Maitriser sa cybersécurité : visibilité et contrôle de bout en bout

Christophe AUBERGER
Cybersecurity Strategist, Cybersecurity Evangelist,
Innovation advocate, CISO Advisor

FY22Q3

Quelles sont les tendances sur la France ?

Nécessité d'une sécurité rapide et efficace

8 entités sur 10
subissent au moins une attaque par an[1]

1200 à 1300
notifications de violation de données personnelles en France depuis la mise en place de la RGPD[2]

Les attaques les plus fréquentes[1]

- 73% phishing
- 50% fraude au président
- 44% Malware

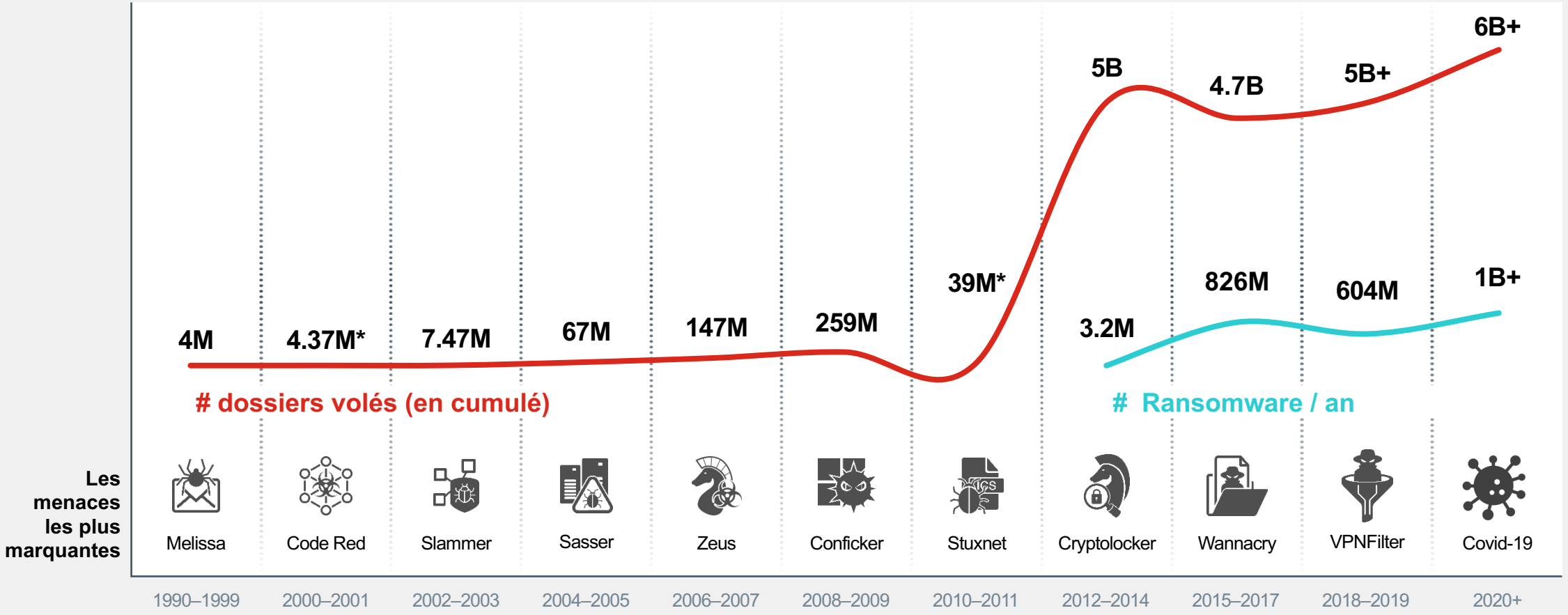
3 mois

Le temps moyen avant de découvrir une cyber attaque

Sources : 1. baromètre CESIN – sondage OpinionWay
2. CNIL

Les attaques sont toujours de + en + sophistiquées

Beaucoup d'attaques reposent encore fortement sur de la manipulation sociale



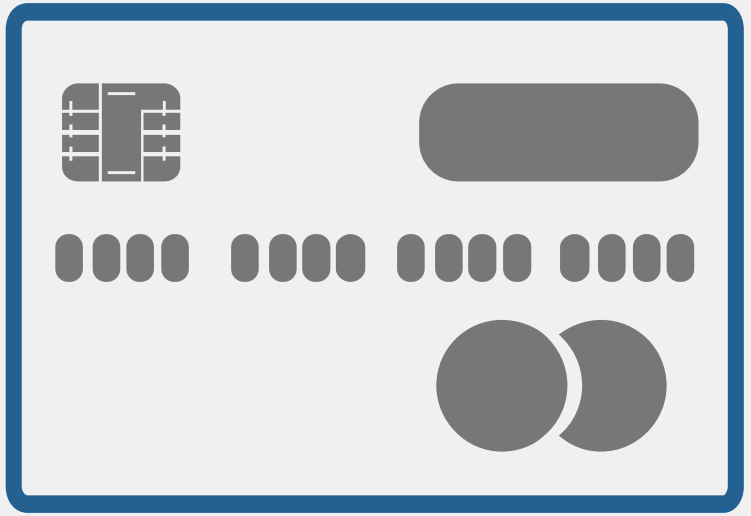
*Many undisclosed | Record Stolen Reference—Breach Level Index | Ransomware stats—Statista

© Fortinet Inc. All Rights Reserved.

Valeur des informations

10x

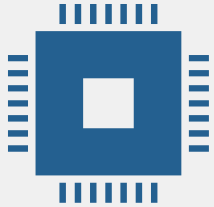
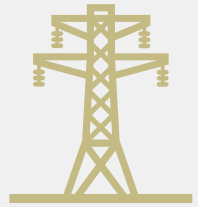
Les **données patient** valent **dix fois** plus qu'un numéro de carte bancaire

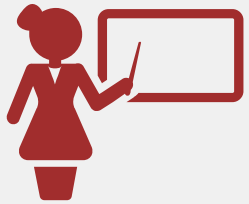


© Fortinet Inc. All Rights Reserved.

Valeur des informations

Coût internationaux des vols de données

Santé	Finance	Phamaceutique	Technologie	Energie
				
$408	$208	$188	$170	$167

Education	Client final	Distribution	Recherche	Publique
				
$166	$140	$116	$92	$75

Source: Ponemon Institute - 2018 Cost of Data Breach Study: Global Overview

© Fortinet Inc. All Rights Reserved.

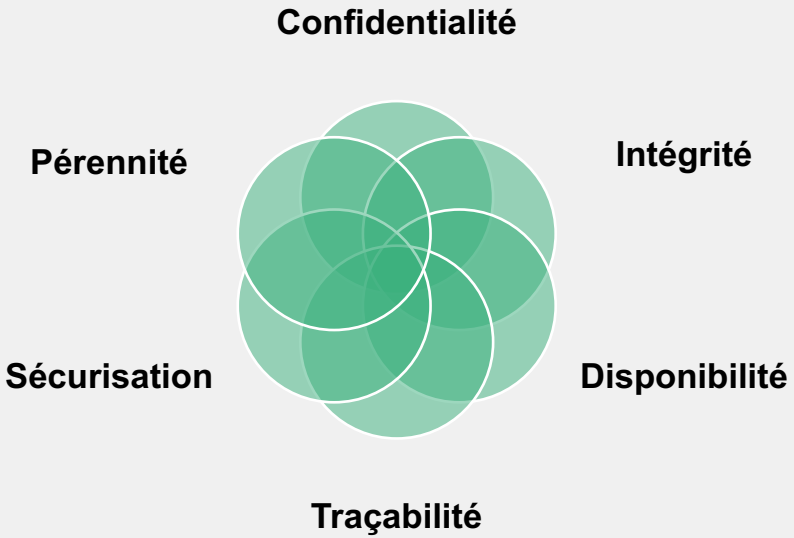
Etablissement de santé: Les enjeux

Le patient au centre de la transformation numérique

- Augmentation de la Surface d'attaque
- Des menaces de + en + sophistiquées
- Complexité de l'Ecosystème des fournisseurs

Partage/Protection des données

Enjeux du DPI



© Fortinet Inc. All Rights Reserved.

Etablissement de santé: Les enjeux

Vulnérabilité des devices (BYOD, Equipements médicaux)

76% | Du secteur fait la transition vers le Mobile/BYOD

72% | Des équipements ne sont pas sûrs

69% | Des applications utilisées sur les périphériques mobiles ne sont pas de sécurisées

Conformité et réglementation

REGULATORY

PCI DSS COMPLIANT

HIPAA COMPLIANT

GOVERNMENT

General Data Protection Regulation

CSCAP

CERTIFICATION

NSS LABS

ICSA labs CERTIFIED ANTI-VIRUS

CNIL.

MINISTÈRE DE LA DÉFENSE

Direction générale de l'offre de soins

asipsanté AGENCE DES SYSTÈMES D'INFORMATION PARTAGÉS DE SANTÉ

ars Agence Régionale de Santé

ISO

ASSISTANCE PUBLIQUE HÔPITAUX DE PARIS

HAS HAUTE AUTORITÉ DE SANTÉ

© Fortinet Inc. All Rights Reserved.

Etablissement de santé: Le contexte actuel

Volet Cybersécurité du plan France relance piloté par l'ANSSI,

Feuille de route du numérique en santé, 2023-2027

Programme CaRE

Des SI complexes

- Réseaux bureautiques et réseaux santé (imagerie, labos,…)
- Architecture multi-sites
- Un grand nombre d'équipements hétérogènes
- Hébergement physique d'entité externes/partenaires

Des équipes restreintes

- Problématique d'expertise sur l'ensemble des solutions
- Compliqué d'assurer le maintien en condition de sécurité
- Nécessité de s'appuyer sur des partenaires

Des SI en forte évolution

- Transformation numérique forte: DPI, BYOD, nomadisme
- GHT
- Evolution vers le Cloud
- Quid de l'hergement de données de santé ?

Une augmentation forte des risques

- Augmentation de la surface d'attaque
- Attaques plus complexes
- Secteur de la santé particulièrement ciblé

CONFORMITE ET REGLEMENTS

© Fortinet Inc. All Rights Reserved.

Les systems d’information ont fortement évolué

Forte distribution

+

Frontières floues

+

Maitrise réduite

= plus de zone de confiance

© Fortinet Inc. All Rights Reserved.


Réseaux
Accès au système d'information
NAC
Orchestration de la sécurité
Sécurité

FortiNAC: pas de confiance pour les équipements d’extrémité

59% visibilité sur moins de 75 % des actifs en réseau.

Visibilité

- Découvre les appareils connectés en quelques secondes.
- Couverture à 100 % avec une grande précision.

Découvrir et classer

57% des appareils IoT sont vulnérables aux attaques de gravité moyenne ou élevée

Contrôle

- Politique dynamique avec segmentation L2-L7.
- Authentification de ré-entrée pour une sécurité renforcée

Segmenter, Authentifier, Autoriser

56% des grandes organisations traitent plus de 1 000 alertes de sécurité chaque jour

Réponse

- Flux automatisé
- Orchestration entre NoC/SoC
- Incorporation avec les dernières informations sur les menaces

Détecter, répondre, corriger

© Fortinet Inc. All Rights Reserved.

Profondeur et portée de FortiNAC

20+

années d'expérience dans la technologie NAC et des innovations continues

21

Méthodes de profilage, actives ou passives

Découvre plus de

71,000+

modèles IoT uniques via les services FortiGuard IoT

2,500+

équipements réseau pris en charge de 95 fournisseurs

Gestion centralisée pour des équipements pouvant se compter en

Millions

© Fortinet Inc. All Rights Reserved.

FortiNAC un large éventail de cas d’usage

Gestion d’inventaire

Visibilité consolidée
Couverture complète

Micro-Segmentation

Des politiques d’accès granulaires, dynamiques et contextuelles

Conformité

Evaluation des risques
Vérification de la conformité

Zero Trust

Zero Trust pour les appareils finaux, accès dynamique, contextuel et basé sur les rôles

Intégration

Appareils BYOD, différents types d'utilisateurs, accès privilégiés, portails captifs,

Processus automatisé

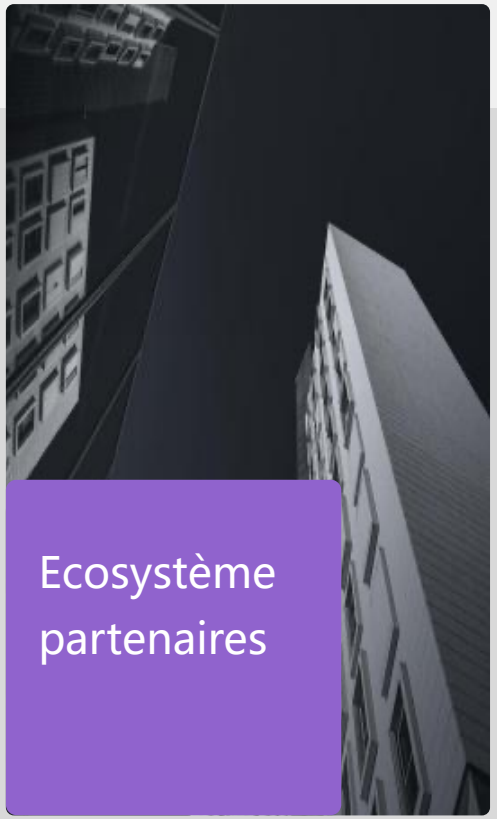
Réponse aux menaces, changement de politique, actions correctives

© Fortinet Inc. All Rights Reserved.

Avantages FortiNAC

Intégration Security Fabric

Multi-Vendeurs



Ecosystème partenaires

Automatisation et Orchestration

Dans la vraie vie

Automatisation et intégration

Partenaires de l'écosystème, orchestration

04

Personnaliser

Réglage fin

Contrôle d'accès granulaire, extension du cas d'utilisation, amélioration des performances

03

Contrôle

Segmentation du réseau, contrôle d'accès, détection des escrocs et réponse

02

Développer

Visibilité

Localisation

Réseau

Concevoir, interagir, tester

01

Equipements

Connectivité

Segment

© Fortinet Inc. All Rights Reserved.


FORTINET