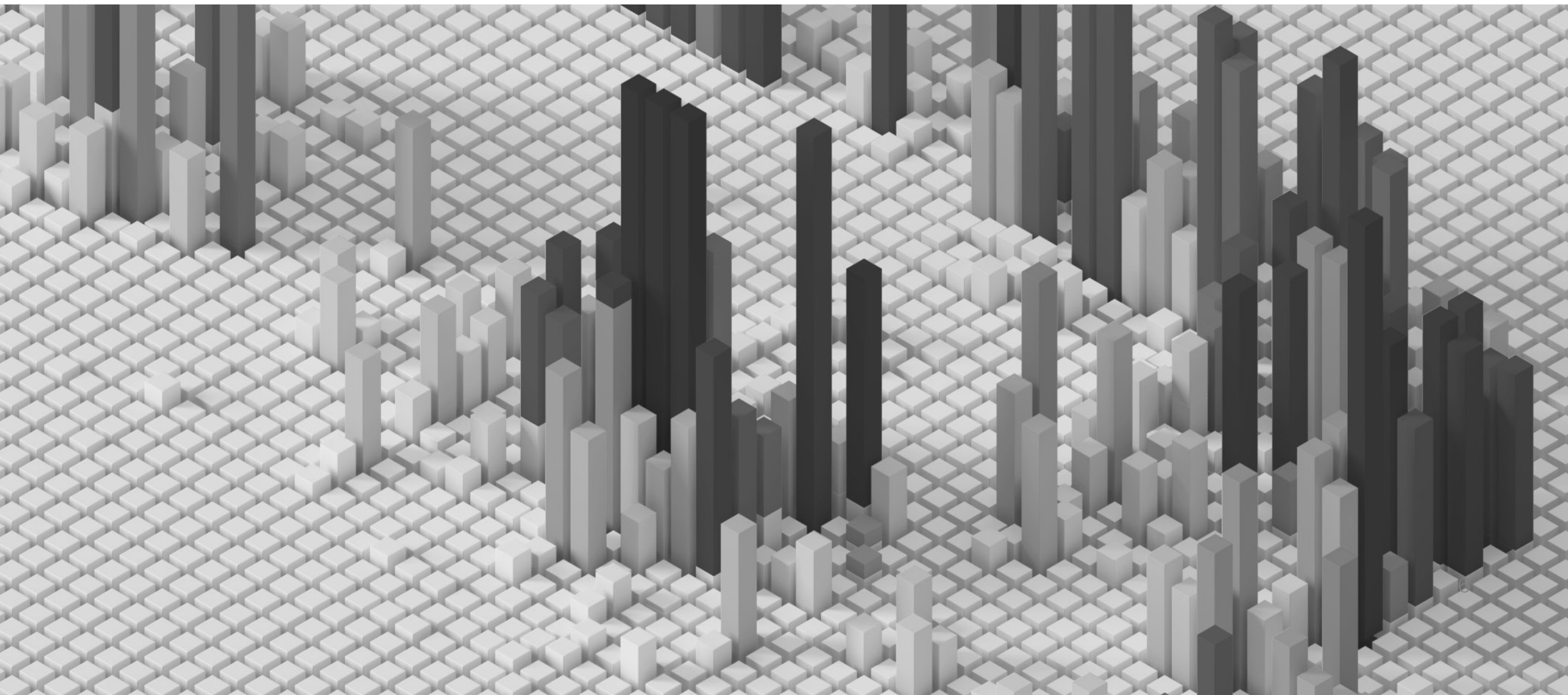
Internal network (in)visibility

Over the last year, 51 percent of respondents have detected internal network scanning and malicious activity inside the perimeter. The situation is worse with lateral movement and use of hacking tools to develop attacks. During the last year, such actions were observed by only 8 and 17 percent of experts, respectively.

What have you observed in internal traffic over the last year?



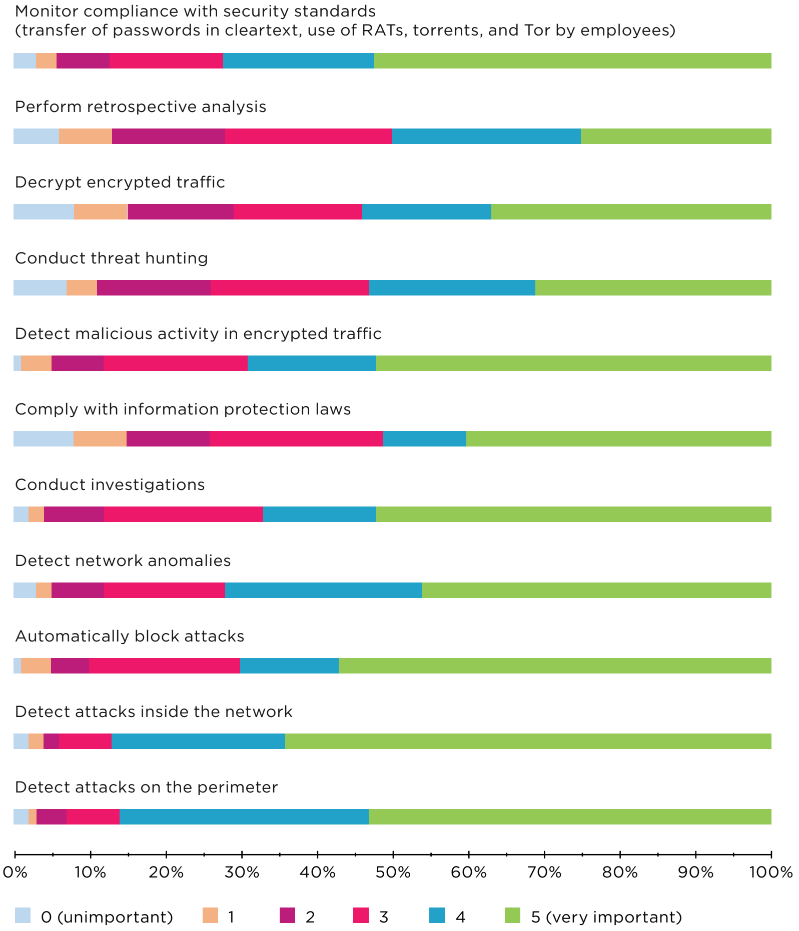
Many protection solutions, such as antivirus software and EDR, can detect network scanning and use of hacking tools. It would seem that the experts we questioned performed detection without using NTA, the capabilities of which include detecting lateral movement and use of hacking tools.



What do traffic analysis tools need to do

For the experts we surveyed, threat detection is the top priority. 88 percent of them give the highest priority scores ("4" or "5") to detection of attacks inside the network; 86 percent indicate detection of attacks on the perimeter, and 71 percent mention detection of network anomalies and security policy compliance.

How vital is it to you to perform each task using traffic analysis tools?



Traffic decryption is at the top of the "less important" tasks. 29 percent of respondents give it a low priority score ("0," "1," or "2"). But this does not mean that they do not care what is going on inside encrypted traffic: 70 percent of respondents at large companies recognize the importance of detecting malicious activity in encrypted traffic ("4" or "5"). If network packets are analyzed properly, detection does not require decryption.

Retrospective analysis is also a lesser priority, for 27 percent. This is probably due to the high cost of traffic storage servers.

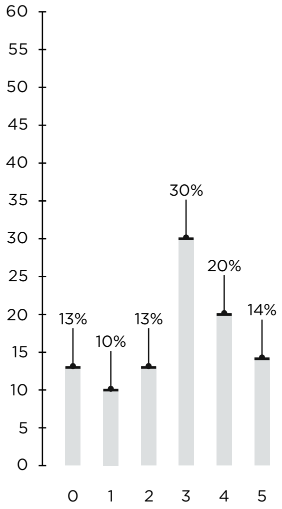
Encryption vs. **network visibility**

The need for network visibility outweighs potential encryption benefits in the eyes of 64 percent of respondents. Worries about traffic encryption were reflected in most responses ("3," "4," or "5") to the following question.

How worried are you that traffic encryption inside infrastructure inhibits network visibility?

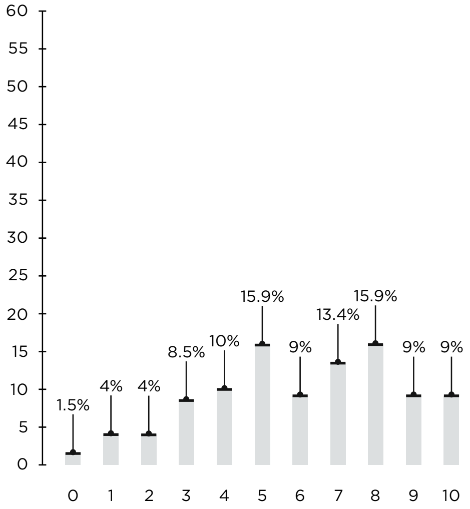
0: I do not care about network visibility, traffic must be fully encrypted within the network.

5: I prefer not to encrypt traffic in order to get full network visibility.



This closely matches the findings of a SANS survey: 56.3 percent of respondents were worried that encryption prevents network visibility (6–10 points).

Level of concern about traffic encryption



Encryption within corporate networks is a thorny issue. In some cases, encryption is necessary—such as if all passwords and emails must be encrypted in transit. However, many infrastructures, especially large ones, have difficulty with encrypting all traffic because of obsolete server equipment and incompatible software. And even then, encryption increases the risk of "going dark" because it makes attacker actions more difficult to detect.

Conclusions

- NTA solutions have a large future ahead of them: companies understand the importance of monitoring the security of internal networks. This is clear from the respondents' stated priorities for what NTA should do.
- Not all companies have NTA monitoring of internal networks in place. We can conclude this based on what the surveyed security experts managed to detect inside their perimeters over the last year.
- Most respondents do not support full encryption of corporate networks, giving NTA the maximum of opportunities to detect malicious activity. Those who do choose to encrypt traffic as much as possible can also benefit from NTA for detecting anomalies and malware.

About Positive Technologies

ptsecurity.com
pt@ptsecurity.com
facebook.com/PositiveTechnologies
facebook.com/PHDays

For 18 years, Positive Technologies has been creating innovative solutions for information security. We develop products and services to detect, verify, and neutralize the real-world business risks associated with corporate IT infrastructure. Our technologies are backed by years of research experience and the expertise of world-class cybersecurity experts.

Over 2,000 companies in 30 countries trust us to keep them safe.

Follow us on social media (LinkedIn, Twitter) and the News section at ptsecurity.com.