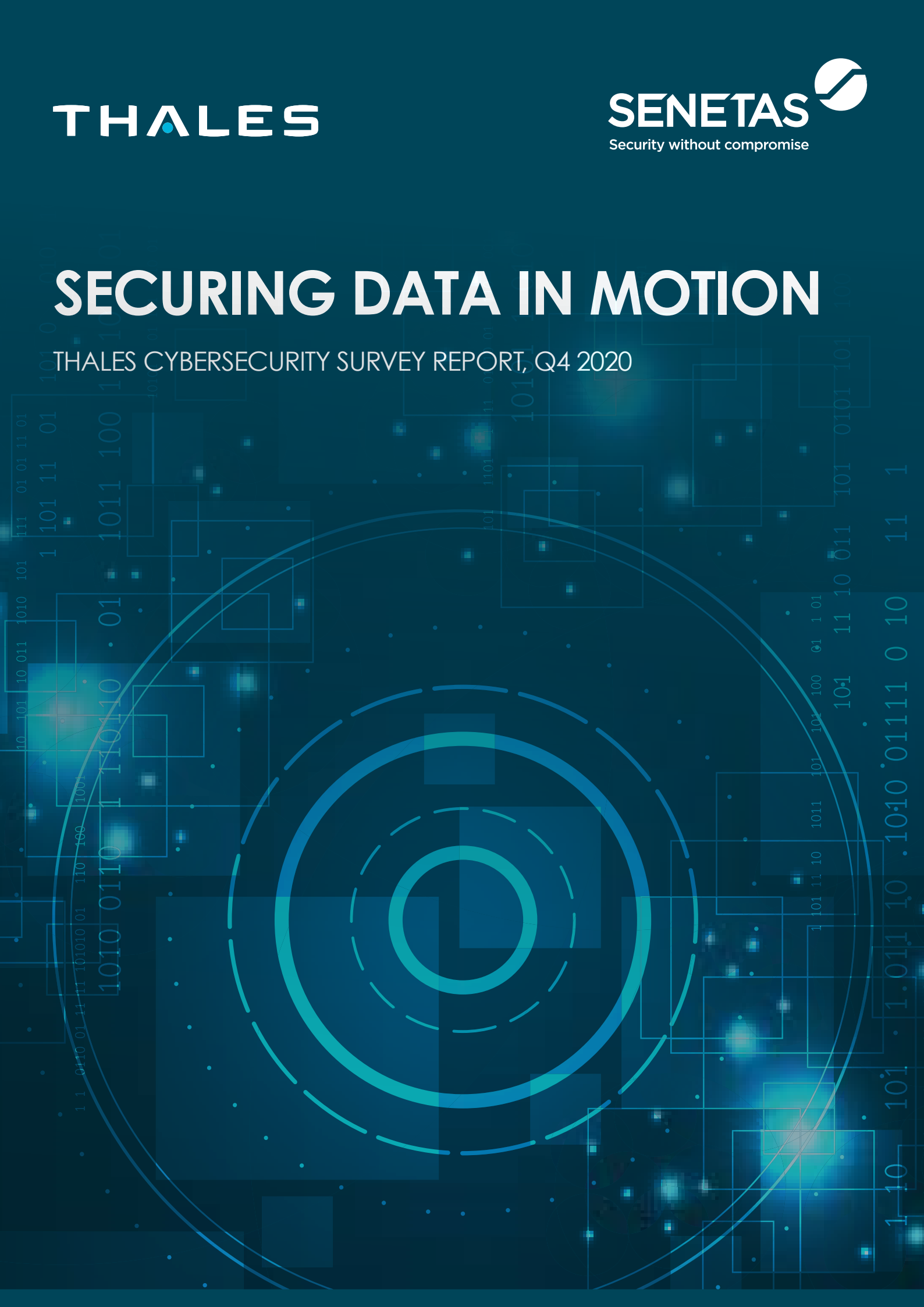
THALES

SENETAS
Security without compromise

SECURING DATA IN MOTION

THALES CYBERSECURITY SURVEY REPORT, Q4 2020



INTRODUCTION

Continued adoption of cloud services, remote working, 5G and IoT applications means more data is in motion than ever before. The result is unprecedented demand for (and dependency upon) high-speed wide area networks.

IDC predicts that organizations will be transferring 57% of their data from the edge to the core by 2022, up from 36% a year ago, "meaning enterprises will need to manage a lot more data in motion."

This exponential growth in data represents potentially rich pickings for hackers, cybercriminals and state-sponsored actors. Cyberattacks on network data are becoming increasingly persistent and sophisticated, threatening loss of IP, citizen privacy, data sovereignty and a wide range of sensitive or confidential data.

This report reveals that just 9% of respondents feel their organisations have effective cybersecurity strategies. Over two thirds (69%) mistakenly believe firewalls protect/encrypt network data in motion. Finally, whilst 85% recognise the efficacy of dedicated network security solutions, just 13% use them.

Content

EXECUTIVE SUMMARY

This survey was conducted among representatives from hundreds of global enterprises and data network solution providers. All respondents are involved in the purchase or recommendation of information security solutions.

The findings point to a need for many organizations to make network data security a higher priority, with just a small minority (less than one in ten) believing they have a proactive strategy in place that can effectively meet the volving threat landscape.

Key Findings:

- Only 9% of enterprises believe they have proactive cybersecurity strategies in place that address evolving threats.
- 58% of organizations say they encrypt their data in motion.
- 44% of respondents mistakenly believe private networks are inherently secure.
- 54% of enterprises feel confident that their network data security solution positions their organization well against cyber threats.
- 70% of enterprises rely upon network operations staff to regularly implement time-consuming and disruptive software patches to keep security solutions up to date.
- 69% of respondents rely upon firewalls or IPsec for encrypting network data in motion, rather than using purpose-built network data encryption security solutions.
- 61% of respondents say their organization has yet to develop a strategy for quantum computing-related security issues.

There are positive signs that organizations are becoming more aware of the need to protect data in motion with high-assurance solutions*. For example, 85% believe the separation of duties provided by dedicated security devices is important for maximum data protection.

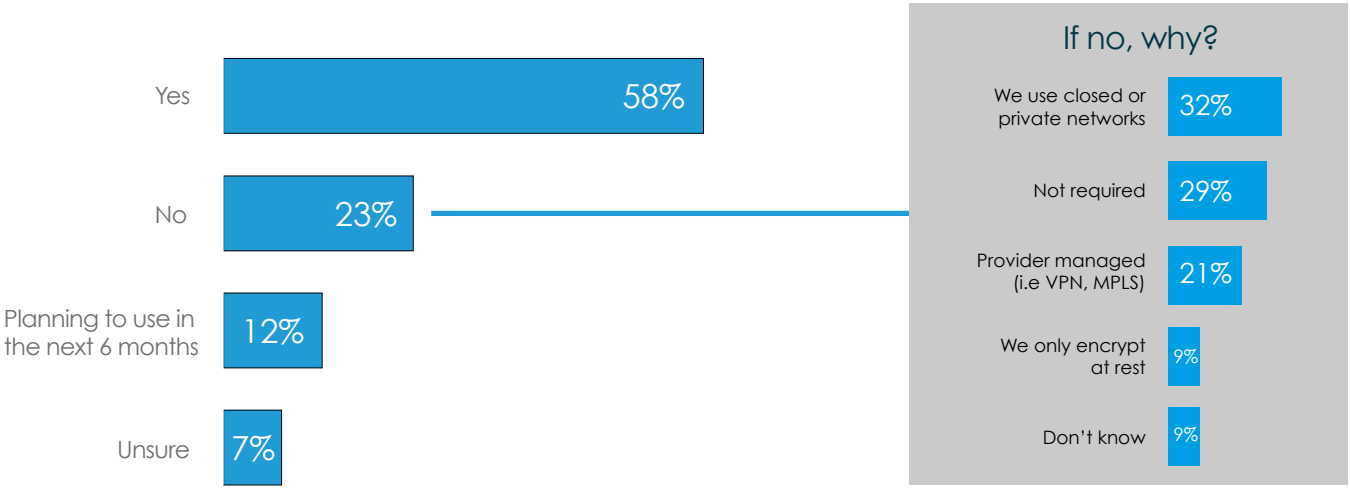
Significantly, 86% also believe that best-practice encryption key management plays a vital role in encryption security.

The report's findings provide insight into the challenges organizations and their service providers face when securing data in motion. It also offers practical suggestions on how to improve your security stance by providing long-term data protection without impacting on network performance or adding to management overhead.

*High-assurance solutions feature four key components: separation of duties, standards-based encryption algorithms, best-practice key management and authenticated, end-to-end encryption.

RESULTS & IMPLICATIONS

1. Do you encrypt data in motion across your organization's network infrastructure?



Analysis

42% of respondents either don't currently encrypt data in motion or don't know if they do. When asked why they do not encrypt data in motion, 32% say it's because they rely upon private networks and a further 29% say it's not required.

Implications

The findings reveal some potentially serious misconceptions about the inherent security of private or public networks. Data in motion across either infrastructure is equally susceptible to breaches. Not all data has the same value or sensitivity.

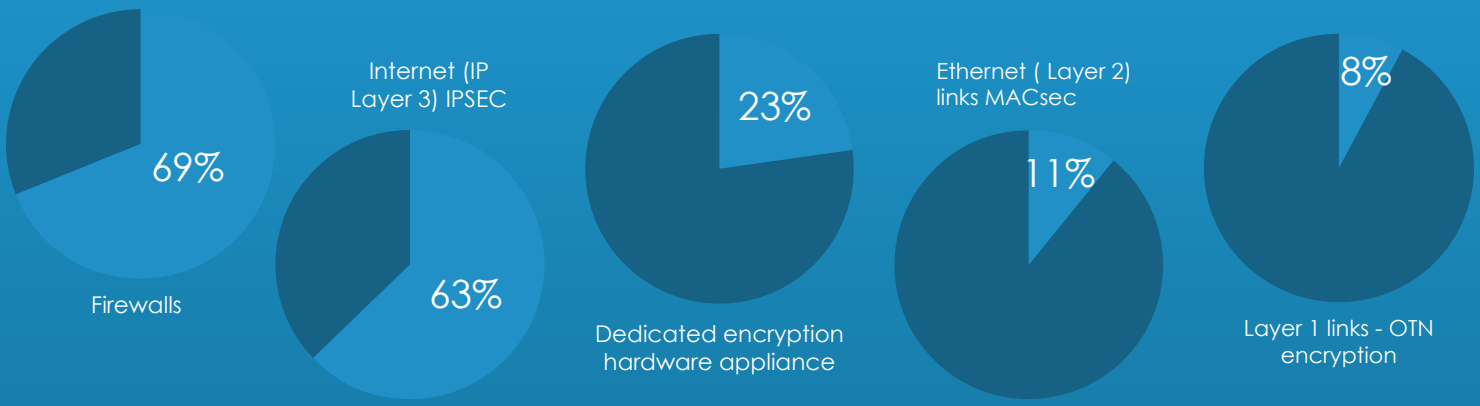
However, organisations should be aware of what data is traversing specific network links and that higher value and higher volume data is at greater risk. The loss, theft or misdirection of sensitive data may not become apparent for some time.

In the interim, significant harm may be done. There appears to be a disconnect between the perceived importance of network data security amongst service providers and their customers.

93% of service providers believe network data should be encrypted, whereas 29% of end-user organizations believe they do not need to encrypt. This suggests service providers have an important role to play in educating their customers about the importance of network data security.

Beware of the dangers of not encrypting network data in motion.

2. Which of the following solutions does your organization use to encrypt data in motion?



Analysis

69% of enterprise respondents say they use firewalls to encrypt data in motion. Whilst firewalls are an essential component of cybersecurity, they are designed primarily to monitor, filter or block traffic. IPsec (Layer 3) solutions were also prevalent. The 63% that say they use IPsec should assess their fitness for purpose when utilizing high-speed networks operating at 1Gbps or above.

Implications

Despite obvious cybersecurity overlaps, there are substantial differences between prevention and protection technologies. As important as firewalls are to protect digital assets against cyberattacks, they do not protect against the successful breach of unencrypted network data.

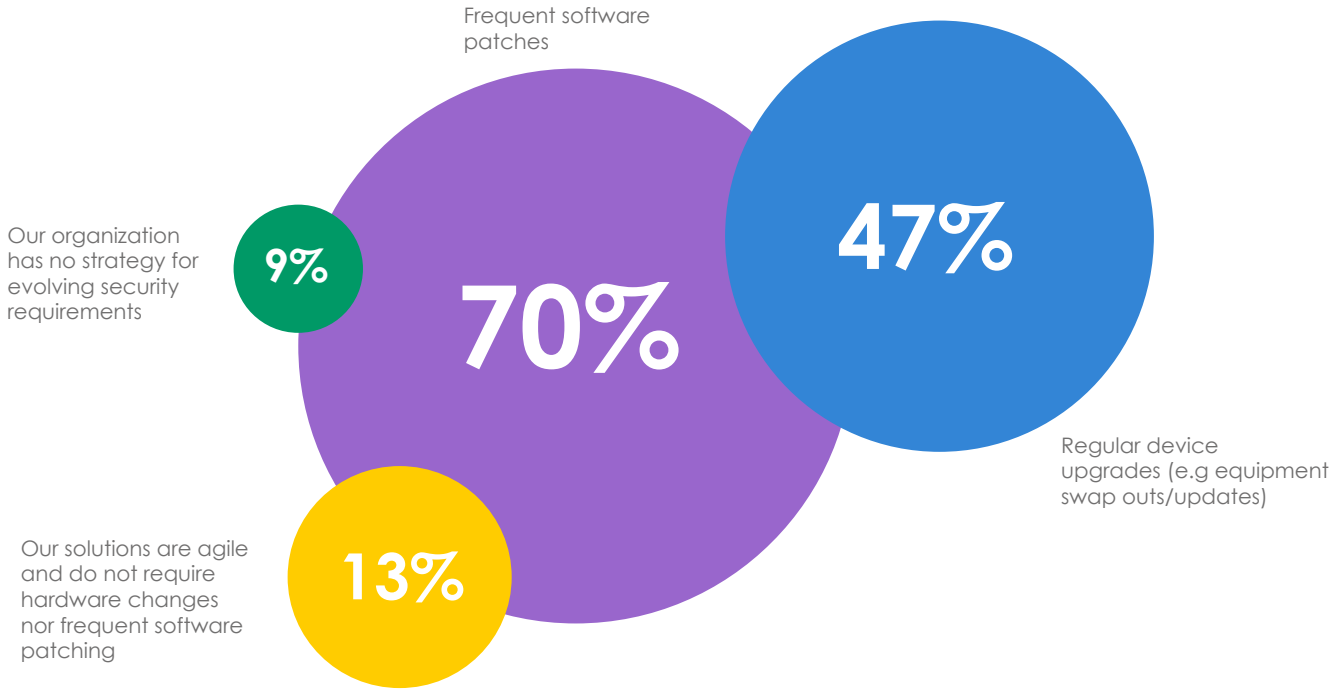
Protocols such as MACsec and IPsec that are embedded within routers and switches (multifunction devices) were not originally designed for today's network applications and security demands. The use of these legacy protocols, that lack cryptographic agility, can adversely affect network performance. Additionally, these dual-purpose devices are more vulnerable to cyberattack and subject to significant performance degradation in terms of bandwidth and latency.

These multi-purpose devices do not generally feature best-practice encryption key management, such as client-side only keys and automated key rotation. By comparison, dedicated appliances provide a higher level of performance and assurance, including near zero latency and network overhead, end-to-end authenticated encryption and built-in cryptographic agility.

Less than a quarter of enterprises (23%) use dedicated hardware encryption appliances to protect network data in motion. This may indicate a lack of awareness of the security, performance and efficiency benefits they provide, which make them ideal for securing data centre interconnections, big data and cloud applications.

Inadequate solutions are heavily used to protect network data in motion.

3. How does your organization address changes to encryption processes brought about by evolving security standards and cyberthreats?



Analysis

70% of respondents say their organizations still rely upon frequent software patches to ensure security is updated. 47% say their security solutions require regular device upgrades to address evolving cybersecurity standards and threat landscapes. 9% of organization admit to having no strategy in place to meet their evolving cybersecurity requirements.

Implications

Over the past twenty years, advances in purpose-built encryption technology have seen performance increase as costs decrease. Despite this, a surprisingly large number of organizations still rely upon outdated software patching or hardware replacement to maintain network security.

Software patching frequently introduces unnecessary risk; both in terms of a delay in bringing systems up to date and the inevitable interruption of network operations. It may also overwhelm the underlying compute power, causing performance issues.

A reliance on frequent patching is not sustainable in the long run. If an organization is not constantly patching or updating, they expose their critical data and systems to risk. If they are constantly patching, it frequently leads to a rip and replace hardware refresh.

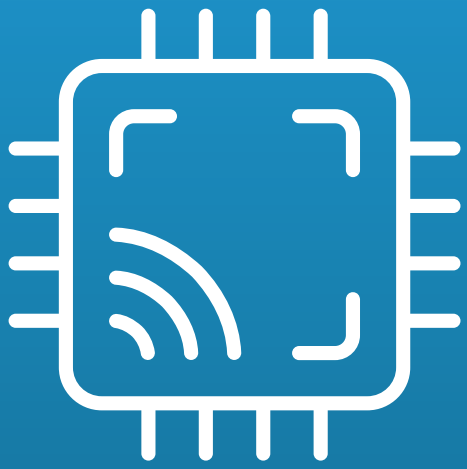
The demands on network infrastructure evolve over time, so organizations need to evaluate their current security solutions. Are they agile enough to address emerging threats and meet the changing demands on bandwidth, architecture and security? Do they provide long-term data protection at a sustainable TCO?

Avoid frequent patching and device swaps; dedicated encryption solutions are a better option.

4. How is your organization preparing for the security threats posed by quantum computing?

61%
Strategy undefined

27%
Not a short-term priority



12%
Quantum Resistant Algorithms

8%
Quantum Key Distribution

Analysis

73% of respondents recognize that quantum computing will represent a significant threat to classical cybersecurity strategies and technologies. Despite this acknowledgement, just 20% have started incorporating quantum-resistant solutions. The potential for quantum computers to render today's cryptographic protocols redundant has been well publicized. It is, perhaps, surprising to find that over a quarter of respondents (27%) do not believe quantum computing represents a significant threat in the foreseeable future.

Implications

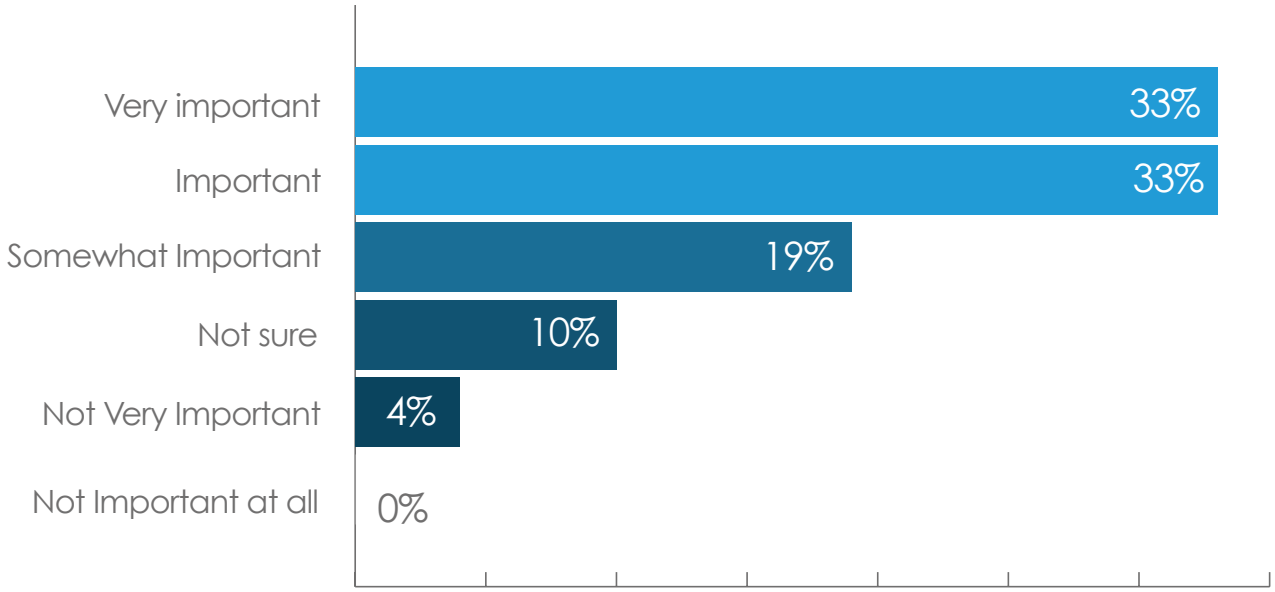
In recent years, the quantum computer has moved beyond the realms of probability to reality. Massive investment by governments and privately-owned enterprises has seen significant breakthroughs, including the commercialization of quantum computing power and the achievement of quantum supremacy (where a quantum computer out-performs the most powerful classical computer).

The exponential increase in computing power inherent in quantum technologies arguably represents the greatest threat to cybersecurity in history. Whilst experts disagree on the precise timing of the arrival of commercially viable quantum computers, they are missing the point. Much of today's data has long-term intrinsic value. Encrypted data that is captured today can be stored and decrypted at some point in the future.

Technologies are available today that can help cybersecurity professionals transition to a quantum-resistant state. Quantum Key Distribution (QKD) is widely used to ensure the integrity of key exchange over public and private networks. The latest generation of dedicated hardware encryption appliances offer a hybrid encryption model, featuring the best of today's proven classical algorithms and the NIST shortlisted quantum-resistant algorithms slated for standardization in 2022.

Quantum computing poses a threat to data security both today and in the future. Act now.

5. How important is separation of duties when evaluating network data encryption solutions?



Analysis

85% of respondents say separation of duties is at least somewhat important when evaluating network data security solutions. On the surface, this contradicts previous findings as only 23% of organizations are using dedicated hardware appliances.

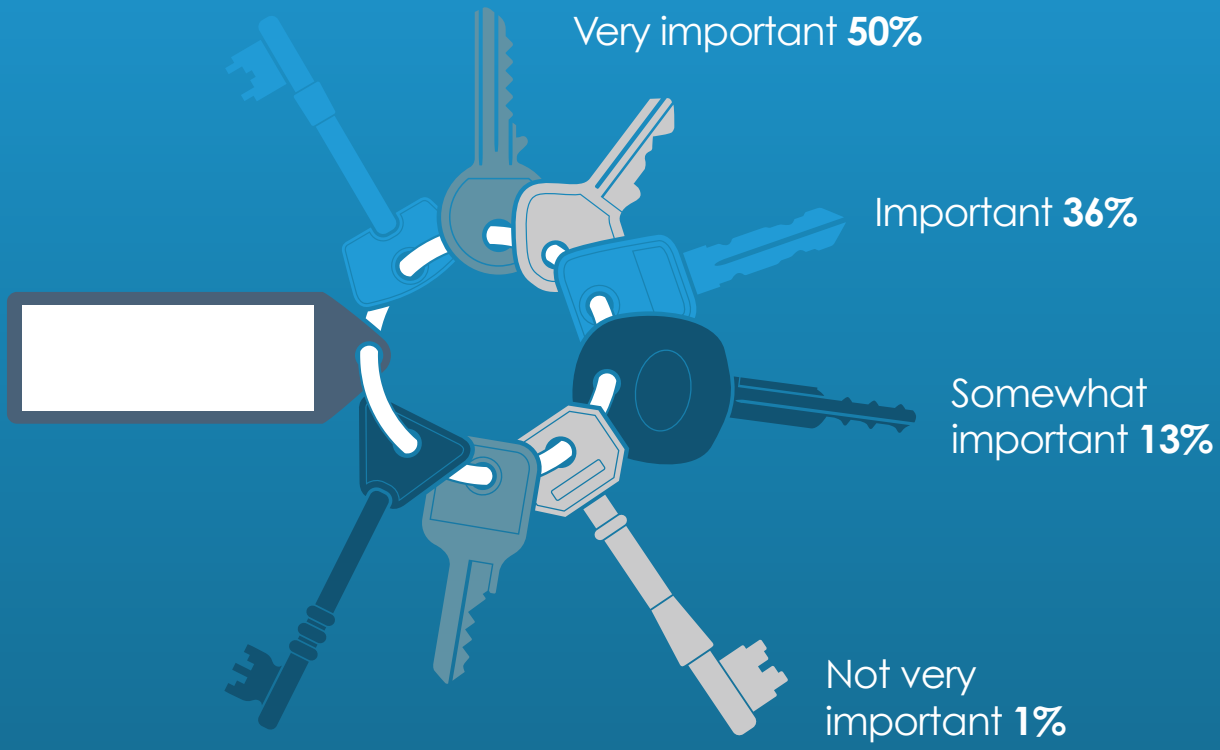
Implications

Separation of duties requires a dedicated network encryption device, keeping network data security and network data transport functionality apart.

Multi-function network devices, such as routers and switches with embedded encryption functionality, expose the network to unnecessary risk. They weaken the system by creating a single point of failure and a single vulnerability for attackers to exploit.

Avoid frequent patching and device swaps; dedicated encryption solutions are a better option.

6. How important are issues related to encryption key material quality, such as randomness and lifecycle management, when adopting an encryption solution?



Analysis

99% of those surveyed recognize that encryption key management plays an essential role systems' security.

Implications

Any cryptographic solution is only as strong as its keys. Best practice encryption key lifecycle management impacts everything from key generation to storage, activation, distribution, rotation, expiration and destruction. Client-side only key storage ensures nobody, not even the OEM, has access to your keys.

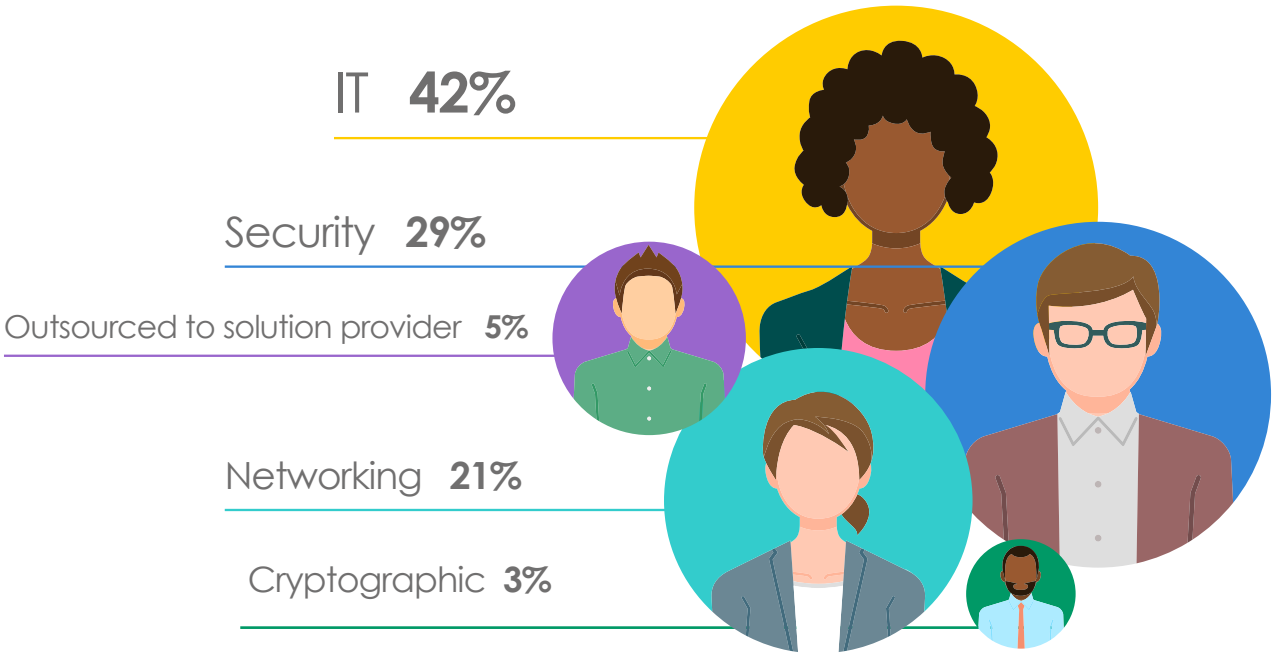
Randomness (entropy) is also important. The greater the degree or randomness used to generate your encryption keys, the stronger they will be.

Agility plays a significant role in key management. To provide long-term network data security, cryptographic systems need to adapt to the evolving demands of data in motion. This includes the ability to operate across multiple networks with layer-agnostic encryption and key management.

Higher-level security certifications, such as NIST 140-2 Level 3, provide greater protection assurance than uncertified or even Level 1 or Level 2 devices. Certification by independent bodies such as FIPS, Common Criteria or NATO provides an additional level of assurance that your chosen solution is fit for purpose.

Don't leave the keys under the mat. Key management is essential to network data security.

7. Within end-user organizations, who is responsible for key management and network encryption?



One of the challenges highlighted by this research is underscored by a seemingly simple question: Who is responsible for key management and network encryption? According to solution provider respondents, the answer is "its complicated".

Identifying which group of stakeholders is responsible for network data security can be challenging. Solution provider respondents indicated responsibility is divided amongst the broader IT teams, plus specialist networking and security professionals. In 5% of cases, it's outsourced to third party service providers.

The findings reflect what is often a fragmented approach to the evaluation, purchase, deployment and management of network data encryption solutions amongst major enterprises. 63% of organizations appear to be relying upon the IT and networking teams to manage data encryption.

Traditionally, these teams are targeted on network performance and availability, not security. With just 29% of solution providers saying they are engaged with security teams during product evaluation and purchase, there is a chance that IT and networking teams are handing their security counterparts a less than optimal solution for network data security.

Clearly, there needs to be greater collaboration and communication among security, IT and networking teams up front in order to properly balance both network performance and data security. The growing trend towards adoption of DevSecOps is an important consideration for enterprises that want to ensure that their security solutions work seamlessly and flexibly within the underlying network architecture used by business teams.

It's not always clear who has overall responsibility for the purchase of encryption solutions.

SOLUTIONS FOR ENCRYPTING DATA IN MOTION

Today's networks demand flexible, network layer agnostic and cryptographically agile solutions to ensure long-term data security. IT security professionals and network managers alike demand maximum protection and ease of management, without impacting on network performance.

The optimal encryption solution for secure network data in motion:

- Secure hardware devices, dedicated to network data encryption
- Policy-based, network layer-agnostic data protection
- End-to-end, authenticated encryption
- Secure encryption key storage and management
- Maximum data throughput with minimal latency and data overhead
- Cryptographic agility, enabling entropy, key distribution and algorithm flexibility
- Hybrid encryption, featuring classical and quantum-resistant algorithms
- Simple, centralized encryptor deployment and management
- Independent security certification

Senetas high-speed encryption solutions have been successfully deployed in more than 45 countries, across a wide range of markets, including: healthcare, government & defence, financial services, critical infrastructure, utilities and cloud service providers.

Our solutions are used to secure wide-area networks, data center interconnections, business continuity, big data analytics, cloud storage, CCTV monitoring and secure multi-location links. These and other environments are hotbeds of substantial amounts of data in motion across physical and virtual networks.

Senetas encryption security solutions for network data in motion are optimized for maximum agility through their Field Programable Gate Array (FPGA) architecture. The benefits begin with separation of security duties in tamper-resistant devices; policy-based support for multi-Layer network protocols (Layers 2, 3 and 4), and GCM authenticated encryption.

They not only support today's proven AES 256-bit algorithms, but also support hybrid-encryption (the addition of quantum resistant algorithms, quantum key distribution and quantum random number generation) for long-term data security in a post quantum world.

Senetas encryption solutions are distributed and supported internationally (outside Australia and New Zealand) by Thales – the world leader in digital security and defence. Senetas CN and CV Series encryption solutions are sold by Thales as part of its Cloud Protection and Licensing portfolio.

For further details, visit www.senetas.com

ABOUT THIS STUDY

Data contained within this report are derived from an online research survey conducted during the fourth quarter of 2020. The respondent pool comprised TechTarget's global database of IT and security professionals, as well as solutions providers involved in purchasing or recommending information security solutions.

The results include 406 respondents from enterprise (end-user) organizations and 101 respondents from solutions provider organizations. Respondents worked in organizations across the globe, including Europe, Asia, Middle East, Africa and North America. All contributors were involved in making purchase decisions or recommendations on security solutions.

GLOBAL SUPPORT

THALES

Senetas encryption solutions are distributed and supported internationally (outside Australia and New Zealand) by Thales

Thales is the world leader in digital security and defence, servicing over 30,000 customers across 180 countries. Senetas products are sold by Thales under its brand.

ANZ PARTNER COMMUNITY

Senetas works directly with customers and their service providers across Australia and New Zealand. We provide technical consultancy and support to data networks providers, systems integrators and cloud service providers. Visit our ANZ Partner Page for full details.

www.senetas.com

Senetas is a leading developer of end-to-end encryption security solutions; trusted to protect enterprise, government, defence, Cloud and service provider network data in over 40 countries.

From certified high-assurance hardware and virtualised encryption, to secure file-sharing and collaboration with data sovereignty control, all are based on the same crypto-agile platform and deliver security without compromise.

Regional Contacts:

Asia	**T:** +65 8307 3540	**E:** infoasia@senetas.com
Australia & New Zealand	**T:** +61(03) 9868 4555	**E:** info@senetas.com
Europe, Middle East & Africa	**T:** +44 (0)1256 345 599	**E:** info@senetas-europe.com
The Americas	**T:** +1 949 436 0509	**E:** infousa@senetas.com

GET IN TOUCH

Are you looking for a service provider to help you select and implement a network data encryption solution? Contact Senetas and we'll help you find the right one.

Senetas works with IT infrastructure service providers and systems integrators across the globe, to help specify the optimal encryption solution for their customers' needs.

Customers may contact Senetas directly to discuss their requirements; or ask their service provider to speak to us on their behalf.

ENCRYPTION SECURITY WITHOUT COMPROMISE

Whatever your network security needs, Senetas has an encryption solution to suit. Our certified high-assurance encryptors protect data across networks operating at speeds from modest 10Mbps to ultra-fast 100Gbps and support all network topologies.

Our virtualised encryption solution, for virtual CPE and virtualised WAN, supports bandwidths of up to 5Gbps. It provides policy-based, end-to-end encryption across multi-Layer networks.

Senetas encryptors are recognised globally for delivering maximum data security and crypto-agility, without compromising network or application performance.

SECURE FILE SHARING

SureDrop offers all the flexibility of a drop-box style solution, with the added benefit of best-in-class encryption security and 100% control over data sovereignty.

For customers seeking additional layers of content security, SureDrop is also available with the Votiro Disarmer extension.

DISARM MALICIOUS CONTENT

Votiro Disarmer leverages patented Content Disarm & Reconstruction (CDR) technology to protect your files from the most advanced, persistent cyber-attacks. It sanitises incoming files, eliminating the risks associated with zero-day or undisclosed attacks, whilst preserving 100% file functionality.

XX-XX0521

SENETAS