École 2600

Cours Zero Trust

Introduction

Juillet 2023

Présentation de l'enseignant

- Jean-Christophe TOUVET
  - Consultant et auditeur sécurité informatique depuis 1994
  - Enseignant et formateur depuis 1998
    - Sécurité réseau
    - Management du risque informatique
    - Audit de systèmes de management
  - Certifié ISO 27001 Lead Auditor en 2008
  - Certifié EBIOS & ISO 27005 Lead Risk Manager en 2015
  - Fondateur et manager de 3 équipes d'audit SSI puis manager de 2 équipes PASSI
    - EdelWeb, Bull, ESR Consulting, Devoteam et CGI Business Consulting
  - Coanimateur du GT IS0 27002:2022 du Club 27001 et *animateur du GT Zero Trust du CLUSIF*

Photographie non contractuelle ☺

Démarche pédagogique et planning

- Cours magistral
- Évaluation
  - Questionnaire sur le cours
- Planning

	9h30	10h30	11h30	12h30	13h30
11 juillet	Cours		*Déjeuner*	Cours	
17 juillet	Cours		*Déjeuner*	Évaluation	

Le concept de Zero Trust

Pourquoi le Zero Trust ?

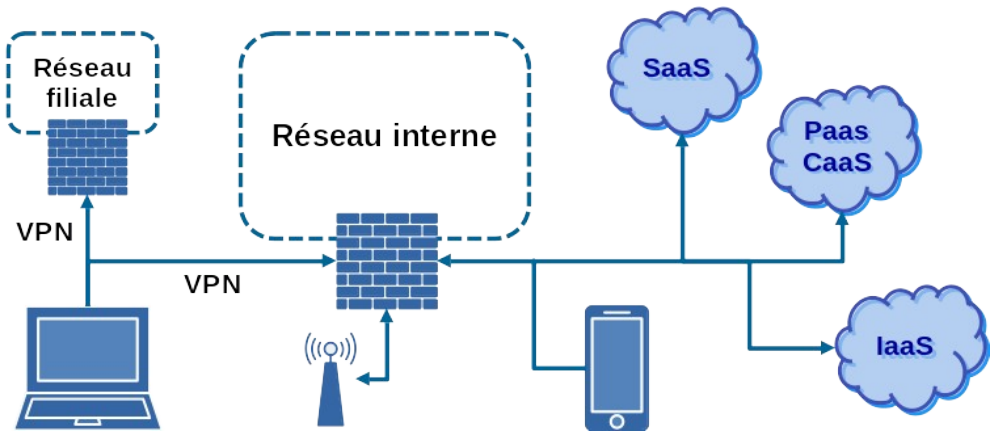
Les motivations pour adopter un nouveau modèle de cybersécurité

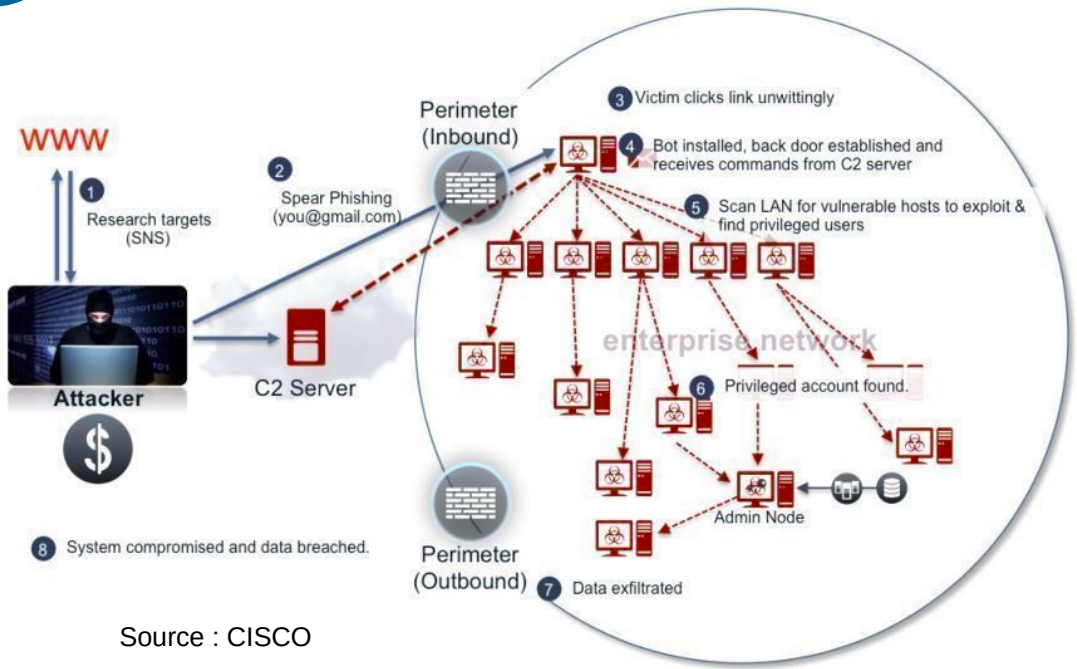
Les systèmes d'information sont de plus en plus complexes

- Multiplication des sites
- Mobilité et télétravail
- BYOD, IoT, OT
- Usage croissant des services Cloud

&

Le modèle de sécurité périmétrique traditionnel peut être aisément contourné





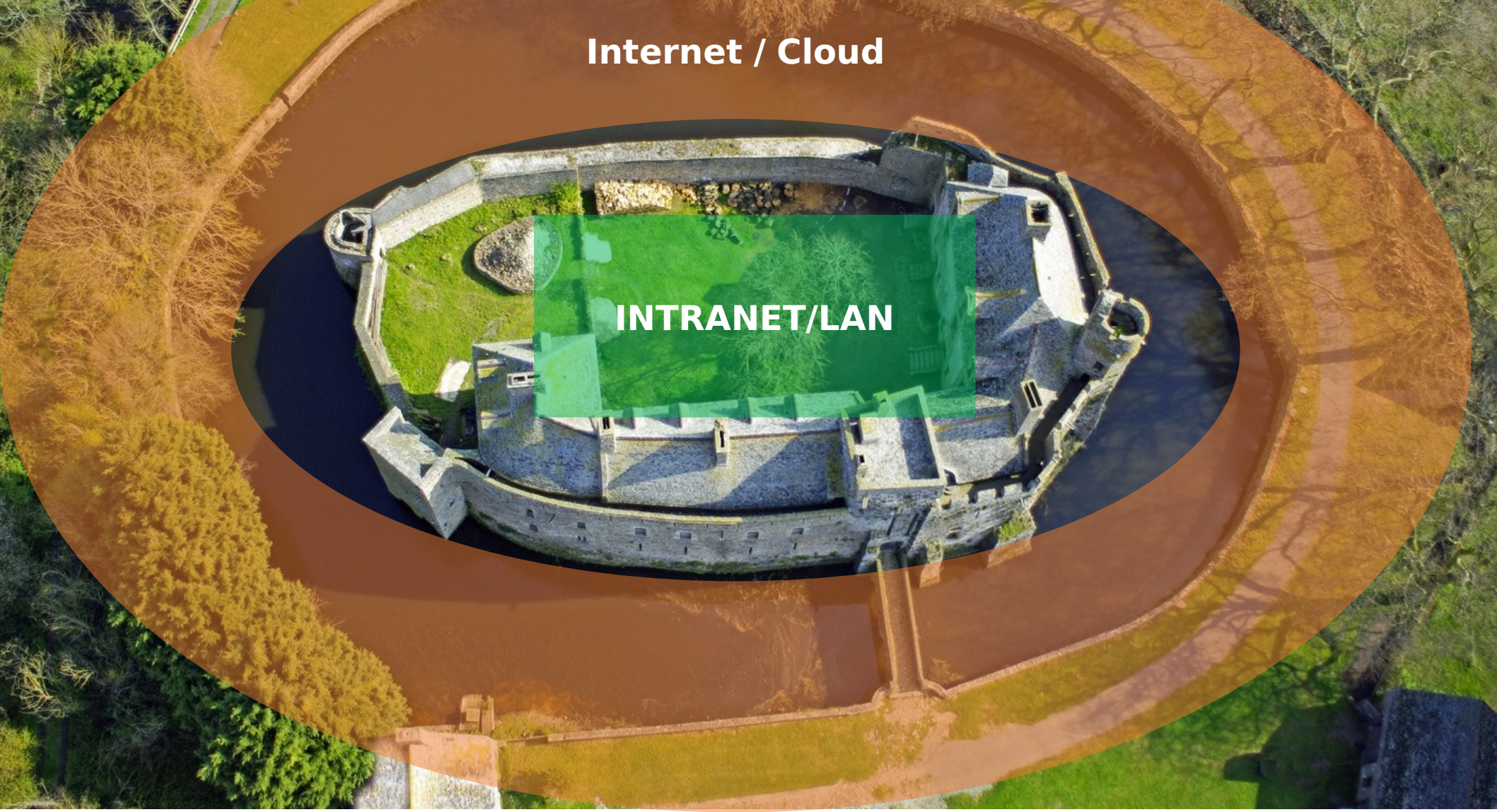
Source : CISCO

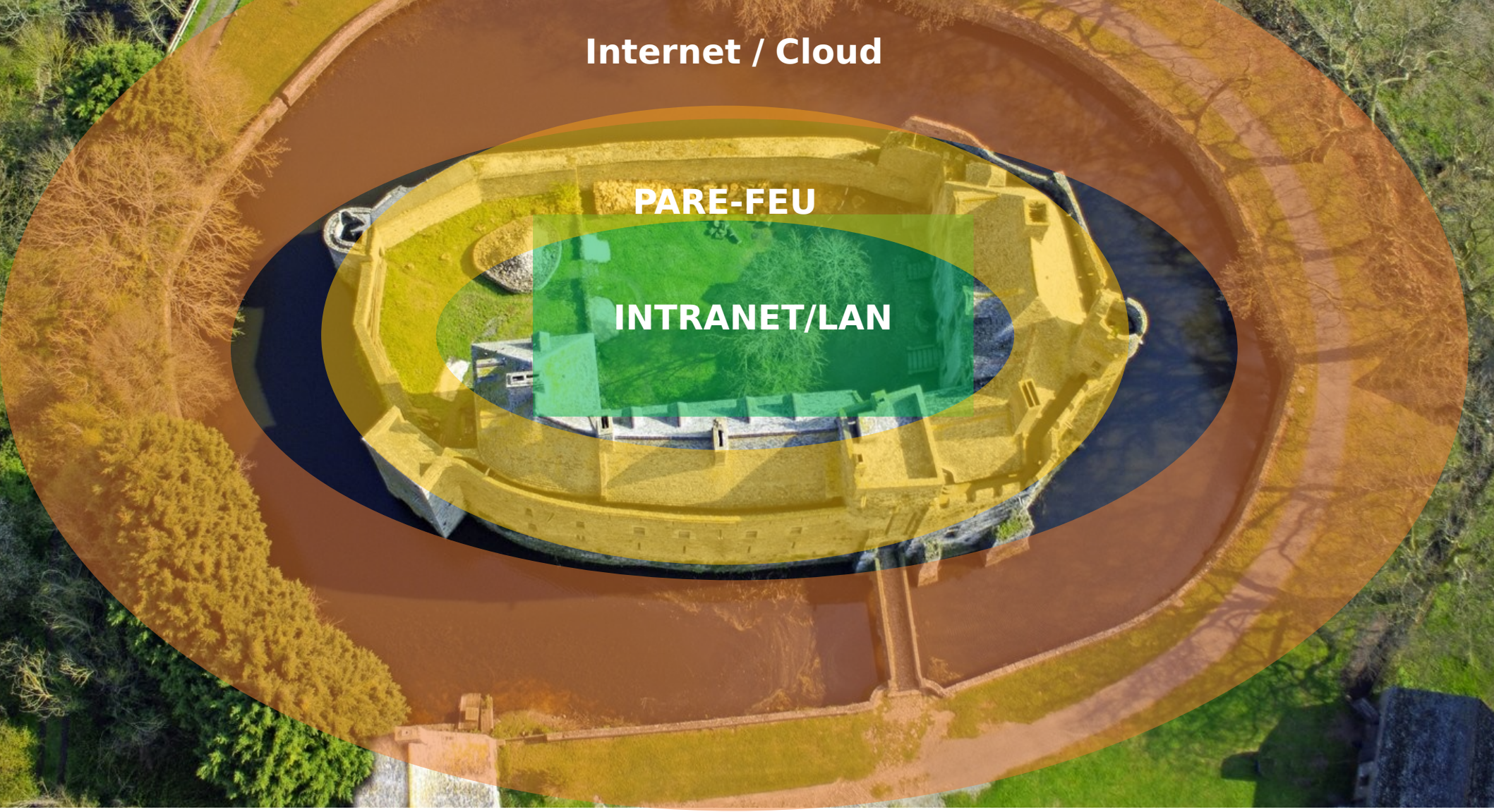
Un peu d'histoire : les prémices

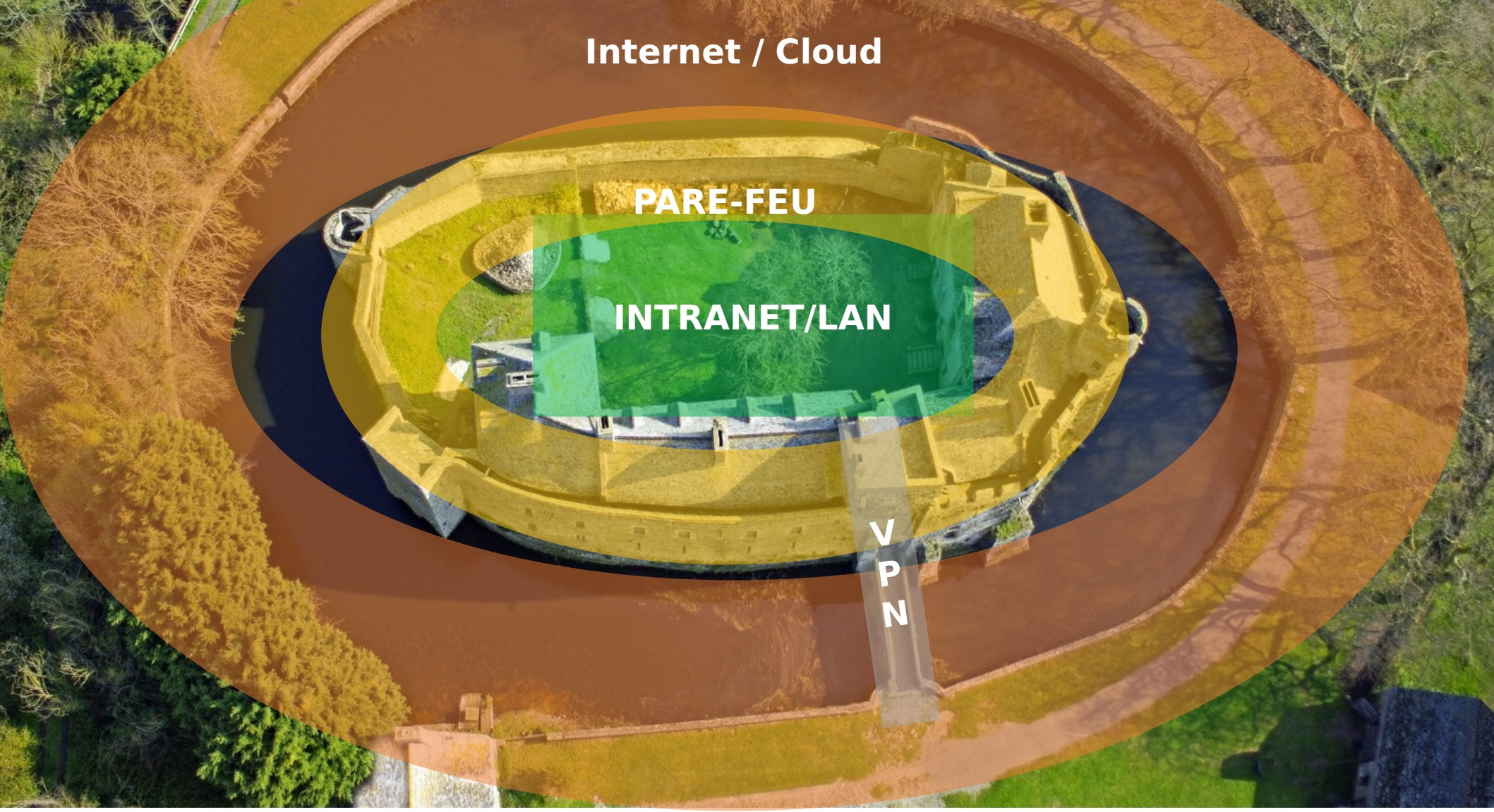
- Notion de « dépérimétrisation »
  - Forum Jericho (2004)
  - https://collaboration.opengroup.org/projects/jericho/
- Formulation « Zero Trust »
  - Cabinet d'analystes Forrester Research (2010)
  - https://www.virtualstarmedia.com/downloads/Forrester_zero_trust_DNA.pdf
- Projet « BeyondCorp »
  - Google (depuis 2009, premières publications en 2014)
  - https://www.beyondcorp.com/
- Concept « assume breach »
  - Microsoft (2014)
  - https://www.microsoft.com/en-us/download/details.aspx?id=36036

Un peu d'histoire : l'adoption du concept

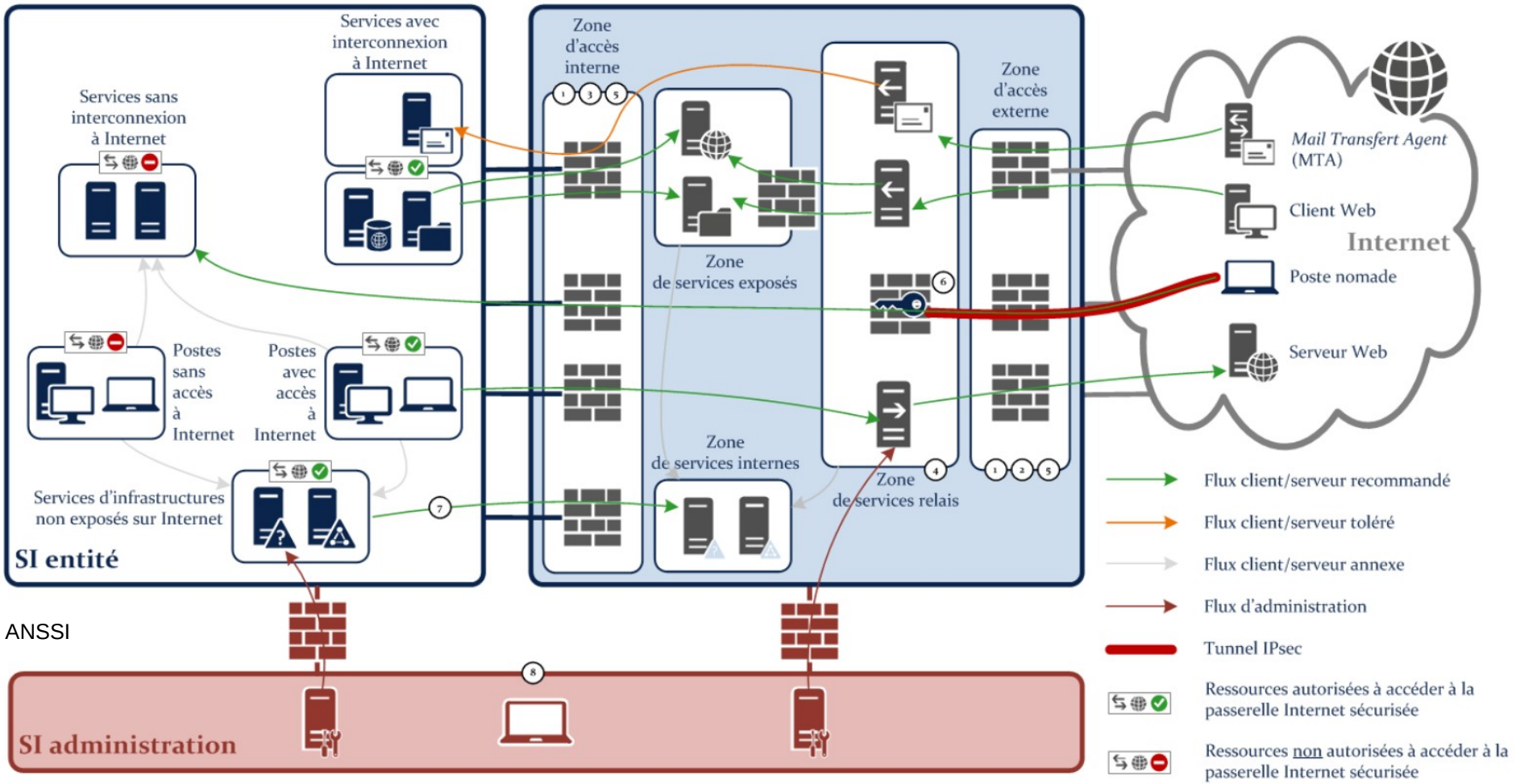
- « Zero Trust Architecture »
  - NIST : National Institute of Standards and Technology américain (2019)
  - https://csrc.nist.gov/publications/detail/sp/800-207/final
- Executive Order on Improving the Nation's Cybersecurity
  - Gouvernement américain (mai 2021)
  - https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
- Avis scientifique et technique sur le modèle Zero Trust
  - ANSSI (avril 2021)
  - https://www.ssi.gouv.fr/agence/publication/le-modele-zero-trust/
- Moving the U.S. Government Towards Zero Trust Cybersecurity Principles
  - Office of Management and Budget américain (septembre 2021)
  - https://zerotrust.cyber.gov/downloads/Office of Management and Budget - Federal Zero Trust Strategy - DRAFT For Public Comment - 2021-09-07.pdf


Internet / Cloud
INTRANET/LAN



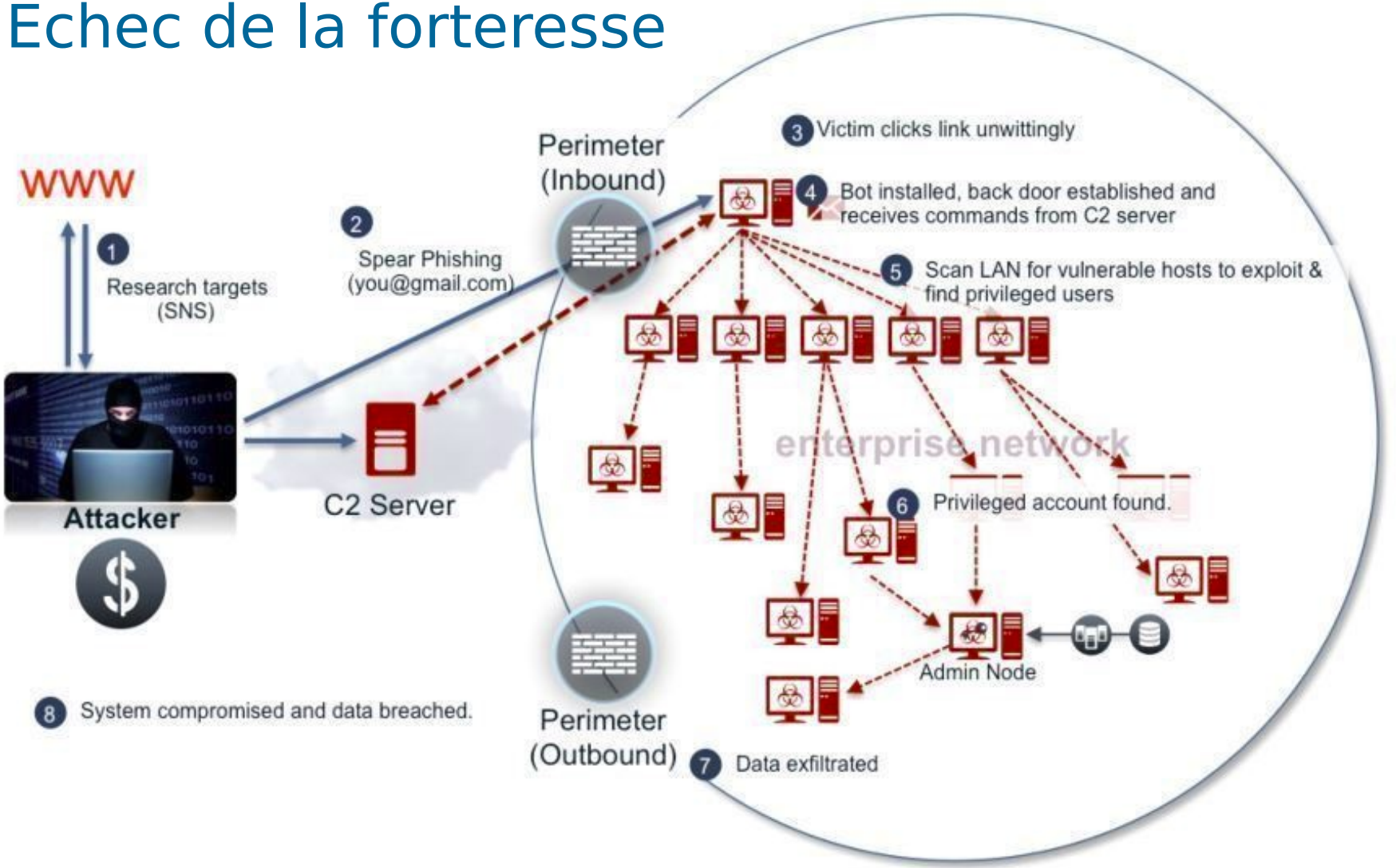

Internet / Cloud
PARE-FEU
INTRANET/LAN
VPN

Sécurité périmétrique : modèle forteresse



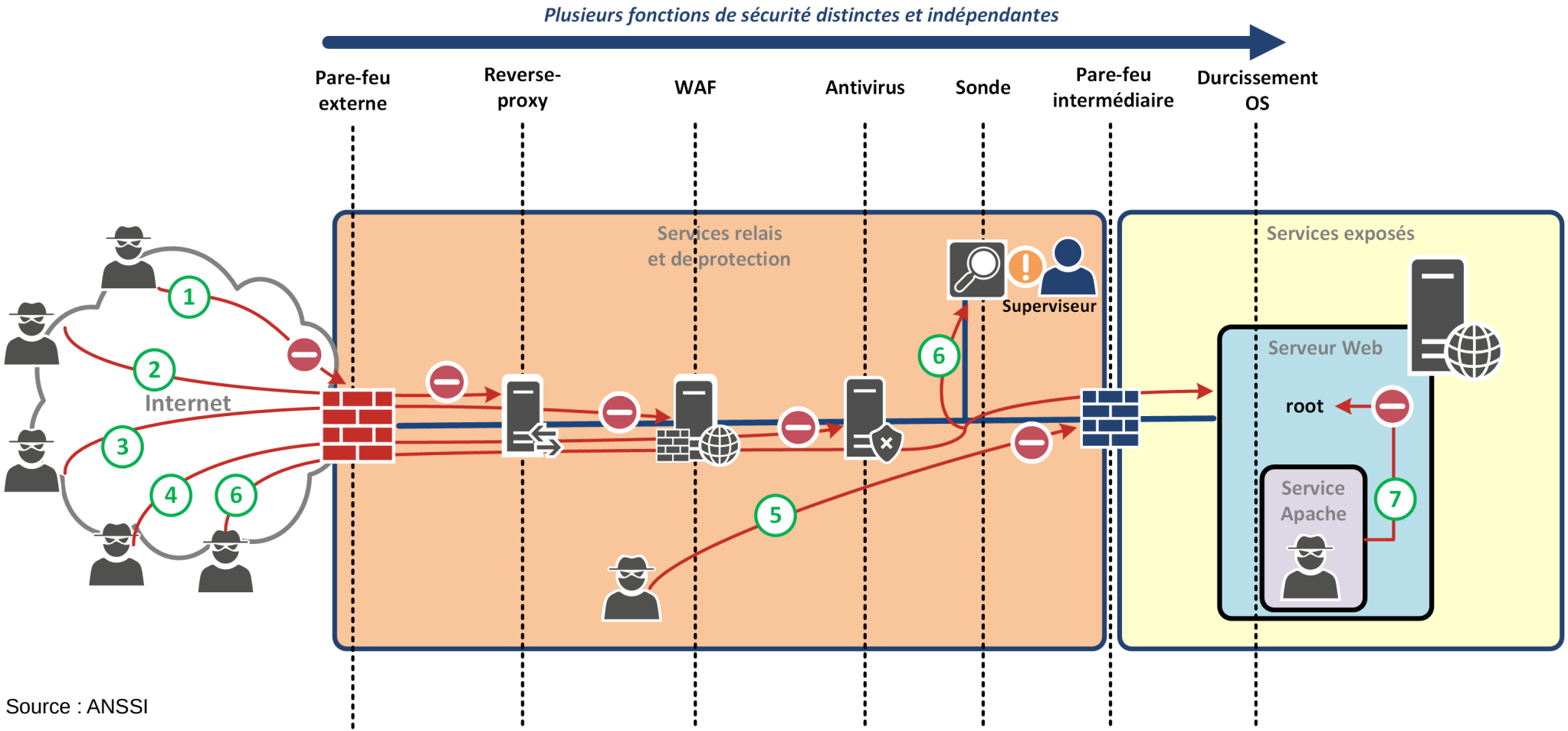
Source : ANSSI

Échec de la forteresse



Source : CISCO

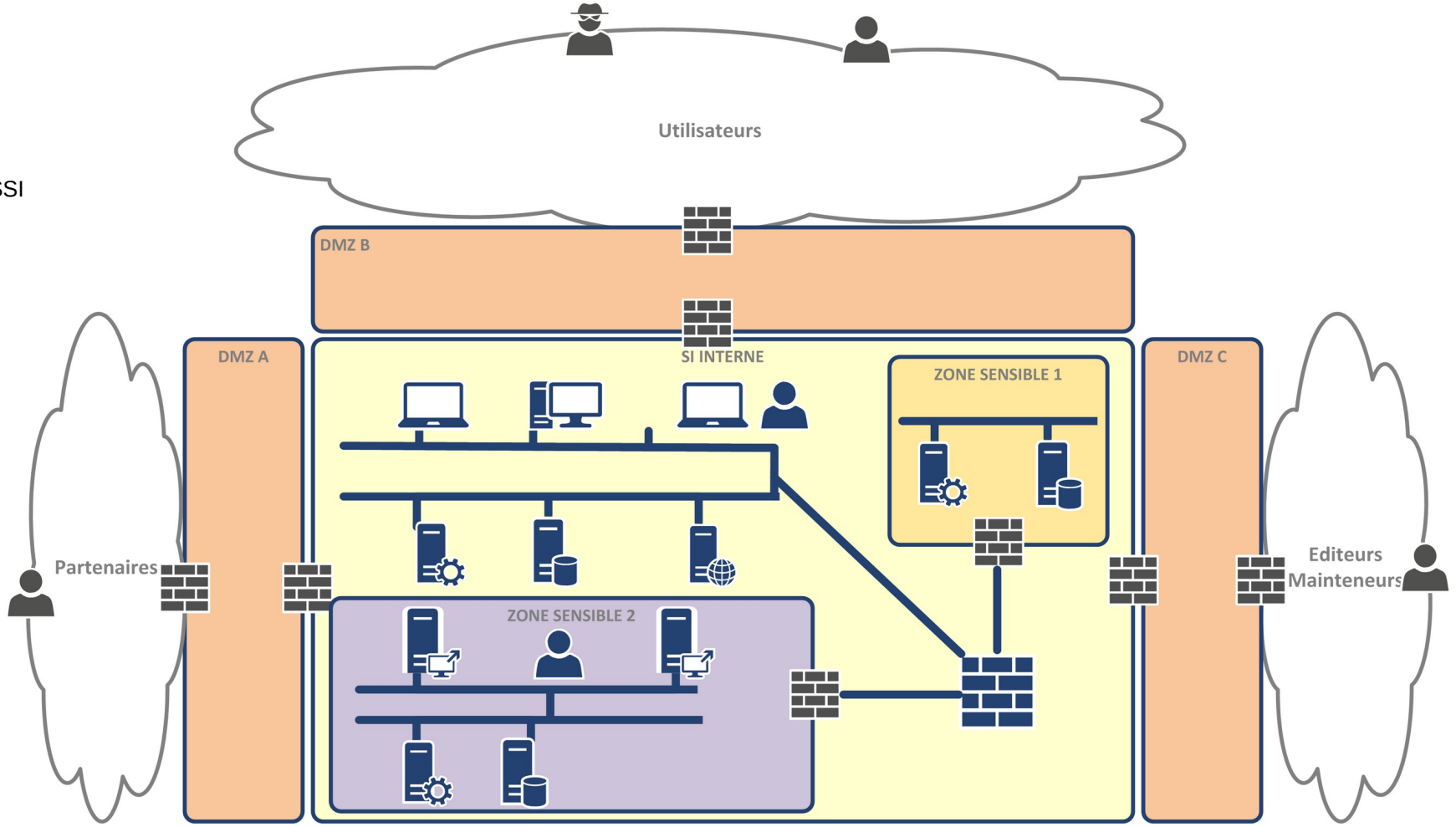
Principe de défense en profondeur



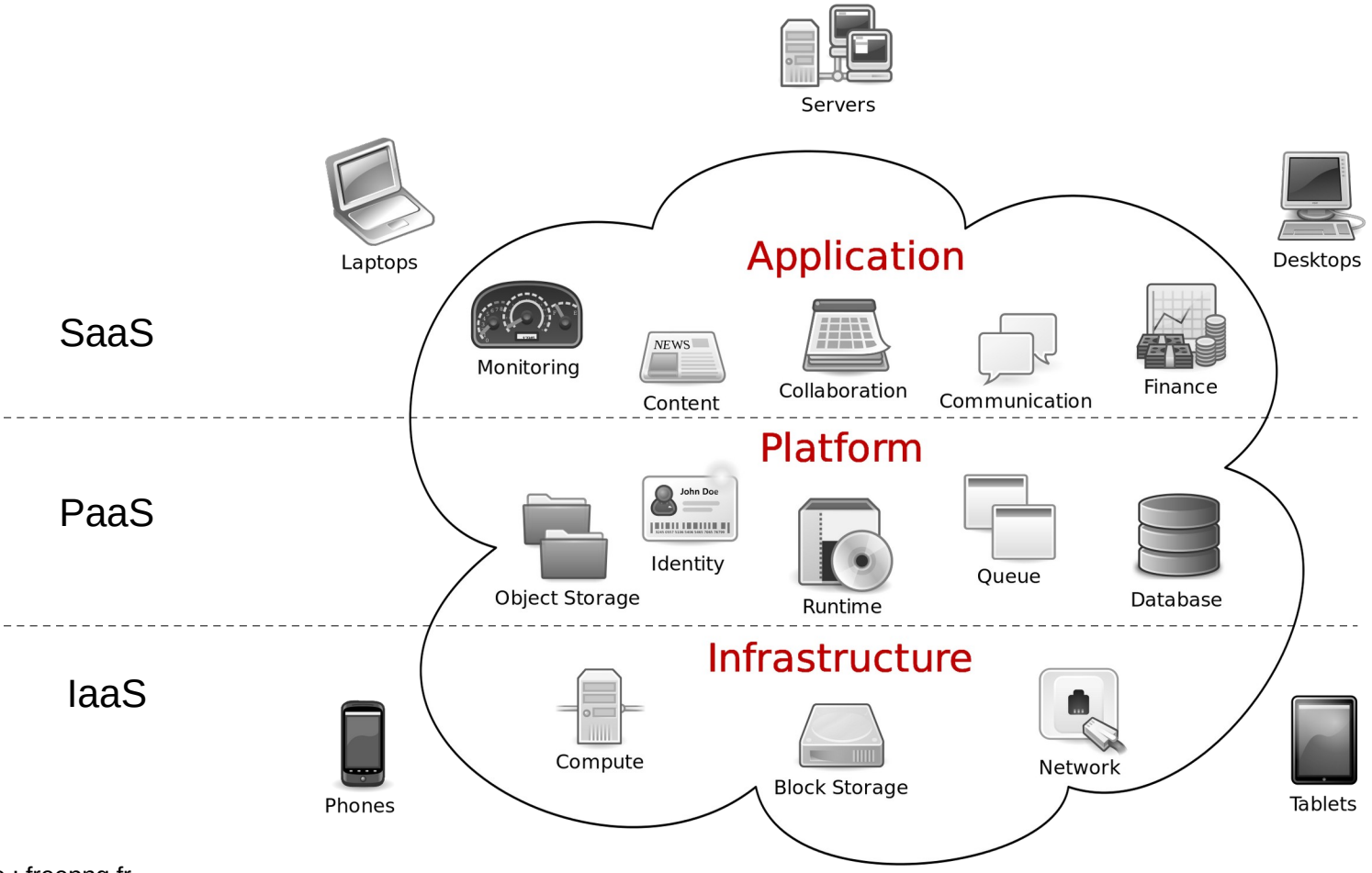
Source : ANSSI

Sécurité périmétrique : modèle aéroport

Source : ANSSI



Et le Cloud dans tout ça ?



Source : freepng.fr

Le concept de Zero Trust

- Nouveau paradigme « *never trust, always verify* »
  - Modèle de sécurité pour le Système d'Information : la confiance numérique dans l'identité d'une personne ou d'un appareil n'est jamais implicite et doit être constamment vérifiée, au plus près des ressources à protéger
- Le paysage a évolué, la protection périmétrique et « statique » pratiquée durant des décennies n'est plus pertinente (sauf exceptions)
  - Besoin de réponse aux « nouvelles » menaces cyber
  - Adoption massive du Cloud : les frontières du SI ne sont plus physiquement délimitées, on ne sait plus déterminer clairement ce qui est « dedans » ou « dehors »
  - Nouveaux usages
- On passe d'un modèle de sécurité basé sur des règles de confiance implicites comme une adresse IP ou l'identité supposée de l'utilisateur, à un contrôle d'accès dynamique qui analyse en permanence les actions réalisées, l'environnement (par exemple le type d'appareil utilisé pour se connecter et son état de santé), l'évolution des menaces, etc.

Évolution du modèle Forrester

Modèle 2010

Originellement 3 principes

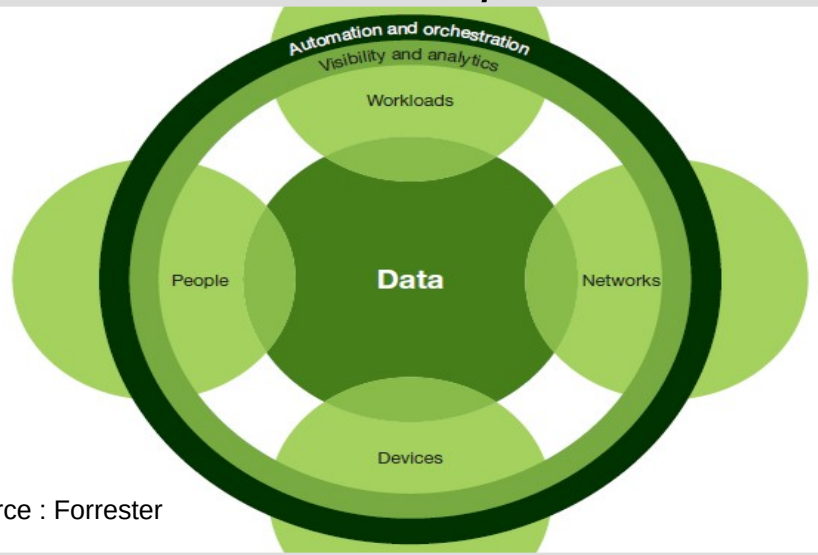
- **S'assurer que toutes les ressources sont accédées de manière sécurisée, quelle que soit la localisation de l'appelant**
- **Adopter une stratégie de moindre privilège et imposer un contrôle d'accès strict**
- **Inspecter et loguer tout le trafic**

Conçu par John Kindervag, qui a quitté Forrester pour rejoindre Palo Alto Networks, leader du NGFW, en tant que directeur technique

Conçu pour que NGFW soit le roi du Zero Trust ?

Modèle 2017

Étendu à 7 piliers



Source : Forrester

Chase Cunningham (DrZeroTrust) prend la relève et ajoute les piliers identité, « workload » et données. Il inclut l'automatisation & orchestration ainsi que la visibilité & analytique de manière transverse.

Quelques définitions

- NGFW (Next-Generation Firewalls)
  - Firewalls de Nouvelle Génération – depuis la fin des années 2000 ☺
  - Terme popularisé par Palo Alto Networks
    - En fait sur une idée pas nouvelle du tout, puisque déjà dans les années 1990 les partisans du « filtrage applicatif » de Check Point Software prétendaient atteindre le même niveau de sécurité que les solutions « lourdes » bastion / proxy applicatif
    - Quelques innovations et astuces techniques ont permis de faire la différence
- Dans le contexte du Zero Trust :
  - Le terme « *workload* » fait référence aux applications, services, traitements ou ressources informatiques qui nécessitent une protection
  - La « posture de sécurité » fait référence à l'état global de sécurité d'un système, d'un réseau ou d'une organisation par rapport à l'approche Zero Trust ; cela englobe les politiques, les pratiques et les mesures de sécurité mises en place

Le point de vue de l'ANSSI

- **Définitions**
  - « *Concept d'architecture dédié au renforcement de la sécurité d'accès aux ressources et aux services*
  - *Pas une technologie en soi / pas une solution logicielle « tout-en-un »*
  - *Modification du paradigme de la stricte logique périmétrique qui a longtemps prévalu*
  - *Remise en cause de la confiance implicite »*
- **Précautions de mise en œuvre**
  - « *Si une mise en œuvre du modèle est envisagée, elle ne peut être que progressive*
  - *Le recours à des solutions de sécurité nouvelles qui doivent s'intégrer dans un système global de défense sans s'y substituer*
  - *Le recours à de telles solutions est ardu, susceptible d'entraîner des erreurs d'installation ou de configuration, d'accroître la vulnérabilité des systèmes d'information, de donner aux entreprises un faux sentiment de sécurité »*

https://www.ssi.gouv.fr/agence/publication/le-modele-zero-trust/

CARTA : le « presque Zero Trust » de Gartner

CARTA = ***Continuous Adaptive Risk and Trust Assessment***

1. Remplacez les barrières de sécurité statiques par des plateformes de sécurité contextuelles, adaptatives et programmables
2. Découvrez, surveillez, évaluez et hiérarchisez les risques en continu, de manière proactive et réactive
3. Effectuez des évaluations des risques et de la confiance dès le commencement des projets numériques
4. Instrumentez l'infrastructure pour une visibilité globale et complète des risques, incluant la gestion des données sensibles
5. Utilisez l'analytique, l'IA, l'automatisation et l'orchestration pour réduire le temps de détection et de réponse, ainsi que pour permettre les évolutions nécessaires
6. Architecturez la sécurité en tant que système intégré, adaptatif et programmable, et pas en silos
7. Mettez en place une prise de décision continue en fonction des risques sur les données et sous la responsabilité des propriétaires de celles-ci

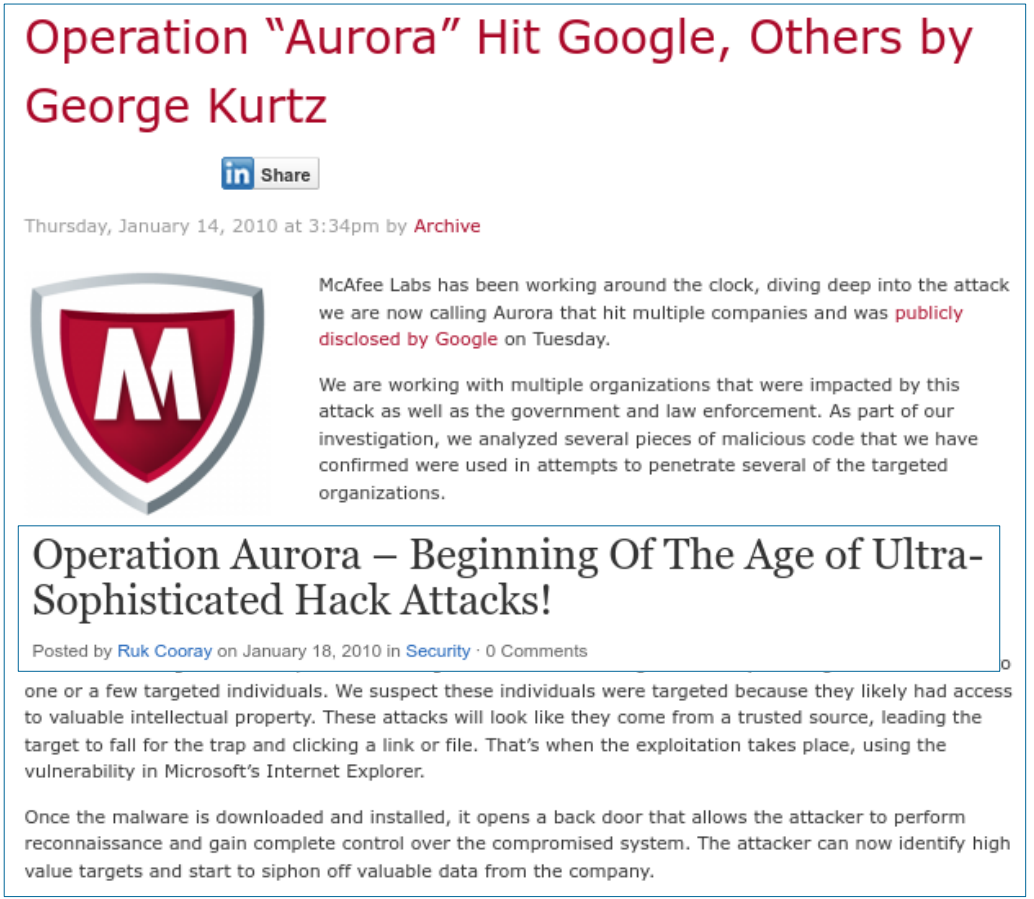
« BeyondCorp »
Le Zero Trust selon Google

Pourquoi BeyondCorp ?

2009 : premières réflexions après que Google ait été touché par un APT (opération Aurora)

2011 : la genèse de BeyondCorp

- **Contexte**
  - Une protection périmétrique prise en défaut donne à l'adversaire la possibilité de gagner des privilèges (tous ?) dans le réseau interne
  - Multiplication des usages / besoin d'augmenter la productivité
    - Utilisateurs en mobilité
    - Appareils hétérogènes
    - Usage grandissant des services Cloud
- **Objectif**
  - Tous les employés de Google peuvent travailler depuis n'importe où, sans nécessiter une connexion VPN traditionnelle vers le réseau interne privilégié



Operation "Aurora" Hit Google, Others by George Kurtz

Share

Thursday, January 14, 2010 at 3:34pm by Archive

McAfee Labs has been working around the clock, diving deep into the attack we are now calling Aurora that hit multiple companies and was publicly disclosed by Google on Tuesday.

We are working with multiple organizations that were impacted by this attack as well as the government and law enforcement. As part of our investigation, we analyzed several pieces of malicious code that we have confirmed were used in attempts to penetrate several of the targeted organizations.

Operation Aurora – Beginning Of The Age of Ultra-Sophisticated Hack Attacks!

Posted by Ruk Cooray on January 18, 2010 in Security · 0 Comments

one or a few targeted individuals. We suspect these individuals were targeted because they likely had access to valuable intellectual property. These attacks will look like they come from a trusted source, leading the target to fall for the trap and clicking a link or file. That's when the exploitation takes place, using the vulnerability in Microsoft's Internet Explorer.

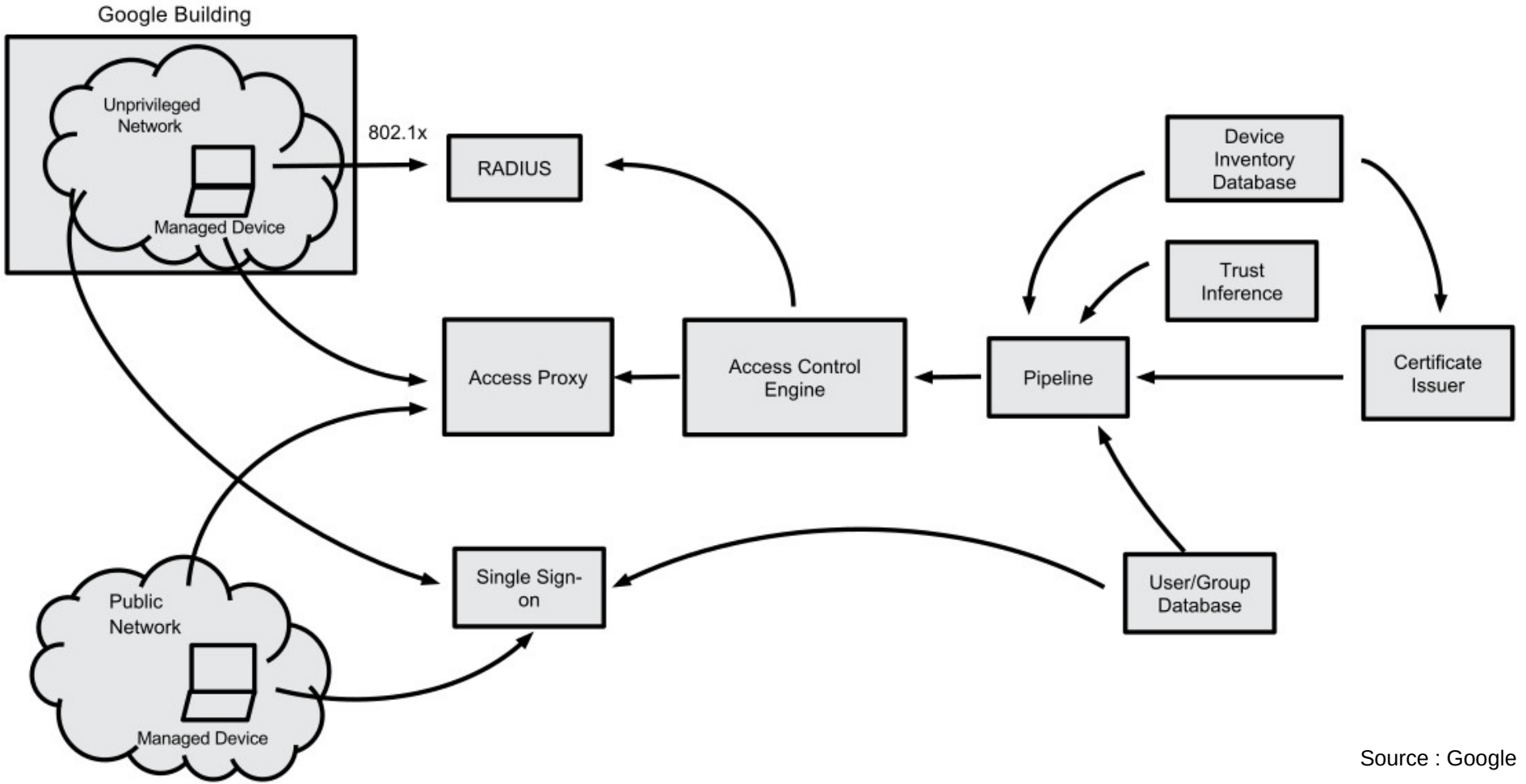
Once the malware is downloaded and installed, it opens a back door that allows the attacker to perform reconnaissance and gain complete control over the compromised system. The attacker can now identify high value targets and start to siphon off valuable data from the company.

Sources : McAfee & SPORKINGS

BeyondCorp : le Zero Trust selon Google

- Généralisation du 802.1x
- Tout encapsuler dans HTTPS
  - Accès aux ressources via *reverse proxy* obligatoirement
- Authentifier l'utilisateur **et** son poste de travail
- Authentification résistante au phishing (U2F)
- Fonctionne sur Chromebook
- Pas de solution sur étagère, Google Workplace / G-suite est ce qui s'en rapproche le plus
- Proxy Cloud incluant la gestion des identités
  - https://cloud.google.com/iap/

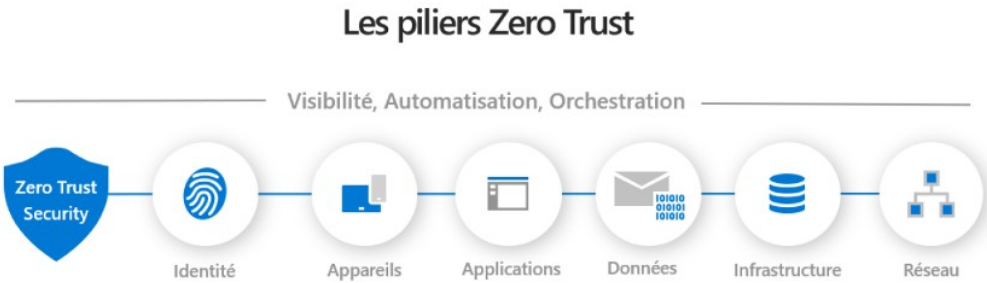
Architecture BeyondCorp



Source : Google

Le Zero Trust selon Microsoft

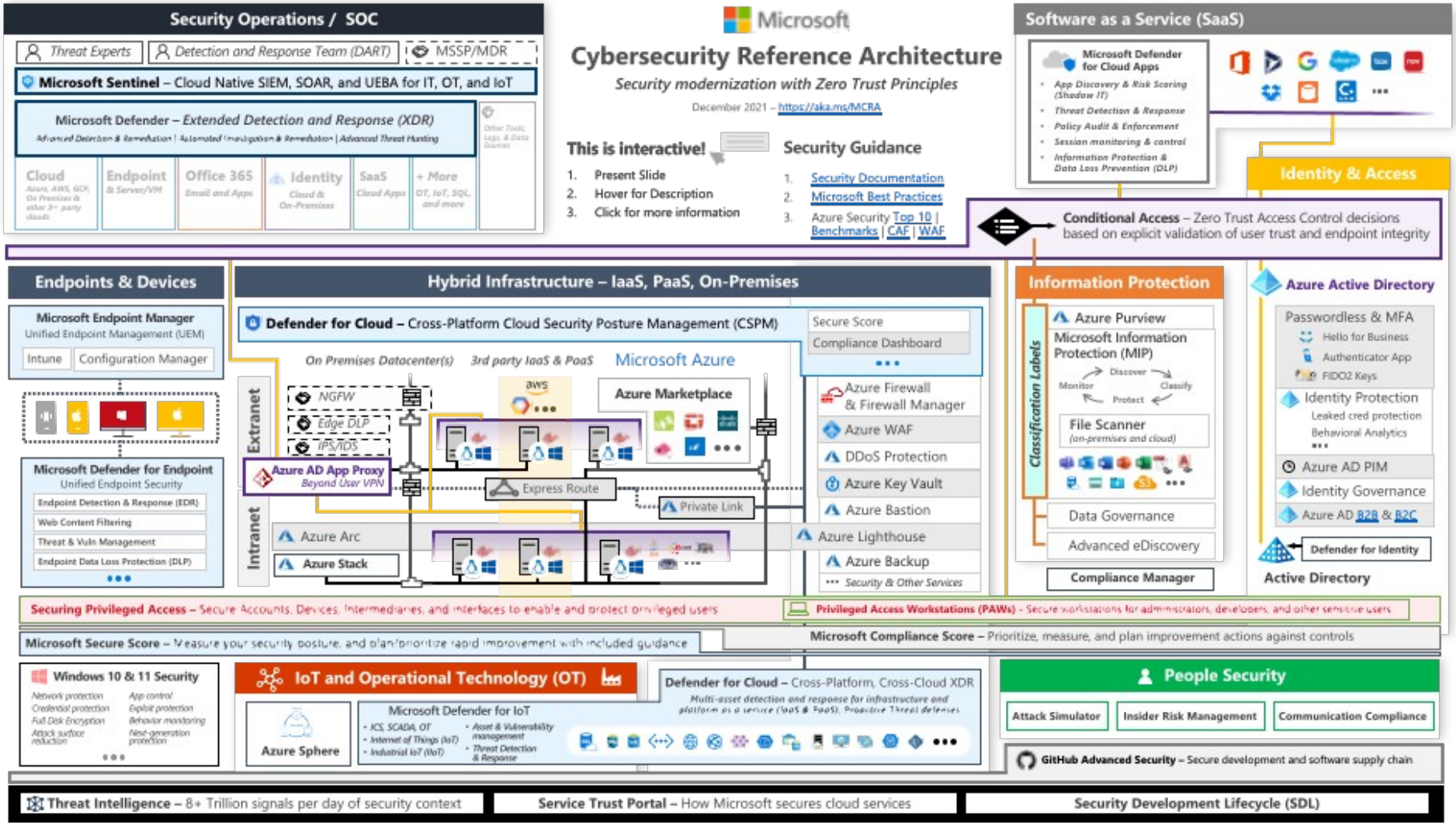
Le Zero Trust selon Microsoft



Source : Microsoft

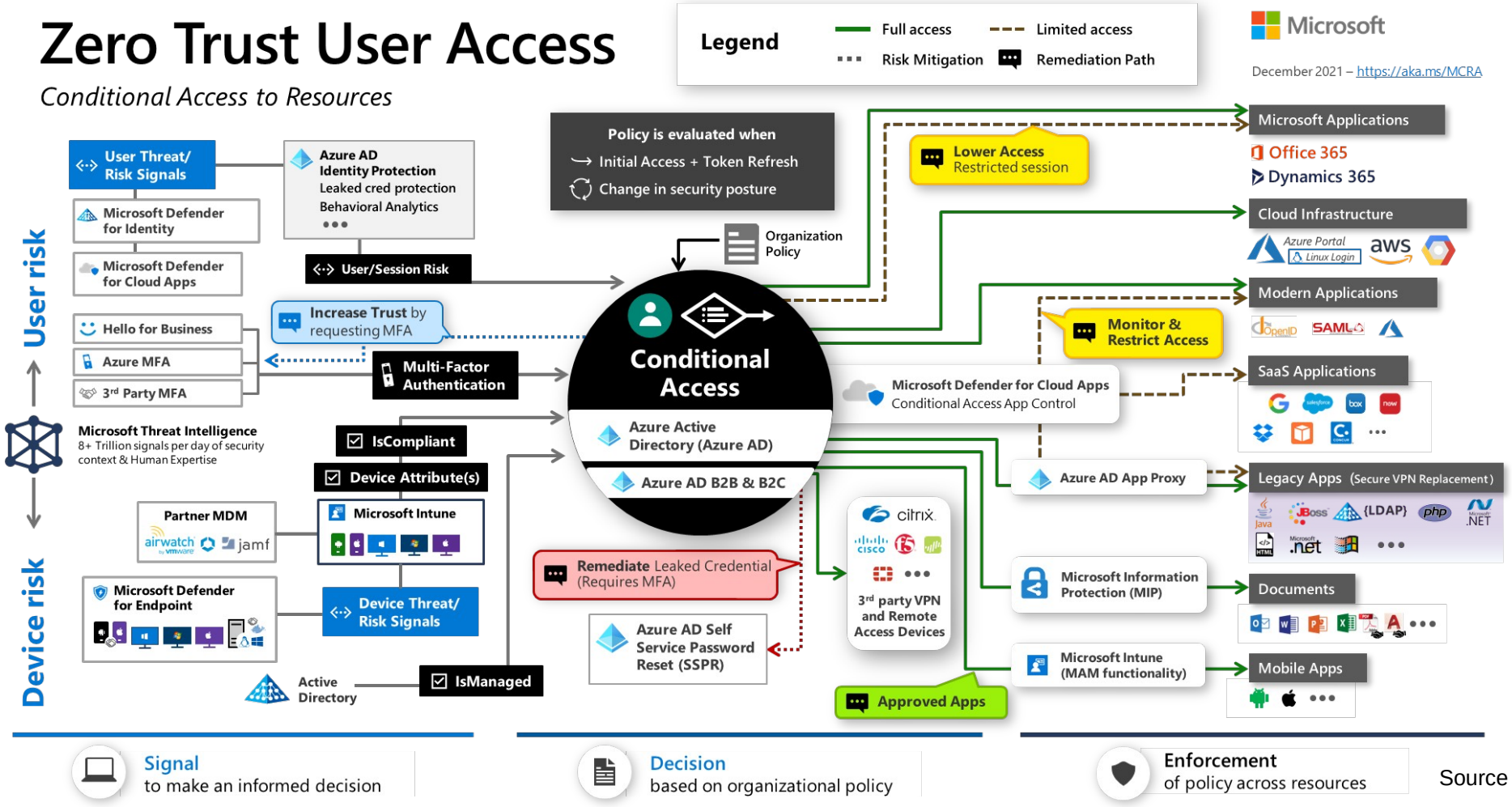
- **Vérifier explicitement** (*verify explicitly*)
  - Vérification dynamique de chaque demande d'accès à une ressource (donnée, application, etc.)
  - Décision basée sur l'identité du demandeur, l'état de son appareil, son emplacement et la ressource visée, plus tous les éléments de contexte permettant d'évaluer le risque en continu ⇒ **l'identité est le nouveau périmètre**
- **Appliquer le principe de moindre privilège** (*use least privilege access*)
  - JEA / JIT (*Just Enough Access / Just In Time*)
  - En lien avec une évaluation dynamique du risque
- **Présupposer la compromission** (*assume breach*)
  - Minimiser l'impact d'une compromission par la micro-segmentation, le chiffrement de bout-en-bout, la surveillance continue et l'automatisation de la détection / réponse aux menaces

Architecture ZT selon Microsoft



Source : Microsoft

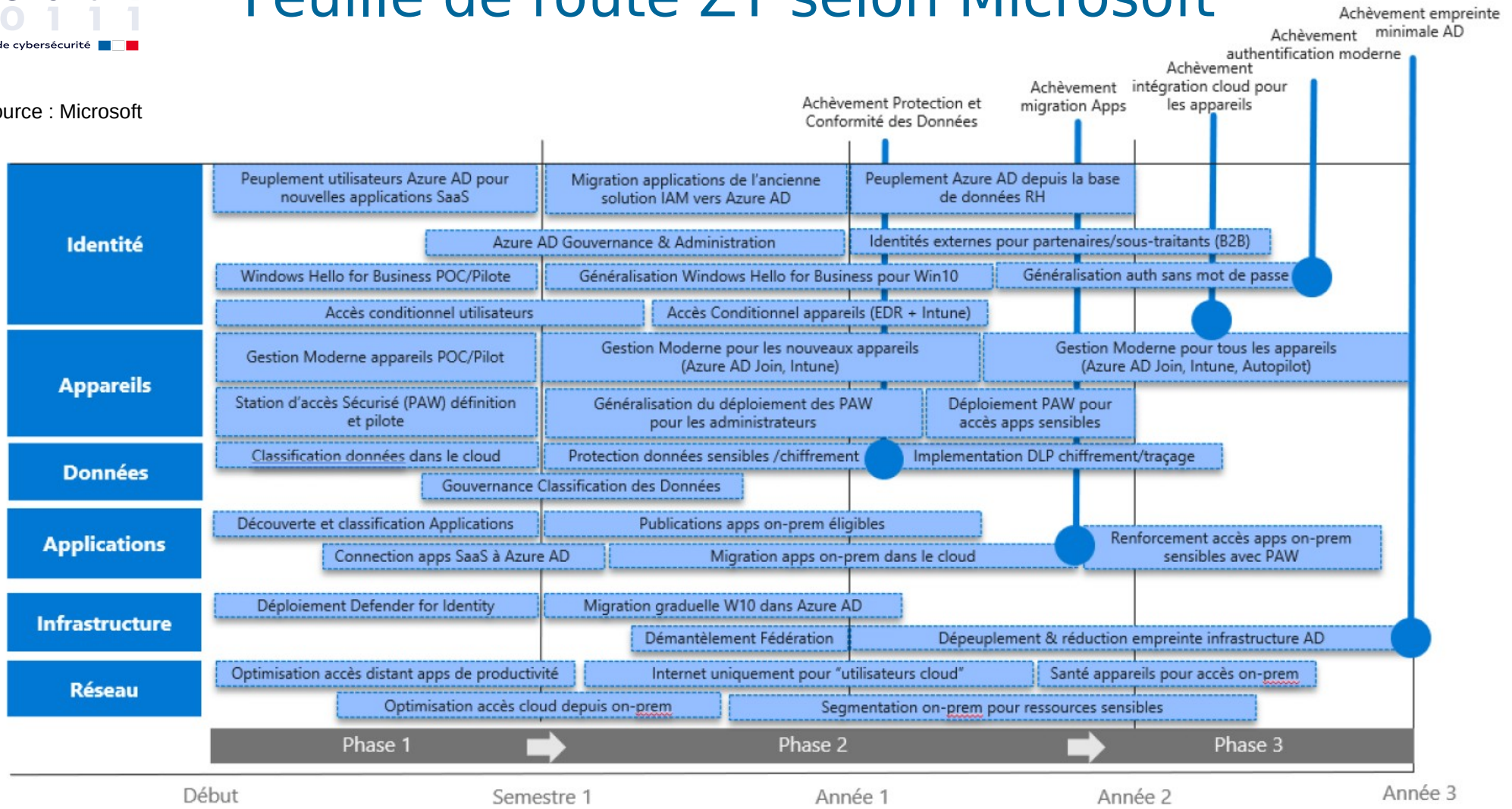
Accès utilisateur ZT selon Microsoft



Source : Microsoft

Feuille de route ZT selon Microsoft

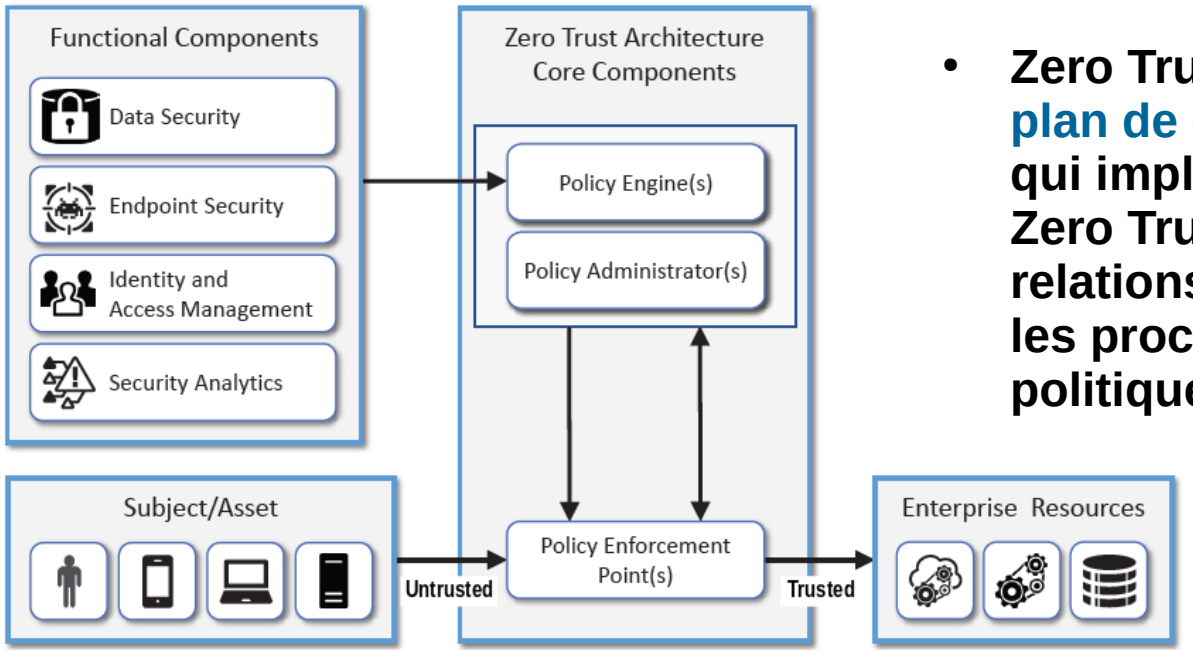
Source : Microsoft



Le Zero Trust selon le NIST

Zero Trust (Architecture) selon le NIST

- ZT et ZTA : définitions du NIST
- **Zero Trust (ZT) : ensemble de concepts et d'idées conçus pour minimiser l'incertitude par l'application de décisions d'accès unitaires, pertinentes et à moindre privilège dans les systèmes d'information et services, en considérant le réseau comme potentiellement compromis**



- **Zero Trust Architecture (ZTA) : plan de cybersécurité d'entreprise qui implémente les concepts du Zero Trust en englobant les relations entre les ressources du SI, les processus opérationnels et les politiques d'accès**

Source : NIST

Principes Zero Trust du NIST

- Toutes les sources de données et les traitements informatiques sont considérés comme des ressources
- Toutes les communications sont sécurisées sans tenir compte de l'emplacement réseau
- Chaque accès à une ressource est accordé séparément sur la base de sessions unitaires
- Les accès aux ressources sont déterminés par des politiques dynamiques – incluant l'état observable de l'identité de la source, de l'application/service accédé et de l'appareil qui effectue la requête – et pouvant inclure d'autres attributs comportementaux ou environnementaux
- L'entreprise surveille et mesure l'intégrité et la « posture de sécurité » de tous les appareils impliqués
- Toutes les authentifications et autorisations sont dynamiques et strictement contrôlées avant qu'un accès à une ressource ne soit accordé
- L'entreprise collecte autant d'informations que possible sur l'état de santé des appareils, réseau, infrastructure et communications et les utilise pour améliorer sa posture de sécurité

Variantes de l'approche ZT

- Identités
- Micro-segmentation
- Cloisonnement réseau

Une implémentation ZT complète inclut des éléments de ces 3 variantes

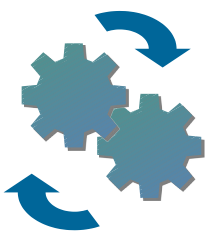
En résumé (tentative), selon le NIST

- Le Zero Trust assume que :
  - Le réseau interne de l'entreprise ne doit pas être considéré comme une zone de confiance implicite
  - Certains appareils du réseau peuvent ne pas appartenir à l'entreprise ou être non configurables par celle-ci
  - Aucune ressource n'est intrinsèquement fiable

Principe 1

Moindre privilège des accès (juste le temps nécessaire, seulement ce qui est nécessaire)

Et pas « ouvert / fermé »

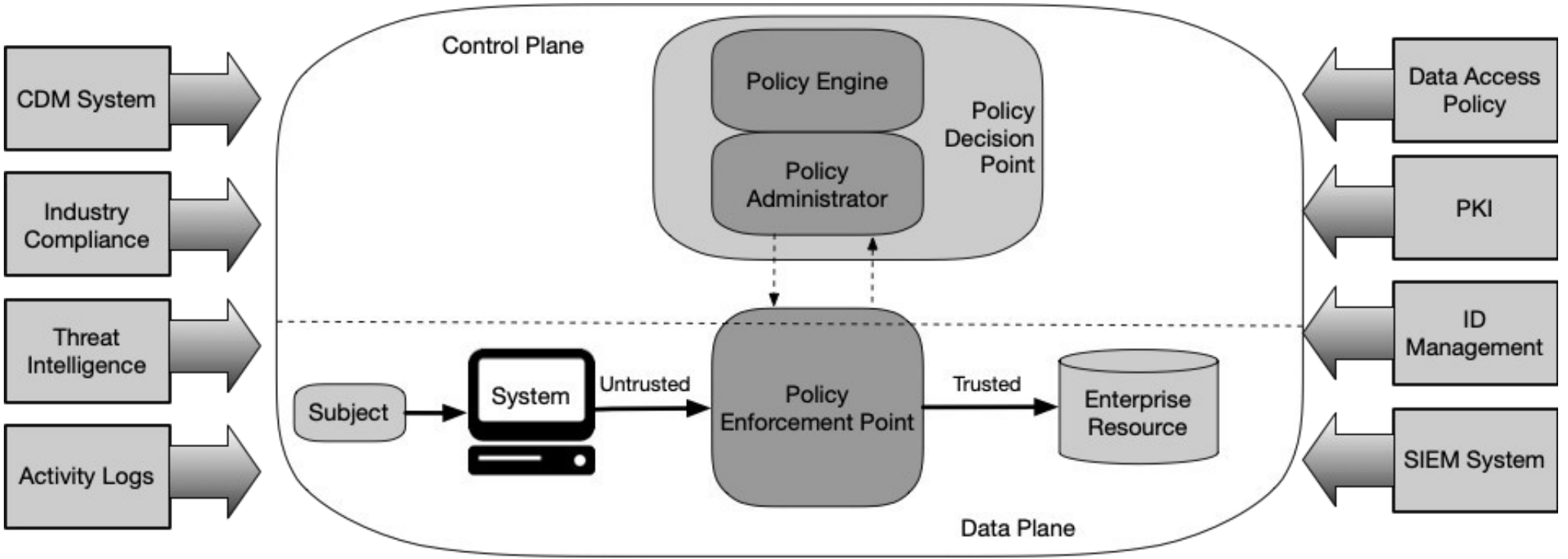


Principe 2

Évaluation continue du risque & contrôle d'accès adaptatif avec autorisations dynamiques exploitant des attributs multiples, incluant l'identité et la posture de sécurité

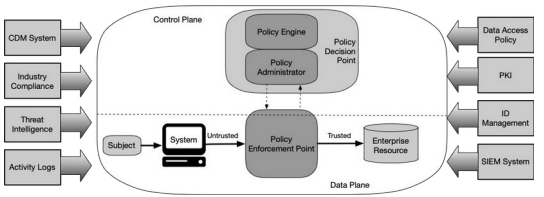
Pas d'autorisation permanente

Modèle d'architecture Zero Trust du NIST



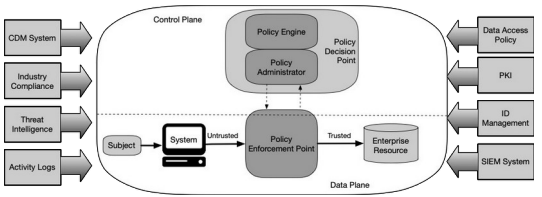
Source : NIST

Scénario d'accès générique



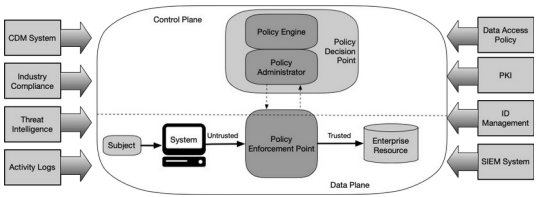
- Une **identité** (*subject*) accède à une **ressource** (*resource*) depuis un **appareil** (*system*)
- La demande arrive sur un **composant d'accès conditionnel** (*PEP*) chargé d'appliquer les **politiques de sécurité** (ex. *data access policy*)
- Ce composant s'appuie sur une **autorité centrale de décision** (*PDP*) qui évalue le **niveau de risque** (ou score de confiance) pour l'identité et l'appareil associé à cette demande d'accès
  - Son moteur (*policy engine*) tient compte des informations sur l'identité (groupes/rôles, localisation, privilèges), l'appareil (système d'exploitation, géré par l'entreprise ou non, état de santé, à jour de correctifs de sécurité…) et plus globalement sur le contexte d'accès
    - L'utilisateur a-t-il l'habitude de se connecter depuis cet emplacement ou ce pays ?
      Le même utilisateur s'est-il authentifié récemment depuis un autre endroit éloigné qui indiquerait un voyage impossible ?
      L'appareil depuis lequel l'utilisateur se connecte est-il son poste habituel ?

Scénario d'accès générique



- En y ajoutant des informations sur les menaces et en considérant la ressource ciblée, le couple PEP/PDP applique les politiques de sécurité qui lui permettent de prendre la décision d'autoriser l'accès ou de le refuser
  - L'accès peut être autorisé sous condition, par exemple sous réserve d'une authentification multi-facteurs
  - Un accès réduit à l'application ou aux données, par exemple uniquement en lecture, peut être également imposé dans certaines circonstances
- L'**évaluation en temps réel des politiques de sécurité** nécessite de mettre en place une supervision transverse pour capter les évènements en provenance des diverses sources et être capable de les traiter de manière efficace afin de détecter (par exemple) les signaux faibles indicateurs d'un début d'attaque en cours

Scénario d'accès générique



- Le dispositif de **diagnostic et remédiation en continu** (*CDM*) :
  - Collecte les événements en provenance de sources de données liées à l'identité (annuaires, SSO...), aux appareils (logs de sécurité, client EDR...), au réseau (pare-feu, trafic réseau…), aux applications, etc.
  - Les événements sont analysés en continu en vue de détecter le plus rapidement possible les prémices d'une attaque
  - L'objectif est de pouvoir réagir au plus vite pour éviter la propagation de la compromission, en isolant les éléments compromis puis en effectuant les actions de remédiation nécessaires
  - On trouve cette notion de surveillance et alerte en mode continu dans les fonctions principales de certaines solutions Cloud Security Posture Management (CSPM), dont l'utilisation est préconisée dans le cadre d'une implémentation Zero Trust dans le Cloud

Scénario d'accès : exemple

- Utilisateur appartenant au service achats souhaitant se connecter sur l'application financière depuis son poste de travail géré par l'entreprise
  - L'utilisateur s'est authentifié multi-facteurs
  - C'est bien un utilisateur du groupe achats avec des autorisations pour accéder à l'application visée
  - Il se connecte depuis un appareil référencé, géré par l'entreprise et conforme
  - RàS au niveau de l'information sur les menaces, ex. rien n'indique que l'identité de l'utilisateur a été compromise

    ⇒ Jeton d'accès accordé, avec les privilèges strictement nécessaires pour le temps de la session (limité, surtout en cas d'inactivité)
- Le même utilisateur se connecte depuis un appareil non géré par l'entreprise

  ⇒ Jeton d'accès accordé avec des privilèges réduits, ex. lecture seule ou impossibilité de valider un achat

Différence entre Zero Trust, ZTNA et SASE

- Zero Trust définit des principes et prône une approche plus globale en termes de piliers (modèle NIST/CISA) avec comme point de départ l'identité
- ZTNA (*Zero Trust Network Access*) est une implémentation du contrôle d'accès par coupure des flux réseau dans une vision sécurité grâce à des analyses réalisées au niveau réseau, ce qui semble moins adapté aux applications et services Cloud
- SASE (Secure Access Service Edge) pousse encore plus loin l'approche en intégrant ZTNA et les technologies SD-WAN, dans une volonté d'inclure le réseau d'entreprise dans le Cloud en conservant une vision de sécurité périmétrique

« Un réseau étendu défini par logiciel ou Software-Defined Wide Area Network (SD-WAN) est une architecture WAN virtuelle, dans laquelle n'importe quel mélange de types de transport de réseau – non seulement la commutation multi protocole par étiquette (MPLS), mais aussi l'Internet à large bande, la téléphonie cellulaire et le satellite – peuvent être virtualisés et liés, puis gérés de manière centralisée par logiciel, afin de connecter en toute sécurité les utilisateurs aux applications et aux postes de travail conformément à la politique »
Source : Citrix