ARC
DATA SHIELD

L'INTÉRÊT DE LA TECHNOLOGIE DE CLOISONNEMENT FORT POUR LA SÉCURITÉ DES ACTIFS CRITIQUES

OSSIR

PRESENTATION OSSIR
12 NOVEMBRE 2025

Par Arnaud COMBIER - ARC Data Shield

-I- ARC Data Shield: Présentation

ARC Data Shield développe et commercialise une gamme d'appliances réseau innovantes qui permet de protéger les actifs des attaques protocolaires comme les ransomwares.

Notre solution de rupture, brevetée, permet d'assurer la protection des attaques protocolaires de façon matérielle, par notre électronique dédiée, sans crainte de faille de type zero-days.

Arnaud COMBIER

Président fondateur

- fondateur et inventeur de la technologie
- 15 ans d'expérience en conduite d'études et informatique industrielle
- 10 ans d'expérience en cybersécurité des systèmes sensibles

MARINE NATIONALE — 4 ans

DGA DIRECTION GÉNÉRALE DE L'ARMEMENT

cea dam — 3 ans

Chronologie de l'Entreprise :

2018 — Lancement des travaux de recherche sur la technologie

2021 — Dépôt du brevet de la technologie au cœur du Digital Air Gap®

2022 — Création de la structure ARC Data Shield
Lancement R&D version commerciale

2023 — Sortie de la première version de présérie du Digital Air Gap®

2024 — Lancement de la version série du Digital Air Gap® et des versions Transfert et Sauvegarde

2025 — Accroissement du réseau de partenaires intégrateurs, évaluation de la solution en vue de sa certification ANSSI, lancement de la version protocolaire Modbus TCP.

2026 — Début de l'export sur les marchés européens.

ARC DATA SHIELD

Notre objet: sécuriser les biens des organisations

Dans le cadre de l'Industrie 4.0, la convergence entre l'IT et l'OT redéfinit le paysage industriel en favorisant une connectivité accrue entre les systèmes.

L’exposition des systèmes industriels aux risques cyber est de plus en plus importante. La sécurisation de l'interface entre ces deux domaines devient impérative pour faire face aux menaces émergentes dans le domaine de la cybersécurité.

Arrêt des systèmes	Corruption de données	Vol de données

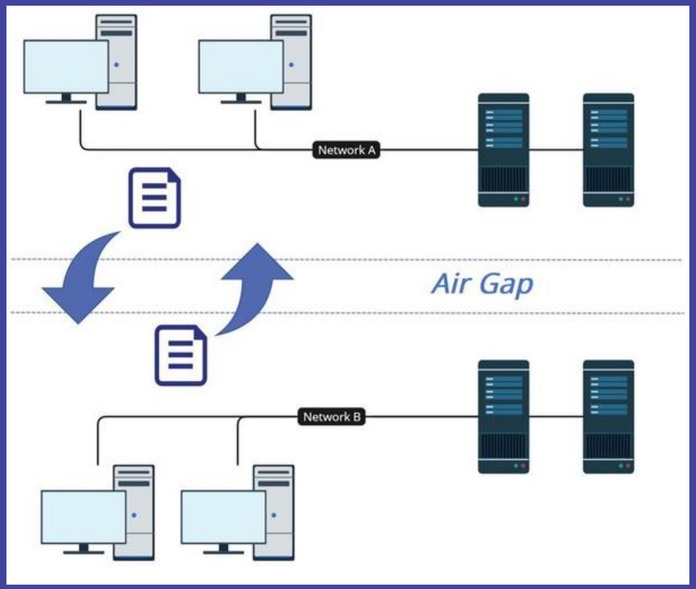
60% des RSSI des entreprises françaises estiment que les cyberattaques ont un impact direct sur le business. (CESIN)

Besoin d’une solution simple, robuste et performante pour protéger les actifs critiques matériels et immatériels des attaques protocolaires

-II- Le cloisonnement fort “Air Gap”

1-Le cloisonnement fort “Air Gap”: définition

Un cloisonnement fort ou air gap physique désigne une méthode d’isolation d’un système afin de le maintenir **sans flux de communication quel qu’il soit**, filaire ou non filaire.
Le système doit être déconnecté de tout réseau Ethernet, bus de données, moyens radio ou autre.



2-Segmentation réseau versus cloisonnement fort:

Le cloisonnement fort est donc très différent de la segmentation réseau :

- la segmentation réseau est basé sur des moyens de protection par séparation logique et filtrages pour rendre plus sûre l’utilisation de flux de communication.
- la segmentation structure le trafic en zones pour faciliter la sécurité et l’isolation fonctionnelle. Elle apporte différents mécanismes de séparation de flux pour retarder un attaquant, sa progression et latéralisation par une succession de moyens logiques successifs.

NOTA: Le but de la segmentation est de renforcer la protection des flux de données, alors que le but du cloisonnement fort est de protéger les actifs de toute attaque protocolaire.

3-Le cloisonnement fort “Air Gap”: historique et avantages

- 1970s–1980s — Origines : environnements militaires/nucléaires fermés, isolement physique par défaut.
- 1990s — Industrialisation : ICS/SCADA, premières data diodes et cloisonnements forts.
- 2000s — Connexion OT–IT : DMZ industrielles, guards/CDS, procédures de transfert outillées.
- 2010s — Choc ransomware/ICS : retour au hors-ligne discipliné et durcissement des processus.
- 2020s — Hybride : mix flux durci ou diodes physique + logique/opérationnel + immutabilité (WORM/Object Lock) pour les sauvegardes.

“Une solution de sauvegarde hors ligne reste considérée comme plus robuste qu’une solution WORM en ligne”

ANSSI - Sauvegardes des systèmes d’informations - les fondamentaux

4-Les avantages d’un Air Gap matériel:

- Réduction drastique de la surface d’attaque : pas (ou très peu) de chemins réseau exploitables, donc beaucoup moins d’intrusions possibles.
- Blocage des mouvements latéraux : même si un domaine est compromis, l’assaillant ne peut pas “rebondir” vers la zone isolée.
- Protection des sauvegardes et données critiques : les ransomwares ne peuvent atteindre et endommager des copies réellement isolées.
- Résilience accrue : continuité d’activité facilitée (les environnements isolés restent opérationnels en cas d’incident majeur côté IT).
- Maîtrise des échanges : chaque transfert est volontaire, contrôlé, journalisé et auditable.
- Réduction du risque interne : un compte ou un admin compromis ne suffit pas à atteindre la zone isolée.
- Conformité & gouvernance : répond aux exigences élevées (OIV/OCI, environnements classifiés,...)
- Simplicité du modèle : moins de dépendances et d’outils d’inspection continus côté réseau.

5-L’utilisation du terme Air Gap pour différentes technologies

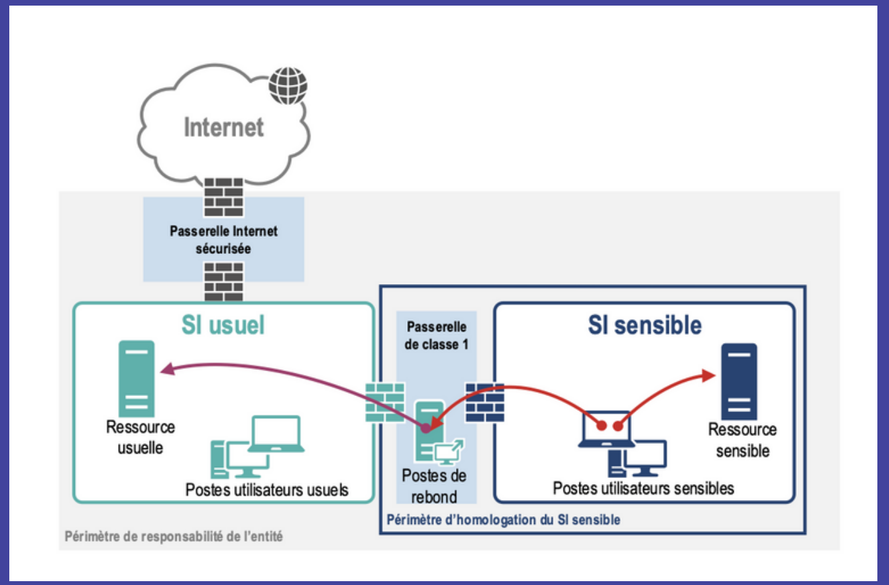
Sur le marché il est employé les termes “Air Gap”ou de cloisonnement réseau pour des technologies très différentes :

- Des solutions de segmentation réseau avec des fonctions logicielles d’immuabilité
- Des Air Gap Logiques: des passerelles avec des OS durci et des diodes logiques (logicielles)
- Des Air Gap physique temporaires: Des passerelles qui active un flux sur événements ou horaires définis.
- Des Air Gap partiels: des passerelles qui établissent un flux durci par une électronique à base de FPGA.
- Des Air Gap unidirectionnels: les diodes réseaux qui permettent la transmission de données dans un seul sens.

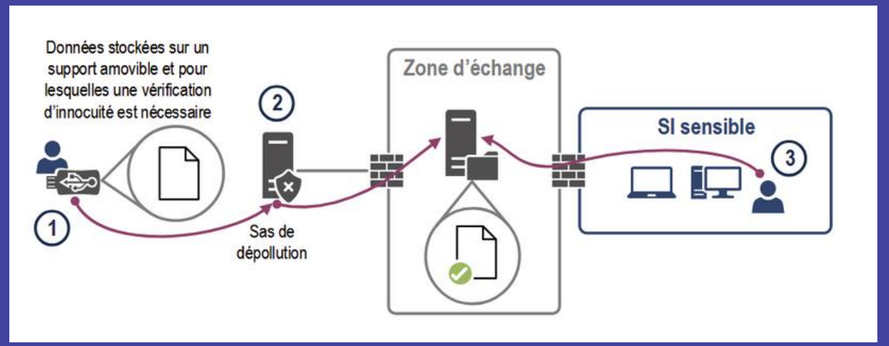
6-La protection de SI sensibles:

L'instruction interministérielle n° 901/SGDSN/ANSSI (II 901) les objectifs et les mesures de sécurité minimales relatifs à la protection des informations sensibles, notamment celles relevant du niveau Diffusion Restreinte (DR)

SI sensible: segmentation robuste avec une passerelle de classe 1



SI sensible: cloisonnement fort échanges par médias amovibles



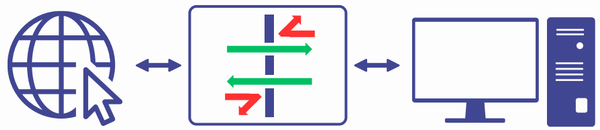
7-Les principales technologies de segmentation et cloisonnement matériel

Les solutions existantes:

PARE FEUX

- Niveau de sécurité +
- Coûts +
- Flexibilité +++

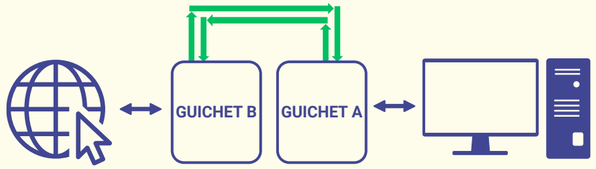
SEGMENTATION



PASSERELLE DE RUPTURE PROTOCOLAIRE

- Niveau de sécurité ++
- Coûts ++
- Flexibilité ++

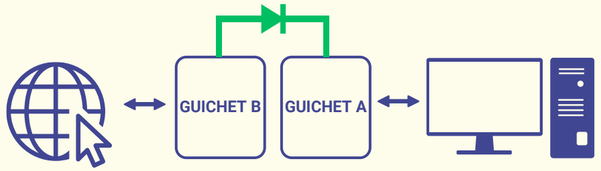
CLOISONNEMENT FORT PARTIEL



DIODES RÉSEAUX

- Niveau de sécurité +++
- Coûts +++
- Flexibilité +

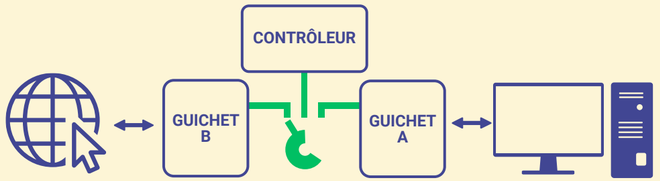
CLOISONNEMENT FORT UNIDIRECTIONNEL



DIGITAL AIR GAP

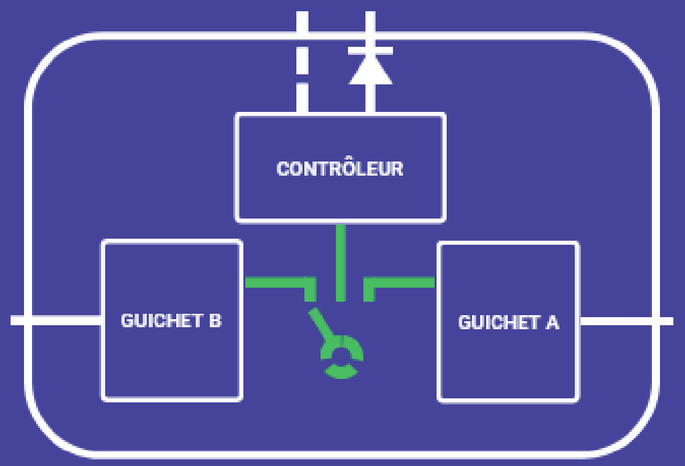
- Niveau de sécurité +++
- Coûts +
- Flexibilité +++

CLOISONNEMENT FORT TOTAL



-III- La solution Digital Air Gap:

La sécurité par conception



01

Un cloisonnement fort

Nos solutions Digital Air Gap garantissent un cloisonnement physique total entre les réseaux, permettant des transferts de données sans établir de communication directe, grâce à un système breveté de transfert.

02

Des échanges de données contrôlés

Le contrôleur isolé, situé entre les réseaux A et B, pilote les échanges de données tout en assurant des services de sécurité et de contrôle des flux.

03

Une sortie log indépendante et unidirectionnelle

Un port de sortie Syslog indépendant et unidirectionnel pour transmettre les journaux d'événements et d'actions réalisées sur la passerelle de manière sécurisée.

04

Une interface d'administration ergonomique

Un port d'administration indépendant avec une interface web dédiée, facilitant la configuration et l'administration du système.

ARC DATA SHIELD

AVANTAGES TECHNOLOGIQUES

Pare-feux

Coûts	+
Niveau de sécurité	+
Flexibilité	++
	+

Passerelle de rupture protocolaire

Coûts	+
Niveau de sécurité	+ +
Flexibilité	+ +
	+

Diodes réseaux

Coûts	+++
Niveau de sécurité	+++
Flexibilité	+

Digital Air Gap

Coûts	+
Niveau de sécurité	+++
Flexibilité	++
	+

STORMSHIELD

CISCO

FORTINET

paloalto NETWORKS

WatchGuard

seclāb

OWL Cyber Defense

CHAPSVISION DATA MAKE SENSE

THALES

FOX IT FOR A MORE SECURE SOCIETY

ARC DATA SHIELD

\+ : faible
++ : moyen
+++ : elevé

ARC DATA SHIELD

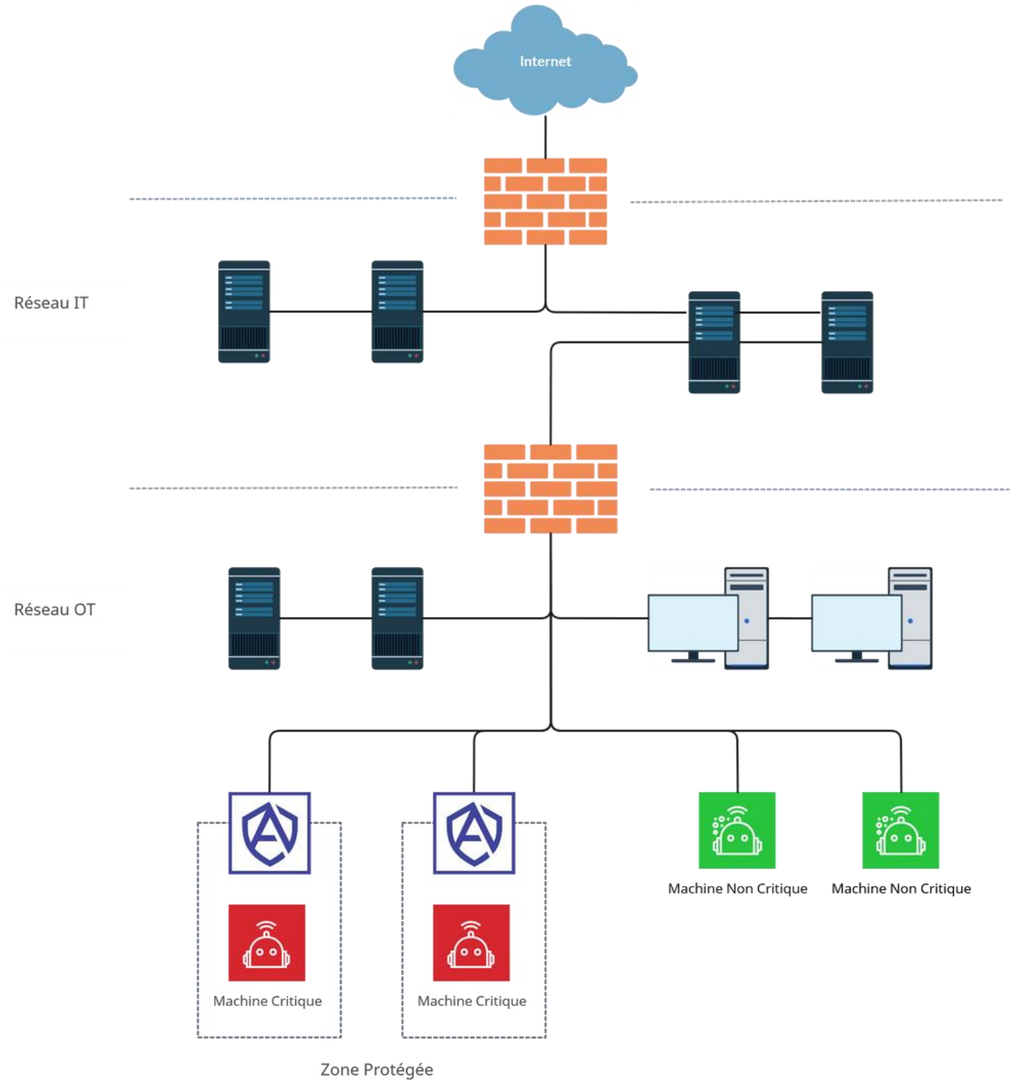
CAS D’USAGE

Protection équipement industriel

Apporter un cloisonnement fort et permettre uniquement les échanges de données autorisés

Protection des équipements industriels et médicaux:

- équipements conçus sans sécurité
- équipements ne supportant pas les mises à jour
- équipements ne supportant pas de solutions de sécurité
- équipements critiques



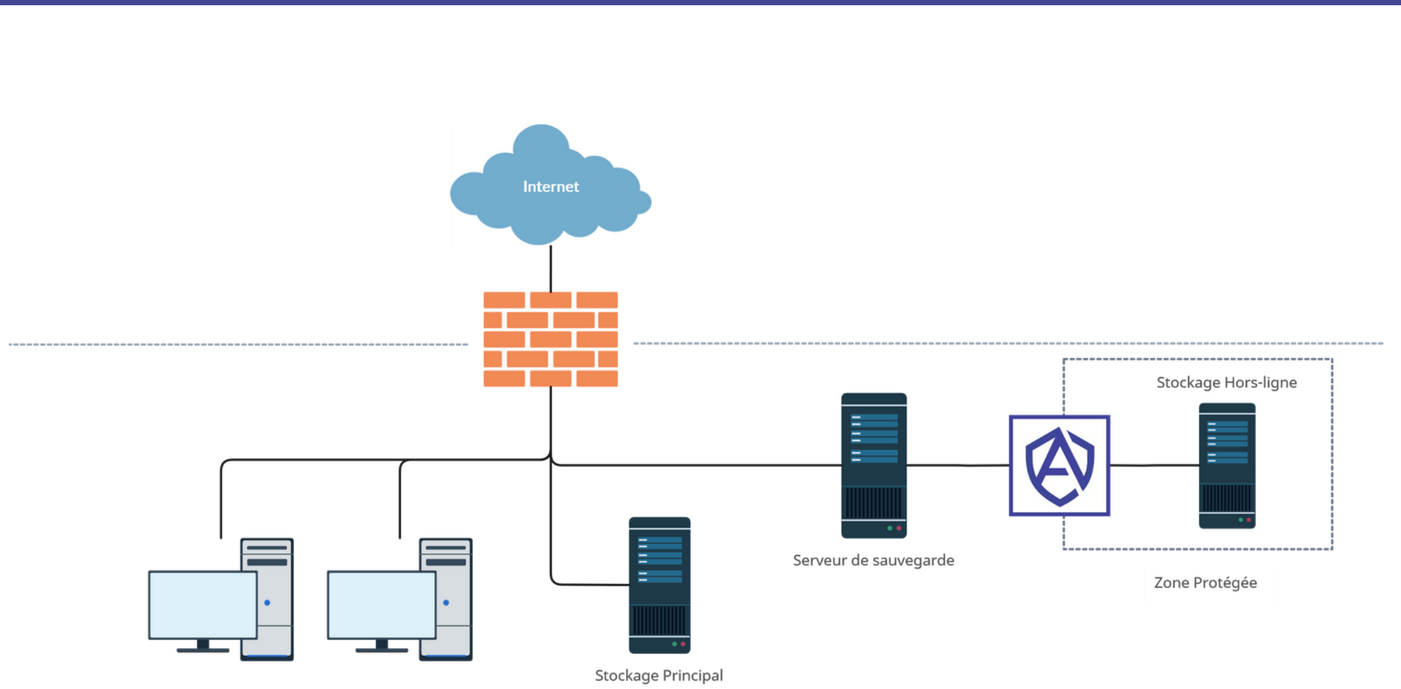
CAS D’USAGE

Protection des sauvegardes

Mise hors d’atteinte des copies de sauvegardes

Transfert dans un stockage hors réseau

- Mise hors d’atteinte y compris des postes d’administration (cas de postes compromis)
- Immuabilité des sauvegardes transférées



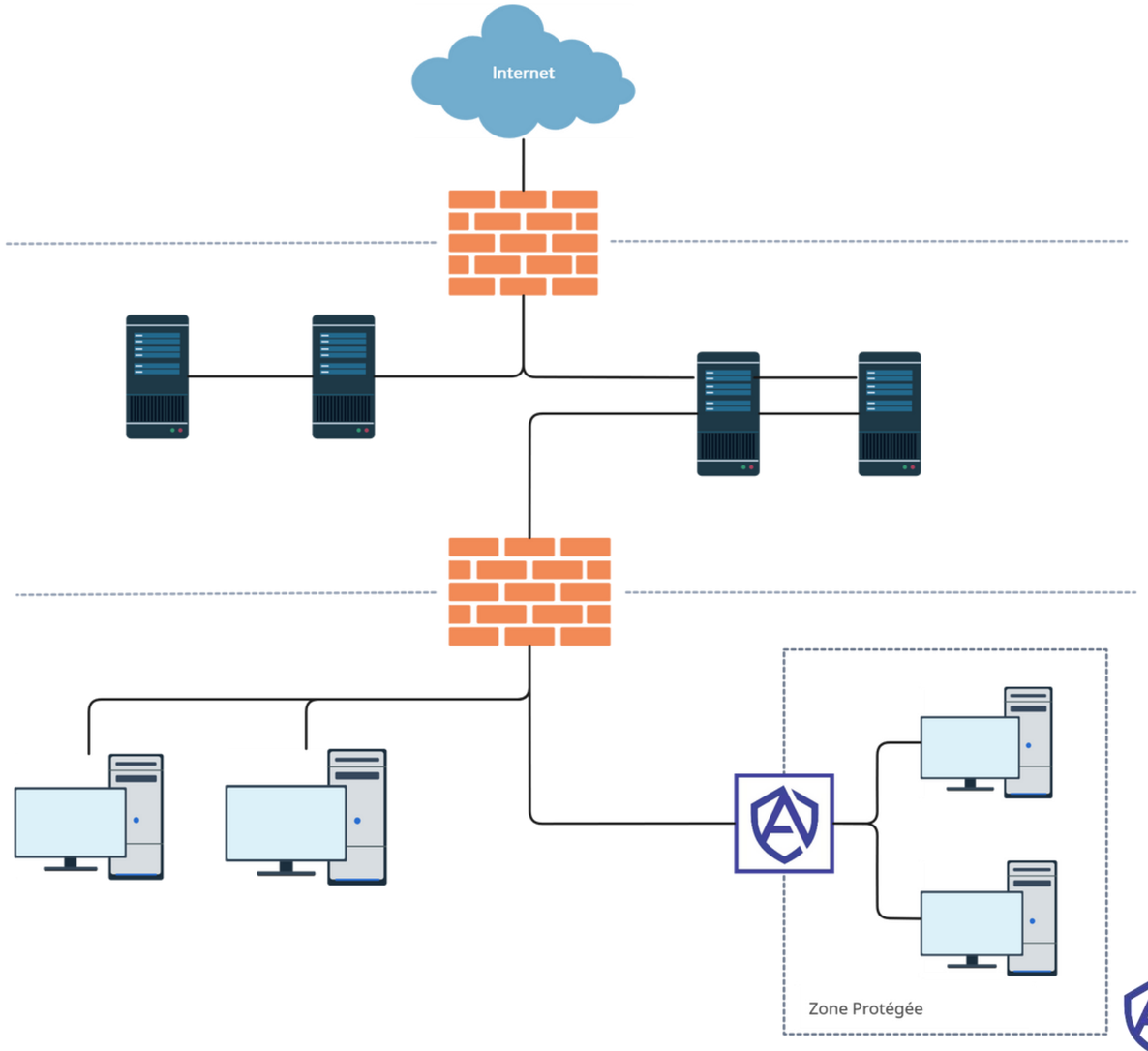
CAS D’USAGE

Protection R&D

- Cloisonnement fort de réseaux hébergeant des informations confidentielles
- Modules logiciels additionnels pour répondre aux différent besoins: analyse antivirale, contrôle de type, chiffrement/déchiffrement, contrôle de signature...

Éliminer les erreurs et contraintes opérationnelles:

- Déchiffrement et analyse de toutes les données entrantes en environnement isolé avant transmission au réseau à protéger
- Chiffrement de toutes les données sortantes pour assurer une confidentialité sans faille



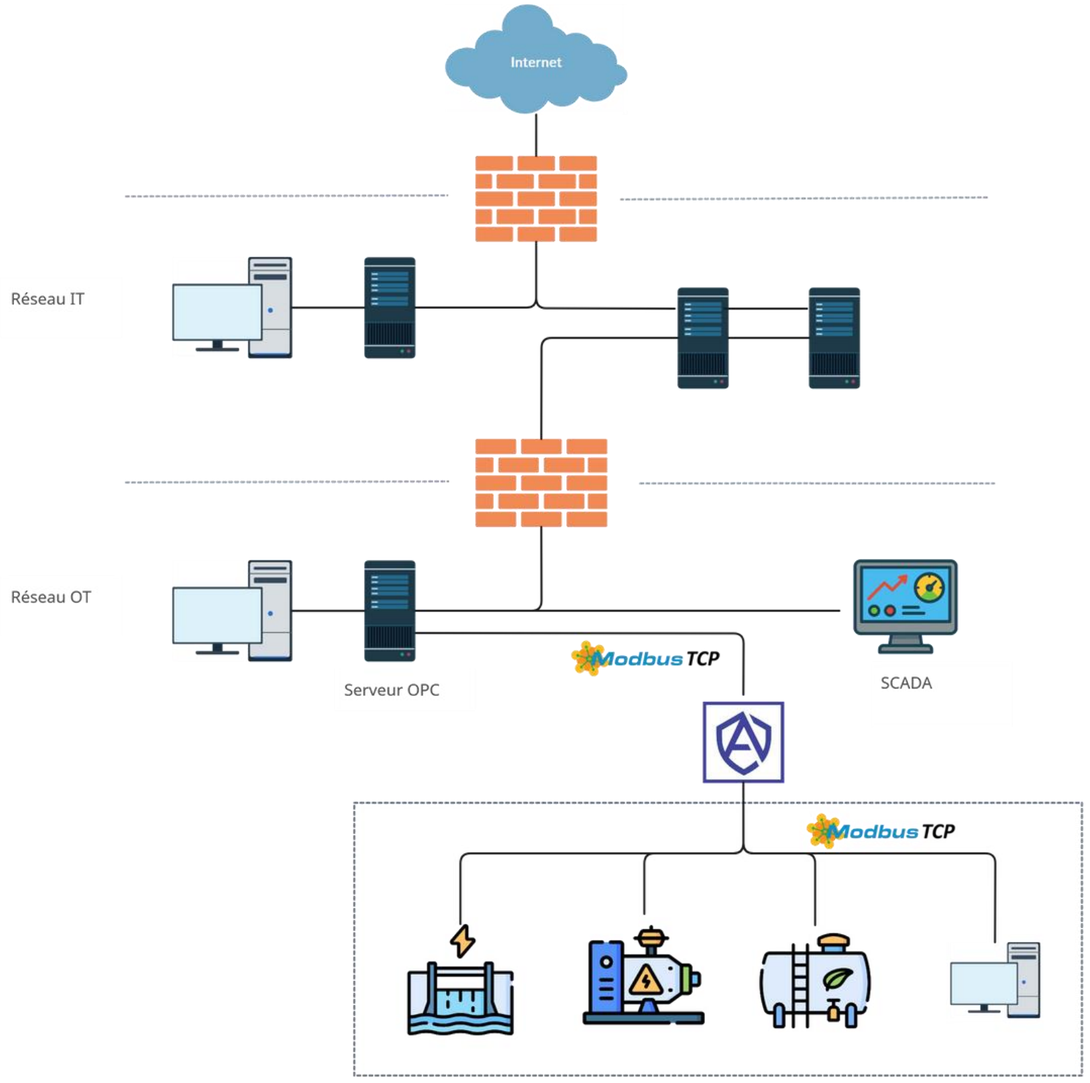
ARC DATA SHIELD

- Protège les contrôle-commandes de toute attaque protocolaire y compris de corruption des moyens de supervision SCADA.
- Protection de l’intégrité des programmes et données des automates industriels

CAS D’USAGE

Modbus TCP: Protection des contrôle-commandes critiques

Protection des contrôle-commandes critiques des attaques protocolaires et de toute corruption du fonctionnement



Réseaux des équipements critiques protégés

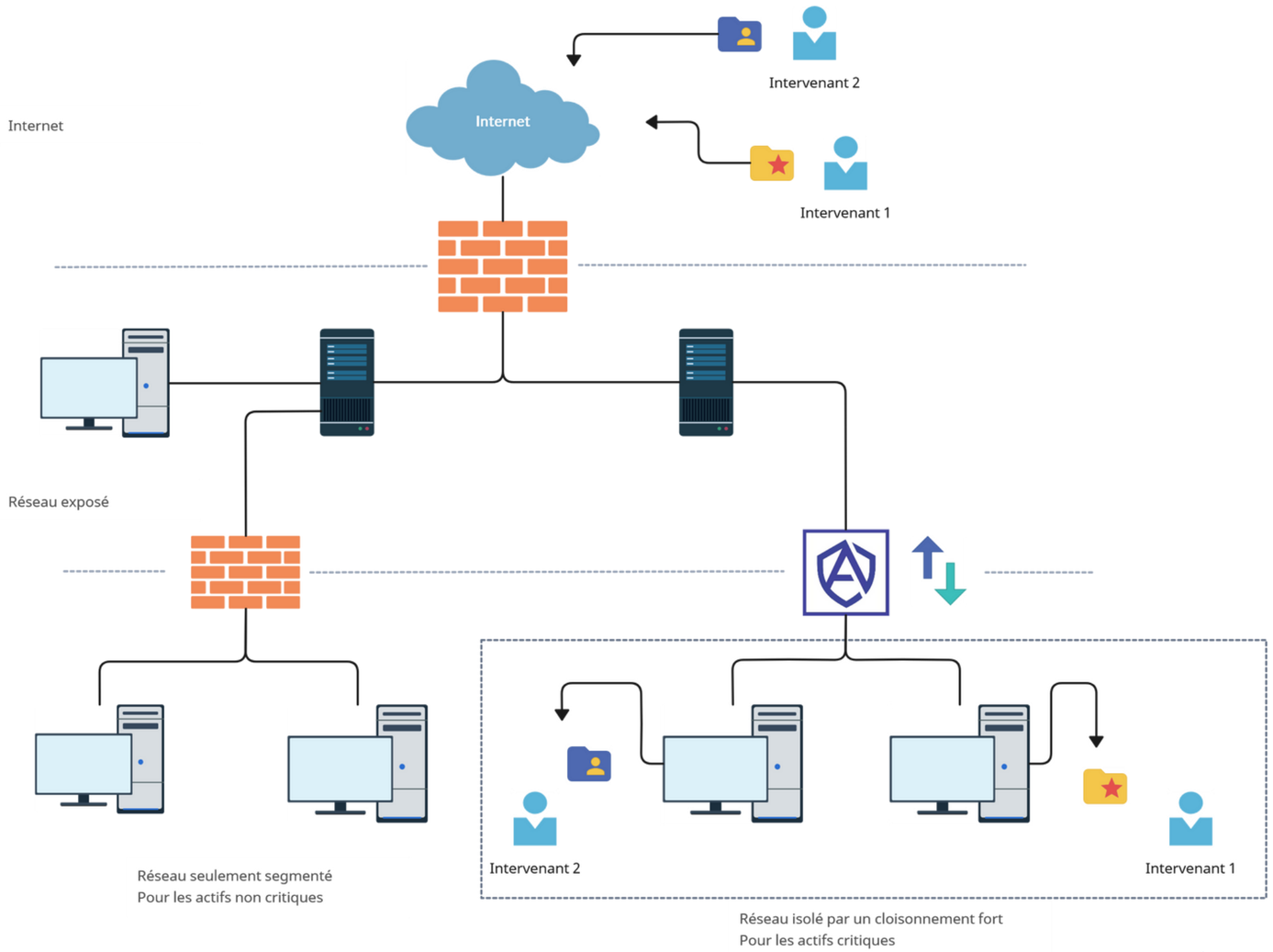
ARC DATA SHIELD

CAS D'USAGE

Station blanche réseau

- Automatisation des transferts depuis des accès Internet nominatifs et sécurisés pour déposer / récupérer sur le guichet extérieur des données en fonction des droits alloués
- Contrôle multiple des données à échanger entre les 2 réseaux.
- Mise à disposition des données autorisées dans des partages dédiés du réseau sécurisé.
- Élimination des erreurs de transfert manuel et gain de temps considérable pour les équipes d'administration.

Maîtriser les données entrantes et sortantes des intervenants réalisant des prestations sur vos réseaux tout en conservant l'isolation.



Notre modèle Digital Air Gap PRO ONE

L'équilibre coût / performance optimisée

Une appliance conçue autour de composants sélectionnés pour leur efficience, sécurité et fiabilité.

Une interface d'administration simplifiée

Un port d'administration indépendant des 2 réseaux A et B avec une interface web conçue pour faciliter la configuration.

Une sortie log indépendante et unidirectionnelle

Une sortie de log au format Syslog unidirectionnelle pour transmettre les journaux d'événements et d'actions réalisées par la passerelle.

Nos services complémentaires

Modules de services logiciels

Un catalogue étendu de modules de services optionnels pour répondre à tous vos besoins et cas d'usages.

Service support

Accès aux mises à jour logicielles
Hotline de support
Expédition express d'un produit de prêt en cas de panne matérielle
Extension de garantie jusqu'a 5 ans

Protégez vos actifs critiques, contactez-nous :

Notre valeur ajoutée

- Sécurité matérielle permanente
- Cloisonnement fort assuré
- Echanges contrôlés
- Intégration simplifiée
- Longue durabilité

ARC Data Shield

www.arc-data-shield.fr
contact@arcds.fr

MADE IN FRANCE

ARC Data Shield SAS – 1 Rue du Château de Bel Air 44470 CARQUEFOU – FRANCE