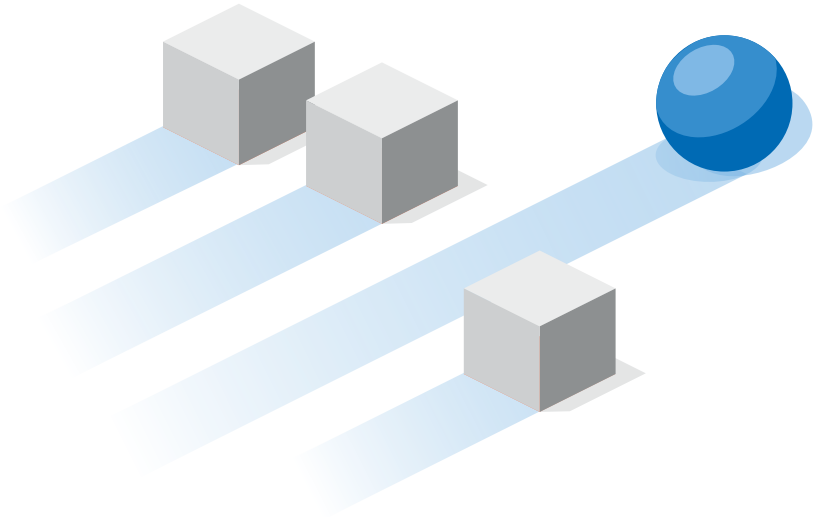
SOPHOS



The Achilles Heel of Next-Gen Firewalls

Results of a global study of 3,100 IT managers in 12 countries

Network security is the bedrock of every organization's cyber defenses, the foundation on which other protection services such as endpoint, server, mobile and encryption are layered. It's the trusty work horse that plays a pivotal role in keeping organizations moving.

To better understand the realities of network security today, Sophos commissioned leading research specialist Vanson Bourne to conduct an independent survey of 3,100 IT managers spanning 12 countries and six continents.

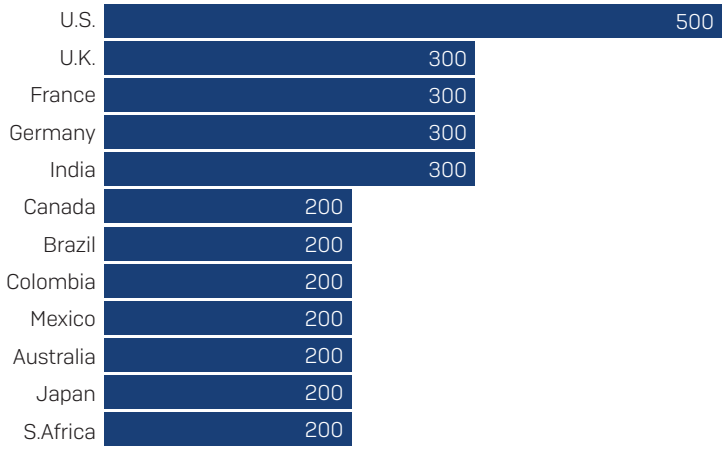
The results reveal the day-to-day experiences of IT teams across the globe when it comes to network threats and next-gen firewalls. The survey sheds new light onto the practical reality of today's network security and the challenges IT teams face. It also reveals the Achilles heel of next-gen firewalls: the struggle to balance performance, privacy, and protection.

A Sophos Whitepaper January 2020

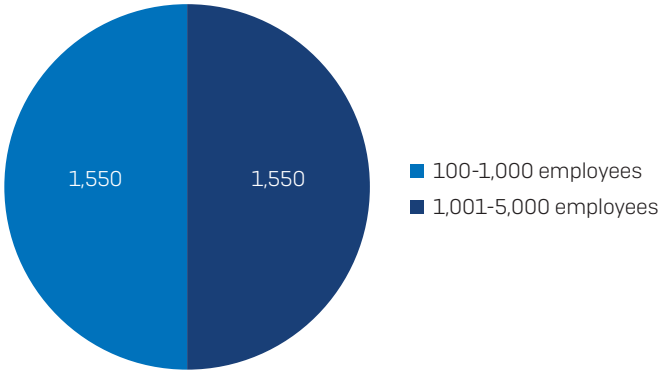
The survey

U.K.-based research house Vanson Bourne interviewed 3,100 IT decision makers between December 2018 and January 2019. To provide a representative size split within each country, respondents were divided equally between 100- 1,000 user organizations and 1,001-5,000 user organizations.

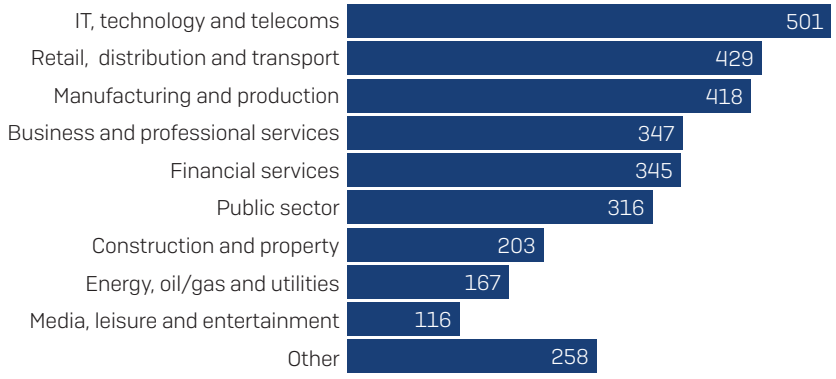
Number of respondents per country



Split of respondents by organization size



Split of respondents by industry



Expect to find a threat on your network

The first takeaway from the survey is that organizations should expect to be hit by a cyberthreat. Over two-thirds (68%) of respondents fell victim to a cyberattack in the last year.

This propensity to fall victim to a threat is not the result of a lack of protection: 91% of affected organizations were running up-to-date cybersecurity protection at the time of the attack. However, good intentions and good practices are clearly not enough: there are still holes in organizations' defenses that enable threats to get through.

The survey also highlighted the wide range of tactics and techniques used by cybercriminals to disseminate their attacks. Data from IT teams that were aware of how the threat entered their organization reveals that:

- 33% entered via email
- 30% entered via a malicious or compromised website
- 23% via software they were using
- 14% via a USB stick/external device

In 20% of cases, however, the IT team was unaware of the threat's entry point. This lack of visibility highlights a significant challenge for IT teams when it comes to securing their organization: if you don't know how the threat got in it's difficult to prevent future attacks.

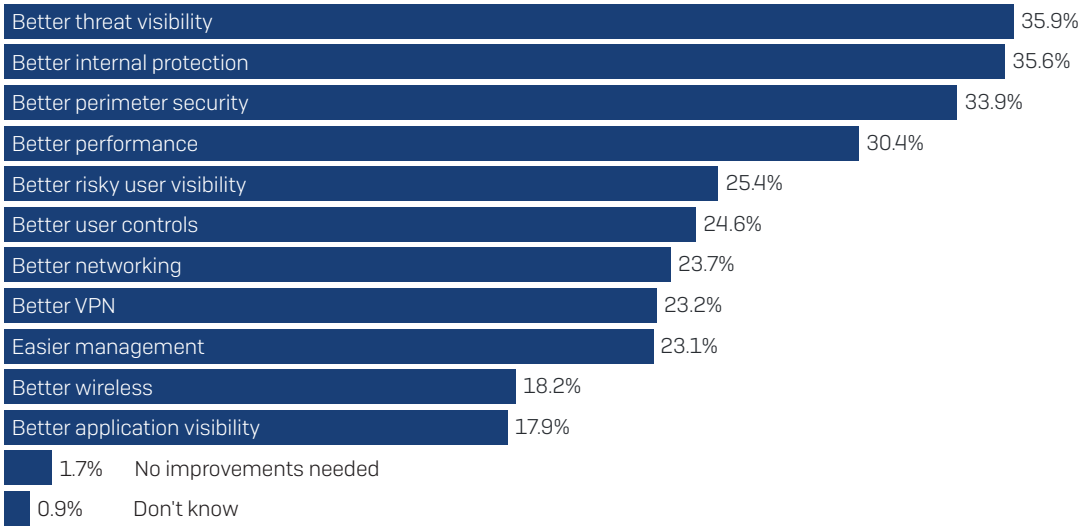
The longer the threat remains in the network, the greater the risk to the organization. The survey revealed that, on average, it took organizations 13 hours to detect threats in their network. Clearly in this time hackers have the opportunity to deliver myriad payloads.

At the same time, 17% of IT managers don't know how long the threat was in their environment before they found it, further demonstrating the visibility issues IT teams face when it comes to network security.

Firewall enhancement wish list

Better threat visibility topped the global list of improvements the survey respondents want from their firewall, with 36% including it in their top three desired enhancements. The fact that visibility outranked (just!) better protection to the top spot illustrates just how significant an issue lack of insight is for IT teams.

The biggest improvements respondents would like to see in their network firewall (combination of responses ranked first, second and third)



The need for better threat visibility was strongest in Australia and Canada, where 41% of respondents included it in their top three improvements, closely followed by those in the U.S. where 40% gave it a podium place. Respondents from Japan were the only ones to buck the trend with just 21% including better threat visibility in their firewall enhancement wish list.

Given the prevalence of network threats, it's not surprising that better perimeter security was also high on the respondents' wish list, with 34% including it in their top three desired enhancements.

However, security wasn't the only area where respondents wanted to see improvements in their firewall. Three in ten listed better performance as one of the most important improvements they need from their firewalls.

Overall, a clear picture emerged: it's no longer a question of better performance or better protection. Rather, today's IT teams require both performance and protection.

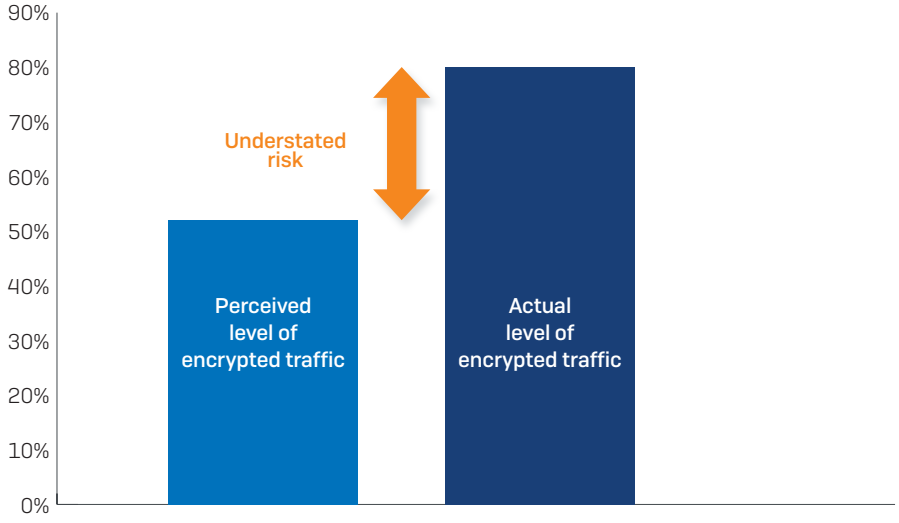
The understated risk: encrypted traffic

Encryption keeps network traffic private, but it doesn't keep it secure. In fact, encrypted traffic is a huge security risk because it renders firewalls blind to what is flowing through the network, preventing them from identifying and blocking malicious content. It's like airline passengers covering themselves in a full-length blanket and remaining anonymous when passing through security screening.

Hackers are actively exploiting encryption to enable their attacks to enter undetected. Illustrating the scale of the issue, SophosLabs research revealed that, in the first eight months of 2019, 25% of URLs called by malware were using encryption.

The level of encrypted network traffic is rising rapidly. Data from the Google Transparency Report indicates that over 80% of web sessions are now encrypted across all platforms, up from 60% just two years ago. However, survey respondents appear to have a different impression: on average, they feel that only 52% of their network traffic is encrypted. Responses were consistent across all countries surveyed, with everyone falling between Japan (46% encrypted) and Germany (57% encrypted).

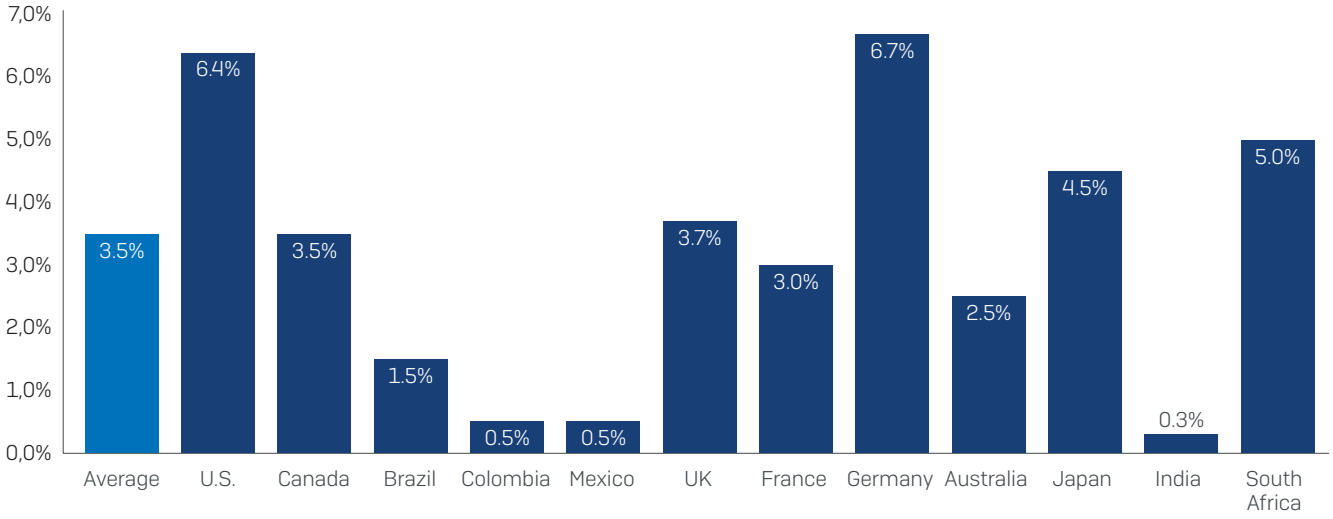
The discrepancy between perceived and actual levels of encryption together with the widespread use of encryption in cyberattacks suggests that encrypted traffic is an understated security risk. IT teams have been caught unaware by the rapid increase in levels of traffic encryption. Furthermore, based on current trends, the percentage of traffic that is encrypted will increase further in the near future.



The Achilles heel of network security

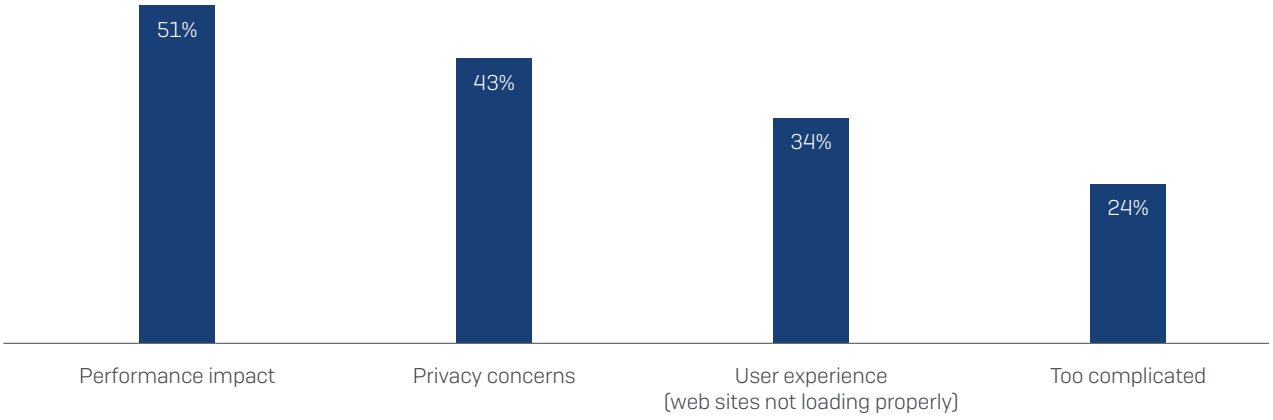
While 82% of survey respondents agreed that TLS inspection is necessary, only 3.5% of organizations are decrypting their traffic to properly inspect it. Germany and the U.S. top the chart with over 6% of respondents decrypting all their traffic; conversely, India, Colombia, and Mexico have the lowest rates of decryption.

Percentage of organizations that decrypt all their network traffic to properly inspect it



The survey revealed that organizations are not decrypting their network traffic for a number of reasons: concerns about firewall performance; a lack of proper policy controls; poor user experience; and complexity.

What stops your organization from decrypting all your network traffic to properly inspect it? (select all that apply)

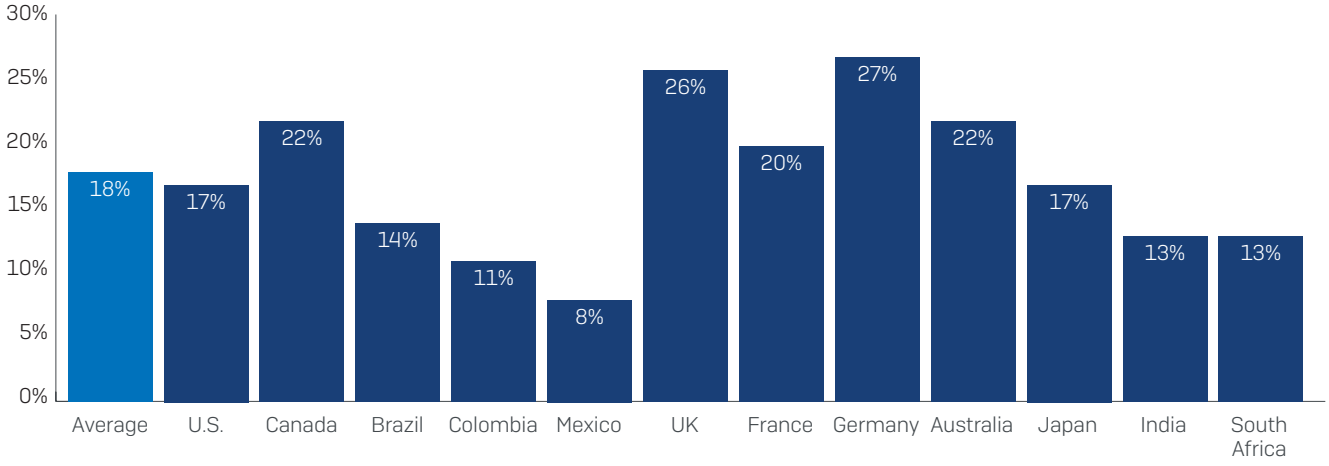


The reality is that most organizations need to carefully balance performance, privacy, and security. However, they lack the tools needed to do so effectively and efficiently. As a result, they are choosing to allow encrypted traffic to pass unchecked, putting themselves at risk from hidden network threats.

This inability to balance performance, privacy, and protection is the Achilles heel, the hidden weakness, of many next-gen firewall and UTM solutions.

At the same time, a significant minority of survey respondents were unaware of the need to decrypt network traffic. In both Germany and the U.K., over a quarter of respondents said it was not necessary to decrypt all network traffic; conversely, in Mexico just 8% shared this view.

Percentage of survey resondents who think it's not necessary to decrypt all network traffic



This indicates that the security industry still has a job to do when it comes to educating on the risks associated with encrypted network traffic.

Firewall capabilities to minimize the risk from encrypted traffic

As we approach 100% network traffic encryption, Sophos recommends that you look for the following five capabilities in your next firewall:

1. **The latest TLS 1.3 and cipher suite support.** While adoption of TLS 1.3 is still in the early days, it would be unwise to buy a firewall without TLS 1.3 support.
2. **A streaming engine solution** that enables inspection of all TLS traffic across all ports/protocols and is faster using fewer connections than a traditional web proxy-based solution.
3. **Robust certificate validation** able to handle invalid, self-signed, revoked, or untrusted certificates to avoid potential malicious Man-in-the-Middle (MITM) attacks.
4. **Powerful and flexible policy tools** that provide granular control over what to decrypt and inspect, enabling you to build the right balance of privacy, protection, and performance for your organization.
5. **High performance**, with sufficient connection handling, efficient decryption, hardware acceleration, and overall power to handle your encrypted traffic volumes efficiently.

Introducing Sophos XG Firewall: Designed for the modern encrypted internet

The Xstream Architecture in XG Firewall offers a ground-up solution to eliminating the network traffic blind spot without impacting performance. It delivers:

- High performance – a lightweight streaming engine with high connection capacity
- Unmatched visibility – into your encrypted traffic flows and any errors
- Top security – supporting TLS 1.3 and all modern cipher suites with robust certificate validation
- Inspection of all traffic – being application and port agnostic
- A great user experience – with extensive interoperability to avoid breaking the internet
- Powerful policy tools – offering the perfect balance of performance, privacy, and protection

Conclusion

Current trends indicate that, the by the end of 2020, over 90% of network traffic will be encrypted. At the same time, hackers will continue to exploit encryption in their cyberattacks. To minimize the security risk from encrypted network traffic, organizations should decrypt all their network traffic as standard. This will help deliver the improved threat visibility and network protection that IT teams need. At the same time, firewall performance remains a key requirement. When choosing your next firewall look for a solution that can balance your performance, protection and privacy needs.

Learn more and start an instant online demo at www.sophos.com/xgfirewall

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

2019-12-12 WPNA (NP)

SOPHOS