Key Insight Brief

3 Stratégies
pour un accès distant sécurisé dans les environnements industriels

wallix

Le support à distance révolutionne l'efficacité opérationnelle dans les environnements industriels. Du diagnostic à la surveillance continue, en passant par le transfert de fichiers et au dépannage, la demande pour des solutions ayant besoin d'accès distant robuste est plus élevée que jamais.

Cependant, sécuriser les accès distants n'est pas une mince affaire, c'est un puzzle complexe qui nécessite une réflexion stratégique globale.

Soyez le champion de la gestion des accès distants

Il est évident qu'on ne peut plus se passer d'intervention de tiers à distance!

Cependant, le déploiement rapide et parfois désorganisé de passerelles VPN par les fabricants et les prestataires externes a considérablement augmenté la surface d'attaque des réseaux industriels.

Cette situation oblige les organisations industrielles à équilibrer l'efficacité opérationnelle avec le besoin de solutions de cybersécurité efficaces.

Mais **sécuriser l'accès distant n'est pas un jeu d'enfant**. C'est vaste et complexe, et parfois, on peut se retrouver perdu sans savoir par où commencer.

Ce qui pourrait vraiment aider à ce stade est de mettre en place un plan d'actions solide. Et pour simplifier encore plus, nous l'avons décomposé en **trois stratégies simples.**

01 Mise en œuvre du cadre de sécurité Zero Trust

Vous avez probablement entendu parler de « Zero Trust ». Le concept peut vous sembler familier, et si vous ne l'avez pas encore mis en œuvre dans votre organisation, n'attendez plus! Zero Trust est désormais un incontournable!

Contrairement aux modèles de sécurité traditionnels qui assurent la confiance au sein d'un périmètre réseau, **l'architecture Zero Trust nécessite une vérification continue** de tous les utilisateurs et dispositifs, quel que soit l'endroit d'où ils accèdent au réseau.

Cette stratégie garantit que seuls les personnes authentifiées et autorisées peuvent accéder à des ressources réseau spécifiques.

Mais par où commencer ?

Il est de coutume d'évaluer et de cartographier tous vos actifs et ressources réseau dans un premier temps pour avoir une image claire de votre environnement. Mais dans le même temps il est **indispensable de déployer la 1ère brique de votre sécurité pour verrouiller l'entrée dans votre réseau** de production. Mettez en place des **contrôles d'accès granulaires avec outil de gestion des privilèges (PAM).** Cela vous permettra en plus d'assurer la vérification continue pour surveiller et auditer continuellement l'accès et l'activité réseau.

Pourquoi tous ces efforts ? Les avantages parlent d'eux-mêmes :

> **Réduire** significativement les accès non autorisés**.**

> Améliorer la **visibilité et le contrôle** des activités sur votre réseau de production.

> Empêcher le **mouvement latéral** des attaquants d'une machine à une autre.

02 Centraliser et Unifier pour Simplifier

Le **déploiement d'un point d'entrée unique** pour accéder à vos systèmes OT est clef. Cette approche simplifie les connexions extérieures, éliminant ainsi le besoin de multiples accès VPN non contrôlés.

Cependant, cela doit être fait avec des **outils conviviaux** qui s'alignent parfaitement sur les processus OT existants pour garantir une sécurité fluide **sans perturber la production**.

C'est précisément ce que fournissent les outils de gestion des accès à privilèges (PAM) dont les objectifs principaux sont de :

> **Isoler** votre environment de production avec la **rupture protocolaire** gérée par un PAM centralisé

> **Traçabilité** de toutes les connexions distantes, quelque soit son origine (prestataire de services, fabricant, équipe internes, etc**.**

> **Surveiller** ce que la personne authentifiée fait sur les cibles.

> **Restreindre l'accès** à des zones spécifiques ou à des équipements pour éviter les actions non autorisées.

> **Gestion déléguée** des comptes utilisateurs pour laisser les équipes de production ajouter en temps reel des tierces persones (WALLIx One RA)

03 Surveillance continue et detection des anomalies

Pourquoi est-ce si important ?

Parce qu'utiliser des outils de cybersécurité centralisés avancés pour **détecter des activités inhabituelles ou des violations en temps réel** permet de réagir rapidement avant que des dommages significatifs ne

Intégrez des solutions d'analyse comportementale et de détection d'anomalies. Configurez des alertes en temps réel pour les activités suspectes ou non autorisées, tout en remontant ces informations au sein d'un SIEM (Security information and event management) afin de renforcer la gestion des accès et minimiser les risques liés aux privilèges excessifs.

Intégrez des solutions d'analyse comportementale et de détection d'anomalies. Configurez des alertes en temps réel pour les activités suspectes ou non autorisées.

La surveillance continue permet de :

> **D'enregistrer** au travers de logs l'ensemble des évènements,

> Détecter les attaques tôt. Couplée avec un SIEM, il devient facile de **stopper les menaces** avant qu'elles ne causent des dommages.

> **Analyser les** événements pour améliorer la posture de sécurité..

> **Être conforme aux normes** de plus en plus nombreuses (NIS2, IEC 62443, ISO 27001, etc.

Etude de cas

Un fabricant de vêtements de travail de haute qualité protège ses serveurs critiques et son infrastructure, assurant des opérations fluides et une fiabilité inégalée.

Voulez-vous connaître les mesures qu'ils ont prises ?

La suite à la prochaine page...

Comment un Engelbert Strauss a sécurisé ses serveurs et ses automates

Prenons l'exemple d'Engelbert Strauss, un fabricant renommé de vêtements de travail de haute qualité. Avec une infrastructure étendue comprenant **80** équipements, **1 200** employés et **10** sites, ils ont dû faire face à plusieurs défis pour l'implémentation de leur cybersécurité :

> **Infrastructure** : Garantir que leur environnement de production reste fiable et protégé.

> **Gestion des mots de passe et des identités** : Établir un système robuste de gestion des mots de passe et des identités pour les utilisateurs externes et internes.

> **Expérience utilisateur** : Rationaliser les procédures pour offrir une expérience utilisateur fluide.

Quelle solution pour répondre à ces défis?

Tout d'abord, Engelbert Strauss et WALLIX avons centralisé le contrôle et la surveillance de tous les accès distants ayant accès aux actifs critiques de la société.

Engelbert Strauss peut ainsi garder un œil attentif sur **qui accède à quoi**.

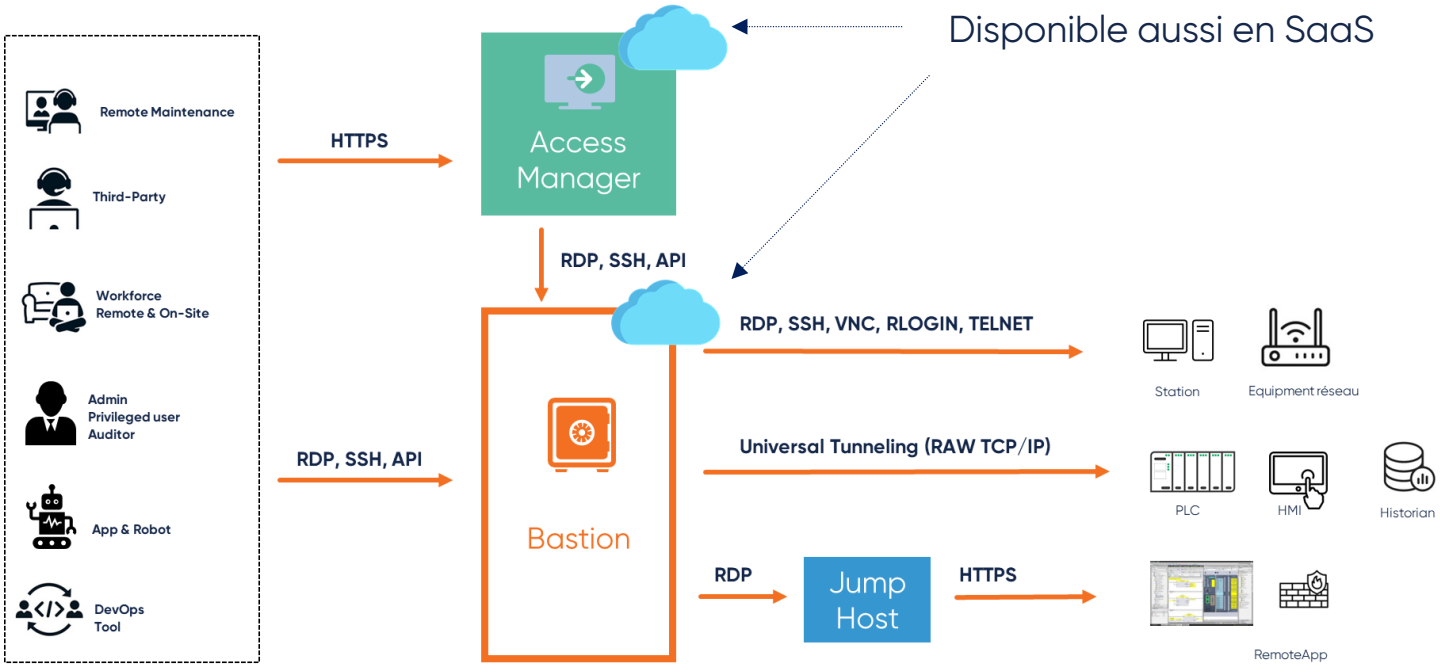
WALLIX a également intégré son système de gestion des accès à privilèges (PAM) avec le système existant de gestion des événements et de la sécurité (SIEM). Cette intégration était cruciale pour contrôler aux l'accès différents systèmes de l'entreprise pour des utilisateurs distants.

Principaux avantages de la solution :

> **Utilisation plus efficace** des ressources du département informatique

> Meilleur **contrôle et surveillance** de l'accès aux serveurs

> Très peu de demandes de support



Coralie JESUS

› Sales Manager

Bonjour ! J'espère que le résumé que j'ai préparé vous a été utile. Mais qui suis-je ? Je suis Coralie, votre interlocutrice chez WALLIX.

Alors, pourquoi ai-je préparé cela ? Mon objectif était de mettre en évidence les **grands changements que la transformation numérique** apporte dans le secteur de l'industrie.

Je reviendrai bientôt avec des témoignages spécifiques de nos clients dans votre secteur unique et sensible !

Questions? Partagez-les

wallix

Éditeur de logiciels de cybersécurité, WALLIX est le spécialiste européen de la sécurisation des accès et des identités numériques. Les technologies de WALLIX permettent aux entreprises de répondre aux enjeux actuels de protection des données. Elles garantissent la détection et la résilience aux cyberattaques permettant ainsi la continuité d'activité. Elles assurent également la mise en conformité aux exigences réglementaires concernant l'accès aux infrastructures informatiques et aux données critiques. WALLIX s'appuie sur un réseau de plus de 300 revendeurs et intégrateurs à travers le monde. Cotée sur Euronext (ALLIX), WALLIX accompagne plus de 2000 organisations dans la sécurisation de leur transformation numérique.

› 250 bis, rue du Faubourg Saint-Honoré
75008 Paris, France

› +33 1 53 42 12 81

› contact@wallix.com