Microsoft

IA et cybersécurité : enjeux et influences croisées ?

Mathieu Moreux
Product Marketing Manager, Cybersecurity
@mamoreux

« demain, il n’y aura pas une seule application, une seule expérience à laquelle vous participerez **qui ne sera pas pilotée par l’intelligence artificielle »**

Satya Nadella

Problématique

COMMENT L'IA PEUT-ELLE CONTRIBUER À MIEUX DÉTECTER ET RÉPONDRE AUX CYBER MENACES ?

COMMENT SÉCURISER L'IA ET PROTÉGER LES ALGORITHMES CONTRE LES DÉTOURNEMENTS ?


Véhicules
Villes intelligentes
Capteurs
Systèmes énergétiques
Places de marché
Equipement
Extension du patrimoine numérique
Partenaires
Clients
Citoyens
Chaines d'approvisionnement
Sur place
Manufacturiers
Terminaux mobiles

La nécessité d’une sécurité intelligente

30%	Le pourcentage de malwares qui sont des zero-day
3 mois	Le temps moyen avant de découvrir une cyber attaque
50%	Pourcentage des alertes traitées par les équipes de sécurité
$1.37M	Le coût annuel moyen lié au traitement des faux-positifs
1.87M	La pénurie d’experts cybersécurité dans le monde d’ici à 2021

La vue de Microsoft sur les menaces

12,000,000
tentatives d'accès frauduleux

4,000
ransomwares

167,000,000
malwares

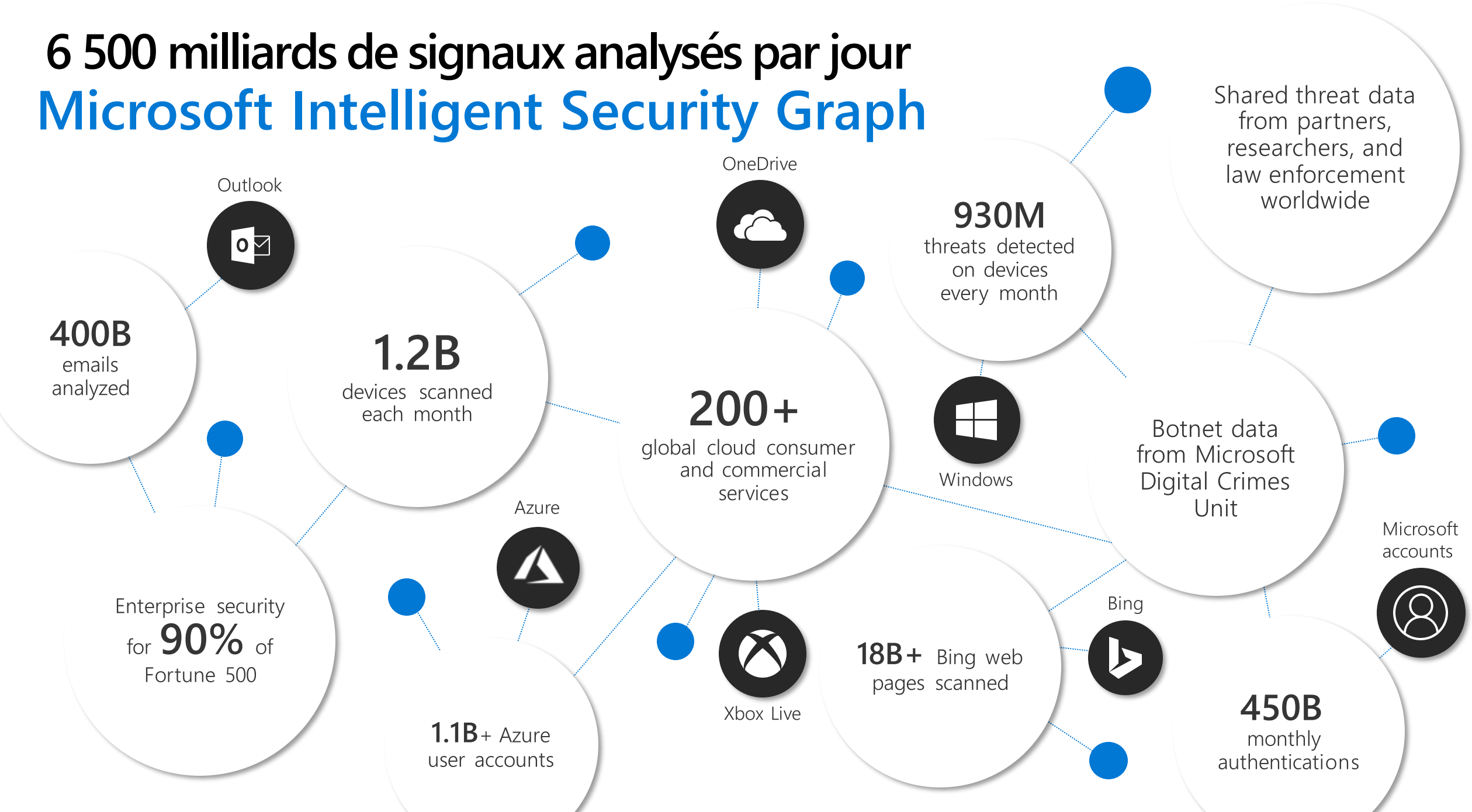
96%
des malwares sont polymorphiques

Objectif de l'intelligence artificielle

Construire des méthodes et des systèmes qui apprennent des données et s'améliorent avec l'expérience

6 500 milliards de signaux analysés par jour

Microsoft Intelligent Security Graph



Les atouts

Protéger nos utilisateurs le plus rapidement possible

Classifier un malware inconnu en quelques minutes

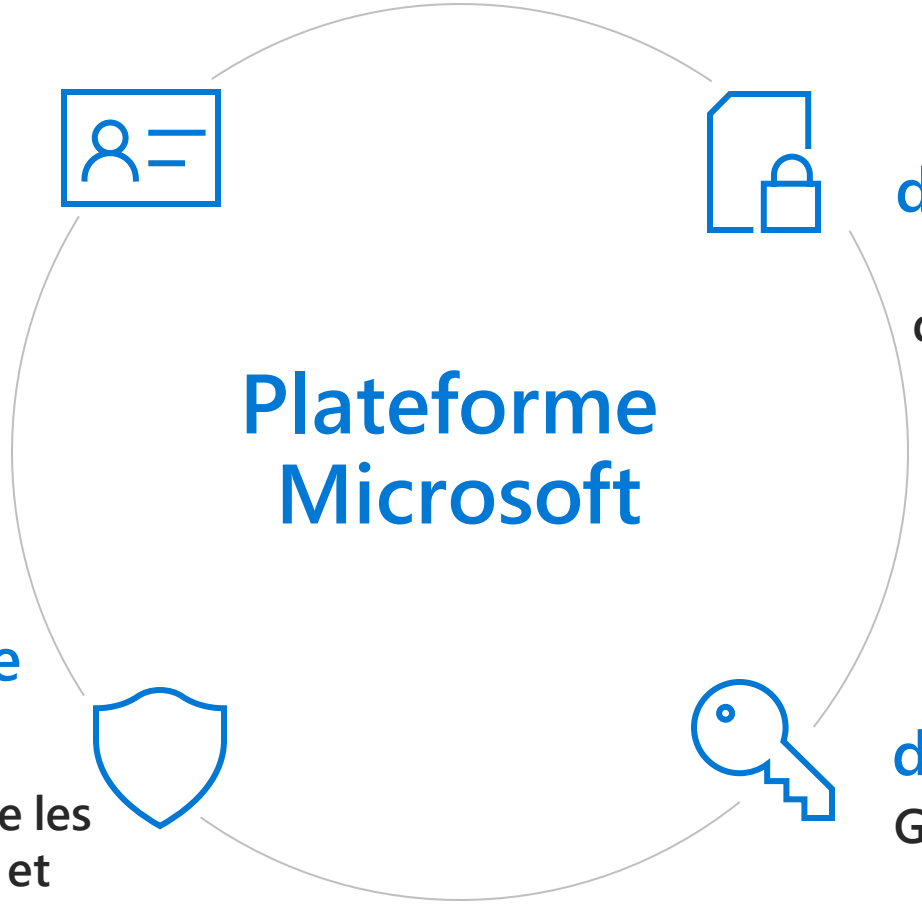
Traiter des millions de nouveaux malwares par jour

Hiérarchiser et prioriser les alertes

Détecter, répondre et remédier de manière automatisée

Collaborer avec l'intégration de modèles de ML open source

Une sécurité intelligente intégrée et non facultative



Gestion des accès et des identités

Protégez l'identité des utilisateurs et contrôlez l'accès aux ressources importantes

Protection des informations

Assurez-vous que les documents et les e-mails ne sont consultés que par des personnes autorisées

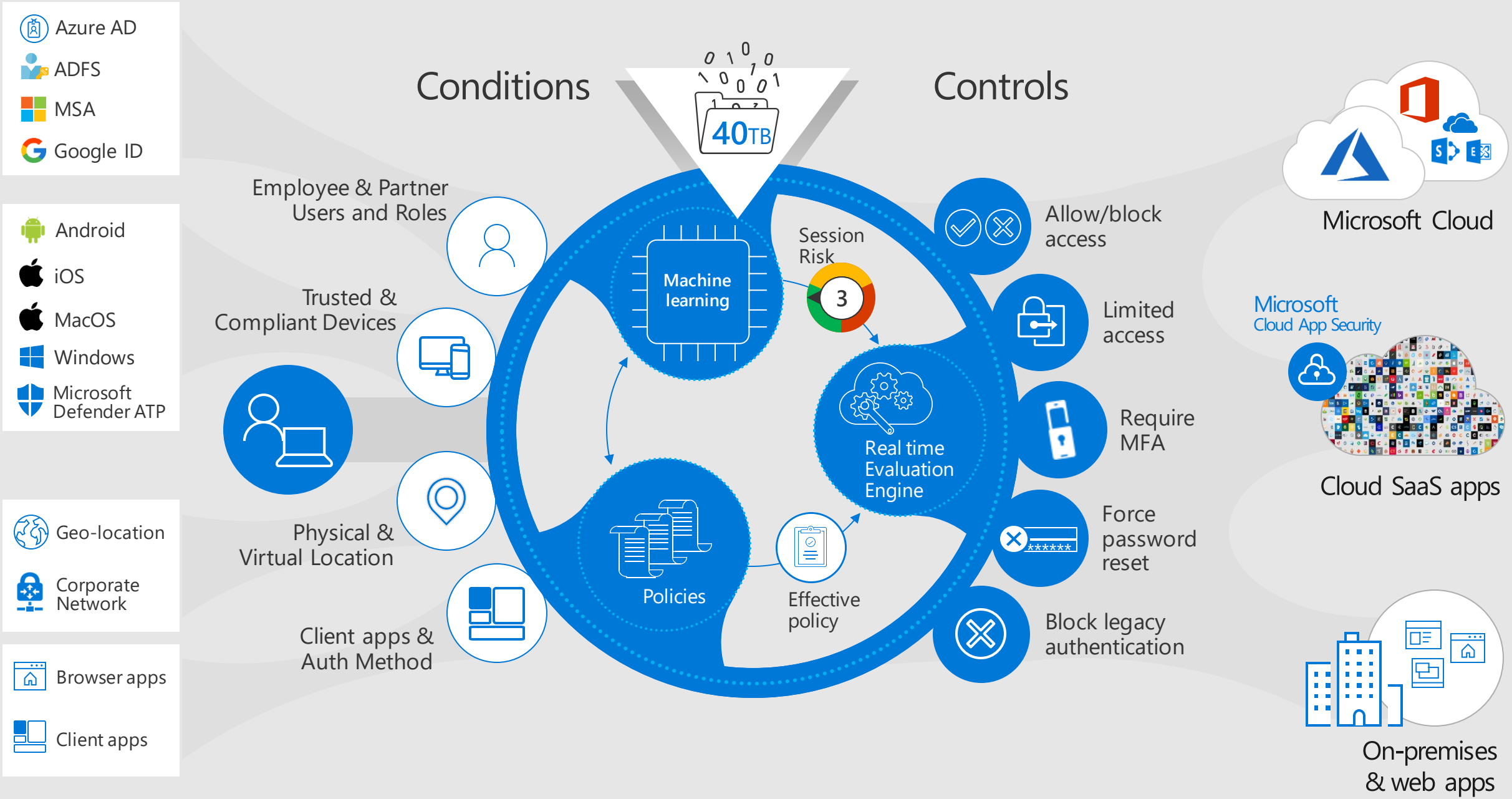
Protection contre les menaces

Protégez-vous contre les menaces avancées et répondez rapidement en cas d'attaque

Gestion de la sécurité

Gagnez en visibilité et en contrôle sur vos outils de sécurité

Un exemple : l'accès conditionnel dans Azure Active Directory pour l'IAM



L'exemple de BadRabbit

Ransomware polymorphique dans une fausse mise à jour d'Adobe Flash Player

Application du machine-learning local et du machine learning cloud

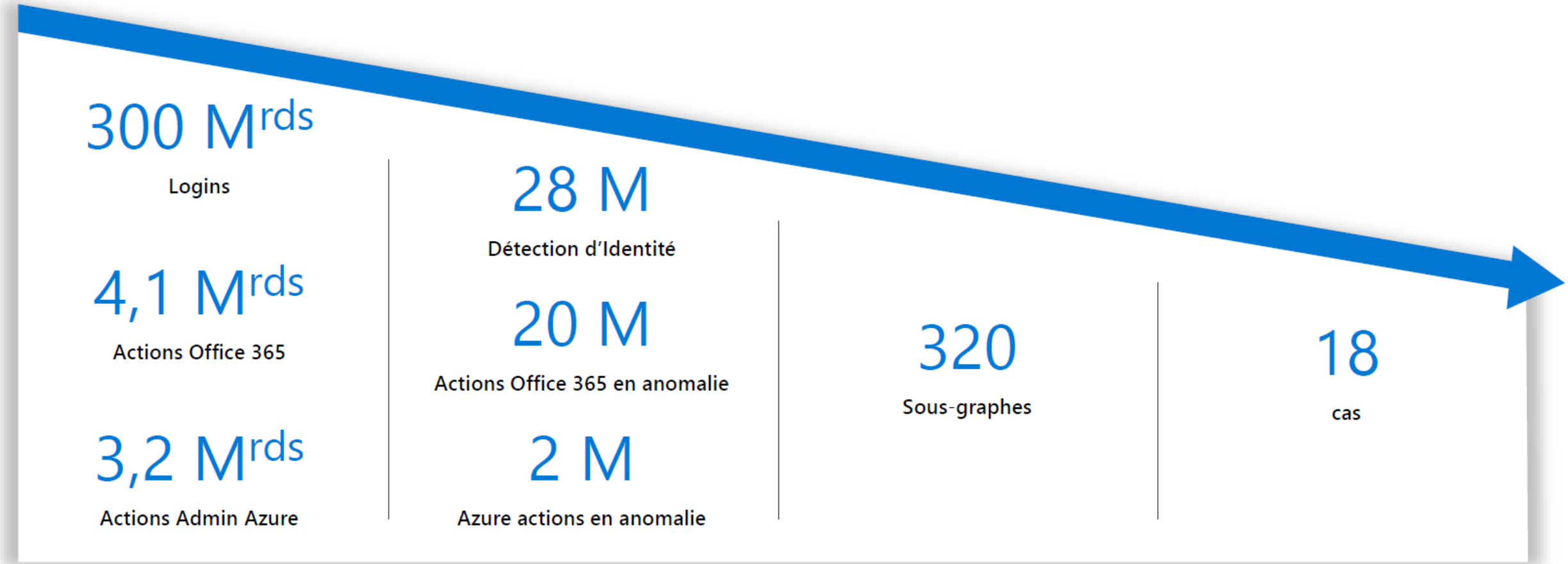
Détecté et bloqué en 14 minutes après sa 1ère apparition

Bilan : 9 PC Windows infectés sur 1 milliard

https://chroniques-cybersecurite.microsoft.fr/

Réduction de la fatigue due aux alertes

Analyse des activités sur plusieurs services de Coud Computing



Événements bruts de la couche de service

Comportements anormaux et détections

Conversion en un graphe

Note chaque sous-graphe grâce au Machine Learning

Limites et contraintes

Formation des équipes et redéploiement des compétences

L'IA et ses capacités d'auto-apprentissage peuvent être détourné
Exemple de Microsoft Tay Bot sur Twitter en 2016

Problématiques de sécurité du code et des algorithmes

Problématiques de performances : l'IA a besoin d'une connectivité cloud

Microsoft

Merci.