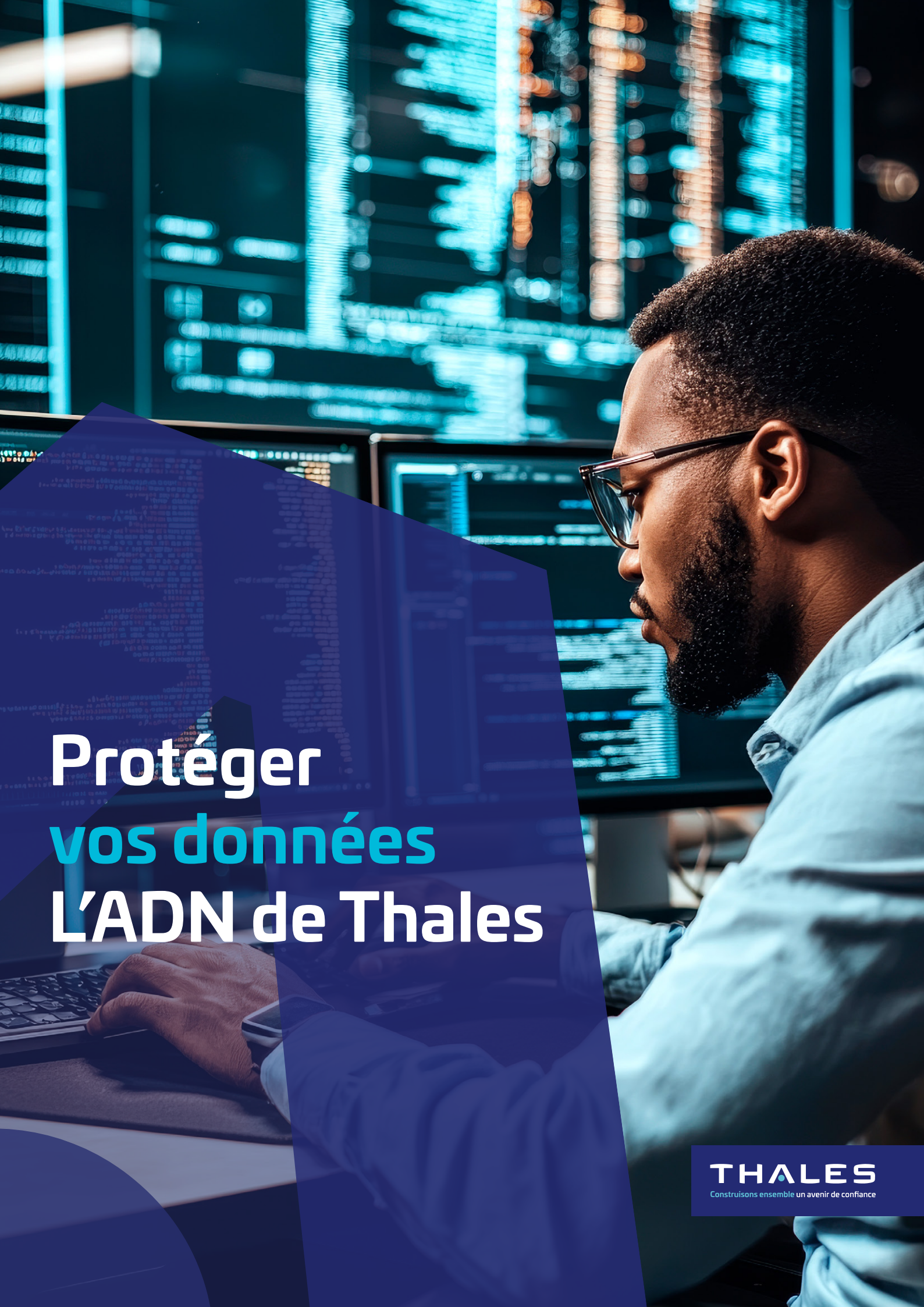


Protéger vos données L'ADN de Thales

THALES
Construisons ensemble un avenir de confiance

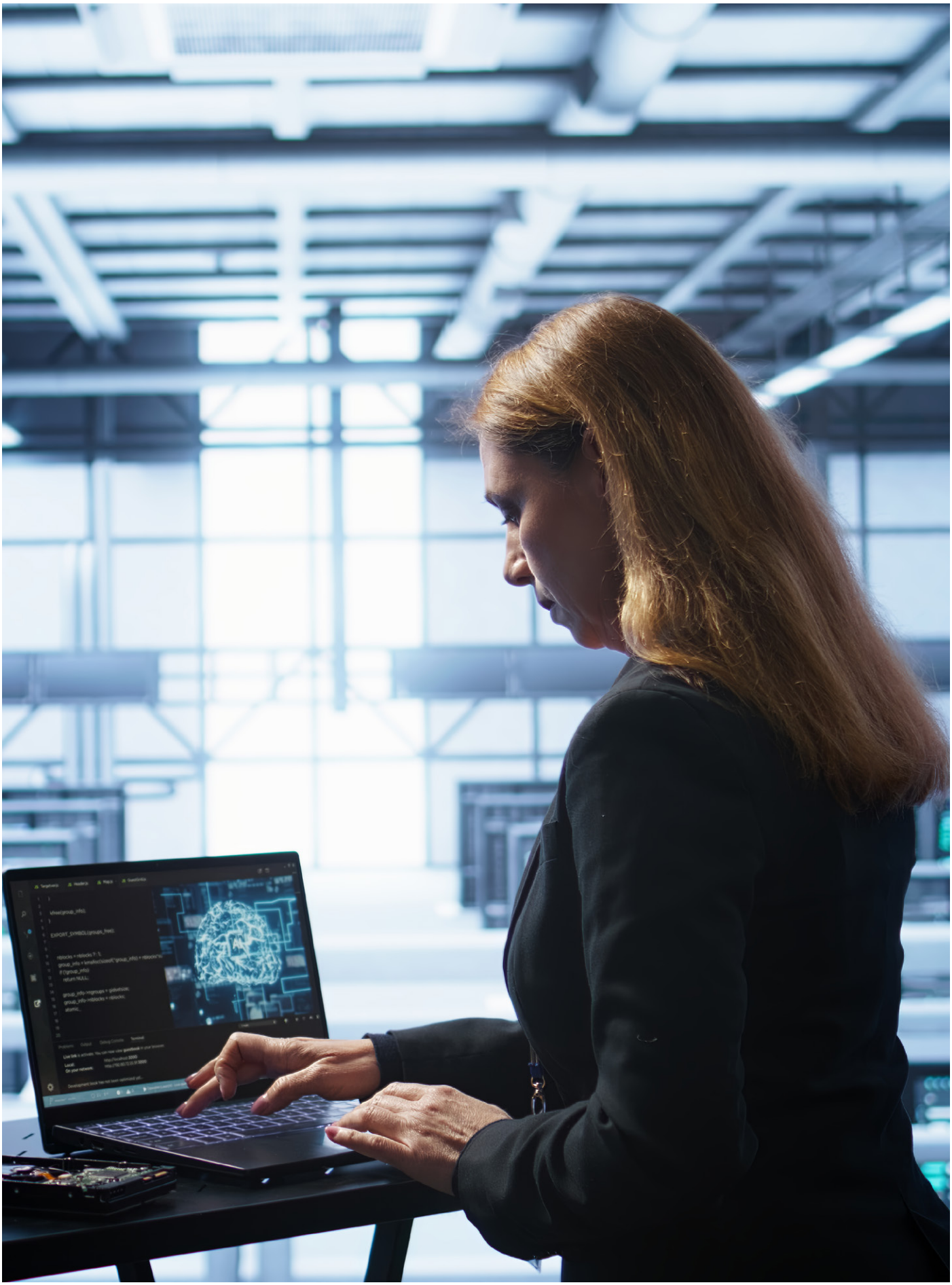
Notre siècle est résolument porté par le numérique. Mais une révolution n'apporte jamais que des opportunités, elle soulève aussi de nouveaux risques. Les cybermenaces aujourd'hui.

En 5 ans, la croissance et la professionnalisation de la cybercriminalité ont naturellement conduit les organisations publiques et privées à se protéger davantage. Partout dans le monde, et en Europe en particulier, la réglementation s'est aussi durcie pour protéger les données personnelles et sensibles.
Mais les attaquants se renouvellent vite. Dans son panorama de la cybermenace 2023, l'ANSSI souligne notamment que « l'écosystème cybercriminel profite aujourd'hui d'outils et de méthodes diffusés largement pour cibler des secteurs particulièrement vulnérables ». Et son directeur général, Vincent Strubel, insiste :

> «l'un des grands enseignements de ce Panorama est qu'il n'est désormais plus possible de prendre du retard en matière de cybersécurité, face à des attaquants de plus en plus persévérants».

> Néanmoins, l'évolution rapide des usages numériques et les promesses de l'IA et des IA génératives que testent déjà nombre d'entreprises dans le monde font que les outils de la cybersécurité doivent eux aussi toujours évoluer, ce sans constituer un frein à l'agilité et à la performance économique. Les entités doivent donc pouvoir compter sur des experts aguerris et sensibles à leurs contraintes métiers.

Fort de 40 ans de recherches et de réalisations en matière de protection des identités et des données, Thales a donc plus que jamais à cœur de leur fournir des solutions robustes mais simples, et une approche d'anticipation et d' innovation en mesure de garantir des stratégies de protection durables face aux cybermenaces.



1
Contexte et défis de la protection des données

Réglementations et conformité

Face à l'accroissement des volumes de données en circulation et au renouvellement continu des cybermenaces, le contexte règlementaire et normatif s'est durci pour armer les entreprises et protéger leurs ressources ainsi que celles de leurs clients, prestataires et partenaires.

> Adopté en 2016 par l'Union européenne, le **RGPD** encadre le traitement des données personnelles sur le territoire de l'Union européenne. Il a eu le grand mérite de sensibiliser les entreprises et le grand public depuis la notion de donnée personnelle jusqu'aux enjeux relatifs à leur protection.

> À l'échelle mondiale, **les normes ISO/IEC 27001** Gestion de la sécurité de l'information et **ISO/IEC 27002** Contrôles de la sécurité de l'information ont évolué depuis leur première publication en 2005 et mis en avant l'importance de la séparation des données et des tâches ou **Segregation of Duties (SoD)** en anglais. Elles exigent ainsi des organisations que dans le cadre des processus d'exploitation des Services, des personnes différentes exécutent des procédures différentes afin qu'aucune n'ait le contrôle sur l'ensemble du processus.

> Dernière obligation majeure en la matière, **l'arrêté SCHREMS II**, rendu le 16 juillet 2020 par la Cour de justice de l'UE, invalide le régime de transferts de données entre l'Union européenne et les Etats-Unis. Il contraint donc les organisations transférant des données vers les Etats-Unis, celles opérant dans les clouds publics des grands CSP AWS, Google Cloud ou Azure par exemple, à des mesures de chiffrement et d'anonymisation de leurs données par exemple.

Depuis, la ségrégation des rôles et la maîtrise souveraine des clés de chiffrement se sont donc imposées parmi les leviers indispensables en matière de protection face aux cybermenaces. Ils font notamment partie des best practices publiées par la Cloud Security Alliance (CSA).
De leur côté, les fournisseurs de cloud européens sont très attentifs aux délibérations sur le projet de système européen de certification de cybersécurité sur les services cloud (EUCS), projet en cours depuis décembre 2019. Dans une récente lettre, ils s'inquiètent de la possibilité évoquée de supprimer toute référence aux dispositions relatives à la souveraineté du régime principal (y compris en cas de passage à une attestation internationale de profil d'entreprise (ICPA), ce qui contredirait les exigences de protection des données les plus sensibles des organisations européennes et le fait de favoriser le développement de solutions cloud en Europe.

L'IMPACT

L'impact de ces réglementations sur les entreprises n'est donc pas anodin. À chaque fois, elles sont dans l'obligation de mettre en œuvre des analyses, des réorganisations et des solutions adaptées de chiffrement et de gestion des clés, alors que, souvent, la cybersécurité au sens large, ne constitue pas leur cœur de métier.

Adoption du cloud et maîtrise des données

L'évolution des réglementations et des normes n'intervient pas hors contexte. C'est bien l'accroissement des usages numériques et les risques associés qui la justifient.

94%

des entreprises utilisent au moins un service de Cloud Computing.

À cet égard, on assiste notamment à un mouvement accéléré des applications des entreprises vers le cloud ou plutôt vers les clouds : cloud public, cloud privé, cloud hybride ou encore multicloud. Selon le dernier rapport « State of Cloud », 94 % des entreprises utiliseraient au moins un service de Cloud Computing. Une adoption massive qui s'explique par les avantages de flexibilité, d'évolutivité, d'agilité ou encore d'accélération de déploiement de services IT permis par le cloud.

PRUDENCE

Néanmoins, parce que le move to cloud engendre un déplacement des données, des applications, des capacités de calcul ou encore de ressources numériques, il faut aux entreprises s'organiser et se doter de solutions leur permettant d'avoir une gestion fine et dynamique de leurs données afin de les maîtriser partout et tout le temps. L'arrêt Schrems II ou les conseils de la Cloud Security Alliance le rappellent. C'est d'autant plus vrai dans les environnements multicloud qui accroissent la complexité et la difficulté pour sécuriser les workloads cloud.

Menaces émergentes

Face à l'accroissement des volumes de données en circulation et au renouvellement continu des cybermenaces, le contexte règlementaire et normatif s'est durci pour armer les entreprises et protéger leurs ressources ainsi que celles de leurs clients, prestataires et partenaires.

« La résistance quantique est déjà présente »

DISCUSSION AVEC NICOLAS ANEAS, REGIONAL PRE-SALES MANAGER CHEZ THALES

LE PAYSAGE DE LA CYBERCRIMINALITÉ NE CESSE D'ÉVOLUER AVEC L'APPARITION D'ATTAQUES DE PLUS EN PLUS SOPHISTIQUÉES. QUELLE MENACE VOUS SEMBLE DEVOIR ÊTRE SURVEILLÉE POUR LES ANNÉES À VENIR ?

Parmi les tendances émergentes à considérer dès aujourd'hui, il y a la résistance quantique ou la gestion de la menace quantique. Cette menace est déjà bien identifiée en réalité. Quand l'ordinateur quantique sera abordable et à la portée d'un plus large public, il permettra de produire des attaques autrement plus puissantes et insidieuses que celles que nous connaissons aujourd'hui.

À QUELS TYPES DE CYBERATTAQUES PEUT-ON S'ATTENDRE ?

Nous en identifions principalement deux. La première s'appuie sur la logique « **Store now, decrypt later** », c'est-à-dire qu'elle va consister à stocker aujourd'hui des données volées mais cryptées pour demain les déchiffrer grâce à la puissance de calcul quantique. Aujourd'hui des pirates sont donc déjà certainement en train de collecter et d'archiver des données dans l'attente d'avoir la bonne puissance et les bons algorithmes pour y accéder et les utiliser à des fins malveillantes.

Et nous pouvons craindre des attaques sur l'intégrité et l'authenticité de document dont la validité à long terme doit être assurée. Je m'explique : on sécurise aujourd'hui ce type de document par des signatures électroniques effectuées avec des clés cryptographiques qui demain pourraient être compromises par la puissance de calcul quantique et permettre donc de forger de nouvelles signatures valides sur des documents falsifiés volontairement.

Ces menaces sont réelles et nous imposent de travailler dès aujourd'hui à une transition post quantique, d'évaluer, si ce n'est pas déjà fait, les environnements les plus à risques et définir les stratégies de migration ou d'hybridation vers le post-quantique.

Top 10 OWASP des menaces IA dans le cadre des applications LLM

Les progrès rapides de l'IA générative, lesquelles s'appuient sur le Large Language Model (LLM), conduisent aussi à une évolution des risques qu'il est nécessaire d'anticiper pour disposer d'une cyber-protection à la hauteur.

C'est en ce sens qu'a été conduit le projet **OWASP Top 10 for Large Language Model Applications.** Il vise à sensibiliser :

Développeurs Concepteurs Architectes Gestionnaires Organisations

aux risques de sécurité potentiels lors du déploiement et de la gestion de Large Language Models (LLM). Le projet fournit notamment une liste des 10 vulnérabilités les plus critiques souvent observées dans les applications LLM, soulignant leur impact potentiel, leur facilité d'exploitation et leur prévalence dans les applications du monde réel.

EXEMPLES

Parmi cette liste figurent par exemple :

- **les injections rapides,**
- **les fuites de données,**
- **l'empoisonnement des données d'entrainement,**
- **le sandboxing inadéquat**
- **l'exécution de code non autorisée.**

L'objectif est de sensibiliser à ces vulnérabilités, de suggérer des stratégies de remédiation et, à terme, d'améliorer la sécurité des applications LLM.

2

Chaque Cas d'usage client trouve ses solutions en fonction de son degré de sensibilité

Thales : expertise et offre globale à la pointe globale

Thales propose aujourd'hui à ses clients une offre complète pour les accompagner de bout en bout dans la protection de leurs données. Elle s'articule autour de 3 pilliers.

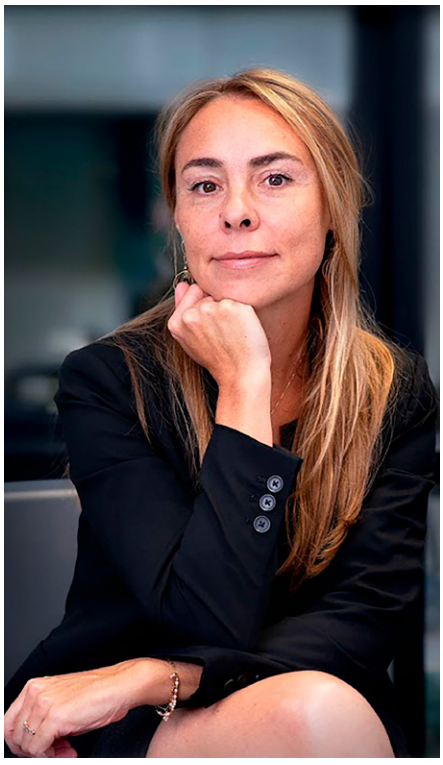
> Le conseil et l'accompagnement d'abord pour définir une roadmap de protection de la donnée pertinente par rapport à la sensibilité de l'entreprise, aider à son déploiement, et finalement sensibiliser les différentes équipes aux problématiques réglementaires et à la manipulation de données sensibles.

> Une Tool Box complète : Baptisé **CipherTrust**, le portefolio de produits développés par Thales propose des solutions à la pointe en matière de chiffrement des données et de gestion des clés de chiffrement et des identités. Ses Hardware Security Modules (HSM) ont été les premiers HSM validés FIPS 140-3 Level 3. De quoi protéger la donnée dans tous ses états : au repos, en cours de traitement, en transit, mais aussi offrir des solutions d'externalisation des clés de cryptage. Ainsi faisant, les clients s'appuyant sur des CSP américains seront en mesure de générer et gérer des clés de chiffrement en totale indépendance de manière à garantir la bonne ségrégation des rôles et une maîtrise souveraine de ces clés.

«Cette offre se structure autour de plusieurs axes dont un important qui est l'axe réglementaire.»

«Qu'est-ce qui est exigé aujourd'hui par la loi ? Qu'est-ce que je dois protéger et comment je m'y prends ? Nous accompagnons donc les entreprises pour cartographier leurs données et déployer une roadmap de protection de la donnée de A à Z, laquelle inclut toute la partie opérationnelle, et donc l'accompagnement au changement des équipes. Notre objectif est clair : mettre en place dans chaque entité que nous accompagnons un framework de protection de la donnée robuste et de bout en bout.»

MARCIA RODRIGUES LOPES, DIRECTRICE DES OFFRES DATA PROTECTION POUR LES ACTIVITÉS NUMÉRIQUES DE THALES

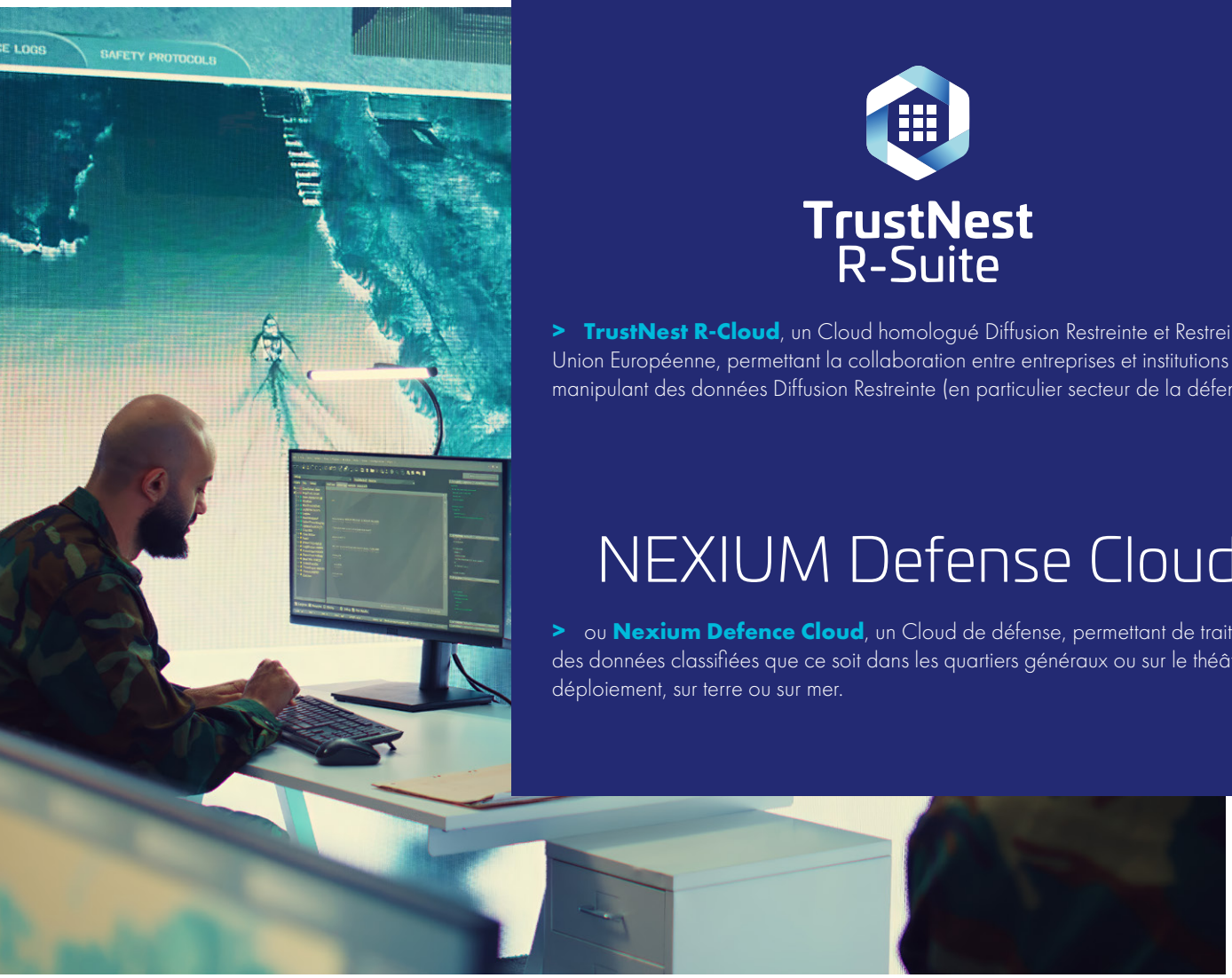


> Une offre de services managés inédite, pour une gestion optimale de la criticité : l'offre de services managés de Thales a été construite pour que les entreprises puissent lui confier sereinement l'ensemble de la chaîne de protection de leurs données sensibles. Les équipes du **Thales Service Center**, rodées aux outils de la **suite CipherTrust** et coutumières de la gestion de dispositifs critiques, gèrent tout à partir d'outils installés dans les datacenters français du groupe. Ce **service plug & play** est unique sur le marché et a déjà séduit nombre de clients, notamment ceux œuvrant dans des secteurs critiques comme l'Assurance.

Cloud sécurisé : un partenariat innovant

Thales en tant qu'intégrateur de ses solutions accompagne aussi des clients qui sont plus tournés vers des problématiques de protection de la donnée packagée sur des environnements comme des cloud de confiance.

Thales aujourd'hui, à l'instar de ce qui est fait d'ailleurs sur **CipherTrust**, est à l'origine de la création de **S3NS**, une joint-venture créée il y a quelques années entre Google Cloud et Thales. Cette offre cloud de confiance est entrée dans le processus de qualification SecNumCloud de l'ANSSI.
En matière de cloud sécurisé, Thales propose également à ses clients d'autres offres, parmi lesquelles :



TrustNest
R-Suite

> **TrustNest R-Cloud**, un Cloud homologué Diffusion Restreinte et Restreint Union Européenne, permettant la collaboration entre entreprises et institutions manipulant des données Diffusion Restreinte (en particulier secteur de la défense).

NEXIUM Defense Cloud

> ou **Nexium Defence Cloud**, un Cloud de défense, permettant de traiter des données classifiées que ce soit dans les quartiers généraux ou sur le théâtre de déploiement, sur terre ou sur mer.

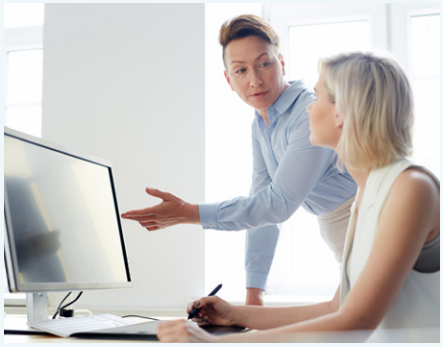
Flexibilité et adaptabilité : Cas d'usage spécifiques

Voici quelques exemples de cas d'usage des solutions mises en œuvre par Thales pour ses clients dans des secteurs aussi variés que les ressources humaines, la finance, ou la santé.

RH ET EXTERNALISATION DES CLÉS DE CHIFFREMENT

Une entreprise du secteur RH a fait appel à Thales pour se conformer à la législation européenne et l'arrêt Schrems II en particulier et rester conforme à la norme ISO 27 001. Conduite à manipuler des données de personnels très sensibles sur des environnements AWS, il lui fallait notamment garantir l'externalisation de ses clés de chiffrement et de la gestion de ces clés, et l'anonymisation de ces données.

> La sécurité n'étant pas le cœur de métier de cette entreprise, elle a choisi de déléguer entièrement la responsabilité de son dispositif de protection des données à Thales et fait le choix de son offre de services managés.



CLOUD HAUTEMENT SÉCURISÉ POUR LES ACTEURS DE LA FINANCE

Une entreprise du secteur financier souhaitait héberger son dispositif CIAM (Customer Identity and Access Management) dans un environnement Google Cloud afin de bénéficier des services proposés par ce grand cloud service provider.

> Thales a donc pu l'aiguiller vers l'offre S3NS de manière à profiter de l'agilité du cloud tout en sécurisant son système de gestion des identités et des accès, avec l'assurance d'œuvrer demain dans un cloud de confiance.

Microsoft 365

PROTÉGER LES DONNÉES SUR OFFICE 365

Thales apporte ses solutions de protection à de nombreuses entreprises dont les collaborateurs utilisent la suite Office 365 au quotidien. C'est notamment le cas dans le secteur pharmaceutique. Alors que Microsoft propose aujourd'hui une fonctionnalité de chiffrement baptisée DKE (Double Key Encryption), Thales vient renforcer la protection des données traitées sur les environnements Office 365 par un connecteur DKE au sein de sa plateforme Ciphertrust.

3
Vision et engagement futurs de Thales

Développement continu et R&D

La protection des données est une activité qui demande maturité et anticipation. Thales a donc fait de l'amélioration continue un crédo pour proposer une offre robuste et durable.

Le groupe se montre ainsi pro-actif pour assurer une veille approfondie sur les cybermenaces actuelles et en devenir, et développer des outils de protection à la hauteur des risques.

«Thales contribue notamment à la création d'algorithmes résistants aux menaces quantiques.»

NICOLAS ANEAS, REGIONAL PRE-SALES MANAGER CHEZ THALES.

Au sein d'un consortium d'acteurs réunissant notamment IBM, PQShield, NCC Group ou encore des mathématiciens de l'université Brown, Thales a ainsi co-développé l'algorithme Falcon. Algorithme qui a été sélectionné en 2022 par l'Institut des normes et de la technologie du ministère américain du Commerce (NIST) pour en faire un standard de signature numérique capable de résister aux futures cyberattaques quantiques.

En mars 2024, Thales a pris la tête d'un nouveau consortium dédié à la cryptographie post-quantique. Baptisé Resque et financé par le gouvernement, l'Union européenne et Bpifrance, ce consortium rassemble des PME, une start-up, mais aussi l'ANSSI et l'Institut national de recherche en sciences et technologies du numérique.

« La standardisation de ces différents algorithmes est essentielle pour une industrialisation globale et permettre ainsi la transition PQC, poursuit Nicolas Aneas. Cette standardisation s'achève pour les premiers algorithmes mais chez Thales, nous avons déjà anticipé et avons testé les algorithmes pré-sélectionnés par le NIST (dont l'algorithme Falcon) dans nos HSM (Hardware Security Modules). Nous proposons des Starter Kit de résistance quantique sur la base de nos équipements HSM et Chiffreur Réseaux afin que nos clients et partenaires puissent d'ores et déjà se familiariser et tester ces nouveaux algorithmes qui constituent les briques du futur de la cybersécurité. »

Thales travaille aussi de concert avec d'autres acteurs pour développer des cas d' usages basés sur le Confidential computing avec Intel et des clouds providers. L'objectif étant le chiffrement de bout en bout, en permettant à un client de s'assurer qu'il se trouve bien sur une machine confidentielle vérifiée, avant d'accéder à ses données sensibles auparavant chiffrées grâce à des outils Thales.

Expansion des services et solutions

Pour compléter aussi son offre de protection des données de bout en bout, Thales a validé plusieurs acquisitions ces deux dernières années.

En 2022, le groupe a notamment acquis l'européen One Welcome, acteur européen expert dans la gestion d'identités et des systèmes CIAM.

Fin 2023, il a aussi finalisé l'acquisition de l'américain Imperva, acteur reconnu pour ses capacités à sécuriser les end-points applicatifs. Thales complète ainsi l'étendue de son expertise en proposant des capacités de protection des applications qui mènent aux données, de protection des identités et de protection des données elles-mêmes.

OBJECTIF

L'objectif de Thales est aussi d'apporter des réponses adaptées à la complexité des environnements des entreprises pour simplifier et uniformiser leur processus de protection des données en évitant les silos sans rogner sur la robustesse et la performance de ses solutions.

Conclusion

Permettre à ses clients de remplir leurs missions et de protéger leurs ressources critiques fait partie des ambitions historiques de Thales.

Face au développement et à la croissance de la cybercriminalité, le groupe s'est donc naturellement investi dans la recherche de solutions de sécurité à la hauteur. Il veut aujourd'hui être le partenaire de confiance des entreprises dans la protection des données.

Thales s'en donne les moyens en continu. A travers des partenariats de recherche et d'affaires inédits, à travers le développement et l'expérimentation de nouvelles briques technologiques, à travers l'acquisition de compétences nouvelles, et bien sûr à travers l'accompagnement et la sensibilisation des entreprises, de leurs décideurs et de leurs collaborateurs. Car on ne peut construire un avenir de confiance sans écoute, sans partage et sans implication.

THALES

Construisons ensemble un avenir de confiance

19 Av. Morane Saulnier,
78140 Vélizy-Villacoublay
+33 (0) 1 57 77 80 00

thalesgroup.com