LIVRE BLANC

Démystifier le Zero Trust au sein des environnements OT

De la confiance implicite vers le Zero Trust

Synthèse

Encore récemment, les réseaux de type OT (operational technology) couvrant des sites industriels comme les usines ou les infrastructures critiques étaient cloisonnés, et donc déconnectés d'Internet. Désormais, les environnements IT et OT, autrefois distincts, sont davantage interconnectés : c'est le résultat d'une transformation numérique qui s'est opérée et d'une connectivité étendue aux collaborateurs distants. Cette connectivité améliore le cycle de production grâce à un partage de données et à des outils cloud qui permettent aux entreprises de générer davantage de valeur. Cependant, cette convergence entre IT et OT présente un inconvénient majeur : les cybermenaces, en constante évolution, accèdent plus facilement aux environnements OT plus ouverts qu'auparavant. Une réalité susceptible de remettre en cause les avantages escomptés de cette convergence.

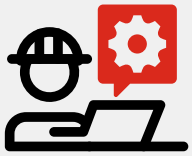
Les systèmes OT sont particulièrement vulnérables, car conçus pour faire implicitement confiance à tous les utilisateurs et dispositifs présents dans leur environnement. Dans ce contexte, les entreprises sont invitées à évoluer vers un modèle de cybersécurité Zero Trust, qui vérifie en permanence le niveau de confiance des utilisateurs et des dispositifs tout en contrôlant l'accès sur la base d'informations contextuelles.

Les évolutions du concept de confiance dans l'OT

Historiquement, en matière de protection de leurs systèmes, les concepteurs, constructeurs et opérateurs de systèmes d'automatisation et de contrôle industriels (IACS - industrial automation and control systems) savaient comment les protéger. Ils considéraient que ces derniers s'abstiendraient d'exécuter un programme présentant un danger pour un opérateur humain ou pour l'outil de production. La plupart des technologies IACS ont été conçues en intégrant l'idée d'une confiance implicite. Ainsi, toutes les connexions établies au sein d'un périmètre OT protégé car cloisonné, étaient à l'abri des cybermenaces proliférant à l'extérieur. Cette confiance par défaut a constitué, pendant des années, une stratégie de sécurité efficace en raison d'un OT isolé par rapport à l'Internet public.

En outre, les systèmes de contrôle industriel (ICS pour industrial control system) sont généralement conçus pour durer. Les technologies déployées peuvent être opérationnelles pendant 20 ans ou plus. L'utilisation de systèmes ICS sur le long terme se justifie souvent par des impératifs métiers, ainsi que par des exigences en matière de sécurité et de fiabilité).[2] Cependant, des connexions externes vers les systèmes OT se sont généralisées et cette réalité n'a pas vraiment été anticipée.

Les environnements OT sont de plus en plus connectés aux réseaux informatiques (ce qu'on appelle la convergence IT/OT ou Industrie 4.0). Les avantages sont au rendez-vous, comme faire appel aux capacités natives du cloud ou améliorer la prise de décision en exploitant des données provenant à la fois des sphères IT et OT.[3] Cette convergence peut, en outre, réduire les besoins en espace, consolider le parc de matériel physique, accélérer les délais de déploiement, engendrer davantage d'économies, doper les performances et décloisonner les ressources des environnements IT et OT.[4] Cependant, cette convergence obère la protection de l'OT, ce qui remet en cause les notions de confiance explicite et de « security by design ».



« Les environnements IT sont souvent nécessaires pour configurer et gérer les dispositifs OT. Ils constituent également le périmètre où les données clés doivent être collectées, normalisées, traitées et communiquées afin que l'entreprise puisse gérer efficacement ses ressources OT. Cette capacité à relier les réseaux d'entreprise et industriels répond à un besoin de l'entreprise. Cependant, comme de plus en plus de ressources informatiques migrent vers des environnements cloud, les actifs OT sont maintenant exposés à de nouveaux risques de sécurité. »[1]

Les trois quarts des entreprises de l'OT ont signalé au moins une intrusion au cours de l'année écoulée. Ces incidents dus à des logiciels malveillants (56 %) et au phishing (49 %) sont les plus courants. Près d'un tiers des personnes interrogées ont déclaré avoir été victimes d'une attaque par ransomware.[5]

L'émergence du Zero Trust dans la cybersécurité

Au niveau conceptuel, le terme Zero Trust se détourne du principe d'une confiance implicite et privilégie l'existence présumée d'une menace ou d'un incident : ainsi, tout utilisateur ou dispositif ne sera considéré comme étant de confiance qu'après vérification.

Dans la pratique, dans un contexte Zero Trust, les utilisateurs et les dispositifs ne se voient plus accorder automatiquement un accès en fonction de leur emplacement sur le réseau. Au contraire, chaque transaction est évaluée pour statuer sur son niveau de confiance. Des niveaux d'accès différenciés peuvent être accordés en fonction des facteurs contextuels associés à une demande d'accès. Les permissions sont réévaluées de manière fréquente.

Les approches pour déployer un modèle Zero Trust peuvent varier considérablement. D'ailleurs, certains termes qui qualifient cette approche peuvent prêter à confusion en l'absence de définitions claires.

- **Une solution d'accès Zero Trust** (ZTA - zero-trust access) se concentre sur l'identification et la surveillance des utilisateurs et des dispositifs qui accèdent au réseau. Alors que de plus en plus d'utilisateurs travaillent à distance et que les objets connectés industriels (IIoT) prolifèrent dans les environnements OT, les entreprises doivent vérifier en permanence tous les utilisateurs et dispositifs lorsqu'ils accèdent aux applications et aux données.
- Une solution d'**accès réseau Zero Trust** (ZTNA - zero-trust network access) n'autorise aucun accès aux applications tant que l'identité de l'utilisateur ou du terminal requérant n'a pas été validée. L'accès réseau Zero Trust est souvent cité comme une évolution naturelle des réseaux privés virtuels (VPN) traditionnels qui supposent que tout ce qui est validé par les fonctions de sécurité périmétrique est fiable. Contrairement à un VPN, le ZTNA étend le modèle Zero Trust au-delà du réseau et réduit la surface d'attaque en dissimulant les applications, celles-ci n'étant pas visibles depuis Internet.

Aux États-Unis, l'intérêt pour le Zero Trust s'est renforcé après la publication en 2021 d'un décret de la Maison Blanche visant à garantir l'application de pratiques de sécurité essentielles dans toutes les agences officielles et à faire migrer le gouvernement fédéral vers une architecture Zero Trust.[6]

Zero Trust : quelles réponses à quelles problématiques ?

Un Zero Trust efficace répond à plusieurs besoins urgents des entreprises en matière de cybersécurité :

- Accompagner la mobilité des collaborateurs sans perturber l'opérationnel, ni affecter les politiques de contrôle d'accès en vigueur
- Unifier la stratégie de sécurité de l'entreprise en ce qui concerne les utilisateurs, les ressources et (indirectement) les applications, indépendamment de leur localisation physique
- Contribuer à prévenir les cybermenaces de se propager au sein d'une entreprise en réévaluant en permanence l'identité et la posture de sécurité des utilisateurs et des dispositifs pour chaque session

Les défis du Zero Trust en environnement OT

Pour déployer efficacement une solution Zero Trust comme le ZTA en environnement OT, les responsables sécurité doivent s'interroger sur le fonctionnement des ICS en environnement OT et étudier leur sécurité.

1. Les clauses de la garantie offerte par un fournisseur de système d'automatisation peuvent-elles impacter le fonctionnement du réseau ? Cette problématique, assez fréquente, doit faire l'objet d'un examen approfondi en amont.
2. Les technologies ZTA sont-elles compatibles avec les technologies existantes dans les environnements OT ? La durée de vie des systèmes ICS, souvent supérieure à 20 ans, doit être prise en compte.
3. Les entreprises dépendent souvent d'intégrateurs systèmes et de fabricants OEM pour l'intégration et l'activation de leurs services. Sont-elles préparées à accueillir des technologies ZTA susceptibles de perturber les sous-systèmes actuellement intégrés et opérationnels ?
4. Les fabricants d'équipements OEM et les intégrateurs systèmes peuvent également exiger un accès à distance dans le cadre de leur garantie ou de contrats d'exploitation et de maintenance externalisés.
5. En règle générale, les systèmes du parc ICS/OT sont « headless » : ils ne disposent pas d'une interface pour interagir avec les utilisateurs. Les adresses IP (Internet Protocol) sont souvent statiques et il est difficile d'imaginer de ré-authentifier une connexion avec un dispositif dépourvu d'interface utilisateur. Comment la solution ZTA va-t-elle gérer cette contrainte propre aux environnements OT ?
6. Les environnements OT étant traditionnellement cloisonnés, ils utilisent parfois des mots de passe statiques, autrement dit qui ne sont pas générés par Active Directory (AD) à l'aide de politiques de gestion d'informations d'identification sécurisées.
7. Certains éléments OT (automates programmables, interfaces homme-machine) sont susceptibles de ne pas être compatibles avec les protocoles nécessaires à une intégration dans un environnement ZTA. Par conséquent, le ZTA peut ne pas convenir à certains dispositifs ou systèmes OT.
8. Certaines technologies ICS en environnement OT peuvent être affectés à des opérations de sécurité et peuvent nécessiter un accès simple et ininterrompu aux systèmes pour exécuter des fonctions de sécurité. Par conséquent, l'application de ZTA pour de tels ICS ne devrait pas grever la sécurité de l'infrastructure.

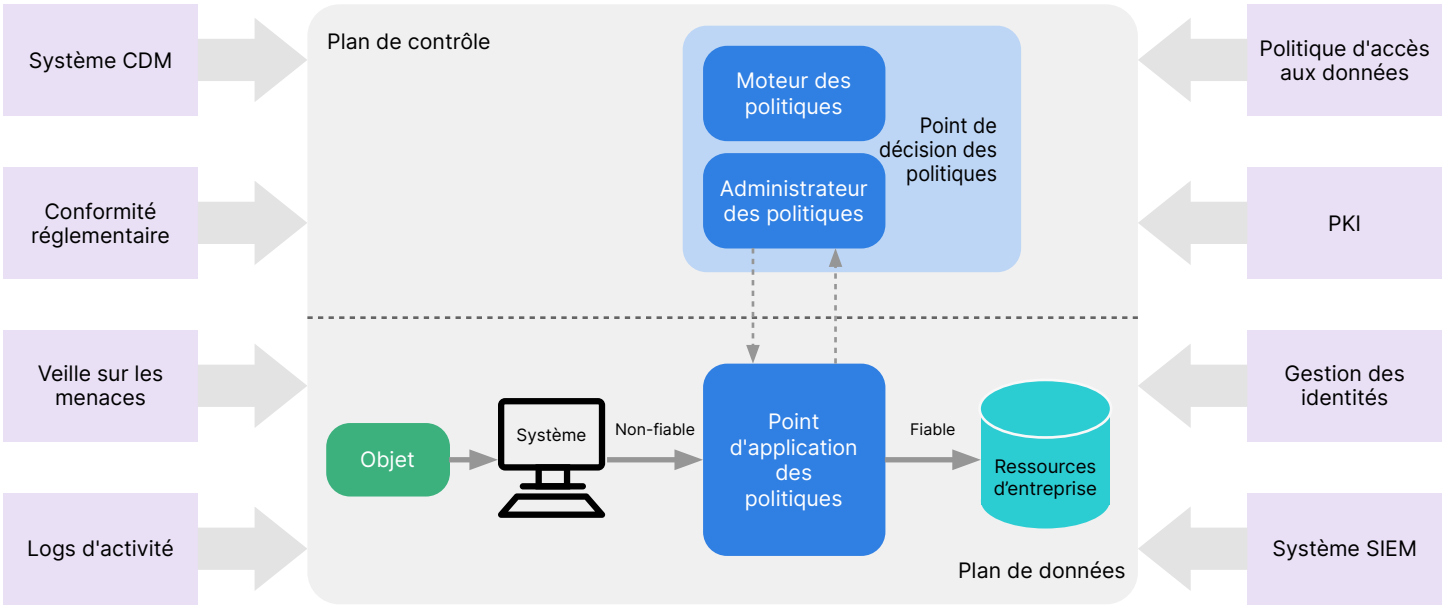
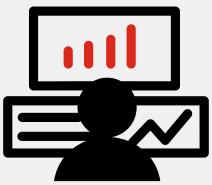


Schéma 1 : composants logiques du NIST SP 800-207 Core Zero Trust[7]

Un autre défi majeur lié au Zero Trust au sein des environnements IT/OT interconnectés est que les entreprises doivent établir des identités distinctes entre ces deux environnements. L'adoption efficace du ZTA nécessite une solution qui unifie les opérations de sécurité pour deux domaines de gestion qui convergent, mais qui présentent des priorités différentes. Le maintien de centres opérationnels de sécurité (SOC) distincts pour l'IT et l'OT est une source de complexité et de risques potentiels lorsqu'il s'agit de gérer les ressources et les politiques dans les deux environnements, d'intégrer et d'analyser les données des systèmes IT et OT, et de mener des actions de restauration en cas de cyber-intrusion.

L'acquisition et la maintenance de solutions Zero Trust nécessiteront également un savoir-faire et des ressources opérationnelles en interne pour gérer les logs et les contrôles d'accès. Avec des budgets limités, de nombreuses entreprises peuvent actuellement avoir du mal à trouver, embaucher et conserver le personnel de sécurité qualifié requis pour déployer et maintenir des solutions Zero Trust. Dans ces cas, il est important d'examiner si un fournisseur propose un service de support dédié.



Le nombre de responsables de la sécurité OT qui considèrent que la posture de sécurité de leur entreprise est « très mature » a chuté de 21 % à 13 % cette année, ce qui suggère que les professionnels de l'OT sont de plus en plus sensibilisés et qu'il existe des outils plus efficaces pour évaluer de matière autonome l'arsenal de cybersécurité des entreprises.[8]

Faire le premier pas vers le Zero Trust

Alors que la convergence IT/OT s'accélère, les responsables de la sécurité doivent évoluer vers un modèle Zero Trust afin de préserver leurs environnements OT des perturbations dues à des événements de sécurité internes ou externes. Aujourd'hui, le déploiement du Zero Trust en environnement OT doit s'effectuer selon trois axes :

- **Les collaborateurs :** commencez à sensibiliser les utilisateurs aux risques de la convergence IT/OT pour les former à la manière dont les solutions Zero Trust peuvent contribuer à sécuriser l'entreprise contre les menaces opportunistes.
- **Les processus :** une sécurité OT fondée sur une confiance implicite n'est plus d'actualité. Les politiques et protocoles de sécurité doivent désormais reposer sur une confiance vérifiée en permanence en fonction d'éléments de contexte. Les entreprises ont besoin d'un contrôle complet et permanent sur les personnes et dispositifs présents sur le réseau, y compris les fournisseurs de solutions d'automatisation et les fournisseurs de services.
- **La technologie :** évaluez les solutions Zero Trust pour les environnements OT et gardez à l'esprit qu'elles peuvent impacter votre chaîne d'approvisionnement au sens large. Privilégiez un fournisseur de sécurité Zero Trust avec des partenariats solides dans l'écosystème technologique.

[1]« IT, OT, and ZT : Implementing Zero Trust in Industrial Control Systems », Université Carnegie Mellon, 18 juillet 2022.

[2] Idem.

[3]« Converge IT and OT to turbocharge business operations' scaling power », McKinsey & Company, 28 juin 2022.

[4] « 2023 State of Operational Technology and Cybersecurity Report », Fortinet, mai 2023.

[5] Idem.

[6]« How to Create a Comprehensive Zero Trust Strategy », Fortinet, 15 mai 2023.

[7]« SP 800-207: Zero Trust Architecture », NIST, août 2020.

[8]« 2023 State of Operational Technology and Cybersecurity Report », Fortinet, mai 2023.

octobre 26, 2023 11:41 AM
2177370-0-0-FR