heliaq
Solutions

COMMENT MAÎTRISER LES ACCÈS À PRIVILÈGES ET RÉDUIRE VOS RISQUES AVEC HELIAQ

Sécurisez vos comptes à privilèges avant qu'il ne soit trop tard

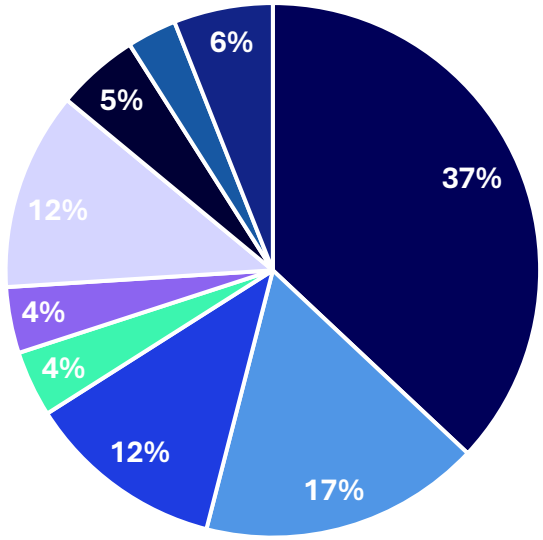
1

Contexte de la menace

heliaq
Solutions

Panorama de la cybermenace 2024

Répartition des victimes d'attaques par le biais de rançongiciels



- PME/TPE/ETI
- Entreprise stratégique
- Association
- EPA, EPIC (1)
- Autre
- Collectivité territoriale/locale
- Etablissement de santé
- Etablissement d'enseignement supérieur
- Ministère

(1) Établissement public administratif / industriel et commercial

3,8M€

Le coût moyen d'une violation de données pour une entreprise en France (perte de productivité, réparation des systèmes, impacts réputationnels)

93%

Des actions malveillantes répertoriées en 2025 reposent sur seulement dix techniques principales. Parmi elles, l'exfiltration de données chiffrées et l'injection de processus furtifs

86%

Des incidents et signalements transmis à l'ANSSI entre janvier 2022/décembre 2023 dans le secteur de la santé concernaient des établissements de santé

47%

Des données professionnelles hébergées sur le cloud peuvent être considérées comme sensibles

Sources :
Panorama de la cybermenace 2024- ANSSI
CERTFR-2024-CTI-010 – Secteur de la Santé
CERTFR-2025-CTI-001 – Cloud Computing

2

Cybersécurité – Notre démarche

Un défi complexe et dynamique

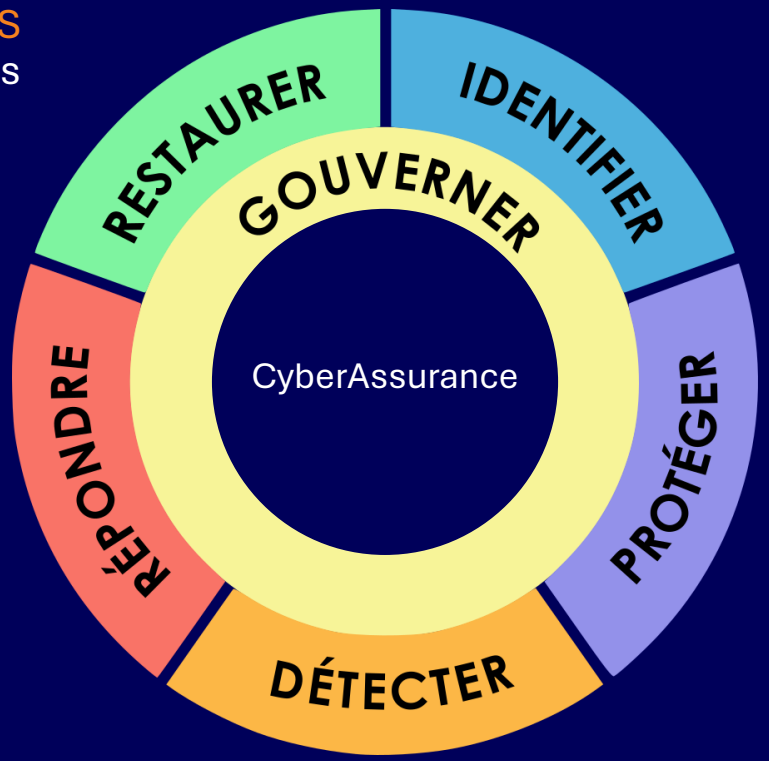
heliaq Solutions

Notre démarche maîtrisée pour une protection 360°

*L'offre **Heliaq SECaaS** est locative et comprend un socle de base (matériels et logiciels / licences) et s'appuyant sur une équipe d'experts dédiés à la sécurité.*

Backup aaS
Disaster Recovery aaS
Backup On Premises

Audits techniques (exposition, pentest…)
Audits de Gouvernance
Audits de maturité SSI
Audits de conformité / certification ISO 27001
AuditsCyber+ : exposition, vulnérabilités, intrusion, M365, AD, Dark Web, Maturité SSI



Audit Forensique
Gestion de crise
CyberRescue (CSIRT)

CyberPhish
SecMails
Firewalling aaS
Network aaS
EDR Managed
CyberPam

Phishing, PAM, filtrage mail, Firewall, WAF, SSE, SASE, DLP, MDR, MFA, UEM, Wi-Fi, AD, Patching, …

Security Operations Center

Orange : offres OPEX « as a Service »
Blanc : mode projet

heliaq Solutions

Comptes à privilèges – C’est quoi ?

Définition - Rappel

Un **compte privilégié** est un compte d'utilisateur d'une entreprise qui **dispose de privilèges élevés**, c'est-à-dire qu'il dispose **d'autorisations** et de **droits d'accès aux systèmes**, aux bases de données, aux applications et à l'infrastructure réseau de l'entreprise que la majorité des autres utilisateurs n'ont pas.

Ces comptes figurent **toujours** parmi les principales cibles des attaquants

Il est **IMPERATIF** de mettre en place une solution de gestion des accès à privilèges (PAM)
pour **protéger ces comptes critiques**

3

Cyberattaques
→ Exemples concrets

Utilisation d’un compte à privilèges forts

heliaq
Solutions

Exemple N°1 – Attaque d'une Mairie de 3200 habitants

150.000€ de préjudice évité

En mars 2015, la Mairie en question a découvert une **cyberattaque d'ampleur** et échappe In Extremis à un préjudice de 150k€ :

- Réception **d'un mail avec pièce jointe frauduleuse** par un agent de la mairie
- **Exécution** de la pièce jointe par cet agent !
- **Installation d'un logiciel malveillant** et récupération du **compte à privilège du DGS** (Directeur Général des Services)
- **Prise de contrôle total** des systèmes informatiques de la Mairie – Tentative de commandes à des fournisseurs
- **Usurpation** d'identité du DGS auprès des fournisseurs

Ce qu'il faut retenir :

- Avant tout chose : Il **faut FORMER les utilisateurs du SI** client aux risques Cybers (Campagnes de Phishing et e-Learning)
- Le compte du DGS avait-il « **trop** » de privilèges ?
- Les **comptes à privilèges doivent être protégés**. Même en interne au sein du SI

Exemple N°2 – Cyberattaque contre un Hôpital Privé (60k patients)

Entre 120.000 et 530.000 dossiers patients « volés »

En juin 2025, l'hôpital privé s'est vu **voler plusieurs milliers de dossiers patients** via un compte à privilège :

- **Exploitation d'une faille** d'un logiciel interne
- Récupération d'un **identifiant à privilège octroyé à un médecin**
- 120.000 à 530.000 dossiers patients **volés** (Noms, adresses, numéros de Sécurité Sociale, dates naissance, etc…)
- **Fuite massive** de données personnelles et de santé

Ce qu'il faut retenir :

- **Une seule** compromission est suffisante !
- Réfléchir à donner des **accès à privilèges à un médecin** !?
- Etudier et **protéger** ces accès à privilèges

Exemple N°3 – Attaque d'un groupe Hôtelier en 2018 (2053 établissements)

Violation des données de 500 millions de clients !

En novembre 2018, le groupe Hôtelier annonce une **importante violation de données concernant 500 millions de leurs clients**

Scénario des Cyberattaquants :

- Accès au **compte à privilège du fournisseur tiers** ayant les accès à la base de données de réservation du groupe
- Introduction au réseau du groupe et **déplacements latéraux**
- **Augmentation des privilèges** en interne (Via Active Directory) avec la technique « pass-the-hash »
- Installation de **logiciels malveillants** et vols des données **pendant 4 ans** ! (Dont les documents financiers)

Ce qu'il faut retenir :

- Cette attaque **ne visait pas le groupe hôtelier au départ** mais bien son fournisseur
- Les comptes d'accès « aux clients » de ce fournisseur **n'étaient pas protégés**
- Enfin, ce fournisseur accédait à son client sans protection des comptes à privilèges !

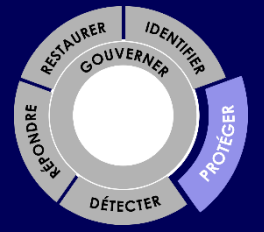
Double responsabilité :

- **Non protection des comptes** du client du fournisseur
- **Non protection des accès** des fournisseurs chez le client

4

Un Bastion ? C’est Quoi ?

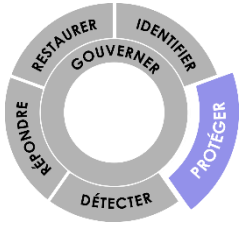
Rappels - Définitions



heliaq
Solutions

Privileged Acces Management – Qu’est ce qu’un « PAM »

Gestion des accès à privilèges



Objectifs : **Sécuriser, surveiller et contrôler l’utilisation des comptes à privilèges**

But : **Protéger les comptes ayant des droits d'accès élevés** représentant une cible de choix pour les cyberattaques.

Comment : En limitant, en enregistrant et en surveillant les accès de ces comptes

- **Réduire la surface d’attaque** en limitant les accès privilégiés aux seuls utilisateurs et aux moments nécessaires
- **Contrôler l'accès** via l’authentification forte avec une approbation préalable
- **Auditer et surveiller les sessions privilégiées** pour détecter des comportements anormaux ou malveillants
- **Sécuriser les mots de passe** via des coffres-forts numériques qui automatisent leurs changements réguliers

Fonctionnalités :

- **Gestion des comptes** à privilèges
- **Coffre-fort** à mots de passe sécurisé
- **Session management** (enregistrement vidéo des sessions, contrôle en temps réel)
- **Contrôle d’accès granulaire** (qui peut accéder à quoi, quand et comment)
- **Audit** et traçabilité complète

5

La solution Heliaq Cyber**PAM**

Une solution simple avec un partenaire reconnu

heliaq Solutions

wallix

Présentation de la solution WALLIX PAM

Solution de gestion des accès à privilèges

Fonctionnalités principales d'une solution PAM :

- Gestion d'un **workflow** de demandes d'accès avec processus d'approbations automatisés
- **Proxy** d'accès avec **enregistrement et surveillance** (traçabilité et enregistrement de toutes les activités)
- **MFA** et **SSO** pour une sécurité renforcée

Pourquoi déployer une solution PAM ?

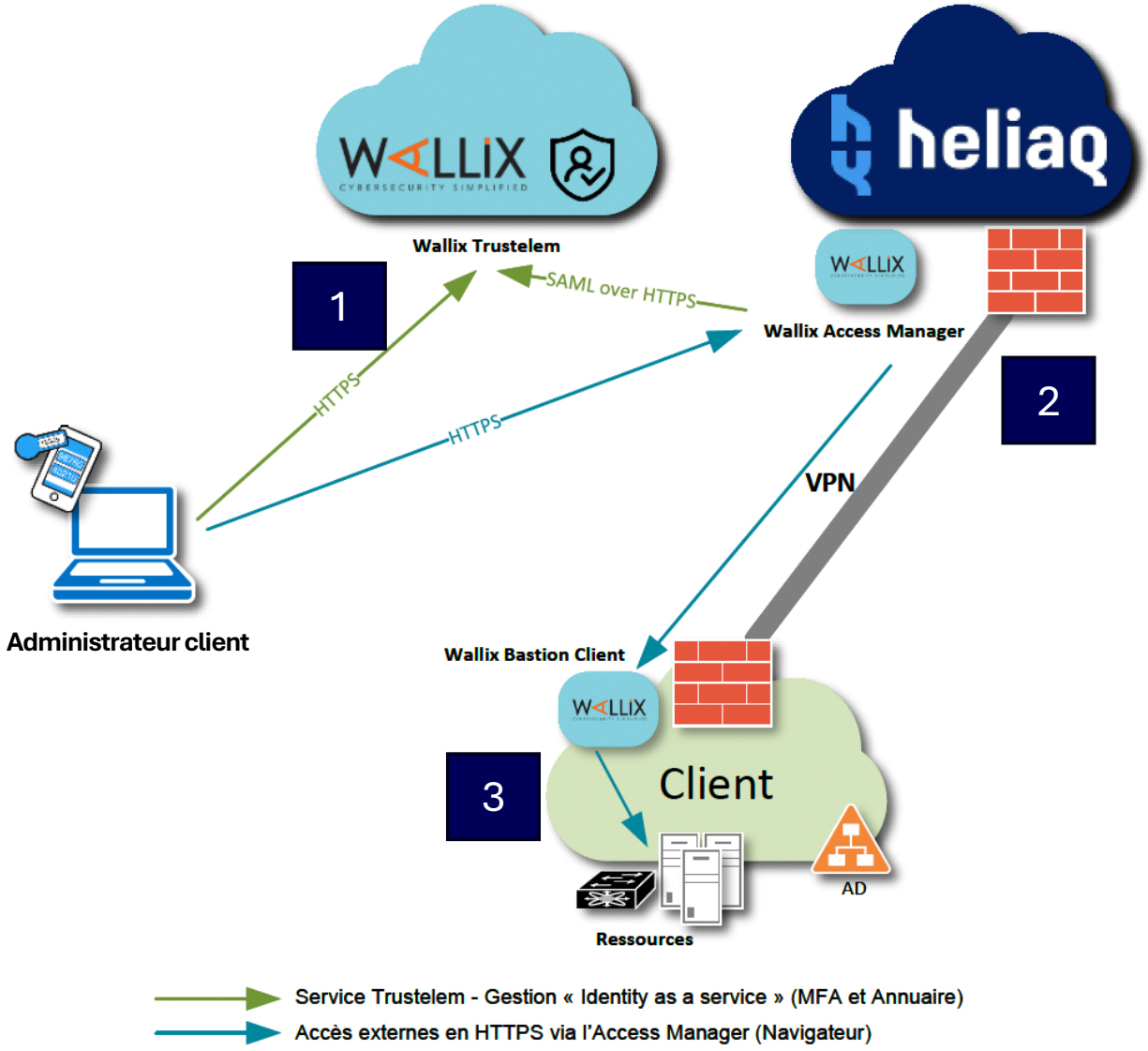
- **Réduction des risques** de sécurité liés aux comptes privilégiés
- Conformité aux **normes** réglementaires (RGPD, ISO 27001, ...)
- **Détection** des comportements anormaux et **prévention** des menaces
- Déploiement **possible sur tout type d'infrastructure**
- Choix de Wallix → Solution **souveraine et reconnue**

Les solutions WALLIX sont reconnues par les principaux analystes du secteur

Gartner FORRESTER® kuppingercole ANALYSTS FROST & SULLIVAN

Présentation de la solution WALLIX PAM

Solution de gestion des accès à privilèges

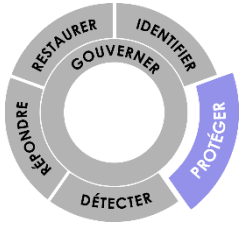


Processus d'accès :

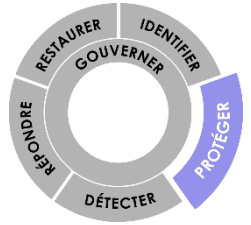
1. **Validation** de **l'authentification** avec **MFA** au travers de Trustelem
2. **Accès** à l'Access Manager qui **envoie les informations d'authentification au Bastion client** via un tunnel VPN IPSec
3. **Accès** aux ressources à administrer **via le Bastion** Client, toujours à travers du même tunnel VPN IPSec

Présentation de la solution CyberPAM

Points essentiels



Pourquoi Heliaq ?



1 PROTEGER LES ACCES DES COMPTES A PRIVILEGE

Mise en place d'une solution fiable et reconnue permettant ces contrôles

Solution complète incluant le coffre-fort et l'enregistrement des sessions

LE + : Une solution souveraine et reconnue par les organismes de certifications

2 SERVICES MANAGES, PILOTAGE ET SUIVI

Solution surveillée et mise à jour régulièrement

Une assistance illimitée des équipes de Cybersécurité d'Heliaq Solutions

LE + : Une surveillance 24/7 et une équipe à votre disposition

3 ET PLUS ENCORE

Une solution à la carte adaptable à votre SI et vos usages

LE + : tout est inclus → Licences, services, stockage des logs et des enregistrements, le service…

MERCI !

heliaq
Solutions