Check Point
SOFTWARE TECHNOLOGIES LTD

RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES DE L'UE

UNE CONFORMITÉ EFFICACE ET EFFICIENTE GRÂCE À CHECK POINT

WELCOME TO THE FUTURE OF CYBER SECURITY

SOMMAIRE

Le règlement général sur la protection des données de l'Union européenne (« RGPD ») augure des changements de fond en matière de protection des données personnelles. Sa portée étendue s'applique à toute entreprise dans le monde amenée à gérer les informations privée des citoyens de l'UE. Il impose une liste complète de protections sur ces données, de limites quant à leur utilisation, ainsi que de notifications des clients et d'obtention de leur consentement, dans un large éventail de situations. Essentiellement, le RGPD impose des pénalités importantes en cas de non-conformité. Le RGPD prend effet mi 2018, ce qui signifie que les entreprises doivent commencer à planifier leur stratégie de conformité dès maintenant. Les solutions Check Point permettent aux entreprises de prendre des mesures immédiates de conformité avec un impact minimal sur les applications et les opérations. Ce livre blanc présente une vue d'ensemble de la réglementation, puis décrit la manière dont Check Point peut aider les entreprises à prendre des mesures rapides pour se mettre en conformité.

> « Les données personnelles doivent être traitées de manière à assurer la sécurité appropriée des données personnelles, y compris les protéger contre le traitement non autorisé ou illégal et contre les pertes accidentelles. »
>
> *— RGPD, Article 5*

CONTEXTE : RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES DE L'UE

Le nouveau règlement général sur la protection des données de l'Union européenne (UE 2016/679, communément appelé « RGPD ») aura des conséquences importantes sur de nombreuses entreprises dans le monde entier. En faisant de la protection des données personnelles un droit fondamental (non seulement un droit du consommateur), le RGPD impose des responsabilités politiques et techniques importantes à toute entreprise amenée à gérer les données personnelles des citoyens de l'UE, que cette entreprise soit ou non active dans l'UE. Le règlement prendra effet en mai 2018, ce qui signifie que les entreprises doivent commencer à travailler sur leur conformité dès à présent.

Une des principales raisons pour lesquelles le RGPD aura potentiellement tant d'impact est l'ampleur des pénalités en cas de non-conformité. Les amendes pourront atteindre jusqu'à 4 % du chiffre d'affaires mondial d'une entreprise. En outre, une notification devra être émise dans un délai très court (72 heures) lorsque le contrôle des données personnelles est compromis. Cette notification peut inclure à la fois les organismes gouvernementaux chargés de la conformité et les citoyens concernés eux-mêmes. Indépendamment des amendes, il convient de préciser que l'objectif principal de ce règlement est de promulguer des droits de confidentialité tout en préservant la possibilité de laisser les données personnelles « circuler librement ». Dans son champ d'application le plus étendu, le RGPD ne devrait pas être considéré comme préventif, mais comme facilitateur ! Il présente les règles selon lesquelles le traitement des données et des informations personnelles est autorisé.

ÉLÉMENTS CENTRAUX DU RGPD

DROITS DE CONFIDENTIALITÉ ACCORDÉS PAR LE RGPD

Au cœur du RGPD, l'objectif est de définir les droits de protection des données accordés à tous les citoyens de l'UE. L'objectif de la réglementation est d'apporter ces droits, quelle que soit l'entreprise qui traite les données personnelles d'un citoyen et le lieu où se déroule le traitement. Par conséquent, les éléments essentiels du RGPD détaillent un certain nombre de « droits des citoyens de l'UE » en ce qui concerne la manière dont leurs données personnelles sont utilisées. La liste est vaste et nécessitera des changements importants dans les applications, les politiques et les procédures, afin d'assurer la conformité. Par exemple :

- Les entreprises doivent obtenir le consentement des citoyens pour traiter leurs données, et ce consentement doit être obtenu d'une manière qui soit claire pour les citoyens (pas une page de texte juridique avec une case à cocher « Accepter » en bas).
- Elles doivent mettre à disposition de tous les citoyens des informations exactes sur les données recueillies, leur utilisation, le lieu où elles sont traitées et avec quelles autres entreprises les données peuvent être partagées.
- Elles doivent fournir une explication sur la logique impliquée dans tout traitement automatisé effectué sur les données d'une personne.
- Il existe un « droit à l'oubli », c'est-à-dire le droit de demander à ce que toutes les données concernant un individu soient supprimées, ainsi qu'un droit de transférer facilement les données d'une entreprise à une autre.

L'ensemble assez étendu de droits imposera un fardeau important sur toute entreprise amenée à gérer les données de citoyens de l'UE.

> « ...les entités de contrôle et de traitement doivent mettre en œuvre les mesures appropriées pour assurer un niveau de sécurité adapté au risque, y compris...la capacité d'assurer la confidentialité, l'intégrité, la disponibilité et la résilience des systèmes et des services de traitement »
>
> *— RGPD, Article 32*

PRINCIPES DU RGPD

Au-delà des droits des citoyens, le RGPD définit un ensemble de « principes » qui régissent tout traitement de données personnelles. L'idée est de définir les conditions dans lesquelles le traitement des données est autorisé. Si une entreprise ne peut démontrer son fonctionnement dans ces conditions, ses activités peuvent être considérées comme étant illégales en vertu du RGPD.

Un principe clé est que les données ne peuvent être collectées « qu'à des fins précises, explicites et légitimes », ce qui signifie qu'il ne sera pas acceptable de collecter des données en premier puis de déterminer comment elles pourraient être utilisées ultérieurement. En outre, seule une quantité minimale de données nécessaires pour effectuer ces tâches peut être collectée. Les entreprises ne peuvent conserver les données dans un format permettant d'identifier facilement les personnes impliquées, lorsqu'elles ne sont plus nécessaires pour répondre à l'objectif initial.

Plus important encore pour les professionnels de la sécurité, le RGPD stipule que les données doivent être traitées de manière à garantir la « sécurité, l'intégrité et la confidentialité des données ». Cependant, le RGPD ne détaille pas la liste des contrôles techniques devant être implémentés pour répondre à ces exigences. À la différence, par exemple, de PCI DSS, RGPD maximise la flexibilité et n'offre qu'un ensemble de directives de base. Ces directives sont incluses dans l'Article 32 du RGPD et précisent que les entités contrôlant et traitant des données doivent implémenter des contrôles qui garantissent :

1
LA PSEUDONYMISATION ET LE CHIFFREMENT DES DONNÉES PERSONNELLES

2
LA CONFIDENTIALITÉ, L'INTÉGRITÉ, LA DISPONIBILITÉ ET LA RÉSILIENCE DES SYSTÈMES ET DES SERVICES DE TRAITEMENT

3
LA POSSIBILITÉ DE RESTAURER L'ACCÈS AUX DONNÉES PERSONNELLES ET LEUR DISPONIBILITÉ EN TEMPS OPPORTUN EN CAS D'INCIDENT PHYSIQUE OU TECHNIQUE

4
UN PROCESSUS POUR TESTER ET ÉVALUER RÉGULIÈREMENT L'EFFICACITÉ DES MESURES TECHNIQUES ET ORGANISATIONNELLES POUR ASSURER LA SÉCURITÉ DES TRAITEMENTS

Le RGPD aligne ces contrôles sur une approche axée sur le risque et note que les contrôles devraient être « intégrés dans » les systèmes et les applications lors de leur conception, plutôt qu'ajoutés après coup.

Conformément aux meilleures pratiques de sécurité, le RGPD exige également la disponibilité des données. Le texte du cadre requiert que les entités traitant des données fournissent : « ...la possibilité de restaurer l'accès aux données personnelles et leur disponibilité en temps opportun en cas d'incident physique ou technique ». Par conséquent, pour être conformes au RGPD, les entreprises doivent mettre en place des systèmes et des processus suffisants pour maintenir la haute disponibilité des données personnelles. Elles doivent également tester et évaluer régulièrement les mesures de sécurité mises en œuvre pour protéger ces données.

> « ...l'entité de contrôle doit, *au moment de la détermination des moyens de traitement* et au moment du traitement lui-même, mettre en œuvre des mesures techniques et organisationnelles appropriées...conçues pour implémenter les principes de protection des données...de manière efficace et d'intégrer les protections nécessaires au traitement... »
>
> *— RGPD, Article 25*

PRÉPARATION AU RGPD

Se préparer au RGPD est difficile pour deux raisons :

1. Le règlement est tout nouveau et il n'existe aucun précédent d'audit antérieur sur lequel une entreprise peut s'appuyer.

2. De nombreux aspects du RGPD sont toujours « en cours ». Par exemple, le RGPD introduit le concept de codes de conduite : des politiques et des contrôles spécifiques à des secteurs qui pourraient être adoptés pour faire preuve de conformité. Cependant, aucun code de conduite n'existe actuellement. Comme autre exemple, le RGPD établit un Contrôleur européen de la protection des données (CEPD) pour « jouer un rôle actif dans l'application de la législation européenne en matière de protection des données ». Cependant, la formalisation du CEPD est encore en cours et les spécificités doivent encore être déterminées.*

Néanmoins, le délai limité restant jusqu'à ce que le règlement entre en vigueur exige que les entreprises commencent le processus de planification de leur stratégie dès à présent. Le tableau suivant résume les domaines d'intervention recommandés et les éléments d'action pour commencer le processus de préparation au RGPD (les éléments ci-dessous ne sont pas classés par ordre chronologique) :

Domaine de préparation au RGPD	Actions recommandées
Recrutement	Identifier le sponsor exécutif et le responsable technique, et décider de recruter ou d'externaliser le responsable de la protection des données
Audit et classification des données	Localiser les données personnelles applicables. Cartographier les flux de données et les systèmes pertinents, y compris les systèmes de sauvegarde et les systèmes des tiers
Analyse des risques	Évaluer les risques en fonction des types, du volume et des systèmes de traitement des données
Journalisation des activités et identification des failles	Établir une solide piste d'audit des activités sur les systèmes applicables, en particulier les activités d'administration et d'accès aux données, ainsi que la journalisation enrichie sur l'ensemble des protections afin d'identifier des failles potentielles
Contrôles fondamentaux	Spécifier les contrôles de base sur les systèmes applicables et définir les projets d'implémentation

Ces domaines de préparation couvrent un large éventail d'activités. Ce document se concentre principalement sur les contrôles fondamentaux associés à la confidentialité, l'intégrité et la disponibilité des données protégées.

* Check Point mettra à jour ce document à mesure que les aspects du RGPD sont clarifiés.

CONTRÔLES DE SÉCURITÉ FONDAMENTAUX.

Les directives du RGPD reposent sur une approche fondée sur les risques afin d'assurer la confidentialité et la sécurité des données d'un individu. Plus précisément, le RGPD propose que les entités concernées mettent en œuvre des mesures appropriées en fonction de la valeur ou des dommages associés à la perte d'informations personnelles.

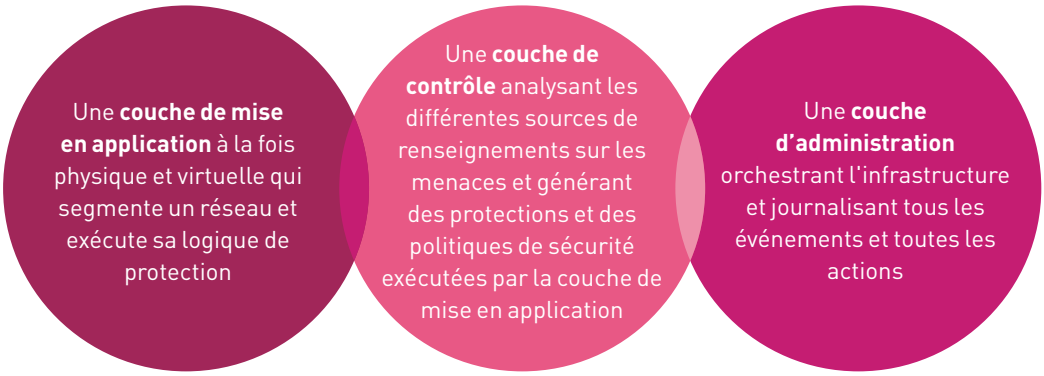
Le RGPD ne précise pas les contrôles exacts que les entreprises doivent mettre en œuvre pour être conformes. Néanmoins, les meilleures pratiques en matière de sécurité générale suggèrent que ce qui suit devrait constituer un bon point de départ :

1 CLASSIFICATION DES DONNÉES	2 GESTION DES CHANGEMENTS DE CONFIGURATION	3 CONTRÔLES ADMINISTRATIFS ET SÉPARATION DES RESPONSABILITÉS	4 CONFIGURATION SYSTÈME SÉCURISÉ
5 CONTRÔLE DES ACCÈS	6 SEGMENTATION RÉSEAU	7 CHIFFREMENT ET PSEUDONYMISATION	8 PRÉVENTION DES FUITES DE DONNÉES
9 PRÉVENTION DES ATTAQUES DDOS	10 SURVEILLANCE DES ACTIVITÉS DES UTILISATEURS	11 GESTION DES VULNÉRABILITÉS	12 REPRISE SUR INCIDENT

IMPLÉMENTATION DE CONTRÔLES DE SÉCURITÉ FONDAMENTAUX AVEC LA PROTECTION LOGICIELLE CHECK POINT

Jusqu'à ce que les directives d'implémentation du RGPD et les normes de certification soient mieux établies, les entreprises peuvent s'appuyer sur des méthodologies existantes reposant sur une approche fondée sur les risques. La protection logicielle Check Point (SDP) en est un modèle.

L'architecture SDP utilise une approche de sécurité à trois niveaux qui partitionne l'infrastructure de sécurité en trois couches interconnectées :



Le choix des protections pertinentes implémentées dans la couche de mise en application repose sur une compréhension du risque associé à un événement de sécurité. Dans le cas du RGPD, un tel événement pourrait être la perte ou la modification des données personnelles d'un individu, ou une faille du réseau qui donnerait accès aux données de l'individu.

La protection logicielle Check Point prend pleinement en charge les meilleures pratiques précédemment notées en matière de contrôle. Une description supplémentaire de l'implémentation des contrôles est disponible dans l'annexe et comprend les éléments suivants :

Contrôle	Prise en charge par Check Point
Classification des données	La technologie de prévention de perte de données intégrée à la passerelle permet de détecter les données personnelles circulant sur le réseau, surveiller les contenus et bloquer les transmissions de données non autorisées. Check Point Capsule Docs propose également des outils de classification des contenus.
Gestion des changements de configuration	Les blades SmartWorkflow et SmartLog établissent des contrôles d'approbation des changements, intègrent la journalisation complète des changements de configuration et produisent automatiquement des rapports à des fins d'audit.
Contrôles administratifs et séparation des responsabilités	La gestion de la sécurité prend en charge des autorisations granulaires et permet la journalisation en fonction des rôles, afin de faciliter la séparation des responsabilités sans impacter l'efficacité opérationnelle.
Configuration système sécurisé	La blade Compliance garantit que les définitions de sécurité de l'architecture d'une entreprise sont compatibles avec le RGPD.
Segmentation réseau	La segmentation réseau intégrée au pare-feu de nouvelle génération isole les données, afin de réduire considérablement les risques et le coût de la conformité. La segmentation peut être définie par des paramètres applicatifs ou de données, ce qui simplifie la segmentation selon les directives de protection des données.

Contrôle	Prise en charge par Check Point
Chiffrement et/ou pseudo-nymisation	La solution Endpoint de Check Point étend la protection des données à toute l'entreprise. Sa blade Full Disk Encryption chiffre les disques durs des ordinateurs des collaborateurs, et Media Encryption and Port Protection chiffre et contrôle les connexions au stockage amovible. La solution protège également les documents grâce à sa technologie Capsule Docs de gestion des droits. Les accès à distance gérés par appliance de sécurité et VPN chiffré de site à site protègent les données en mouvement.
Prévention des pertes de données	Une solution reposant sur des politiques de sécurité pour surveiller les contenus et journaliser les activités en fonction de règles standardisées ou personnalisées. Des notifications en temps réel sensibilisent les utilisateurs aux directives en matière de protection de la confidentialité, avec blocage optionnel des actions qui enfreindraient les contrôles du RGPD.
Prévention des attaques de déni de service distribué	Des protections dédiées, mais aussi le pare-feu et le système de prévention des intrusions, stoppent les attaques volumétriques et les attaques ciblant les applications en temps réel.
Surveillance des activités des utilisateurs	L'agent UserCheck fournit une notification en temps réel aux utilisateurs lorsqu'ils interagissent avec des applications ou des contenus confidentiels, ou se comportent d'une manière qui enfreint les politiques de sécurité. Journalisation reposant sur des identités et des groupes.
Gestion des vulnérabilités	Le système de prévention des intrusions empêche les tentatives d'exploitation des vulnérabilités connues en attendant l'application de correctifs. La technologie SandBlast de prévention avancée des menaces identifie et stoppe les attaques avancées et inconnues dans le Cloud, sur le réseau, les postes et les appareils mobiles.
Reprise sur incident	Des options virtuelles et physiques de haute disponibilité évitent les points de défaillance individuels, dont notamment ClusterXL ainsi que la prise en charge du routage dynamique et des protocoles de basculement, en transférant le trafic vers les systèmes aux meilleurs temps de réponse.

RÉSUMÉ

Le nouveau Règlement Général sur la Protection des Données de l'Union Européenne (RGPD) aura des conséquences importantes sur de nombreuses entreprises dans le monde entier. Le RGPD est une règlementation émergente. Les éléments constituant une conformité acceptable ne sont pas encore pleinement compris. Cependant, l'intention de la réglementation en matière de protection des données est claire et il est donc possible de commencer à planifier la conformité dès à présent. Des stratégies devraient être étudiées et développées le plus tôt possible dans des domaines tels que la classification des données et la définition du champ d'application, les politiques d'utilisation des données, les notifications et les pistes d'audit. Les solutions Check Point ont longtemps été utilisées par des entreprises de toute taille et de tout type pour implémenter des contrôles de conformité dans le cadre de règlementations semblables au RGPD. Par conséquent, la combinaison de ces solutions avec une approche fondée sur le risque permet aux entreprises d'accélérer leur mise en conformité de manière avérée et opérationnellement efficace.

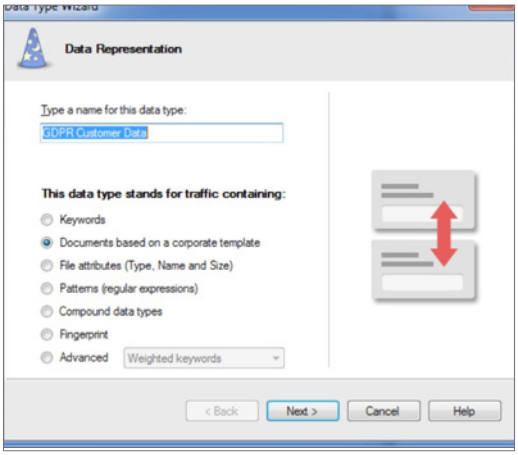
ANNEXE :

SOLUTIONS CHECK POINT POUR CONTRÔLES RGPD

Check Point propose une gamme de solutions pouvant aider les entreprises à implémenter des architectures de sécurité adaptées aux thèmes du RGPD. Les technologies fonctionnent dans les trois couches de l'architecture SDP.

Classification des données

Check Point fournit des solutions, telles que la blade Data Security (prévention des pertes de données), que les entreprises peuvent utiliser pour implémenter rapidement des directives de classification des données.



Les entreprises peuvent charger des modèles directement dans les outils de gestion de la solution. Ces modèles peuvent inclure des niveaux de confidentialité liés à des éléments de données et peuvent inclure des filigranes, des icônes et une terminologie pour aider les utilisateurs à comprendre les règles auxquelles s'appliquent les types de fichiers. La solution identifie le degré de correspondance des fichiers qui traversent le réseau à ces modèles, et autorise ou bloque leur transmission en temps réel.

Les solutions Check Point comprennent également des outils permettant aux administrateurs de définir rapidement des référentiels et des segments réseau pour lesquels les contrôles de sécurité des données devraient être implémentés. L'offre Capsule Docs (gestion des droits) s'intègre directement à Microsoft Office et Adobe Acrobat pour ajouter la classification des données lors de la création des documents

Gestion des changements de configuration

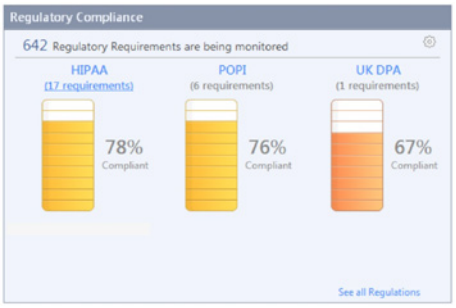
Les programmes de sécurité des données nécessitent une combinaison de processus et de contrôles technologiques. Dans le domaine des processus, les entreprises doivent vérifier si des modifications ont été apportées aux systèmes impliqués dans le traitement des données ainsi que ceux qui protègent les éléments de données eux-mêmes. Le système d'administration de Check Point comprend des fonctions telles que SmartLog, qui journalise les modifications apportées par les administrateurs aux règles de sécurité ainsi que les événements spécifiques liés à la sécurité des données au niveau du réseau et des postes. Ceux-ci peuvent être configurés pour catégoriser automatiquement les modifications pertinentes dans des rapports que les auditeurs et les responsables de la confidentialité des données peuvent examiner, afin de s'assurer que les changements identifiés sont conformes ou entrent en conflit avec les directives pertinentes de confidentialité des données. Des solutions telles que SmartWorkflow peuvent également introduire des étapes de gestion des changements, afin que les tentatives de modification des paramètres de configuration obéissent à un processus d'approbation avant leur mise en œuvre.

Contrôles administratifs et séparation des responsabilités

L'un des principaux préceptes de tous les cadres de sécurité est la séparation des responsabilités. Ce principe vise à garantir que seuls les individus devant accéder à certaines informations et systèmes puissent le faire. La définition et la modification des politiques de sécurité sont un domaine auquel cette directive s'applique clairement.

Les praticiens responsables des règles de contrôle des accès devraient être distincts de ceux qui supervisent la prévention des menaces ou la sécurité des données, afin qu'une seule personne ne puisse modifier la totalité de l'architecture de sécurité d'une entreprise. Les solutions d'administration de Check Point intègrent ce principe et permettent aux administrateurs de définir des règles attribuées à des utilisateurs individuels ou à des types d'utilisateurs. Cela s'applique aux différents types de contrôles de sécurité ainsi qu'à des règles spécifiques dans la politique de sécurité de l'entreprise.

Configuration système sécurisée



La blade Check Point Compliance propose une méthode automatisée pour évaluer si la configuration des définitions de sécurité de l'architecture d'une entreprise est conforme aux réglementations gouvernementales.

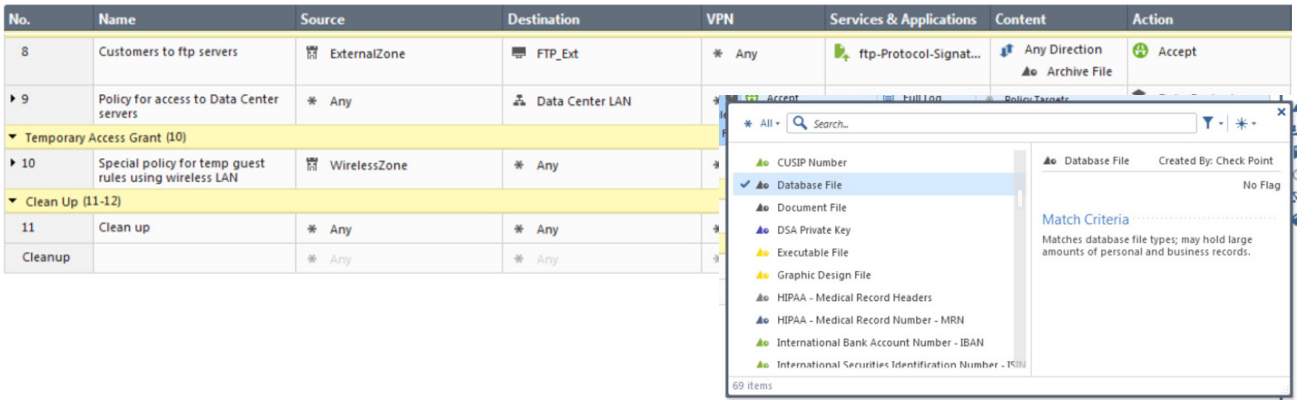
La solution examine les paramètres des politiques de sécurité et des équipements en temps réel, et les compare aux contrôles spécifiques des différentes réglementations. Elle détermine ensuite le degré de conformité des définitions des configurations et des bases de règles au cadre réglementaire pertinent.

Les administrateurs peuvent mettre à profit cette information pour accélérer leurs préparatifs en vue du RGPD. La solution comprend un éventail de cadres réglementaires européens et d'autres pays, y compris un ensemble initial de contrôles pour le RGPD.

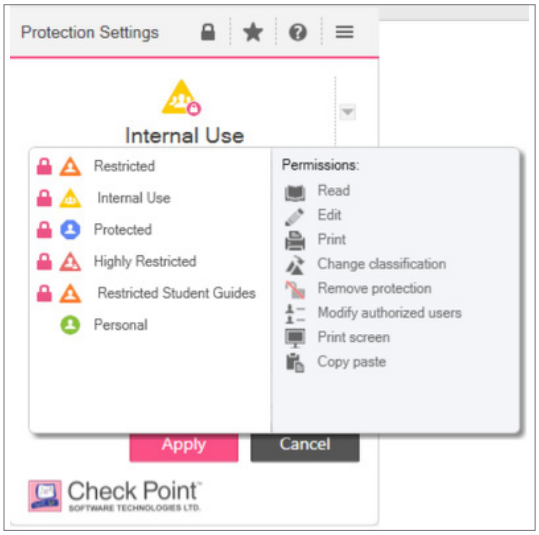
Segmentation reposant sur le réseau

Le cadre du RGPD met l'accent sur le fait que la sécurité des données devrait être intégrée aux processus d'une entreprise et non ajoutée par la suite. Check Point aide les entreprises à créer des architectures de sécurité cohérentes avec cette approche intégrée.

La segmentation du réseau peut être définie selon les paramètres du réseau, des applications et des données, dans la même règle. Cette connaissance des contenus facilite la segmentation des réseaux en fonction des directives de sécurité des données.



Chiffrement et pseudonymisation



La pseudonymisation et/ou le chiffrement devraient être implémentés dans tous les systèmes traitant ou stockant des enregistrements de données concernant des individus. La clé de cette recommandation est l'obligation de chiffrement des données lors de la création des fichiers pouvant inclure des informations personnelles.

L'application Check Point Capsule Docs s'intègre à des outils de productivité tels que Microsoft Office, et peut être configurée afin que tout contenu créé par les utilisateurs soit chiffré et rendu inaccessible à des tiers non autorisés. Ces protections s'intègrent aux clients de messagerie tels qu'Outlook, pour empêcher les utilisateurs d'envoyer accidentellement des fichiers aux mauvais destinataires. Cette fonction s'applique aux ordinateurs, aux appareils mobiles et aux systèmes dans le Cloud avec lesquels les utilisateurs interagissent.

La solution Check Point Endpoint Security comprend une grande variété de technologies de chiffrement, notamment :

- Chiffrement IPSec et SSL des données en transit via tunnel VPN d'accès à distance
- Chiffrement des disques et des supports amovibles
- Protection des ports pour contrôler l'utilisation des ports physiques sur les appareils des utilisateurs finaux

Prévention des pertes de données

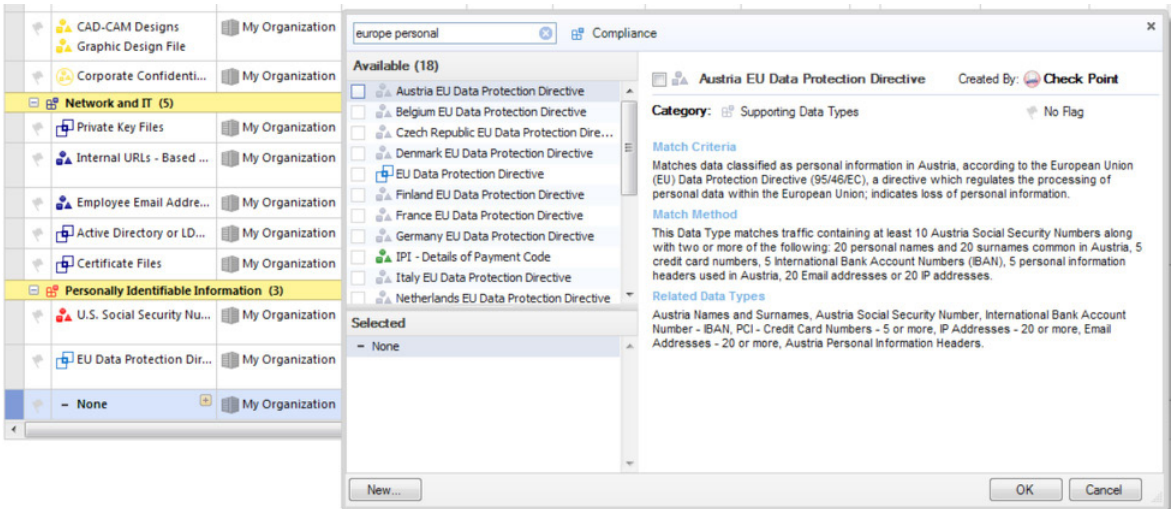
Les incidents de fuite de données ont lieu en raison d'une erreur humaine ou d'une intention malveillante. L'implémentation de contrôles couvrant ces deux scénarios peut être complexe et peut nécessiter beaucoup de temps. Check Point simplifie le processus de protection des données en fournissant aux administrateurs une base de données des types de fichiers courants. Cela est particulièrement vrai pour les informations personnelles identifiables (IPI). Les fonctionnalités de prévention des pertes de données de Check Point peuvent automatiquement rechercher différents formats d'IPI dans le trafic. La solution inspecte également les contenus en fonction de règles associées à différents cadres réglementaires.

Les stratégies de prévention des pertes de données de Check Point peuvent être définies afin que les utilisateurs soient avisés en temps réel lorsque leur comportement enfreint les directives de l'entreprise. Cela contribue à renforcer les programmes de sensibilisation à la sécurité, qui sont souvent des éléments clés des cadres réglementaires de protection des données et des informations.

Prévention des attaques de déni de service distribué

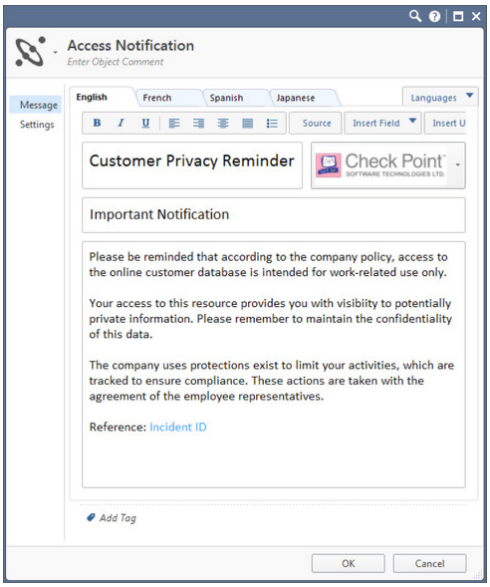
Le RGPD suggère que les entreprises assurent l'accès des individus à leurs informations à tout moment. Compte tenu du volume quasi constant d'attaques de déni de service sur Internet, il peut être difficile pour les entreprises de se conformer à cette recommandation et d'assurer que les services en ligne soient systématiquement disponibles.

Check Point propose un ensemble de fonctionnalités pour simplifier cet effort. Des protections DDoS dédiées stoppent les attaques volumétriques et les attaques ciblant les applications, en temps réel. Les fonctionnalités de prévention des intrusions et du pare-feu Check Point peuvent également être utilisées pour restreindre les connexions et bloquer les paquets malformés associés au comportement des attaques DDoS.



Surveillance des activités des utilisateurs

Les utilisateurs représentent le lien le plus faible dans tout programme de sécurité des données. Leurs erreurs et leurs comportements malveillants ouvrent la porte à des attaques et entraînent des fuites de données.



Pour répondre à ce défi, les entreprises peuvent tirer parti d'une combinaison de fonctionnalités dans la gamme de solutions Check Point :

1. La prise en charge des identités définit des règles en fonction des attributs et des identités des collaborateurs et des groupes de collaborateurs.
2. UserCheck fournit des notifications en temps réel aux utilisateurs lorsqu'ils interagissent avec des applications ou des contenus confidentiels, ou se comportent d'une manière qui enfreint les règles.
3. Les fonctions de journalisation mettent en évidence les événements de sécurité, tels que les fuites de données, et incluent les noms et les identifiants des personnes associées aux événements.

La possibilité de capturer des preuves sur les ordinateurs des utilisateurs est particulièrement intéressante en matière de surveillance des activités des utilisateurs. La solution Check Point Endpoint Security comprend une fonction d'analyse qui journalise les incidents d'exfiltration de données causés par des comportements intentionnels ou des logiciels malveillants.

Gestion des vulnérabilités

Les pratiques de sécurité standard recommandent aux entreprises de rechercher régulièrement des vulnérabilités afin de déterminer si leurs applications et leurs composants réseau sont sensibles aux attaques. Il s'agit d'une étape importante pour limiter les options à disposition des agresseurs pour enfreindre les systèmes et dérober des données personnelles confidentielles.

La correction des vulnérabilités identifiées lors du processus d'évaluation des systèmes comporte des difficultés. La mise à jour des systèmes d'exploitation et des applications dans toute l'entreprise peut prendre du temps. Les technologies de prévention des intrusions de Check Point peuvent immédiatement bloquer les tentatives d'exploitation de vulnérabilités connues, avant le processus d'application de correctifs.

Avec l'augmentation du nombre d'attaques zero-day, les entreprises doivent également envisager des moyens de bloquer les tentatives d'exploitation de vulnérabilités inconnues. Celles-ci ne sont pas identifiées durant les processus de recherche de vulnérabilités standard. Les solutions SandBlast de Check Point permettent d'identifier et de stopper les attaques avancées et inconnues. SandBlast couvre le réseau, le Cloud et les postes. La technologie émule des fichiers dans des instances virtualisées des systèmes d'exploitation pour déclencher des processus d'attaque, et les solutions SandBlast suppriment également à la volée les contenus actifs ou malveillants des fichiers

Reprise sur incident

Les recommandations du RGPD associées à la reprise sur incident visent à garantir que les individus puissent avoir accès à leurs données à tout moment. Le respect de ces recommandations requiert plusieurs couches de redondance. Les composants du réseau et des applications doivent être configurés dans des clusters haute disponibilité afin que la perte potentielle d'un système individuel n'entraîne pas de perturbation au niveau du service. Les solutions de Check Point fournissent plusieurs options de haute disponibilité pour écarter les points de défaillance individuels, notamment des technologies de clustering natives telles que ClusterXL, ou la prise en charge du routage dynamique et des protocoles de basculement qui utilisent le réseau ou des hyperviseurs pour transférer le trafic vers les systèmes les plus rapides.

Check Point propose également plusieurs options de passerelle virtuelle. Celles-ci permettent aux entreprises d'appliquer leurs architectures de sécurité dans des plates-formes de virtualisation publiques et privées, et ainsi développer rapidement des sites de reprise sur incident dotés de leur ensemble complet de données et de contrôles de sécurité réseau.

CONTACTEZ-NOUS

Siège mondial

5 Ha'Solelim Street, Tel Aviv 67897, Israël | Tél. : +972 3 753 4555 | Fax : +972 3 624 1100
Email : info@checkpoint.com

Siège français

120 avenue Charles de Gaulle, 92200 Neuilly sur Seine, France | Tél. : +33 (0)1 55 49 12 00
Email : info_fr@checkpoint.com | www.checkpoint.com

Check Point®
SOFTWARE TECHNOLOGIES LTD

