



# La stratégie cybersécurité de Microsoft

Bernard Ourghanlian

**Chief Technology & Security Officer**

Microsoft France

Notre vision de la sécurité

“Businesses and users are going to use technology only if they trust it”

Satya Nadella

CEO, Microsoft Corporation





## NOTRE ENGAGEMENT SUR LA **CONFIANCE**



TRANSPARENCE



RESPECT DE LA VIE PRIVEE



CONFORMITE



SECURITE



FIABILITE



## NOTRE ENGAGEMENT SUR LA **CONFIANCE**



TRANSPARENCE



RESPECT DE LA VIE PRIVEE



CONFORMITE



# SECURITE



FIABILITE

# Le paysage de la cybersécurité évolue rapidement



Le cyberspace est devenu le nouveau champ de bataille



Les compétences en matière de sécurité sont rares



Presque tout peut être attaqué



# Rapport « Microsoft Digital Defense »

Septembre 2020

Résumé et faits saillants

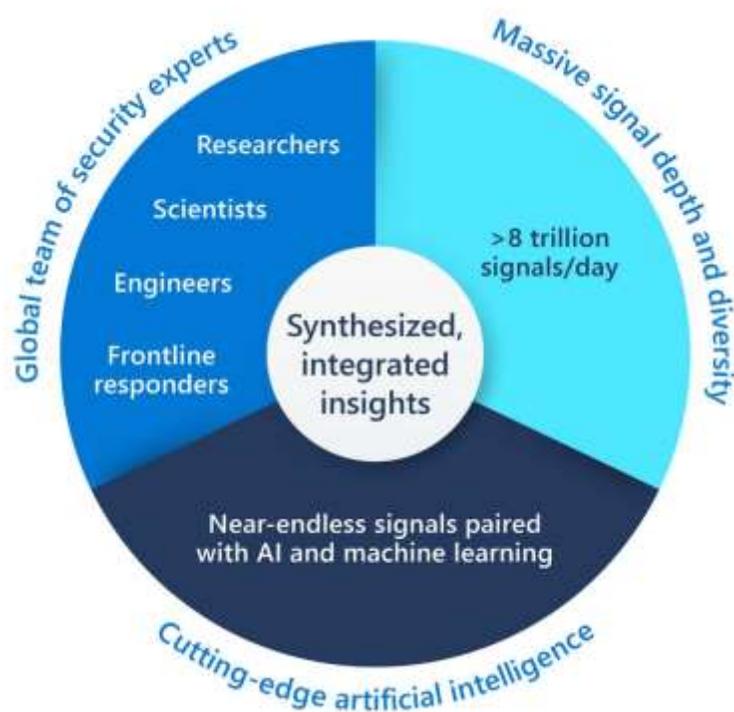
<https://aka.ms/digitaldefense>

# Sommaire

-  Introduction
-  Chapitre 1 : L'état de la cybercriminalité
-  Chapitre 2 : Menaces des états
-  Chapitre 3 : Sécurité et travail à distance
-  Chapitre 4 : Apprentissages exploitables

# Construire le rapport

Synthétiser les contributions d'experts, de praticiens et de défenseurs de Microsoft



## Nos domaines de focalisation en 2020

- 1 L'état de la cybercriminalité
- 2 Menaces des états
- 3 Sécurité et travail à distance
- 4 Apprentissages exploitables

## Équipes contributrices

Cyber Defense Operations Center  
Customer Security and Trust  
Detection and Response Team  
Digital Security & Risk Engineering

Digital Security Unit  
GitHub Security Lab  
IoT Security Research Team  
Microsoft Defender Team

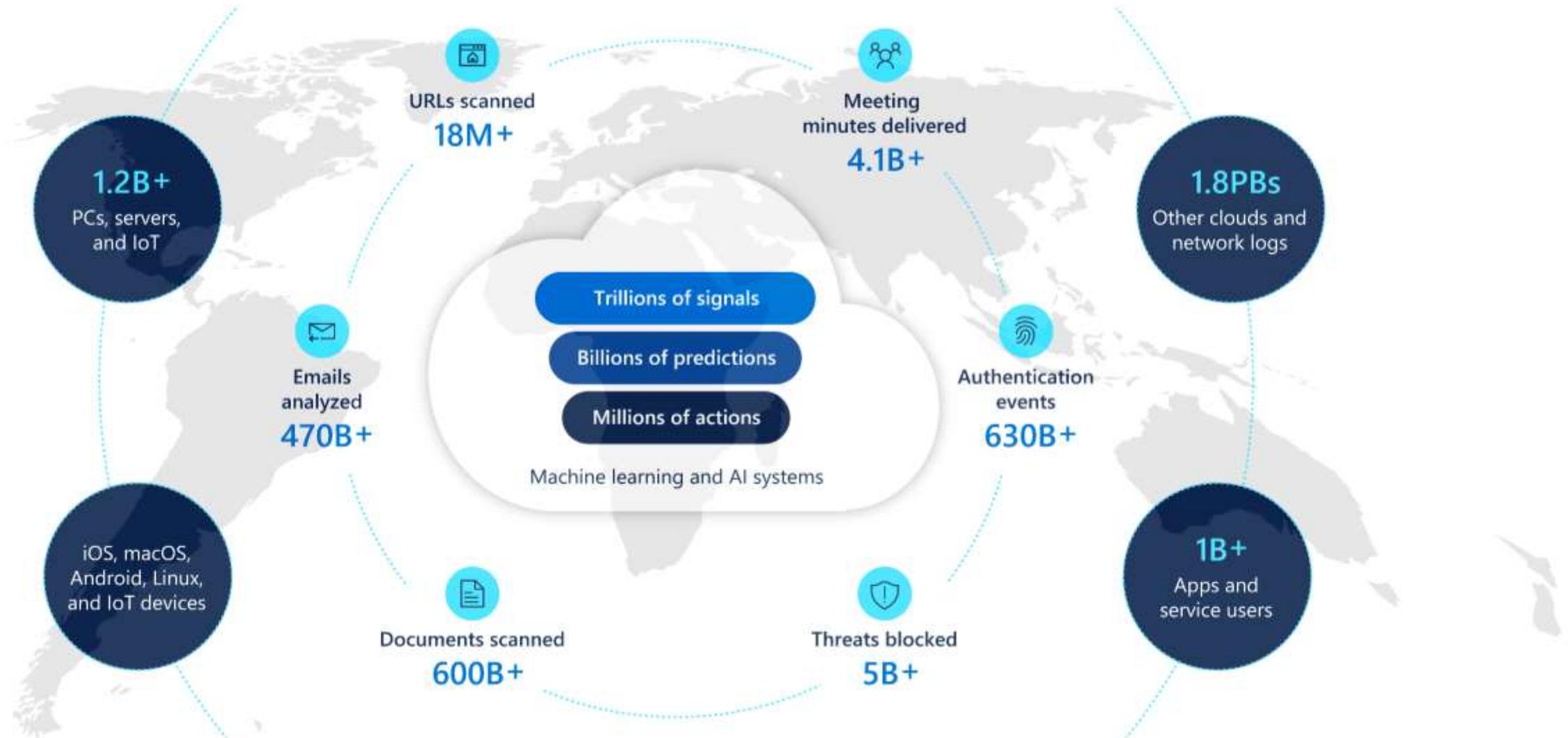
Microsoft Digital Crimes Unit  
Microsoft Security Response Center  
Microsoft Threat Intelligence Center



# Des informations uniques éclairées par des milliards de signaux

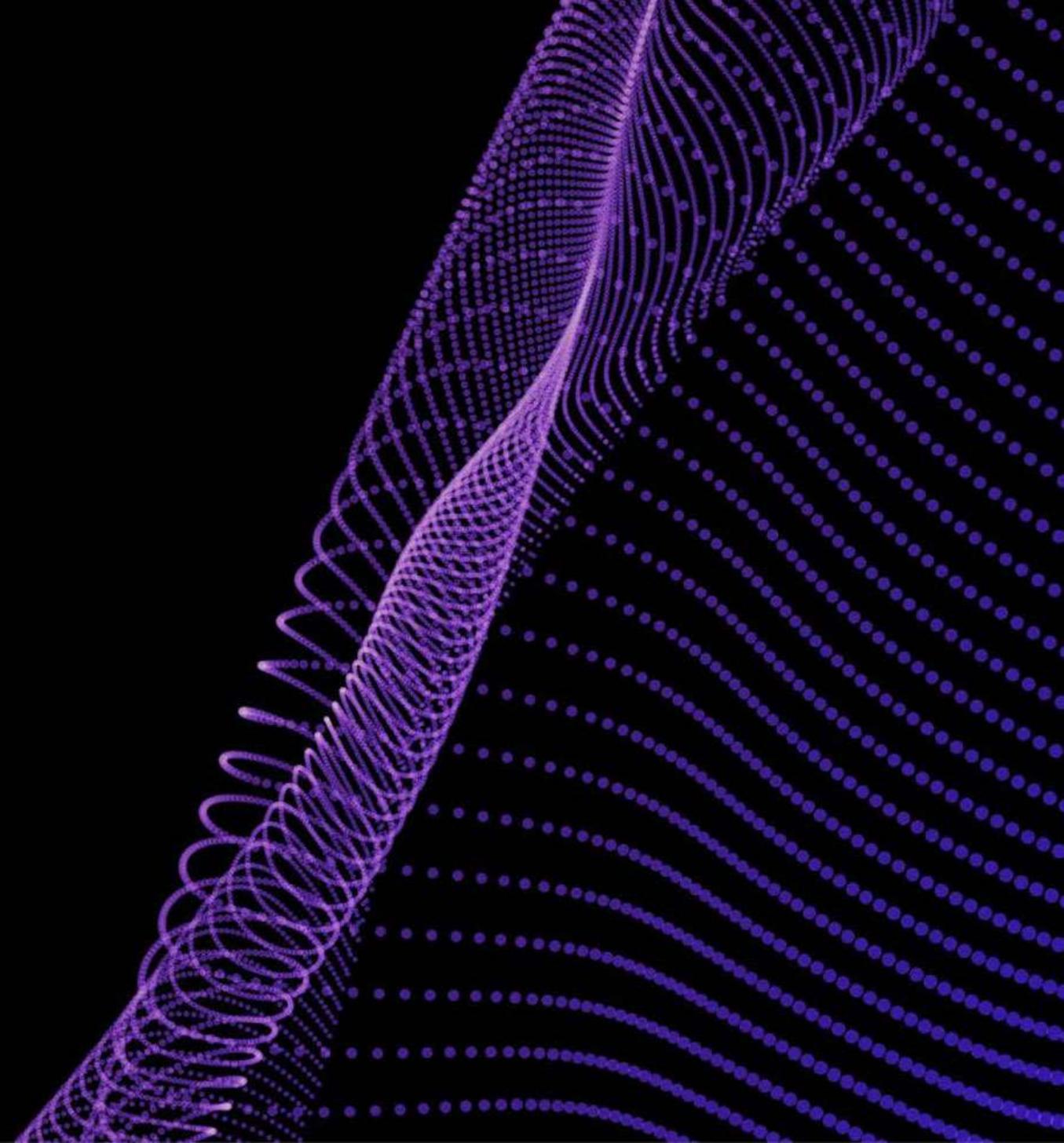


Volume mensuel et diversité des signaux utilisés par les opérations de sécurité Microsoft



# 1

## L'état de la cybercriminalité

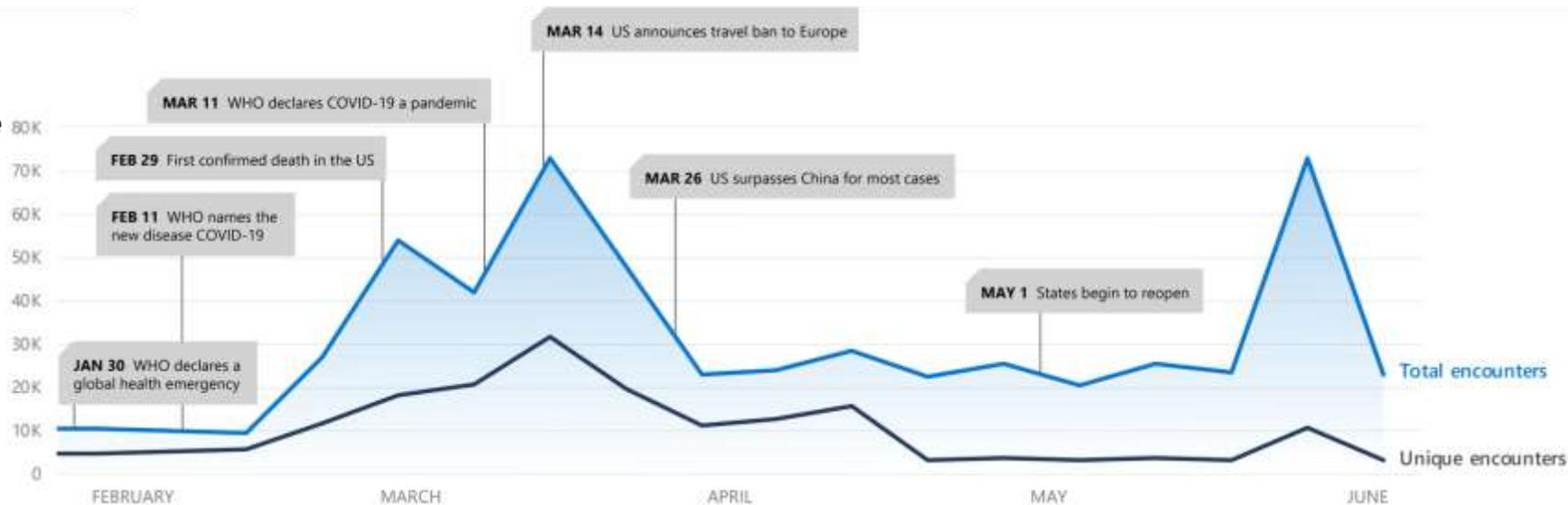


# La cybercriminalité suit les enjeux du jour

Les apparitions de malwares s'alignent sur les titres de l'actualité



## Attaques sur le thème du COVID : États-Unis



## Attaques sur le thème du COVID : Corée du Sud





# Phishing et compromission de messagerie professionnelle

Détections au cours de l'année écoulée :

6T   
Messages scanned

~13B   
Malicious emails blocked

~1.6B   
URL-based email phishing threats blocked

~1.7-2B   
URL payloads being created each month, orchestrated through thousands of phishing campaigns

Nous constatons trois principaux types de phishing :

Hameçonnage des informations d'identification

Compromission de messagerie professionnelle

Combinaison

Top 5 des marques usurpées :

Microsoft  
UPS  
Amazon  
Apple  
Zoom

Campagnes de phishing : Top 10 des industries ciblées :

|                         |                                   |
|-------------------------|-----------------------------------|
| Comptabilité et Conseil | Santé                             |
| Grande Distribution     | Chimie                            |
| Services informatiques  | Haute technologie et électronique |
| Immobilier              | Services juridiques               |
| Education               | Services externalisés             |

*Jusqu'à il y a quelques années, les cybercriminels avaient concentré leurs efforts sur les attaques de logiciels malveillants pour un meilleur retour sur investissement.*

*Plus récemment, ils se sont concentrés sur les attaques de phishing dans le but de récolter les informations d'identification des utilisateurs.*

# Rançongiciel

Une menace humaine à fort impact

## Ce que nous voyons :

### Microsoft Detection and Response Team (DART)

- Les ransomwares continuent d'être la raison la plus courante de nos engagements en réponse aux incidents (Octobre 2019—Juillet 2020).

### Microsoft Threat Protection Intelligence

- Les cybercriminels effectuent des balayages massifs et à grande échelle de l'Internet pour trouver les points d'entrée vulnérables, puis conservent cet accès jusqu'au moment le plus avantageux pour frapper.

*Dans certains cas, les cybercriminels sont passés de l'entrée initiale au sein du SI au rançonnage de l'ensemble du réseau en moins de 45 minutes.*

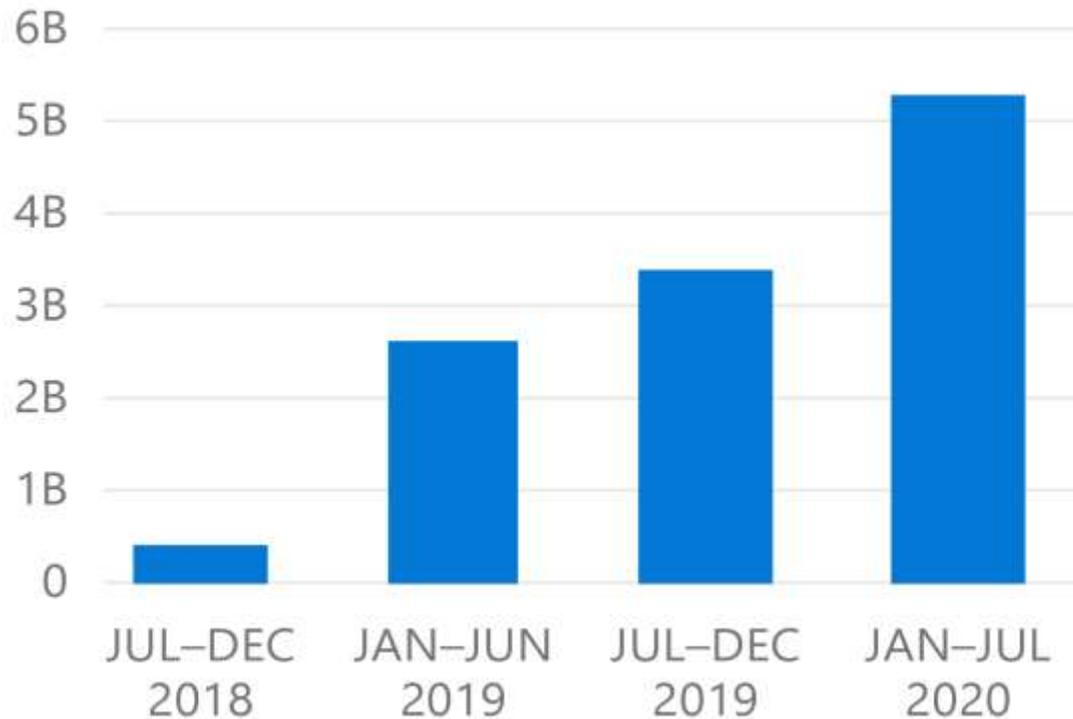


# Informations sur la sécurité IoT

Les menaces IoT ne cessent de s'étendre et d'évoluer



## Nombre total d'attaques sur les pots de miel



Les données de pots de miel au premier semestre 2020 indiquent une augmentation d'environ 35% du volume d'attaque total par rapport au second semestre 2019.

*La gestion des vulnérabilités joue un rôle crucial dans la sécurisation des actifs IoT.*



# Rapport de risque CyberX

Données de 1800 réseaux de systèmes de contrôle industriels

71%

Des sites ont d'anciennes versions de Windows sans correctifs réguliers

64%

Ont des mots de passe non chiffrés facilitant la compromission

66%

Des sites qui ne se mettent pas automatiquement à jour avec les dernières définitions AV

54%

Ont des objets accessibles à distance permettant aux attaquants de pivoter sans être détectés

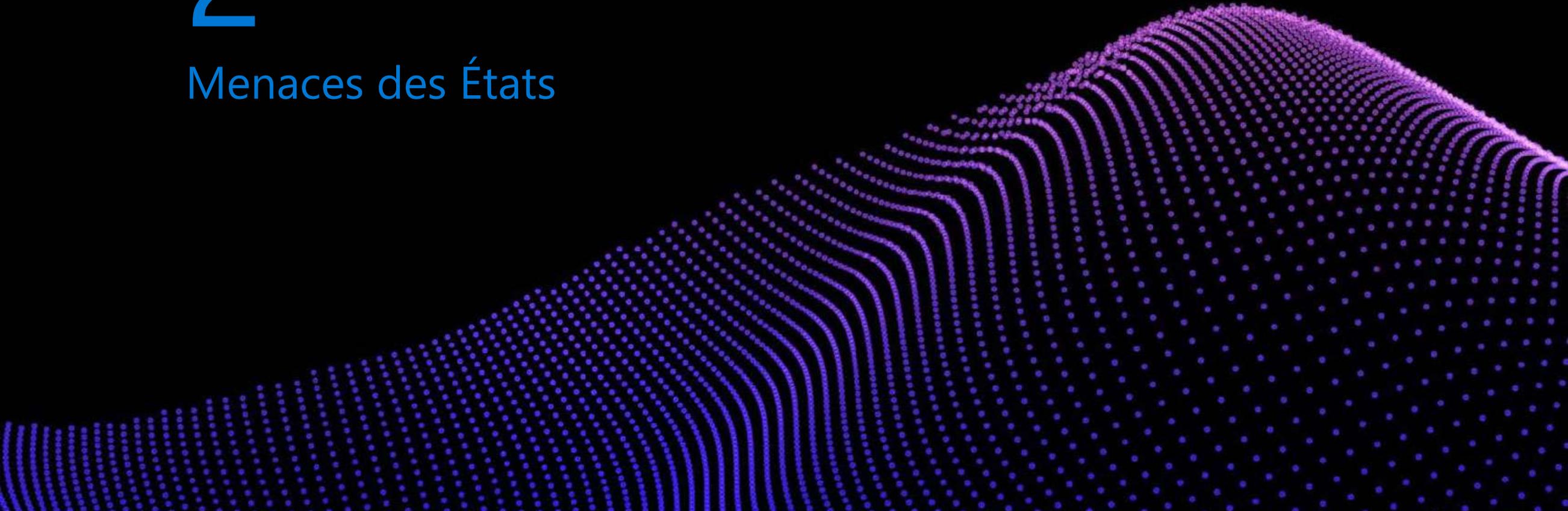
27%

Des objets systèmes de contrôles industriels qui ont des connexions directes à Internet

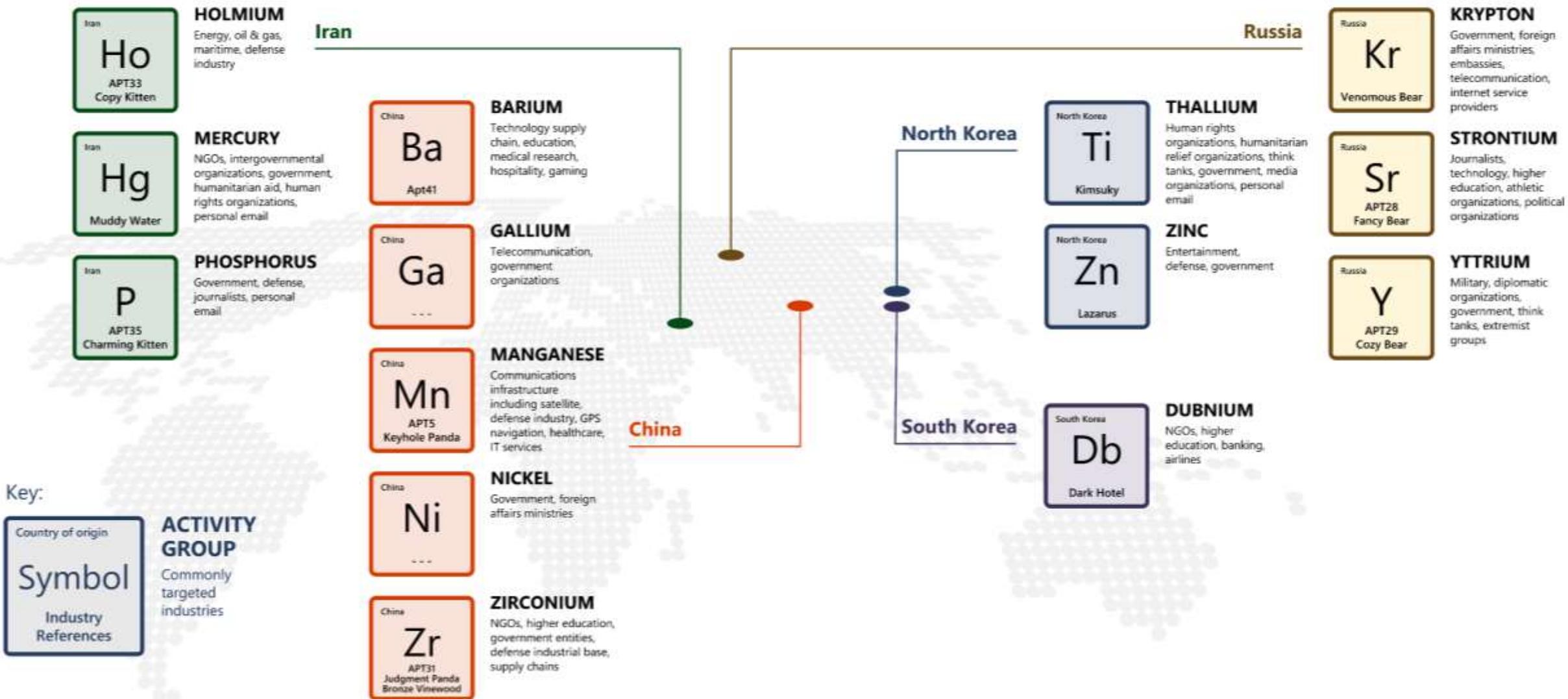
*CyberX : récemment acquis par Microsoft*

# 2

## Menaces des États



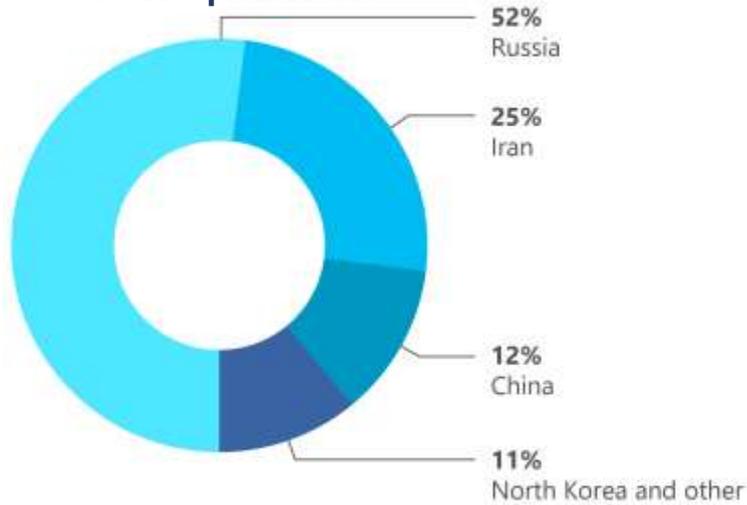
# Exemples d'acteurs étatiques avec leurs activités



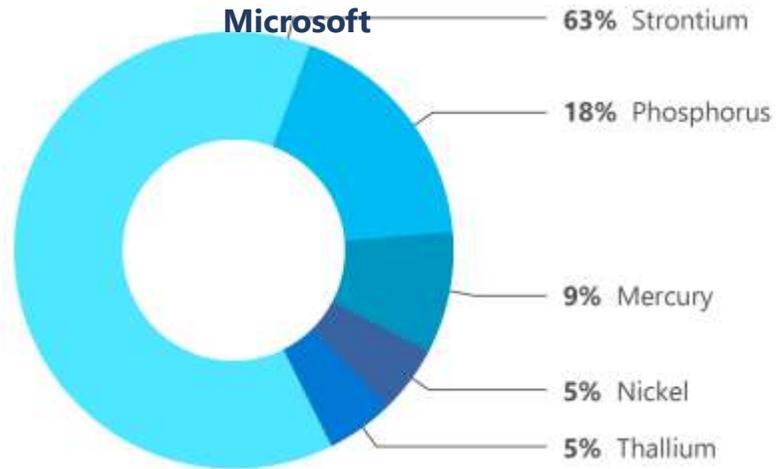
# Suivi des menaces des États (Juillet 2019 – Juin 2020)



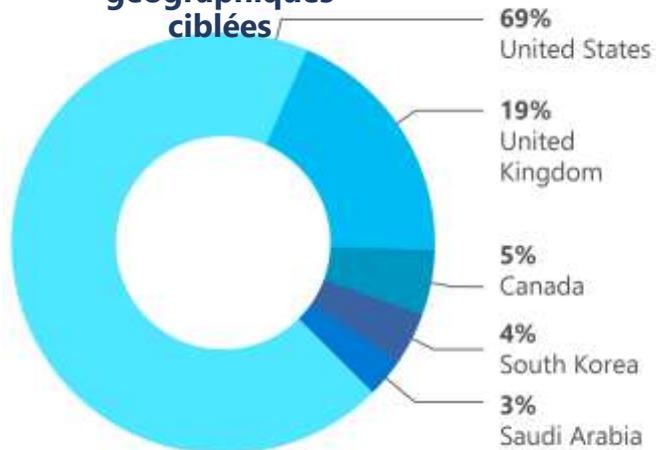
Pays d'origine de l'activité pour NSNs\*



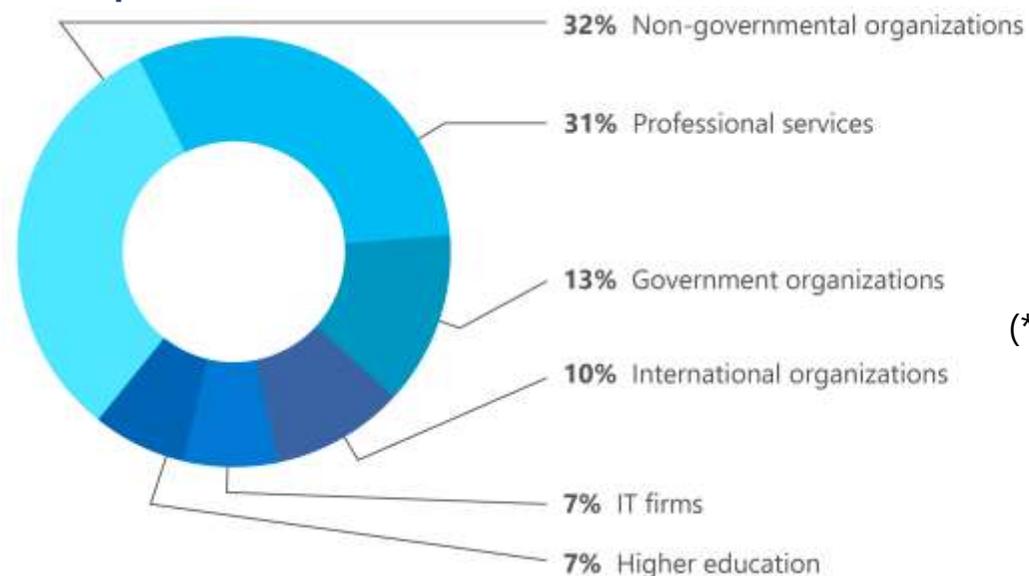
Les 5 principaux groupes d'activités des États détectés ciblant les clients



Top 5 des régions géographiques ciblées



Les 6 principaux secteurs ciblés par les NSN délivrées



Plus de 90% des Notifications des États-Nation ont été délivrées **en dehors** des secteurs des infrastructures essentielles.

(\*)NSN = Nation State Notification



# Menaces des acteurs étatiques

Acquérir une compréhension plus profonde

## Objectifs opérationnels communs

- Espionnage
- Disruption ou destruction

## Techniques d'attaque courantes

- Reconnaissance
- Malware
- Récolte des informations d'identification
- Exploits sur Virtual Private network (VPN)

## Reconnaissance

Exemple d'itérations de formats de noms utilisés par PHOSPHORUS

J.Smith@contoso.com  
John.smith@contoso.com  
John.m.smith@contoso.com  
JohnSmith@contoso.com  
johnmsmith@contoso.com

## Récolte d'informations d'identification

THALLIUM dépense des ressources importantes pour acheter et utiliser des domaines d'imitation qui ressemblent au nom de l'organisation ciblée.



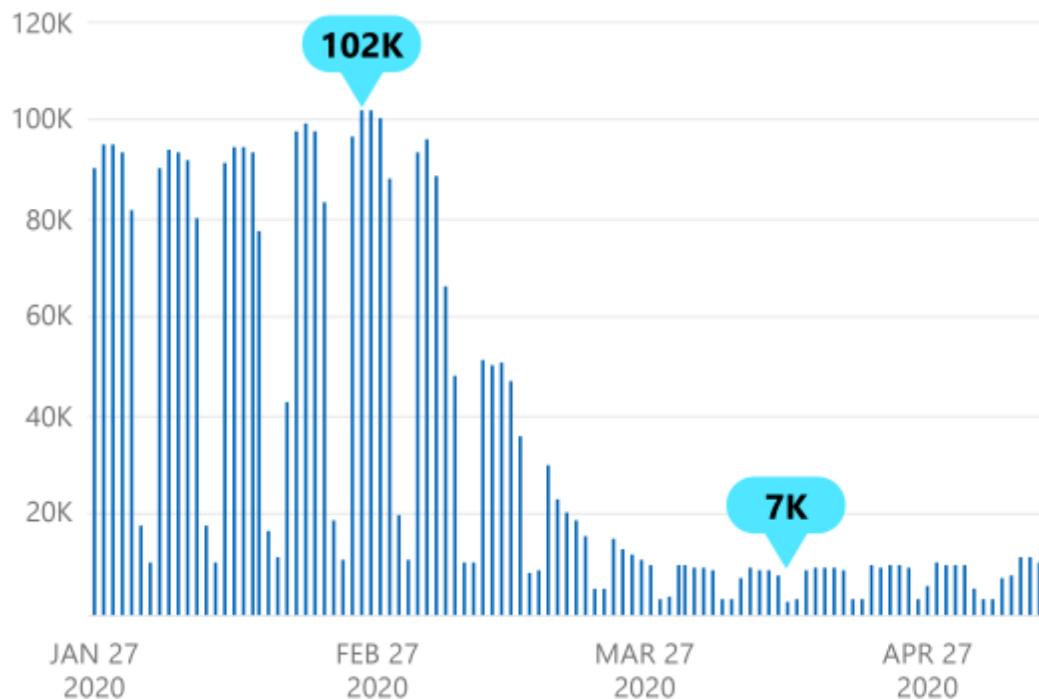
# 3

## Sécurité et travail à distance



# Infrastructure pour des collaborateurs distants

Changement de la notion de périmètre de sécurité d'entreprise



 Les scans de badges d'employés Microsoft pour l'accès aux bâtiments illustrent l'immédiateté et l'ampleur de la transition.

*Conçues à l'origine pour le travail au bureau, de nombreuses infrastructures n'étaient pas préparées à l'immédiateté et à l'ampleur de la transition vers le travail à distance.*

## Sécurité de l'infrastructure : stratégie Zero Trust

- Traiter chaque tentative d'accès comme si elle provenait d'un réseau non approuvé
- Éliminer les terminaux inconnus ou non gérés - IDaaS au lieu de compter sur l'architecture réseau

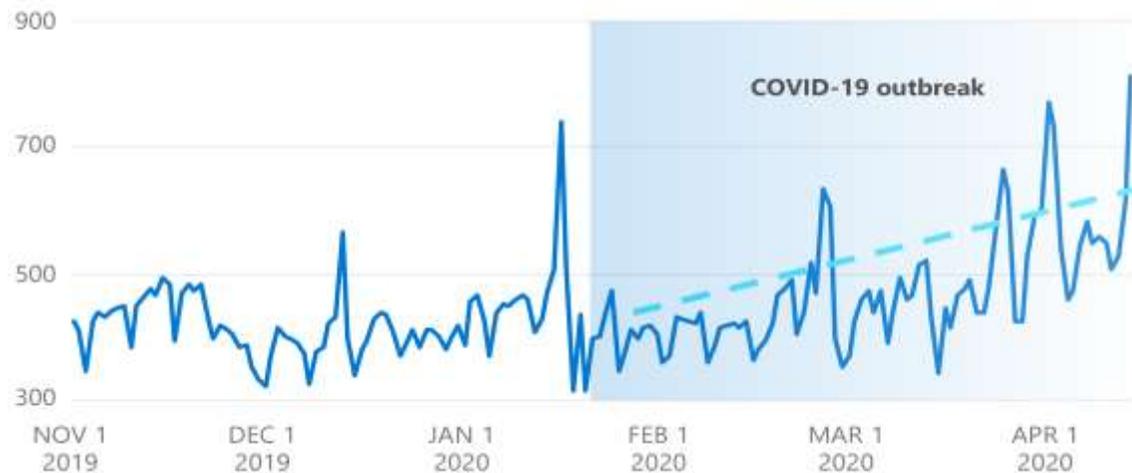


# Attaques sur l'infrastructure: DDoS

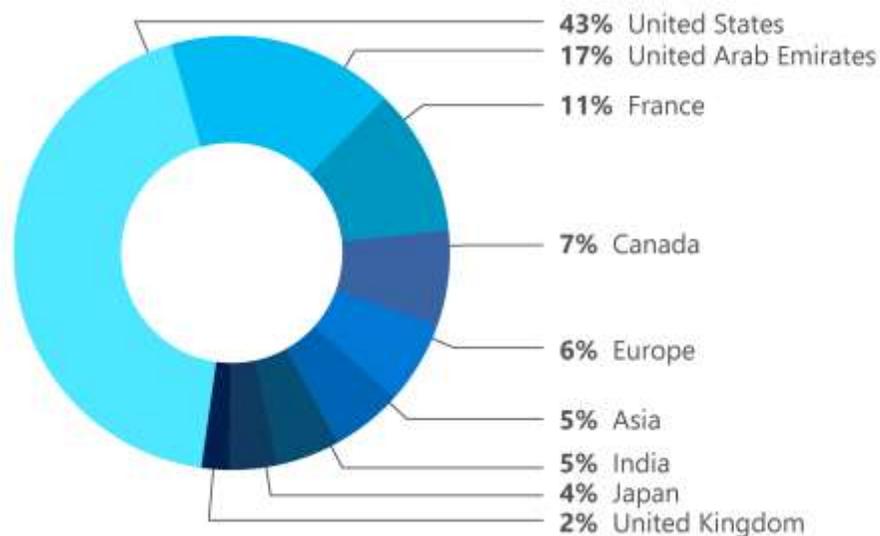
Ce que voient les chercheurs de Microsoft sur les menaces



Nombre  
d'attaques  
DDoS  
pendant  
l'épidémie de  
COVID-19



Distribution de la région de  
destination (Janvier—Juin 2020)



*Microsoft a atténué 600 à 1000 attaques DDoS uniques chaque jour de mars, soit environ 50% de plus que les niveaux pré-COVID-19.*

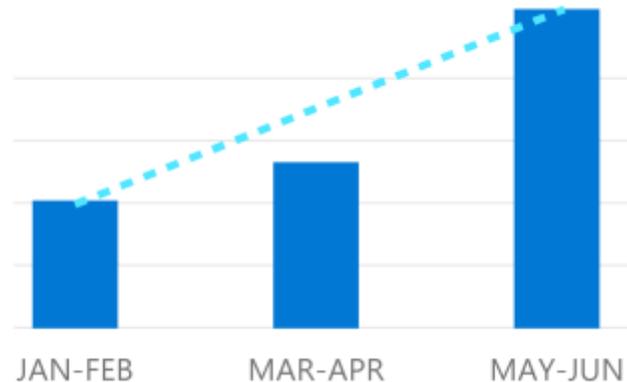
# Gestion des identités et des accès



## Attaques basées sur l'identité

Tentatives d'attaque de force brute de mot de passe contre les comptes Azure AD

Azure Active Directory a connu une augmentation des attaques basées sur l'identité utilisant la force brute sur les comptes d'entreprise au cours du premier semestre 2020.



## Des méthodes d'authentification fortes sont essentielles pour se défendre contre ces attaques

Volume hebdomadaire de demandes d'activation d'authentification multi-facteurs, 3 février— 6 avril 2020



Doublement approximatif des demandes d'activation MFA après le début du COVID-19, à mesure que les politiques de travail à domicile ont été adoptées.

# Résilience d'entreprise : la nouvelle réalité

Leçons apprises et stratégies déployées pour survivre à la pandémie

- ✓ Étendre la limite de sécurité de l'entreprise au-delà du périmètre sur site
- ✓ Donner la priorité à des performances résilientes
- ✓ Valider la résilience de l'infrastructure humaine

*Dans une certaine mesure, la réponse de l'entreprise au COVID-19 a changé nos procédures opérationnelles **ainsi que le vocabulaire même que nous utilisons** pour décrire les mesures réactives et les leçons apprises.*



# 4

Apprentissages exploitables



# Apprentissages exploitables : ce que vous pouvez faire aujourd'hui

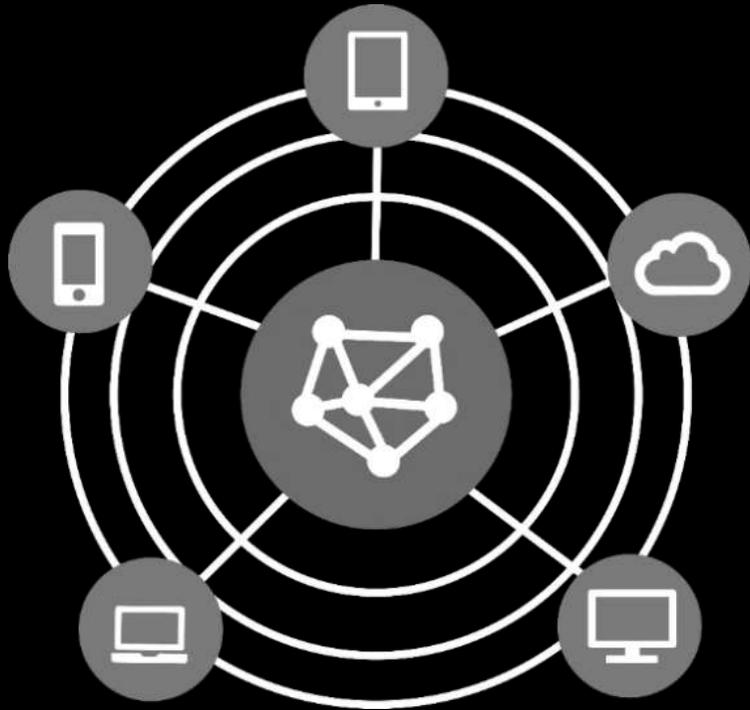
Le « top 5 » sur les 20 résumés dans le rapport

- 1 Adopter l'authentification multi-facteurs (MFA)
- 2 Utiliser une bonne hygiène de messagerie
- 3 Patcher les applications et les systèmes
- 4 Limiter l'accès avec le moindre privilège
- 5 Ralentir les attaques grâce à la segmentation du réseau

*Ralentir les attaques grâce à la segmentation du réseau*

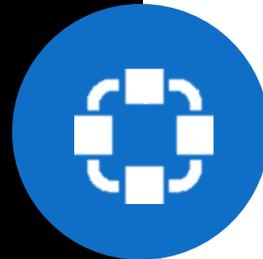


# Cyberattaques récentes



## Rapides

Se propagent dans l'entreprise en quelques minutes, laissant très peu de temps pour réagir et laissant les défenseurs entièrement dépendants des contrôles préventifs et des processus de récupération.



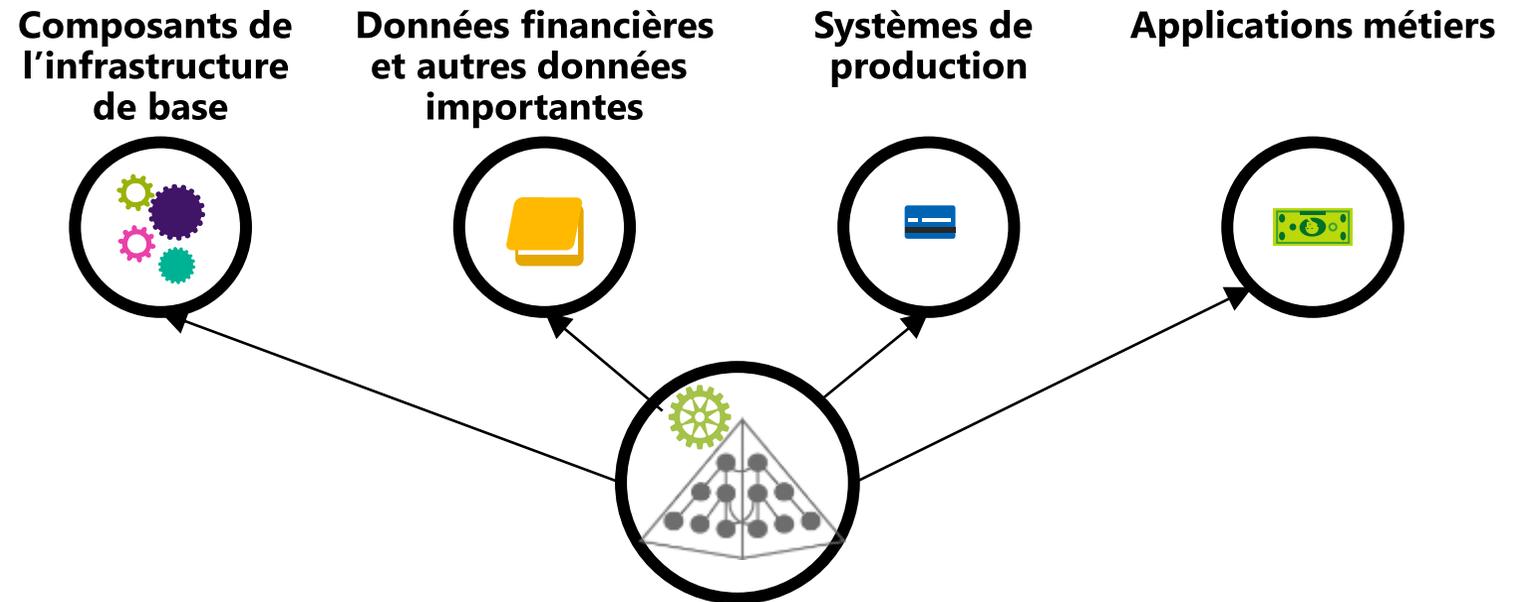
## Automatisées

Aucune interaction humaine requise après le début du cycle d'attaque. Techniques automatisées de traversées multiples.

# Pourquoi les hackers aiment-ils Active Directory ?

Les infrastructures Active Directory sont le **point central de la majorité de la sécurité des organisations mondiales.**

Identifiants des utilisateurs, boîtes aux lettres, données d'entreprise et financières : **ils sont tous régis par l'infrastructure d'annuaire**, qui agit en tant que détenteur de la clé principale de l'entreprise.



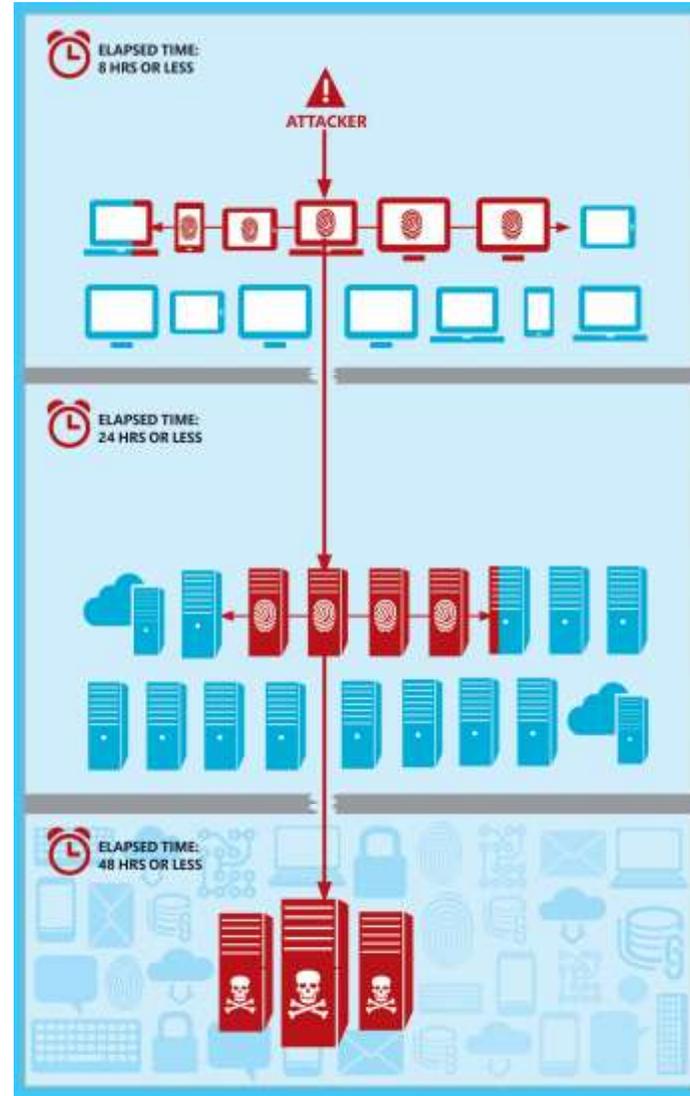
**Active Directory a la pouvoir sur...**

Les attaquants voient **Active Directory comme une arborescence** dans laquelle toutes les informations d'identification accordent l'accès à **une branche de serveurs**. Ils traversent cet arbre, **récoltant les informations d'identification** en cours de route, se connectent aux serveurs, exfiltrent les données jusqu'à ce qu'ils atteignent la **racine : privilèges d'administrateur de domaine qui donne un contrôle total sur l'environnement.**

# Schéma commun des cyberattaques

## Schéma rapide et automatisé :

1. Compromission du compte administrateur local
2. Vol des informations d'identification d'un autre utilisateur lorsqu'il se connecte
3. Réutilisation de ces informations d'identification pour accéder à d'autres systèmes
4. Vol des informations d'identification de l'administrateur de domaine
5. Contrôle de l'Active Directory et accès à toutes les ressources



## Obtenir les informations d'identification

L'ingénierie sociale et les programmes de phishing sont utilisés pour inciter les employés à exécuter un logiciel malveillant et à obtenir des informations d'identification.

## Récupérer les données

L'attaque ne s'arrête pas là. Les attaquants recherchent le prochain ensemble d'informations d'identification avec des autorisations élevées pour accéder aux serveurs. Ils peuvent commencer à exfiltrer les données de l'entreprise.

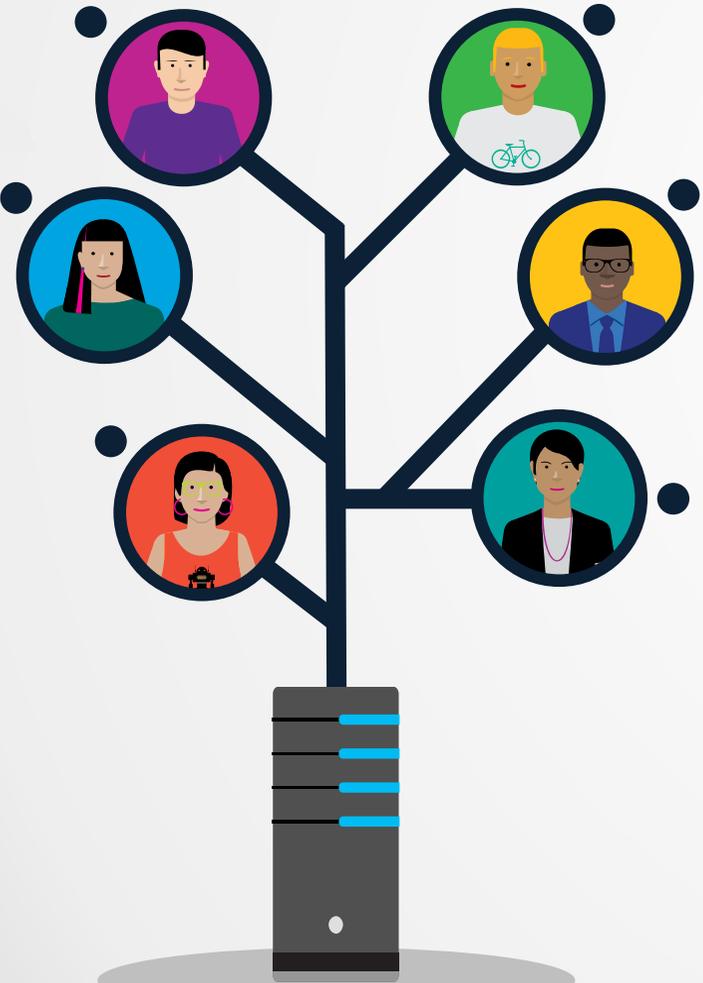
## Obtenir un contrôle total

Le but ultime de l'attaquant peut être d'accéder aux contrôleurs de domaine, le centre de contrôle de toutes les informations d'identification et d'identités.

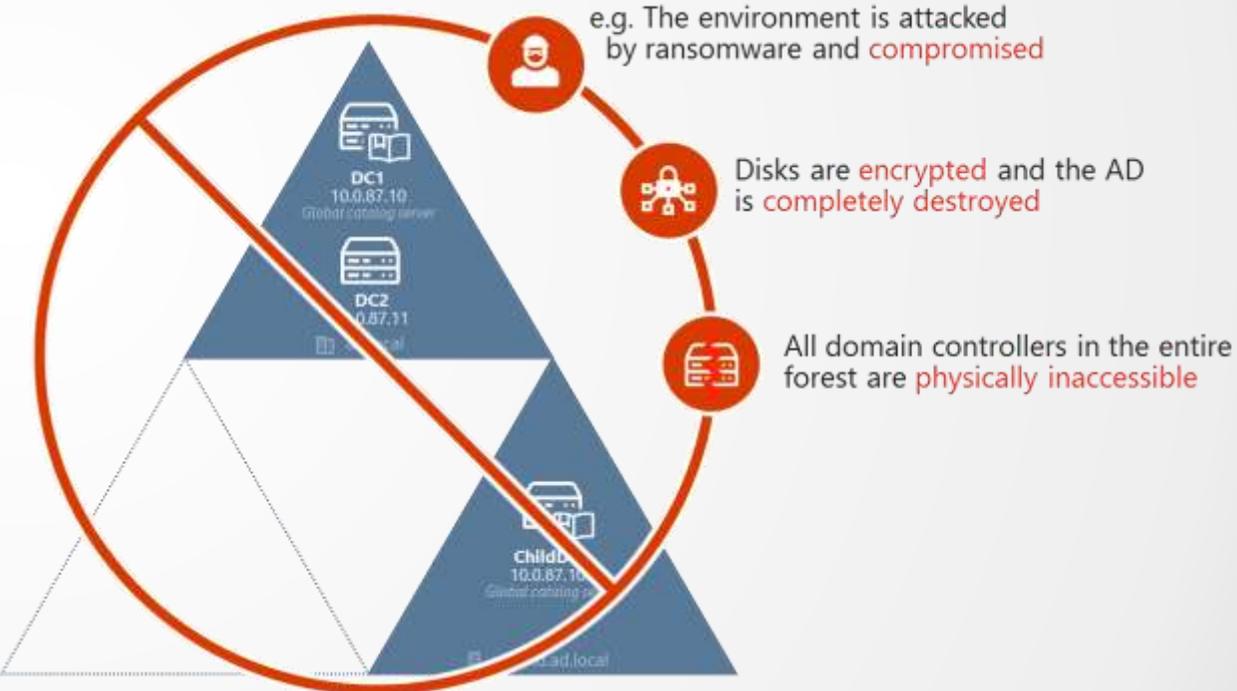
# Que peut-il se produire lorsque Active Directory est compromis ?



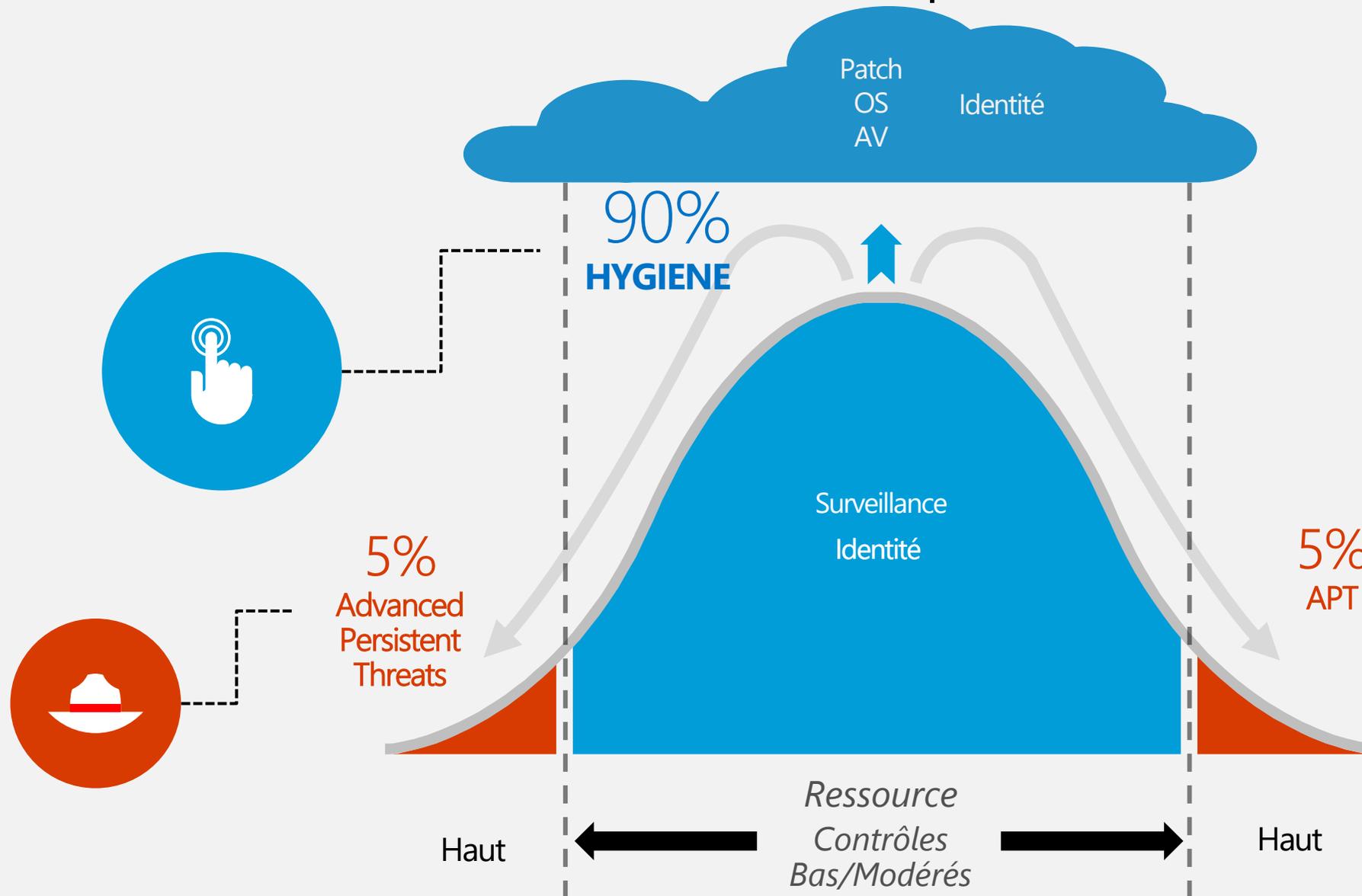
## Vol d'Information



## Destruction



# Atténuation efficace des risques



# Les entreprises sont en chemin dans leur transformation

Nécessite un périmètre de sécurité d'accès et d'identité moderne

Technologies Cloud

Périmètre d'entreprise moderne

Adoption SaaS

Office 365



Infrastructure as a Service

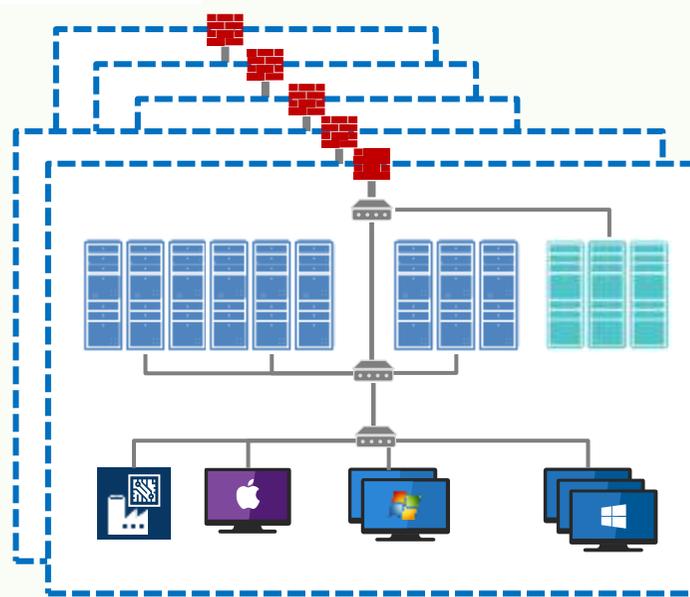
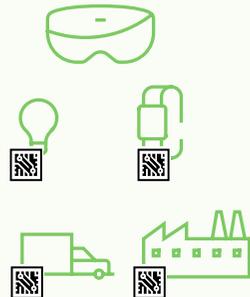


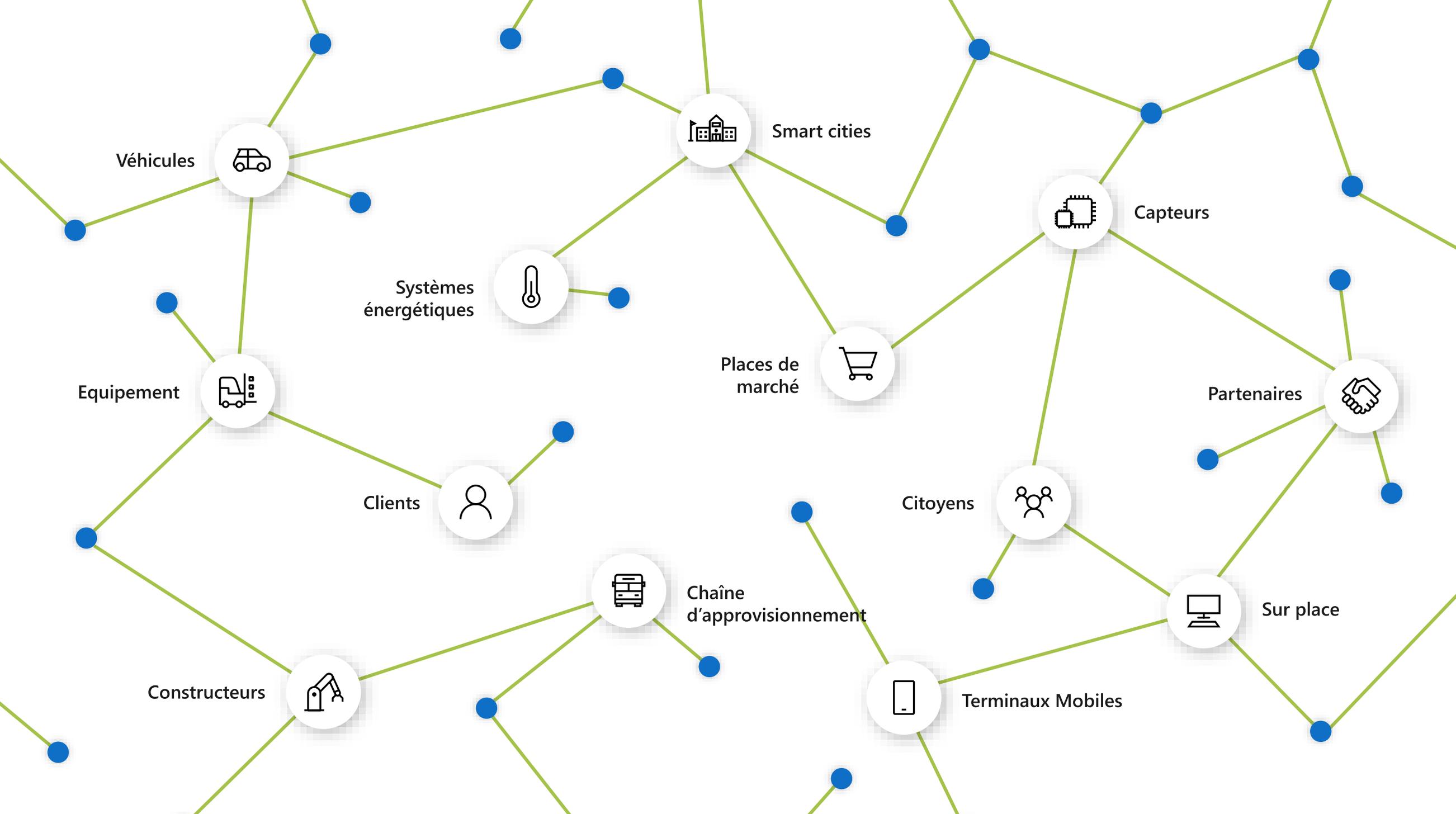
Platform as a Service

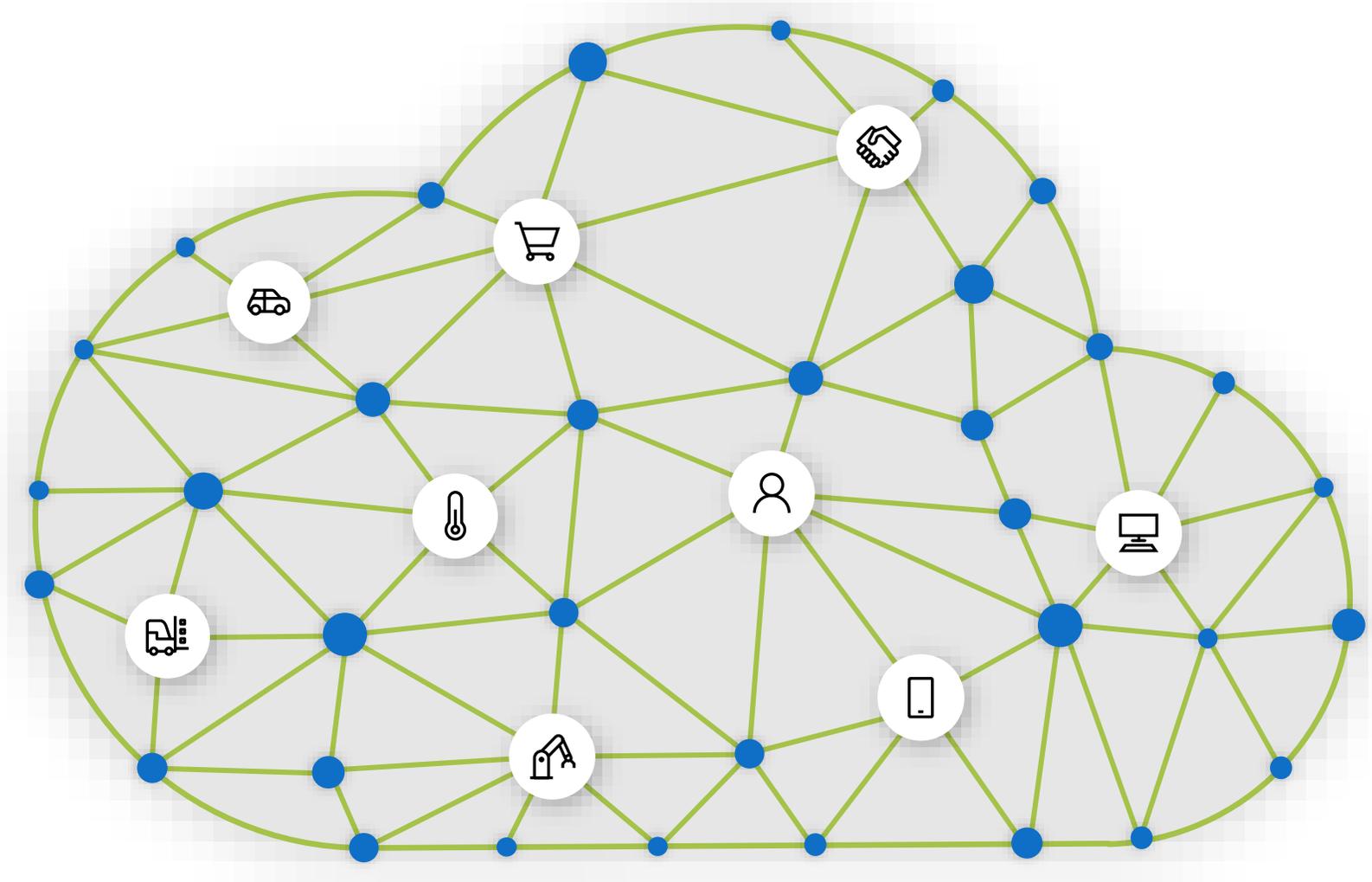


Expérience mobile de qualité

Internet des objets







Détection d'anomalies

Protection des points de terminaison

Sécurité de l'infrastructure

Sécurité Cloud Hybride

Sécurité données et applications

Détection des Fraudes

Data loss prevention

Gestion des menaces

Gestion de la sécurité

**Les solutions sont déconnectées**  
Solutions de sécurité multiples

Sécurité du Datacenter

Cloud Access Security Broker

Gestion des droits numériques

Gestion des identités et des accès

Outils de conformité

Détection des menaces

Sécurité IoT

Sécurité des emails

# Dans les Nouvelles...

The Washington Post

BloombergBusiness

News

Markets

Insights

Security

THE WALL STREET JOURNAL.

THE CIO REPORT

InformationWeek

DARKReading

CONNECTING THE INFORMATION SECURITY COMMUNITY

Attacks  
Privacy

The New York Times

BUSINESS INSIDER

TECH

## Microsoft doubled down on security – and it worked

Max Slater-Robins

Nov. 17, 2015, 10:58 AM 2,455

FACEBOOK

LINKEDIN

TWITTER

EMAIL

PRINT

Microsoft has increased its focus on information security, and the strategy seems to be working.

Satya Nadella, the CEO of Microsoft, gave a speech at the Government Security Forum in Washington, D.C. on Tuesday,



hackers

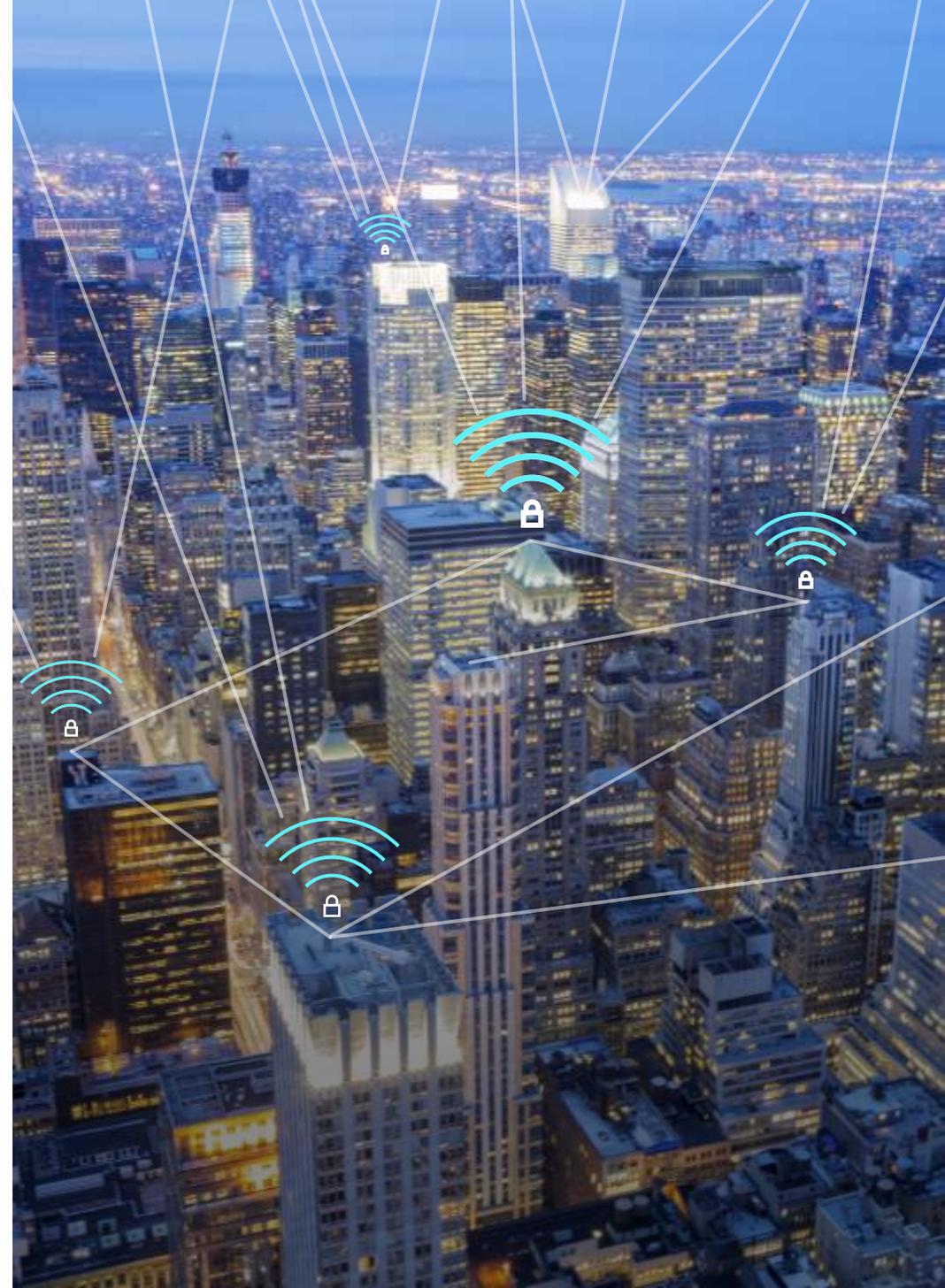


Germany in Berlin.

Berlin last week.

# Stratégie Sécurité de Microsoft

Assurer la sécurité numérique de nos clients pour permettre leur transformation digitale grâce à une plateforme complète, des renseignements uniques et de larges partenariats



*"Security is our top priority and we are committed to working with others across the industry to protect our customers."*

**Satya Nadella**  
*Chief Executive Officer, Microsoft Corporation*



# Les impératifs du CISO

Recruter...

LesEchos.fr

LES ECHOS: Tapez votre recherche

OK

le jectif tech, médias, hightech

## La pénurie de compétences « cyber » s'accroît

+  
Infos

FLORIAN DÉBES · FLORIAN DÉBES | LE 11/07/18 À 17H56

TOUTE L'ACTUALITÉ / EMPLOI / FORMATION

## Orange Cyberdefense forme à la sécurité avec l'ECE Paris et Microsoft

Véronique Arène, publié le 27 Avril 2018

Le problème s'aggrave encore à mesure que les entreprises prennent conscience. Dès septembre 2018, l'ECE Paris proposera une spécialisation en master 2 (bac+5) axée sur l'identité et la gestion des accès en environnement Microsoft en France, co-créée avec Microsoft et Orange Cyberdefense.



A l'ECE Paris, les étudiants du cycle « Cybersécurité Défensive » acquerront des compétences concrètes sur la cybersécurité des environnements Microsoft. Crédit. D.R.

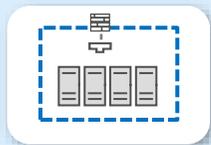
# Constuire un programme de cybersécurité résiliente

| Responsabilité                      | SaaS      | PaaS   | IaaS   | On-prem |
|-------------------------------------|-----------|--------|--------|---------|
| Information et Données              | Client    | Client | Client | Client  |
| Terminaux (Mobiles et PC)           | Client    | Client | Client | Client  |
| Comptes et Identités                | Client    | Client | Client | Client  |
| Infrastructure Identité et Annuaire | Client    | Client | Client | Client  |
| Applications                        | Microsoft | Client | Client | Client  |
| Contrôles Réseau                    | Microsoft | Client | Client | Client  |
| Systèmes d'exploitation             | Microsoft | Client | Client | Client  |
| Machines Physiques                  | Microsoft | Client | Client | Client  |
| Réseau Physique                     | Microsoft | Client | Client | Client  |
| Datacenter Physique                 | Microsoft | Client | Client | Client  |

Microsoft
  Client



**ETABLIR UN PERIMETRE MODERNE**



**MODERNISER LA SECURITE DE L'INFRASTRUCTURE**



**« FAIRE CONFIANCE MAIS VERIFIER »  
CHAQUE FOURNISSEUR DE CLOUD**

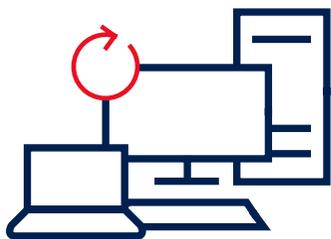
# Concevoir pour la défaillance – Un changement de mentalité s'impose

## HIER

## AUJOURD'HUI

### Fiabilité :

Conçu pour ne pas échouer



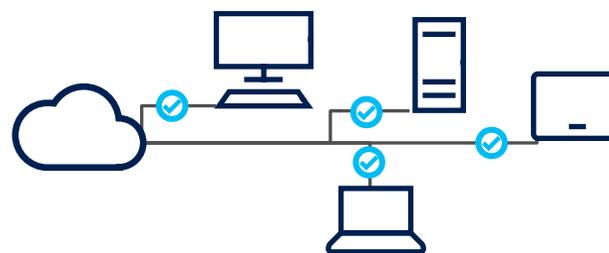
### Prévenir :

Toute attaque possible



### Résilience :

Conçu pour récupérer rapidement



### Présupposer la compromission :

Protéger, détecter et répondre pendant les phases d'attaque



# Exécuter une stratégie duale pendant la transition

**ATTAQUANTS EXPLOITANT L'IDENTITE**

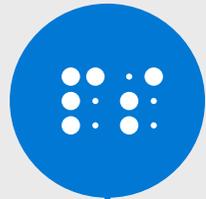
**SECURISER LES SCENARIOS MODERNES (CLOUD, MOBILE, IOT)**

**IDENTITE MODERNE  
(Contrôles des Identités)**

**PERIMETRE CLASSIQUE  
(Contrôles Réseau)**

**RESEAU A « CONFIANCE ZERO »**

# « Zero Trust » – Quand tout a commence ?



**2004**

Concept de dé-périmétrisation du Jericho Forum



**2010**

Forrester utilise le terme « Zero Trust »



**2009**

Attaque de l'opération Aurora



**2014**

Google BeyondCorp est publié

Le battage médiatique sur « Zero Trust » décolle

# Zero Trust

Une approche de la sécurité qui traite chaque tentative d'accès comme si elle provenait d'un réseau non approuvé.



# Zero Trust n'est pas ...

LITERAL - Vous ne pouvez pas construire une stratégie pratique autour de la vérification à 100%

UN ADJECTIF - Vous n'allez pas « être » « Zero Trust »

À VENDRE - La technologie « Zero Trust » n'existe pas

INSTANTANNE – Vous ne pouvez pas vider l'océan avec une petite cuillère.

UNE RÉVOLUTION - Construisez sur ce que vous avez.

# Zero Trust est un état d'esprit

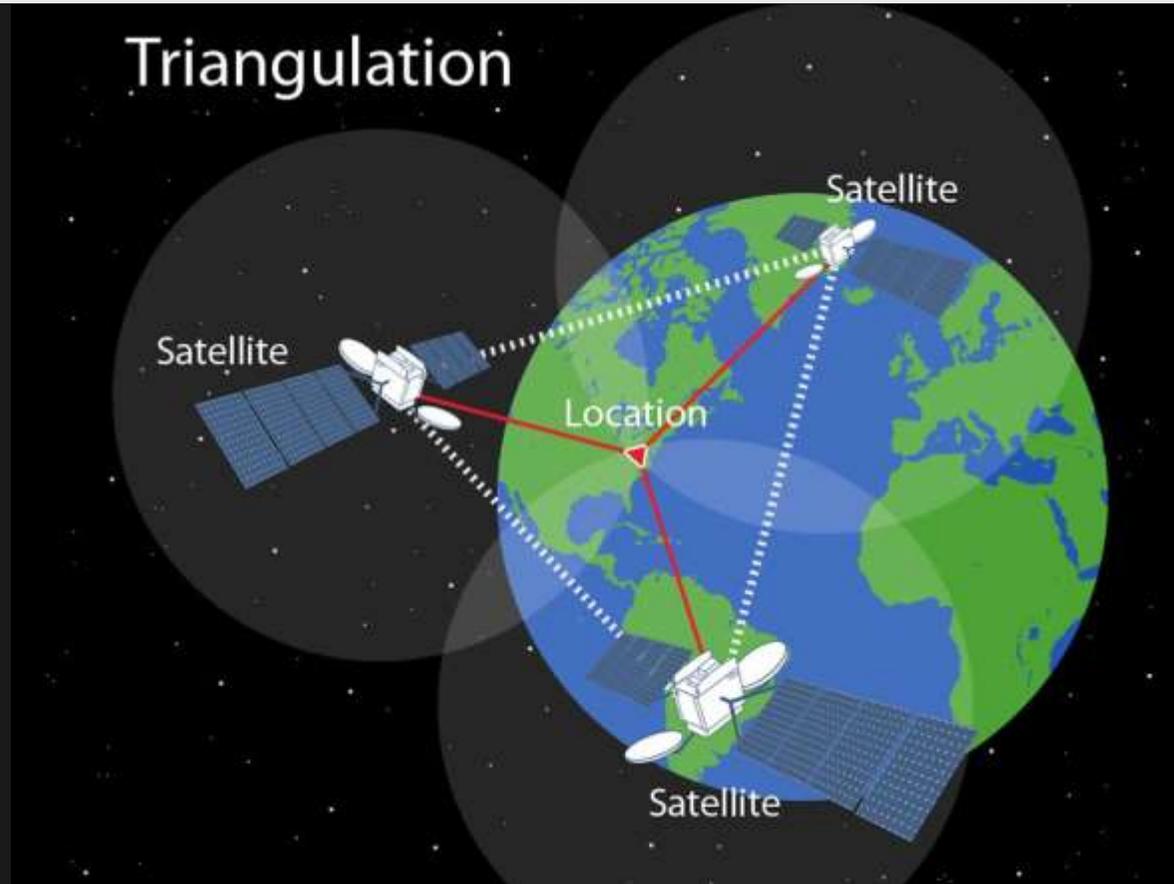
- L'un des plus grands avantages de Zero Trust est un changement de mentalité
- Une approche de la sécurité qui traite chaque tentative d'accès comme si elle provenait d'un réseau non approuvé
- Une approche de la sécurité qui assume un risque omniprésent
- Comment nous comportons-nous dans un environnement de risque omniprésent ?

Etat d'esprit :  
Tout est sur l'Internet ouvert.



# Etat d'esprit :

Ne faites confiance à aucune source unique.



# Etat d'esprit :

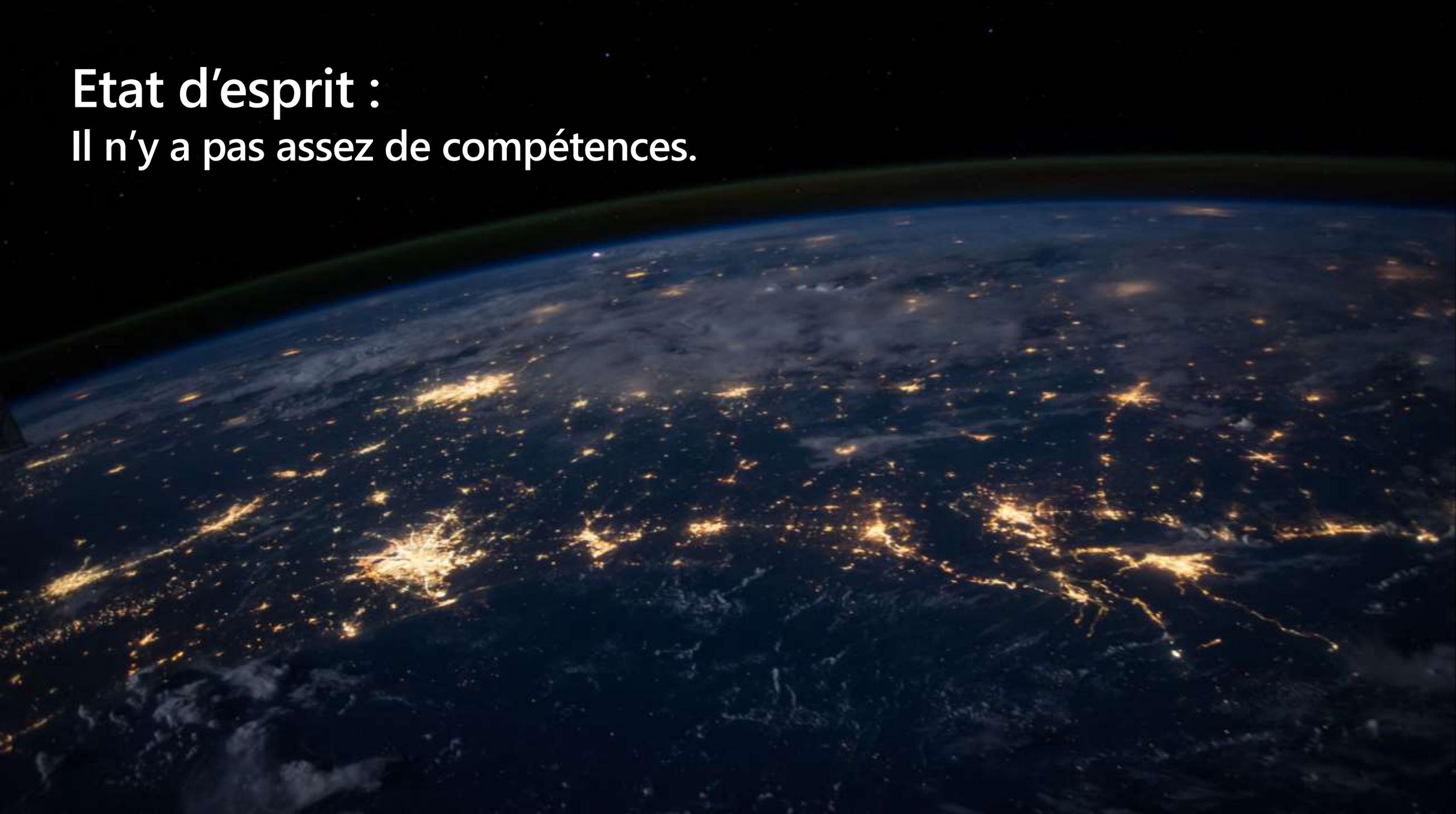
## Convinement des brèches



# Etat d'esprit : Standards = Sécurité



**Etat d'esprit :**  
**Il n'y a pas assez de compétences.**



# Etat d'esprit : Présupposez une violation

ars TECHNICA

BUZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE STOR

HACKING THE HACKERS —

## Nation-sponsored hackers likely carried out hostile takeover of rival group's servers

Like an episode of *Spy vs. Spy*, Russian-speaking Turla appears to hijack OilRig's network.

DAN GOODIN - 6/20/2019, 6:00 AM



Enlarge

41

If nation-sponsored hacking was baseball, the Russian-speaking group called Turla would not just be a Major League team—it would be a perennial playoff contender. Researchers from multiple security firms largely agree that Turla was behind breaches of the [US Department of Defense in 2008](#), and more recently the [German Foreign Office](#) and [France's military](#). The group has also been known for [unleashing stealthy Linux malware](#) and using [satellite-based internet links](#) to maintain the stealth of its operations.

ars TECHNICA

BUZ & IT TECH S

WIPER, NO WIPING! —

## DHS cyber director warns Iranian "wiper" hack attacks

"Wiper" attacks targeting US companies' data are on rise.

SEAN GALLAGHER - 6/24/2019, 1:58 PM



Enlarge / An effective wiper of sorts.

77

With tensions between the US and Iran on the rise following the downing of a US military drone last week, the director of the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency is warning that Iran is elevating its efforts to do damage to US interests through destructive malware attacks on industrial and government networks.



## Hackers linked to China stole private data from wireless telcos around the world

Chris Smith @chris\_writes  
June 25th, 2019 at 11:44 AM

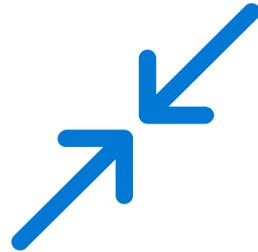
Share Tweet

C'est pire  
que vous  
le pensez.

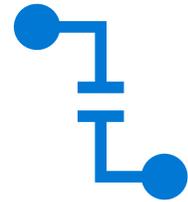
# Principes du Zero Trust



Verifiez  
explicitement



Utiliser l'accès  
le moins privilégié



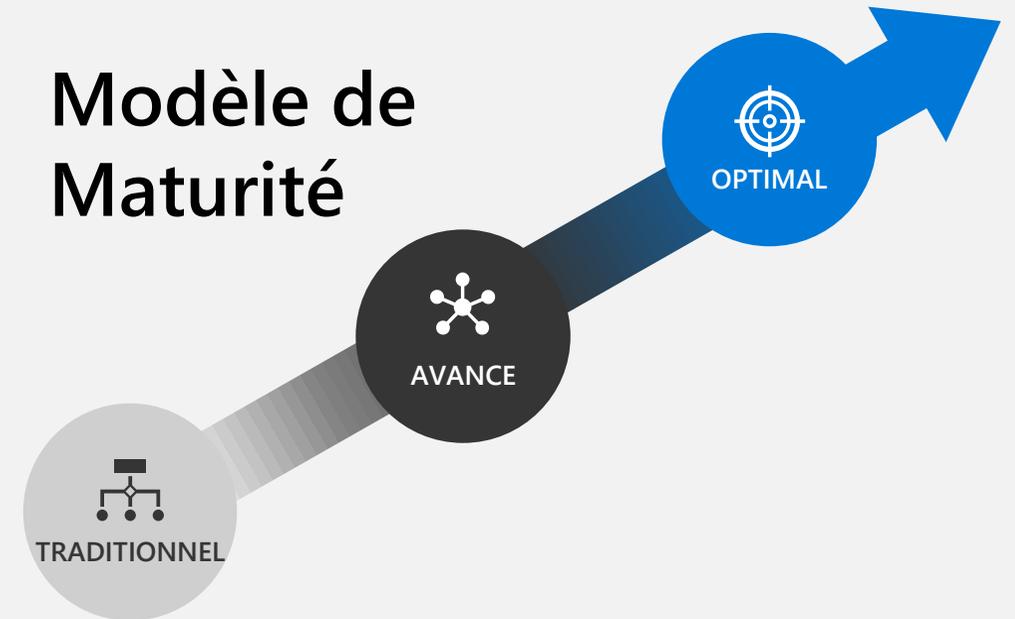
Présupposez la brèche

# Dans un modèle Zero Trust,

- Chaque demande d'accès est fortement authentifiée, autorisée dans les limites de la politique et inspectée pour les anomalies avant d'accorder l'accès.
- Tout, de l'identité de l'utilisateur à l'environnement d'hébergement de l'application, est utilisé pour éviter toute violation.
- Nous appliquons les principes de micro-segmentation et d'accès les moins privilégiés pour minimiser les mouvements latéraux.
- Des informations et des analyses riches nous aident à identifier ce qui s'est passé, ce qui a été compromis et comment éviter que cela ne se reproduise.

# Faire de Zero Trust une réalité

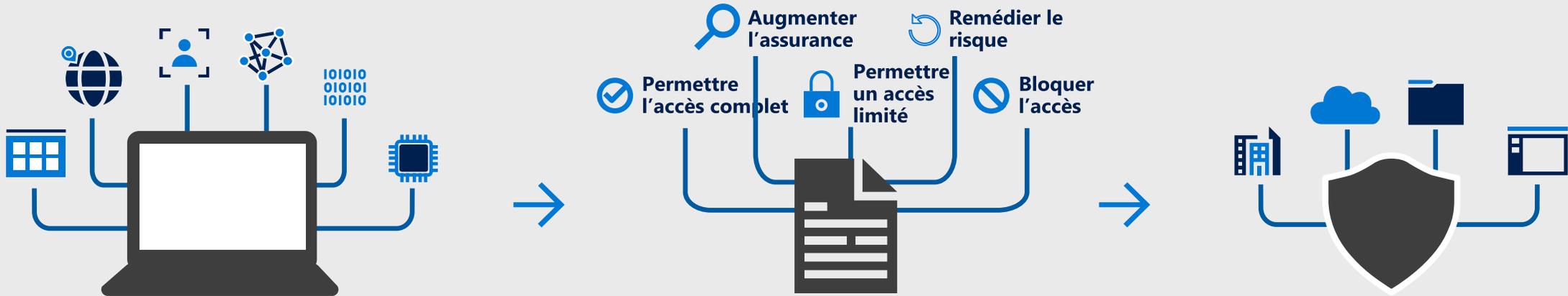
- Est-ce que vous assimilez le Zero Trust ?
- Avez-vous mis en place une équipe virtuelle avec vos parties prenantes ?
- Savez-vous où vous voulez arriver ?
- Savez-vous où vous en êtes aujourd'hui ?
- Avez-vous l'adhésion du niveau CxO pour combler cet écart ?



Télécharger aujourd'hui en [aka.ms/ztmodel](https://aka.ms/ztmodel)

# Stratégie de Contrôle « confiance zéro »

Ne jamais faire confiance. Toujours vérifier.



## Signal

*Pour prendre une décision éclairée*

### Risque terminal

- Gestion du terminal
- Détection des menaces
- Et plus encore...

### Risque utilisateur

- Authentification multi-facteur
- Analyse comportementale
- Et plus encore...

## Décision

*Fondée sur les politiques de l'organisation*

**S'applique aux requêtes entrantes**

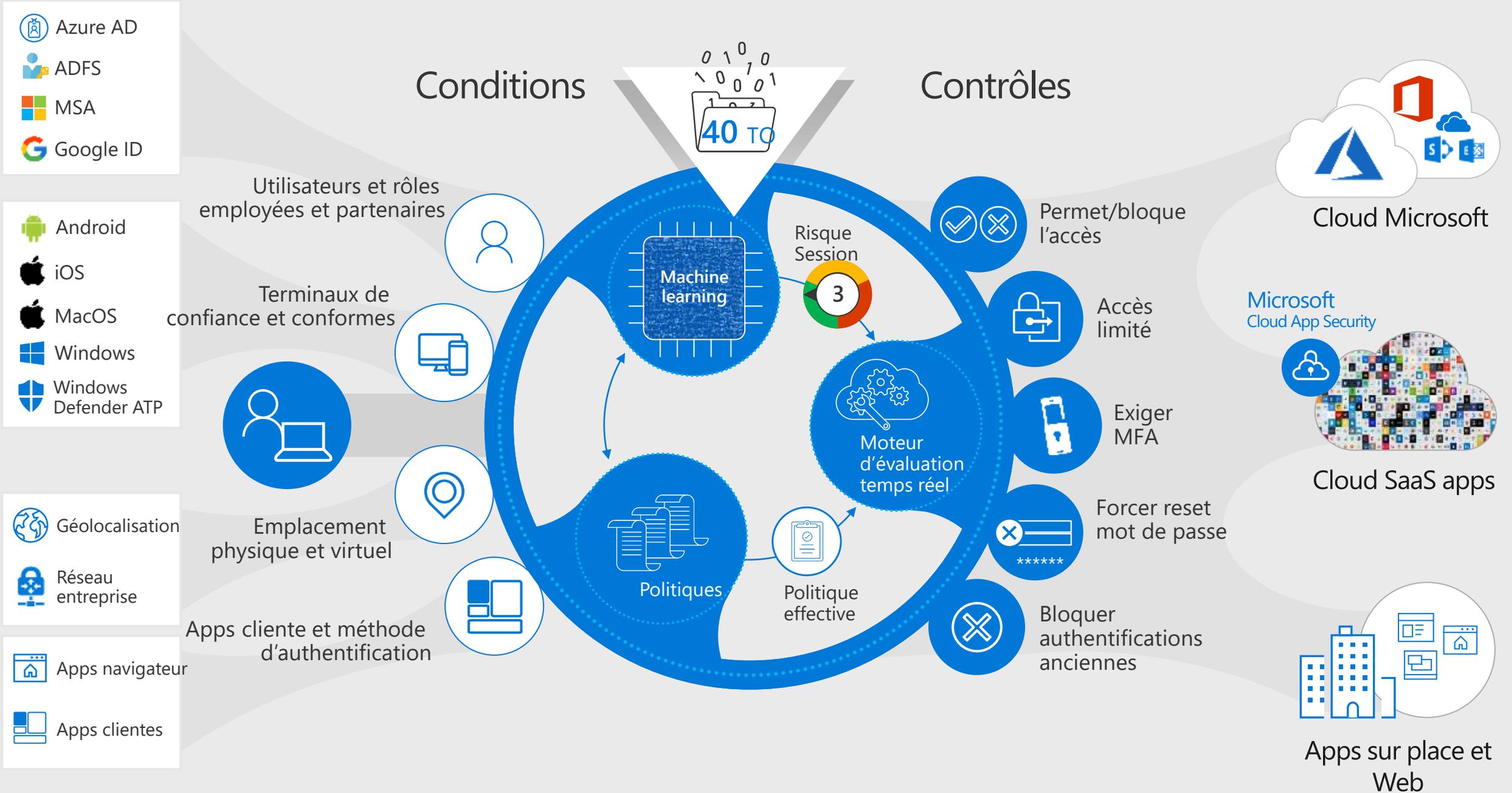
**Réévaluer pendant la session**

## Application

*Des politiques sur l'ensemble des ressources*

**Applications modernes**  
**Applications SaaS**  
**Applications anciennes**  
**Et plus...**

# Accès conditionnel Azure AD (« Confiance zéro »)



- Azure AD
- ADFS
- MSA
- Google ID

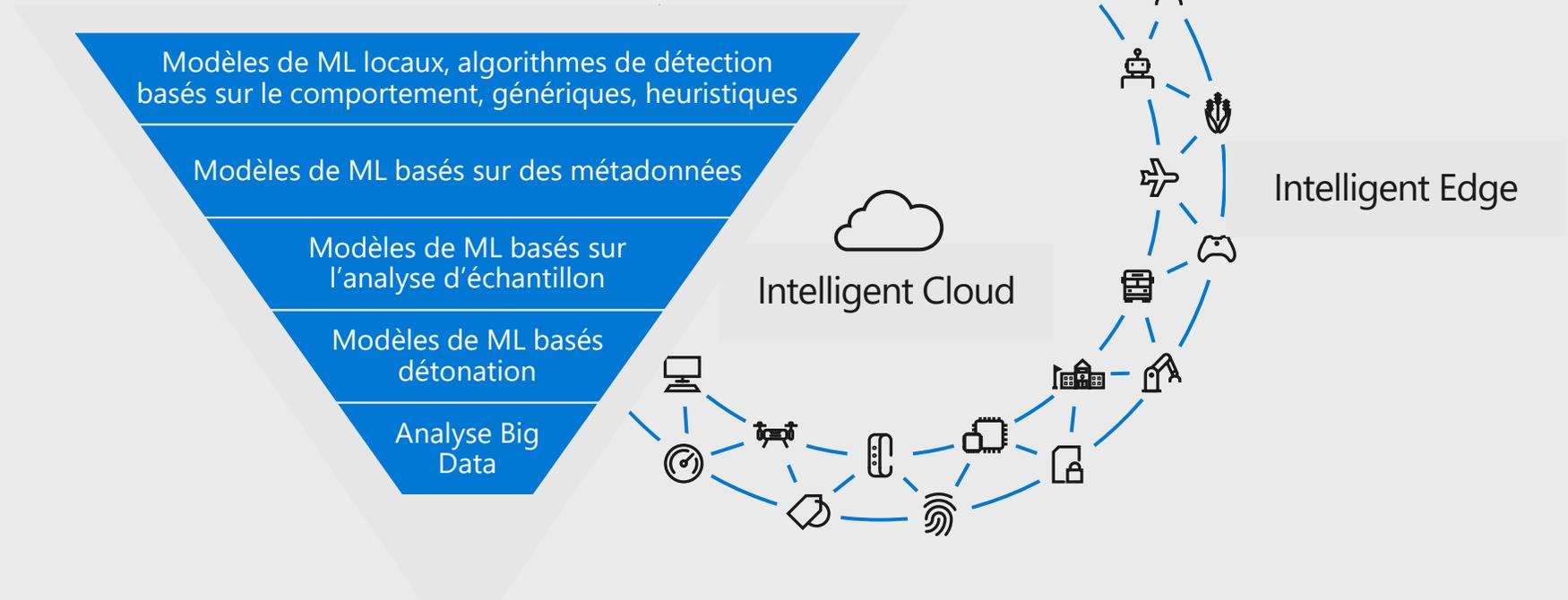
- Android
- iOS
- MacOS
- Windows
- Windows Defender ATP

- Géolocalisation
- Réseau entreprise

- Apps navigateur
- Apps clientes

# Stopper les cyber-attaques

Les renseignements du monde réel  
à l'œuvre grâce à l'IA



**2017** **Octobre 2017** – Des modèles de ML à base de détonation dans le Cloud ont identifié [Bad Rabbit](#), protégeant les utilisateurs 14 minutes après la première survenue.

**6 mars** – Des algorithmes de détection basés sur le comportement ont bloqué plus de 400 000 instances du trojan [Dofoil](#).

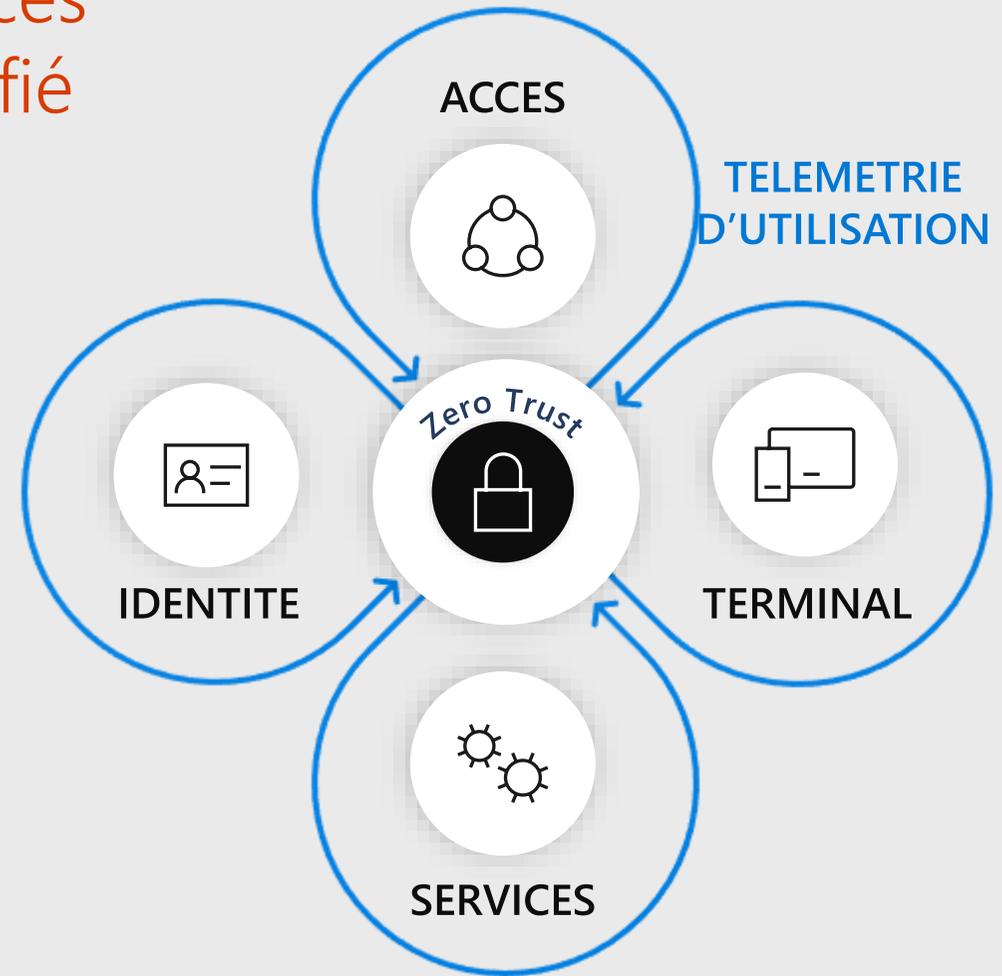
**3 février** – Les algorithmes de ML client ont arrêté automatiquement l'attaque de malware [Emotet](#) en temps réel.

**2018** **Août 2018** – Des algorithmes Cloud de Machine Learning ont bloqué une campagne hautement ciblée pour délivrer la malware [Ursnif](#) à moins de 200 cibles.

# Zero trust

« Identité forte + santé du terminzi + accès utilisateur avec le moindre privilège vérifié avec la télémétrie »

- ✓ Les actifs sont transférés du réseau interne vers Internet... à l'exception des actifs les plus critiques
- ✓ Expérience utilisateur améliorée avec une utilisation d'Internet en premier lieu
- ✓ Surface d'attaque réduite de l'environnement
- ✓ Télémétrie complète, intelligence artificielle pour la détection des anomalies, vérification de l'état du service



# Notre approche de mise en œuvre



## IDENTITE

- Éliminer les mots de passe et migrer vers Windows Hello
- Définir l'authentification multi-facteur comme le défaut



## TERMINIAL

- Exiger que tous les appareils soient gérés de manière moderne.
- S'assurer que tous les terminaux répondent aux exigences de santé



## ACCES

- Déplacer les appareils et les utilisateurs vers les segments de réseau respectifs
- Accordez un accès et des autorisations minimaux



## SERVICES

- Toutes les applications et services appliquent les principes de Zero Trust
- Exiger que les applications et services fournissent leur certificat de santé

# Principales phases du « Zero trust »

## Pre-Zero Trust

- ✓ Gestion des appareils non requise
- ✓ Authentification à un facteur pour les ressources
- ✓ La capacité de faire respecter une identité forte existe

## Vérifier Identité



- ✓ Tous les comptes d'utilisateurs sont configurés pour une application forte de l'identité
- ✓ Identité forte appliquée pour O365
- ✓ Droits d'utilisateur avec le moindre privilège
- ✓ Éliminer les mots de passe - modèle basé sur la biométrie

## Vérifier Terminal



- ✓ État de l'appareil requis pour SharePoint, Exchange, Teams sur iOS, Android, Mac et Windows
- ✓ Données d'utilisation pour les applications et les services
- ✓ Gestion des périphériques requise pour l'accès réseau à plusieurs niveaux

## Vérifier Accès



- ✓ Internet uniquement pour les utilisateurs
- ✓ Établir des solutions pour les appareils non gérés
- ✓ Modèle d'accès le moins privilégié
- ✓ État de l'appareil requis pour le réseau d'entreprise filaire / sans fil

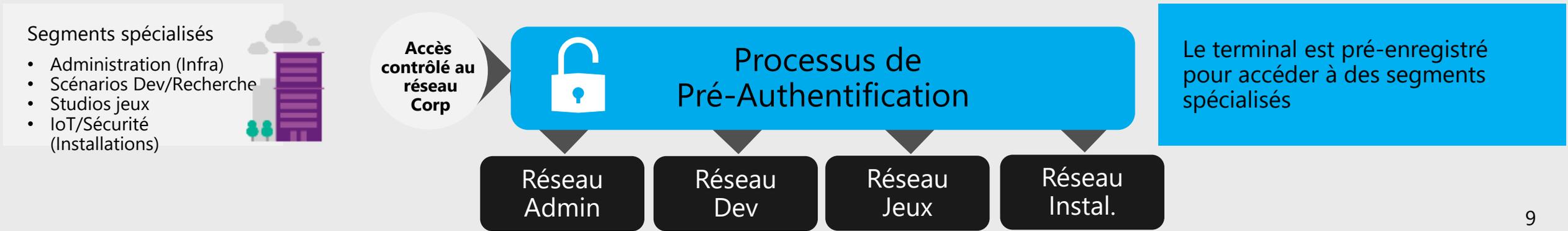
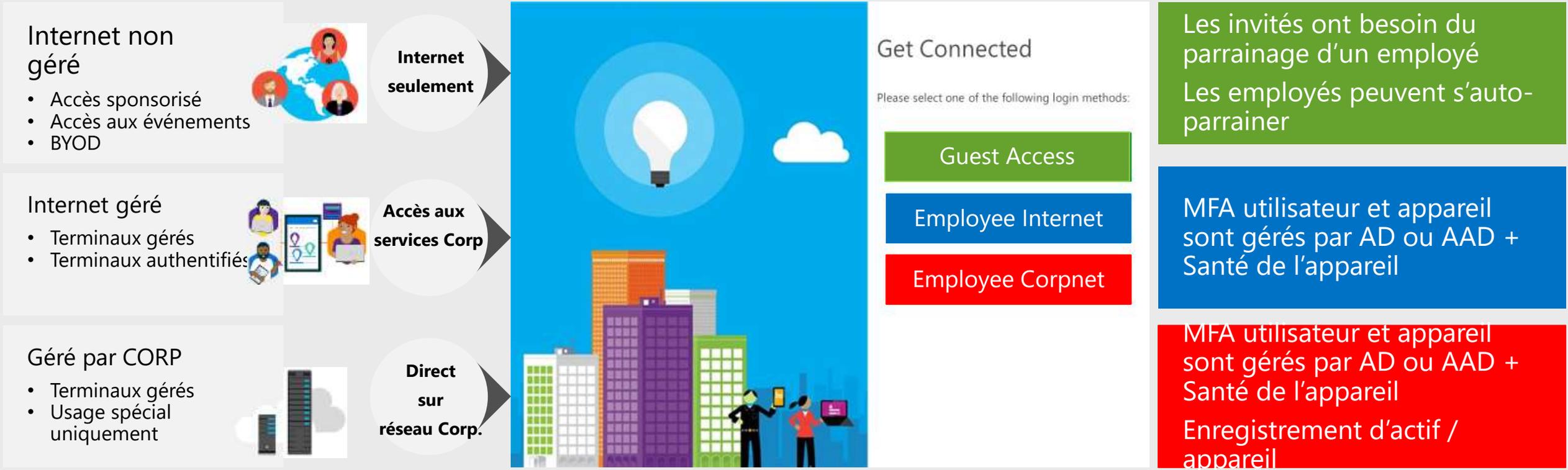
## Vérifier Services



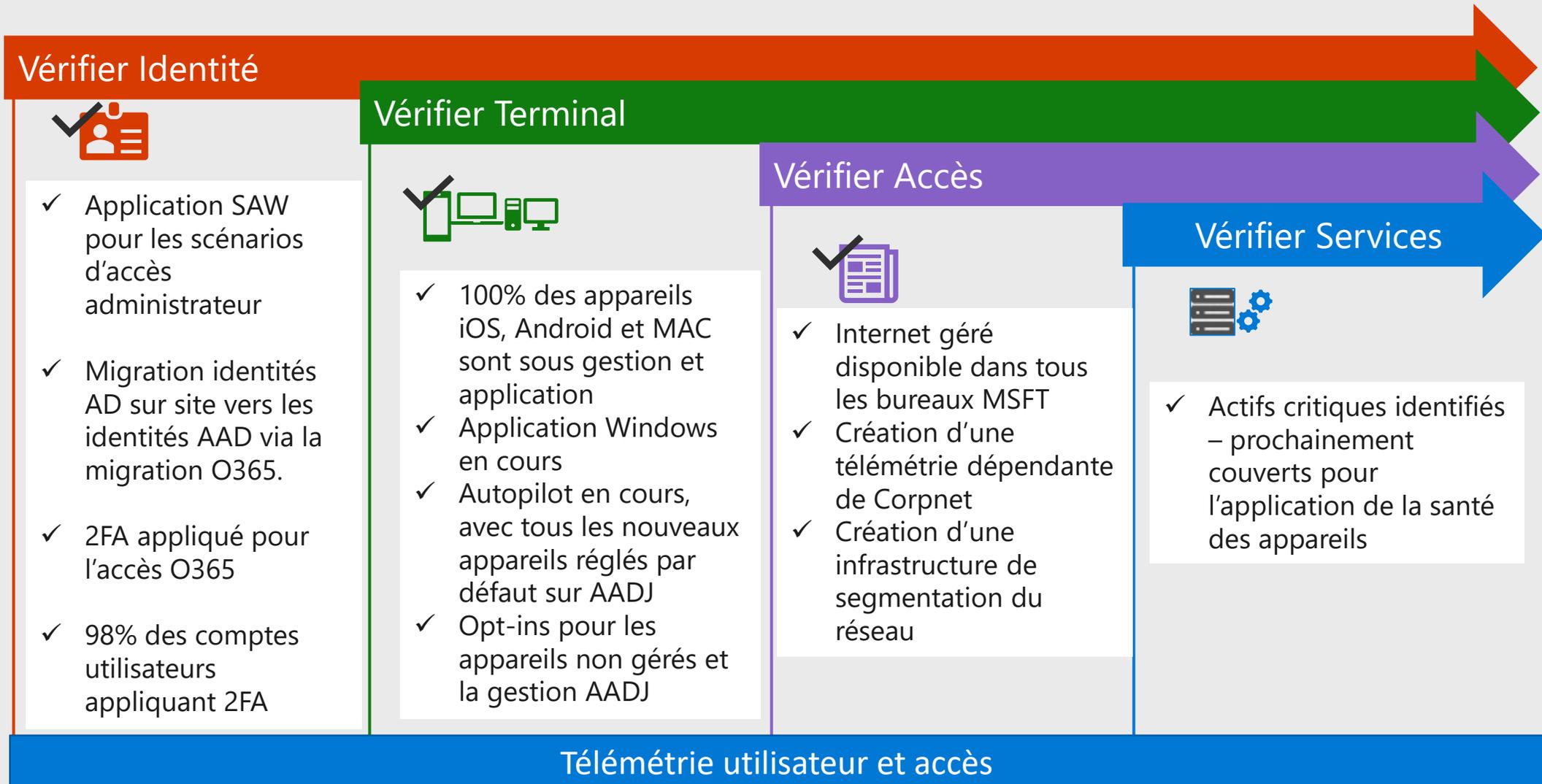
- ✓ Élargir la couverture des exigences relatives à l'intégrité de l'appareil
- ✓ Concept de santé du service et POC (**Futur Distant**)

Télémétrie des utilisateurs et des accès

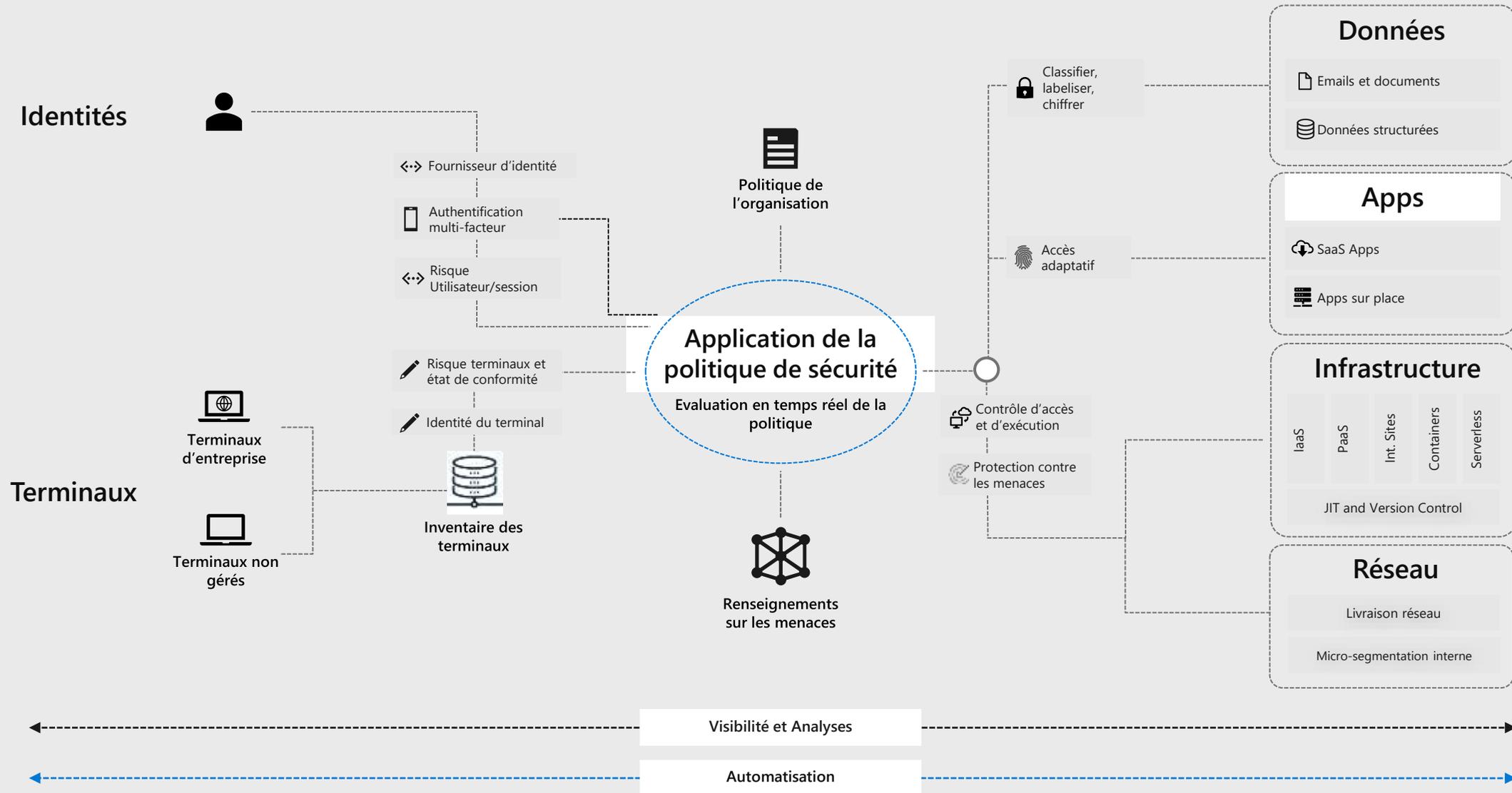
# Réseau Zero Trust –Segmentation Réseau



# Principales phases du « Zero trust » - Progrès

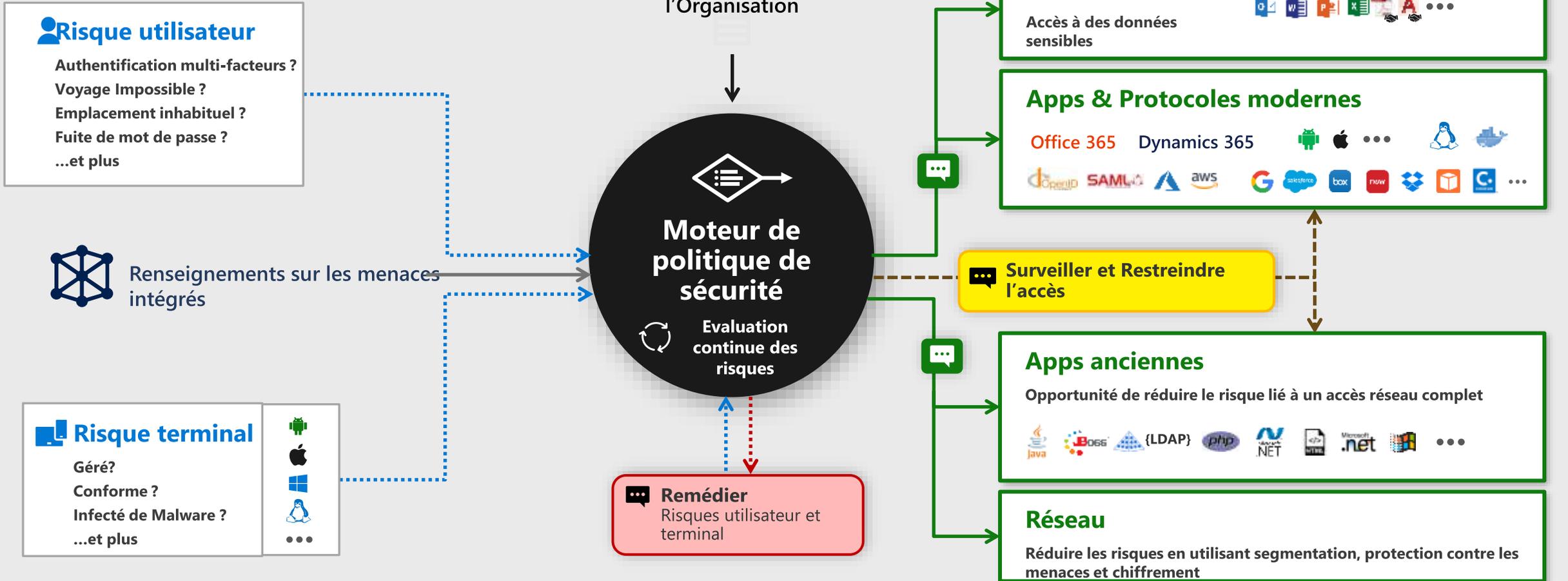


# Architecture « Zero Trust »



# Modèles Zero Trust

Approche moderne de l'accès



## Signal

pour prendre une décision informée



## Décision

basée sur politique organisationnelle



## Application

de la politique sur les ressources

# Approche sécurité de Microsoft

## Opérations

Des opérations de sécurité qui fonctionnent pour vous



# Sécurité Microsoft



## Technologie

Technologie de niveau entreprise



## Partenariats

Des partenariats pour un monde hétérogène

## Opérations

Des opérations de sécurité qui fonctionnent pour vous



# Sécurité Microsoft



## Technologie

Technologie de niveau entreprise



## Partenariats

Des partenariats pour un monde hétérogène

# Une fondation sûre à l'échelle mondiale

Chaque **Datacenter physique** est protégé par une protection multicouche de classe mondiale



Plus de **100** datacenters à travers la planète

Sécurisé avec une **sécurité opérationnelle** de pointe

- Accès restreint
- Surveillance 24x7
- Experts en sécurité globale



**Infrastructure cloud mondiale** avec protection matérielle et réseau personnalisée

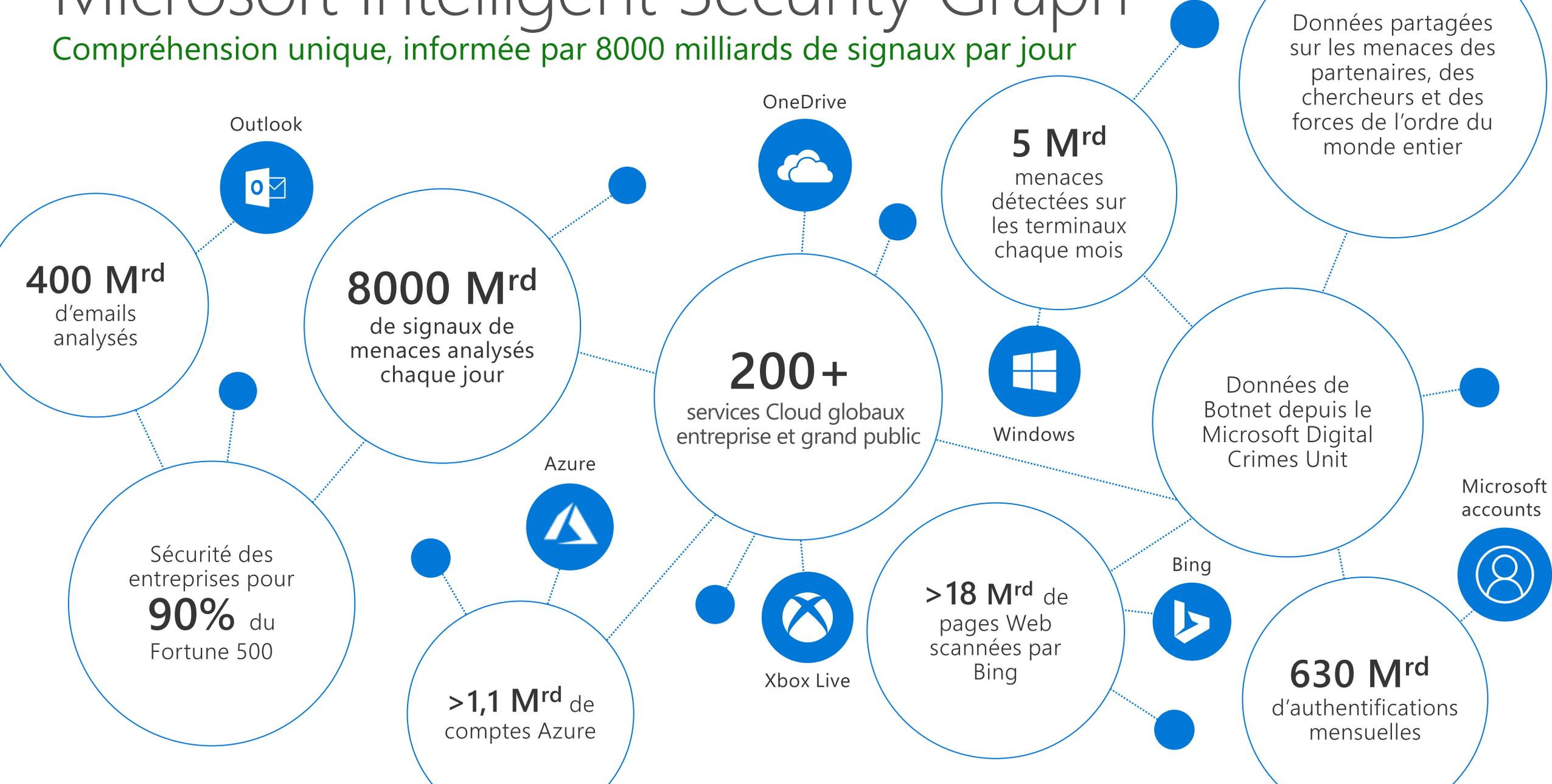




Des opérations de sécurité qui  
fonctionnent pour vous

# Microsoft Intelligent Security Graph

Compréhension unique, informée par 8000 milliards de signaux par jour





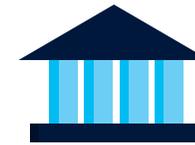
# Des partenariats pour un monde hétérogène



**Partenariat  
avec des pairs**



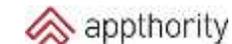
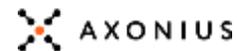
**Travailler au sein  
d'alliances  
industrielles**



**Travailler avec les  
états**

# Microsoft Intelligent Security Association

La collaboration renforce la protection



Faire équipe avec nos partenaires de sécurité pour construire un écosystème de solutions de sécurité intelligentes qui mieux se défendront contre un monde de menaces accrues

# Fast IDentity Online : l'alliance FIDO

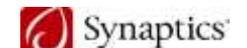
Le plus grand écosystème du monde pour une authentification interopérable basée sur des standards

Sécurité sur place et sur le web

Crédentités des utilisateurs  
mobiles sécurisés

Authentification sécurisée

## Membre du conseil d'administration FIDO



“ The first step in creating a safer internet must come from our own industry, the enterprises that create and operate the world’s online technologies and infrastructure. ”

**Brad Smith**

President and Chief Legal Officer, Microsoft



## Cybersecurity Tech Accord

Plus de 60 entreprises mondiales travaillent ensemble pour améliorer la sécurité, la stabilité et la résilience du cyberspace.

# Appel de Paris pour la confiance et la sécurité dans le cyberspace

67 Etats

358 Entreprise

139 Organisations de la société civile





Multi-cloud

SIEM

Azure Sentinel



Partenariats



Prévenir

Protéger

Microsoft Defender

XDR

XDR : eXtended Detection & Response

SIEM

# Azure Sentinel



Multi-cloud



Partenariats

Cloud natif, toute donnée, toute entité



Cloud natif



Toute donnée



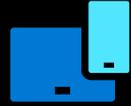
IA



Automatisation



Identités



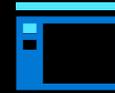
Terminaux



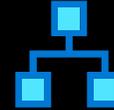
Données



Infrastructure



Apps



Réseau

Microsoft Defender

XDR

← Protection inter-domaines →

### Microsoft 365 Defender

- Identities
- Terminals
- Apps
- E-mail
- Apps Cloud
- Docs

### Azure Defender

- SQL
- VMs Servers
- Containers
- Network
- IoT
- Azure App Services

# Microsoft Defender

XDR

# Les meilleurs produits de sécurité Microsoft 365



## Identités

Microsoft Defender  
for Identity



Anciennement Azure Advanced  
Threat Protection



## Terminaux

Microsoft Defender  
for Endpoint



Anciennement Microsoft Defender  
Advanced Threat Protection



## Apps Cloud

Microsoft Cloud  
App Security



## Données utilisateur

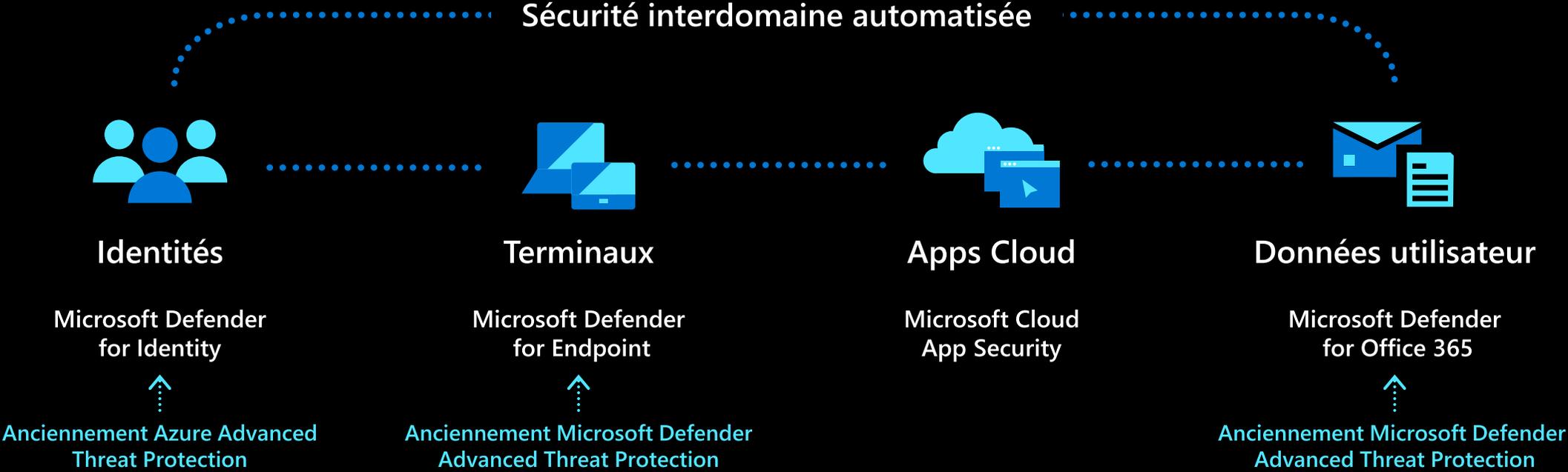
Microsoft Defender  
for Office 365



Anciennement Microsoft Defender  
Advanced Threat Protection

Passer des silos individuels à une sécurité coordonnée entre domaines

# Microsoft 365 Defender



Passer des silos individuels à une sécurité coordonnée entre domaines

# Microsoft 365 Defender

Sécurité inter-domaines automatisée



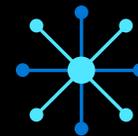
Un seul portail  
- entités unifiées



Protection active  
coordonnée contre les  
menaces



Réparation  
automatique des actifs  
affectés



Analyse et intelligence des  
menaces unifiées



Chasse aux menaces  
Inter-domaines

Management · APIs · Connecteurs

En apprendre davantage :  
<http://aka.ms/m365d>

L'essayer aujourd'hui :  
<http://security.microsoft.com>

# Notre stratégie sécurité

Assurer la sécurité numérique de nos clients pour permettre leur transformation digitale grâce à une plateforme complète, des renseignements uniques et de larges partenariats



# Merci !

ευχαριστώ    Salamat Po    متشكراً    شكراً    Grazie  
благодаря    ありがとうございます    Kiitos    Teşekkürler    谢谢  
ឧបត្ថម្ភ    Obrigado    شكریه    Terima Kasih    Dziękuję  
Hvala    Köszönöm    Tak    Dank u Wel    ДЯКУЮ    Tack  
Mulțumesc    спасибо    Danke    Cám ơn    Gracias  
多謝晒    Ďakujem    תודה    നന്ദി    Děkuji    감사합니다

# Discussion

