HEXATRUST

CLOUD CONFIDENCE & CYBERSECURITY

Zero Trust

Du concept à la pratique

EDITION
2025

L'association en quelques mots...

Hexatrust regroupe et fédère les champions français et européens de la cybersécurité, du cloud de confiance et du digital workplace.

L'association rassemble des startups, PME et ETI à la pointe de l'innovation : éditeurs de solutions de cybersécurité, fournisseurs de cloud de confiance (SaaS, PaaS, IaaS), intégrateurs, hébergeurs, avocats, courtiers en assurance, établissements de financement et acteurs publics.

Ce collectif incarne l'excellence technologique européenne, avec un portfolio de solutions de confiance assurant protection, transparence et efficacité. Présents à l'international, les membres d'Hexatrust déploient leurs technologies innovantes et expertises de pointe à travers le monde.

L'UNION FAIT LA FORCE

Défendre

Accompagner les évolutions réglementaires et défendre les intérêts de nos adhérents

Représenter

Porte-parole de nos membres au sein des instances représentatives de la filière et animateur d'un écosystème tourné vers le développement entrepreneurial

Promouvoir

Valoriser la filière en France et à l'international et faire connaître au plus grand nombre les enjeux de la cybersécurité et du cloud de confiance

Unis pour construire ensemble une filière engagée pour un monde numérique plus sûr, résilient et protecteur des données.

SOMMAIRE

Le mot du Président

Jean-Noël DE GALZAIN
Président Hexatrust
Founder & CEO WALLIX Group

On dit que « la liberté des uns s'arrête où commence celle des autres ». Comment préserver cette philosophie dans un univers numérique où l'interconnexion modifie les frontières du monde réel, en véhiculant de nouveaux risques pour les entreprises et les organisations : les risques numériques. La confiance n'exclut pas le contrôle. L'approche et la philosophie Zero Trust correspondent ainsi à l'idée que la confiance se construit en réservant à chacun l'accès numérique qui lui correspond, avec les prérogatives qui sont les siennes. C'est une approche qui correspond à la réalité des défis liés à la transformation numérique de notre société.

Gestion dynamique des identités et des accès numériques, sécurité des terminaux et des utilisateurs, protection des données et des applications, sécurité du réseau et de l'infrastructure, sécurité hybride et dans le cloud, intelligence artificielle de confiance, la mise en œuvre d'une stratégie Zero Trust dans une organisation nécessite ainsi une approche holistique de la cybersécurité. Au delà des aspects techniques, la gouvernance est clé, avec une démarche transverse tant au niveau des projets applicatifs, des métiers, et bien sûr de la direction informatique. Les parties prenantes doivent agir en étant alignées autour d'une feuille de route progressive, partagée et comprise de tous.

Dans un contexte où la confiance et la souveraineté sont intimement liées, il est bon de savoir qu'il existe une gamme complète de solutions technologiques et d'acteurs en France et en Europe, ayant une approche souveraine de la cybersécurité et de la gestion des données. Encore fallait-il les réunir, ce qu'a fait Hexatrust avec ce Livre Blanc « Zero Trust, du concept à la pratique ».

Avec les évolutions européennes autour de la résilience (Directive NIS2, DORA), sur la protection des données (RGPD, EUCS) et la sécurité de l'utilisateur (Cyber Resilience Act), la notion de responsabilité est élargie au delà de la direction informatique, à la direction générale des organisations et des entreprises. Elle est également élargie aux sous-traitants et aux fournisseurs intimement liés à leurs clients stratégiques. **Étendre la confiance au cœur des systèmes d'information est vital : l'union fait la force. Ceci justifie pleinement l'ambition d'Hexatrust d'incarner une réponse aussi souveraine qu'innovante sur les grands défis numériques d'aujourd'hui et demain.**

Edito

Thierry LEBLOND
Pilote GT Zero Trust Hexatrust
CEO & Cofondateur PARSEC

Zero Trust : simple tendance marketing ou réelle révolution en cybersécurité ?
Le paradigme Zero Trust n'est ni une tendance marketing, ni un produit commercial. Ce concept est ancien. Je citerai notamment le principe du « moindre privilège ». Ce principe de Zero Trust doit être compris et mis en œuvre comme une stratégie de protection des ressources informatiques.

Est-ce une approche coûteuse et complexe ou une solution à la portée de tous ?
La mise en œuvre se fait par étape, projet par projet. Il y a autant de façon de le mettre en œuvre que d'organisations. Au début, il faut opter pour une approche progressive et modeste et comme toujours en informatique, il n'y a pas de « Grand Soir ». Les outils existent et il faut faire les bons choix selon sa propre analyse de risque. Comme toujours en informatique, le chantier le plus important, c'est d'accompagner le changement des usages.

S'il ne fallait retenir qu'un seul principe du Zero Trust, lequel serait-il ?
Le principe de base tient en une phase : « Ne jamais faire confiance et toujours vérifier ». Ce principe doit s'appliquer partout au niveau des cinq piliers techniques décrits dans cette brochure. On peut protéger les data en intégrité et confidentialité par du chiffrement de bout-en-bout (E2EE) ou du pare-feu applicatif (WAF), sécuriser les terminaux de confiance par une solution d'EDR, sécuriser les accès par une authentification MFA en continu et protéger les flux réseaux par une solution de NDR. Un cloud certifié SecNumCloud complétera l'approche souveraine.

Quels bénéfices concrets peut apporter le Zero Trust dans les organisations ?
En médecine, le « silence des organes », est la santé. En SSI, la sérénité, la sûreté de fonctionnement, la sécurité et la résilience d'un système d'information sont des bénéfices qui n'apparaissent en creux, que quand ils font défaut. Une organisation, qui bâtit son système en intégrant le fait que l'ennemi est déjà à l'intérieur, est plus résiliente. Quand l'attaque est déclenchée, elle ne fera tomber qu'une petite sous-partie du système, dont la remédiation sera instantanée.

Edito

Guillaume POUPARD
Adhérent Hexatrust
Directeur général adjoint Docaposte

Bien qu'ouvrant la voie à de nouvelles évolutions et innovations, les technologies en plein essor telles que l'intelligence artificielle élargissent, en contrepartie, à la fois la surface d'attaque face aux cybermenaces et leur efficacité.

Dans un contexte d'attaques de plus en plus sophistiquées, ciblées et variées, l'approche Zero Trust gagne en popularité et est souvent mise en avant. En toile de fond, le sujet de la cybersécurité au global devient crucial pour toutes les organisations, publiques comme privées, ce dont on peut réellement se féliciter. Cette nouvelle approche repose sur une vision des SI fondée sur un postulat : on ne peut pas accorder sa confiance par défaut et se cacher derrière une protection « périmétrique » qui a longtemps dominé ; il faut aujourd'hui toujours tout vérifier, en interne comme en externe.

Dans un contexte où les entreprises et organisations publiques travaillent de plus en plus avec une infrastructure cloud hybride, associant systèmes « legacy » internes, clouds privés et clouds publics, et où les usages numériques personnels et professionnels tendent à s'imbriquer fortement du fait du télétravail notamment, l'approche Zero Trust entend favoriser la sécurisation globale des entités privées et publiques.

En somme, le Zero Trust remet en cause la confiance implicite accordée dans le cadre du modèle traditionnel de défense périmétrique et se veut un aboutissement de la logique de « défense en profondeur » que l'ANSSI, entre autres, promeut de longue date. Autre conséquence positive : le Zero Trust, s'il est bien mis en œuvre, peut faire sens dans le contexte réglementaire qui continue à se développer. Corollaire de la directive NIS2, le projet de loi Résilience, pour commencer, va mettre au diapason les entités assujetties (et tous leurs partenaires) afin d'assurer un niveau élevé et commun de cybersécurité dans l'ensemble de l'UE. La mise en œuvre ambitieuse d'une cybersécurité au juste niveau face aux agressions qui vont malheureusement continuer à rapidement se développer est essentielle, que ce soit chez les grands acteurs soumis aux diverses réglementations ou chez les plus petits.

Le Zero Trust, comme d'autres concepts modernes d'architecture sécurisée, doit y contribuer en s'appuyant notamment sur le savoir-faire réel des acteurs français réunis au sein d'Hexatrust !

Partie I

Comprendre le Zero Trust


LE PRINCIPE DU ZEROTRUST, C'EST DE PARTIR DU PRÉSUPPOSÉ QUE L'ENNEMI EST DÉJÀ DANS NOTRE S.I.
ALLONS, ALLONS, NE SOYONS PAS PARANOÏAQUES.
HACK
FiX

Zero Trust : vers une sécurité sans compromis.

La sécurité sans faille est une quête mythique impossible : cela n'existe pas.

> *Le Zero Trust est devenu le préalable nécessaire pour (r)établir la confiance pour tous.*
>
> *Il n'y a pas de confiance sans cybersécurité ; la cybersécurité repose parfois sur l'absence d'une confiance accordée a priori. Dans un monde de plus en plus hyper-connecté, « distribué », transactionnel, qui exige une cybersécurité collective et collaborative, le Zero Trust apparaît aujourd'hui comme une réponse aux enjeux démultipliés de cybersécurité. En rendant la confiance explicite, le Zero Trust contribue à la cyberrésilience d'un système de plus en plus complexe et intriqué. Les technologies de gestion des identités, de contrôle d'accès, de détection, de réaction, d'orchestration, de micro-segmentation, d'invisibilité, etc., promettent ainsi une sécurité multicouche et granulaire, centrée sur les extrémités du réseau.*
>
> *À l'heure du cloud public, du télétravail, des organisations étendues, de l'extension sans fin de notre surface d'attaque et de leur corollaire, la multiplication des menaces informatiques, les forteresses numériques et la confiance implicite qui y régnait ont vécu. Bien sûr, cette mutation n'est pas un long fleuve tranquille, certains lui reprochant l'illusion de sécurité qu'elle procurerait, la complexité technique induite, la difficulté de l'expérience utilisateur, son acceptation sociétale limitée, etc. Mais qu'on le veuille ou non, le Zero Trust, voire la méfiance, sont bel et bien devenus le préalable nécessaire pour (r)établir la confiance pour tous.*
>
> **Général Marc Watin-Augouard & Guillaume Tissier, Fondateur et Directeur général du Forum InCyber**

Au-delà d'une expression marketing, le concept de Zero Trust incarne un changement de paradigme en matière de cybersécurité : un nouveau standard en matière de gouvernance et d'architecture informatique.

Il propose une approche qui transcende les limites des architectures fondées sur un web centralisé à qui l'on fait pleinement confiance en lui substituant ***le principe de ne jamais faire confiance et de toujours vérifier (« Never trust, always verify »)***.

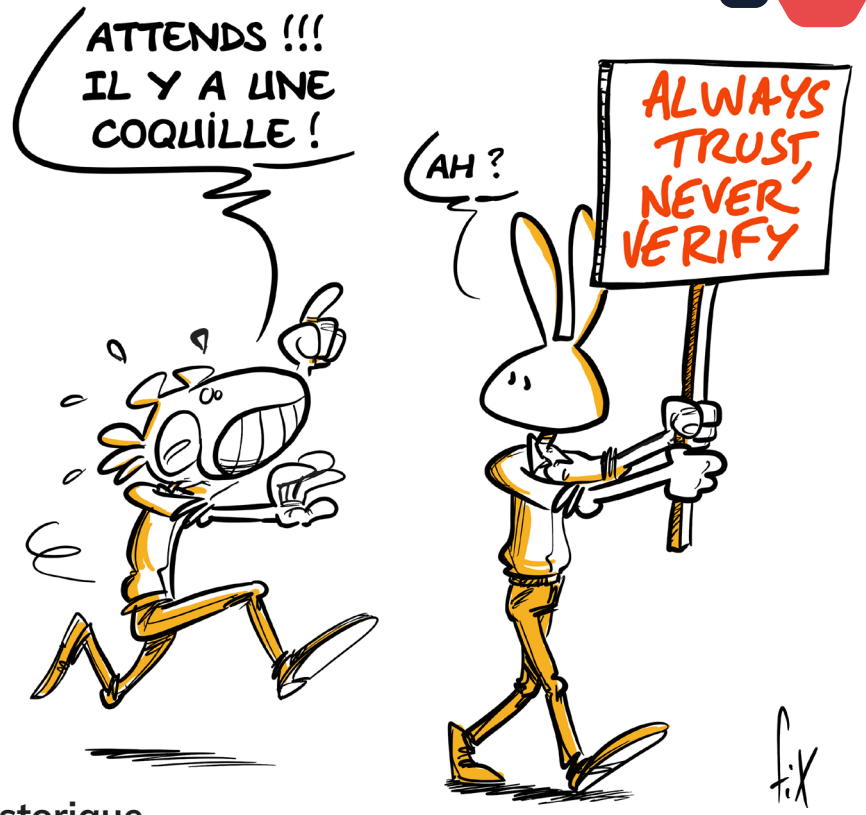
Ce concept consiste à se défier de tous les intermédiaires : fournisseurs de cloud, infogéreurs infrastructure réseau ou internet, administrateurs système, lois extra-territoriales et, a contrario, à confier à l'utilisateur final la maîtrise de sa sécurité sur son périmètre de responsabilité, notamment celle des données, au plan matériel, humain et logiciel. Les utilisateurs peuvent être externes (prestataires, infogéreurs), internes avec des droits élevés (administrateurs système, utilisateurs à privilège) ou simples utilisateurs.

Les menaces

La cybercriminalité a franchi un cap, évoluant d'une logique d'individus isolés ou de petits groupes opportunistes à une véritable industrie structurée. Désormais, les attaquants n'ont plus besoin d'être des experts en sécurité informatique. Ils agissent comme maillons d'une filière criminelle organisée, où des places de marché spécialisées permettent d'acheter des données sensibles ou des outils développés par des experts, eux-mêmes connectés à des chercheurs en vulnérabilités. Cette industrialisation a considérablement abaissé la barrière à l'entrée, favorisant une explosion des cyberattaques, **qui augmentent de près de 30 % chaque année, selon les analystes.**

Parallèlement, les menaces avancées, connues sous le nom **d'APT** (Advanced Persistent Threats) et souvent soutenues par des États-nations, ont changé de stratégie. Ces attaques, autrefois discrètes et axées sur l'exploration des systèmes, se sont transformées en opérations agressives et ciblées, conçues pour perturber durablement, voire détruire, les infrastructures visées.

Enfin, de nouvelles formes de menaces juridiques émergent sur le terrain numérique. En utilisant le droit extraterritorial comme une arme, certains acteurs détournent les données partagées sur le cloud ou échangées en ligne pour les retourner contre leurs propriétaires, exacerbant les tensions entre États et renforçant les enjeux géopolitiques du cyberespace.



Historique

Le concept de modèle **Zero Trust** est né lors du Forum de Jéricho en mai 2007[1] qui a introduit 11 commandements de sécurité dont notamment le n°6 « *Toutes les personnes, tous les processus et toutes les technologies doivent avoir des niveaux de confiance déclarés et transparents pour que toute transaction puisse avoir lieu* » et le n°7 « *Les niveaux d'assurance de confiance mutuelle doivent être déterminables*».

En 2010, le cabinet Forrester en simplifie la philosophie : « le trafic réseau n'est pas fiable ». C'est en quelque sorte la fin du modèle de sécurité fondé sur les protections périmétriques : l'ennemi est désormais à l'intérieur du réseau. Puis, en 2011, il relie le concept à l'ancien modèle - « Trust but Verify and invert it ».

En 2018, Palo-Alto renforce le modèle avec un principe radical de « ***ne jamais faire confiance, toujours vérifier*** »[2]. Cette dernière définition est utilisée dans l'industrie comme principe de confiance zéro.

En 2020, l'évolution des menaces conduit l'organisme américain NIST (National Institute of Standards and Technology) à normaliser les architectures Zero Trust.

1 https://collaboration.opengroup.org/jericho/commandments_v1.2.pdf
2 «Never Trust, Always verify» : https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture

Le NIST SP 800-207 « **Zero Trust Architecture** »[3] propose un schéma directeur pour l'implémentation d'une architecture Zero Trust, des modèles de déploiement et des cas d'utilisation généraux où la stratégie Zero Trust peut améliorer la posture de sécurité globale d'une entreprise.

Le Zero Trust désigne désormais un ensemble de principes de cybersécurité qui transforme les défenses traditionnelles, fondées sur des périmètres statiques, en un modèle centré sur les utilisateurs, les actifs et les ressources.

Il suppose qu'aucune confiance implicite n'est accordée aux composants et aux acteurs du SI qu'ils soient humains, matériels ou logiciels, sur la seule base de leur emplacement physique ou réseau ou sur la base de la propriété des biens. L'authentification et l'autorisation de l'utilisateur et du dispositif sont des fonctions distinctes réalisées avant l'établissement d'une session vers une ressource d'entreprise.

La stratégie Zero Trust a été largement documentée dans plusieurs publications françaises de référence :

- Un avis scientifique de l'ANSSI[4].
- Un rapport du CIGREF[5] (association de grands utilisateurs d'informatique).
- Une analyse aprofondie du CLUSIF[6].

De plus, selon le 10ème baromètre du CESIN[7], le concept de Zero Trust continue de gagner en maturité, étant déjà en place ou en cours de déploiement dans 74 % des entreprises interrogées.

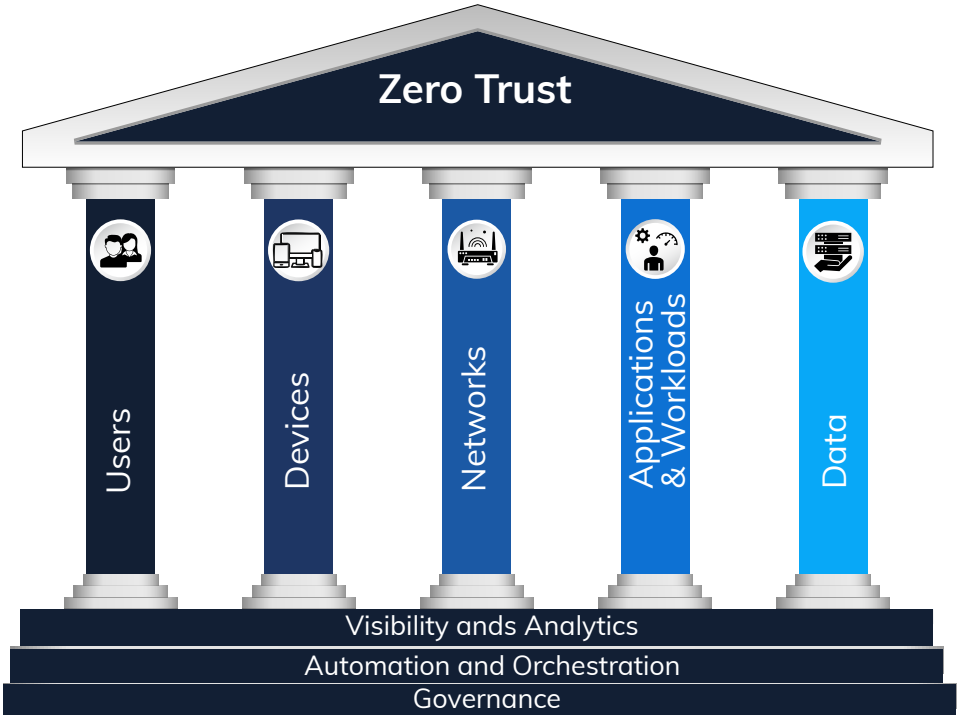
Selon les recommandations de l'ANSSI, le concept de Zero Trust n'est pas une solution clé en main, mais une remise en cause de la « confiance implicite » accordée dans le modèle périmétrique, s'appuyant sur des contrôles dynamiques et granulaires :

- L'accès aux ressources doit être accordé sur la base du besoin d'en connaître ;
- L'accès doit être donné sur la base du plus faible niveau de privilège nécessaire pour réaliser la tâche ;
- Les demandes d'accès doivent être contrôlées de la même manière quelles que soient leurs origines (le périmètre « intérieur » ou « extérieur » de l'entité) ;
- La politique d'accès aux ressources doit être dynamique et prendre en compte un large nombre d'attributs (identités de l'accédant et de la ressource accédée, sensibilité des ressources sollicitées, analyse comportementale de l'utilisateur, horaires d'accès, etc.) ;
- L'entité doit veiller à la sécurité de tous ses actifs à l'occasion lors des demandes d'accès et de manière récurrente durant l'usage ;
- Les authentifications et autorisations d'accès aux ressources doivent faire l'objet de réévaluations régulières.

3 NIST SP 800-207 « Zero Trust Architecture » : https://csrc.nist.gov/publications/detail/sp/800-207/final
4 Agence Nationale de Sécurité des Systèmes d'Information : https://cyber.gouv.fr/publications/le-modele-zero-trust
5 CIGREF « Vers une philosophie Zero Trust - Une rupture dans la continuité pour la sécurité des applications » : https://www.cigref.fr/wp/wp-content/uploads/2022/02/Vers-une-philosophie-Zero-Trust-Une-rupture-dans-la-continuite-pour-la-securite-des-applications-fevrier-2022.pdf
6 CLUSIF (Association de promotion de la cybersécurité, réunissant entreprises et administrations autour du développement des bonnes pratiques pour la sécurité du numérique) « Que faut-il savoir du zero trust ? » https://clusif.fr/publications/que-faut-il-savoir-du-zero-trust/
7 10eme baromètre CESIN : https://cesin.fr/articles-slug/?slug=2354-2354-Communiqu%C3%A9+de+Presse+-+10%C3%A8me+%C3%A9dition+du+barom%C3%A8tre+annuel+du+CESIN

Les besoins de sécurité Zero Trust et les solutions

Les besoins de sécurité s'articulent autour d'une succession de protections, au centre desquelles se situent les données à protéger. En progressant du niveau le plus central vers le plus périphérique, il est essentiel, sans prétendre à l'exhaustivité, de couvrir diverses fonctions de sécurité.



Les piliers Zero trust

- **Pilier "Users" (personne ou machine) :** sécurité des identités par authentification multifacteurs (MFA) de préférence en continu et infrastructure de gestion des clés (PKI) ;
- **Pilier "Devices" :** sécurité des terminaux par Endpoint Détection & Réponse (XDR) et antivirus et conformité ;
- **Pilier "Networks" :** sécurité des réseaux par Zero Trust Network Access (ZTNA), Réseau Privé Virtuel (VPN), chiffreur softless ou Network Detection & Response (NDR) ;
- **Pilier "Applications & Workloads" :** sécurité des applications par contrôle des accès, des transactions et du comportement des utilisateurs ;
- **Pilier "Data" :** sécurité des données par signature et chiffrement de bout-en-bout (End-to-end encryption), Data Centric Security (DCS) et Data Loss Prevention (DLP).

La sécurité des infrastructures, assurée par des environnements conformes aux exigences de SecNumCloud ou par des mécanismes avancés tels que les enclaves cryptographiques, constitue une base essentielle et transversale pour soutenir tous ces piliers.

Le modèle Zero Trust, initialement utilisé pour les systèmes IT, s'étend aux systèmes cyber-physiques (CPS) incluant IoT (Internet of Things) et OT (Operational Technology), essentiels dans les infrastructures critiques. Cette approche est cruciale pour protéger ces technologies souvent exposées à des risques spécifiques (longue durée de vie, mises à jour limitées, connexions peu sécurisées).

En milieu industriel, par exemple, le Zero Trust impose des contrôles stricts (authentification et autorisation constantes) à chaque connexion réseau, limitant la propagation de menaces.

Dans les architectures de confiance zéro, la sécurité des données est supposée se situer au plus près de l'utilisateur et de son terminal, donc à la périphérie du système d'information et non au niveau de l'infrastructure centrale qui est supposée compromise :

- Identification et authentification en continu, voire identité auto-souveraine ;
- Moindre privilège ;
- Journalisation et historisation ;
- Micro-segmentation des réseaux et des ressources ;
- WORM (Write Once / Read Many : anti-ransomware) ;
- Contrôle exclusif des données par des clés locales ;
- Multi-cloud.

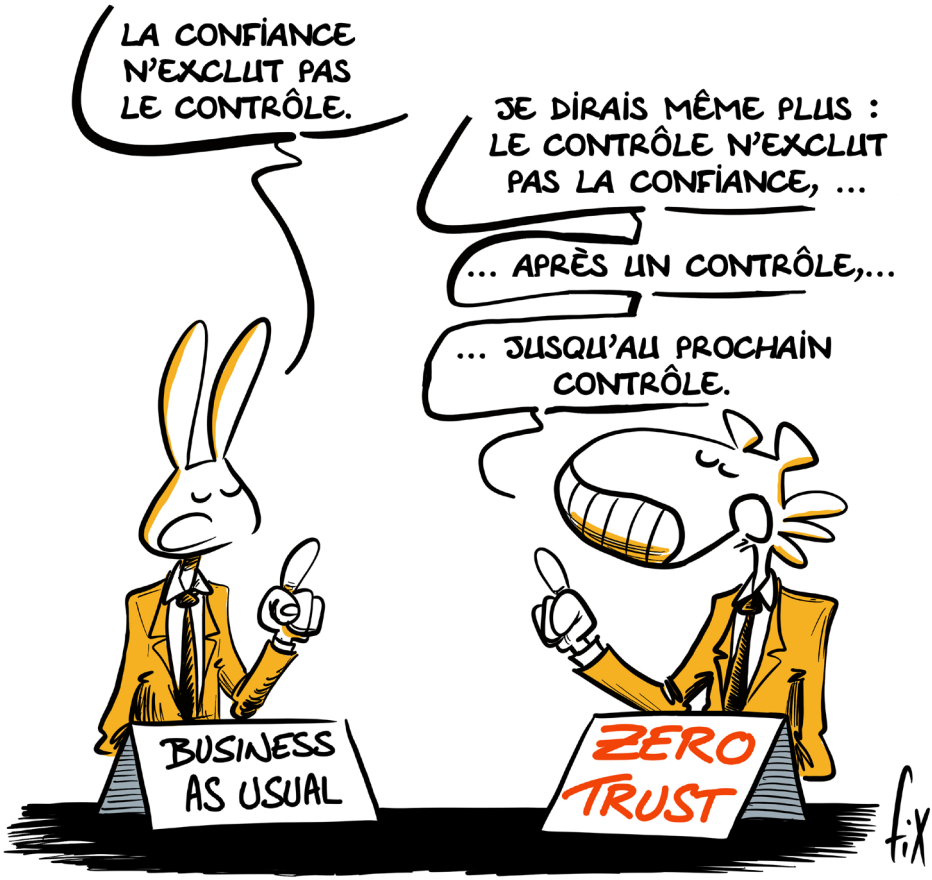
Les limites du modèle et les réponses

Il ne peut exister de sécurité absolue dans un système fini de composants de sécurité, puisque le dernier vérificateur ne peut pas être vérifié. Le modèle Zero Trust a ses propres limites, car pour vérifier, nous devons accepter comme « de confiance » un ultime tiers de confiance, celui qui est chargé de la vérification. Une façon de contourner ce paradoxe consiste à accepter quelques axiomes de base :

- Mon logiciel, préférentiellement ouvert, fait l'objet d'une certification par un tiers de confiance neutre ;
- Je suis le seul utilisateur en qui j'ai confiance. Et moi seul suis habilité à distribuer ma confiance ;
- À partir du moment où j'accepte de travailler sur un réseau (public ou non), mon terminal d'accès à ce réseau est ma seule entité matérielle de confiance ;
- Enfin, mon système logiciel Zero Trust doit être ma seule entité de confiance logicielle.

L'asymptote « Zero Trust »

La sécurité des systèmes d'information est une lutte entre le glaive et le bouclier. Il n'y a pas de sécurité ultime et pourtant il est vital de s'en rapprocher. Cette démarche est d'autant plus difficile qu'une bascule complète vers un modèle de Zero Trust apparaît peu envisageable pour les entités dotées d'un patrimoine informatique hérité et sédimenté. En ce sens, on peut dire que la stratégie de la confiance zéro, s'apparente plutôt à une asymptote Zero Trust, comme la flèche de Zénon d'Élée qui n'atteint jamais sa cible, mais s'en rapproche à l'infini.



Le paradigme Zero Trust : ne jamais faire confiance, toujours vérifier !

Le Zero Trust est une stratégie de sécurité qui impose de vérifier chaque utilisateur et appareil sans accorder de confiance par défaut.

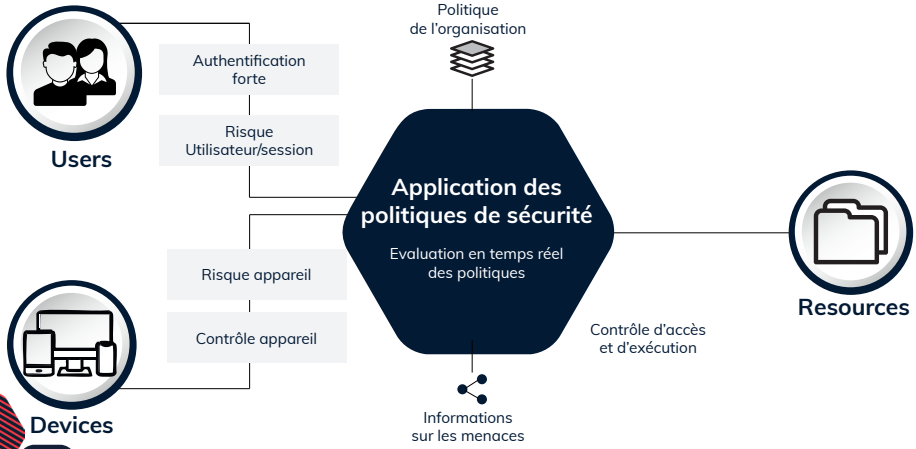
Principe fondamental

Au lieu de supposer que tout ce qui se trouve à l'intérieur du périmètre du réseau est sûr, le modèle Zero Trust traite chaque requête d'accès comme si elle provenait d'une source non fiable. Ceci ne veut pas dire supprimer les protections réseau, mais d'ajouter l'architecture Zero Trust pour que l'architecture soit résiliente face à un réseau attaqué.

Comment ça marche ?

- **Vérification stricte et continue de l'identité :** chaque utilisateur et appareil doit s'authentifier et prouver son identité avant d'accéder aux ressources.
- **Autorisation granulaire :** l'accès aux données et applications est accordé selon le principe du moindre privilège. Les utilisateurs n'ont accès qu'aux ressources dont ils ont besoin pour effectuer leur travail.
- **Micro-segmentation :** les ressources et le réseau sont cloisonnés en segments plus petits et isolés pour limiter l'impact d'une compromission.
- **Surveillance et réponses à incident continues :** le trafic réseau et les terminaux sont surveillés en permanence pour détecter les activités suspectes.

Principe



Transition vers le Zero Trust : étapes et bonnes pratiques

L'ANSSI rappelle combien une transition complète vers un modèle Zero Trust semble difficilement envisageable pour les organisations disposant d'un système d'information hérité et complexe. En effet, cela impliquerait une refonte totale de leur architecture informatique. Face à ces contraintes, les promoteurs du Zero Trust privilégient une mise en œuvre progressive et structurée.

Une stratégie couramment proposée consiste à envisager l'adoption du Zero Trust en deux étapes. La première implique l'intégration au système d'information « traditionnel » d'un éventail de solutions, telles que des outils de chiffrement, des dispositifs de prévention des fuites de données (Data Loss Prevention), ou encore des contrôles de conformité comme les systèmes NAC (Network Access Control). De son côté, le NIST prône une approche incrémentale, envisageant d'abord la mise en place de systèmes hybrides combinant principes Zero Trust et modèle périmétrique.

Avant tout déploiement, une mise à jour de l'analyse des risques s'avère indispensable. Elle repose sur une cartographie précise du système d'information, avec une distinction claire entre les périmètres pouvant être intégrés au modèle Zero Trust (par exemple, les applications Web et cloud) et ceux qui en seront exclus.

Les leviers de l'ANSSI pour adopter le Zero Trust

L'ANSSI recommande plusieurs leviers d'action permettant de moderniser un système d'information traditionnel tout en adoptant les principes du Zero Trust :

- **Renforcer la gouvernance des identités :** l'accès aux ressources doit être conditionné par l'identification de l'utilisateur et de son équipement, en tenant compte de critères environnementaux (heure, localisation, etc.). Les référentiels d'identité, éléments centraux du modèle, doivent être rigoureusement mis à jour pour refléter fidèlement l'état des utilisateurs (arrivées, départs, mobilités).

- **Mettre en place une segmentation granulaire et dynamique des ressources :** cette micro-segmentation regroupe les actifs en clusters métier et isole les flux entre eux, indépendamment des adresses IP. En utilisant des couches d'abstraction telles que les tags ou VXLAN, les ressources sont protégées en fonction de leur sensibilité et de leur exposition aux menaces.

- **Adopter des moyens d'authentification à l'état de l'art :** l'authentification multifactorielle étant un prérequis, il est crucial de choisir des solutions robustes, comme des certificats issus d'une infrastructure de gestion de clés (IGC) ou des jetons FIDO.

- **Renforcer les capacités de détection :** les journaux de sécurité doivent être configurés et centralisés dans des solutions SIEM, avec des équipes SOC suffisamment formées pour réagir rapidement en cas d'alerte.

- **Assurer une configuration conforme aux standards de sécurité :** par exemple, le chiffrement TLS doit être paramétré selon les recommandations de l'ANSSI.

- **Accompagner la conduite du changement :** les utilisateurs, premiers concernés par la cybersécurité de leur organisation, doivent être informés et formés sur les nouveaux modes d'accès et d'authentification.

En conclusion, cette transition doit s'opérer de manière maîtrisée afin de protéger les données et actifs critiques, sans fragiliser le système historique. Notamment, les postes d'administration doivent être exclus du modèle Zero Trust, conformément aux recommandations de l'ANSSI. L'utilisation de postes dédiés, connectés via un tunnel VPN IPsec sécurisé, reste une pratique à privilégier.

Partie II

Cartographie des acteurs

GOVERNANCE

algosecure

conscio Technologies

USERS

CLOUD IAM

digitalberry

EVERTRUST

fair trust

HIA secure
the ultimate smart security

OpenSezam
Trust Authentication

TrustBuilder

wallix

DEVICES

ERCOM
Cyber Solutions by Thales

HarfangLab

ITRUST.

sekoia

THEGREENBOW

VirtualBrowser

NETWORKS

clever cloud

CUSTOCY

GATEWATCHER

ITRUST.

Olfeo

P4S

sekoia

snowpack

CARTOG

Zer
Tru

IT INTEGRATOR

DOCAPOSTE

eXcelsior Safety

EXIPTEL
Experts réseaux & cybersécurité

ise SYSTEMS

Smart Global Governance

wallix

INFRASTRUCTURES

3DS OUTSCALE

SCALITY

Ugloo

DATA

ERCOM Cyber Solutions by Thales

GLIMPS

linphone

Olvid

PARSEC Trust the Cloud

PRIMX MAKE ENCRYPTION HAPPEN

PRIVATE DISCUSS

retarus

seald

Sonar Clarity

RAPHIE

ro

ust

APPLICATIONS & WORKLOAD

ATEMPO

Altospam

JALIOS

NetExplorer

odrive

</ɹǝvǝʞSense>

Sharekey Secure Business Privacy

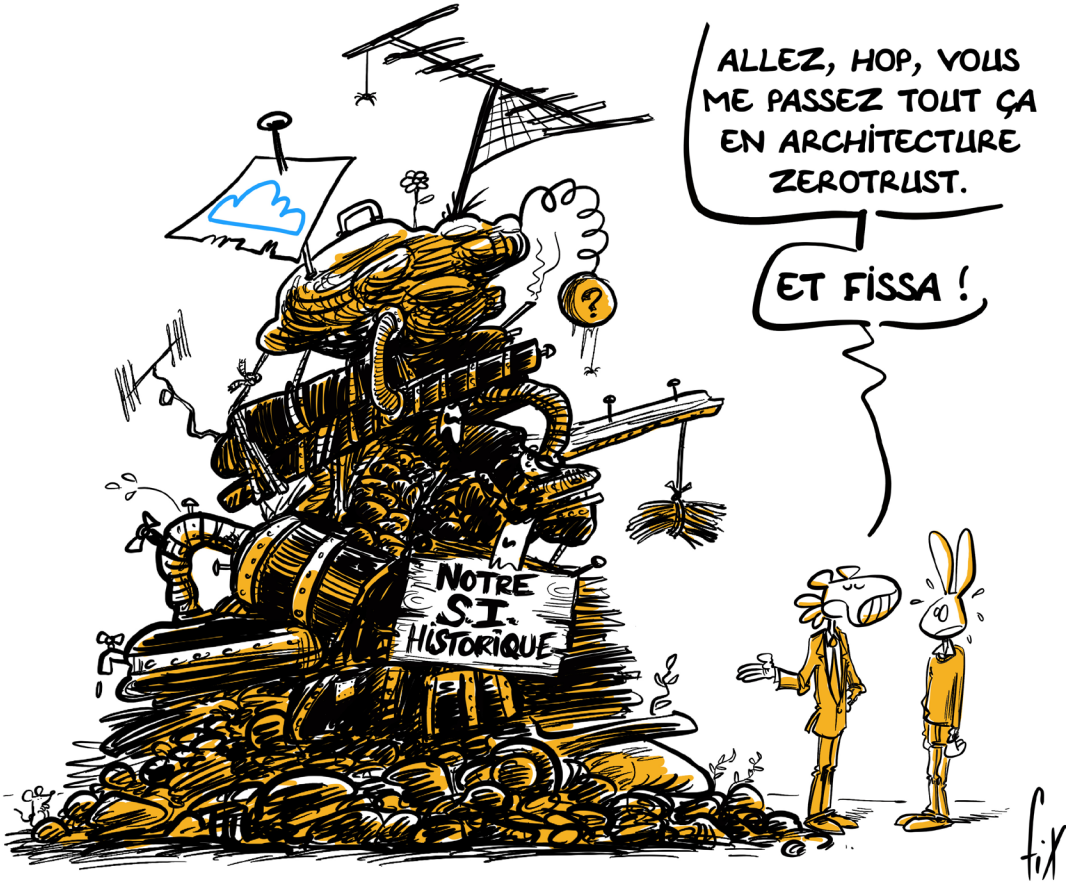
UBIKA

Whaller

EY

CNS IDENTITY & ACCESS

LOGIN SÉCURITÉ


ALLEZ, HOP, VOUS ME PASSEZ TOUT ÇA EN ARCHITECTURE ZEROTRUST.
ET FISSA !
NOTRE S.I. HISTORIQUE
?
fix

Partie III

Témoignages et cas d'usages

PARSEC propose une suite logicielle Data Zero Trust compatible avec Office 365 certifiée CSPN par l'ANSSI.

Conçue pour protéger la confidentialité et l'intégrité des données, elle permet des échanges sécurisés en interne comme en externe, avec déploiements sur cloud souverain, Saas ou On Premise.

Le Service du Soutien de la Flotte de la Marine nationale intègre le Zero Trust avec PARSEC, pour la sécurité de données sensibles.

MARINE NATIONALE

Besoin

Dans le but de sécuriser les échanges de plans 3D entre les acteurs de la plateforme MainChain (solution de notre partenaire Vistory) et de tracer l'ensemble des actions effectuées sur les imprimantes 3D, le Service de Soutien de la Flotte (SSF) a exprimé le besoin de disposer d'un outil simple et sécurisé, fonctionnant selon le principe du Zero Trust.

Solution

Pour répondre à cette exigence, le SSF intègre PARSEC, qui est déjà partiellement déployé en interministériel sous le nom de ResanaSecure. Dans son utilisation actuelle, Parsec, certifié CSPN par l'ANSSI, offre au SSF un service collaboratif entièrement sécurisé et une traçabilité complète de leurs impressions 3D, quel que soit le nombre de sites de production impliqués.

Bénéfice client

Cette intégration permet une synchronisation de confiance des fichiers entre différents sites distants et leurs utilisateurs, garantissant ainsi une gestion sans compromis du « droit-à-en-connaître », un partage sécurisé de fichiers même très volumineux, en mode Zero Trust avec une possibilité de révocation cryptographique, sur un réseau contraint voire intermittent. PARSEC contribue aussi à l'atteinte des objectifs réglementaires de la directive NIS2 : chiffrement des données de bout-en-bout, sécurité de la chaîne d'approvisionnement, sauvegarde et reprise rapide des données critiques, politique de sécurité dynamique. Le nombre d'invités est illimité ce qui rend la solution très économique.

Déploiement

1. Un serveur de métadonnées chiffrées.
2. Un logiciel de crypto-partage certifié CSPN sur tous les terminaux utilisateurs.
3. Le bootstrap d'une ou plusieurs Organisations de confiance.
4. Le branchement de votre PKI (quand elle existe).
5. L'enrôlement des invités externes quel qu'en soit le nombre.

Certification VISA DE SÉCURITÉ

UBIKA, éditeur français pionnier du WAF en Europe, propose le seul produit certifié du marché. Il permet de sécuriser les accès et de contôler le comportement des utilisateurs des applications Web et API de l'organisation, quelle que soit la confiance accordée au device et au réseau utilisés pour se connecter

BPCE renforce l'accès aux applications pour une approche Zero Trust

Jérémy Renard
Team leader adjoint INET SAS Externes, BPCE

Besoin

La sécurité Zero Trust repose sur le renforcement de l'accès aux applications, en partant du principe que les menaces peuvent venir de n'importe où. Aucune entité, qu'elle soit interne ou externe, n'est présumée digne de confiance par défaut. Le WAAP (Web Application & API Protection) constitue l'ultime barrière de protection de nos applications et des données qu'elles exposent contre des menaces comme les injections, le credential stuffing, et les attaques par force brute.

Solution

La solution d'UBIKA a permis d'instaurer une politique de sécurité précise, adaptée aux différents points d'accès à nos services numériques, avec des autorisations granulaires pour les applications critiques. Elle apporte des possibilités comme la surveillance des comportements utilisateurs, l'analyse des horaires et lieux d'accès, la réputation des adresses IP. Le WAAP peut aussi être programmé pour appliquer une sécurité plus stricte fondée sur le contexte ou pour vérifier l'identité de l'utilisateur via des challenges d'authentification. Cette approche renforce l'efficacité de la sécurité dans une stratégie Zero Trust. Tous les utilisateurs, même internes, doivent s'authentifier avant d'accéder aux applications, limitant les risques d'introductions malveillantes via des devices ou réseaux non sécurisés. La surveillance continue permet de traiter toute activité suspecte, provenant de l'intérieur comme d'une source externe.

Bénéfice client

Nos applications et nos API sont protégées et la disponibilité de nos services n'est pas perturbée par les attaques. Nous pouvons donc nous concentrer sur notre cœur de métier sans nous soucier de la sécurité de nos données. De plus, cela renforce la confiance de nos clients dans le fait que nous prenons leur sécurité au sérieux.

snowpack Lauréate 2024 du prix des Assises & du Forum InCyber, Snowpack protège les organisations des cyberattaques menées depuis Internet, en rendant invisible leur surface d'attaque externe.

Elle pousse l'approche Zero Trust plus loin, agissant comme une couche d'indépendance entre l'infrastrusture et les données en transit.

Comment un OIV dans le secteur du nucléaire renforce l'efficacité de son SOC, en combinant la furtivité de Snowpack et la RBI (Remote Browser Isolation) de VirtualBrowser ?

Besoin

Le client, acteur majeur de la recherche technologique, fait face en permanence à des cybermenaces, et notamment à des alertes rattachées à des campagnes et liens de phishing ciblant ses collaborateurs. Pour réagir efficacement, il souhaite, à travers son SOC dont l'ambition est d'être conforme avec le référentiel PDIS de l'ANSSI, accéder à ces liens pour comprendre l'attaquant, sans pour autant risquer de compromettre son identité (ie. sans exposer ses IPs), ni risquer d'introduire des charges malveillantes dans son SI.

Solution

Afin d'accéder aux charges utiles sans risquer d'être corrompu, l'utilisation conjointe des solutions de « Remote Browser Isolation » de Virtual Browser et d'invisibilité de Snowpack fournit un système de RBI non marqué sans tiers de confiance.

Bénéfice client

Le couplage des solutions Virtual Browser et Snowpack apporte les bénéfices suivants :

- Le client est assuré de ne pas introduire de charges utiles malveillantes dans son SI.
- Le système d'anonymisation n'est pas tiers de confiance, il est aveugle et ne peut pas modifier les requêtes clients. Ainsi la nature des menaces recherchées par le client et l'expertise opérationnelle de son SOC restent inconnues du fournisseur du service (i.e. Virtual Browser et Snowpack).
- Les attaquants ne peuvent en aucun cas rattacher l'IP du client ni à Virtual Browser, ni à son utilisateur. Les attaquants ne peuvent donc pas déterminer si leur attaque a atteint, même partiellement, sa cible.

Enfin, la solution globale permet au client de se conformer à certaines exigences du référentiel ANSSI PDIS, notamment l' article IV.3.16.

ERCOM est le spécialiste de la collaboration sécurisée. Cryptobox est la solution souveraine de partage de fichiers jusqu'au niveau Diffusion Restreinte.

Facilitez la collaboration tout en vous protégeant des piratages et fuites de données ! Disponible en SecNumCloud, Saas, On Premise ou hybride.

Sécuriser la collaboration pour le Campus Cyber et pour ses Membres grâce à l'outil de confiance Cryptobox

Michel Van Den Berghe
Président du Campus Cyber

Besoin

Le Campus Cyber, lieu totem de la cybersécurité en France, encourage activement les échanges entre ses Membres dans le but de favoriser le partage d'informations et de renforcer la résilience face aux enjeux numériques d'aujourd'hui. Pour soutenir ces interactions tout en répondant aux exigences de sécurité propres à ses missions, le Campus Cyber a choisi de mettre à disposition de son écosystème un outil collaboratif hautement sécurisé.

Solution

Cryptobox est une solution qui permet aux organisations de partager des données en toute confidentialité. Chaque utilisateur décide avec qui il partage ses données, que ce soit au sein de son organisation ou avec des partenaires externes, et peut définir les niveaux d'accès dans chaque workspace. L'administrateur n'a aucun accès aux données ni aux workspaces, assurant ainsi la sécurité et la confidentialité des informations.
Les données sont chiffrées de bout-en-bout, directement sur le terminal de l'utilisateur, avec des clés qui ne transitent jamais par le cloud. L'utilisateur n'a ainsi qu'à se fier à la sécurité de son terminal (un aspect également couvert par Cryptosmart d'Ercom) et aux personnes qu'il invite, selon les principes du Zero Trust.

Bénéfice client

Grâce à Cryptobox, hébergé dans une infrastructure certifiée SecNumCloud, le Campus Cyber offre à ses Membres un outil collaboratif souverain. Le cloisonnement par workspace permet aux contributeurs du Studio des Communs, Collèges de la gouvernance, Communautés d'intérêt et autres projets actifs, d'organiser les échanges et de gérer la diffusion des informations de manière efficace et sécurisée, renforçant la confiance dans la robustesse de l'outil face aux enjeux numériques d'aujourd'hui.

HIAsecure offre une authentification cognitive forte et passwordless, conforme NIS2, DSP2, et RGPD.

Sa technologie Zero Trust élimine la confiance implicite et garantit un contrôle d'accès rigoureux, protégeant les ressources sensibles tout en offrant une expérience utilisateur simple et sécurisée.

Construire un environnement Zero Trust : eMANA mise sur HIAsecure pour sécuriser ses utilisateurs

Raynald Wauters
eMANA

Besoin

Chez eMANA, nous accompagnons nos clients dans la gestion intelligente de leurs communications électroniques. Cependant, la question de la sécurité s'est imposée comme un défi majeur. Nos utilisateurs, souvent confrontés à des cyberattaques ciblant les accès, attendent une solution fiable et simple pour protéger leurs données sensibles. Les systèmes traditionnels s'appuyant sur des mots de passe présentent trop de vulnérabilités, augmentant les risques de piratage et d'usurpation d'identité. Il nous fallait une approche moderne, conforme à des standards stricts comme le Zero Trust et la réglementation (NIS2 et RGPD), tout en garantissant une expérience fluide.

Solution

Dans cette optique, nous avons adopté les solutions HIAsecure, qui s'alignent parfaitement sur notre approche Zero Trust. Leur méthode fondée sur l'intelligence humaine permet aux utilisateurs de générer un code unique sécurisé à partir d'un message instantané. Ce processus non seulement améliore considérablement la protection des données, mais élimine aussi les failles des systèmes de mot de passe traditionnels. Nos clients bénéficient désormais d'une sécurité accrue sans compromettre l'expérience utilisateur.

Bénéfice client

En intégrant HIAsecure, nous renforçons nos défenses contre les cyberattaques tout en respectant les exigences réglementaires, comme NIS2 et RGPD. Cette collaboration nous permet d'instaurer une relation de confiance durable avec nos clients, un atout majeur dans un environnement Zero Trust.

HIAsecure s'est révélé être un partenaire indispensable dans notre mission d'allier innovation, simplicité et sécurité.

Olfeo, expert en gestion et sécurisation des accès Internet, offre des solutions SSE intégrant filtrage web, DLP, CASB et inspection en temps réel du trafic web.

Avec une approche Zero Trust, il assure la protection contre les menaces, sur site ou en mobilité, pour une cybersécurité maximale.

Le CHU de Poitiers déploie la solution de passerelle de sécurité web Olfeo avec la gestion des accès web Zero Trust

Pierre Taveau
RSSI chez CHU POITIERS

Besoin

Le CHU de Poitiers a déployé la solution Olfeo avec la fonctionnalité Trust-Centric sur 7000 postes et 5 sites, une décision visant à renforcer la sécurité des infrastructures numériques. Dans un contexte où les cybermenaces se multiplient et où les données de santé constituent des cibles particulièrement sensibles, l'adoption d'une approche de sécurité robuste et innovante est devenue impérative. C'est dans cette optique que le CHU a opté pour la technologie d'Olfeo, qui permet un filtrage strict des contenus consultés par les utilisateurs en s'assurant qu'ils proviennent de sources vérifiées et de confiance.

Solution

La fonctionnalité Trust-Centric d'Olfeo s'inscrit dans une approche de sécurité qui repose sur le principe de « ne jamais faire confiance, toujours vérifier ». Ce modèle préconise un contrôle d'accès rigoureux à toutes les ressources, indépendamment de leur localisation par rapport au périmètre de l'organisation. En ne permettant l'accès qu'aux contenus vérifiés, l'approche Trust-Centric incarne ce paradigme, réduisant ainsi le risque d'exposition aux logiciels malveillants et autres cyberattaques.

Bénéfice client

Cette mise en œuvre au CHU de Poitiers ne se contente pas seulement de protéger les données critiques. Elle garantit également que les équipes médicales et administratives puissent travailler en toute sérénité, tout en ayant des droits d'accès très granulaires en fonction des responsabilités et missions. L'intégration d'Olfeo dans leur stratégie s'inscrit dans une vision proactive de la cybersécurité Zero Trust, assurant à la fois la protection des patients et la fiabilité des services hospitaliers.

WALLIX sécurise les identités et les droits d'accès des utilisateurs, humains et machines, pour réduire les usurpations d'identité, les accès non autorisés et les violations de données.

Avec WALLIX One, une plateforme SaaS unique pour l'identification, la gouvernance des accès et la gestion des privilèges, WALLIX instaure une première ligne de défense transparente. Son approche Zero Trust minimise les risques liés aux identifiants compromis tout en garantissant un accès rapide aux environnements IT et OT de l'entreprise.

Le SIAPP contrôle les actions de ses prestataires externes et sécurise l'accès aux équipements industriels (SCADA)

SIAAP
Service public de l'assainissement francilien

Besoin

Le SIAAP(Syndicat Interdépartemental pour l'Assainissement de l'Agglomération Parisienne) joue un rôle vital dans le traitement des eaux usées pour la région Île-de-France, impactant directement la santé publique et l'environnement. Afin de renforcer la sécurité de ses infrastructures, le SIAAP souhaitait s'équiper d'une solution répondant à deux grandes problématiques : contrôler les identités et accès des prestataires externes et sécuriser l'accès au SCADA (système de supervision permettant contrôler les équipements sur tous sites, mais aussi pour collecter et enregistrer les données des opérations).

Solution

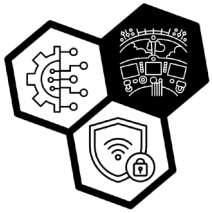
L'adoption rapide de WALLIX par le SIAAP a renforcé la supervision des accès et des activités des prestataires sur l'ensemble des systèmes et équipements. Cela a permis d'améliorer la gestion des accès externes, tout en assurant une surveillance et une traçabilité efficaces des opérations réalisées. La nécessité de sécuriser l'accès aux supervisions SCADA pour certains agents du SIAAP, en particulier pendant les périodes d'astreinte, a été efficacement adressée par les solutions de WALLIX. Les agents peuvent se connecter en toute sécurité à une station stratégiquement positionnée entre les firewalls IT et les équipements industriels OT.

Bénéfice client

Cette approche Zero Trust a non seulement renforcé la sécurité globale en établissant des pratiques de sécurité conformes aux normes requises, mais a également réduit la charge de travail des équipes IT et améliorer l'efficacité opérationnelle de l'ensemble des agents. La capacité de WALLIX à s'intégrer aisément dans des architectures et environnements IT/OT hétérogènes, en contrôlant efficacement les mots de passe, les identifiants et la gestion des privilèges, a permis une mise en œuvre rapide et efficace du contrôle sur les actions des prestataires externes et des agents internes.

THEGREENBOW TheGreenBow est un éditeur de solutions logicielles de Cybersécurité dont l'expertise repose sur la sécurisation des communications. TheGreenBow est le premier acteur à obtenir une certification CC EAL3+ de l'ANSSI pour son client VPN Windows. Ce produit détient également le label « Utilisé par les armées françaises ». Il atteste de la mise en œuvre du logiciel par les services du Ministère des Armées Françaises. Il a été octroyé en 2019, puis renouvelé en 2024.

Sécuriser les accès VPN au réseau grâce aux certificats utilisateurs



Besoin

Le Client, un OIV acteur majeur du secteur de la Défense très exposé du fait des tensions géopolitiques, doit assurer la protection des communications distantes à ses différents systèmes d'information (SI usuels, SI homologués sensibles, SI homologués DR). Différents types de endpoints et de profils d'utilisateurs sont à protéger : ordinateurs portables sous Windows pour des collaborateurs nomades, postes de travail sous linux pour des administrateurs réseaux et les développeurs... La conformité avec les réglementations en matière de cybersécurité, comme la LPM, est requise.

Solution

Pour répondre aux exigences de sécurité, les Clients VPN TheGreenBow Windows et Linux ont été déployés avec différentes configurations de tunnels IPsec dont certains permettent d'accéder à des environnements DR. Ces différents tunnels permettent de répondre à l'exigence de cloisonnement des informations. Pour renforcer la phase d'authentification, les utilisateurs doivent utiliser une carte à puce embarquant un certificat qui leur est propre pour ouvrir leur session et monter leur tunnel.

Bénéfice client

Les connexions de milliers d'utilisateurs, en interne et à distance, sont authentifiées et sécurisées. La confiance donnée aux différents individus est garantie par l'utilisation de certificats « personnels » qui sont vérifiés systématiquement par une infrastructure de gestion de clés (PKI). Enfin, les tunnels VPN IPsec garantissent l'intégrité et la confidentialité des informations échangées, en évitant ainsi tout risque de fuite de données.

Oodrive, pionnier européen de la suite collaborative de confiance, développe des solutions collaboratives sécurisées, souveraines et qualifiées SecNumCloud.

Plus de 2,5M d'utilisateurs collaborent sur leurs projets clés sans compromettre la confidentialité et l'intégrité de leurs données sensibles.

Le ministère des Armées adopte la solution Oodrive Work pour collaborer plus efficacement en situation de mobilité.

MINISTÈRE DES ARMÉES
Liberté
Égalité
Fraternité

Besoin
En 2014, la DIRISI cherchait une solution performante de partage de fichiers sur son réseau interne sécurisé. Avec la généralisation du télétravail, il devenait nécessaire de disposer d'une solution qui réponde aux besoins croissants de collaboration à distance tout en assurant la sécurité des échanges et du stockage des fichiers

Solution
La DIRISI a déployé la solution Oodrive Work, éditée par Oodrive, leader européen de la gestion des données sensibles. Oodrive Work a permis de répondre à ces besoins en offrant un service de partage de fichiers sécurisé, évolutif et adapté aux exigences du ministère des Armées. Le nombre de licences a rapidement augmenté, passant de 4 000 en 2020 à 50 000, et en 2024, 200 000 utilisateurs et partenaires externes collaborent sur les espaces de travail sécurisés Oodrive Work. Labelisée UAF, la solution permet également de gérer des fichiers volumineux sans limite de taille et de s'adapter aux besoins variés des utilisateurs, y compris pour des cas d'usages supplémentaires comme la sauvegarde de médias de smartphones ou la synchronisation des répertoires de travail.

Bénéfice client
La solution Oodrive Work a permis à la DIRISI de fournir des services numériques efficaces et sécurisés aux forces et agents du ministère des Armées, facilitant le travail en mobilité de manière souple, sécurisée et simple. Elle a été un acteur clé dans la transformation digitale du ministère, permettant une collaboration fluide et la gestion sécurisée des données sensibles, tout en répondant aux besoins croissants d'usage et de flexibilité.

Certifications OODRIVE

SHAREKEY est une application de collaboration suisse, souveraine et complète : tout-en-un (messenger, drive, visio, notes,...), entièrement chiffrée et très intuitive.

Elle répond aux besoins croissants en matière de gestion de crise, de protection des dirigeants, COMEX, CODIR et de sécurisation des échanges de données sensibles, sur tout type d'appareil, partout dans le monde, à l'intérieur comme à l'extérieur des organisations.

Zero Trust & confidentialité : comment LINKAPITAL sécurise ses transactions M&A avec SHAREKEY ?

Grégory Sabah
Associé Fondateur

Besoin

Les opérations d'ouverture du capital, de cession d'entreprise ou de M&A (fusion et acquisition) nécessitent des échanges quotidiens de données sensibles et stratégiques. Ces transactions imposent des exigences élevées en matière de sécurité, de protection et de confidentialité des informations échangées. Le risque de fuite de données constitue une préoccupation majeure dans le choix de la solution adoptée. Pour répondre à ces enjeux, LINKAPITAL, banque d'affaires indépendante engagée auprès des entrepreneurs, recherchait une solution garantissant à la fois une protection optimale et une simplicité d'utilisation.

Solution

SHAREKEY, avec son approche Zero Trust by Design, répond parfaitement à ces défis. La solution garantit un chiffrement app-to-app pour toutes les communications et échanges, avec des clés de chiffrement décentralisées dans un crypto wallet intégré à l'application. Les données sont hébergées chiffrées dans un cloud souverain en Suisse, qui, par conception, ne permet pas d'accès, même par les employés de SHAREKEY. L'application permet de partager des informations sensibles et de communiquer en toute sécurité, quel que soit le type d'appareil ou le lieu, à l'intérieur comme à l'extérieur des organisations. Conçue pour répondre aux besoins des exécutifs, elle associe une interface épurée et intuitive à des fonctionnalités avancées pour une expérience utilisateur optimale.

Bénéfice client

SHAREKEY a permis à LINKAPITAL d'adopter une suite collaborative répondant aux exigences suivantes :

- **Sécurité et confidentialité élevées** grâce au chiffrement et à l'hébergement souverain.
- **Prise en main rapide** avec une interface intuitive conçue pour les exécutifs.
- **Souveraineté totale** éliminant les risques liés aux lois extraterritoriales.
- **Flexibilité globale** sans géo-restriction.
- **Outil tout-en-un :** chats, channels, visioconférences, datarooms, et partage sécurisé de liens, entièrement chiffrés.

Belledonne Communications développe Linphone, une plateforme sécurisée pour appels VoIP, messagerie instantanée et visioconférence.

Protégez les communications de votre organisation avec une application simple à utiliser, sécurisée et 100% open source, disponible on-premise ou en SaaS.

Sécuriser les communications dans une organisation publique, en garantissant simplicité et mobilité.

Besoin

Une organisation publique, dont les activités nécessitent des échanges sensibles et confidentiels, cherchait une solution pour protéger les communications par Internet entre ses agents. Elle avait besoin d'une application offrant un haut niveau de sécurité, mais simple à adopter, afin de faciliter son usage quotidien. La mobilité constituait un enjeu clé : ses agents, souvent en déplacement, devaient pouvoir utiliser une solution multiplateforme, accessible sur ordinateurs et smartphones. L'organisation souhaitait également garantir la souveraineté de ses données, en évitant toute dépendance vis-à-vis de prestataires tiers.

Solution

L'organisation a adopté Linphone, associé à Flexisip, le serveur SIP de Belledonne Communications. Linphone garantit un chiffrement de bout-en-bout pour voix, vidéo et texte, grâce à des technologies robustes, résistantes aux attaques quantiques. Les contenus restent inexploitables même en cas de compromission du serveur. Compatible avec mobiles et PC, Linphone propose une interface intuitive favorisant une adoption rapide, même pour des utilisateurs peu technophiles, sans compromis sur la sécurité. Flexisip a été déployé on-premise et intégré à l'infrastructure VoIP existante.

Bénéfice client

L'organisation garantit un haut niveau de confidentialité pour ses communications tout en offrant à ses agents une solution simple et ergonomique. La compatibilité multiplateforme assure une continuité d'usage, au bureau comme en déplacement. Le déploiement on-premise permet de conserver le contrôle sur l'infrastructure et les données, renforçant ainsi la souveraineté numérique. En choisissant des solutions open source basées sur des standards ouverts, elle bénéficie de transparence, flexibilité et indépendance vis-à-vis des fournisseurs, assurant la pérennité et l'adaptabilité de ses outils.


ZEROTRUST:
MAKE TRUST
GREAT AGAIN
TOUS ENSEMBLE !
TOUS ENSEMBLE !
fix

NOTES

NOTES

NOTES

HEXATRUST
5-7 rue Bellini, 92800 Puteaux
Date de publication : Février 2025
Les crédits : AdobeStock_908140124 - FIX Illustration

HEXATRUST

CLOUD CONFIDENCE & CYBERSECURITY

Retrouvez Hexatrust et ses membres :

www.hexatrust.com