BeyondTrust

Évaluation de la cybersécurité des technologies opérationnelles (OT)

Identifier et traiter les risques de sécurité des accès à distance et de conformité pour vos systèmes OT.

Le paysage des technologies opérationnelles a évolué

Pendant de nombreuses années, les systèmes industriels se sont appuyés sur des protocoles et des logiciels propriétaires. Ces solutions existantes manquaient d'automatisation, nécessitaient une administration manuelle par le personnel et ne disposaient d'aucune connectivité externe.

Aujourd'hui, le paysage des technologies opérationnelles (OT) est bien différent. De plus en plus de systèmes industriels sont connectés non seulement pour adopter de nouvelles fonctionnalités et de l'efficacité grâce à des intégrations technologiques, mais également pour fournir du big data et des analyses intelligentes. Ces systèmes modernisés nécessitent un accès à distance de la part des fournisseurs, des employés, des opérateurs, des prestataires et des sous-traitants qui travaillent hors-site.

Cette transition de systèmes isolés vers des systèmes connectés a généré une série de nouveaux risques pour la sécurité. Les cyberattaques contre les infrastructures critiques n'ont jamais été aussi nombreuses. Au cours de l'année écoulée, 89 % des entreprises des secteurs de l'électricité, du pétrole et du gaz, ainsi que de la fabrication ont subi des cyberattaques qui ont compromis la production et l'approvisionnement en énergie. Par ailleurs, 72 % d'entre elles déclarent avoir subi des perturbations informatiques dans leurs environnements ICS/OT au moins six fois au cours de l'année.[1]

Pour mieux faire face aux risques engendrés par l'adoption du cloud, la transformation digitale, le télétravail et l'interconnectivité croissante, les entreprises et les organismes gouvernementaux adoptent les principes du Zero Trust. Pourtant, près de 80 % des organisations d'infrastructures critiques n'ont pas adopté de stratégies de Zero Trust.[2]

Permettre un accès à distance sécurisé et faire respecter les principes du Zero Trust à vos systèmes OT est essentiel pour maintenir la productivité et la continuité des activités de votre organisation.

« La gestion des cyber-risques liés aux employés connectés travaillant à distance est une question urgente et exige des améliorations des programmes de cybersécurité industrielle IT et OT existants. Les approches VPN et RPC conventionnelles n'offrent pas la sécurité nécessaire et sont trop difficiles à gérer. Les employés connectés ont besoin du Zero Trust dans tous les systèmes et ressources industriels.

Les employés connectés travaillant dans des milieux industriels ont besoin du Zero Trust. ARC View. 11/2021

Gestion de la sécurité des accès à distance

Aujourd'hui, les employés à distance et les fournisseurs tiers utilisent de plus en plus d'ordinateurs portables personnels et d'autres périphériques (comme dans le cas du dispositif « Bring Your Own Devices », ou BYOD) pour se connecter à distance aux systèmes OT à partir de leurs réseaux domestiques, qui disposent de moins de contrôles de sécurité qu'un environnement d'entreprise. **Ces connexions à distance ont rendu floue la segmentation IT-OT et élargi la surface d'attaque en créant de nouveaux points d'entrée que les hackers peuvent exploiter.**

Les systèmes industriels étant de plus en plus connectés, ils sont également de plus en plus exposés aux vulnérabilités. Bien que les VPN soient efficaces pour fournir un accès à distance de base aux systèmes non sensibles, ils ne disposent pas des fonctions de sécurité avancées, de la visibilité, de l'évolutivité et de la rentabilité nécessaires dans le cadre de l'accès à distance aux périphériques OT/IoT actuels.

Les hackers profitent de la dépendance accrue à l'égard des VPN pour trouver de nombreuses vulnérabilités inédites dans ces systèmes. Les VPN sont devenus des cibles très attrayantes pour les acteurs malveillants.

Si vous supervisez l'infrastructure OT/IoT de votre organisation, vous avez la responsabilité fondamentale de protéger votre entreprise, votre infrastructure, ainsi que d'assurer la sécurité et la confidentialité de vos clients.

Les éléments clés à prendre en compte sont les suivants :

- Maintenir la conformité et la continuité des activités, tout en protégeant les systèmes critiques
- Maintenir la sécurité de votre environnement OT et des périphériques IoT sans entraver la souplesse opérationnelle ou compromettre la sécurité

Votre équipe dispose-t-elle d'une solution d'accès à distance adaptée afin de gérer de grandes quantités d'opérateurs, de sous-traitants et de fournisseurs qui se connectent à distance à votre réseau ?

Le défi de l'accès à distance

Utilisez ces questions comme guide afin d'identifier la solution d'accès à distance la mieux adaptée à votre environnement OT.

Savez-vous qui a accès à votre réseau OT, pour quoi faire et pendant combien de temps ?

Non	Les VPN « toujours actifs » n'offrent aucune visibilité ni aucun contrôle sur l'activité des utilisateurs individuels, en particulier sur un périphérique partagé.
Oui	Restreindre les protocoles non approuvés et orienter les sessions approuvées vers un chemin prédéfini réduit la **surface d'attaque.**

Êtes-vous en mesure de recueillir des données détaillées pour toutes les sessions d'accès à distance, afin de les examiner en temps réel ou ultérieurement ?

Non	L'impossibilité d'examiner ou de suivre l'activité des utilisateurs à distance pose un problème de sécurité et de conformité.
Oui	La possibilité d'avoir les journaux de session détaillés crée une piste d'audit qui permet d'assurer la responsabilité et la conformité.

Suivez-vous le principe du moindre privilège pour votre réseau OT ?

Non	Les VPN de type « tout ou rien » permettent des niveaux d'accès supérieurs à ceux dont ont besoin les opérateurs, les fournisseurs ou les vendeurs dans le cadre de leurs fonctions.
Oui	L'accès en fonction des rôles et la responsabilité individuelle pour les comptes partagés permettent une approche globale de la gestion de la sécurité des accès à distance.

Protégez-vous les identifiants utilisés par les opérateurs et les fournisseurs à distance ? Limitez-vous la connaissance des mots de passe à privilèges ?

Non	Les mauvaises pratiques en matière de gestion des mots de passe sont monnaie courante dans le secteur de l'OT et ont été exploitées dans de nombreuses brèches notoires.
Oui	La sécurisation des comptes à privilèges dans un coffre-fort de mots de passe permet non seulement de protéger ces derniers, mais aussi d'améliorer l'expérience des utilisateurs en les injectant automatiquement dans la session.

Vous conformez-vous au modèle Purdue en interagissant uniquement avec une couche supérieure ou inférieure du réseau industriel ?

Non	L'« air-gapping » isole les réseaux d'usine et d'entreprise en séparant les couches et en définissant la manière dont les machines et les processus doivent interagir.
Oui	L'utilisation d'appliances garantit une séparation logique et physique du réseau afin de respecter le modèle Purdue.

Disposez-vous d'une méthode unique pour planifier et approuver l'accès à distance pour une durée déterminée à votre réseau OT ?

✖ Non	Des flux de travail inefficaces ralentissent les délais en matière d'OT et d'IT, frustrent les utilisateurs finaux et créent des failles de sécurité.	✔ Oui	La consolidation de la programmation, du suivi, de l'approbation et de l'audit de l'accès à distance réduit la charge administrative et accélère le processus.

Vos réseaux IT et OT sont-ils séparés ?

✖ Non	L'utilisation de périphériques personnels par les employés à distance, a rendu floue la segmentation IT-OT, élargissant ainsi la surface d'attaque.	✔ Oui	Le déploiement d'une solution d'accès à distance basée sur une appliance permet aux réseaux OT et IT de travailler séparément, en gardant les données isolées.

Utilisez-vous l'authentification multifacteur (MFA) pour l'accès à distance ?

✖ Non	L'absence de MFA facilite grandement le détournement d'un compte, l'obtention d'un accès à privilèges et la réalisation de mouvements latéraux.	✔ Oui	L'utilisation d'un MFA native ou de fonctionnalités TOTP (mot de passe à usage unique basé sur le temps) offre une protection contre un vecteur d'attaque courant.

Disposez-vous d'un processus structuré pour le provisionnement et le déprovisionnement de l'accès à distance ?

✖ Non	Le provisionnement de l'accès peut être un processus complexe comprenant de nombreux répertoires et systèmes différents.	✔ Oui	L'application de politiques et de contrôles aux utilisateurs qui accèdent à des ensembles dispersés d'endpoints (même couvrant diverses régions géographiques) permet d'obtenir un processus plus efficace et plus précis.

Toutes les données en transit sont-elles chiffrées lors de l'utilisation de l'accès à distance ?

✖ Non	Les anciens périphériques ou systèmes d'exploitation peuvent ne pas prendre en charge les nouvelles normes de chiffrement, ce qui les rend vulnérables aux attaques « man in the middle ».	✔ Oui	L'utilisation des dernières normes de chiffrement, telle que TLSv1.2, même lors de l'accès à des périphériques plus anciens, permet d'atteindre un niveau de sécurité plus élevé pour l'accès à distance.

Si vous avez répondu « non » à l'une de ces questions, VOTRE ORGANISATION COURT UN DANGER.

Accès à distance sécurisé aux systèmes OT avec BeyondTrust

Privileged Remote Access de BeyondTrust permet aux organisations de sécuriser les réseaux industriels sans perturber les opérations, compromettre la sécurité ou risquer la non-conformité. Notre solution sans VPN fournit un accès à distance sécurisé dans une solution unique et flexible qui simplifie les déploiements et assure une évolutivité maximale, tout en permettant aux opérateurs et fournisseurs distants d'être productifs.

Les principales fonctionnalités sont les suivantes :

- Visibilité et contrôle complets de l'accès à distance aux systèmes OT
- Application du principe du moindre privilège avec des contrôles d'accès granulaires
- Séparation des réseaux
- Réduction de la charge administrative et simplification des flux de travail
- Création de pistes d'audit complètes

L'utilisation de Privileged Remote Access de BeyondTrust en remplacement de votre VPN d'entreprise pour les opérateurs, les fournisseurs ou les vendeurs tiers afin d'accéder aux environnements OT, élimine les angles morts de l'accès à distance, réduit la surface d'attaque et favorise la productivité. Protégez vos processus ainsi que vos profits, et sécurisez l'accès à l'infrastructure, tout en réduisant de manière significative les vulnérabilités et les incidents de sécurité.

« Secure Remote Access (SRA) de BeyondTrust offre aux utilisateurs à distance autorisés une méthode de haute sécurité et de Zero Trust pour accéder aux ressources IT et OT critiques. »

Les employés connectés travaillant dans des milieux industriels ont besoin du Zero Trust. ARC View. 11/2021

Tout au long du processus d'évaluation des solutions de support à distance, gardez à l'esprit ces exigences professionnelles :

VPN contre Privileged Remote Access de BeyondTrust

FONCTIONNALITÉ	VPN	BEYONDTRUST
Accès à distance	●	●
Connexion sécurisée	●	●
Accès à la couche réseau (Protocol Tunneling)	●	●
Trafic chiffré	●	●
Virtualisation de la couche application		●
Bureau à distance		●
Accès RDP proxy		●
Accès VNC par proxy		●
Accès SSH par proxy		●
Surveillance de session		●
Enregistrement de session		●
Accès Just-in-Time		●
Architecture Zero Trust		●
Intégration de la gestion des accès privilégiés (PAM)		●
Sécurisation des équipements personnels		●
Intégration aux solutions ITSM		●
Gestion des mots de passe et stockage des identifiants		●
Déploiement dans le cloud ou sur site (appliance virtuelle)		●
Accès sans agent		●
Grande compatibilité avec les différents systèmes d'exploitation et plateformes		●
Prévention des mouvements latéraux		●
Piste d'audit et rapports de session		●

Zero Trust et systèmes OT

Le NIST définit le Zero Trust comme « un ensemble de paradigmes de cybersécurité en évolution, qui font passer les défenses d'un périmètre statique basé sur le réseau à un périmètre centré sur les utilisateurs, les actifs et les ressources.[3] ». Le Zero Trust est de plus en plus pertinent pour les systèmes de contrôle industriel, car les technologies et le télétravail ont atténué ou éliminé le recours à un pare-feu traditionnel et à un périmètre où les réseaux sont cloisonnés.

Les lignes directrices du NIST constituent des instructions claires pour les organisations qui souhaitent savoir comment adopter les principes du Zero Trust. De nombreuses organisations intègrent ces principes dans leurs stratégies de sécurité.

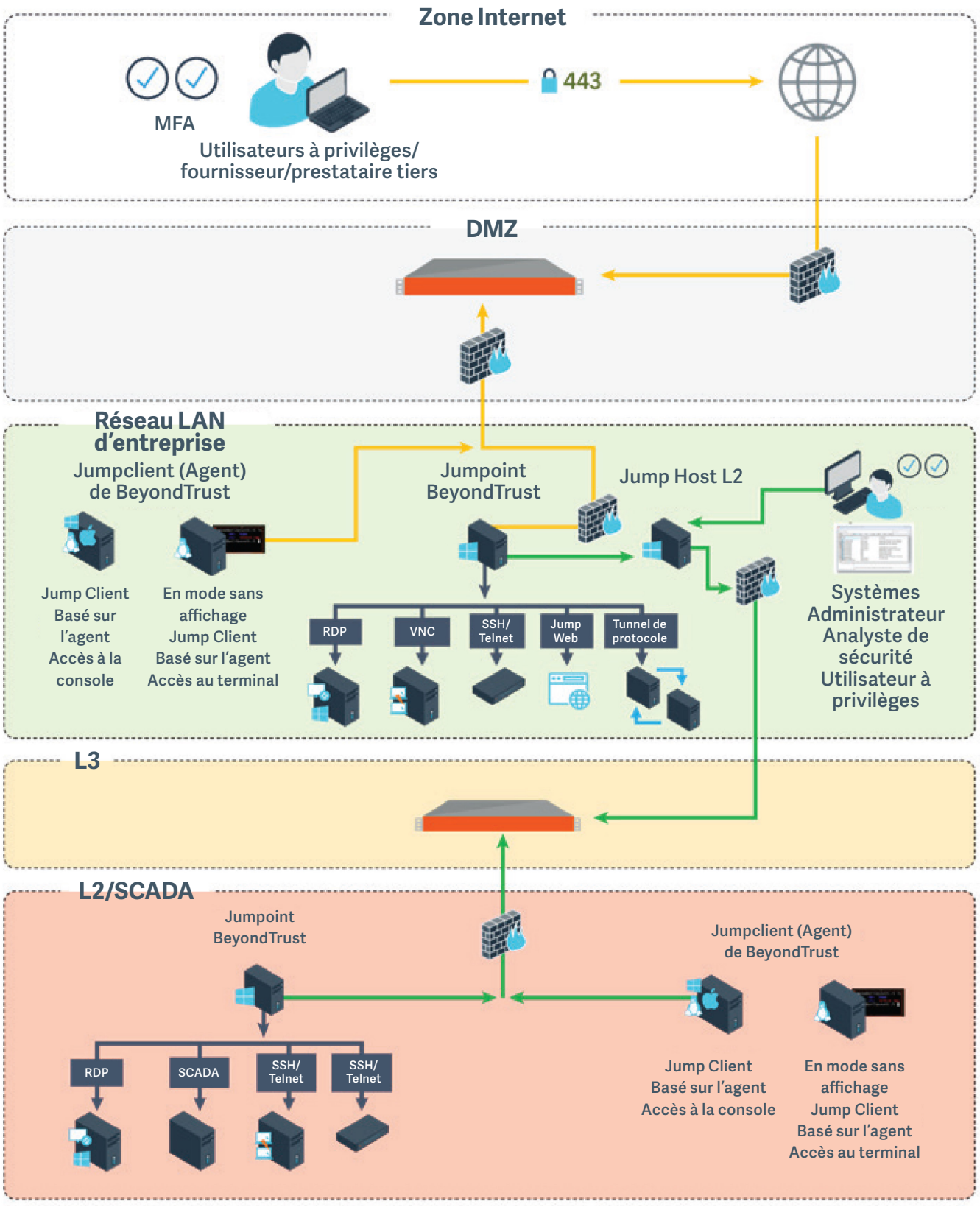
Privileged Remote Access de BeyondTrust aide les organisations à adopter une approche Zero Trust en :

- Appliquant le principe du moindre privilège pour les sessions d'accès à distance
- Traitant les périphériques gérés avec le même niveau de confiance que pour ceux qui ne le sont pas, à savoir une confiance nulle
- Fournissant un accès aux applications indépendant de l'accès au réseau
- Enregistrant toutes les activités effectuées à l'aide de l'accès à distance et des fonctionnalités à risque telles que copier/coller
- Activant la sécurité par API pour protéger l'intégrité des données envoyées depuis les périphériques de l'IoT vers les systèmes de back-end

La granularité de Privileged Remote Access pour atteindre les objectifs du Zero Trust garantit que tous les accès à distance des utilisateurs et de l'infrastructure sont appropriés, gérés et documentés, quelle que soit la façon dont le périmètre a été redéfini.

[1]The State of Industrial Cybersecurity. Trend Micro. Juin 2022
[2]Rapport sur le coût d'une violation de données. IBM. Juillet 2022.
[3]Publication spéciale du NIST 800-207, Zero Trust Architecture. Août 2020.

Réseaux OT : déploiement du Privileged Remote Access



En savoir plus ou planifier une démo

https://www.beyondtrust.com/fr/solutions/operational-technology

À PROPOS DE BEYONDTRUST

BeyondTrust est le leader mondial de la sécurité intelligente de l'identité et de l'accès, permettant aux organisations de protéger les identités, de contrer les menaces et de fournir un accès dynamique afin de renforcer et de sécuriser l'environnement de travail hybride. Nos produits intégrés et notre plate-forme offrent la solution de gestion des accès privilégiés (PAM) la plus avancée du secteur, permettant aux organisations de réduire rapidement leur surface d'attaque dans les environnements traditionnels, cloud et hybrides.

Avec un héritage d'innovation et un engagement ferme envers les clients, les solutions BeyondTrust sont simples à déployer, à gérer et à adapter à l'évolution des entreprises. 20 000 clients, dont 75 des 100 premières entreprises du classement Fortune et un réseau mondial de partenaires nous font confiance.
Pour en savoir plus, rendez-vous sur **beyondtrust.com/fr**