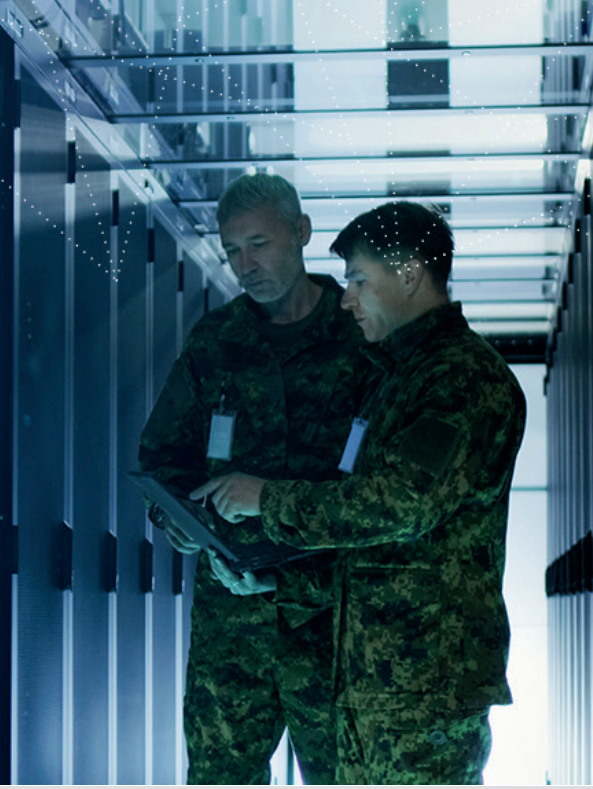
STORMSHIELD

CONFORMITÉ EN MATIÈRE DE CYBERSÉCURITÉ POUR LES ORGANISATIONS DU SECTEUR DE LA DÉFENSE



Les organisations militaires, les ministères de la Défense et les forces armées nécessitent une protection particulièrement puissante pour leurs systèmes d'information. À l'heure actuelle, la guerre cybernétique est étroitement liée à la sécurité nationale, et la meilleure attaque nécessite également une défense imparable. La sécurité, la fiabilité et la disponibilité revêtent par conséquent un caractère majeur lorsque les enjeux sont aussi élevés.

> RÉGLEMENTATIONS EUROPÉENNES : CONFORMITÉ REQUISE

> OBLIGATIONS DE CONFORMITÉ FACULTATIVES

> RÉGLEMENTATIONS PROPRES À CHAQUE PAYS

> POUR CHAQUE PROBLÈME, IL EXISTE UNE SOLUTION STORMSHIELD

> LA CONFORMITÉ NE FAIT PAS TOUT

> RÉGLEMENTATIONS EUROPÉENNES : CONFORMITÉ REQUISE

Les organisations de défense doivent se conformer aux réglementations de cybersécurité européennes suivantes :

Règlement général sur la protection des données (RGPD)

Le RGPD est une réglementation de l'Union européenne conçue pour unifier les lois relatives à la confidentialité des données en Europe, protéger et responsabiliser l'ensemble des citoyens européens en ce qui concerne la confidentialité de leurs données, et repenser l'approche des organisations en matière de confidentialité des données. Cela crée de nouvelles contraintes et exigences pour les responsables informatiques et opérationnels, les directeurs de l'information et les directeurs de la sécurité informatique.

L'exigence principale de cette réglementation est la « protection des données par défaut », qui définit la protection des données personnelles comme un élément intrinsèque des systèmes et services. Les produits Stormshield aident les organisations à se conformer à ces exigences en améliorant la cyber-résistance de leur infrastructure. De plus, Stormshield Data Security fournit des fonctionnalités de chiffrement des données, qui est considéré par le RGPD comme une mesure technique appropriée pour garantir le niveau de sécurité adapté selon le risque.

Diffusion Restreinte OTAN

Cette classification de sécurité s'applique aux informations sensibles dont la divulgation non autorisée, l'altération ou la non-disponibilité nuirait aux intérêts de l'OTAN. Si des informations classées dans la catégorie « Diffusion Restreinte OTAN / NATO Restricted » sont diffusées en dehors d'une zone sécurisée avec accès physique restreint, cette classification requiert que ces informations soient chiffrées par des produits certifiés.

Stormshield Network Security et Stormshield Data Security ont reçu la certification « Diffusion Restreinte OTAN ». Ces outils peuvent donc être déployés dans des environnements sensibles pour chiffrer les informations classées dans la catégorie « Diffusion Restreinte OTAN », et pour permettre une transmission sécurisée des informations classées.

Cybersecurity Act

Le règlement européen Cybersecurity Act constitue une réponse à la menace croissante des cyberattaques en renforçant les prérogatives de l'agence européenne pour la cybersécurité (ENISA) et en se dotant d'un cadre européen de certification de cybersécurité. Le cadre européen de certification de cybersécurité vise à renforcer la sécurité des produits connectés, des appareils de l'Internet des objets et des infrastructures critiques au moyen de certificats. Une certification des produits, des procédés et des services qui sera valable dans l'ensemble des États membres. Les 3 niveaux définis (« Élémentaire », « Substantiel » et « Élevé ») permettront aux utilisateurs de déterminer le niveau d'assurance de la sécurité et garantiront que les éléments de sécurité auront été vérifiés de manière indépendante.

Les produits Stormshield ont déjà atteint le niveau « Qualification Standard » décerné par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) en France. Sachant que le niveau « Élevé » du cadre européen correspond au niveau de « Qualification Élémentaire » de l'ANSSI – qui est inférieur au niveau de « Qualification Standard » –, les produits Stormshield répondent donc déjà aux attentes de l'ENISA en matière de cybersécurité.

Vous voulez en savoir plus ? C'est parti !

> OBLIGATIONS DE CONFORMITÉ FACULTATIVES

Si elles le souhaitent, les organisations du secteur de la Défense peuvent se conformer aux normes suivantes pour améliorer leur niveau de cybersécurité. Toutefois, ces normes ne revêtent aucun caractère obligatoire en vertu de la législation actuelle.

Critères Communs / Niveaux d'assurance d'évaluation (EAL3+, EAL4+, etc.)

Les Critères Communs pour l'évaluation de la sécurité des technologies de l'information constituent une norme internationale (ISO/CEI 15408) pour la certification de la sécurité informatique. Cette norme garantit que le processus de spécification, de mise en place et d'évaluation d'un produit de sécurité informatique a été mené de façon rigoureuse, standard et répétable à un niveau correspondant à l'environnement prévu pour l'utilisation. Dans le cadre de cette norme, le niveau d'assurance d'évaluation (Evaluation Assurance Level – EAL3+, EAL4+, etc.) du produit indique avec quel degré de minutie celui-ci (p. ex. un pare-feu) a été testé. Cette certification est reconnue par une trentaine de pays à l'échelle mondiale (en Europe, en Amérique du Nord, en Asie et au Moyen-Orient).

Les produits Stormshield n'ont pas simplement reçu la certification Critères Communs : ils ont atteint le niveau « Qualification standard » beaucoup plus élevé, décerné par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) en France. Pour obtenir ce statut à l'indice de confiance très élevé, le produit doit :

- Obtenir une certification de haut niveau avec un objectif de sécurité défini et validé par l'ANSSI
- Obtenir de bons résultats à l'analyse complémentaire effectuée par l'ANSSI, y compris à l'audit du code source du produit.

Veuillez noter que la « Qualification Standard » est un prérequis pour qu'un produit soit classé dans la catégorie « Diffusion Restreinte », « Diffusion Restreinte OTAN » ou « Restreint UE » nécessaire à la manipulation des informations classées.

Technologie de l'information ISO/CEI 27000 – Techniques de sécurité – Systèmes de gestion de la sécurité de l'information

La série ISO/CEI 27000 est une famille de normes de sécurité de l'information qui fournit un cadre reconnu à l'international relatif aux meilleures pratiques de gestion de la sécurité de l'information. Avec son champ d'action très large, cette série s'applique aux organisations de toute taille dans tous les secteurs.

Le système de gestion de la sécurité de l'information (ISMS, Information Security Management System) fournit une approche systématique pour assurer en continu la sécurité de l'infrastructure sensible. Étant donné la nature dynamique de la sécurité et du risque liés aux informations, le concept ISMS intègre un système d'analyse et d'amélioration continues pour répondre aux évolutions des menaces, des vulnérabilités ou des impacts des incidents.

Les produits Stormshield sont conçus pour assurer la sécurité de l'infrastructure sensible. Un journal standard permet aux organisations de centraliser toutes les informations, afin d'identifier les tendances et les vulnérabilités potentielles. Une interface hautement intuitive permet aux utilisateurs de facilement mettre en place les améliorations.

> RÉGLEMENTATIONS PROPRES À CHAQUE PAYS

ROYAUME-UNI

Data Protection Act 2018

Similaire au RGPD, le Data Protection Act est une loi de protection des données spécifique au Royaume-Uni. Il stipule que les données personnelles doivent être couvertes par « un niveau approprié de protection » selon les risques encourus en cas de faille de sécurité. Cela inclut un niveau de sécurité empêchant toute manipulation non autorisée ou illégale, toute perte accidentelle, toute destruction ou tout endommagement des données. Le secteur de la Défense est en partie dispensé de l'application de cette législation, tant que les données personnelles sont utilisées aux fins de protection et de prévention des citoyens.

Les produits Stormshield aident les organisations à se conformer à ces exigences en améliorant la cyber-résistance de leur infrastructure. De plus, Stormshield Data Security fournit des fonctionnalités de chiffrement des données, qui est considéré par le RGPD comme une mesure technique appropriée pour garantir le niveau de sécurité adapté selon le risque.

> RÉGLEMENTATIONS PROPRES À CHAQUE PAYS

FRANCE

Loi de Programmation Militaire (LPM)

La Loi de programmation militaire (LPM) fixe les orientations relatives à la politique de défense de la France. Face à la multiplication des cyberattaques menées par des hackers, des terroristes voir même des États, la cyber défense constitue un axe clairement défini dans la LPM. Elle intègre donc un volet de cybersécurité et liste les OIVs répartis dans 12 secteurs d'activité, dont le secteur de la Défense.

Étant tous qualifiés par l'ANSSI, cette confiance dans les produits Stormshield permettent aux OIVs de déployer ces solutions de sécurité afin d'augmenter le niveau de protection des Systèmes d'Information d'Importance Vitale (SIIV). À titre d'exemple, Stormshield Network Security assure la segmentation des réseaux, la sécurisation des accès distants, l'authentification des utilisateurs et la gestion des vulnérabilités. Déployé en complément d'un antivirus, Stormshield Endpoint Security (SES) propose une protection en profondeur des postes de travail contre les attaques sophistiquées. SES peut également améliorer la sécurité des systèmes d'exploitations obsolètes ; détecter et gérer les incidents et assurer une protection contre les attaques par rebond.

Référentiel Général de Sécurité (RGS)

Le Référentiel général de sécurité (RGS) s'impose aux systèmes d'information mis en œuvre par les autorités administratives dans leurs relations entre elles et dans leurs relations avec les usagers. Elles ont ainsi pour obligation de mettre en oeuvre la sécurisation de leurs échanges électroniques. Ce Référentiel propose une méthodologie ainsi que des règles et bonnes pratiques à destination des administrations.

La protection des données est ici une dimension essentielle. La solution Stormshield Data Security fournit des capacités de chiffrement des données en répondant aux exigences de qualification des produits de sécurité et des prestataires de services de confiance. Les autres gammes de produits Stormshield aident également les administrations à se conformer à ces exigences tout en augmentant la résilience de leur infrastructure.

Guides de bonnes pratiques de l'ANSSI

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) est un véritable organe moteur en matière de cybersécurité en France et produit régulièrement des guides de bonnes pratiques. Il ne s'agit pas ici de réglementations à proprement parler mais davantage d'aides à la décision dans la sélection de vos prestataires, de vos solutions de cybersécurité voir de mise en place de ces dernières. De la cryptologie aux postes de travail en passant par les réseaux, une bibliographie riche et passionnante.

> RÉGLEMENTATIONS PROPRES À CHAQUE PAYS

ALLEMAGNE

Normes du bureau fédéral pour la sécurité de l'information (BSI)

Les normes BSI constituent, en Allemagne, un élément de base de la méthodologie IT-Grundschutz. Les normes BSI actuelles sont les suivantes :

- 200-1 (exigences générales pour un système de gestion de la sécurité de l'information)
- 200-2 (exigences de base pour le développement d'un système performant de gestion de la sécurité de l'information)
- 200-3 (toutes les étapes liées aux risques pour la mise en place d'une protection informatique basique)

Loi sur la sécurité informatique (IT-Sicherheitsgesetz) et loi BSI (BSI-Gesetz)

Les sections 8a - 8d BSIG sont particulièrement pertinentes quant à la sécurité de l'infrastructure critique des technologies de l'information et des prestataires de services numériques.

Les produits Stormshield de confiance et certifiés permettent de déployer des solutions de sécurité qui améliorent le niveau de protection des systèmes informatiques. À titre d'exemple, Stormshield Network Security assure la segmentation des réseaux, la sécurisation des accès distants, l'authentification des utilisateurs et la gestion des vulnérabilités. Déployé en complément d'un antivirus (le cas échéant), Stormshield Endpoint Security (SES) propose une protection en profondeur des postes de travail contre les attaques sophistiquées. SES peut également améliorer la protection des systèmes d'exploitation obsolètes, détecter et gérer les incidents, et assurer une protection contre les attaques par rebond. Stormshield Data Security aide à prévenir les fuites de données grâce au chiffrement des informations sensibles.

Loi fédérale sur la protection des données (BDSG)

La section 22 (2) de la loi BDSG concerne les exigences spéciales en matière de sécurité des données qui doivent être satisfaites lorsque des catégories spécifiques de données personnelles sont traitées. Le paragraphe 64 (3) de la loi BDSG répertorie les objectifs des mesures appropriées pour l'évaluation des risques liés aux données.

L'exigence principale de cette réglementation est la « protection des données par défaut », qui définit la protection des données personnelles comme un élément intrinsèque des systèmes et services. Les produits Stormshield aident les organisations à se conformer à ces exigences en améliorant la cyber-résistance de leur infrastructure. De plus, Stormshield Data Security fournit des fonctionnalités de chiffrement des données, qui constitue une mesure technique appropriée pour garantir le niveau de sécurité adapté selon le risque.

> RÉGLEMENTATIONS PROPRES À CHAQUE PAYS

ITALIE

Qualifications de sécurité (DPCM 22 luglio 2011)

Les qualifications de sécurité (AP et NOSI) permettent aux organisations de conclure un contrat avec les administrations publiques afin de pouvoir participer aux appels d'offres pour l'obtention de contrats « réservés » ou de niveau supérieur, et plus spécifiquement dans le cas d'appels d'offres qui impliquent la manipulation d'informations classées dans les catégories Secret/Top secret/ Confidentiel/Hautement confidentiel.
De telles qualifications impliquent que les organisations mettent en place des mesures de sécurité spécifiques couvrant les aspects logique, physique et technique.

Loi 124/2007 (sécurité et nouveau protocole de confidentialité des systèmes d'information pour la république italienne) - Amendée par la loi 133/2012

Le DIS (Dipartimento delle Informazioni per la Sicurezza), l'AISE (Agenzia Informazioni e Sicurezza Esterna) et l'AISI (Agenzia Informazioni e Sicurezza Interna) peuvent correspondre avec tous les organismes publics de défense et prestataires qui fournissent, sous le régime des autorisations, des concessions ou des conventions, des services d'utilité générale, et leur demander de collaborer pour l'exécution de leurs fonctions institutionnelles. À cette fin, ils peuvent notamment conclure des accords avec les prestataires susmentionnés (voir l'art. 13 de la loi pour en savoir plus).

D.P.C.M. 6 novembre 2015 (protocole de signature électronique pour les documents secrets/confidentiels)

Le protocole est contraignant en Italie pour tous les prestataires, publics et privés, en possession des qualifications de sécurité requises pour la gestion des informations classées. De plus, le protocole indique comment générer, signer et vérifier les signatures numériques, et explique le processus de validation temporaire des documents électroniques classés.

> RÉGLEMENTATIONS PROPRES À CHAQUE PAYS

ITALIE

Directive 1 agosto 2015 (cadre national italien pour l'application de la cybersécurité)

La Directive applique les objectifs définis avec le cadre national pour la cybersécurité, ce qui permet la coordination des administrations publiques et le partenariat avec tous les opérateurs privés qui contrôlent les infrastructures informatiques et télématiques considérées comme des fonctions critiques au niveau national. La Directive exige de l'Agenzia per l'Italia Digitale (AgID) qu'elle développe des normes pour les administrations.

Décret 18 maggio 2018, n. 65 (mise en place en Italie de la directive (UE) 2016/1148 - NIS)

La loi établit des mesures pour une sécurité au niveau national, avec notamment la mise en place d'un CSIRT (également appelé CERT), en définissant les obligations des « opérateurs de marchés critiques » du s.c. et des prestataires numériques au niveau des procédures liées aux failles de sécurité, de la coopération internationale sur les problèmes de sécurité et de l'adoption d'une stratégie nationale de cybersécurité.

Les produits Stormshield de confiance et certifiés permettent aux Opérateurs d'Importance Vitale (OIV) et Opérateurs de Services Essentiels (OSE) de déployer des solutions de sécurité qui améliorent le niveau de protection des Systèmes d'Information Essentiels (SIE). À titre d'exemple, Stormshield Network Security assure la segmentation des réseaux, la sécurisation des accès distants, l'authentification des utilisateurs et la gestion des vulnérabilités. Déployé en complément d'un antivirus (le cas échéant), Stormshield Endpoint Security (SES) propose une protection en profondeur des postes de travail contre les attaques sophistiquées. SES peut également améliorer la protection des systèmes d'exploitation obsolètes, détecter et gérer les incidents, et protéger contre les attaques sophistiquées.

D.P.C.M. 17 febbraio 2017 (orientation sur la sécurité et la cybersécurité nationales italiennes relatives à la technologie de l'information - décret Gentiloni)

La Directive définit l'organisation institutionnelle en charge de la sécurité et la cybersécurité informatiques nationales, en établissant les obligations et responsabilités de chaque entité (CISR, CISR Tecnico, rôle et directives du DIS, Nucleo per la Sicurezza Cibernetica et ses obligations). La Directive établit également les mesures des « opérateurs de marchés critiques » ainsi que les prestataires du secteur de la communication.

> RÉGLEMENTATIONS PROPRES À CHAQUE PAYS

ITALIE

D.P.C.M. 27 gennaio 2014 (cadre stratégique national italien pour l'espace cybernétique - QSN)

Le cadre stratégique national pour l'espace cybernétique vise à garantir l'efficacité et l'interopérabilité des ressources dédiées à la défense commune, et la prise en charge de l'intégration complète du cyberdomaine dans le processus de planification de la défense de l'OTAN et dans la doctrine militaire, afin d'assurer le déploiement de fonctionnalités puissantes contre les cyberattaques.

Stormshield Network Security a obtenu les certifications « Diffusion Restreinte OTAN » et « Restreint UE ». Par conséquent, ces produits peuvent être déployés dans des environnements sensibles pour permettre une diffusion sécurisée des informations classées. Cela contribue à l'interopérabilité internationale avec l'OTAN et les institutions de l'Union européenne.

Plan triennal 2019-2021 pour une autorisation préalable par l'AgID

Le Plan établit les mesures réglementaires pour les administrations publiques italiennes, y compris la mise en place de la plate-forme Infosec, un essai pour la diffusion nationale automatique d'un IoC qualifié, des directives nationales pour une autorisation préalable sur la cybersécurité et l'obligation de mise en place des directives de l'AgID sur les mesures de sécurité.

Mesures de sécurité minimales de l'AgID (mise en place du DPCM 1 agosto 2015)

Cette Directive italienne vise à la mise en place des mesures de l'AgID pour lutter contre les cybermenaces et pour fournir les mesures de sécurité nécessaires au secteur de la Défense en matière de contrôles techniques et organisationnels.

Les produits Stormshield aident les organisations à se conformer à ces exigences en améliorant la cyber-résistance de leur infrastructure. À titre d'exemple, Stormshield Network Vulnerabilty Manager est intégré au niveau réseau dans les produits Stormshield Network Security et contribue à la gestion des vulnérabilités.
De plus, Stormshield Endpoint Security accroît le niveau de sécurité de l'antivirus traditionnel en bloquant les menaces sophistiquées. Enfin, Stormshield Data Security, produit ayant reçu la certification « Restreint UE », aide à se conformer aux exigences de protection des données.

> RÉGLEMENTATIONS PROPRES À CHAQUE PAYS

ESPAGNE

Loi du code de cybersécurité espagnole

Ce Code met à disposition des avocats un outil répertoriant les règles mises à jour qui ont un impact direct sur la cybersécurité. Il facilite ainsi l'étude et l'analyse d'une problématique déjà essentielle pour atteindre un niveau de protection adéquat des entreprises, institutions et citoyens dans un état de droit social et démocratique.

Les produits Stormshield aident les organisations à se conformer à ce plan en améliorant la cyber-résistance de leur infrastructure. Stormshield Network Security garantit une protection de pointe avec des fonctionnalités de gestion des menaces unifiées. De plus, Stormshield Endpoint Security accroît le niveau de sécurité de l'antivirus traditionnel en bloquant les menaces sophistiquées. Enfin, Stormshield Data Security fournit des fonctionnalités de chiffrement des données, qui constitue une mesure technique appropriée pour garantir le niveau de sécurité adapté selon le risque.

Loi espagnole de protection des infrastructures critiques (Ley PIC)

La loi de protection des infrastructures critiques (Ley PIC 8/2011) est complétée par le décret royal 704/2011. Les deux principaux objectifs de cette norme sont les suivants : répertorier toutes les infrastructures qui fournissent des services essentiels à notre société et concevoir un plan qui comprend des mesures de prévention et de protection efficace contre les menaces possibles dont sont victimes ces infrastructures, tant en matière de sécurité physique que de sécurité des informations et technologies de communication.

Les produits Stormshield de confiance et certifiés permettent à l'infrastructure critique de déployer des solutions de sécurité qui améliorent le niveau de protection des systèmes d'information essentiels. À titre d'exemple, Stormshield Network Security assure la segmentation des réseaux, la sécurisation des accès distants, l'authentification des utilisateurs et la gestion des vulnérabilités. Déployé en complément d'un antivirus (le cas échéant), Stormshield Endpoint Security (SES) propose une protection en profondeur des postes de travail contre les attaques sophistiquées. SES peut également améliorer la protection des systèmes d'exploitation obsolètes, détecter et gérer les incidents, et assurer une protection contre les attaques par rebond.

> RÉGLEMENTATIONS PROPRES À CHAQUE PAYS

ESPAGNE

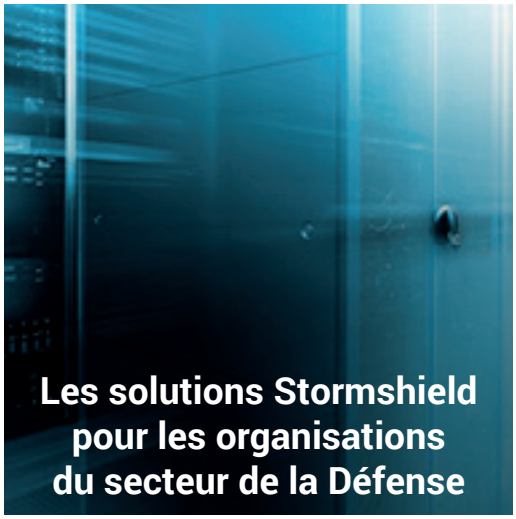
Plan de sécurité national espagnol, Décret royal 3/2010 du 8 janvier

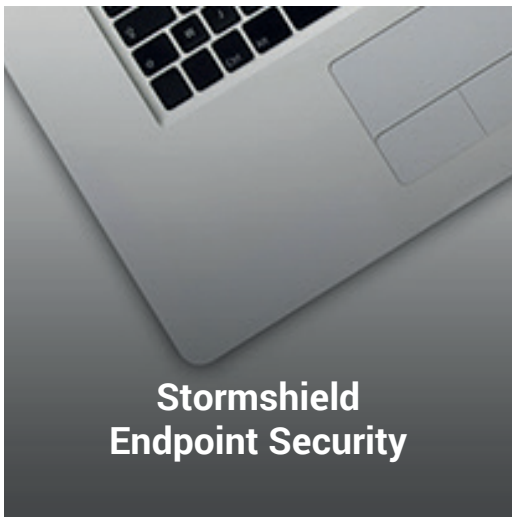
Ce plan s'applique comme dans toute autre organisation gouvernementale. Les systèmes qui gèrent des informations classifiées doivent en complément se plier à l'exigence de produits qualifiés par le Centre National de Cryptologie espagnol (CCN).

Les produits Stormshield aident les organisations à se conformer à ce plan en améliorant la cyber-résistance de leur infrastructure. Stormshield Network Security garantit une protection de pointe avec des fonctionnalités de gestion des menaces unifiées. Notre gamme SNS est d'ailleurs la seule gamme européenne qualifiée « Productos Cualificados » et l'unique gamme de pare-feux qualifiée « Productos Aprobados » par le CCN. Elle peut donc répondre à l'exigence de produit qualifié. De plus, Stormshield Endpoint Security accroît le niveau de sécurité de l'antivirus traditionnel en bloquant les menaces sophistiquées. Enfin, Stormshield Data Security fournit des fonctionnalités de chiffrement des données, qui constitue une mesure technique appropriée pour garantir le niveau de sécurité adapté selon le risque.

> POUR CHAQUE PROBLÈME, IL EXISTE UNE SOLUTION STORMSHIELD.

Les produits et solutions Stormshield pour les organisations du secteur de la Défense





> LA CONFORMITÉ NE FAIT PAS TOUT

Le grand nombre de réglementations et normes est devenu un véritable casse-tête pour toutes les organisations. Bien que ce guide fournisse des indications sur les réglementations applicables à chaque industrie, rappelez-vous que la conformité ne fait pas tout. N'oubliez pas que chaque organisation doit cartographier et gérer les risques pour garantir sa propre sécurité.