THALES
Building a future we can all trust

How Secure is Your Data in Motion?

Global survey of IT and security decision makers highlights serious concerns about the security of data in motion across networks and what you should do about it

5 Key Findings

How does your organization stack up?

01 Beware of the danger of not encrypting network data in motion

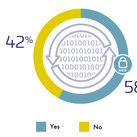
What's notable:

- **42%** of respondents either don't encrypt their data in motion or don't know if they do
- Of those, 32% say they are using closed or private networks and 29% cite encryption is not required

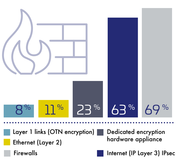
What it means:

- Organizations may not fully understand the extent of cybersecurity threats to data in motion
- Solutions provider organizations are more aware of clients' risks than client—93% of service providers believe network data should be encrypted as opposed to 29% of their customers

Do you encrypt data in motion over your organization's data networks?



Inadequate solutions are heavily used for protecting network data in motion



02 Inadequate solutions are heavily used for protecting network data in motion

What's notable:

- **69%** of enterprise respondents say their organizations use firewalls for encrypting data in motion
- Only 23% of enterprises use dedicated hardware encryption appliances to protect network data in motion

What it means:

- Lack of awareness of performance and security benefits of dedicated encryption appliances (vs. penalties for dual purpose devices)
- Many use IPSec, which is an outdated protocol, not designed for high bandwidth networks that require low overhead and low latency

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

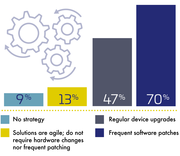
What's notable:

- **70%** of organization respondents still use frequent software patches to ensure security is updated
- 47% of respondents say their solutions require regular device upgrades to address changes in security requirements

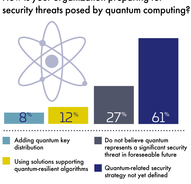
What it means:

- By using dedicated encryption solutions, organizations can ensure they are within compliance and reducing the need for costly/timely patching and updates

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



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



04 The cyber-threat of quantum computing and the importance of crypto-agility

What's notable:

- **73%** recognize quantum is a threat, but 61% have yet to define a strategy for a post-quantum world

What it means:

- Decision makers are starting to look at solutions to ensure that data protected by encryption today will still be protected when quantum computing becomes a reality. Encryption strategies should include crypto-agile solutions that are post-quantum crypto ready.

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

What's notable:

- The majority of respondents see the value in separating security aspects from the network functionality
  86% believe issues related to encryption key material quality are important or very important when adopting a network encryption solution

What it means:

- Decision makers recognize that effective data in motion security requires both separation of duties and ensuring the encryption keys are secure

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

How important are issues related to encryption key material quality?

What should you do to ensure your Data in Motion is secure?

Security, IT, and networking teams need to work together to provide an optimal solution that meets performance, security and budgetary requirements within modern network architectures. Start by focusing on these DevSecOps best practices:

Dedicated encryption
For maximum security, network performance

Independent
Policy-based network layer-agnostic data protection

Protect data & network
End-to-end authenticated encryption

Secure keys
Secure management and storage of encryption keys

Centralized system
Simplified and reliable deployment and management

Crypto-agile
Designed-in cryptographically agile platform

DISCOVER MORE ABOUT THALES HIGH SPEED ENCRYPTORS

READ THE FULL REPORT: SECURITY WEAKNESSES IN DATA IN MOTION

Follow us on:

THALES
Building a future we can all trust

> cpl.thalesgroup.com <

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