

WatchGuard, anonymisation des données utilisateurs et règlement général européen sur la protection des données

Dossier technique

WatchGuard Technologies, Inc.

Publication : Mai 2016

Introduction

Alors qu'Internet ne cesse d'évoluer, la question de la confidentialité des données utilisateurs est au centre de toutes les préoccupations. De nombreux pays se sont engagés à élaborer des normes réglementaires sur le déplacement, le stockage, la visualisation et les rapports de données contenant des informations permettant une identification personnelle des utilisateurs.

L'Union européenne (UE) établit des normes avec les réglementations les plus strictes au monde en matière de protection des données et de confidentialité. En avril 2016, le Parlement européen a officiellement adopté le **règlement général sur la protection des données** ou **RGPD**, qui entrera en vigueur le 25 mai 2018. Les obligations dans le cadre du RGPD sont notables, et la responsabilité (notamment du personnel d'entreprise) s'avère une composante importante de la conformité. Les menaces internes constituent toujours une source majeure de violations et d'utilisation abusive de données. Le chiffrement de toutes les informations est un bon début, mais les entreprises ont encore un long chemin à parcourir pour être réellement conformes à la réglementation à venir.

Les entreprises européennes devront prouver leur conformité avec les mesures du RGPD, notamment les suivantes :

- **Réalisation d'une évaluation de l'impact de la protection des données** avant de la mettre en œuvre, afin de constater le risque encouru
- **Mise en œuvre de la protection des données dès la conception et par défaut** : les entreprises devront concevoir la protection des données dans leurs infrastructures de service et évaluer ces déploiements dans une perspective de responsabilisation
- **Application des mesures techniques et organisationnelles sur les unités de traitement des données**
 - Déclaration des failles de sécurité au responsable du contrôle
 - Désignation d'un délégué à la protection des données*

- **Attribution de pseudonymes aux données personnelles** : les informations permettant une identification personnelle sont rendues anonymes dans la mesure où elles ne peuvent être pas imputables à leur propriétaire durant leur traitement

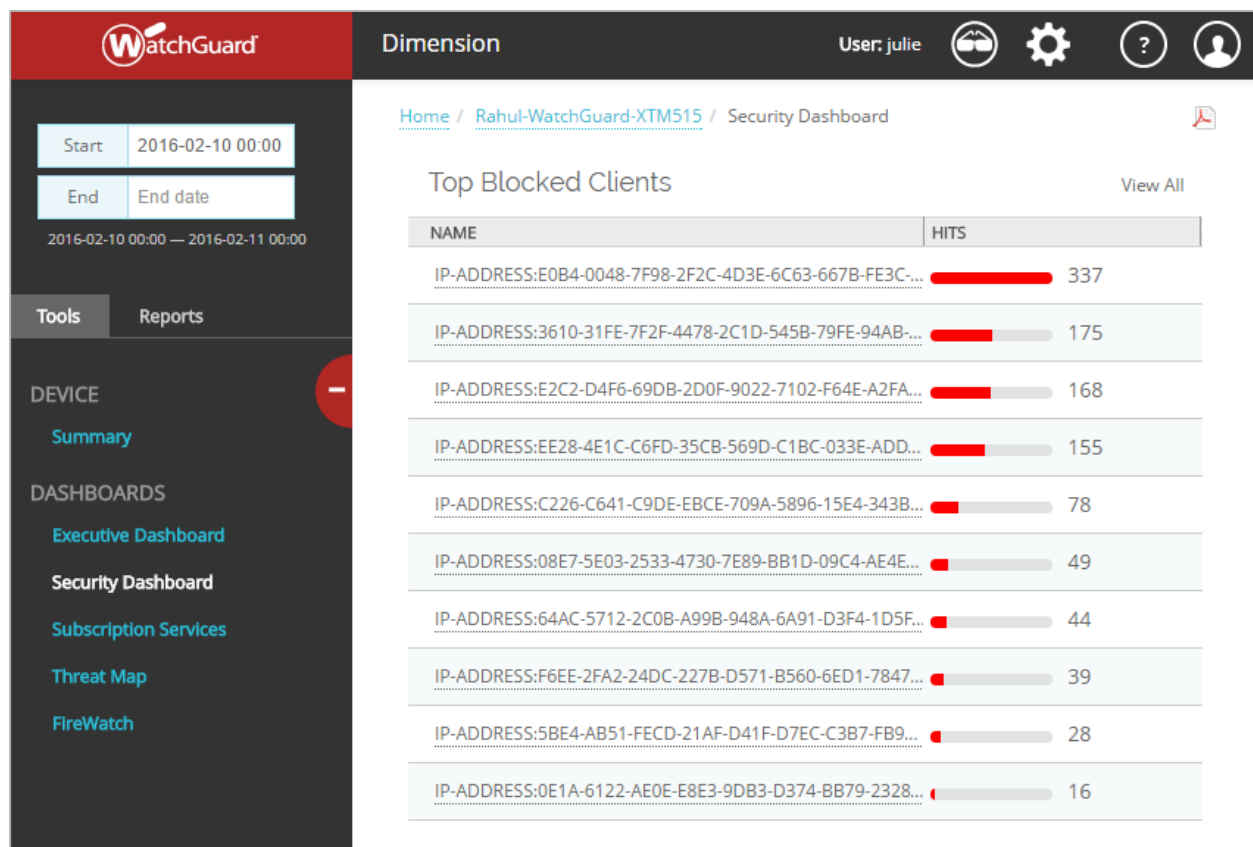
**Toutes les entreprises ne seront pas obligées de créer une telle fonction. Cependant, la responsabilité et la confidentialité des données utilisateurs sont obligatoires dans tous les services de traitement des données.*

WatchGuard et l'anonymisation des données utilisateurs

La plateforme de visibilité réseau **Dimension™ de WatchGuard**, intégrée gratuitement à toutes les appliances de sécurité WatchGuard Firebox, offre une nouvelle fonctionnalité encore plus puissante d'**anonymisation des données utilisateurs** afin de permettre aux entreprises de respecter les exigences du RGPD. Ce service, qui fonctionne de manière très simple, est facilement accessible et configurable, et a été conçu dans un contexte de menaces internes réelles, afin de garantir la conformité au RGPD.

En quoi consiste l'anonymisation des données utilisateurs ?

L'anonymisation des données utilisateurs consiste à remplacer les informations permettant une identification personnelle présentes dans les rapports, les tableaux de bord et les pages de synthèse de Dimension par des champs de texte codé. Lorsqu'elle est activée, l'anonymisation des données utilisateurs code les noms d'utilisateurs, les adresses IP, les noms d'hôtes et les noms de périphériques mobiles à l'aide de séquences alphanumériques uniques, générées de manière aléatoire. Les séquences d'anonymisation sont uniques pour chaque session anonyme. Ainsi, les mêmes éléments de données



des informations permettant une identification personnelle seront codés de manière différente lors de chaque session, afin d'empêcher leur réutilisation.

Figure 1. Le mode Anonyme permet un chiffrement au niveau de la plateforme de visibilité réseau uniquement. Il ne permet pas de chiffrer la base de données.

Si les utilisateurs se connectent à Dimension alors que le mode Anonyme est activé, ils ont accès à une vue restreinte des pages que leur rôle Utilisateur leur permet de consulter. De plus, lorsque la fonctionnalité est activée, les messages du journal et les rapports détaillés ne sont pas disponibles. Les tableaux de bord de visibilité réseau Dimension disponibles en mode Anonyme sont les suivants :

- Tableau de bord global
- Tableau de bord de sécurité
- Tableau de bord des services d'abonnement
- Cartographie des menaces
- FireWatch

En ce qui concerne la création de rapports, seuls les rapports de synthèse sont disponibles en mode Anonyme. La fonction d'analyse des détails dans les rapports de synthèse, les rapports clients et les rapports détaillés n'est disponible que lorsque le mode Anonyme est désactivé.

Comment activer l'anonymisation des données utilisateurs ?

Lors de la première configuration de Dimension sur une appliance Firebox, il est possible d'activer l'anonymisation des données utilisateurs via l'assistant de configuration Dimension. Si Dimension est déjà déployé, l'anonymisation des données utilisateurs peut être activée via les pages Gestion du serveur et Gestion des accès.

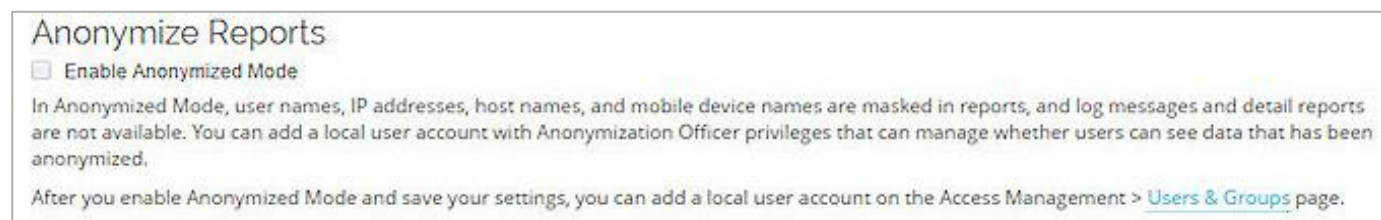


Figure 2. Configuration de l'anonymisation des données après le déploiement de Dimension sur une appliance Firebox.

Qu'est-ce que le responsable de l'anonymisation des données ?

Le **responsable de l'anonymisation des données** est un nouveau rôle disponible dans Dimension pour prendre en charge la conformité au RGPD, semblable au nouveau rôle de délégué à la protection des données présenté dans la réglementation du RGPD. Le rôle de responsable de l'anonymisation des données a été créé de sorte qu'une personne disposant ou non de compétences techniques puisse l'occuper. Il permet de respecter le principe d'authentification du « double regard » ou de la double connexion. Par exemple, si un administrateur informatique a besoin de désactiver le mode Anonyme de Dimension, il doit d'abord obtenir l'approbation du responsable de l'anonymisation. Cela permet

d'éviter les situations où une seule personne détient tous les accès aux informations permettant une identification personnelle, sans aucune responsabilité ou vérification externe.

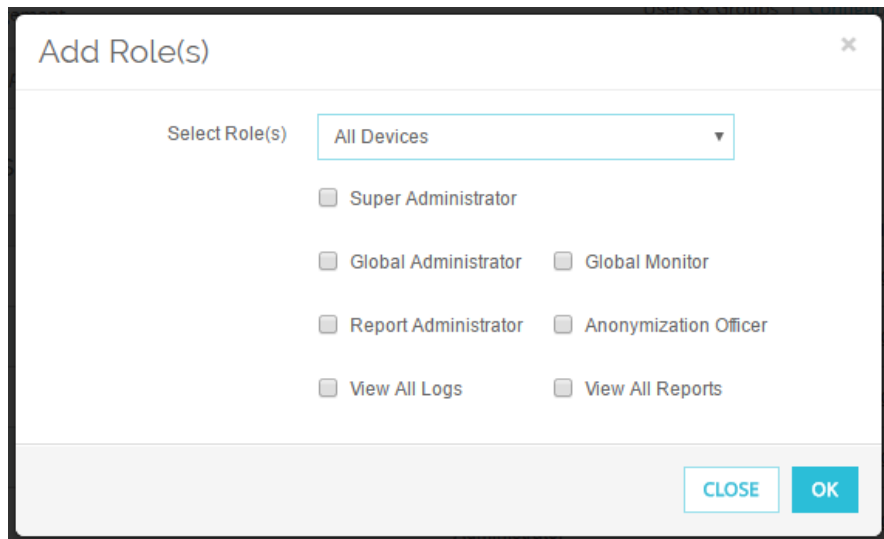


Figure 3. La fonction d'anonymisation des données utilisateurs permet de désigner aisément un responsable de l'anonymisation.

Contrôle

Le contrôle survient lorsque le mode Anonyme d'une session Dimension est désactivé. Dimension enregistre toutes les activités réalisées. Ainsi, les actions de l'utilisateur sont suivies, permettant aux entreprises de responsabiliser leurs équipes informatiques lorsqu'elles ont accès à des données contenant des informations permettant une identification personnelle. Le contrôle peut survenir dans Dimension lorsque le mode Anonyme est activé ou désactivé. Lorsque le mode Anonyme est activé, le contrôle peut être limité aux sessions désanonymisées.

Administrator Logging

- ☐ Send an audit log message when an administrator selects any page in Dimension
 - ☐ Only send audit log messages when Anonymized Mode is enabled and the Anonymization Officer has also logged in to disable Anonymized Mode

You must log out and log in again for changes to this option to take effect. Changes to this option apply to all future administrator sessions.

Figure 4. La configuration est très simple, que vous souhaitiez créer un journal de contrôle de toutes les actions réalisées dans Dimension, ou limiter cet enregistrement aux sessions désanonymisées pour lesquelles le mode Anonyme est activé.

Pour en savoir plus sur l'anonymisation des données utilisateurs et les puissants outils de visibilité réseau Dimension de WatchGuard, visitez le site www.watchguard.com/ua.

ADRESSE :

La Grande Arche
Paroi Nord
92044 PARIS LA DÉFENSE

SITE WEB :

www.watchguard.com

**SERVICE COMMERCIAL
AMÉRIQUE DU NORD :**

+1.800.734.9905

**SERVICE COMMERCIAL
INTERNATIONAL :**

+1.206.613.0895

À PROPOS DE WATCHGUARD

WatchGuard® Technologies, Inc. est un leader mondial de solutions de sécurité métier intégrées et multifonctions qui associent de manière intelligente matériel standard du secteur, fonctions de sécurité de pointe et outils de gestion basés sur des règles. WatchGuard fournit des solutions de protection puissantes mais faciles à utiliser à des centaines de milliers d'entreprises dans le monde. WatchGuard a établi son siège social à Seattle, dans l'État de Washington, et possède des bureaux aux États-Unis, en Europe, en Asie-Pacifique et en Amérique latine. Pour en savoir plus, visitez le site WatchGuard.com.

Le présent document ne contient aucune garantie expresse ou tacite. Toutes les spécifications peuvent faire l'objet de modifications, et les futurs produits, caractéristiques ou fonctionnalités prévus seront fournis dès qu'ils seront disponibles. © 2016 WatchGuard Technologies, Inc. Tous droits réservés. WatchGuard, le logo WatchGuard et WatchGuard Dimension sont des marques commerciales ou des marques déposées de WatchGuard Technologies, Inc. aux États-Unis et/ou dans d'autres pays. Toutes les autres marques appartiennent à leurs détenteurs respectifs.

Référence WGCE66913_051316