cpl.thalesgroup.com

THALES
Building a future we can all trust

Protecting commercial network data in motion



White Paper

Contents

3 **Protecting high-speed commercial data networks**

4 **An evolving breach landscape**

4 **The business of cyber-crime**

5 **Prevention versus protection**

7 **Combining Hardware and Virtualized Encryption**

7 **Security versus performance and network link use**

8 **CN Series Hardware Encryption**
8 CN9000 Series
8 CN6000 Series
8 CN4000 Series

9 **What makes CN series encryptors stand out?**

10 **High-Assurance Encryption**

10 **Network Independent Encryption**

11 **CV1000 Virtualized Encryption**

11 **Enhanced key security**

11 **DPDK acceleration - performance up to 15 Gbps**

12 **About Thales**

Protecting high-speed commercial data networks

Modern organizations have become dependent upon the fixed, high-speed data networks that serve as their core network infrastructure; providing Big Data, Cloud, SaaS and other digital transformation technologies.

These critical technologies and applications generate huge volumes of data. Data that is often transmitted across wide and Metro Area Networks; exposing it to a variety of cyberthreats. Unfortunately, this data in motion is often over-looked when it comes to cybersecurity planning.

Across the world, commercial organizations are required to comply with a wide variety of cybersecurity regulations. Adherence to these standards, whether independent or sector specific, are often a prerequisite to operate within the sector.

However, private and public-sector organizations alike need to understand that managing cybersecurity risks to network data goes well beyond essential privacy and compliance issues.

Some of the risks are serious enough that they can threaten the core of an organization's operations; its value, intellectual property, business intelligence or physical assets.

Despite the high-profile stories of data breaches that have dominated the headlines since the beginning of the century, research repeatedly highlights that these risks are being under estimated; or worse still, ignored.

This is often because of a presumption that core network infrastructure, such as high-speed Ethernet networks, are safe. They are not.

Whether your network infrastructure is carrier-provided (public) or corporate-owned (private), it could be carrying large volumes of data, streamed at anything from 10 Mbps to hundreds of Gbps.

As a result, it is a high-value target for eavesdropping and all manner of cyber-attacks. As James Caplan from McKinsey and Company puts it "The larger the data volume, the greater the risk."

When it comes to securing core network infrastructure, the risk is even greater. The vulnerabilities present in major vendors' network devices (such as routers and switches) place an additional burden on infrastructure managers.

Interrupting day-to-day network operations to implement a long list of security software patches is nobody's idea of best practice.

Assuming they can stay up to date with the latest patches, IT professionals are still fighting a losing battle. High-speed networks are not inherently secure and breaches are inevitable.

As innovation and collaboration sit at the heart of modern infrastructure, potentially sensitive or valuable data is constantly in motion across core networks for a variety of reasons:

- Data center network links for data storage with multiple redundancy for back-up and disaster recovery planning
- Sharing with collaborating partners, suppliers and customers across WAN and MAN links
- Big Data analytics used for research and development
- Cloud and SaaS applications for day-to-day operations

An evolving breach landscape

In a global economy, data has become the life-blood of commercial organizations of all sizes. Protecting this data should be priority.

The commercial sector is among the most cybersecurity aware sectors in the world. As big data applications and the IoT have come to dominate day-to-day operations, they have focused the minds of cybersecurity professionals.

Gartner predicts organizations will spend nearly $6.69 billion on cloud security in 2023, rising almost 27% year-over-year.[1]

The commercial sector's involvement in high-value innovation, science and technological development makes it a high priority target for cyberattacks from a variety of vectors; including cyberactivists, organized crime syndicates, global competitors, even state-sponsored attacks.

As tighter regulations come into force and organizations are bound by mandatory breach notifications, the true scale of the problem is becoming apparent.

The breach landscape has been dominated by web-based vectors in recent years, as cybercriminals seek to gain from identity theft, financial or account access.

No industry sector is safe, with high-profile breaches spanning healthcare, energy, telecommunications, banking, retail and technology companies.

The Yahoo breach in 2013 was the largest ever, with 3 billion users' account details compromised because of ineffective data security.

The cost of a data breach continues to rise. In its 2022 report, IBM puts the average cost of a data breach at $4.35 million.[2]

Consider eavesdropping on core network infrastructure. How and when would an organization know its data streams are the subject of eavesdropping?

When eavesdropping is discovered, what damage has already been done and what future damage may be done?

- What products have been compromised?
- What R&D investment has been lost?
- Which customers will no longer buy your products?
- What will the downstream effect be – i.e. damage to reputation, trust and brand?

This downstream effect has become increasingly damaging, where manufacturers with unique product technologies discover their intellectual property has been stolen.

In the US, rogue state actors eavesdropped on the core network infrastructure of international advertising and marketing agencies used by global enterprises.

Concerns among agencies and their clients identified that business critical product development, pricing and other secrets had reached competitors in foreign states. The costs to the agencies and customers involved are being measured in hundreds of millions of dollars.

The business of cyber-crime

Cybercrime is not limited to activities of common criminals and bored teenagers. It is now a key domain and skillset of terrorists and state-sponsored hackers.

Like any well-run business, cybercriminals have plans based on objectives – whether to do serious harm, engage in espionage (industrial, defense or state), or just make money.

A recent Verizon Cyber Security Report states, "Cybercriminals care most about ROI (return on investment), so make yourself expensive to hack."

The report suggests where would-be hackers discover high-quality data protection, rather than a challenge to overcome, it acts as a deterrent and encourages them to "move on and attack organizations that are not so well protected".

Cybercriminals have become more skilled and better equipped in recent years, but prevention technologies have struggled to keep pace.

Like most anti-crime measures, prevention is a process of catch up. This, in part, explains the shocking statistics published every year.

1 Gartner Forecast Analysis: Information Security and Risk Management, Worldwide

2 Cost of a Data Breach Report 2022

Prevention versus protection

When it comes to protecting network data in motion, a robust cybersecurity strategy needs to include elements of both prevention and protection.

Prevention uses technologies designed to stop a data breach. Whether that breach occurs while data is in motion or not, breach prevention technologies are key components of any cybersecurity strategy.

However, if there is one truth in data security, it's that it's not a matter of if a breach will occur, but when.

Protection is concerned with safeguarding data in the event of a breach. Only by encrypting your data can you ensure that when prevention fails, your data remains protected.

Not all encryption solutions offer the same level of security, as we look towards the future, encryption solutions must be crypto-agile and provide high-assurance data protection.

High-assurance encryption solutions provide long-term protection for data; well beyond its useful life. They also provide protection against the increased use of traffic flow analysis, where cyber-attackers seek to gain insights from analysing data flow patterns.

It may be surprising to know how much cybercriminals can learn from core network infrastructure traffic flows.

Initially a defense force tactic used to infer intelligence about enemy troop movements, traffic flow analysis has also become an important cybersecurity issue for commercial organizations. Targets are frequently oblivious to the eavesdropping and inferences made by the cyber-attacker.

The future holds greater uncertainty, as new technologies like Quantum Computing evolve.

Although a viable quantum computer may still be five years away, its arrival will render much of the technology currently used to secure public key infrastructure redundant; unless your encryption solution has agility built in.

What is high-assurance encryption?

The term is used to differentiate between encryption methodologies and features. Four critical components make up high-assurance network data encryption:

1. Secure and tamperproof hardware; 100% dedicated to encryption
2. End-to-end, authenticated encryption; ensuring no data is unencrypted when in motion
3. State-of-the-art, zero-touch encryption key management; ensuring only the customer can ever access the keys
4. Use of recognized, standards-based encryption algorithms; such as AES256

In addition to high-assurance criteria, robust encryption should also be officially certified by independent standards authorities as suitable for government and defense use.

Certification represents an independent validation of your chosen solution. The three key standards organizations are:

- Federal Information Processing Standard (FIPS) – United States
- Common Criteria (CC EAL) – International
- North Atlantic Treaty Organization (NATO) – All Member States.

Since developing the first CN encryptor, Thales has chosen to differentiate its products through certification. Multiple certifications form a key part of the certified high-assurance Thales proposition.

We refer to this commitment as Certifications In-Depth. Having developed expertise in security standards and testing requirements, certification is a cornerstone of Thales' hardware encryption design and development.

Critical risk factors

In recent years, four key factors have emerged as critical cybersecurity risks within the commercial sector.

An increase in collaboration has led to the sharing of sensitive information outside of the data security safe zone (with customers, employees, partners and suppliers).

IoT has broken down the borders of traditional infrastructure and exponentially increased the number of access points to the network.

Old-fashioned human or technical error, whilst on the decline, still accounts for a significant amount of all lost or stolen data records.

Security vulnerabilities discovered in core network infrastructure devices significantly add to the cybersecurity risks of data in motion.

Examples include:

- Network devices discovered to have security weaknesses that may be exploited by cybercriminals
- Inferior or poorly engineered devices that promise added encryption security, but use weak encryption processes

In one instance, PC World reported that over 840,000 Cisco networking devices from around the world were exposed to a vulnerability akin to one exploited by a hacking group.

Research by SEC Consult revealed further vulnerabilities in over 900 products; with poor encryption key-management processes used by routers and switches that promise "hybrid encryption".

This highlights three key issues for defense industry organizations that take data security seriously:

- The importance of certified encryption solutions and government evaluations
- Why encryption security must be a 100% dedicated and separated function
- That hybrid network and security products do not offer optimal data protection

> **" Encryption should be enabled for everything by default, not a feature you turn on only if you're doing something you consider worth protecting."**
>
> **– Bruce Schneier**

The real cost of a breach

Cybersecurity experts continue to warn that too many organizations underestimate and underinvest in protecting data in motion.

Whether all data in an organization is sensitive per se, is not the point; nor is it a reason to avoid protecting it with encryption. Data has become the currency of modern business and the rewards for cybercriminals, hackers and terrorists can be significant.

Beyond the potential for privacy breaches, and a failure to meet regulatory compliance obligations, the impact of a data breach can be catastrophic.

Loss or corruption of critical business data and management information can have a wide-ranging impact on day-to-day operations.

Even greater impact would come from the loss of intellectual property or secret information that provides any degree of competitive advantage.

Under new, stricter, data protection regulations, organizations found to be in breach of the rules could face significant financial penalties; especially if it is not a first offense.

The GDPR, though originating within the EU, will impact on just about every organization and includes the potential for eye-watering penalties (up to 4% of global revenues) for repeat offenders.

Emerging regulations will also see individuals within organizations liable for financial penalties and even custodial sentences in the case of negligence.

This will place a greater responsibility and "duty of care" on both data owners and processors within the commercial sector.

Longer-term implications of a breach can also be derived from a loss of reputation or trust; jeopardizing future revenues.

For example, US industrial software developer AMSC – a listed company – discovered that critical software intellectual property had been stolen and was being used by foreign competitors.

Despite swift action by AMSC (with the aid of the FBI), stock values fell from $370 per share to just $5 per share while the matter was being prosecuted.

Combining Hardware and Virtualized Encryption

A lack of vendor compatibility within the network encryption marketplace means organizations looking to secure both core IT infrastructure and virtualized WAN need to think carefully about a choice of technology.

The choice between hardware and virtualized encryption is based on an organization's individual needs and preferences. Often, it is not a case of 'either/or' – but a blend of the two technologies together.

Security versus performance and network link use

Hardware encryptors deliver predetermined high-performance, not able to be matched by software/virtualized encryption. They also provide maximum data security through multi-certified, high-assurance credentials.

Network link use cases

High-speed links (>5 Gbps) are more commonly used to connect IT infrastructure such as data center interconnects, or Big Data feeds.

Encrypting data in motion between branch locations is of equal importance, though network speeds will vary between these locations.

These links ideally require both maximum data protection and best performance, only offered by hardware encryptors.

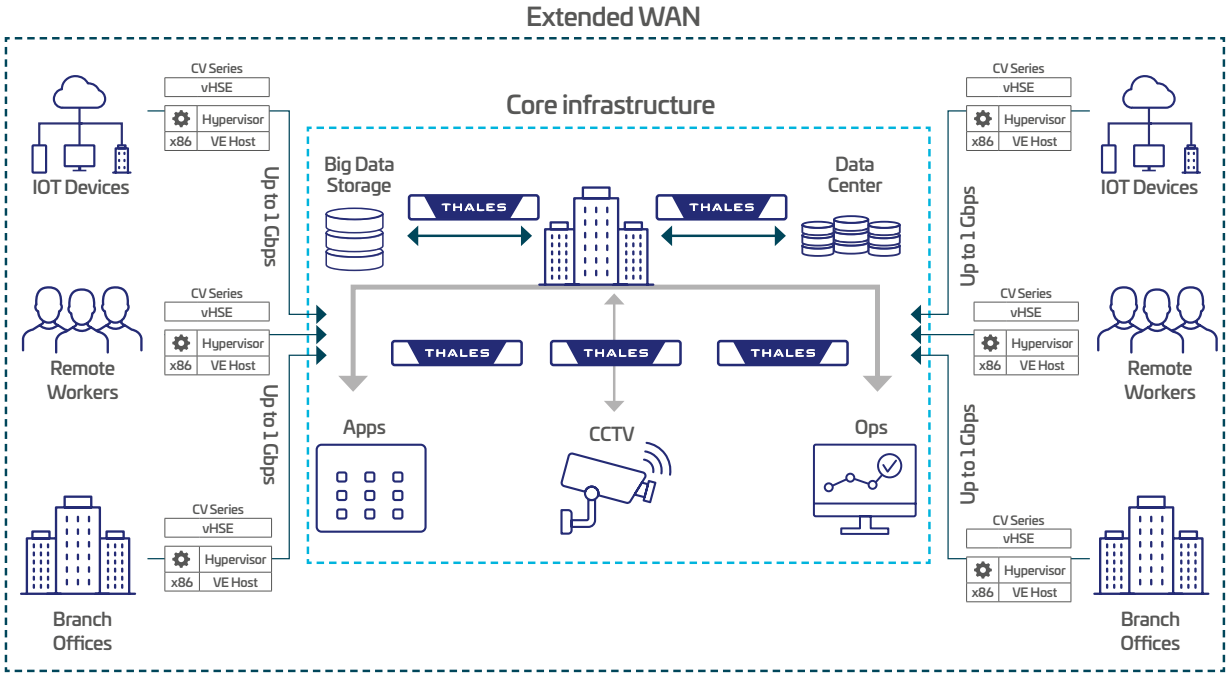
However, for extended WAN links and high-scale virtualized links that typically run at up to 5 Gbps, a virtual encryptor is likely to be a more flexible and cost-effective solution.

Mixed use cases

Organizations often only deploy hardware encryption to protect core IT infrastructure data in motion. Many operate unprotected extended WAN links.

Virtualized encryption provides an opportunity to encrypt all data in motion through a single compatible technology.

Ultimately, organizations should use dedicated hardware encryption for their main feeds, interconnects and branch locations, while virtualized encryption is used to provide scalable, cost-effective encryption for devices at the network edge.



CN Series Hardware Encryption

CN9000 Series

The CN9100 is the world's first commercially available certified high-assurance 100 Gbps Ethernet network encryptor that supports all network topologies.

Like all Thales CN encryptors, the CN9000 Series provides maximum high-assurance network data security, without compromising network and application performance. It boasts ultra-low latency of just 1.5 microseconds in customer testing.

Developed in collaboration with customers and service providers, Thales CN9100 encryptors are designed to meet the exacting requirements of all 100 Gbps use cases, making them an ideal application for securing public and private Cloud networks.

Thales' CN and CV Series encryptors include integrated support for CipherTrust Key Manager (Thales' centralized cryptographic key management solution) that provides maximum security for the storage of master keys, the integrity of security policies and the source of entropy for the generation of cryptographic keys.

CN6000 Series

Thales CN6000 Series encryptors provide highly secure, full line-rate transparent encryption for data moving across both dark fibre and metro/wide area Ethernet networks; in point-to-point, hub & spoke or meshed environments.

The CN6000 Series are rack-mounted, high speed encryptors for business-critical applications; offering 1 Gbps to 10 Gbps bandwidth speeds. They are the optimal choice when you require:

- Efficient, investment-proof data encryption
- Multi-purpose, in-field upgradable and flexible hardware
- Choice of Common Criteria, and FIPS certifications
- Compact 1U form factor with advanced performance and power features

CN4000 Series

Network data security is a challenge to organizations of all shapes and sizes. To help address the encryption demands of smaller organizations and in-field operations, Thales developed the CN4000 series of compact encryptors.

Despite their small form-factor, Thales CN4000 Series encryptors boast the same robust security credentials of their rack-mounted cousins.

The CN4000 series is the ideal low-cost, high-performance encryptor range for small to medium-sized enterprises (SME). They also provide a cost-effective "encrypt everywhere" solution for larger enterprises looking to secure remote or temporary locations connected via networks operating at up to 1 Gbps.

Like all CN hardware encryptors, the CN4000 Series features standards-based encryption, secure key management and the peace of mind that comes from certification by the world's leading independent testing authorities.

What makes CN series encryptors stand out?

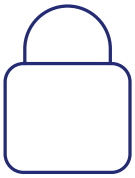


Performance

High Speed
Market-leading performance. Operating anywhere from 10 Mbps or 100 Gbps, Thales encryptors consistently win competitive performance test.

Low Latency
Operating in full duplex mode, at full line speed, without packet loss. Latency is as low as 2 microseconds per unit at 100 Gbps.

Zero Impact
The zero impact of Thales encryptors is not limited to network bandwidth and latency; it extends to network operations and management.

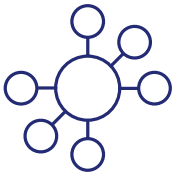


Security

Certification
For more than 20 years, Thales R&D has remained committed to the principle of certification in depth. Thales CN Series encryptors are certified by: FIPS, Common Criteria and NATO.

Key Management
All CN Series encryptors feature state-of-the-art encryption key management. Keys are securely stored and encrypted, and only accessible by you.

Solution Integrity
Thales high-assurance encryption solutions feature dedicated, tamper-proof hardware and provide gapless, end-to-end, authenticated encryption.



Versatility

Crypto Agility

All Thales encryptors are crypto agile; from 100% compatibility and interoperability to customisable encryption and FPGA based flexibility.

Topology Support

Thales CN encryptors operate in point-to-point, point-to-multipoint and fully meshed network topologies.

Flexible Management

Configuration may be performed locally or remotely through the intuitive Thales management software.



Efficiency

Cost Effectiveness

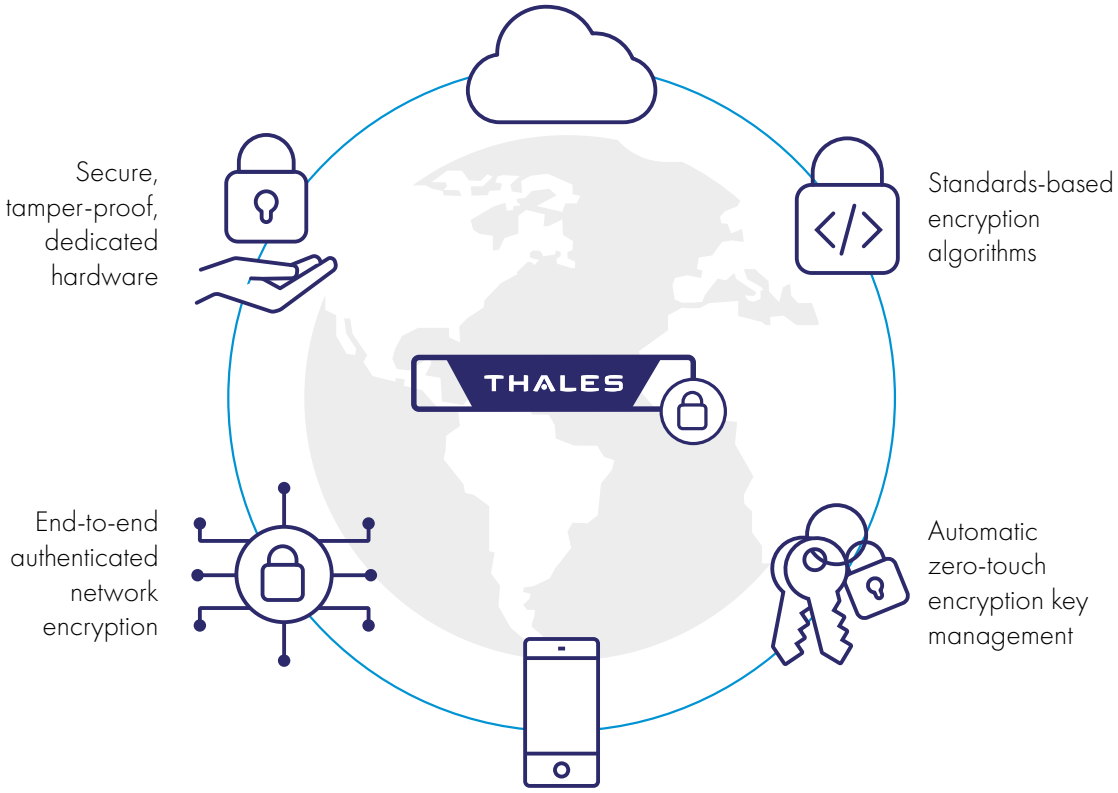
Thales encryptors provide excellent TCO through a mix of network bandwidth savings, ease of management and longevity.

Reliability

All carrier-grade Thales encryptors are hot-swappable, feature dual redundancy and deliver 99.999% uptime.

Flexibility

Use of FPGA technology enables maximum operational flexibility, including use of custom encryption and in-field upgradability.



High-Assurance Encryption

As recommended by leading data security and encryption analysts; for a network encryption solution to be truly robust, and provide long-term data protection (well beyond the useful life of the data), it must be a high-assurance solution.

Not all encryption solutions are created equal. So-called 'hybrid' encryption devices – such as network routers/switches with embedded encryption or those using MACSec or similar standards (not originally intended for WAN and MAN security) provide low assurance data protection.

By contrast, Thales CN Series encryption solutions are certified by the world's leading independent testing authorities as suitable for government and defense applications. They are purpose-engineered for dedicated, high-assurance network data security.

Thales CN Series encryptors' security credentials include all four essential high-assurance features:

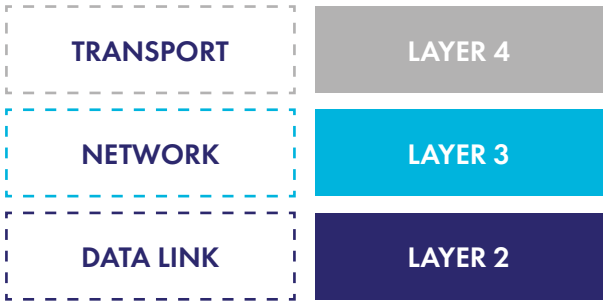
- Secure, tamper-proof hardware; dedicated to network data encryption
- State-of-the-art, client-side, zero-touch encryption key management
- End-to-end, authenticated encryption
- Use of standards-based encryption algorithms

Network Independent Encryption

Many organizations use multiple data network Layer protocols (Layer 2, 3 and 4) to help deliver their business applications and communications services. Recognizing this, Thales has designed-in Network Independent Encryption.

This advanced, network Layer agnostic encryption technology enables destination policy-based, concurrent multi-Layer encryption.

Significantly, customers are still assured of strong, end-to-end encryption as the protected data traverses the various network Layers, for example: from Layer 2 Ethernet to Layer 3 IP network destination.



CV1000 Virtualized Encryption

The CV1000 is a Virtual Network Function (VNF) appliance providing strong and effective data encryption security with designed-in crypto-agility. Designed for virtual CPE, the CV1000 delivers transport-Layer agnostic encryption for high-speed networks at up to 5 Gbps.

As an VNF appliance, the CV1000 stands out from the crowd. Instant scalability means it may be deployed rapidly across thousands of network links. It delivers the same flexibility and scalability as other virtualized network functions.

The CV1000 offers state-of-the-art encryption security and key management without impacting on network or application performance*. Unlike IPSec-type encryption solutions, the CV1000 is transparent to the network; making it ideal for securing your WAN, right to the virtual edge.

Integrated support for CipherTrust Key Manager (Thales' centralized cryptographic key management solution) provides maximum security for the storage of master keys, the integrity of security policies and the source of entropy for the generation of cryptographic keys.

Enhanced key security

The CV1000 is fully compatible with CipherTrust Key Manager.

Available as a hardware appliance or a hardened virtual security appliance, CipherTrust Key Manager provides support for multiple key types: symmetric, asymmetric, secret data and X.509 certificates.

CipherTrust Key Manager simplifies the management of encryption keys across the entire life-cycle; including key generation, storage, backup, distribution, deactivation and deletion.

DPDK acceleration - performance up to 15 Gbps

DPDK Intel libraries enable x86 host device performance acceleration. If the host x86 device and DPDK are optimally configured, the CV1000 will deliver enhanced performance of >1 Gbps up to 5 Gbps.

Consistent performance up to 15 Gbps is dependent upon host configuration and expertise in DPDK setup and configuration.

Environment and architecture factors may also play a role in virtualized encryption performance, as they do in virtualized networks.

Key benefits

Unmatched benefits of the CV1000 expressed by end-user customers and service providers include:

- The CV1000 enables adoption of a virtualized encryption solution that does not compromise on security or network and application performance
- Instant scalability to match the scale and flexibility of virtual and software-defined networks
- No requirement to deploy large numbers of hardware encryption devices to achieve high scale implementation of network encryption
- The CV1000 encryption security and key management model is optimized for strong and effective encryption security
- Through Transport Independent Mode, the CV1000 is suited to a multi-Layer network environment
- Competitively, the CV1000 delivers up to 30% network performance benefit over other solutions
- Ease of deployment with centralized, 'zero touch' provisioning
- 100% interoperability with Thales CN Series encryptors
- As a software implementation of the Thales high-assurance encryption platform, the CV1000 provides a flexible, cost-effective way to encrypt all the way to the virtual edge
- Data center service providers identified the CV1000 as an optimal solution; providing strong and effective encryption security among devices within the data center itself

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.

THALES

Building a future we can all trust

Contact us

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

> cpl.thalesgroup.com <

© Thales - January 2023 • RMv8