DÉCODER LE RGPD

Comment Bitdefender aide les entreprises à se conformer au RGPD

Fabrice Le Page
Marketing Manager

Vincent Meysonnet
Responsable Technique Avant-Vente

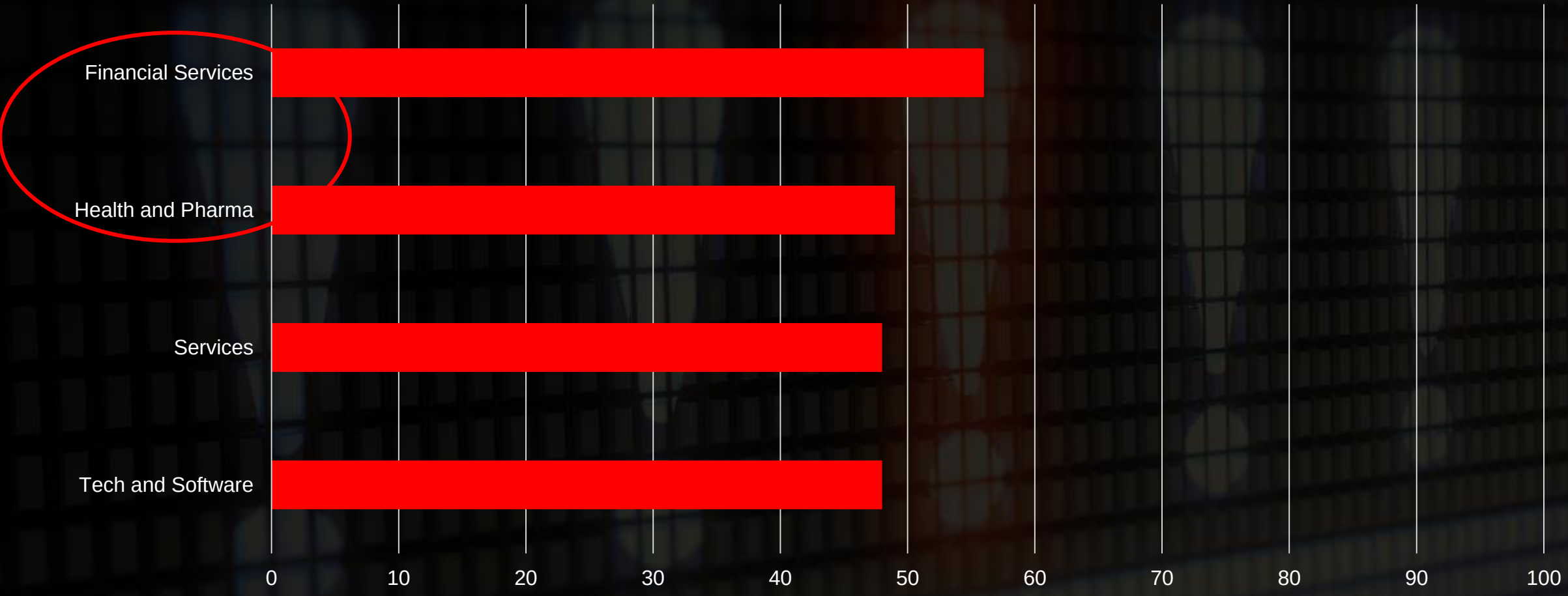
Bitdefender

RÈGLEMENTS SUR LA PROTECTION DES DONNÉES

- NORME DE SÉCURITÉ DE L'INDUSTRIE DES CARTES DE PAIEMENT (PCI DSS)
  Mondial – standard de sécurité des données pour les principaux groupes de cartes de paiement
- LOI SARBANES-OXLEY (SOX)
  U.S. – loi visant à protéger les investisseurs en améliorant l'exactitude et la fiabilité des publications des entreprises -Toutes les industries
- HEALTH INSURANCE PORTABILITY & ACCOUNTABILITY ACT (HIPAA)
  U.S. – obligatoire pour toutes les entreprise du marché de l'assurance maladie et autres entités liées
- HEALTH INFORMATION TECHNOLOGY FOR ECONOMIC AND CLINICAL HEALTH ACT (HITECH)
  U.S. – obligatoire pour toutes les entreprises traitant de données médicales
- GRAMM-LEACH-BLILEY ACT (GLBA)
  U.S. – obligatoire pour les entreprises de services bancaires et financiers

- **NOUVEAU :** RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES (RGPD)
  Mondial – obligatoire pour toutes les entreprises traitant de données personnelles de citoyens de l'Union européenne - Toutes les industries – Mise en place le 25 mai 2018

POURCENTAGE D'ENTREPRISES UTLISANT LE CHIFFREMENT PAR SECTEUR D'ACTIVITÉ



Source : 2016 Global Encryption Trends Study, Ponemon Institute© Research Report

Les données, dont les données personnelles, sont rapidement devenues l'élément vital de l'économie mondiale.
Elles représentent un nouveau type d'actif économique clé.

Bitdefender

OBJECTIFS DU RGPD

DÉFINIR DES RÈGLES UNIFORMES POUR TOUS LES PAYS

Bitdefender

OBJECTIFS DU RGPD

PROTÉGER L'INDIVIDU
EN TANT QUE PERSONNE PHYSIQUE

Bitdefender

OBJECTIFS DU RGPD

RESPONSABILISER LES ENTREPRISES ET LEURS DIRIGEANTS

Bitdefender

QU'EST-CE QUI EST NOUVEAU AVEC LE RGDP ?

- Définition plus large de ce qu'on appelle les "données personnelles" - Toute information relative à une personne physique identifiée ou identifiable
- Portée territoriale accrue - Toutes les entreprises traitant de données de citoyens de l'Union européenne, indépendamment de la localisation de l'entreprise
- Pénalités accrues – jusqu'à 4% du chiffre d'affaires, ne peut pas dépasser 20 millions d'euros
- Pouvoirs d'investigation et de correction étendus - Les autorités de surveillance disposent de larges pouvoirs d'investigation et de correction, y compris les audits de protection des données sur place et le pouvoir d'émettre des avertissements publics
- Définition du rôle des Responsables de traitement (Data Controller) et du sous-traitant (Data processor)
- Notifications des violations de données aux autorités de surveillance et aux personnes concernées au plus tard 72h après la découverte de la violation
- Droit de demander une indemnisation – Le RGPD permet aux particuliers de déposer des plaintes beaucoup plus facilement

VIOLATION DE DONNÉES À CARACTÈRE PERSONNEL

“une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données.”

Article 4(12) du RGPD

Bitdefender

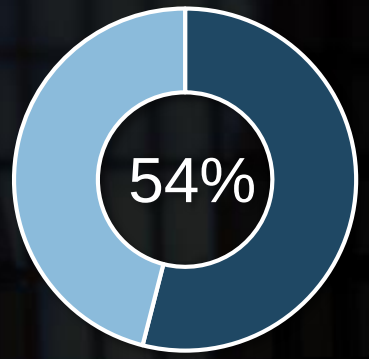
L'APPROCHE DE BITDEFENDER POUR LA PROTECTION DES DONNÉES

L'approche de Bitdefender se décompose en 4 étapes :

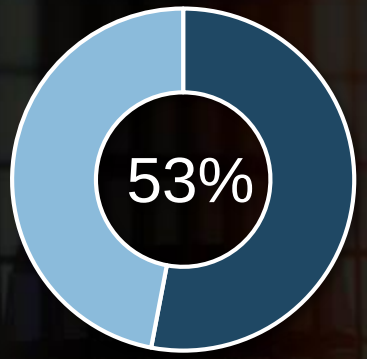
1. Identifier quelles données personnelles vous stockez et traitez
2. Évaluer les risques auxquels vos données sont exposées
3. Définir des contrôles techniques et procéduraux pour atténuer les risques
4. Améliorer la visibilité et la capacité à détecter et à répondre aux incidents

DÉFIS EN MATIÈRE D'IT ET D'IMPLEMENTATION

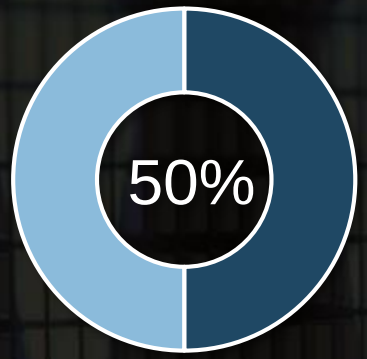
QUELLES EXIGENCES LIÉES AU RGPD VOUS SERONT VOS PLUS GRANDS DÉFIS ?



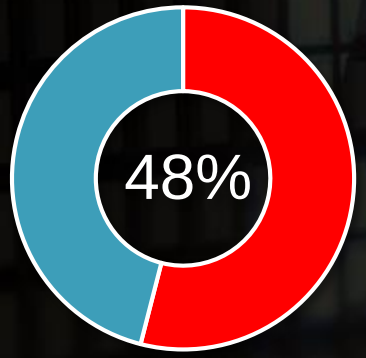
Chiffrement et/ou anonymisation des données



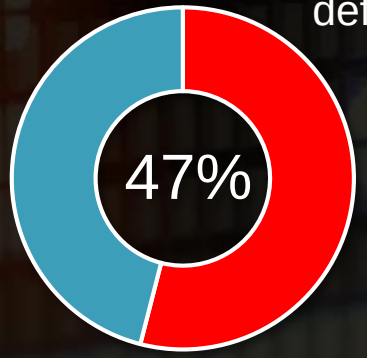
Notification d'une violation de données dans les 72h



Protection des données dès la conception et par défaut



Portabilité des données



Définition des meilleurs process et technologies à mettre en place

IDC ANALYZE THE FUTURE

BITDEFENDER AIDE LES ENTREPRISES À SE CONFORMER AU RGPD

Atténuer le risque d'exfiltration de données par des attaques Web ou des périphériques

- Contrôle de contenu et filtrage Web
- Machine Learning, Process Inspector, Anti-Exploit
- Contrôle des périphériques

Atténuer le risque d'exposition des données à cause de dispositifs perdus/volés

- Full Disk Encryption

Améliorer la visibilité et la capacité à répondre aux incidents de données

- Visibilité en temps réel et rapports sur les incidents
- Arrêt des processus, mise en quarantaine et remédiation

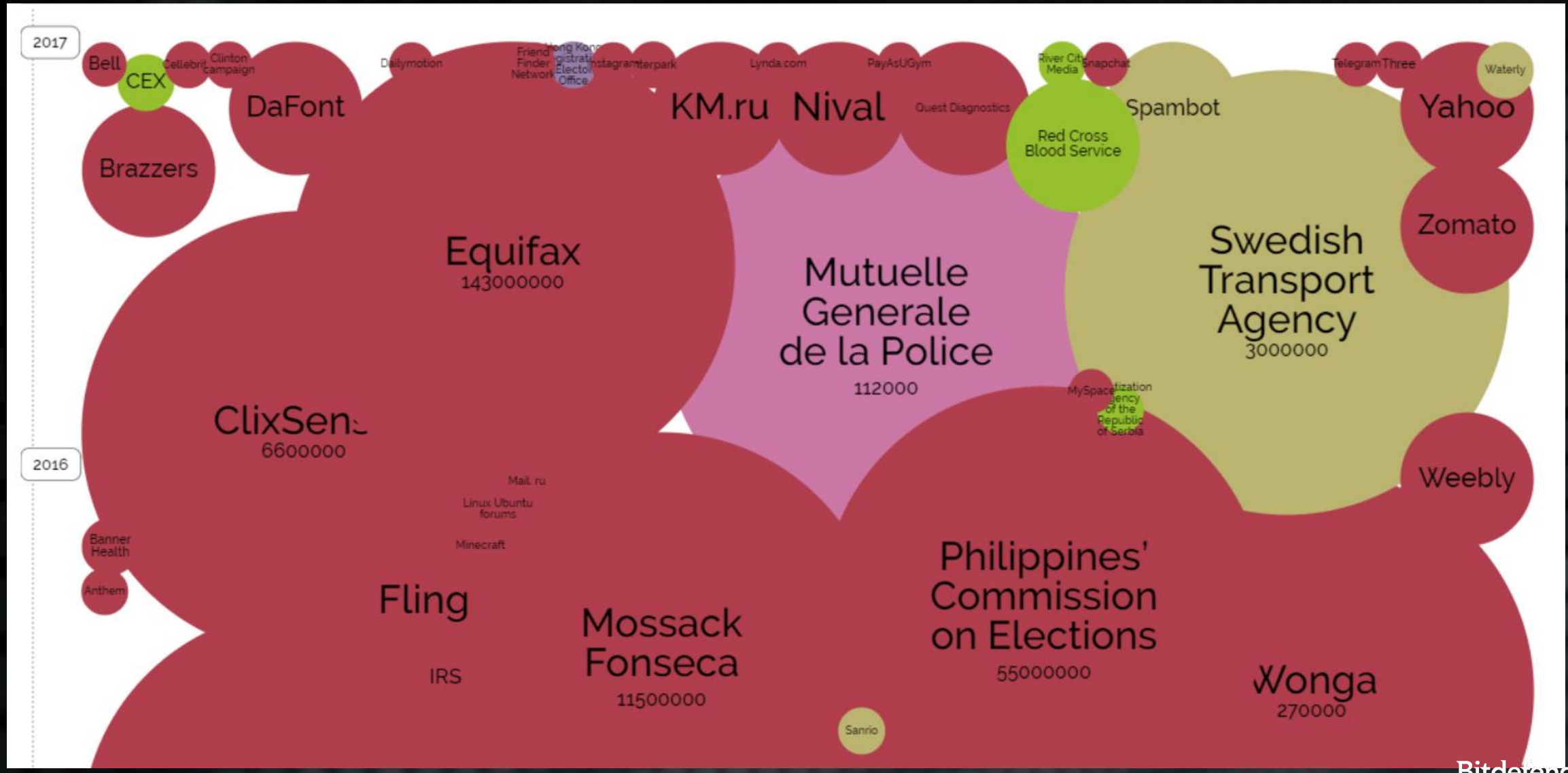
Bitdefender

ATTÉNUER LE RISQUE D'EXFILTRATION DES DONNÉES

VIA DES ATTAQUES WEB OU DES PÉRIPHÉRIQUES AMOVIBLES

Bitdefender

LES PLUS GRANDES VIOLATIONS DE DONNÉES AU MONDE



* - Sources : http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Bitdefender

PLATEFORME DE SÉCURITÉ MULTI-COUCHES NEXT-GEN

RENFORCEMENT & CONTRÔLE

Contrôle des applications

Contrôle de contenu

Antiphishing

Pare-feu

Contrôle des périphériques

Full-Disk Encryption

DÉTECTION MULTI-NIVEAUX

PRÉ-EXÉCUTION

Recherche par signature et dans le cloud

Machine Learning (Local & Cloud)

HyperDetect

Sandbox Analyzer

À L'EXÉCUTION

Anti-Exploit

Process Inspector

ACTION AUTOMATIQUE

Blocage des accès

Quarantaine

Désinfection / Suppresion

Arrêt des processus

Annulation des modifications

VISIBILTÉ & RAPPORTS

Rapports et tableau de bord personnalisables

Indicateurs de compromission

Activités suspectes

Contexte sur les menaces

Alertes et notifications

PLATEFORME DE SÉCURITÉ MULTI-COUCHES NEXT-GEN

Contrôle de contenu

Contrôle des périphériques

Machine Learning
(Local et Cloud)

Anti-Exploit

Process Inspector

Contrôle de contenu

- Analyse du trafic entrant et des e-mails
- Blocage des URL via analyse comportementale et ML
- Filtrage par catégories Web

Contrôle des périphériques

Permet aux administrateurs de gérer les autorisations pour les périphériques externes, tels que les clés USB, les périphériques Bluetooth, etc.

Machine Learning dynamique

Des algorithmes entraînés sur plus de 500M d'endpoints et 3 trillions d'échantillons pour une efficacité maximale avec peu de faux positifs

Protection contre les exploits

Détecte les techniques d'exploits et protège la mémoire des navigateurs, des visionneuses, des lecteurs et des applications bureautiques

Process Inspector

Détection proactive et dynamique des menaces inconnues basée sur la surveillance en continu des processus et des événements système, et le marquage des activités suspectes

Bitdefender

ATTÉNUER LE RISQUE D'EXPOSITION DES DONNÉES

À CAUSE DE DISPOSITIFS PERDUS/VOLÉS

Bitdefender

STATISTIQUES SUR LES PERTES DE DONNÉES EN 2016

554 millions d’enregistrements de données ont été perdus au 1er trimestre 2016

45% des violations de données dans le secteur médical sont liées à la perte d’un appareil

Source : Verizon 2016 Data Breach Investigations Report

Bitdefender

POURQUOI LES ENTREPRISES ONT-ELLES BESOIN DE CHIFFRER LEURS DONNÉES ?

Une exigence pour le business *ET/OU* une exigence de conformité

GRAVITYZONE FULL DISK ENCRYPTION

- Se base sur le chiffrement natif Windows BitLocker and macOS FileVault pour assurer les meilleures compatibilité et performance
- Intégration à la console d'administration GravityZone pour un déploiement, une gestion et une récupération des clés centralisés
- Aucun agent supplémentaire ou serveur de gestion de clés requis
- Rapports dédiés au chiffrement, dans le cadre du RGPD
- Renforcement de l'authentification avant démarrage

Bitdefender

AMÉLIORER LA VISIBILITÉ ET LA CAPACITÉ À RÉPONDRE AUX INCIDENTS DE DONNÉES

Bitdefender

PLATEFORME DE SÉCURITÉ MULTI-COUCHES NEXT-GEN

RENFORCEMENT & CONTRÔLE

Contrôle des applications

Contrôle de contenu

Antiphishing

Pare-feu

Contrôle des périphériques

Full-Disk Encryption

DÉTECTION MULTI-NIVEAUX

PRE-EXECUTION

Recherche par signature et dans le cloud

Machine Learning (Local & Cloud)

HyperDetect

Sandbox Analyzer

ON-EXECUTION

Anti-Exploit

Process Inspector

ACTION AUTOMATIQUE

Blocage des accès

Quarantaine

Désinfection / Suppresion

Arrêt des processus

Annulation des modifications

VISIBILTÉ & RAPPORTS

Rapports et tableau de bord personnalisables

Indicateurs de compromission

Activités suspectes

Contexte sur les menaces

Alertes et notifications

Endpoint Security HD

- Exécution à distance (Sandbox)
- Fournit un meilleur contexte sur les menaces
- Relie les menaces avec les actions des menaces
- Fournit une visibilité améliorée sur les endpoints afin de réaliser des analyses plus détaillées et prendre les actions appropriées
- Expose les menaces suspectes (rapports HD)

Analyses de sécurité

- Détecte des pics dans l'activité des malwares
- Détecte les botnets et les connexions à des serveurs C&C
- Détecte le téléchargement de fichiers suspects (attaques ciblées)
- Détecte l'exécution de processus suspects (attaques sans fichier)
- Détecte les comportements anormaux d'applications et du système (exfiltration de données et mouvement latéral)
- Détecte les menaces internes (utilisateurs malveillants/comptes utilisateurs compromis)

L'APPROCHE DE BITDEFENDER POUR LA PROTECTION DES DONNÉES

L'approche de Bitdefender se décompose en 4 étapes :

1. Identifier quelles données personnelles vous stockez et traitez
2. Évaluer les risques auxquels vos données sont exposées
3. Définir des contrôles techniques et procéduraux pour atténuer les risques
4. Améliorer la visibilité et la capacité à détecter et à répondre aux incidents

MERCI !

PROTECTING **500 MILLION USERS** WORLWIDE

Bitdefender

RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES (RGPD)

Quand : ratifié en 2016, mise en place le 25 mai 2018

Où : règlement de l'Union européenne s'appliquant à toutes les entreprises traitant (directement ou non) de données personnelles de citoyens de l'Union européenne

Directives principales :

- Définit clairement les données personnelles
- Définit les rôles du Responsable de traitement (Data Controller) et du sous-traitant (Data processor)
- Définit les obligations des Responsable de traitement et du sous-traitant (directives non techniques)
- Définit le nouveau rôle du Délégué à la protection des données (Data Protection Officer)
- Redéfinit la gestion de la vie privée
- Définit comment le consentement de l'utilisateur doit avoir lieu
- Définit les droits de la personne concernant ses données personnelles
- Définit l'application et les amendes

RGPD

LES SOLUTIONS BITDEFENDER QUI VOUS AIDENT À ÊTRE CONFORME

GravityZone Full Disk Encryption *en tant qu'add-on*

GravityZone Elite Security – intègre :

- *HyperDetect*
- *Sandbox Analyzer*
- *Protection avancée pour les exploits*

GravityZone Enterprise Security – intègre:

- *Contrôle des applications*

Hypervisor Introspection (HVI)

GravityZone Security for Virtualized Environments

ET SI ON EST PAS AU COURANT D'UNE VIOLATION DE DONNÉES ?

Exemple : Equifax (agence américaine de crédit) a découvert une violation de données en juillet alors qu'elle avait eu lieu en mai ! Violation a utilisé une faille informatique pour laquelle un patch existait !

Difficulté pour l'entreprise : comment justifier le fait de ne pas savoir ce qui se passe au sein même de son infrastructure ?

Légalement : pas précisé clairement dans le RGPD. Ce qui est certain c'est que le RGPD précise que vous avez 72h pour déclarer une violation de données découverte

Conclusion : être proactif, déployer les bons outils, avoir les bonnes procédures et former les employés