CPL.thalesgroup.com

@TechTarget

THALES

Security Weaknesses in Data in Motion Identified in Cybersecurity Survey

TechTarget Custom Media

About this study

A global research report of IT and cybersecurity decision-makers highlights serious concerns about the security of data in motion across networks.

In today's environment of exponential growth in the volumes of data in motion over networks, increasingly sophisticated and state sponsored cybercrime combined with the use of outdated legacy approaches to protecting network data, serious cybersecurity issues need to be addressed. As data network infrastructure is the on-ramp for all organizations' connectivity, the threats to intellectual property, government secrets, sovereignty, citizen identities and critical national infrastructure have never been greater.

Contents

EXECUTIVE SUMMARY

More data is in motion than ever before—a trend that will continue in line with the steep cloud adoption and digital transformation curves, as well as the significant impact of the COVID-19 pandemic on remote working. A number of important factors have significantly increased demand for, and dependency on, high-speed wide-area networks. These include workloads migrating to and from the cloud, real-time global collaboration, big data and cloud data storage, 5G and the expectation of higher bandwidth out to the edge and need for larger and faster aggregation points.

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." However, the reality is that many organizations do not include the requirement for robust data protection in their data management strategies.

Network data in motion has never been more threatened. Both state-sponsored and private, sophisticated cyber-criminals are seeking to steal high-value unprotected data such as intellectual property, government and defense secrets, and scientific and medical research data.

Additionally, with the rapid growth in network data in motion and increasingly sophisticated bad actors comes higher risks of data breaches (nefarious and human or technical errors), data theft through eavesdropping, data misdirection and Denial of Service (DoS) attacks.

This report highlights how organizations need to make network data security a higher priority - requiring advanced solutions through better informed decision making. Conducted with hundreds of global enterprises (commercial, government and industrial) and data network solutions providers, the research reveals a compelling and troubling state of network data security:

- **Only 9%** of enterprises believe they have proactive cybersecurity strategies that address evolving threats
- **Just 58%** of organizations say they encrypt their data in motion. Of those that don't, many using public or private networks are unaware that their networks are not inherently secure.
- **Only 54%** of enterprises feel confident that their network data security solution positions their organization well against cyber threats
- **70%** of enterprises rely upon their network operations staff to regularly implement time-consuming and business disrupting software patches to keep (outdated) security solutions up to date
- **69%** of respondents indicate they rely upon firewalls or IPsec for encrypting network data in motion, rather than using dedicated 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

However, there are some positive signs, as organizations are becoming more aware of the need for data in motion protection solutions. For example, 85% of respondents believe a dedicated purpose-built security solution's 'separation of duties' (security versus network operations) is important for maximum data protection, as opposed to 'integrated solutions' that perform dual network and security functions. Significantly, 86% of respondents also believe that encryption key material is important to their network encryption security solutions.

When it comes to who makes the buying decisions for their network data encryption security, the answer is complicated, according to the surveyed solutions providers. Their responses about whom within customer organizations leads such decisions highlighted fragmented and inconsistent approaches.

These findings provide important insights into the challenges organizations and their solution service providers face when seeking to protect network data in motion. This report also offers practical suggestions on how organizations can improve their security approaches to provide the strongest data protection with minimal network performance impact and reduced management overheads.

91%

of respondents do not believe they have proactive cybersecurity strategies.

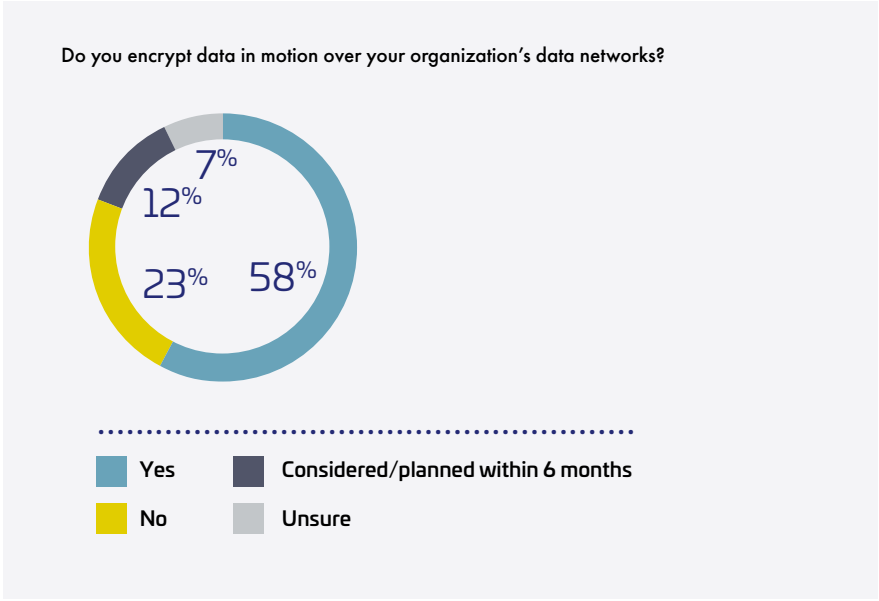
01

Key Findings and Implications

Beware of the dangers of not encrypting network data in motion

Beware of the dangers of not encrypting network data in motion

42% of the respondents either don't encrypt their data in motion or don't know if they do. It's also important to note that, of those that don't currently encrypt their organization's data in motion, 32% say they are using closed or private networks, and another 29% state that encryption is "not required."



Implications:

This finding reveals a serious security misunderstanding about private and public data networks – none are inherently secure. Data traveling across public and private data networks are equally exposed to data breaches. Not all data has the same value or sensitivity, thus organizations should be aware of what data travels across specific network links and that higher value and more sensitive data is at higher risk. Furthermore, higher data volumes (of all types) represent higher value to cybercriminals.

Importantly, data that is stolen, lost, misdirected or intercepted is likely not to be apparent to the owner organization for some time. In many cases, organizations or their solutions provider may not know at all. In the meantime much harm is done.

These findings point to the likelihood that organizations may not fully understand the extent of cybersecurity threats to data in motion across their networks.

The responses also indicate that solutions provider organizations such as VARs, systems integrators and other partners appear to be more aware that their clients' data networks are at risk than the enterprises themselves. This suggests that many enterprises are not fully aware of factors that make their data in motion vulnerable to cyber-attacks and that their solution providers have an important advisory role to help ensure their data is protected.

For example, while 93% of service providers believe network data should be encrypted, 29% of their customers believe they do not need to encrypt that data.

93%

of service providers believe network data should be encrypted.

02

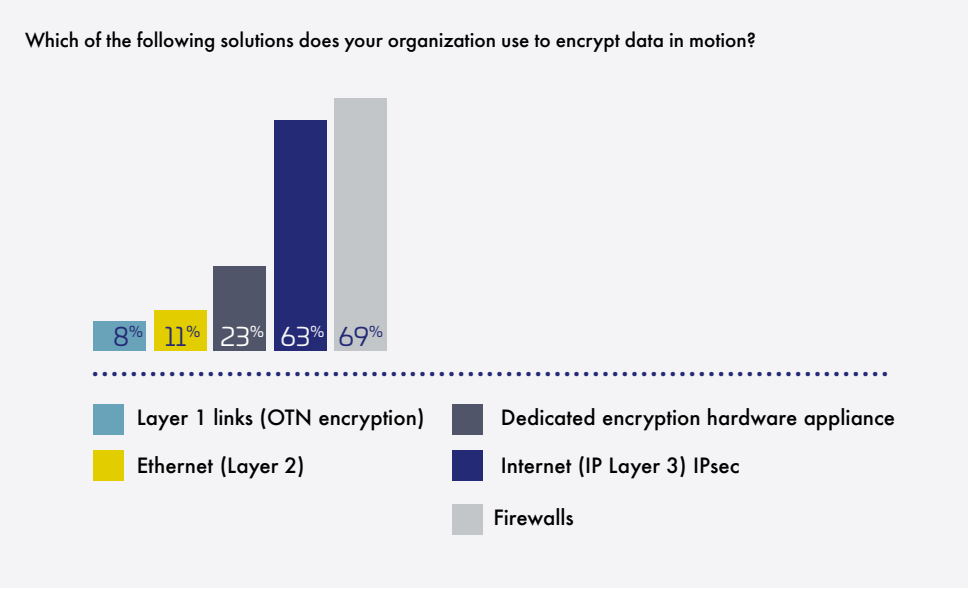
Key Findings

Inadequate solutions are heavily used for protecting network data in motion

Inadequate solutions are heavily used for protecting network data in motion

Despite obvious cybersecurity overlaps, there are substantial differences between anti-malware solutions and data encryption solutions providing protection against theft of unprotected (unencrypted) network data in motion. As important as firewalls are to protect digital assets against cyber-attacks, they do not protect against the successful breach of unencrypted network data.

However, 69% of enterprise respondents say their organizations use firewalls for encrypting data in motion. Whilst firewalls are an essential component of cybersecurity strategies, they primarily address different cybersecurity issues, such as filtering, inspection and application proxy. On the other hand, enterprises using IPsec solutions should determine its fitness for purpose especially when faced with growing demands on 1G-and-above networks versus alternative purpose-built dedicated high performance solutions.



Implications:

Encryption protocols such as MACsec and IPsec added to routers and switches (performing dual purposes) were not originally designed for today's network applications and security requirements. Using such legacy encryption protocols that are not inherently cryptographically agile also adversely affect network performance. Such dual-purpose devices are also more vulnerable to cyberattacks and are subject to significant network performance penalties in terms of bandwidth and latency. They also involve significant hidden operational costs, such as frequent software patches, business disruption, management overheads and the need to purchase additional network bandwidth. These solutions typically do not provide state-of-the-art encryption key management features, such as automated key rotation. Dedicated encryption appliances are generally high performance offerings, providing near zero latency and overheads; are tamper-proof devices, and provide state-of-the-art encryption key management, authentication and cryptographic agility ("high-assurance" solutions).

Of concern is that only 23% of enterprises 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 provided by high assurance dedicated encryption appliances and their significant benefits in applications such as data center interconnections, big data and data in motion to and from the cloud.

69%

of enterprise respondents say their organizations use firewalls for encrypting data in motion.

03

Key Findings

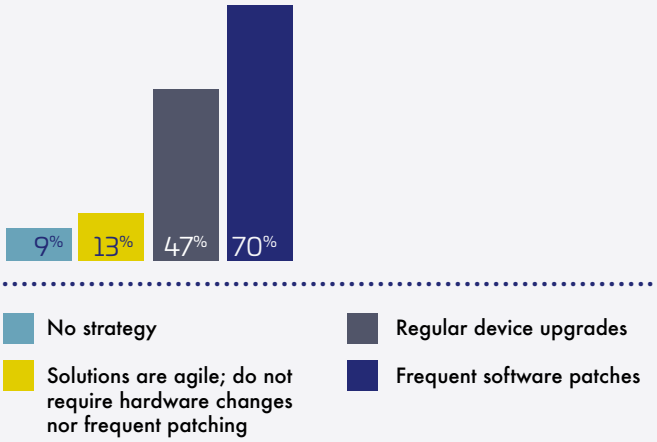
Avoid frequent patching and device swaps; dedicated encryption solutions are a better option

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

It wasn't that long ago that many organizations relied upon outdated and inefficient encryption solutions that involved frequent software patching and hardware replacements to maintain network security. Unfortunately, despite significant advances in state-of-the-art long-term network data encryption solutions (while costs have fallen) in recent years, a surprisingly high number of organizations still utilize inefficient and less secure solutions.

70% of survey respondents say their organizations still use frequent software patches to ensure security is updated. And 47% of respondents say their solutions require regular device upgrades to address changes in security requirements.

How does your organization address changes to encryption processes required by evolving standards and cyberthreats?



Implications:

Software patching typically involves the risks of lengthy delays to bring enterprise security up to date. Many organizations report greater risks of lengthy queues of patches awaiting implementation. That adds to costs of ownership and disrupts network operations and business continuity. It may also overwhelm the underlying compute power, causing system performance issues. Furthermore, patching and device upgrades necessary to ensure up-to-date security put organizations at regulatory risk of compliance breach as well as business disruption.

As cybersecurity threat vectors, network architectures, bandwidth requirements, and even cryptographic standards change over time, organizations should evaluate their encryption solution's long-term security and product benefits. Security features, flexibility, ease of management, cryptographic agility and hardware architecture – all are important to the total cost of ownership. Purpose-built dedicated appliances offer optimal security, performance and management benefits not possible in dual purpose security / networking devices. Purpose-built dedicated appliances maximize security, optimize network performance, minimize management costs and avoid costs of more frequent replacement, and downtime costs of regular security patching across the infrastructure.

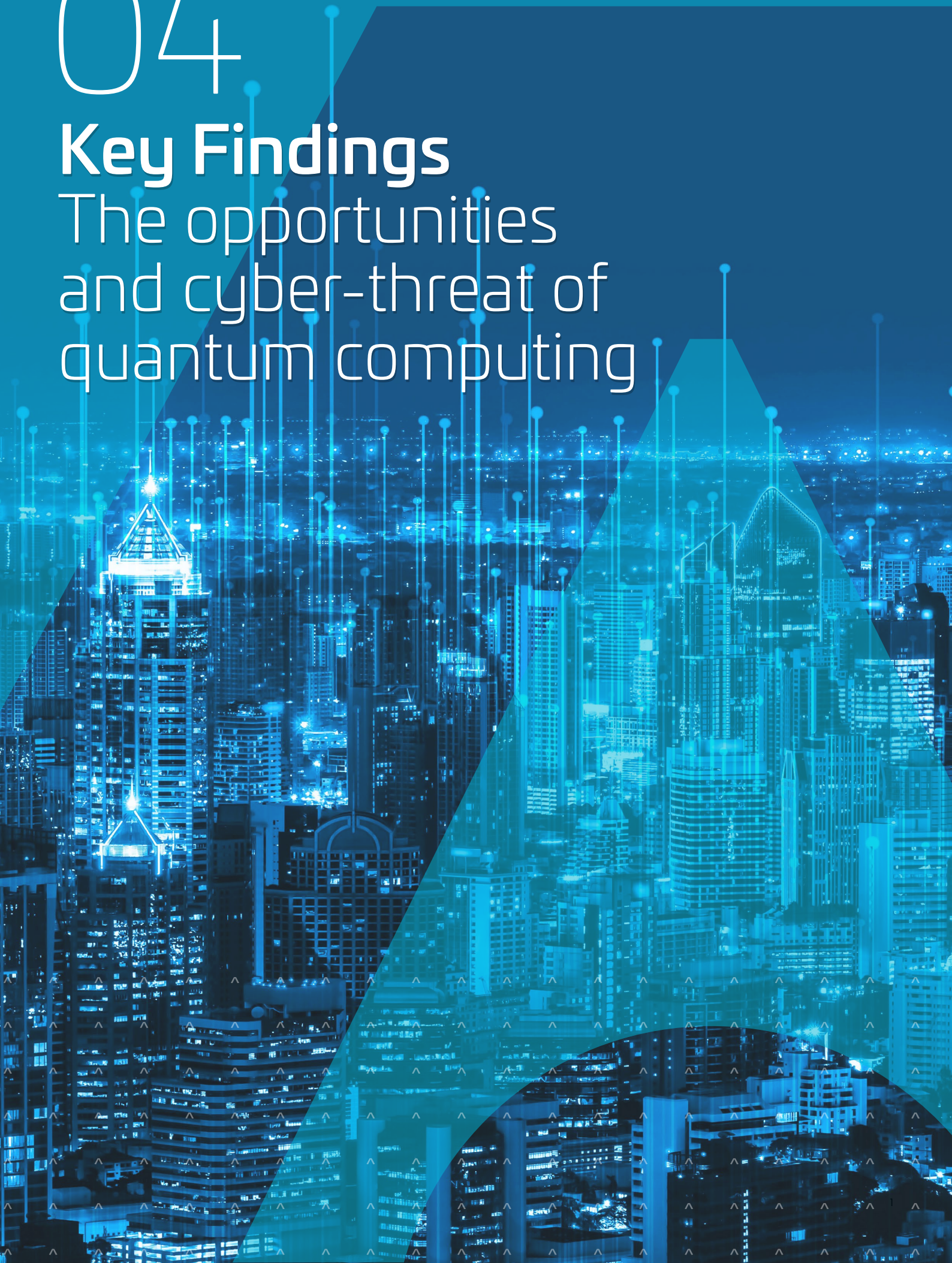
47%

of respondents say their solutions require regular device upgrades to address changes in security requirements.

04

Key Findings

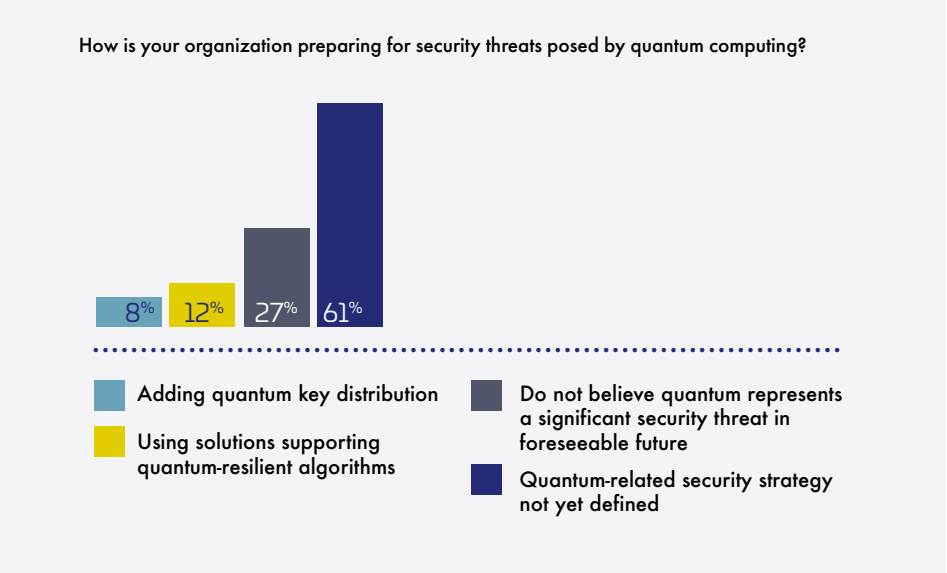
The opportunities and cyber-threat of quantum computing



The opportunities and cyber-threat of quantum computing

Quantum computing has rapidly gained attention and interest among enterprises and solutions providers alike because of its ability to achieve exponential improvements in computational power unavailable in today's classical computing. But, quantum computing also brings with it the greatest threat to cybersecurity in history. That same computational power will make today's classical encryption vulnerable if not obsolete. Quantum-safe algorithms will be essential to ensure long-term data protection. Therefore, organizations must plan for quantum resistant encryption today.

73% of respondents recognize quantum computing represents a significant cybersecurity threat and they must plan to protect data against quantum threats. There are solutions currently available that will ease the evolution to quantum computing by enabling quantum-resistant algorithms and Quantum Key Distribution.



Implications:

As decision-makers increasingly realize that quantum computing will render classical encryption antiquated due to its exponentially greater computing power, there needs to be an understanding of how to ensure that data protected by encryption today will still be protected when quantum computing becomes a reality, as well as how to protect data in the quantum-powered future.

Specifically, cybersecurity experts recommend the use of hybrid encryption by using the best of both worlds—today's proven classical algorithms and a currently shortlisted candidate quantum-resistant algorithm. NIST expects to select a quantum-resistant algorithm standard in 2022. This future-proofing strategy is a smart way for organizations to ensure a quantum-safe future, quantum-safe future, but hybrid encryption requires a cryptographically agile solution platform.

73%

of respondents recognize the future threat of quantum computing.

05

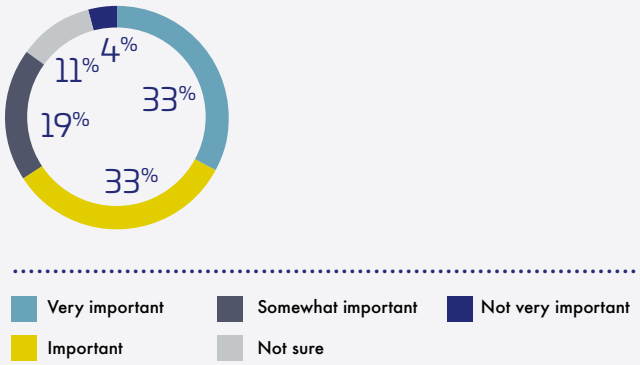
Key Findings

The key "must-haves" for maximum data in motion security

The key "must-haves" for maximum data in motion security

Survey respondents have strong views on what they want in their network encryption solutions to protect their data in motion. First, they overwhelmingly feel separation of duties (requiring a dedicated network encryption device) is important in a network security solution. Here, network data security and network data transport functions are separated, as opposed to encryption security embedded into the network routers and switches. Embedded solutions also weaken the system by creating a single point of failure and providing attackers a single network element and vulnerability to attack.

How important is a network encryption solution's separation of duties when evaluating a security product (rather than bundled dual-function device)?

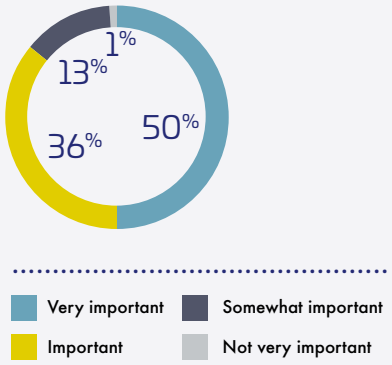


85%

of respondents prefer a dedicated security solution over multi-function devices.

Secondly, respondents overwhelmingly believe issues related to encryption key material quality are important when adopting a network encryption solution: 86% of the respondents call it important or very important.

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



86%

of respondents believe encryption solutions' key material are important.

Implications:

Ensuring the encryption keys are secure is integral to any encryption solution. If the key and/or cryptographic management doesn't meet evolving and demanding requirements for network data in motion, the security will be at risk. These requirements include the ability to work across multiple networks, access controls and automated updates as well as physical protections to provide device anti-tampering. 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. As networks evolve enabling advanced capabilities like software-defined networking (SDN), it's critical that their security manages these changes through network layer-agnostic encryption that supports encryption and key management across the network layers used.

06

Key Findings

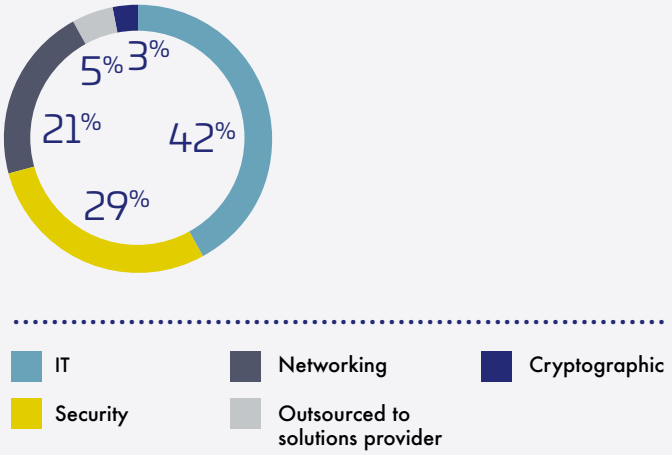
It's not always clear who's responsible for buying encryption solutions

It's not always clear who's responsible for buying encryption solutions

One of the challenges highlighted by this research is underscored by a seemingly simple question: Which one group typically is primarily responsible for encryption key management for network data encryption? According to solution provider respondents, the answer is "it's complicated".

In identifying which department within their enterprises typically makes the decision, solutions providers paint a challenging picture. For example, only 29% of solutions providers indicate that their clients' "security group" is typically in charge of key management for network encryption.

Which group or department, within your clients' organizations, is primarily responsible for key management for network encryption?



This reflects the often-fragmented and rarely universal approach to evaluating, deploying and managing encryption solutions among enterprises. This may shed light on why enterprises seem to care more about network performance and, perhaps, less about security.

Since fewer than 33% of solutions providers say they are dealing with "the security team", by the time decisions on encryption key management are made, IT and networking teams—often heavily focused on both internal and external service-level agreements—may have handed their security counterparts a less-than-optimal encryption solution for network data.

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.

29%

of solutions providers indicate that their clients' "security group" is typically in charge of key management for network encryption.

BEST PRACTICES FOR PROTECTING DATA IN MOTION

With more data in motion across multiple network types facing greater cybersecurity risks than ever before, it is essential that organizations look for solutions that address the new challenges associated with network data security – maximum protection against increasingly sophisticated and state-sponsored cyber criminals; minimal impact on network performance; and management simplicity. Today's networks demand flexible network layer agnostic and cryptographically agile dedicated solutions to ensure long-term future-proof security. Significantly, because network infrastructures have become the go-to for all organizations' connectivity, data in motion has never been more exposed to cyber threats.

The optimal encryption solution for securing network data in motion should include:

- Dedicated encryption security devices, rather than encryption embedded in network data transport routers and switches – for maximum security, network performance and reduced vulnerabilities
- Policy-based network layer-agnostic (independent) data protection – meeting enterprises' use of multiple network layer protocols with the same security and performance attributes
- End-to-end authenticated encryption – protecting the data and network
- Secure management and storage of encryption keys
- Maximum data throughput with minimal latency and data overhead
- Designed-in cryptographically agile platform – enabling entropy, key distribution and algorithm flexibility and hybrid encryption for both today's classical algorithms and tomorrow's quantum-resistant algorithms
- Centralized easy to manage configuration system – ensuring simplified and reliable deployment and management

Organizations should work closely with specialized networking and integration service providers with a strong track record in network data in motion security solutions.

In addition to malware attack threats such as ransomware, cybersecurity strategies should be holistic and reflect the types of data used and in motion across networks. These include their degrees of sensitivity, threat vectors and types of threats faced, such as theft of intellectual property.

“Organizations should work closely with specialized networking and integration service providers with a strong track record in network data in motion security solutions.

HOW THALES CAN HELP MANAGE DATA IN MOTION

Thales offers high-speed encryption solutions that have been successfully deployed in more than 45 countries across a wide range of vertical markets, including healthcare, government agencies and defense organizations, global cloud service providers, banking and financial services, manufacturing, critical infrastructure, telecommunications and more. All share common characteristics of increasing network complexity and dependency, data volumes and threats of increasingly sophisticated bad actors. All depend upon their network infrastructures for access to all their communications.

Thales' solutions have been deployed for use cases including 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, and Thales' solutions provide an impressive scope of benefits, including:

- Maximum security without compromising network performance and business continuity.
- High-assurance solutions delivering:
  - Dedicated tamper-proof encryption security appliances
  - State-of-the-art encryption key management
  - End-to-end authenticated encryption
  - Proven, standards-based algorithms
- Cryptographic agility necessary for quantum-resistant encryption today
- "Set-and-forget" deployment simplicity
- Low management overheads and total cost of ownership
- Centralized management tool for remote management of all encryption devices
- The integrity of multiple security certifications, including FIPS 140-2 level 3, Common Criteria EAL 4+ and NATO

Thales encryption security solutions for network data in motion are optimized for maximum agility through their Field Programmable 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.

CONCLUSION

The research findings discussed in this report highlight the need for organizations to take an informed and comprehensive strategic approach to protecting their network data in motion. Not all encryption solutions are the same – they vary in degree of security, impact on network performance and hidden operational overhead costs. Decision-makers must move from legacy approaches that were not designed for today's complex networks and security requirements. Network architectures, applications, cyber-threats and types of increasingly sophisticated cyber-criminals have changed dramatically. These changes demand purpose-built, dedicated and cryptographic agile encryption appliances to ensure future-proof long-term data security.

For more information about Thales' solutions, please visit https://cpl.thalesgroup.com/

ABOUT THIS STUDY

Data contained within this report are derived from an online research survey conducted during the fourth quarter of 2020. TechTarget's global database of IT and security professionals, as well as solutions providers involved in purchasing or recommending information security solutions, was used as the respondent pool. The results include 406 respondents from enterprise (end-user) organizations and 101 respondents from solutions provider organizations, such as VARs, integrators and service providers. Respondents worked in organizations across the globe, including Europe, Asia, Middle East, Africa and North America, and spanned a range of specific job titles and responsibilities—all involved in making purchase decisions or recommendations on security solutions.

THALES

Contact Us

For all office locations and contact information, please visit cpl.thalesgroup.com/contact-us

>cpl.thalesgroup.com<

TechTarget Custom Media