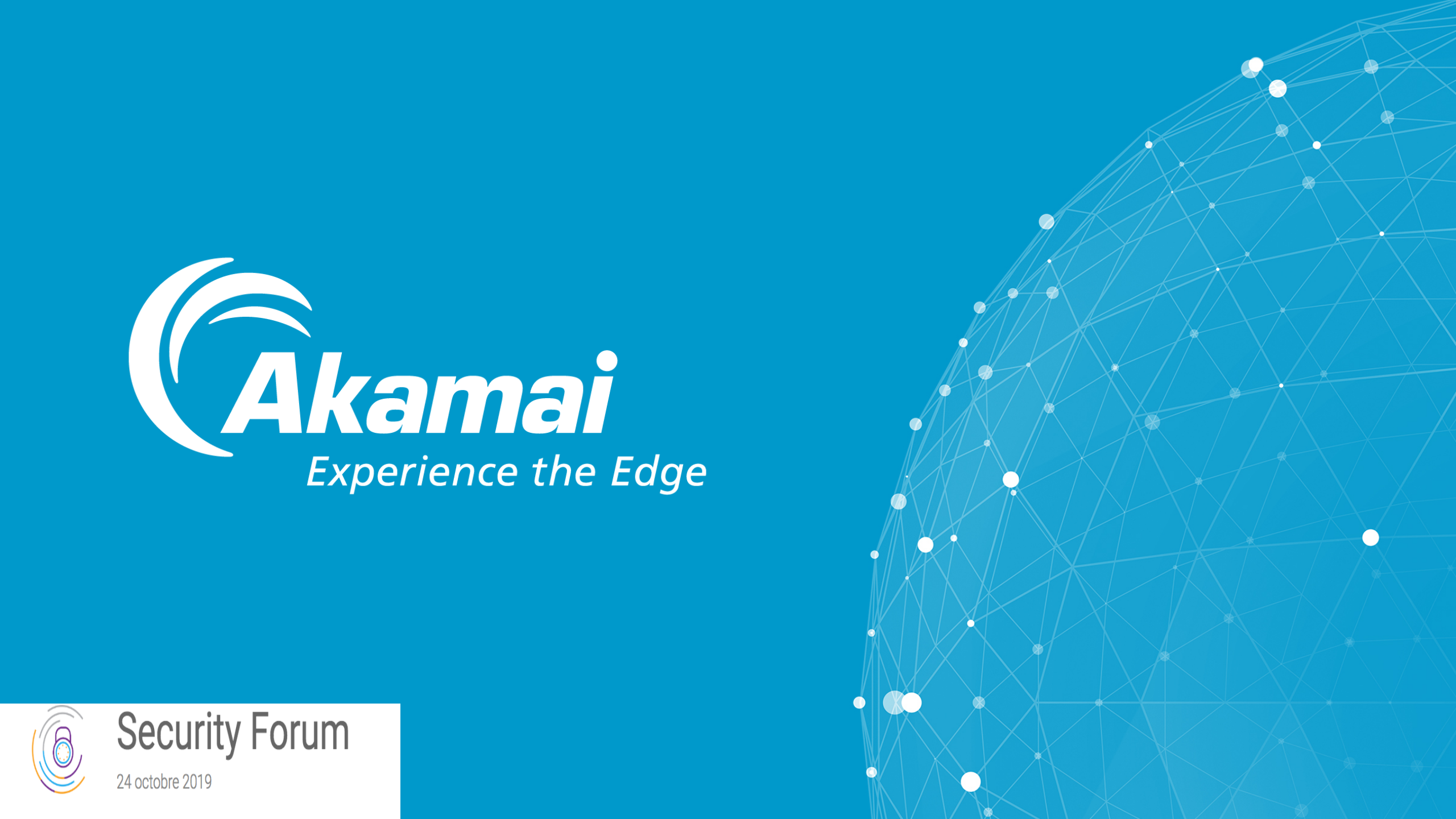


Security Forum

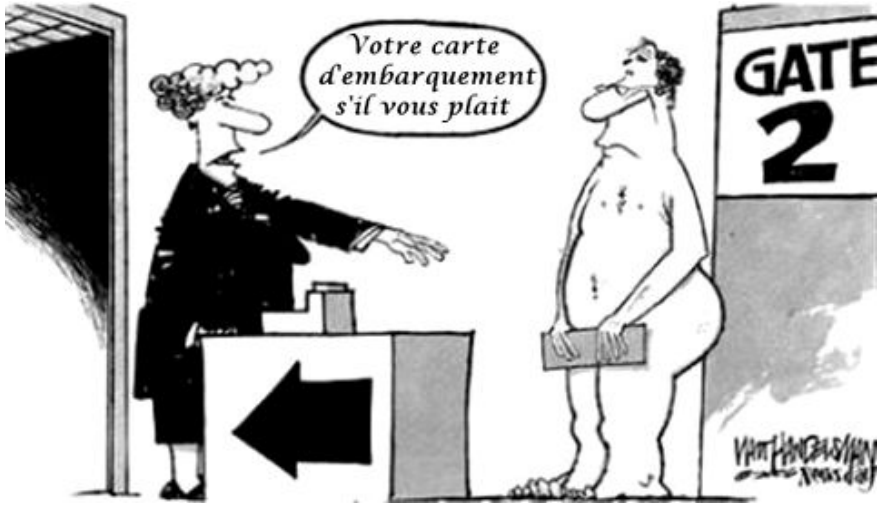
24 octobre 2019

LA DEFINITION ZERO TRUST

Zéro Trust est un modèle de sécurité réseau basé sur un processus strict de contrôle de l'identité. Le cadre impose que seuls les utilisateurs et les terminaux authentifiés et autorisés peuvent accéder aux applications et aux données. En même temps, il protège ces applications et ces utilisateurs contre les menaces avancées sur Internet.

Ce modèle a été introduit pour la première fois par un analyste chez Forrester Research en 2008.

https://www.dailymotion.com/video/x5ims36



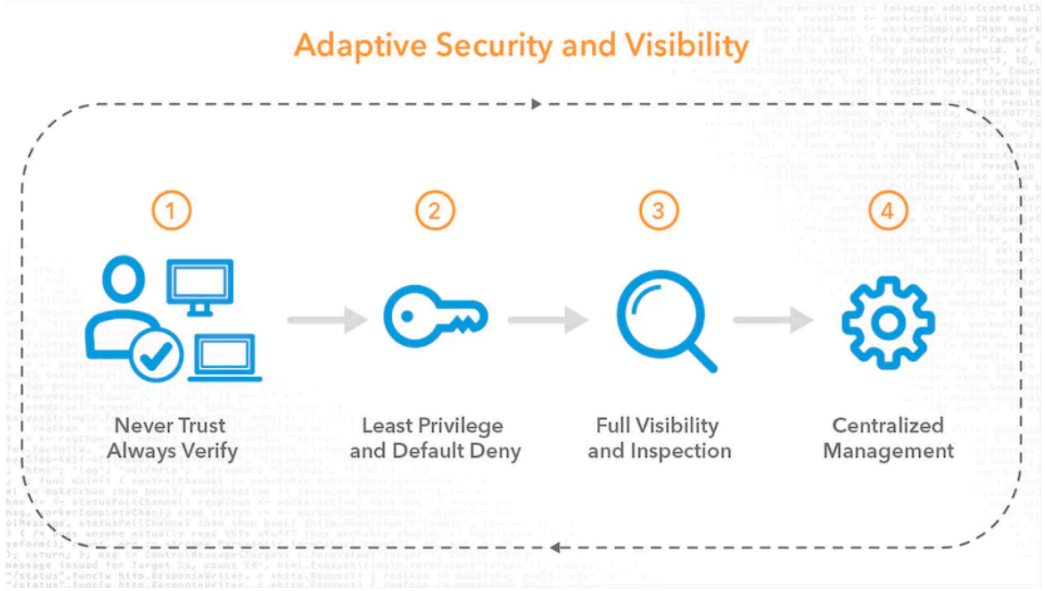
Passez du NAM au ZTNA

Akamai

POURQUOI LA NECESSITE DU ZERO TRUST

Les utilisateurs, les terminaux, les applications et les données sortent progressivement du périmètre de l'entreprise et de sa sphère de contrôle.

La politique qui consiste à faire confiance tout en vérifiant n'est plus envisageable avec l'apparition de menaces avancées qui s'infiltrent dans le périmètre de l'entreprise.



Les nouveaux processus métier qui voient le jour sous l'impulsion de la transformation digitale étendent la surface d'exposition aux risques.

Les périmètres classiques sont complexes, porteurs de risques et ne conviennent plus aux modèles économiques actuels.

LE CONTEXTE CYBER TRES ACTIF

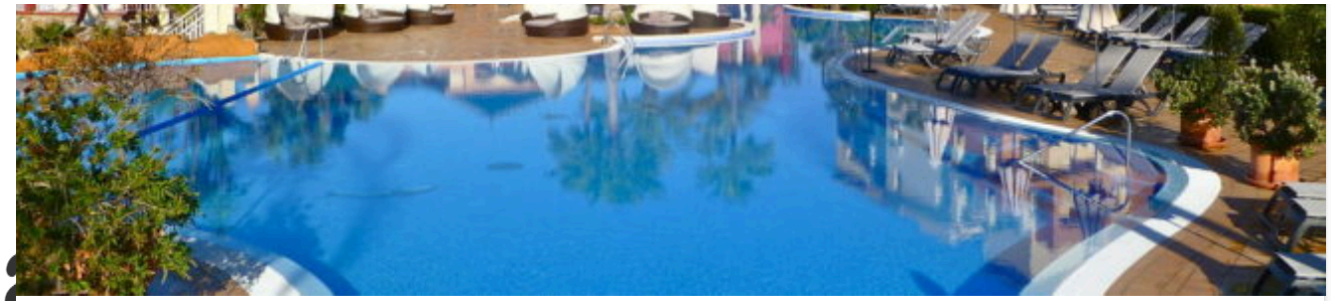
La ville de Baltimore prise en otage par des cybercriminels

Ransomware : un laboratoire de police scientifique belge paie la

Ransomwa
à l'arrêt

Collection #1 : 773 millions de mails et 21 millions de mots de passe ont fuité

ieurs



izaines de

Altran paralysée pa

HÔTELS MARRIOTT : 123 MILLIONS $ D'AMENDE APRÈS LA FUITE DE DONNÉES DE 2018

M6 face à une cyberattaque inédite

Akamai

Applications et utilisateurs sortent du périmètre classique

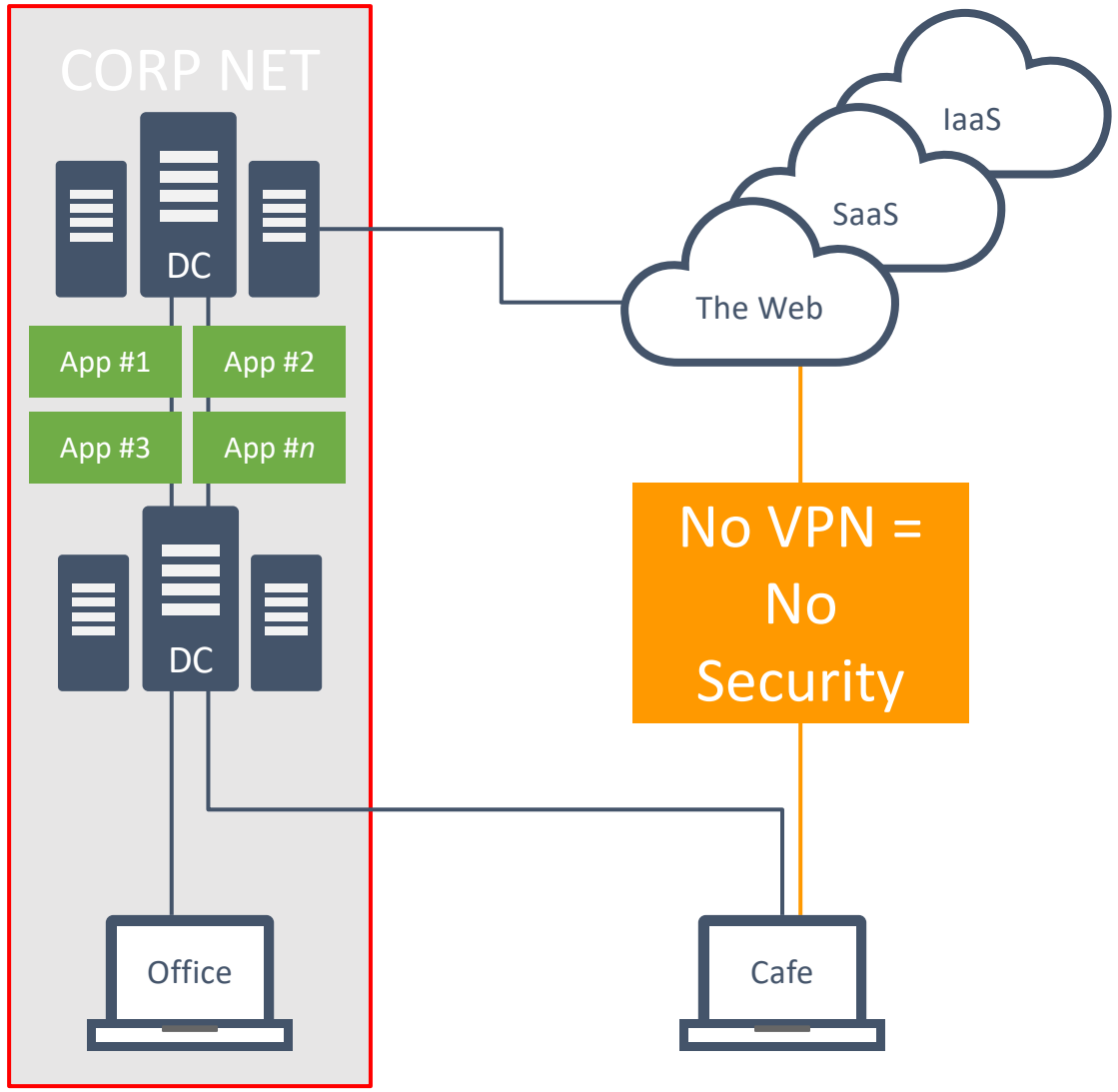
- Dans 40% des entreprises, les **télétravailleurs** représentent 21% à 40% de la masse salariale

- Les Entreprises utilisent des applications dans le cloud près de **50% du temps**

- Environ **10% des entreprises** déclarent connaître avec précision les terminaux qui accèdent à leurs réseaux

- La Majorité des entreprises cherchent à **rationnaliser leurs coûts d'Infrastructure**

Les Utilisateurs et les applications d'entreprise sont de plus en plus mobiles



- Complexité
- Latence
- Risque Sécurité important

Akamai

Les challenges liés à l'accès aux applications sont nombreux

Renforcer la sécurité

Liste blanche des IP, restriction d'ouverture des ports, authentification multi-facteurs

Administration complexe

Charge de travail liée à la création de nouveaux profils et à la maintenance des terminaux

Evolutivité et temps de déploiement

Infrastructure DMZ, modèle historique hardware

Tiers: Fournisseurs, Partenaires, Externes

Nombre exponentiel, Turn-over, mobilité

Terminaux mobiles

Smartphone/tablette avec sécurité limitée

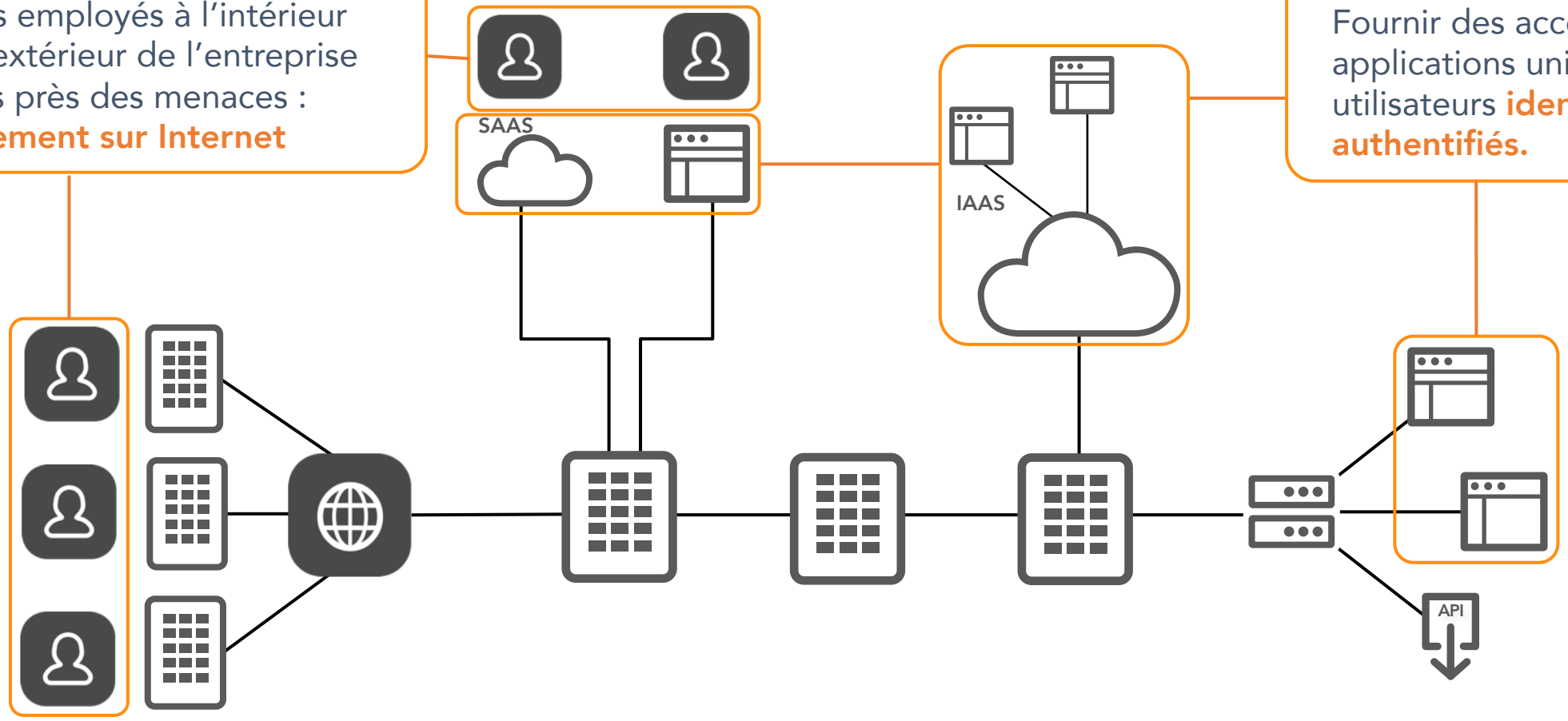
Audit et Surveillance

Visibilité, intégration SIEM , conformité

Adopter une Posture Zéro Trust

Atténuer les attaques subies par vos employés à l'intérieur ou à l'extérieur de l'entreprise au plus près des menaces : **directement sur Internet**

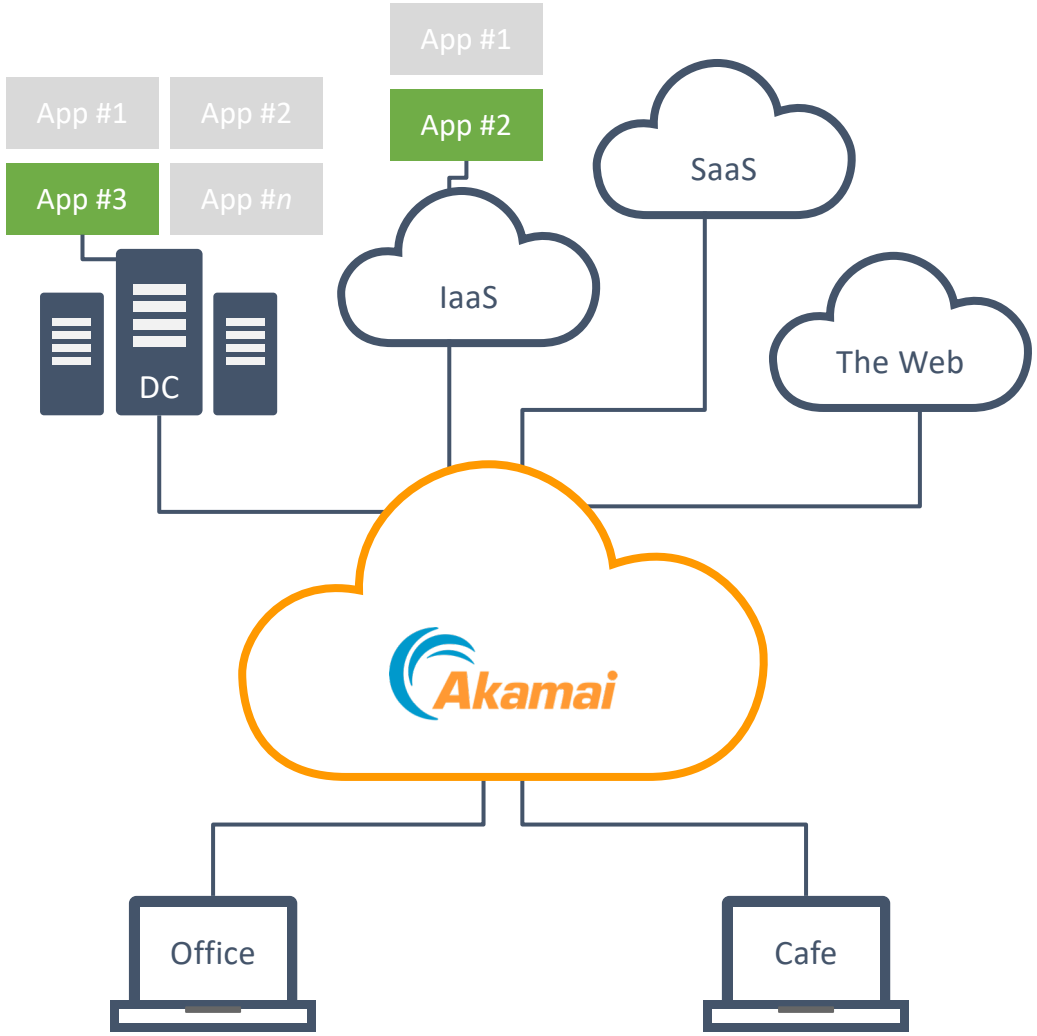
Zéro Confiance
Fournir des accès aux applications uniquement aux utilisateurs **identifiés et authentifiés.**



Applications

Sous votre Contrôle

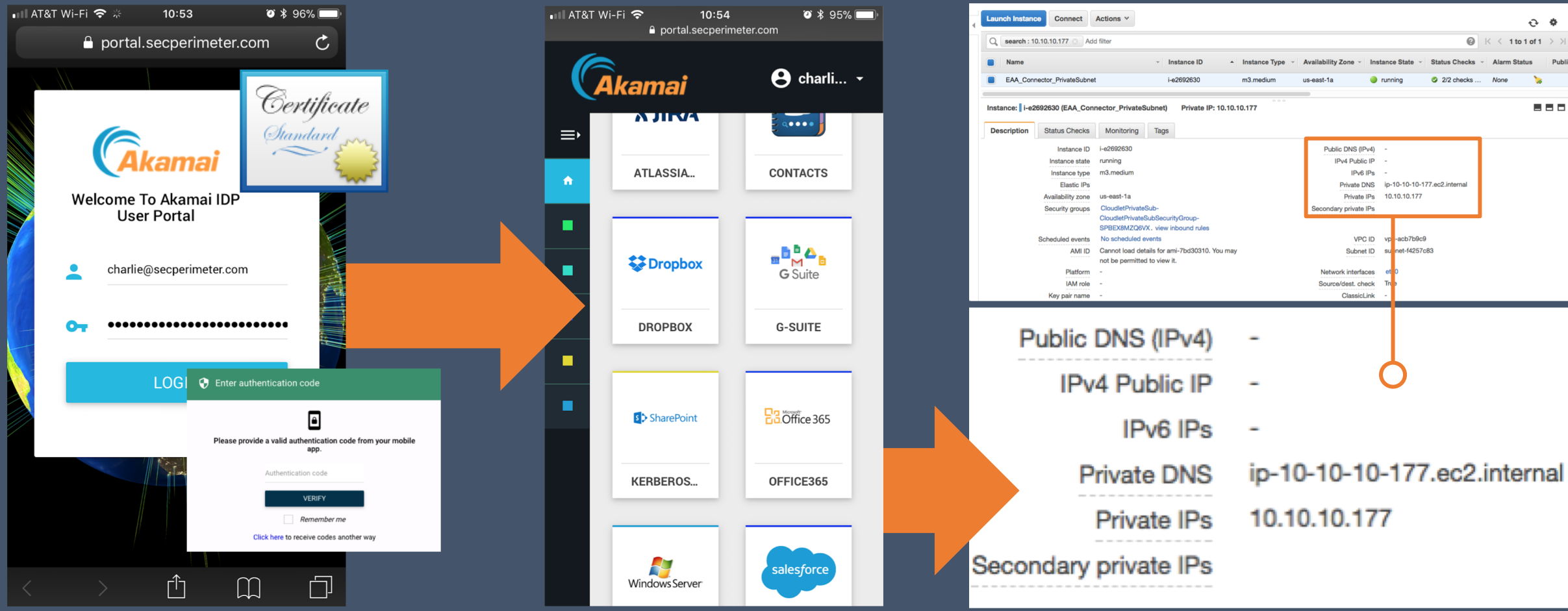
Adopter un schéma Simple et Agile pour vos accès et Protégez vous des Menaces



- Simple
- Agile
- Risque faible

Akamai

Accès Invisible sur Internet et toujours contrôlé



Les Cas d'usage d'adoption de cette approche agile de la Gestion des Accès

Sécuriser les accès des applications **cloud**

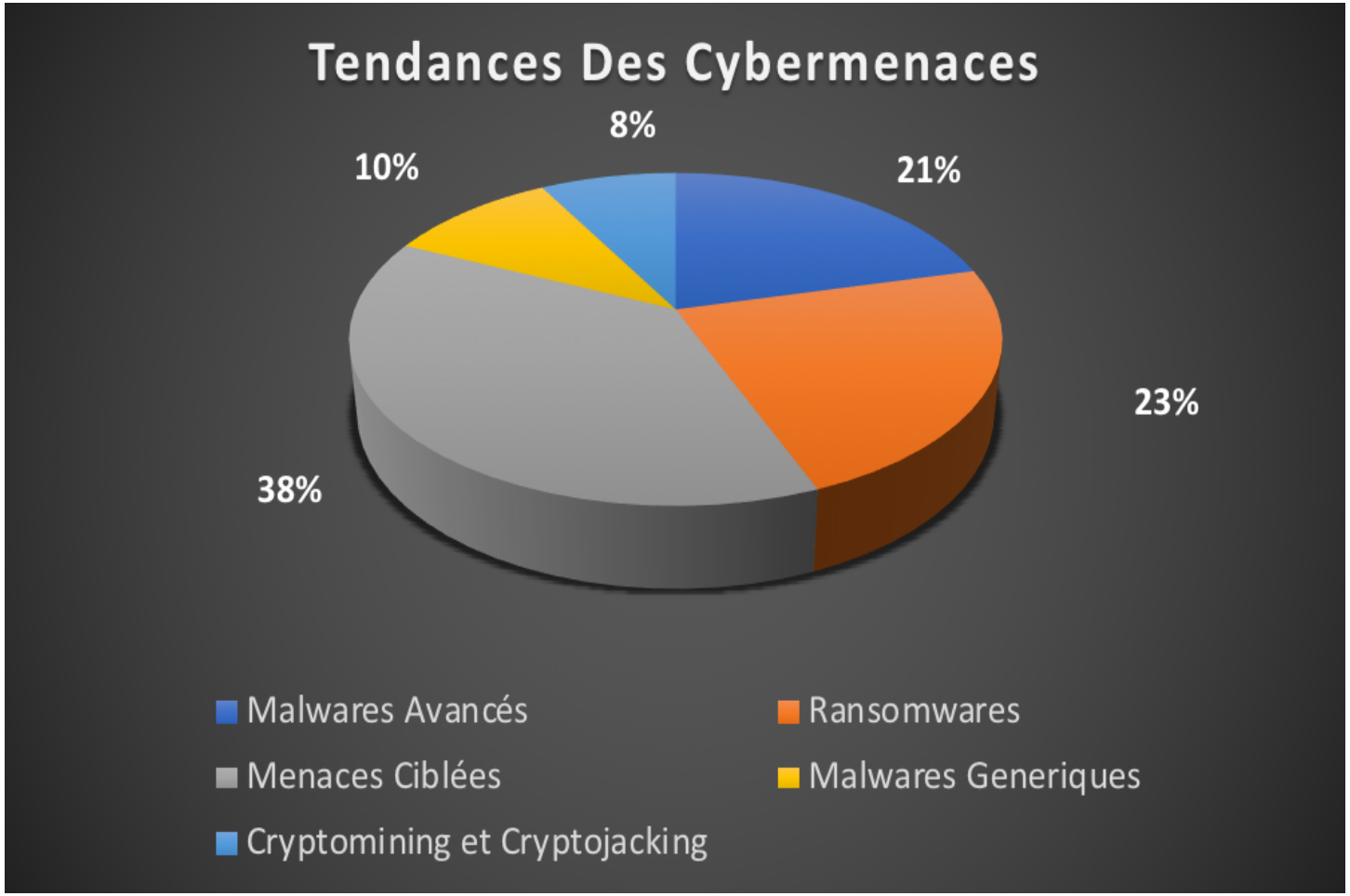
Fusions & Acquisitions (# SI)

Sécuriser les accès aux applications **des partenaires**

Télétravail Substitution du VPN Classique

Applications
Que vous contrôlez
moins

Les Tendances Mondiales des Cyber Menaces



- **Cryptomining/Cryptojacking**

  Utilisation Légitime et malveilante de la CPU pour permettre le chiffrement des crypto monnaies

- **Ransomwares**

  Charge utile malveillante & RaaS

- **Menaces Ciblées**

  Hacking, Vols de privilèges, Vols de crédentials, Mouvement latéraux
  Exploits & exploitation de failles applicatives

- **Malwares Avancés**

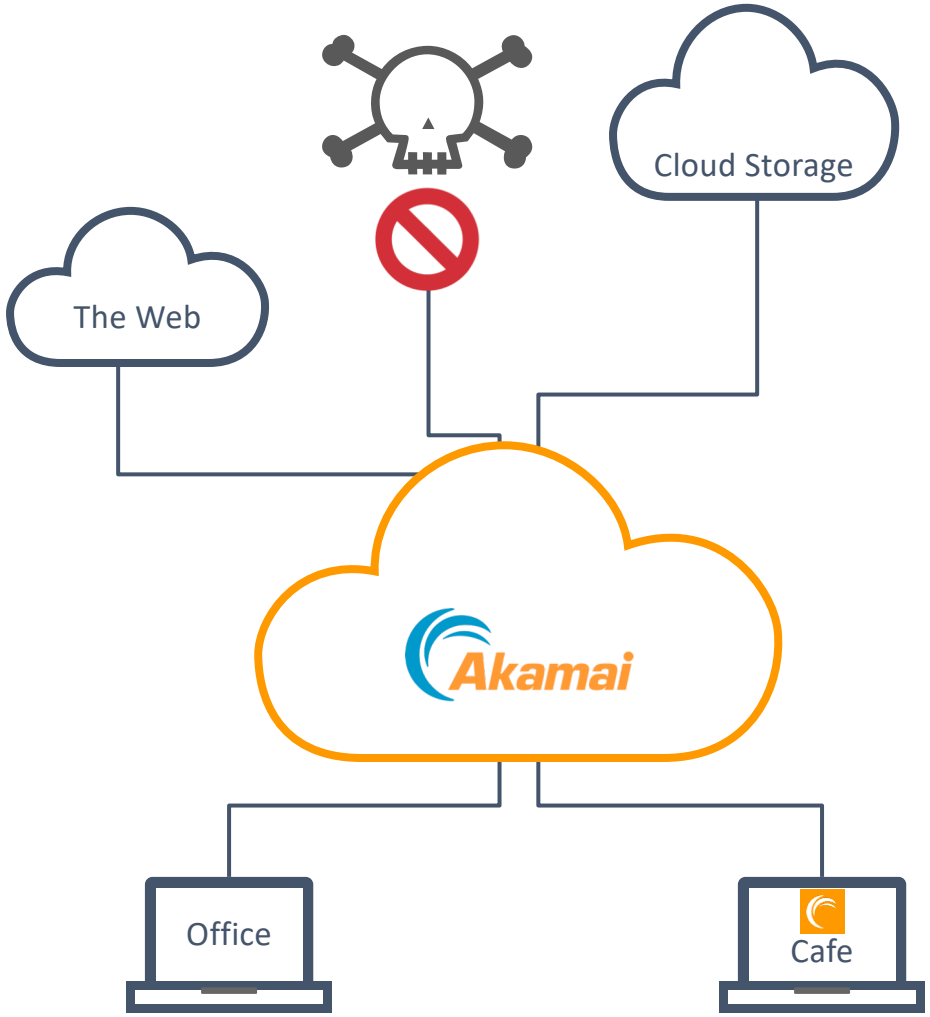
  Attaques Zéro-Day avec différents processus
  Vers, chevaux de Troie, script VB, PDF, attaques sans fichier

- **Malwares Géneriques**

  Première Forme d'attaque

Akamai

Approche évolutive de Prévention des Menaces



Protection des Menaces à travers une Passerelle Internet Gateway

- Identifie & bloque l'accès aux domaines malveillants ,(URLs & contenu)
  - Client & clientless
  - Rampe de lancement DNS
  - Cloud Security Intelligence
- Bloque les communications des devices compromis
- Filtre l'accès de contenu inapproprié
- Prévention d'exfiltration de données via DNS

Les cas d'usage pour une protection optimale

Améliorer votre **Posture** Sécurité en toute **Simplicité**

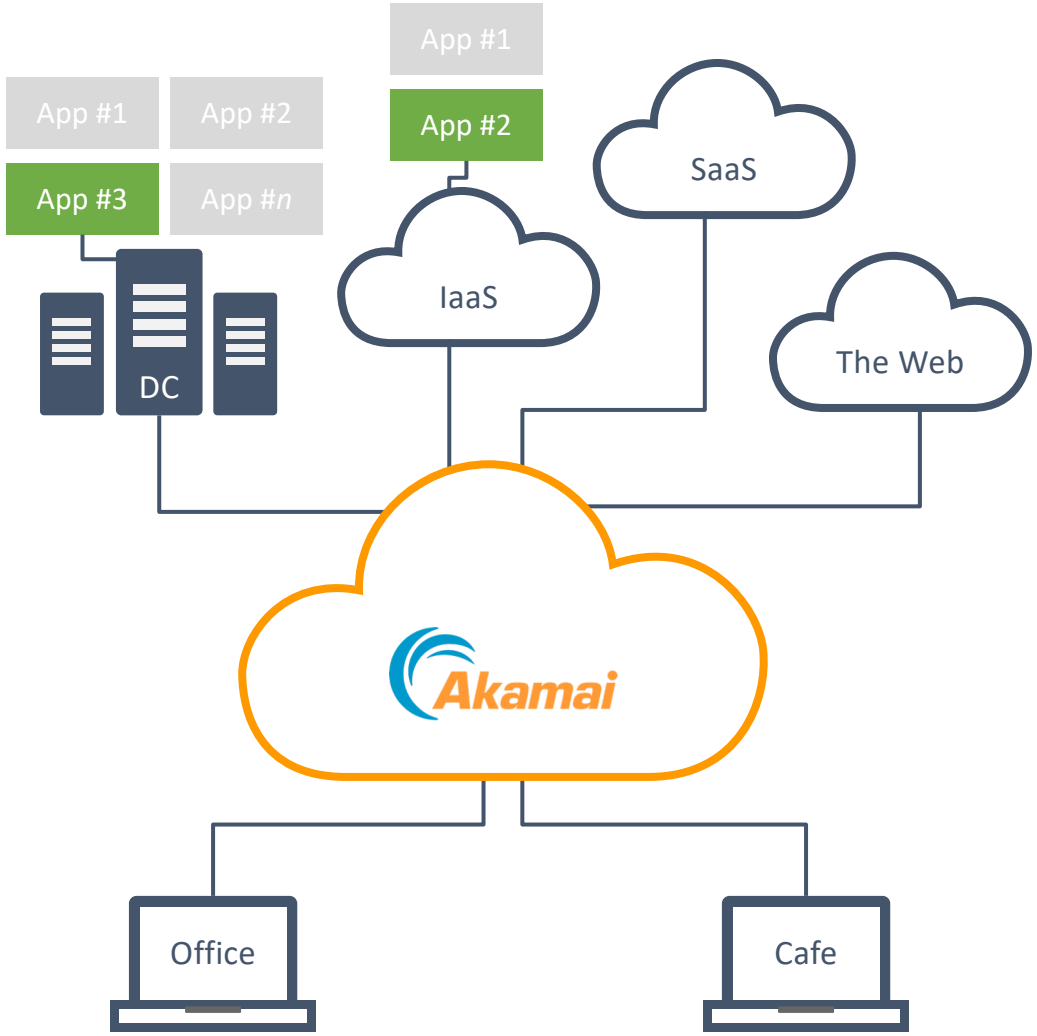
Accès Direct Internet via la Plateforme ($$)

Contrôle & protection Off-net/on-net

Guest Wifi Mise en place d'une politique rigoureuse d'utilisation

Akamai

Zéro Trust est une Posture Technologique



Adopter la plateforme pour sécuriser les applications de l'entreprise et vos collaborateurs

Identity Aware Proxy

- Identité, single sign-on & authentication Multi Facteurs
- optimiser l'accès aux applications, la performance & la sécurité

Secure Internet Gateway

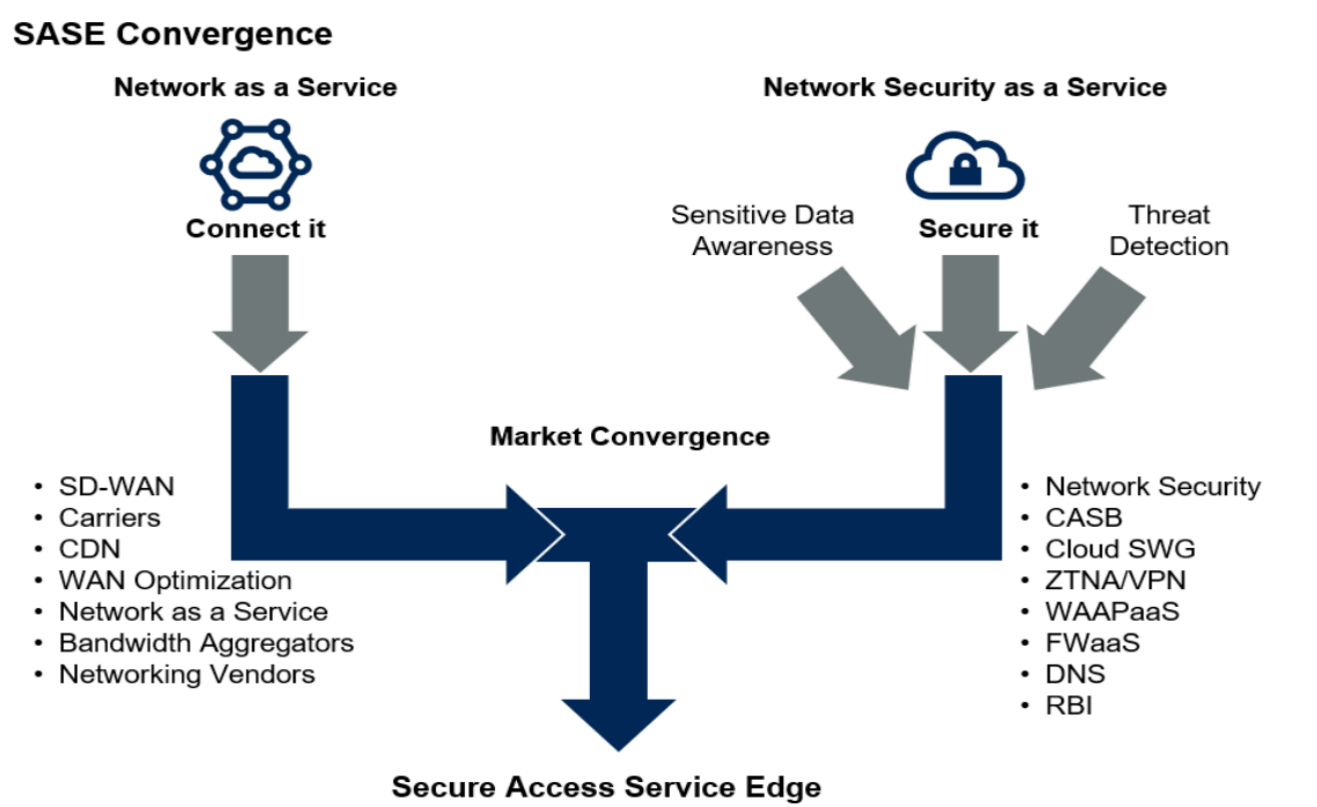
- Protection basée sur le DNS-Intelligence contre l'exfiltration de données, les malwares et les menaces avancées

Akamai

Le Zéro Trust composante du SASE

- By 2023, 20% of enterprises will have adopted SWG, CASB, ZTNA and branch FWaaS capabilities from the same vendor up from less than 5% in 2019.

- By 2024, at least 40% of enterprises will have explicit strategies to adopt SASE, up from less than 1% at year-end 2018.



CDN: content delivery network; RBI: remote browser isolation; WAAPaaS: web application and API protection as a service.
Source: Gartner
ID: 441737

Akamai

MERCI

https://www.akamai.com/fr/fr/solutions/security/zero-trust-security-model.jsp

Julien Pulvirenti
jpulvire@akamai.com

Akamai
Experience the Edge