THALES

thalesgroup.com

Encrypt Everything

A Practical Guide on How to Protect Your Organization's Sensitive Data

Contents

Overview

As an enterprise-wide data security expert, you are being asked to protect your organization's valuable data by setting and implementing an enterprise-wide encryption strategy. But critical data is flowing everywhere. The boundaries are long gone. Data is going from operational to analytical systems, from on-premises to cloud, and from databases to data lakes. The data world is changing faster than ever before; new technologies including big data and micro services are being adopted in multiple ways all at once.

Data security is about the data, not the application, the database, the cloud, the data lake, or any other particular program. What's needed is a holistic data security platform, including a comprehensive portfolio of protection methods and enforcement mechanisms, to protect your most valuable data assets no matter where they reside across the enterprise and beyond. This eBook provides an overview of methodology and best practices that can be used to define and apply data security policies to protect your most critical data assets.

Data security challenges

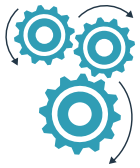
There are four overriding data security challenges:

Explosive data growth

Enterprises of every size and in every industry around the globe are producing more data than ever before. At the same time, there is a greater demand for access to this information. From business intelligence and marketing teams, to partners and third-party vendors, everyone wants their eyes on the data to reduce costs, improve efficiency, develop new products, optimize offerings, and make smarter, data-driven business decisions. To meet these demands, data will need to be produced, stored, and processed in, and shared and distributed to, more places.

New compliance requirements

In response to the evolving global threats targeting personally identifiable information (PII), an increasing number of compliance mandates now aim to strengthen the protection of sensitive data controlled and processed by enterprises. These include the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), Brazil's Lei Geral de Proteção de Dados (LGPD), and more. But organizations need guidance on how to address specific requirements to align with these regulations and industry mandates,
such as PCI DSS.



Operational complexity

Movement to cloud, containers, big data technologies, and disparate tools from multiple vendors adds to complexity. With enterprise security perimeters becoming increasingly blurry, organizations are having difficulty affording, implementing, and managing consistent, unified access policies to distributed IT resources. Every organization has a mix of legacy and new platforms. But data is data, regardless of the silos in question, and sensitive data lost is still sensitive data lost, regardless of where it happened to reside.

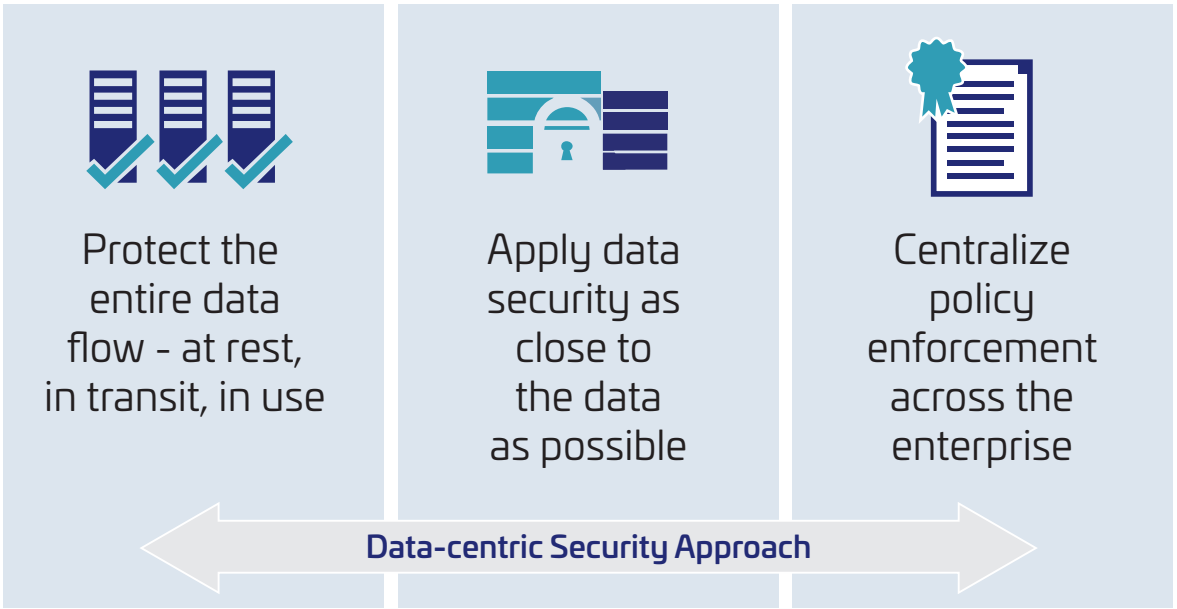
Rapidly increasing threats

From lost business to regulatory fines and remediation costs, data breaches have far-reaching consequences. Defending against data threats is an extremely challenging undertaking—no argument there. A host of new and evolving data security threats involving malware, phishing, machine learning, cryptocurrency and more have placed the data and assets of enterprises, governments and individuals at constant risk.

How to address these data security challenges

A data-centric security approach is integral to virtually every worldwide data compliance regulation and standard, and is a foundational best practice. The defining characteristic of data-centric security is that protection is applied to data itself, independent of the data's location.

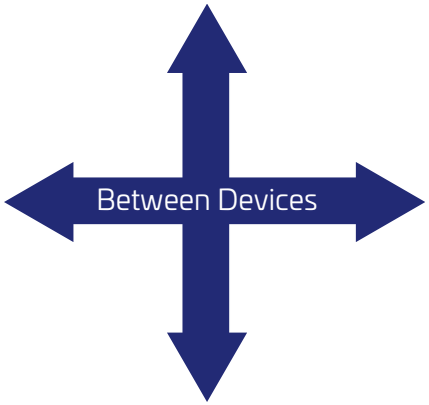
Unfortunately, most data security technology focuses on protecting where data is, rather than the data
itself—for example, protecting all the data stored on a specific laptop or server, or all the data that crosses a specific network. The problem with this approach is that as soon as data moves somewhere else, another solution is required, or data is left unprotected.



Data-centric security, on the other hand, focuses on what needs to be protected—the files containing sensitive information—and applying the appropriate form of protection no matter where the data happens to be. To be effective, this must happen automatically; sensitive information should be identified as soon as it enters an organization's IT ecosystem and should be secured with policy-based protection that lasts throughout the data lifecycle.

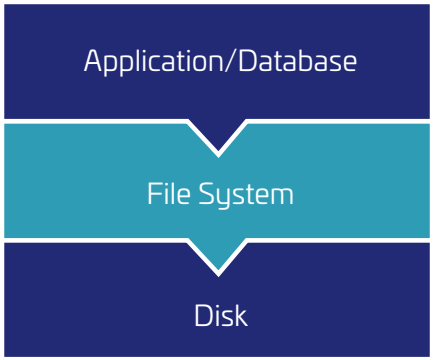
Data can be exposed to risks both in transit and at rest and requires protection in both states. As such, there are many approaches to protecting data in transit and at rest. Encryption plays a major role in data security and is a popular tool for securing data both in transit and at rest. For securing data in transit, enterprises often choose to encrypt sensitive data prior to moving it and/or use encryptors to protect the contents of data-in-transit. For protecting data-at-rest, enterprises can simply encrypt sensitive data in files and databases prior to storing them and/or choose to encrypt the storage drive itself.

Data-in-Motion



SSI, SSH, HTTPS,
IPSEC, Layer 2

Data-in-Rest



Data Encryption, Tokenization,
Data Masking

Once an organization uses encryption technologies to safeguard its data, enterprise security then depends on encryption key and policy management —the ability to generate, distribute, store, rotate, and revoke/destroy cryptographic keys as needed to protect the sensitive information with which they are associated. Best practice data security solutions using cryptography include strong key management and a separation of duties between the systems applying that data protection and those performing key management. Good key management systems will also provide the ability to leverage a hardware-based root of trust for key creation and storage.

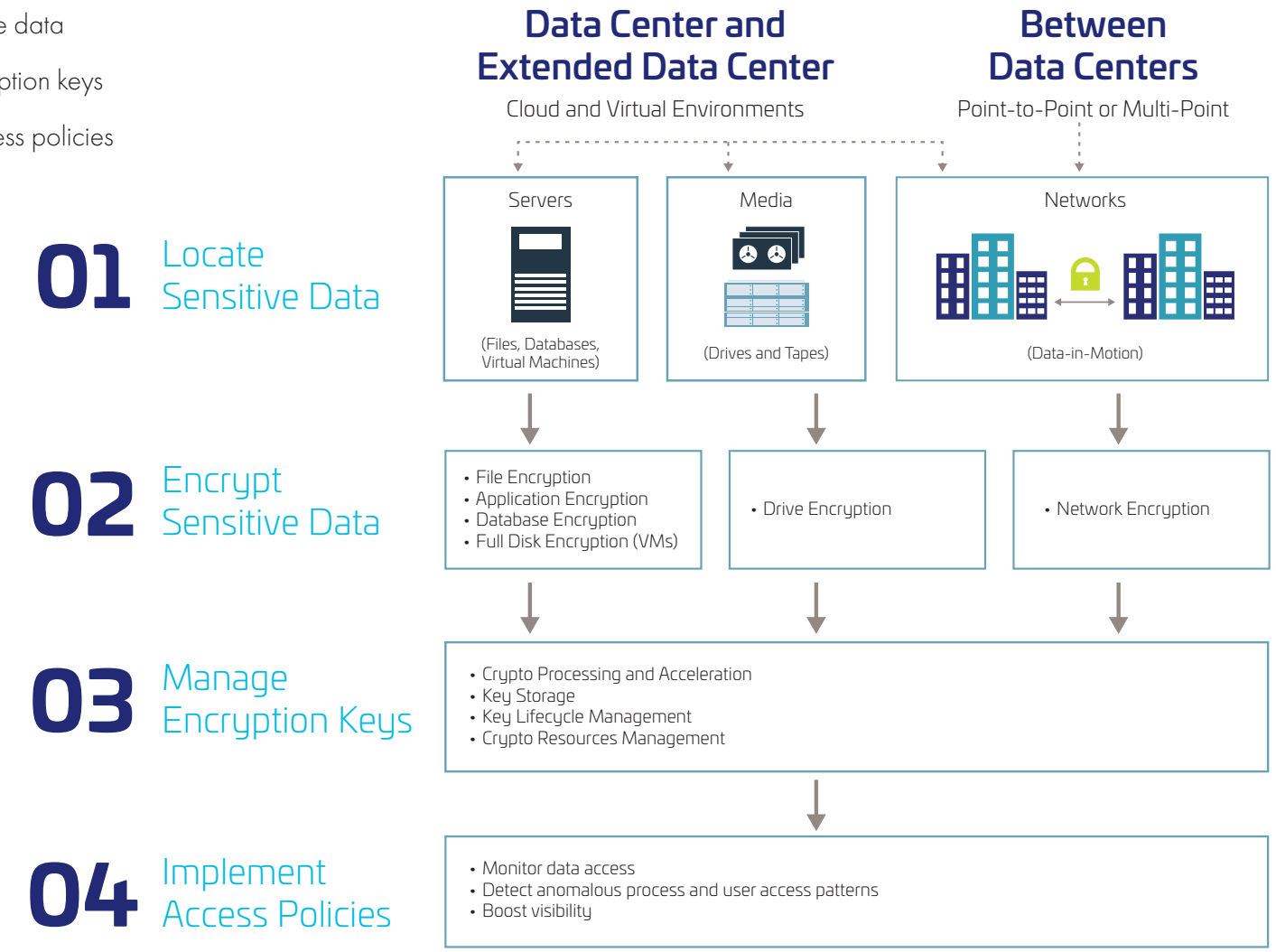
When properly implemented, data-centric security gives the organization complete control over its sensitive data from the moment that each file or database record is created. Access to protected data can be granted or revoked at any time, and all activity is logged for auditing and reporting.

In order to properly execute your data-centric security approach, it's important to note the encryption and data protection methods that are available, the requirements, the applications or data to be protected, and the reasons for applying the chosen protection method. Choosing a vendor with the broadest solution set available, and one that provides centralized key and policy management, will provide easier deployment and management controls when you grow your installed base.

How to approach enterprise-wide data protection

There are four common steps to follow when approaching enterprise-wide data protection:

1. Locate sensitive data
2. Encrypt sensitive data
3. Manage encryption keys
4. Implement access policies



Start by identifying where your most sensitive data assets reside in your on-premises data center and then move to your extended data center (cloud and virtual environments). Search your storage and file servers, applications, databases and virtual machines. Don't overlook the traffic flowing across your network and between data centers. Once this data leaves the confines of your organization, you no longer have control over it.

Next, use a data-centric security solution to encrypt it. Fortunately, the technology to encrypt data at scale, and in a centralized way that does not disrupt the flow of business, is a reality with today's enterprise-ready solutions.

And don't forget the keys. By managing and storing your keys centrally, yet separate from the data, you can maintain ownership and control and streamline your encryption infrastructure for auditing and control.

Effective data security can be a critical differentiator for today's digital businesses. Data is at the heart of almost every organization, and keeping it protected while also facilitating effective usage to drive business value is a key success factor.

What constitutes effective data security?

The best data security solutions will provide an integrated suite of data protection capabilities, which allow organizations to gain greater visibility, use actionable insights, enforce real-time controls, and automate compliance support throughout the data protection journey. Some of the critical data protection capabilities are those in the diagram below:

Data discovery

Data discovery is the process of obtaining actionable information by finding patterns in data from multiple sources with interactive visual analysis. The term is used to express a mode of analysis in which users attempt to get a holistic view of all their data sources, determine where data resides, and discover databases or file sources in their network that potentially contain sensitive or regulated data.

Data classification

Data classification is broadly defined as the process of organizing data by relevant categories so that it may be used and protected more efficiently. Parse discovered data sources to determine the kind of data they contain, matching against a predefined set of patterns or keywords. Then, assign labels based on the data type to inform policies. Data classification is of particular importance when it comes to risk management, compliance, and data security.

Data obfuscation

The essence of data-centric data protection is that the data has its own defense. This happens by making the data unintelligible without the tools necessary to make them intelligible again, and then isolating those tools from the data and carefully controlling access to the tools. Encryption and tokenization are means to make the data unintelligible, and key management is the process of isolating and protecting the tools necessary to make the data intelligible again.

Key management

Encryption key management is administering the full lifecycle of cryptographic keys and protecting them from loss or misuse. The lifecycle includes: generating, using, storing, archiving, and deleting keys. Protection of the encryption keys includes limiting access to the keys (physically, and through user/role access), securely distributing keys across complex encryption landscapes, centralizing key management, and enabling organized, secure key management that keeps data private and compliant (FIPS).

Encryption

Data encryption translates data into another form, or code, so that only people with access to a secret key (formally called a decryption key) or password can read it. Encrypted data is commonly referred to as ciphertext, while unencrypted data is called plaintext. Currently, encryption is one of the most popular and effective data security methods used by organizations. Two main types of data encryption exist: asymmetric encryption, also known as public-key encryption, and symmetric encryption.

Tokenization

Tokenization is the process of turning a meaningful piece of data, such as an account number, into a random string of characters called a token that has no meaningful value if breached. Tokens serve as reference to the original data but cannot be used to guess those values. That's because, unlike encryption, tokenization does not use a mathematical process to transform the sensitive information into the token.

Cloud Security

An enterprise-ready encryption solution should enable you to maintain control and ownership of your data and encryption keys not only on-premises, but also across virtual, public cloud, and hybrid environments. Cloud security varies greatly depending on the cloud provider and deployment model you use. Broadly speaking, there are three options as shown below:

- **Bring your own encryption and centralized key management:** This allows you to secure your sensitive data across your hybrid world with maximum control, visibility, and portability. It is agnostic to clouds, vendors, and location, giving you the flexibility to unify security for operational simplicity and compliance.
- **Cloud encryption services with Bring Your Own Key:** To comply with best practices regarding encryption key management, most mainstream IaaS/PaaS providers offer Bring Your Own Key (BYOK) Application Programming Interfaces (APIs) with some offering Hold Your Own Key (HYOK). In a multi-cloud environment with unique BYOK API's, you are likely to need additional tools to manage BYOK encryption keys.
- **Utilize native encryption services:** These are unique to a cloud service provider and completely managed by them. Depending on your risk profile and sensitivity of data, you may need to complement these services with additional tools for visibility, control
and portability.

Encrypt Everything Strategy

As we've discussed, internal and external risks and threats to your information are growing every—in scope, volume and impact. So, while your organization is under increasing pressure to stay competitive and compliant with new regulations, the ultimate goal is to protect the organization's data. Protecting the digital enterprise is more than protection from cyber-threats, it also includes the confidentiality, integrity and availability of your data.

While no organization is immune to the threat of security breaches, implementing data encryption is a major safeguard that will protect information assets and your organization's reputation. Most organizations agree that encrypting sensitive data, particularly data-at-rest, is a solid data protection strategy. But there is a fallacy in that approach.

First, there is far more data than ever before, and it continues to be created at an astounding rate. Often it is presumed that encryption is a painful endeavor, so it is restricted only to the most valuable information assets. This leads to the problem of data classification. Without data classification, you don't know where that sensitive data sits, what interacts with it, or what that data represents to your organization in terms of worth and determining risk. But what constitutes "sensitive?" Not everyone agrees on what "sensitive" means, so organizations have to spend time and energy defining what "sensitive" means for them. This takes a lot of time and resources to implement.

This is no longer the case. In the past, pervasive encryption was largely abandoned, because it was too expensive in time, in its computational requirements, in its space requirements, in its operational efficiency, and in its management and overall ease of use. These technological challenges led to the practice of encrypting only sensitive data. But nearly all of these obstacles have been removed and solved, clearing a path to a simpler, cost-effective encrypt everything strategy
for CSOs.

Encrypting all of your data ensures that you are always in compliance with various regulatory standards and requirements, as data moves around in the organization and even between on-premises and in the cloud. Just as important, an encrypt everything approach can protect your organization's brand and reputation. Most experts agree that nearly every organization will suffer a data breach at some point – it's a matter of "when", not "if", you'll be attacked. Imagine the peace of mind (and risk reduction) in knowing that any data siphoned out of your organization is encrypted and therefore worthless to the cybercriminal who stole it. Most compliance standards maintain that if your data is encrypted, publicly reporting breached data is not required. Your peers who stick with a sensitive only approach to encryption will need to spend cycles determining if the breached data was sensitive, and if it was encrypted. If it was not, they will have to report the breach publicly. The damage will extend to the company's brand and reputation in the eyes of customers, partners, potential employees and other stakeholders.

Very smart people at very smart companies have come to the conclusion that encrypting a vast majority of their data is one of the best things they can do to reduce risk and assuage customer fears. While no company or CEO wants to discuss a data breach, having a broad-based strategy to make data protection a priority plays well from both a security and marketing perspective.

An encrypt everything strategy ensures that all data is encrypted and protected by strong access controls such that only those persons with a business need to know have access to intended data and only to intended data. Privileged users can be blinded from enterprise data with access only to the metadata, removing the need for data classification. And CSOs are able to assess risk differently by maintaining, modeling and providing access to data in a completely new and different way.

THALES

thalesgroup.com

How Thales can help you secure your data

Thales provides the solutions you need to keep sensitive data-at-rest and data-in-motion safe, even in the event of a breach. With Thales, you apply data protection where you need it, when you need it, and how you need it—according to the unique needs of your business.

Companies, governments and organizations rely on Thales to protect their most sensitive data. Our advanced data encryption, key management, tokenization and hardware security module solutions enable customers to secure digital payments, achieve compliance, and protect and remain in control of their data wherever it resides – across the cloud, data centers, networks and hybrid IT environments.

As described above, there are many techniques and methods that can be used to deploy an encrypt everything strategy, and there may be no "one size fits all" technique, but having the options available on a single unified platform makes it easier for you to secure your data today and in the future.

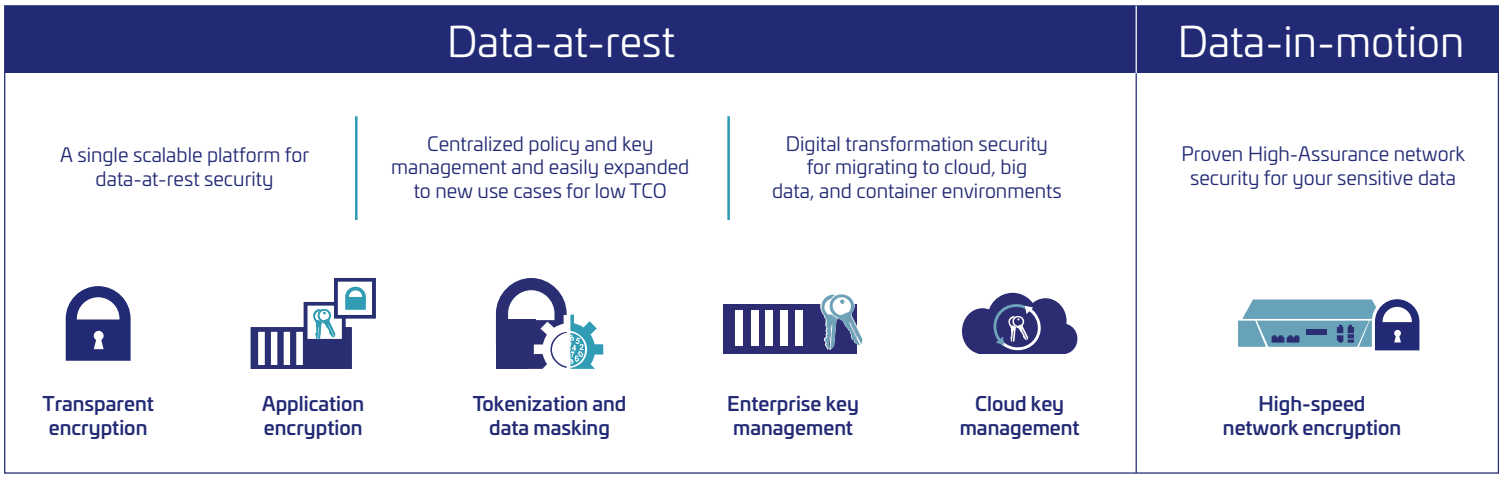
Industry-leading Data Security Solutions from Thales

Thales portfolio of data-at-rest security solutions delivers unmatched protection — securing databases, applications, file servers, and storage in your on-premises, cloud, and virtual environments. The Vormetric Data Security Platform makes it easy and efficient to manage data-at-rest security across your entire organization. Built on an extensible infrastructure, the platform features multiple data security products that can be deployed individually or in combination to deliver advanced encryption, tokenization and centralized key management. This data security solution prepares your organization for the next security challenge and new compliance requirement at the lowest TCO.

In order to protect keys, our industry-leading cloud, general purpose and payment hardware security modules provide the root of trust that protects the cryptographic functions and infrastructure for the most security-conscious organizations in the world.

In addition to our data-at-rest security solutions, Thales offers a range of SafeNet High Speed Network Encryptors to protect sensitive data as it moves across networks at speeds up to 10 Gbps.

This holistic approach means you can meet your immediate data protection needs now, while investing in a solution that provides robust security, a growing ecosystem, and the scalability you need to build a trusted framework for the future.



Summary

Organizations that want to survive and thrive in this age of digital transformation need every advantage they can get: top talent, top strategies, and of course, top technology. Technology, after all, has helped make business transactions faster, more transparent and more efficient. Big data, cloud computing, the "Internet of Things," robotics, bots and other forms of artificial intelligence are all technologies that your organization is probably considering or reviewing, if they are not already in use.

These technologies also blur or eliminate traditional enterprise perimeters, and present new conduits for cyberattacks as attackers simultaneously are becoming more sophisticated. We live in a world of malware, ransomware, spear phishing, insider threats, nation-state attacks, APTs, SQL injections, and social engineering.

There are no "magic bullets" to protect against this reality, but if CSOs and CISOs "follow the money" and focus on an encrypt everything approach to data protection, they can become enablers for new business and technology use while protecting the data entrusted to them by stakeholders, and the reputations and financial strength of the organizations they serve.

With data security solutions from Thales, you can cost-effectively and efficiently manage data-at-rest and data-in-motion security across your entire organization.

THALES

Americas
Arboretum Plaza II, 9442 Capital of Texas Highway North,
Suite 100, Austin, TX 78759 USA
Tel: +1 888 343 5773 or +1 512 257 3900
Fax: +1 954 888 6211 | E-mail: sales@thalesesec.com

Asia Pacific – Thales Transport & Security (HK) Ltd
Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East
Wanchai, Hong Kong | Tel: +852 2815 8633
Fax: +852 2815 814 | E-mail: apacsales.cpl@thalesgroup.com

Europe, Middle East, Africa
350 Longwater Ave, Green Park,
Reading, Berkshire, UK RG2 6GF
Tel: +44 (0)1844 201800 | Fax: +44 (0)1844 208550
E-mail: emea.sales@thales-.com

> thalesgroup.com <