Encrypted Traffic Inspection for Cyber Security

Modern malware and ransomware attacks have become a big issue for enterprises. Many organizations rely on encryption for protection against these attacks. However, encryption is meant to offer privacy, and only acts as a false sense of security. If these enterprises aren't decrypting their traffic, malware attacks can hide behind encryption and make their way into otherwise secure networks, undetected.

Pulse and A10 Networks surveyed 200 technology leaders to find out how their companies are thinking about decryption solutions.

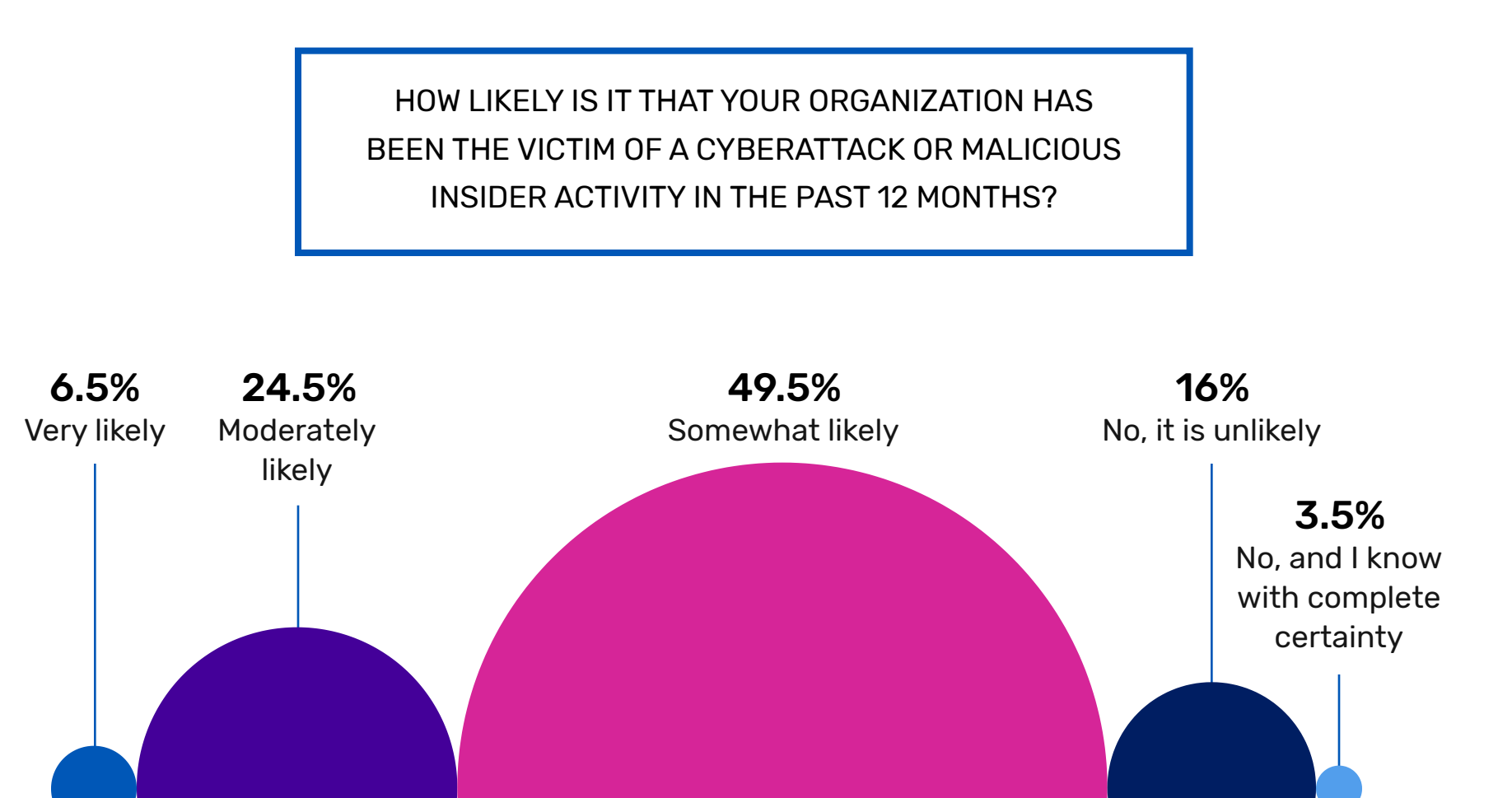
Data collected from June 18 - July 3, 2021

Respondents: 200 technology leaders

Web traffic inspection is an important line of defense against likely cyberattacks, but encryption may be leaving networks vulnerable

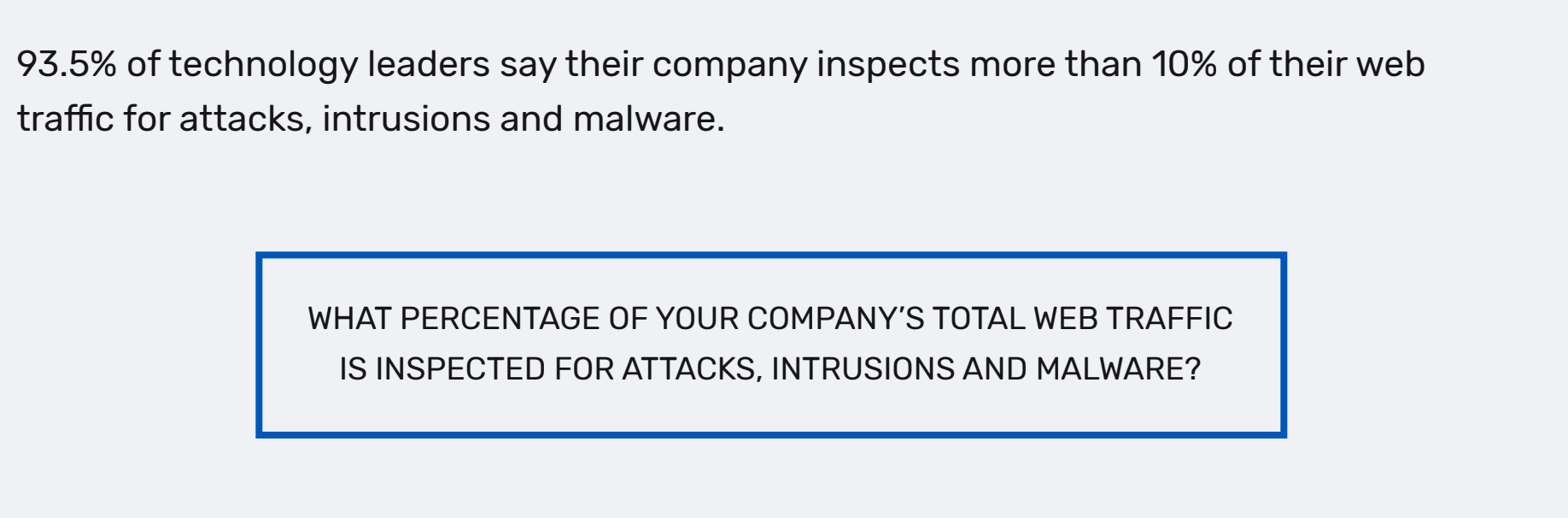
With cyberattacks becoming easier and cheaper to launch, it's no surprise that 80.5% of technology leaders consider cyberattacks at their organization likely.

HOW LIKELY IS IT THAT YOUR ORGANIZATION HAS BEEN THE VICTIM OF A CYBERATTACK OR MALICIOUS INSIDER ACTIVITY IN THE PAST 12 MONTHS?



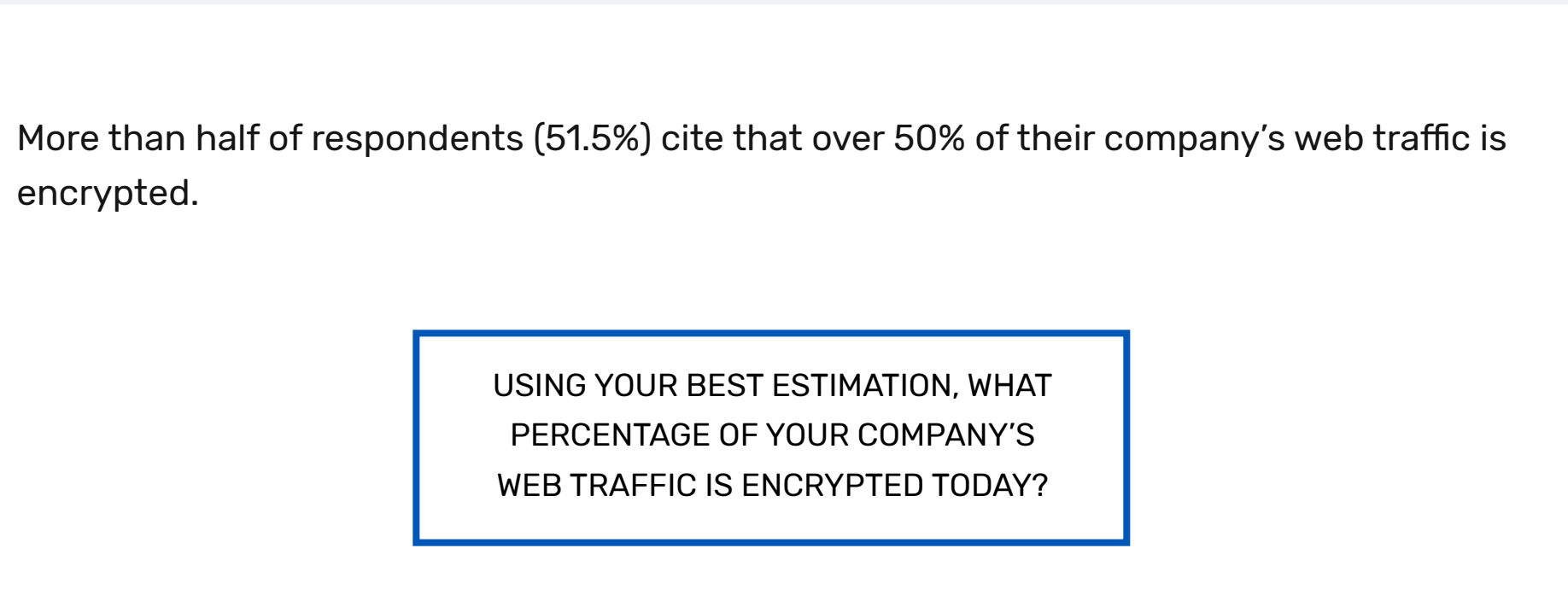
93.5% of technology leaders say their company inspects more than 10% of their web traffic for attacks, intrusions and malware.

WHAT PERCENTAGE OF YOUR COMPANY'S TOTAL WEB TRAFFIC IS INSPECTED FOR ATTACKS, INTRUSIONS AND MALWARE?



More than half of respondents (51.5%) cite that over 50% of their company's web traffic is encrypted.

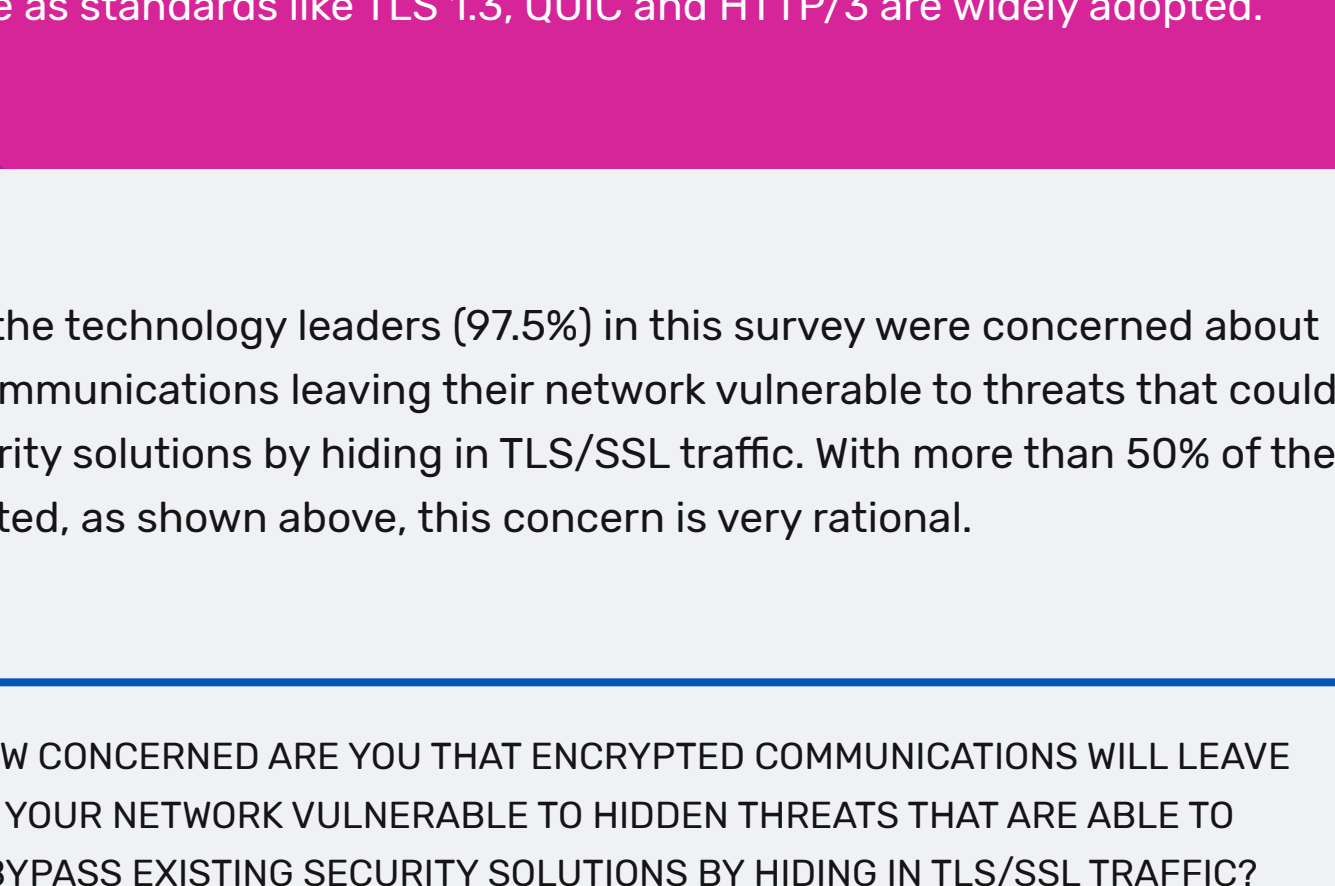
USING YOUR BEST ESTIMATION, WHAT PERCENTAGE OF YOUR COMPANY'S WEB TRAFFIC IS ENCRYPTED TODAY?



Widespread adoption of encryption standards like TLS 1.2 has been driven by companies like Google ranking websites that are encrypted higher than the ones that aren't. We see this percentage going higher in the future as standards like TLS 1.3, QUIC and HTTP/3 are widely adopted.

Almost all of the technology leaders (97.5%) in this survey were concerned about encrypted communications leaving their network vulnerable to threats that could bypass existing security solutions by hiding in TLS/SSL traffic. With more than 50% of the traffic being encrypted, as shown above, this concern is very rational.

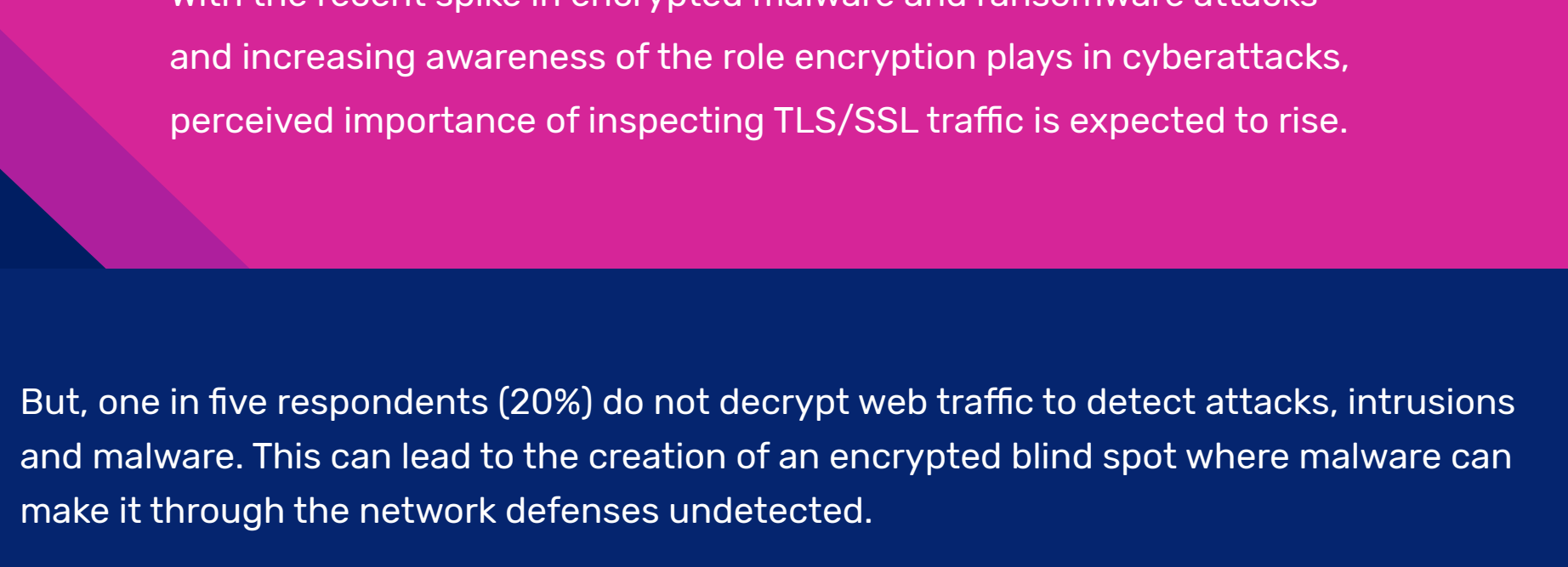
HOW CONCERNED ARE YOU THAT ENCRYPTED COMMUNICATIONS WILL LEAVE YOUR NETWORK VULNERABLE TO HIDDEN THREATS THAT ARE ABLE TO BYPASS EXISTING SECURITY SOLUTIONS BY HIDING IN TLS/SSL TRAFFIC?



Decryption is essential to inspect TLS/SSL traffic but lack of resources and privacy concerns hold some back

The majority of respondents (73%) think that the inspection of TLS/SSL traffic is moderately or very important to their company's overall security infrastructure.

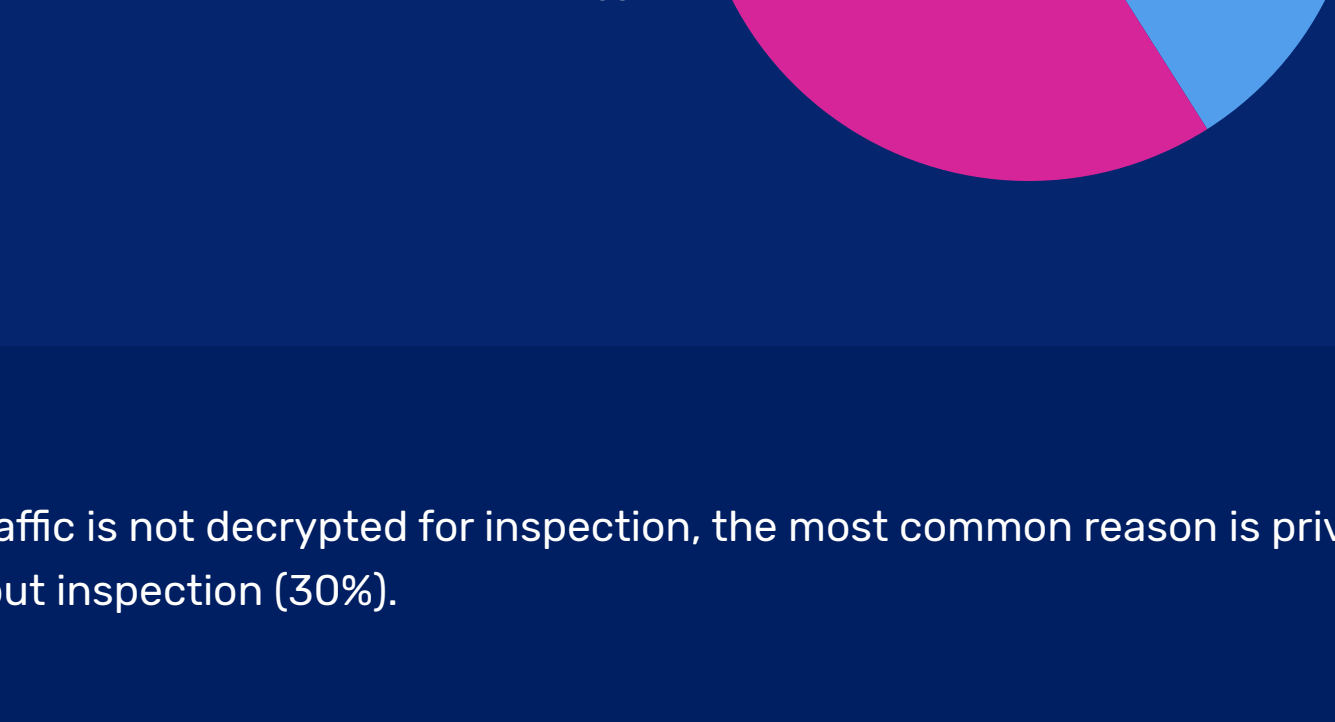
HOW IMPORTANT IS THE INSPECTION OF TLS/SSL TRAFFIC TO YOUR COMPANY'S OVERALL SECURITY INFRASTRUCTURE?



With the recent spike in encrypted malware and ransomware attacks and increasing awareness of the role encryption plays in cyberattacks, perceived importance of inspecting TLS/SSL traffic is expected to rise.

But, one in five respondents (20%) do not decrypt web traffic to detect attacks, intrusions and malware. This can lead to the creation of an encrypted blind spot where malware can make it through the network defenses undetected.

DOES YOUR COMPANY DECRYPT WEB TRAFFIC TO DETECT ATTACKS, INTRUSIONS AND MALWARE?



Where web traffic is not decrypted for inspection, the most common reason is privacy concerns about inspection (30%).

IF YOUR COMPANY DOES NOT INSPECT DECRYPTED WEB TRAFFIC, WHY NOT?

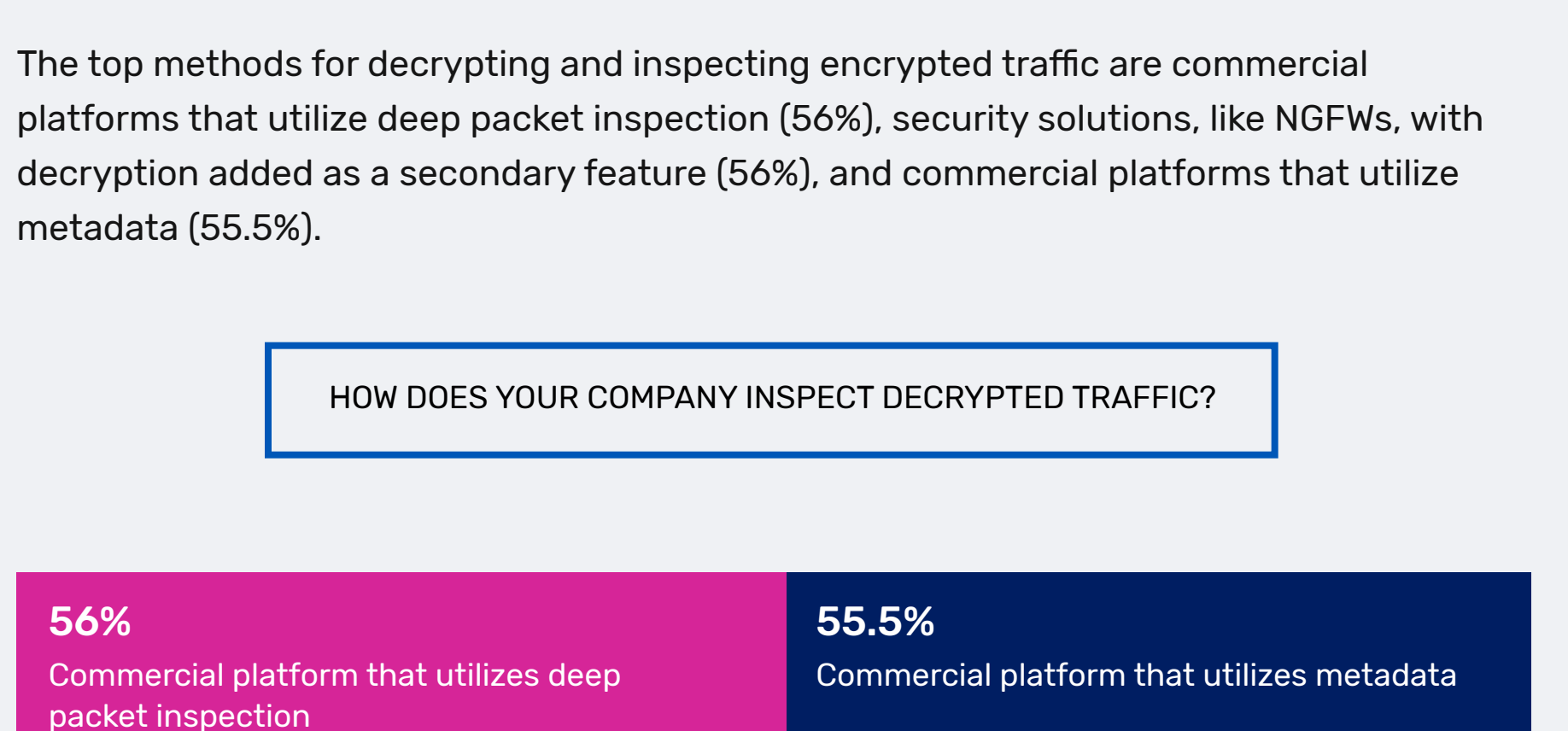
Since encryption and decryption are CPU-intensive processes, organizations that decrypt their web traffic often face performance degradation issues. 80% of technology leaders note that decrypting TLS/SSL traffic during the inspection process causes performance degradation of varying degrees.

WHEN YOUR COMPANY CURRENTLY DECRYPTS TLS/SSL TRAFFIC DURING THE INSPECTION PROCESS, HOW MUCH PERFORMANCE DEGRADATION DOES IT RESULT IN?

An ideal decryption and inspection solution proves ROI, is secure, highly scalable, and meets compliance requirements

The top methods for decrypting and inspecting encrypted traffic are commercial platforms that utilize deep packet inspection (56%), security solutions, like NGFWs, with decryption added as a secondary feature (56%), and commercial platforms that utilize metadata (55.5%).

HOW DOES YOUR COMPANY INSPECT DECRYPTED TRAFFIC?

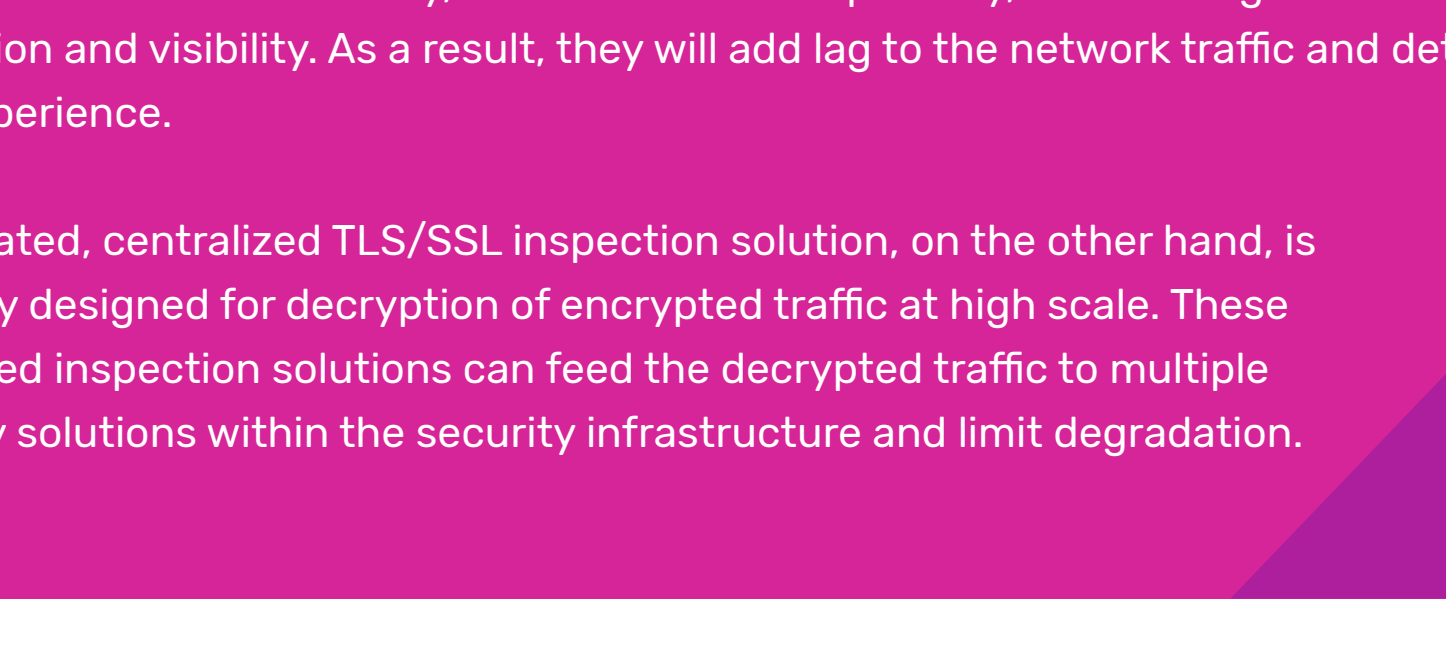


Security solutions with decryption as a secondary feature are not designed for handling these compute-intensive processes. This can subject devices to high levels of performance degradation, which creates performance bottlenecks in the network. Additionally, organizations that rely on more than one security solution, e.g. NGFWs, IPS, DLP, AV solutions etc., must conduct the decryption and re-encryption processes in a distributed way, on each solution separately, in order to gain full traffic inspection and visibility. As a result, they will add lag to the network traffic and deteriorate user experience.

A dedicated, centralized TLS/SSL inspection solution, on the other hand, is primarily designed for decryption of encrypted traffic at high scale. These dedicated inspection solutions can feed the decrypted traffic to multiple security solutions within the security infrastructure and limit degradation.

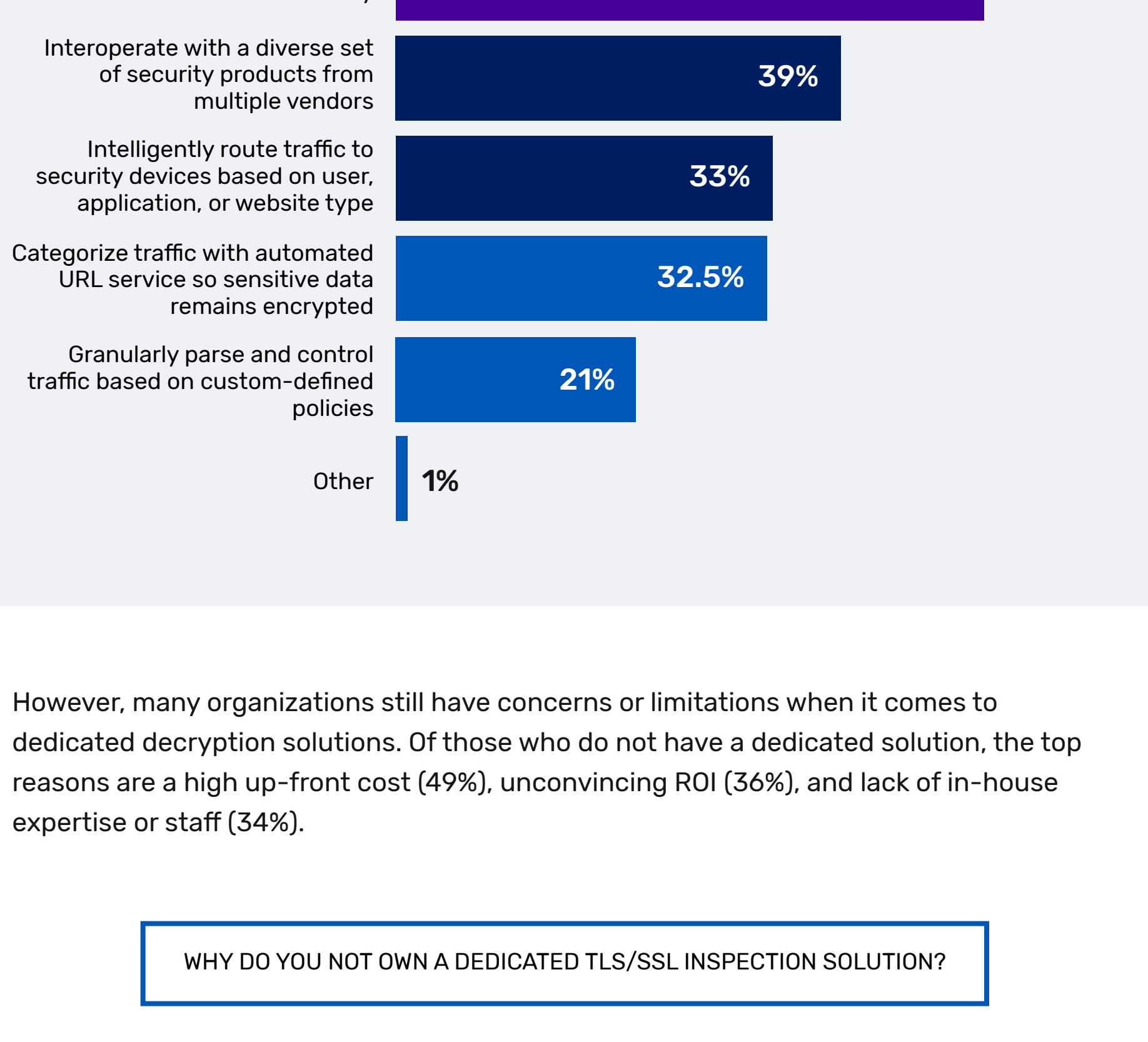
56.5% of tech leaders utilize dedicated TLS/SSL inspection solutions for the decryption of their network's encrypted traffic.

DOES YOUR COMPANY OWN A DEDICATED TLS/SSL INSPECTION SOLUTION WHERE THE PRIMARY FEATURE IS DECRYPTION OF ENCRYPTED TRAFFIC?



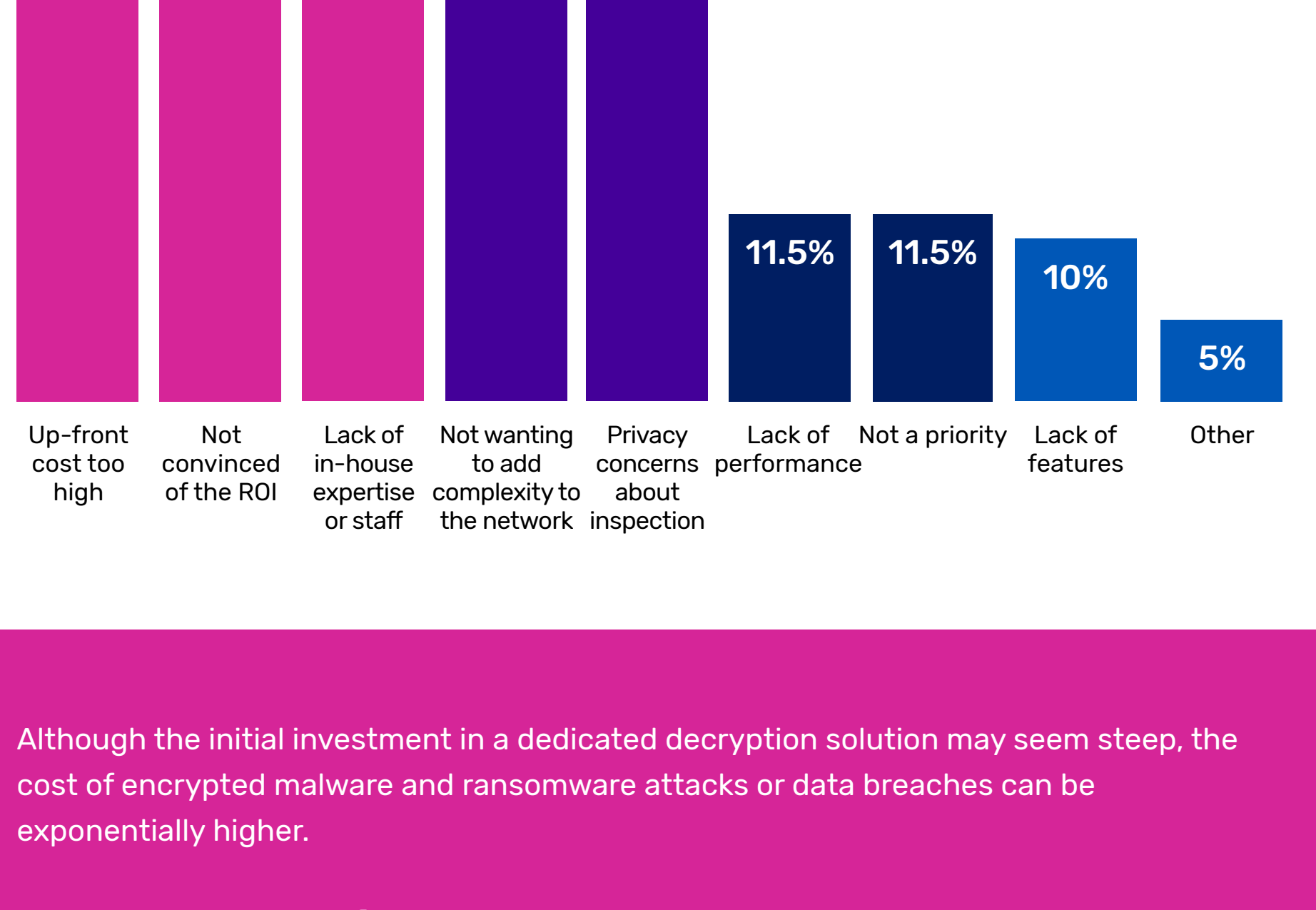
Beyond the ability to decrypt traffic, tech leaders cited the ability to securely manage SSL certificates and keys (63.5%), to satisfy compliance requirements (62%), and to scale to meet current and future SSL performance demands (61%) as the top selection criteria for potential TLS/SSL inspection solutions.

IF YOU WERE TO INVEST IN A TLS/SSL INSPECTION SOLUTION, WHAT WOULD BE YOUR SELECTION CRITERIA OTHER THAN DECRYPTION OF TRAFFIC?



However, many organizations still have concerns or limitations when it comes to dedicated decryption solutions. Of those who do not have a dedicated solution, the top reasons are a high up-front cost (49%), unconvincing ROI (36%), and lack of in-house expertise or staff (34%).

WHY DO YOU NOT OWN A DEDICATED TLS/SSL INSPECTION SOLUTION?



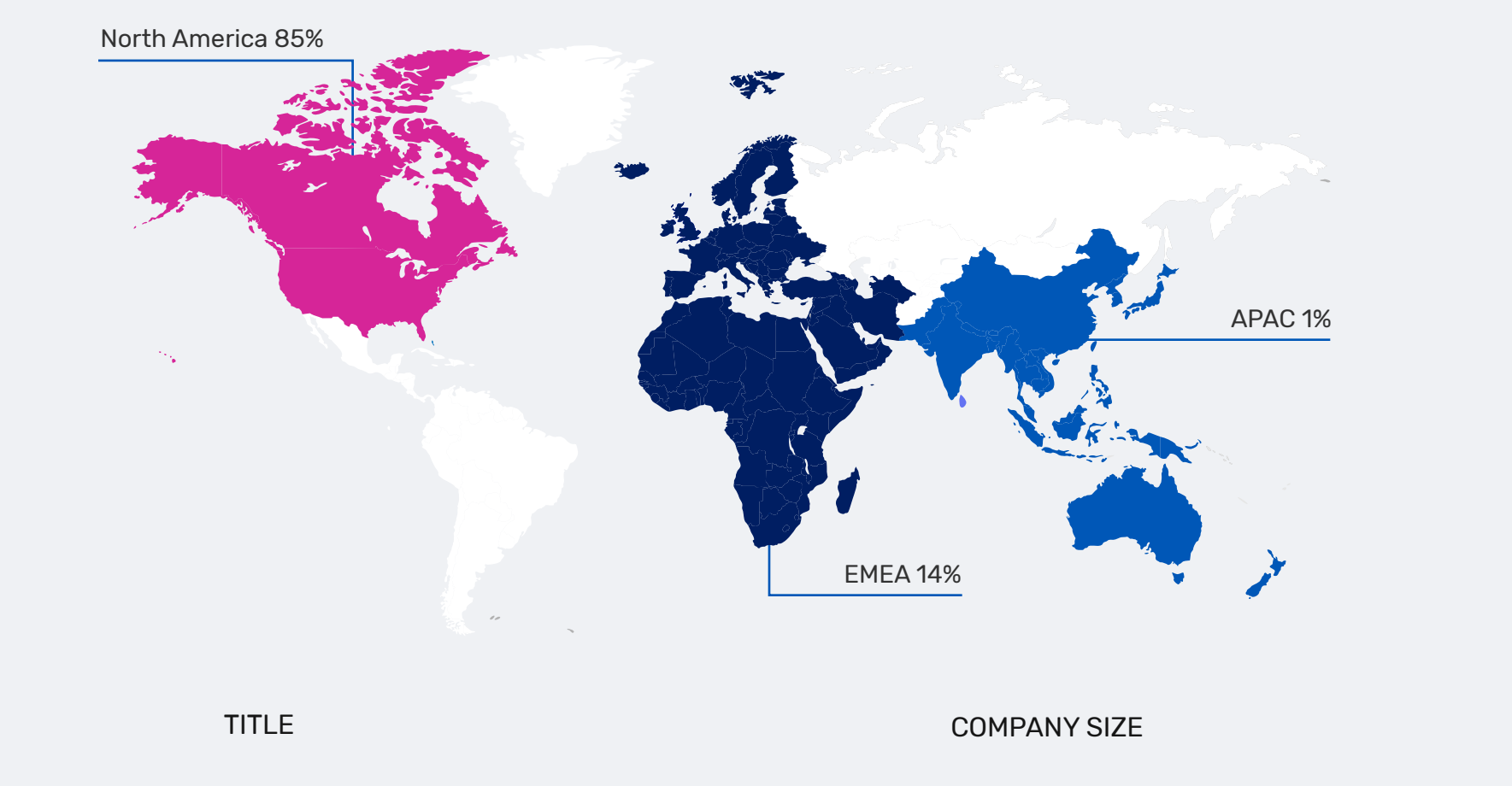
Although the initial investment in a dedicated decryption solution may seem steep, the cost of encrypted malware and ransomware attacks or data breaches can be exponentially higher.

In addition to the direct financial damages, encrypted cyberattacks can cause lost productivity due to deteriorated performance and user experience, brand damage, compliance breaches and the associated penalties, as well as potential lawsuits by disgruntled customers.

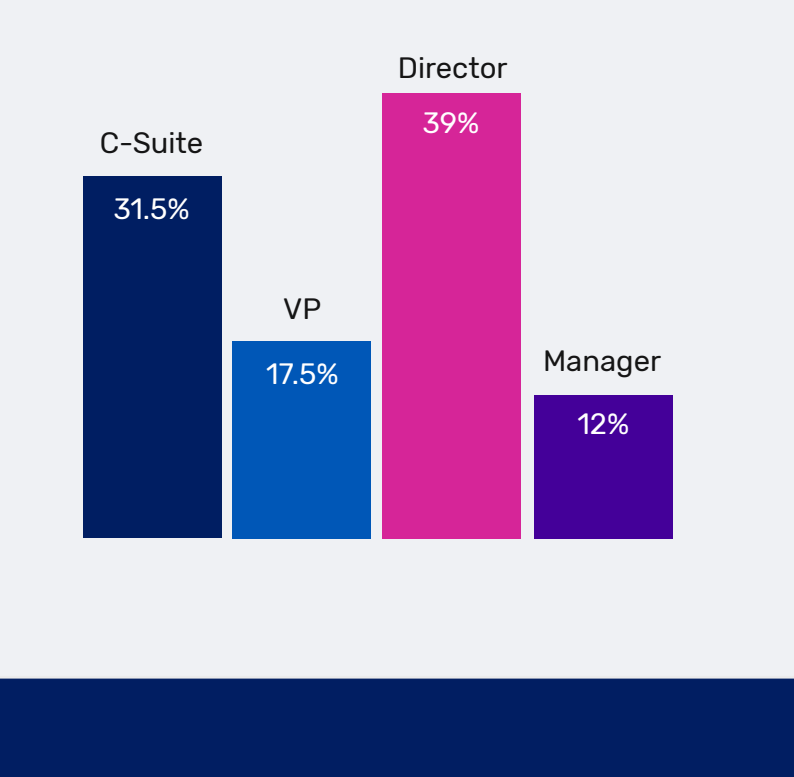
Modern cyberattacks are becoming increasingly sophisticated, easier, and cheaper to launch with each passing day. It is essential that technology leaders have the most effective defensive solutions and strategies in place to stay ahead of these attackers and to protect against the ever evolving cyber threat landscape.

Respondent Breakdown

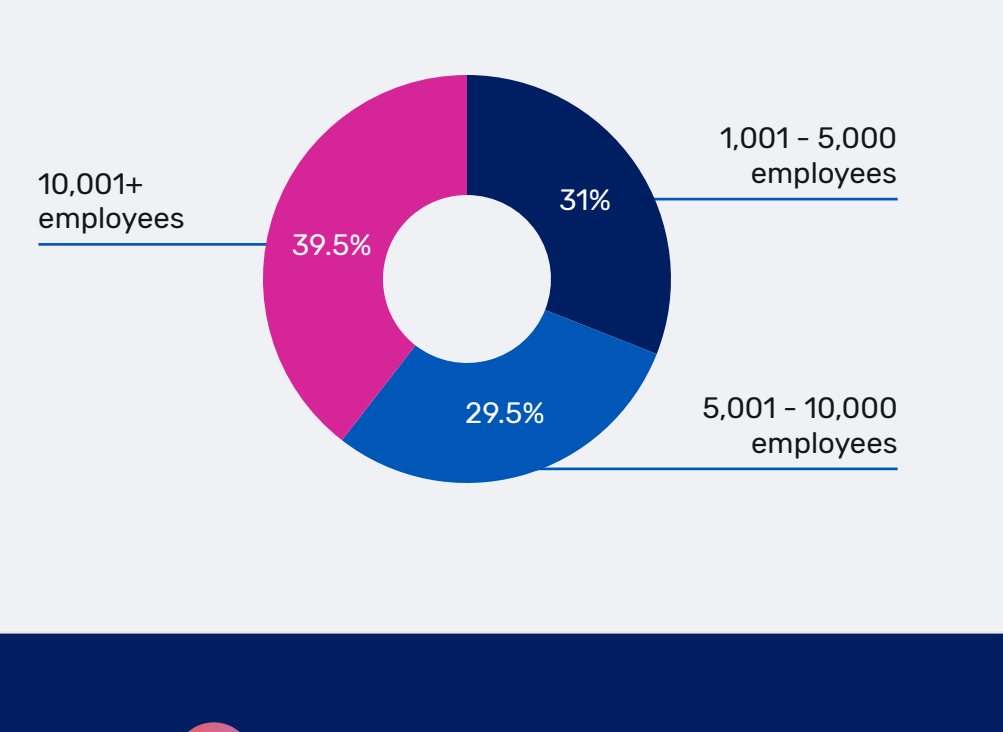
REGION



TITLE



COMPANY SIZE



Insights powered by PULSE