

RESEARCH REPORT

Bringing NetOps and SecOps together to address the menace of encrypted network traffic threats

Introduction

Network security has never been so difficult to manage, as a variety of attackers from amateur trouble-makers and hacktivists to professional cyber-criminals and state-sponsored actors, target web, LAN and WAN traffic. To combat this, security defense teams have turned to encryption as a means of scrambling data and rendering it worthless even if perpetrators intercept data traveling over networks. This minimizes breach impacts, reduces risks, heightens compliance and smooths the path to failover and business continuity.

Today, network encryption is everywhere: at the start of 2019, 87 per cent of web traffic was encrypted, according to the influential venture capitalist Mary Meeker in her most recent [Internet Trends](#) report. That compares to just 53 per cent of encrypted network traffic in 2016.

However, encryption is no panacea and it is complex to manage. It requires data owners to ensure cryptographic compliance and it can make identifying network-borne threats challenging. Today, network encryption is recognized by security experts as a common means of disguising attacks and every sign indicates that the challenge is growing. As a result, network traffic analysis (NTA) tools have evolved to identify suspicious patterns in encrypted traffic – encrypted traffic analysis (ETA) solutions.

But IT departments are already under pressure and managing network encryption adds to their loads. Ideally, they would like to bring together the overlapping worlds of network operations (NetOps) and security operations (SecOps) to accelerate prevent/detect/respond processes. But, too often, these units are islands of insight that talk to each other only on an ‘as needs’ basis.

To better understand the network security and encryption landscape, IDG Connect was commissioned by Flowmon Networks to survey over 100 respondents across the US, Europe and Canada via an online questionnaire. All organizations surveyed had a minimum of 500 employees and most had 1,000 to 4,999 employees. All respondents had IT management roles and 40 per cent held C-suite positions. Our research panel came from across vertical sectors, but more than a quarter came from the technology sector.

The result was an illuminating insight into network encryption, security and the challenges organizations face today.

Page
no.

Contents



Click the home icon to return to this page

-
3. Encryption’s role as a carrier of threats is widely recognized
 4. Confidence in ability to repel attacks is moderate
 5. NetOps and SecOps: Islands or cohorts?
 6. Solutions must let NetOps talk to SecOps
 7. Breached data privacy leads encryption concerns
 8. Traffic decryption is widespread, but it sparks concerns over privacy, performance and people
 9. Is confidence over device monitoring coverage misplaced?
 10. Knowledge of certs is worrying low
 11. Tech to track traffic may be weaker than needed
 - 12. Conclusion and executive summary**
 13. Survey Methodology



Exclusive research by  IDG for Flowmon Networks



20-MINUTE READ

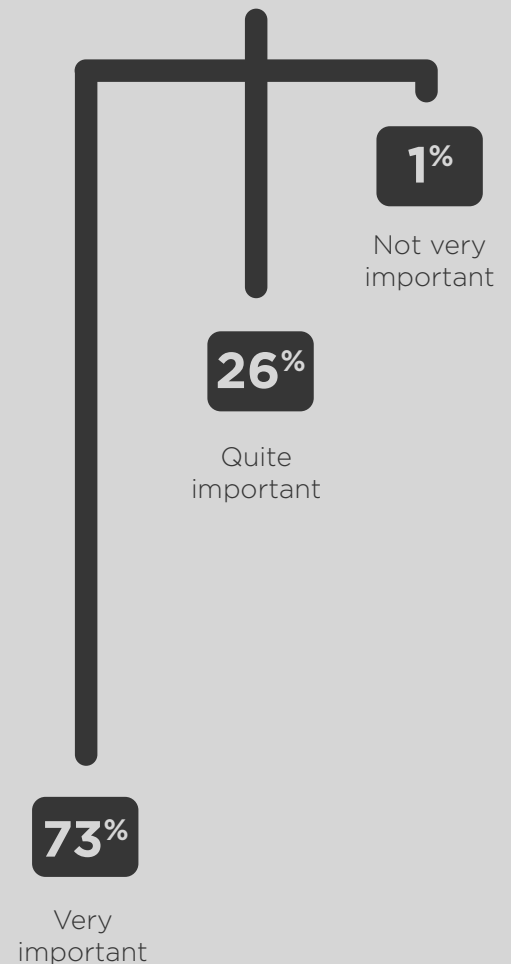
Encryption's role as a carrier of threats is widely recognized

Network encryption has become “part of the furniture” in datacenters and network operations centres. It's widely used and accepted as a tool in the armory of information security and network security professionals. But it can also be a means of carrying security threats.

To test how well known this fact is, we asked our panel how important they felt network encryption was as a potential carrier of threats. Our poll suggested that almost all (99%) of respondents feel that encrypted traffic as a possible source of security threats is either 'quite' or 'very' important: a positive answer suggesting a well-educated audience that is highly aware of the broader threatscape.

So, we can say with confidence that there is wide awareness of encryption as a risk factor, as well as a defense mechanism. And this should come as no great surprise. Throughout IT history, new technologies have been co-opted by malicious actors and scrutinized for potential vulnerabilities. SSL, the most widely used cryptographic defense protocol for internet data communications, is no different. Today, a huge number of companies have been exposed not just to attacks exploiting SSL vulnerabilities but also attacks that employ SSL to mask nefarious attacks over the network and via applications.

How important do you think encrypted network traffic is as a potential carrier of security threats? (Select one only)



Close-up

C-suite respondents are more likely to say this threat is 'very important' (89%).

0100
10101
0010



Confidence in ability to repel attacks is moderate

Having established that encrypted traffic is widely viewed as a potential carrier of threats, how confident did our panel feel about their ability to withstand the challenge? The answer: generally quite positive... perhaps too much so.

Almost six in 10 respondents felt they had very good insights into threats and nearly all the rest felt they had quite good insights. However, two complicating factors may be in play here.

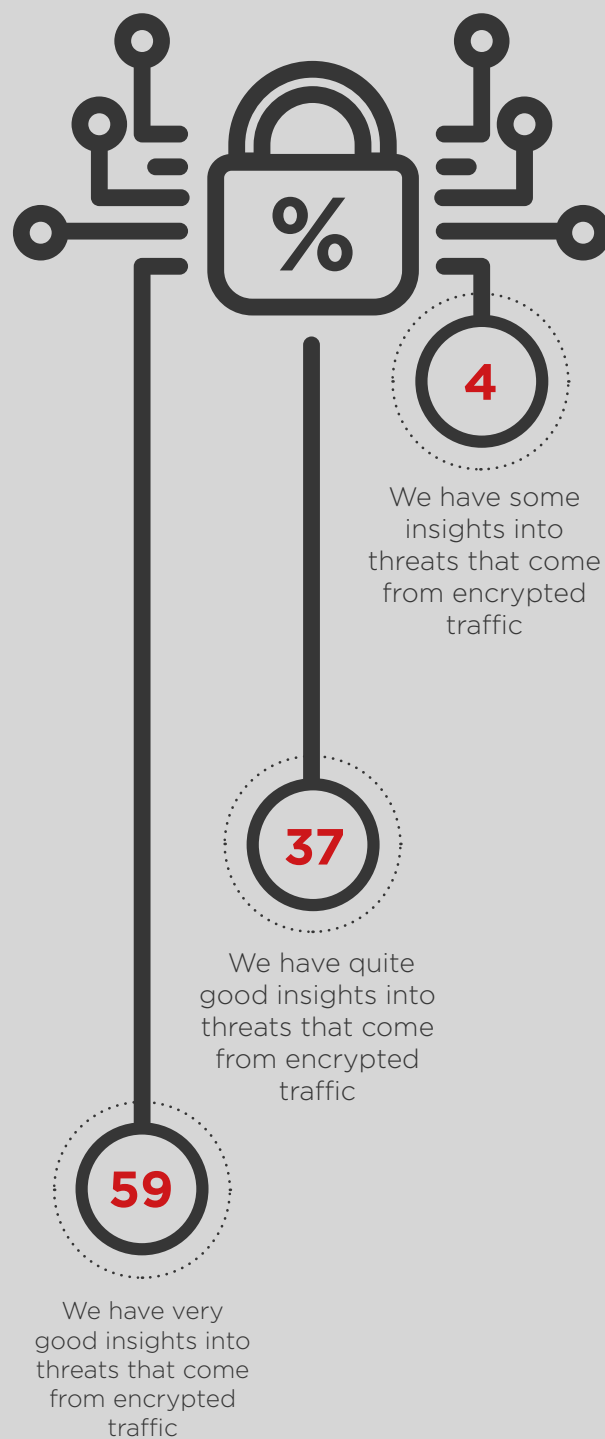
First, our panel might be giving themselves an 'Ivy League' grade, assuming they have better knowledge than is likely to be the case, given the complexities of these environments and an inability to track unknown threats. Many threats come from sources that are undetected by many tools and attackers can lay dormant for months or even years once they have penetrated networks and applications.

Second, insights alone won't be enough to repel attacks: remedial measures will also be needed. So, while some 96% of those polled say they feel quite confident or better, the truth may not be so bright as painted. And note that when we come later in this report to asking about encryption monitoring technologies that are in use, we find that over three-quarters are primarily looking at encrypted traffic on the network perimeter, which is inadequate to protect from insider threats, advanced persistent threats and other, unknown attacks.

Also, as we shall see, only a little over half of respondents (56%) are using network traffic analysis tools capable of intercepting and analysing traffic to sniff out threats and suspicious activity patterns.

Finally, note that, even if there is an element of optimistic confidence in place here, that still leaves over four in 10 (41%) who say they don't feel 'very' confident.

How would you rate your ability to detect threats in encrypted traffic?



Close-up
 Respondents in the Finance/Banking/Accounting/Investment vertical (76%), those working in IT security (77%) and the C-suite audience (70%) are more likely to say they are 'very confident'.

NetOps and SecOps: Islands or cohorts?

An ideal scenario sees NetOps and SecOps teams working hand in hand with deep mutual knowledge of each other's activities and domains. However, this is far from always being the case.

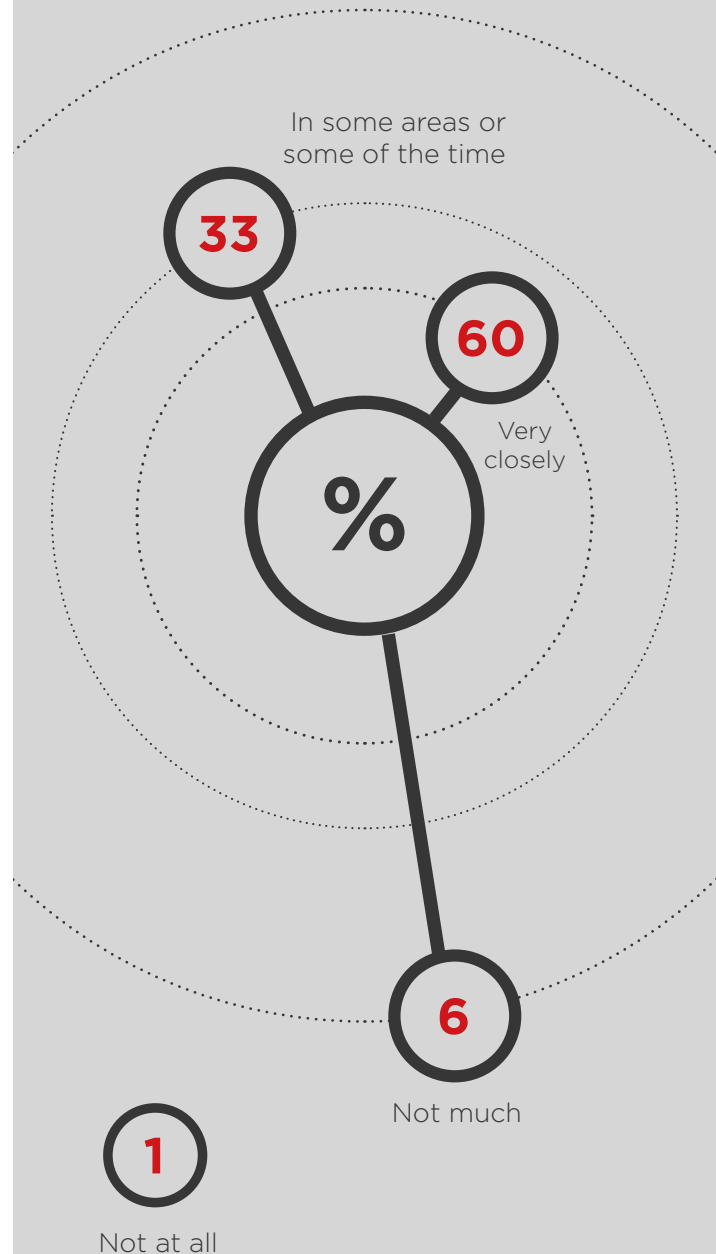


A large majority (93%) of respondents say that network operations and security operations work together at least to some extent. However, again this might hide a more complex reality. NetOps and SecOps are generally forced to cooperate, by circumstances, strategic decisions or otherwise. However, that doesn't mean that this is necessarily always an optimal, formalized or even functional relationship.

Often, these teams will operate effectively as silos, only dovetailing where necessary. Banishing this disconnect and forging links between NetOps and SecOps will be hugely important in securing networks.

How far do your network operations and security operations teams work together to analyze network traffic for security threats?

(Select one only)



Close-up

North Americans (78%), C-level executives (74%), respondents working in Finance/Banking/Accounting/Investment (76%) and in smaller companies with 500-999 staff (68%) were all more likely to answer, 'very closely'.

Solutions must let NetOps talk to SecOps

Given the previous question, we wanted to know what respondents wanted from ETA technology solutions... and the answers we received were highly encouraging.

By a significant distance, the most cited answer was supporting NetOps and SecOps teams in cooperating. This is a welcome verdict because having teams working as a combination is the sign of a healthy and secure ICT department. By pooling respective skills, organizations stand an excellent chance of maintaining slick, safe and compliant operations.

Our panel clearly sees ETA as a way to bring together the two camps to share a single version of the truth. ETA is commonplace but, as referred to earlier, where detection is limited to the perimeter, it leaves the organization vulnerable to many common attack vectors, from 'the enemy within' insiders, advanced persistent threats that lay patiently waiting for months or even years, and attacks of unknown origin that are difficult to parse or have been, at best, only partially recognized or diagnosed.

Other answers were positive too, focusing on speed of operations, rapid threat response and the ability to integrate with other software and services: event logging, ticketing and incident response systems are obvious candidates. As with other technologies, ETA solutions will not be widely adopted and used if they are not scalable, respectful of user privacy, intuitive and if they require lots of manual work to make them work efficiently.

Streamlined deployment, user enablement, having predefined dashboards and the ability to report visually will all help to accelerate response times.

Close-up

C-suite respondents were particularly keen on the notion that ETA can bring NetOps and SecOps in tandem (59%) but also noted flexibility of deployment and ease of deployment (41% each). The UK noted scalability (48%) and ease of deployment (41%) as important. Smaller companies saw performance as key (53%).

What do you see as key attributes of an Encrypted Traffic Analysis solution?

(Select as many as apply.)



49%

Allows SecOps and NetOps to work alongside each other



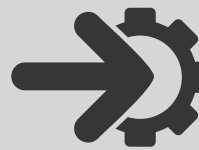
43%

1. Performance
2. Enables rapid response to threats



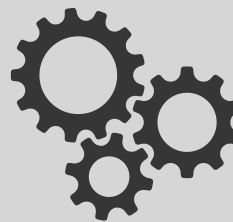
39%

Strengthens security by identifying malicious traffic



36%

Integrates with other software



33%

1. Easy to deploy,
2. Can be installed on-premises, in a remote location, on private or public clouds
3. Reporting and visualization capability



29%

Scalability



19%

No impact on network latency



Breached data privacy leads encryption concerns

When we asked about concerns over encrypted traffic, we received a long and varied list of answers in response. Almost four in five (79%) respondents nominated three or more live issues and all possible responses received significant scores.


However, by far the largest concern, cited by seven in 10 respondents and by more than three in 10 as the biggest single concern, was data privacy. Today, exposure of data is a huge concern and it can lead to punitive fines as well as reputational damage. Rules such as GDPR have only accentuated an already powerful trend and penalties have made data governance a board-level concern.


Our results teach other important lessons. Specifically, while managing encrypted traffic is a critical form of defense for organizations, buyers are very keen that this protection does not come at the cost of data loss, governance, high costs, straggling performance or complexity of deployment and integration, as noted in the previous question.

Close-up

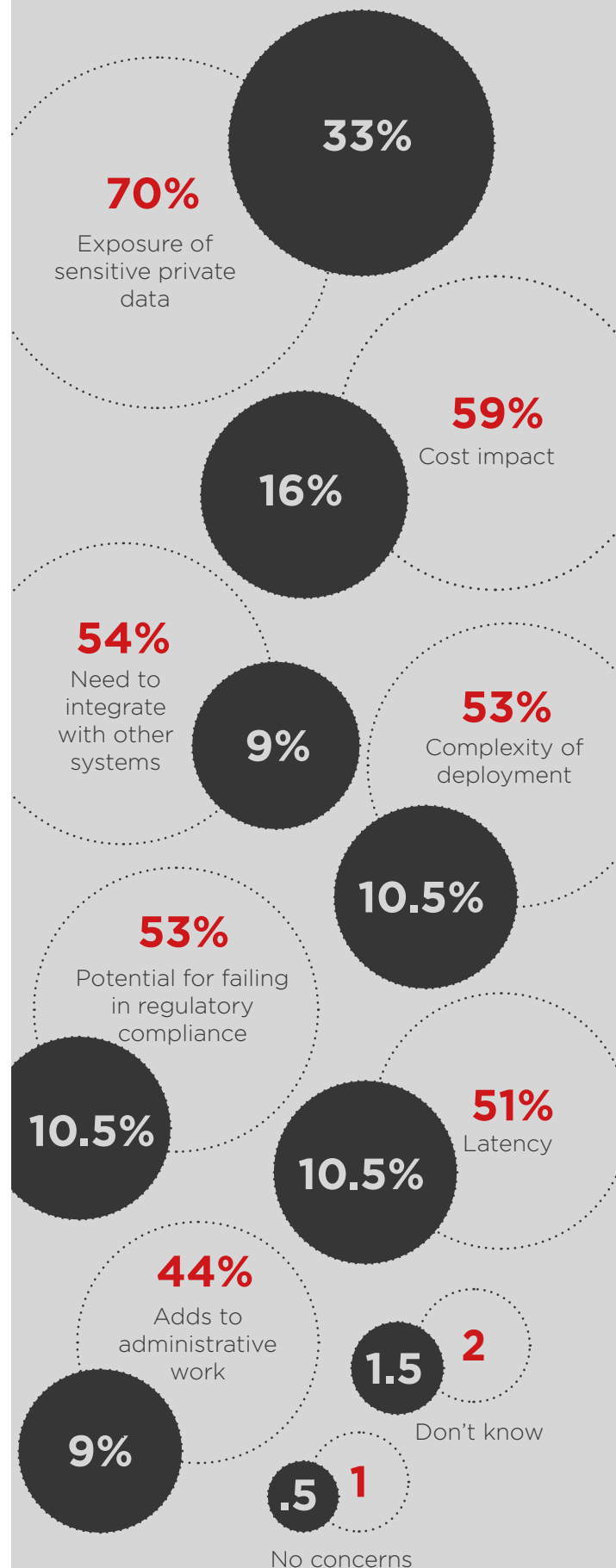
The UK had the highest percentage of respondents saying 'potential for failing in regulatory compliance' was a concern (66%). In Germany, the second most common concern was adding to administrative workloads (66%). For smaller companies (500-999 staff), cost impact was the number-one concern (71%).

KEY

Concern 

Biggest Concern 

What concerns do you have over encrypted traffic? (Select as many as apply.) **And which of these is your biggest concern over encrypted traffic?** (Select one.)



Traffic decryption is widespread, but it sparks concerns over privacy, performance and people

While almost every company we surveyed either has deployed network traffic decryption or is considering it, obstacles remain in the way.

Over a third of the audience fears breaching data privacy and almost a third have concerns over creating performance degradation. This backs up a commonly held feeling about decryption: while it is undoubtedly an important exercise, when things go wrong, they can go very wrong.

Buyers should look out for value but also test for effects on network performance. And of course, people with the skills to manage the decryption systems need to be available and appropriate budgets in place.

Close-up

In the UK, 62% of respondents have already implemented network decryption via the SSL proxy. Germans and Austrians have the highest level of those considering implementation (56%).

Privacy and bottlenecks are key concerns especially for North Americans (47% each). The smallest companies we surveyed also had higher than average privacy concerns. Skills availability was an issue for German and Austrian respondents (25%) and budget is a key issue for the people we polled in the US (21%).

Have you considered decrypting network traffic using SSL proxy? (Select the statement that most closely fits your situation.)*



We have already implemented it



We are considering implementing it

If you have not considered decrypting network traffic as an option, could you explain why? (Choose one statement that most closely fits your situation.)**



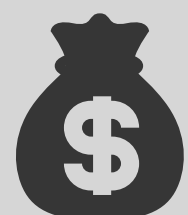
36%
Concern over data privacy

29%
Fear of performance bottlenecks



18%
Lack of available skills

11%
Not enough budget



* 1% answered 'Don't know'

** 6% answered 'None of the above'



Is confidence over device monitoring coverage misplaced?

Most of the audience has some belief, at least, that they have awareness of every device communicating over their networks, but more than half say they are not highly confident.



Again, even this level may indicate false confidence, especially given all the new devices that now have intelligence and communications embedded. As we add BYOD devices, security, cameras, smart building controls and more, it becomes harder to track and understand device behavior across network, especially where those devices haven't been formally sanctioned.

As more devices become IP-enabled this is likely to be a more onerous chore for network owners and it is vital that they use new tools that will help them identify what is attached to their networks to mitigate threats.

How confident are you that you have awareness of every device communicating on your network? (select one only)



Close-up

64% of US respondents are highly confident as are 52% of the technology vertical.



Knowledge of certs is worrying low

When asked about their knowledge of encryption certificates, 82% selected two or more of the possible answers. However, the responses were worryingly low across the board with large numbers lacking knowledge of certs for basic security and governance activities.

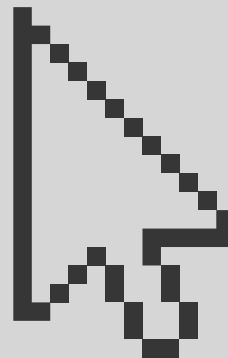
This absence may point towards complexity of managing certificates and some of the challenges indicated in the early answers about managing encryption in accessing people with the necessary skills and budgets to ensure the secure running of operations.



Close-up

North America scored highly for knowledge of malware detection encryption certificates (83%) while Germany excelled in cryptographic compliance (79%).

Does your company have the necessary knowledge of encryption certificates in the following areas? (Select as many as apply.)*



Monitoring user web access

72%



Ensuring cryptographic compliance

69%



Malware detection

66%

* 2% answered 'Other' and 1% answered 'Don't know'



Tech to track traffic may be weaker than needed

Our audience is using a variety of measures to watch over encrypted traffic with over three-quarters citing SSL on-firewall inspection and most having a dedicated SSL proxy and NTA tool of some kind.

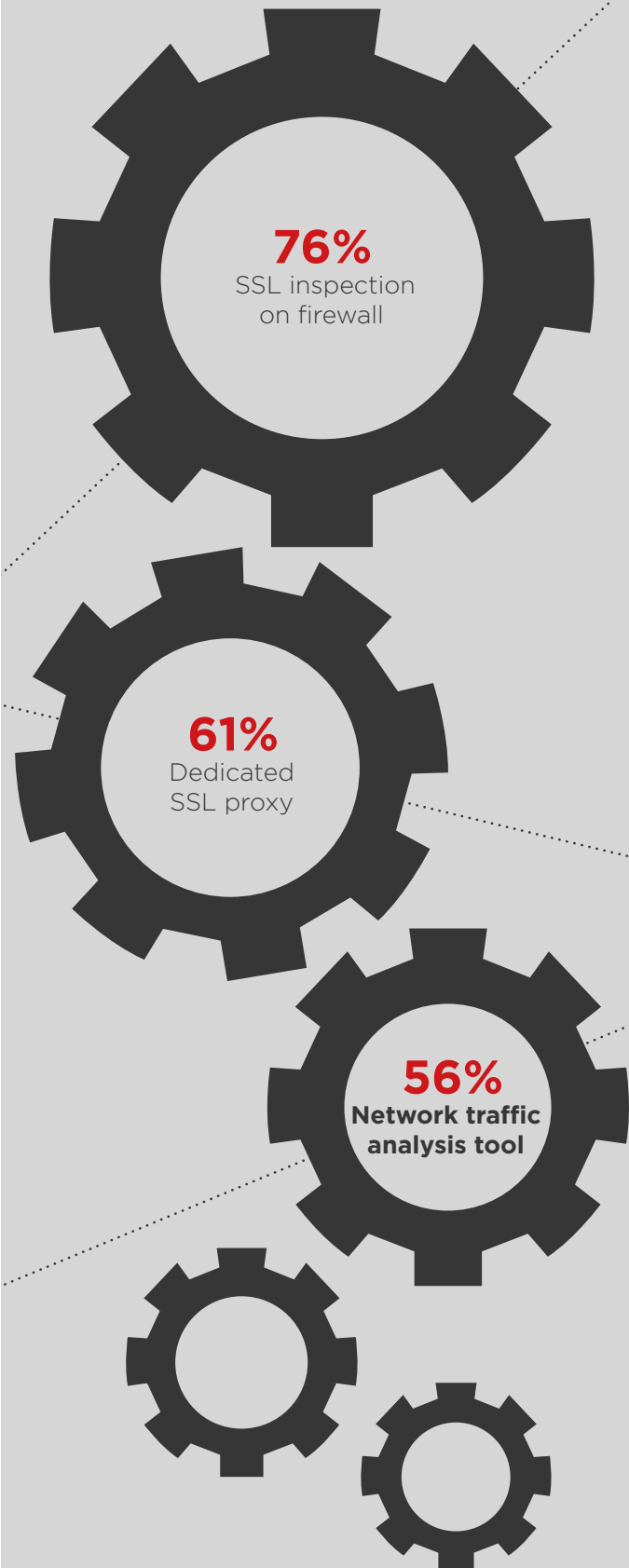


It's important to note here that ETA and SSL decryption aren't mutually exclusive. In fact, best-practice security requires both for different, complementary reasons. Decryption is powerful but expensive and resource-intensive, while ETA is lightweight and covers most cases.

It therefore makes tactical sense to use ETA to monitor holistically the network and reserve the use of decryption for critical assets only.

Our audience is only partially abiding by this rule. Two-thirds of those asked use SSL inspection, but only a third have both SSL inspection and ETA at the same time.

What technologies do you currently use to monitor encrypted traffic? (Select as many as apply.)



Conclusion & executive summary

It has been estimated that encrypted traffic provides the cover for almost half of today's cyber-attacks. The concerted, blended, always-morphing and never-ending character of network-borne attacks masked by encryption demands a response in kind.

Network defenders need to team up and harness all the knowledge and tools at their disposal to confront malicious actors. Cooperation between NetOps and SecOps to pool defense vectors needs to be a default setting for enterprises.

Only by bringing together these front-line forces can organizations hope to defend holistically their information assets because only by cooperating can they rapidly recognize and repel a spectrum of threats.

Encrypted Traffic Analysis (ETA) tools are an essential companion to SSL decryption to protect organizations from today's protean challenges to data integrity.

If you wish to learn more about ETA, visit www.flowmon.com, or if you want to see for yourself how an NTA solution tackles encrypted traffic, try a guided demo at www.flowmon.com/en/try-online-demo.

This research has unearthed key data concerning the encrypted traffic environment.

- There is near-universal consensus (99%) that encrypted network traffic is an important source of security risks
- Four in 10 (41%) respondents feel that they don't have a very good understanding of how to repel such attacks
- A similar number (40%) say that network operations and security operations staff don't work very closely together
- The number-one attribute of ETA tools is that they enable NetOps and SecOps teams to work together
- The biggest potential negative impact of encrypted traffic is exposure of sensitive personal data (70%)
- Over half of respondents (52%) have traffic decryption tools
- Over a third of the audience that have not deployed decryption say the main reason is user privacy (36%)
- Over half (58%) are not highly confident about their knowledge of network-attached device activity



Survey methodology

IDG Connect conducted a survey on behalf of Flowmon Networks to study the network security landscape and network encryption across the US, Canada and Europe, with particular reference to encrypted traffic analysis (ETA).

In late 2019, we surveyed over 100 respondents via an online questionnaire. The audience came from across sectors but 27% worked in the technology vertical. All respondents had IT management titles with 40% in C-suite roles. All came from companies with at least 500 staff, with the highest number (39%) coming from companies with 1,000 to 4,999 staff.

Almost a third (32%) of the audience was from the US and Canada and the same percentage came from Germany and Austria. The UK provided 25% of the panel and Benelux (11%) completed the set.



About Flowmon Networks In a world where technology exists for the benefit of people, secure and healthy digital environments are essential. That's why Flowmon develops an actionable network intelligence solution that enables businesses to ensure their services are running well and securely, and their workforce is productive. Driven by a passion for technology, we have earned the trust of customers who rely on our solution to maintain control over their networks, keep order and overcome uncertainty.



About IDG Connect IDG Connect is the demand generation division of International Data Group (IDG), the world's largest technology media company. Established in 2006, it utilizes access to 44 million business decision makers' details to unite technology marketers with relevant targets from any country in the world. Committed to engaging a disparate global IT audience with truly localized messaging, IDG Connect also publishes market specific thought leadership papers on behalf of its clients, and produces research for B2B marketers worldwide. For more information visit: www.idgconnect.com

