THALES

7 Key WAN security Considerations

Sensitive data is big business for cyber criminals; yet it's puzzling that <30% of organizations deploy encryption to secure it, exposing them to considerable risk[1].

Here are 7 things you should take into consideration when choosing a WAN encryption security solution.

1 2019 Thales Data Threat Report

1: Encrypt Everything

All network traffic between sites should be encrypted

Data in motion should be encrypted across al primary network typesl

Encryption solutions should support all topologies

Encryption should take place in a secure device, within a secure environment

2: Keep things random

It's crucial that your keys aren't **vulnerable** to prediction or bias. If a pattern can be established, you can be hacked.

Make sure you use a Random Number Generator with a high source of entropy , such as True Random Number Generation (TRNG) or Quantum Random Number Generation (QRNG).

3: Secure your keys

Encryption keys must be secure during their entire lifecycle.

Key management must be versatile and optimized for the task.

4: Stay agile

Make sure you have a choice of **cryptographic primitives.**

Your solution should also be **crypto-agile.**

5: Think present and future

Your solution should be able to scale up and down with your changing requirements.

It should also be future-proof; protecting you against emerging threats.

6: Stay certified

Look for a vendor with a commitment to independent security evaluations and audits.

7. Beware of operational impact

Look at the **latency** and data **overhead** impacts on network performance.

Think about the impact that unscheduled network downtime could have. Beware of multi-tasking network routing and encryption devices requiring frequent security patches and software updates, casuing unplanned downtime and business disruption

Discover more about Thales encryption solutions

MACSEC VS HSE WHITE PAPER

CN SERIES HARDWARE ENCRYPTION

Follow us on:

THALES