VARONIS

Our mission is to protect data from insider threats and cyberattacks.

# Are You Protecting Data or Chasing Threats?

## Understanding Insider Threats

# Introduction

We know where our sensitive data lives

Only the right people have access

Cyber threats are detected and stopped

Sustain a secure state without manual effort

# Introduction – la société

- La société:
  - Siège à NY (USA) / 300 développeurs
  - Siège Europe continentale à Paris
  - 1000+ Collaborateurs
  - Présent sur les 5 continents
  - 5000+ clients, 1000 en France
  - 30 à 40 % de croissance par an

Gartner

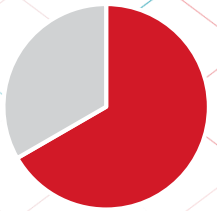
Market Analysis

File analysis is used for three primary reasons:

1. Increase operational efficiency
2. Lower IT costs
3. Mitigate corporate risk

WW File Analysis Market

**Varonis détient 60 % des parts de marché WW – le n°2 en détient 3%**



VARONIS  Autres éditeurs(25)

Data Audit & Protection

VARONIS DATADVANTAGE

Ensure that only the right people have access to the right data at all times, monitor use, alert on abuse.

User Behavior Analytics

VARONIS DATALERT

Detect suspicious activity across disparate platforms in real-time, helping you prevent data breaches.

Data Access Governance

VARONIS DATAPRIVILEGE

Give business users the power to review and manage permissions without IT assistance.

Enterprise Search & eDiscovery

VARONIS DATANSWERS

Deliver relevant search results without exposing sensitive information.

Enterprise File Sync & Share

VARONIS DATANYWHERE

A secure Dropbox alternative that syncs with your existing file shares and NAS.

Data Classification

VARONIS IDU CLASSIFICATION FRAMEWORK

Quickly discover where sensitive information is vulnerable and safely lock it down.

VARONIS

# De quoi cherche t-on à se protéger?

Les données personnelles de quelque 800.000 clients d'Orange ont été dérobées à la suite d'une intrusion informatique dans les serveurs de l'opérateur. Le point sur les informations disponibles sur cette attaque.

Attention danger ! Orange a été victime d'une attaque informatique et des données personnelles de centaines de milliers de ses clients internet ont été dérobées.

## 272 millions de comptes piratés : votre mail est-il dans la liste ? Faites le test

MIS À JOUR : 06-05-2016 15:11 - CRÉÉ : 06-05-2016 14:24

**PROTECTION - Hier, metronews vous rapportait les méfaits d'un jeune collectionneur Russe parvenu à s'emparer de près de 272.3 millions de courriers électroniques et données personnelles. Comment savoir si vous vous êtes fait avoir ? Le site Have I Been Pwned permet d'en avoir le cœur net.**

## Au procès LuxLeaks, le lanceur d'alerte accusé témoigne

Le procès LuxLeaks à Luxembourg entame sa deuxième et dernière semaine avec l'audition, très attendue, d'Antoine Deltour, la principale source de l'affaire.

Les données personnelles de 112.000 policiers ont fuité sur le web

## « SwissLeaks » : révélations sur un système international de fraude fiscale

« Le Monde » a eu accès aux données bancaires de plus de 100 000 clients de la filiale suisse d'HSBC. Elles révèlent l'étendue d'un système de fraude fiscale encouragé par la banque. Des personnalités étrangères et françaises sont impliquées.

## CHRONOPOST EST LA CIBLE D'UNE NOUVELLE CAMPAGNE DE PHISHING

FRÉDÉRIC PEREIRA | 30 septembre, 2016 at 11:00 — 0 COMMENTAIRE

## Ransomware : une attaque toutes les 40 secondes contre les PME

On assiste à un triplement des attaques de ransomware contre les PME en 2016. (Crédit D.R.)

**Entre janvier et septembre 2016, le nombre d'attaques de ransomware contre les entreprises a triplé. En septembre, Kaspersky Lab enregistrait une attaque de ce type toutes les 40 secondes contre une toutes les 2 minutes en début d'année. Une entreprise sur cinq dans le monde est concernée.**

Selon un rapport de l'entreprise de sécurité Kaspersky Lab, entre janvier et septembre 2016, la fréquence des attaques de ransomware contre les entreprises est passée

## The US Now Thinks Snowden 'Probably Downloaded' 1.5 Million Documents That Haven't Been Found

> Wikileaks
> J'effaçais la musique d'un CD musical et je créais un dossier compressé contenant les documents.

## "Panama Papers" : des révélations sur un scandale mondial d'évasion fiscale

MIS À JOUR : 05-04-2016 22:35 - CRÉÉ : 03-04-2016 20:23

**EVASION FISCALE – Des journalistes de 76 pays ont eu accès à des milliers de documents, qui révèlent comment de nombreuses personnalités politiques et sportives ont dissimulé leur argent dans des paradis fiscaux. Parmi les noms divulgués, dimanche, ceux de Michel Platini ou encore Jérôme Cahuzac.**

Yahoo! a été victime d'un piratage massif, confirmé hier soir. Les données liées à 500 millions de ses comptes ont été récupérées par des pirates à la fin de l'année 2014. Parmi elles, des noms, adresses, emails et dates de naissance, mais aussi des mots de passe chiffrés. Selon le communiqué de presse de Yahoo!, les informations bancaires seraient restées hors de portée des hackers.

*Administrateur malveillant*

*Employé malveillant / lanceur d'alerte*

*Ransomware / Autre type de malware*

*Hacker / Hacktivistes*

VARONIS

# Security landscape - 2016

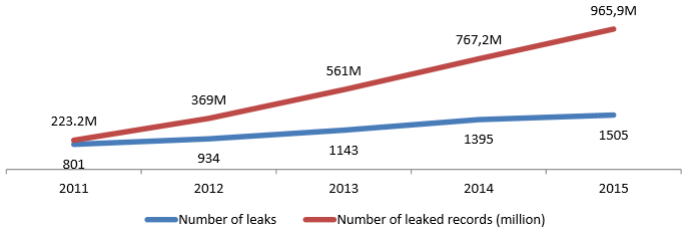



Fig 1. Registered data leaks

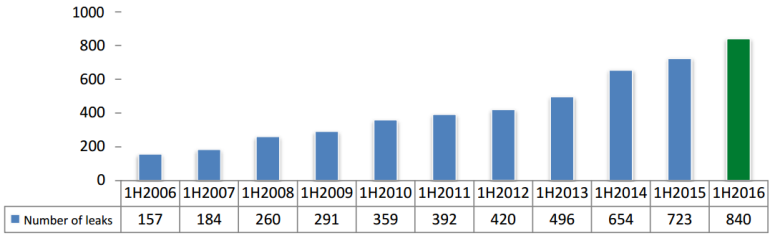



Fig 2. Number of registred data leaks

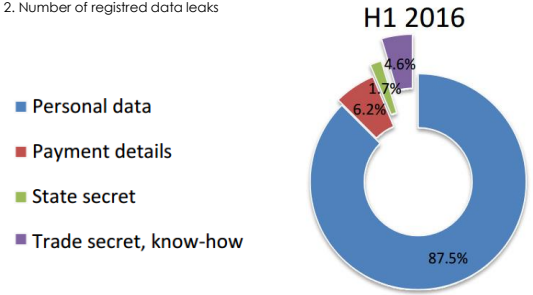



Fig 3. Leaked data types


- In 10 years, leaks have been multiplied by 10 in number
- 23 mega leaks occurred in H1 2016, each resulted in the loss of more than 10 million personal data records.
- In the GDPR context, and considering the high number of Personal Data Leaks records, the risk is huge for all WW companies. There will be lots of fines.

Source:
https://infowatch.com/sites/default/files/report/InfoWatch_Global_Report_2016_ENG.pdf

# Security landscape - 2016

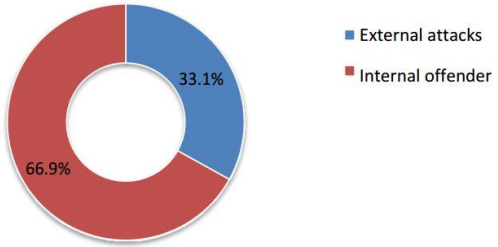



*Fig. 2. Leaks by attack vector[10], H1 2016*

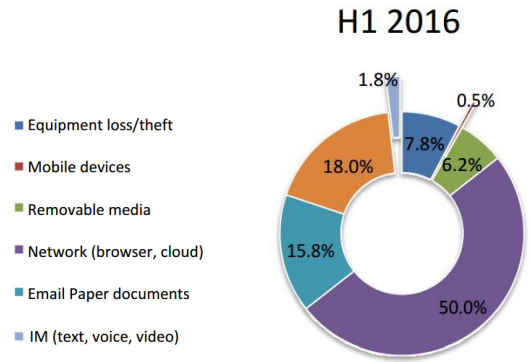



Fig. Leaks by channel

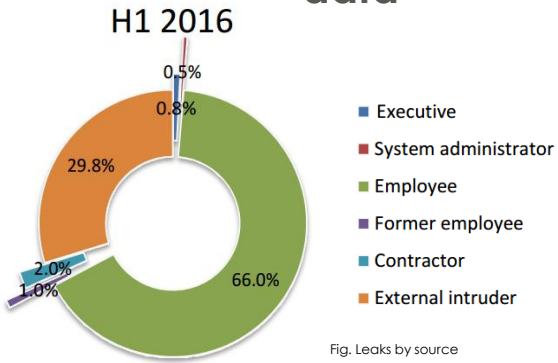
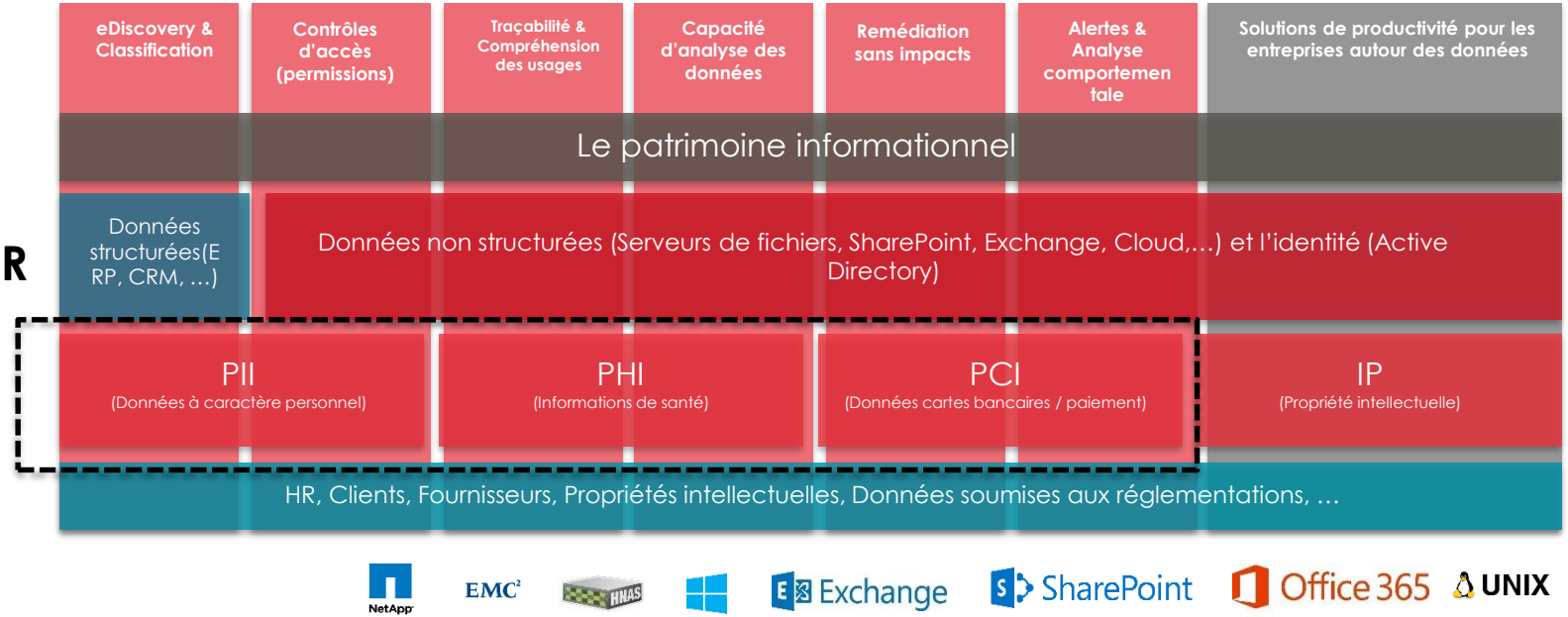



Fig. Leaks by source

- More than 60% of leaks come from insider thread and malicious insiders…
- Data that leaked was mainly from unstructured data:
  - Network + Cloud + Emails = 65%
- So the biggest concern companies should have as per GDPR is avoiding data leaks of personal data by securing **unstructured data**

Source:
https://infowatch.com/sites/default/files/report/InfoWatch_Global_Report_2016_ENG.pdf

# Proposition de valeur VARONIS



# Approche GDPR – sécurisation des données

## DETECT

insider threats by analyzing data, account activity, and user behavior.

1

Cartographie des permissions

Auditer toute l'activité des fichiers et des mails

Découvrir la donnée sensible et stagnante

Detecter automatiquement les comptes administrateurs, de services, et VIP

2

**Détecter les comportements anormaux**

- Crypto intrusion et autre malwares
- Escalade de privilège
- Accès anormal à la donnée personnel
- Fuite Interne
- Exposition de la donnée, …

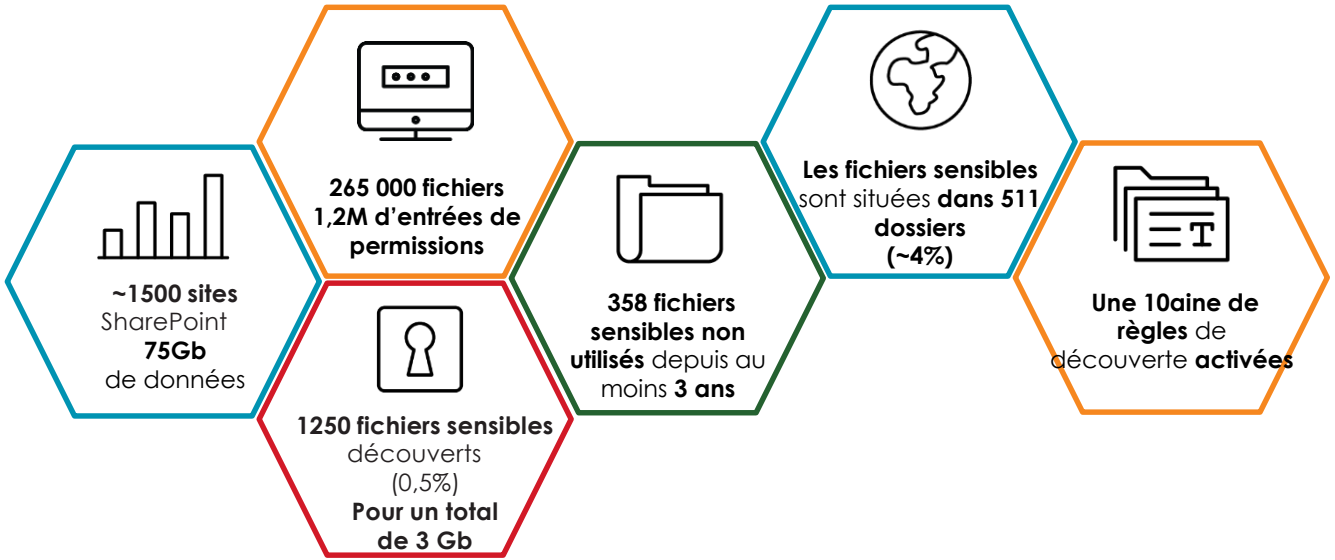
3

**Reporting de découverte sur la prioritization de la donnée sensible.**

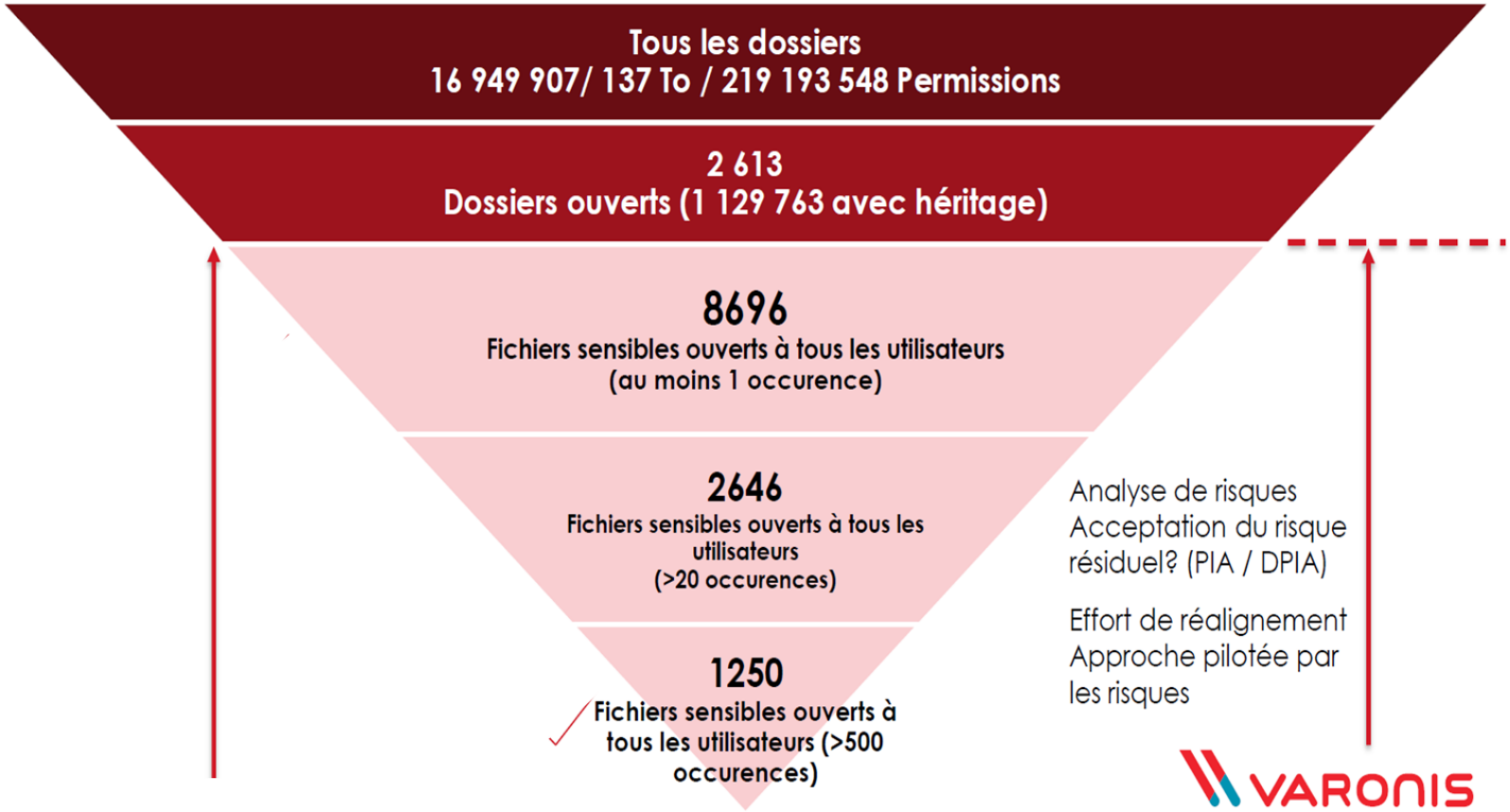
- Données actives vs Données mortes
- PII listing Vs fichiers contenant quelques PII
- Catégorisation des fichiers PII (Santé, Carte de crédits, numéro de Sécurité sociale, …)
- PII par criticité au regard de l'impact business (*ex: nom / prénom et localisation de personnes*)

VARONIS

# Exemples



# Approche GDPR par les risques : sécurisation des données non-structurées



# Approche GDPR – sécurisation des données

## PREVENT

disaster by locking down sensitive and stale data, reducing broad access, and simplifying permissions.

## 1 – Fait par l'IT

Corriger l'active directory et les serveurs de fichiers

Eliminer les groupes globaux

## 2 – Fait par le business et les proriétaires données

Identifier les propriétaires métiers / Acteurs de la donnée
*Article 30*

Purger les accès non nécessaires
*Article 25 & 32*

Les propriétaires métiers font des revues d'habilitation
*Article 25 & 32*

VARONIS

# Approche GDPR – sécurisation des données

## SUSTAIN

a secure state by automating authorizations, migrations, & disposition.

Surveiller en continu tous les Utilisateurs et l'activité fichiers

Détecter et corriger automatiquement les derives de l'état de l'art ou de la politique définie

Mise en quarantaine automatique de la donnée sensible (PII / PHI / PCI)

Automatisation de l'archivage ou de l'accessibilité de la donnée stagnante

Automatiser les revocations d'accès

# Thank You

Julien Chamonal
julien@varonis.com
www.varonis.com