cpl.thalesgroup.com

THALES

Securing high tech industry network data

White Paper

Contents

Cybersecurity considerations for high-tech industries

We all understand the negative impact of data loss, so why is it that so many organizations seem to be failing in their duty of care to protect sensitive personal and commercial data?

Failure may sound harsh, but shareholders, suppliers, customers and employees have a right to expect their data to be protected. They shouldn't expect to suffer harm (loss of share capital, business disruption, stolen IP, privacy breaches and financial penalties) as a result of inadequate cybersecurity.

High-tech industries have become a target of choice for bad actors because of the potentially rich rewards resulting from a successful hack.

The global technology market

The global technology market has continued to see strong growth in recent years. According to the 2021 Global 2000, Forbes' annual ranking of the world's largest public companies, technology companies account for more than $17.9 trillion in market value, up more than 73% year over year, representing close to one-third of the US Stock Market.

Out of the 177 technology companies that claimed a spot on this list81 were from the United States, far more than any other country. China taking second place, closely followed by Japan and Taiwan respectively.

These high-tech organizations, as well as those that fall outside the Global 2000 list, come from a diverse range of sub-industries – from electronics manufacturing and software development to digital media and aerospace.

All of these companies share a common trait: they operate at the leading edge of their respective industries, where IP and network security play a vital role in ensuring competitive advantage.

The very nature of these high-tech industries means that large volumes of data are generated; much of which will be sensitive in nature. This data is an attractive target for cybercriminals.

The threat landscape

The treats facing organizations that operate within high-tech industry verticals are many and varied; ranging from IP theft and eavesdropping to rogue data injection.

The impact of a successful data breach could range from financial to existential losses which, according to the 2021 Cost of a Data Breach Report by IBM Security and Ponemon Institute, can be felt for years to come.

The report shows that, while an average 53% of breach costs come in year one, 38% occur in the second year and 16% more than two years after the event.

Thankfully, effective cybersecurity prevention and protection technologies are readily available, and more cost-effective than ever. For example, the use of end-to-end encryption solutions (both for data at rest and in transit) is considered mandatory by many cybersecurity experts.

Encryption should be considered an everyday part of doing business; especially in high-value and high-tech industries.

The role of the high-tech industry

Ironically, high-tech organizations themselves could play a vital role in shaping the cybersecurity landscape of the future.

Organizations operating at the forefront of technological development will not only unveil countless opportunities for innovation, but also their associated threats as the two come hand-in-hand.

One such example is the space industry where, as we move towards the age of the quantum computer, professionals are turning to satellite technology for the answer to tomorrow's cryptographic technologies.

Quantum Key Distribution (QKD) is a technology that sits at the heart of future quantum communications networks. A network of communications satellites could hold the answer to a cost-effective, global QKD platform.

If your data's worth anything, it's worth encrypting

An unsettled outlook

If cybersecurity is tough today, it will be much tougher tomorrow. Emerging business technologies promise greater security challenges as the Internet of Things (IoT), borderless infrastructure and ubiquitous cloud applications lead to a further explosion in high-speed, high-performance data networks and transmitted data volumes.

High-tech industries' use of emerging IoT and AI technologies, and their collaborative use of public and private cloud infrastructure, introduce new vulnerabilities.

Whilst identity theft and financial account access are major motivators for cyber-criminals, state-sponsored cyber-attacks and hacktivism pose a larger threat to society as a whole. Nuisance hacks are becoming less prevalent, but we are seeing the emergence of cyber-terrorism as an existential threat.

The EU's General Data Protection Regulation (GDPR) was introduced in 2018. In it, a qualifying breach is deemed to be one in which "...data is not protected by strong encryption...".

As the gold standard of data security regulations, the GDPR introduces unprecedented data breach notification requirements and the potential for severe financial penalties in the event of successful breaches of unencrypted data.

The GDPR is important to the global high-tech industry because it doesn't just apply to organizations within the EU, but anyone who trades or collaborates with EU member states.

While regulation is being introduced to encourage standards and ensure sensitive data is kept secure, responsibility for adhering to these standards remains with the organization.

An example of this occurred in 2017 when, despite Australian data privacy regulations and federal government defense supplier data security requirements, it was revealed that a breach of a defense industry contractor's data lead to the theft of 10 gigabytes of sensitive data. None of this data was encrypted.

Rather than meeting standards as the bare minimum, high-tech organizations must look to go beyond them.

Looking beyond losses

Cybersecurity is not simply about protection against data loss or privacy breaches. Of increasing concern is the risk of data manipulation, access control, injection of rogue data and even interference with industrial and other asset control systems (i.e. criticalnational infrastructure).

The impact of a data breach or cyber-attack in some commercial markets can range from minor inconvenience to financial hardship; from the temporary shutdown of an application long-term reputational damage.

For critical infrastructure and high-tech sectors, the stakes could be much higher. A successful hack of an unencrypted network could enable a bad actor to seize control of critical systems, disrupt services and impact the day-to-day lives of millions of people. Strong encryption protects against these acts of cyberterrorism.

In the words of cybersecurity expert and cryptographer, Bruce Schneier, "Encryption should be enabled for everything by default, not a feature you turn on only if you're doing something you consider worth protecting."

Traps for the trusting

US author and consultant Denis Waitley said, "Life is inherently risky. There is only one big risk you should avoid at all costs, and that is the risk of doing nothing."

His words are all the more poignant in a world where the technologies that help drive business opportunities also open doors to cybersecurity threats that will undermine them.

The adoption of new business technologies and collaboration (local and global) among high-tech organizations (partners, customers, suppliers) using Cloud, SaaS, multi-Cloud, IaaS and hybrid-Cloud technologies continues to accelerate.

Significantly, they require more complex and high-performance data networks than ever before to enable them and transmit record volumes of proprietary and control systems data.

The world we know has become dependent upon high-speed data networks. From the outset, these data networks are not inherently secure; and networking devices such as routers and switches often add security vulnerabilities.

A reliance on basic infrastructure to secure network data in motion is effectively a trap for the trusting.

Prevention and protection - *caveat emptor*

There are two key components to data security: prevention and protection.

Prevention technologies (e.g. firewalls) attempt to stop cyber-attacks and data breaches from occurring. They are essential components of a good cybersecurity strategy but cannot work alone. If there is one truth in data security, it's that it's not a matter of if a data breach will occur, but when.

Protection technologies (e.g. encryption) secure the data in the event of a breach. Only encryption ensures that when prevention security fails, the breached data is rendered useless in the hands of unauthorised parties.

Remember, not all encryption solutions are created equal. Your choice of encryption technology should be fit-for-purpose. If you want to ensure long-term protection beyond the useful life of the data, it needs to be purpose-built, dedicated hardware with the agility to adapt to future quantum cryptographic technologies.

Encrypt everything

Three main factors have added to cybersecurity risks in recent years; vulnerable network devices (routers and switches), email sharing of unencrypted documents with third parties (customers, partners and suppliers), and innocent human and technical errors.

Whether all data in an organization is sensitive is not the point. As Schneier emphasises, nor is it a reason not to encrypt. Data has become the currency of modern business and the rewards for cybercriminals, roguestates and industrialspies are significant.

High-tech organizations should not only encrypt all their data in motion; it should be encrypted end-to-end as it flows between network endpoint, be this core infrastructure or equipment at the virtual edge.

Should organizations choose not to do this, resultant eavesdropping and IP theft could have catastrophic implications for the organization, its shareholders and customers alike.

One such example occurred when US industrial software developer AMSC – a listed company – discovered that critical software IP was stolen and used by foreign competitors. Despite swift action and with FBI help, AMSC's stock value fell from $370.00 per share to just $5 per share while the matter was being prosecuted.

Choosing the right encryption solution

When it comes to choosing an encryption vendor, it is important to consider all the possible applications. Just as important is the realization that all encryption solutions are not created equal.

Borderless infrastructure and edge computing sees data flowing across the network from multiple devices at multiple locations, meaning this data must be secured throughout its journey.

In the same way, data transmitted across metro area networks must be secured at all points as a single vulnerability will result in a failure across the network.

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.

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 hardware 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 network encryptors' security credentials include all four, essential high-assurance features:

- Secure, tamper-proof hardware; dedicated to network data encryption
- State-of-the-art encryption key management; featuring secure, client-side key storage
- End-to-end, authenticated encryption
- Standards-based encryption algorithms

For real-time data applications such as financial platforms and CCTV monitoring, latency is a significant issue. While adding a network encryption interface card to an existing switch may seem like an attractive option; it will result in higher latency and lower throughput performance than a dedicated device.

In some instances, using a network interfact controller (NIC) means the same vendor needs to be used throughout the network route and that data is decrypted and re-encrypted at each of the hops.

This is both a security risk and a major key management issue. Dedicated appliances enable data to remain encrypted throughout the network route, irrespective of switch vendor.

If an NIC is used, the lifespan of the encryptor will be tied to the host network device and will need to be replaced when the switch is changed.

Most modern infrastructure comprises multiple network Layers; typically featuring Layer 2, 3 and 4 elements. So, organizations should look for a vendor that provides Layer agnostic encryption where possible.

Thales CV Series virtual appliances provide concurrent, multi-Layer encryption and support DPDK for up to 5 Gbps performance.

Like the CN Series hardware encryptors, our virtual appliances support all topologies, from P2P to Hub & Spoke and fully meshed networks.

To facilitate encrypted file-sharing, the SureDrop secure file-sharing application delivers a familiar box style functionality with high-assurance data protection technology.

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.

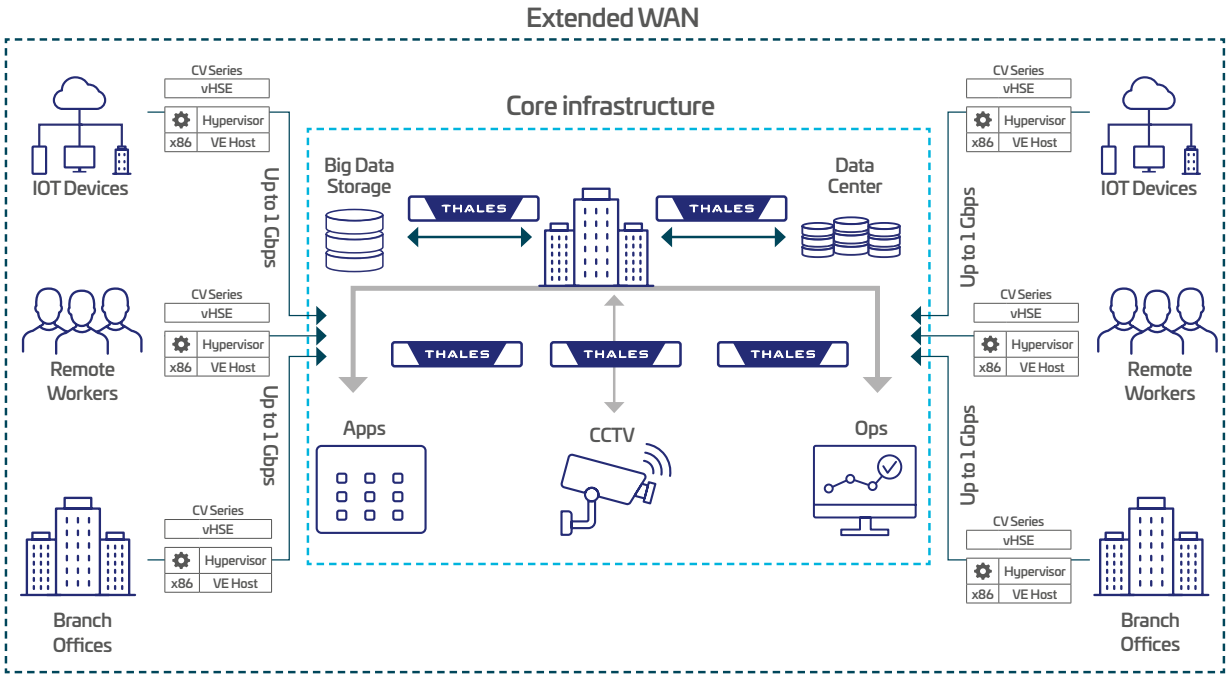
However, for extended WAN links and high-scale virtualized links that typically run at up to 5 Gbps, a virtual encryptor is likely to be a more flexible and cost-effective solution.

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' centralised 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.

Versatility

Crypto Agility

All Thales encryptors are crypto-agile; from 100% compatibility and interoperability to customizable 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 CM7 management software.

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.

Efficiency

Cost Effectiveness

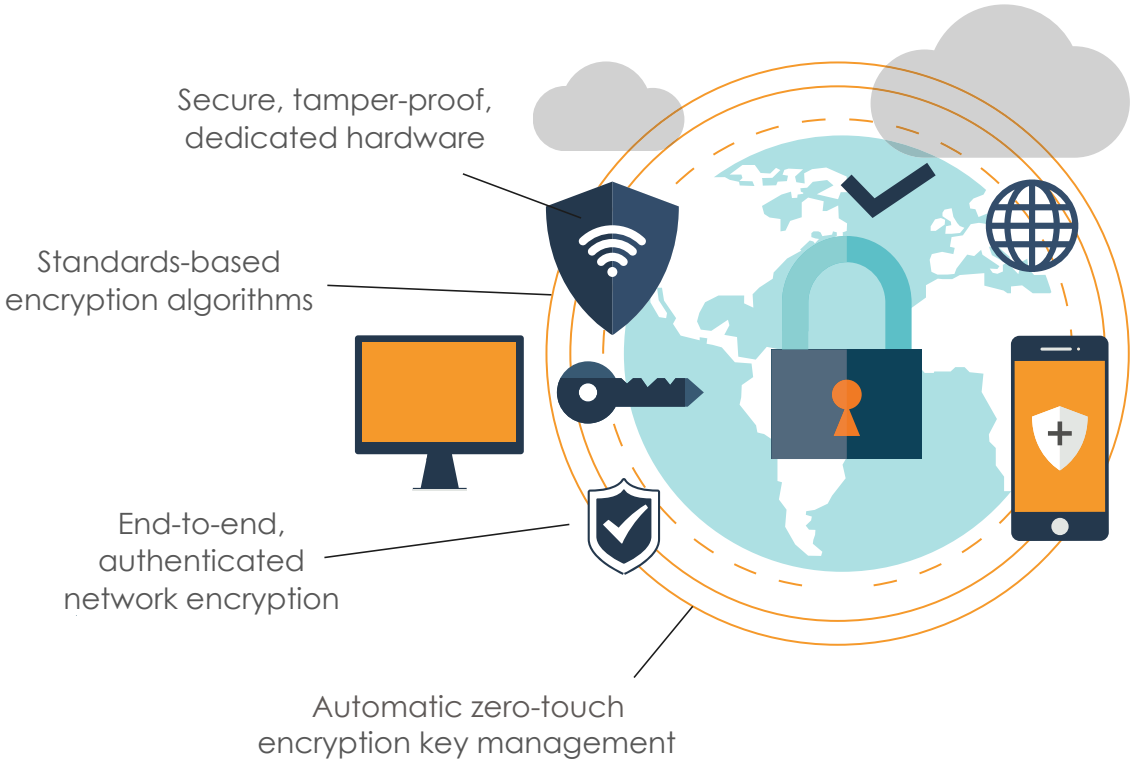
Thales encryptors provide excellent TCO through a mix of network bandwidth savings, ease of management and longevity.

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:

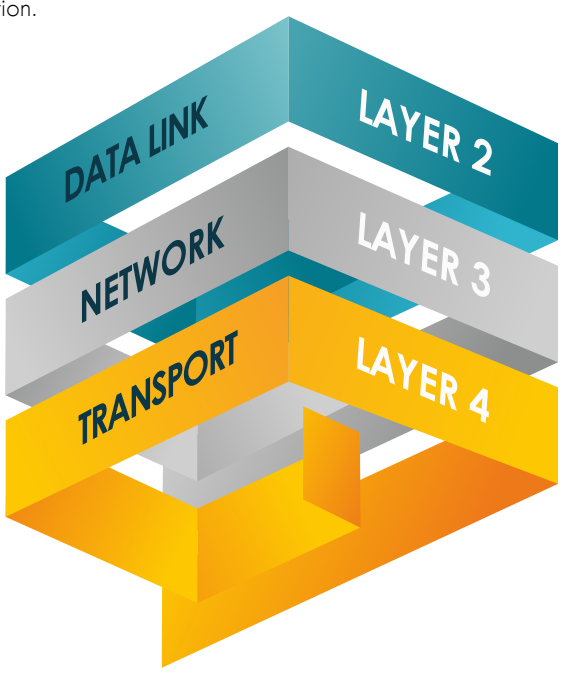
- Secure, tamper-proof hardware; dedicated to network data encryption
- State-of-the-art, client-side, zero-touch encryption key management
- End-to-end, authenticated encryption
- Use of standards-based encryption algorithms

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; the industry's leading centralized key management platform.

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 15Gbps

Data Plane Development Kit (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

SureDrop encrypted file-sharing

No matter where or how the people in your organization work, there is always the need to share and sync files - both internally and externally.

While you want to enable collaboration, data security should always be the first priority. If it's not, the risk of non-compliance and data breaches become a serious problem.

Our customers have been telling us that their mobility and productivity initiatives are frustrated by insufficient levels of security delivered by existing box style file collaboration and sync and share solutions.

While many are user friendly, elegant and effective, they're simply not safe enough.

Thales provides SureDrop to deliver state-of-the-art, standards-based encryption algorithms, key management and 100% file control security - without comprising your user experience.

In design, features and functionality, SureDrop solves the security issue of convenient file-sharing and synchronization, to the highest standards required by governments and large enterprises.

Key benefits

- Available on-premises or from the Cloud
- 100% control over data sovereignty
- Unlimited file size and types
- Standards-based encryption
- Effortless management and control

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

Contact us

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

> cpl.thalesgroup.com <