Cisco Connected Factory, une solution de sécurité globale pour l'usine de demain

Livre blanc Cisco sur l'industrie

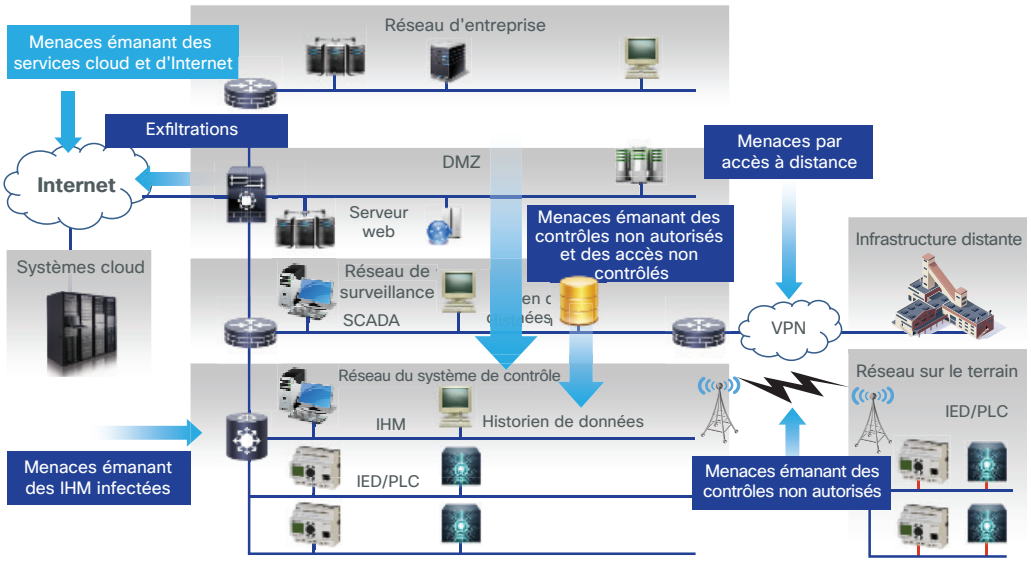
Les entreprises internationales protègent leurs activités industrielles stratégiques avec les solutions de sécurité Cisco Connected Factory

Des menaces croissantes pour les industriels

La cybersécurité est plus que jamais au cœur des préoccupations des plus grands industriels du marché, à juste titre. Malgré les progrès remarquables accomplis ces dernières années en matière de cybersécurité, les secteurs de la fabrication et des opérations industrielles restent des « îlots de vulnérabilité » susceptibles d'être exploités par des hackers. Les systèmes de contrôle industrialisés, pour la plupart mal sécurisés, restent particulièrement vulnérables aux attaques. Étant donné que ces systèmes sont convergés et intégrés avec les technologies IT d'entreprise, les hackers disposent de nouveaux vecteurs d'attaque. Un récent rapport annuel sur les menaces à la sécurité publié par Dell montre que « l'infrastructure vieillissante des machines industrielles présente des challenges considérables en matière de sécurité, qui ne cesseront de croître à l'avenir ».[1]

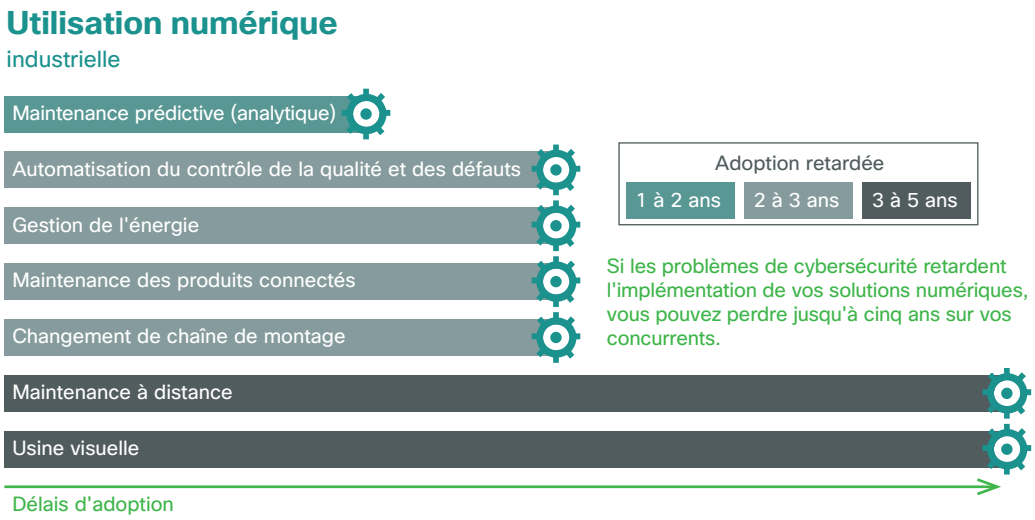
Aujourd'hui, les industriels ont besoin de technologies toujours plus sophistiquées pour contrôler les nouveaux environnements IoT, qui connectent des millions de machines sur des réseaux internationaux. Malheureusement, beaucoup de gestionnaires de site et OT rechignent à mettre en

Figure 1. L'évolution constante des menaces pour les industriels



[1] http://www.dell.com/learn/us/en/ph/press-releases/2015-04-13-dell-annual-threat-report

Figure 2. Lorsque les préoccupations en matière de cybersécurité retardent des initiatives numériques, la croissance potentielle et la position sur le marché en pâtissent



Source : Cisco, 2015.

œuvre des mesures qui risquent d'affecter leurs plannings de production et sont peu enclins à modifier les réseaux isolés existants. En outre, il incombe aux responsables de surveiller tous les accès physiques à l'usine (souvent sur plusieurs sites) des partenaires et des fournisseurs, ce qui augmente la probabilité qu'une personne malveillante parvienne à entrer. En fait, l'erreur humaine est l'une des principales causes d'incident lié à la sécurité. Selon McAfee, « les hackers ont tendance à cibler les systèmes qui peuvent être entièrement compromis, et les réseaux des systèmes de contrôle et d'automatisation industriels (IACS) s'avèrent être des environnements où les cibles sont nombreuses ».[2]

Des violations coûteuses

Les préjudices infligés par les failles de sécurité sont bien connus des entreprises et des opérateurs industriels. Les dommages peuvent être physiques et toucher l'environnement de travail, mais ces attaques peuvent aussi entacher la réputation de la marque et ébranler la confiance des clients. Les pertes financières peuvent s'avérer particulièrement graves pour les industriels, car une attaque peut entraîner des pertes faramineuses (plusieurs millions de dollars) à cause de pannes, perturber les plannings de production et endommager des machines coûteuses. Dans le pire des cas, les travailleurs eux-mêmes peuvent être exposés à des risques sanitaires ou de sécurité.

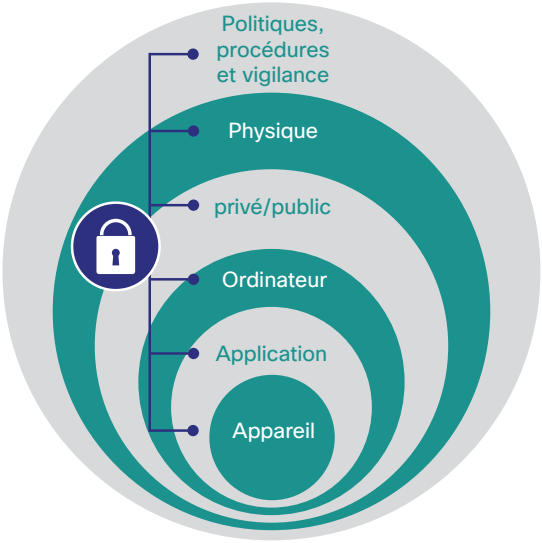
Les industriels qui ne parviennent pas à se protéger contre les menaces sont aussi confrontés à d'autres risques, peut-être encore plus coûteux : une baisse du chiffre d'affaires et la perte de parts de marché. La Figure 1 montre l'impact potentiel des cyberattaques et des retards d'adoption pour les 7 utilisations qui généreront la plus grosse part de valeur numérique dans ce secteur au cours des 10 prochaines années. Toutes ces utilisations imposent aux industriels de doter leurs environnements d'exploitation de nouvelles fonctionnalités numériques. Toutefois, les industriels doivent d'abord avoir confiance en leur stratégie de cybersécurité IT et OT intégrée. Sinon, ils risquent de passer à côté de la valeur et de la hausse de rentabilité promise par celle-ci.

Étant donné le nombre grandissant des menaces à la sécurité auxquelles font face les entreprises aujourd'hui, et le véritable désavantage concurrentiel que subissent les entreprises tardant à déployer des solutions de sécurité, il n'est pas étonnant que la dernière étude de Cisco menée auprès de plus de 350 entreprises ait indiqué que 89 % d'entre elles ont affirmé avoir un dirigeant directement responsable de la sécurité.[3]

[2] https://blogs.mcafee.com/mcafee-labs/is-this-scada-hacking-friday/
[3] http://www.cisco.com/c/m/en_us/offers/sc04/2016-annual-security-report/index.html?KeyCode=001031984

Une stratégie globale

Figure 3 : une défense approfondie



Pour faire face efficacement à ce nouveau degré de dangerosité, les industriels doivent mettre en œuvre de nouvelles stratégies et architectures. « Protéger la périphérie » à l'aide de pare-feu et d'un système de gestion des accès est aussi important qu'une bonne stratégie de segmentation des technologies opérationnelles. Malheureusement, ces deux mesures font souvent défaut sur les réseaux des systèmes de contrôle industriels modernes. Et ce n'est qu'une partie de la solution pour protéger les environnements industriels vulnérables, où les menaces peuvent provenir aussi bien de l'extérieur que de l'intérieur de l'usine, et peuvent même être accidentellement causées par une erreur humaine. Aujourd'hui, les industriels ont besoin de stratégies de défense qui agissent « en profondeur » et comprennent des couches de contrôle de sécurité indépendantes (physique, procédurale et électronique). Alors que les réseaux convergés IT et OT, le cloud computing et les plates-formes mobiles et IoT se généralisent, il est plus que jamais nécessaire d'adopter une approche holistique de la sécurité des données.

Avec la multiplication des terminaux mobiles et des réseaux Wi-Fi et à cause de réseaux OT de plus en plus accessibles et exploitables, les industriels doivent déployer des technologies de sécurité nouvelle génération pour se protéger contre des menaces encore inconnues il y a quelques années. Ce faisant, les leaders en matière de sécurité industrielle peuvent maintenir leur avantage concurrentiel et préserver leurs marques et leur réputation. Il est essentiel d'assurer une connectivité sécurisée au sein des réseaux OT et entre les réseaux IT et OT. Un fabric de réseau sécurisé peut augmenter l'accessibilité des données tout en assurant aux entreprises une hausse de leur efficacité (grâce à l'amélioration de la collaboration), du taux de rendement global, ainsi que de la qualité des produits. De plus, un réseau intégré IT et OT sécurisé aide les industriels à traiter systématiquement les problèmes d'environnement, d'intégrité et de sécurité au sein même de l'usine, et donc à réduire les risques.

> « Nous sommes désormais en mesure de détecter les menaces informatiques jusque-là invisibles. Ce constat a permis de convaincre l'équipe du bien-fondé de la technologie de prévention des intrusions que nous installons sur l'ensemble du réseau industriel. »
>
> *Charles Harper, directeur, National Supply & Pipeline Operations, Air Liquide*

Solution de sécurité Cisco Connected Factory

Depuis des années, Cisco aide les entreprises à sécuriser certaines de leurs opérations les plus stratégiques. Des milliers d'industriels (dont plusieurs grands noms du secteur comme GM, Daimler Trucks North America, Stanley Black & Decker et Air Liquide) ont mis en place des solutions de sécurité Cisco au sein de leur infrastructure de production industrielle pour se prémunir contre les menaces à la sécurité et garantir la continuité des opérations, l'intégrité du système et la sécurité.

La sécurité pour les industriels d'aujourd'hui

Menaces

Les menaces ont évolué dans un monde d'usines et de machines connectées et il est plus important que jamais pour les industriels d'adopter une solution de sécurité avancée. Alors que sites de production et processus commerciaux s'harmonisent davantage, les problèmes de sécurité s'étendent au-delà de l'entreprise et peuvent avoir un impact sur les machines et les opérations.

Une solution de sécurité de nouvelle génération

Pour prospérer dans cet environnement toujours plus menaçant, les industriels d'aujourd'hui doivent adopter une approche holistique de la sécurité, basée sur plusieurs couches de défense et englobant le personnel, les infrastructures et les processus machine.

Un cloud sécurisé pour les usines

Le cloud est voué à se généraliser dans le secteur de l'industrie ; il devient un outil courant pour collecter et analyser les données à moindre coût. Les technologies cloud Cisco destinés aux usines offrent aux responsables et aux experts qui opèrent à distance un accès sécurisé aux données de production, où qu'ils se trouvent, et protègent le trafic des données entre les machines connectées par l'IoT.

Un data center sécurisé pour les usines

Les attaques dirigées contre les data centers des usines peuvent être dévastatrices et engendrer une perte de données et des pannes. Les solutions Cisco IPS fournissent un système de destinées exploitable pour les data centers et bloquent les menaces avant qu'elles puissent interrompre les services du data center. Le déploiement de services sécurisés et résilients est rapide et les pare-feu de Cisco dominent le marché en matière de performances et de facilité de gestion.

Un site sécurisé pour les usines

Les connexions entre les ateliers de production et les bureaux, mais aussi avec l'écosystème de l'entreprise dans son ensemble, se renforcent. Les nouvelles usines doivent bénéficier d'un niveau de sécurité et de protection contre les menaces plus flexible et plus sophistiqué. La gamme Cisco de routeurs sécurisés, de pare-feu, de systèmes de prévention des intrusions, d'IPS sans fil, ainsi que Cisco TrustSec offrent une protection multicouche pour votre atelier de production et tous les éléments auxquels il est connecté.

Des machines sécurisées pour les usines

Aujourd'hui, les entreprises connectent des milliers de machines industrielles dans le cloud et sur les réseaux IoT pour atteindre un niveau d'efficacité et d'innovation inégalé. Malheureusement, cette nouvelle tendance pose des défis de sécurité complexes aux responsables IT et OT. Cisco et ses partenaires proposent des technologies de nouvelle génération qui protègent contre les hackers opérant à l'intérieur comme à l'extérieur de l'usine.

Les solutions de sécurité Cisco transforment différents processus industriels afin de permettre aux entreprises de sécuriser sans risque leur infrastructure, les processus machine et le personnel. Conçus pour assurer un retour sur investissement (ROI) maximal et des résultats tangibles, ces solutions et services incluent les fonctions suivantes :

- **Identification et suivi des ressources.** Cisco permet aux industriels d'identifier et de surveiller toutes les ressources et tous les utilisateurs sur leurs réseaux et de créer une base solide pour un accès à distance sécurisé.
- **Gestion des accès et des identités** Ces solutions facilitent l'accès aux fournisseurs et aux sous-traitants, l'intégration rationalisée des appareils et la mise en application dynamique des politiques.
- **Zones démilitarisées industrielles (DMZ)** Les zones démilitarisées conçues par Cisco pour les activités industrielles agissent comme des zones tampons avancées situées en périmètre des réseaux. Elles veillent à l'application des politiques de sécurité des données entre les réseaux sûrs et non fiables.
- **Technologies de traduction d'adresses réseau (NAT)** Ces solutions d'adressage IP rationalisent les réseaux de machines à l'échelle de l'usine et améliorent la sécurité contre les intrusions via Internet.
- **Services de cybersécurité industrielle** Cisco aide les industriels à protéger leurs ressources et à éviter les interruptions en analysant les risques liés à la cybersécurité, en évaluant les failles de sécurité, puis en concevant et en mettant en œuvre des contrôles de sécurité qui permettent de limiter les risques.
- **Services gérés de sécurité des opérations** Cette solution modulaire de cybersécurité et de conformité pour les environnements opérationnels évolue selon les besoins de l'entreprise et offre des options économiques de prestation à la demande.
- **Architecture réseau des systèmes de contrôle industriels et conception de services** Cisco travaille avec les industriels pour leur proposer des solutions permettant de garantir non seulement une sécurité de nouvelle génération, mais aussi de bonnes performances opérationnelles et un retour sur investissement intéressant.

Voyons à présent comment les industriels utilisent les solutions Cisco pour créer des plates-formes de sécurité globales et ainsi améliorer leur compétitivité.

« Cisco Identity Services Engine révolutionne complètement notre réseau. »

David Kennedy, vice-président, responsable de la sécurité, Diebold Inc

Un contrôle d'accès exhaustif

Accès refusé

Un sous-traitant connecte son ordinateur portable au port ouvert d'un commutateur d'usine pour télécharger un manuel d'entretien. La solution ISE détecte sa connexion et son identité, et lui refuse l'accès au réseau, évitant ainsi une panne potentielle.

Plus les appareils qui se connectent au réseau IACS se multiplient et se diversifient, plus il est difficile de s' s'adapter à l'évolution des techniques de gestion de la sécurité et de réduction des risques. Cisco ISE (Identity Services Engine) offre aux industriels une nouvelle génération de technologies capables de garantir un accès filaire et sans fil hautement sécurisé sur l'ensemble du site, tout en améliorant la gestion centralisée des politiques, l'intégration rationalisée des appareils et une mise en application dynamique des politiques.

Cisco ISE (Identity Services Engine) prend en charge plusieurs référentiels d'identités externes et simplifie l'administration grâce à une interface de gestion intégrée unique pour les réseaux IT et OT. Les industriels disposent désormais d'un système centralisé prenant en compte le contexte pour contrôler efficacement l'accès aux zones industrielles. La solution ISE applique automatiquement le bon niveau de privilège d'accès et les politiques pertinentes en fonction du rôle et du groupe de l'utilisateur. Elle surveille aussi en permanence le réseau pour vérifier que les utilisateurs n'y accèdent qu'à partir d'appareils autorisés et conformes à la politique. Les utilisateurs n'ont accès qu'aux segments du réseau industriel autorisés par la politique, les autres leur sont inaccessibles. À noter que ce processus de blocage est invisible pour les utilisateurs.

Diebold sécurise son réseau mondial de machines avec Cisco ISE (Identity Services Engine)

Premier fabricant mondial de distributeurs de billets, Diebold Inc. n'est plus novice en matière de sécurité. « La sécurité est partie intégrante de notre entreprise », explique David Kennedy, responsable de la sécurité chez Diebold. « Notre priorité en matière de sécurité est d'assurer les revenus de notre entreprise. » Diebold déploie actuellement plusieurs solutions de sécurité Cisco, y compris Cisco ISE (Identity Services Engine), afin de protéger son réseau de 87 000 appareils répartis dans 77 pays.

Avec l'arrivée des nouveaux appareils et des nouvelles technologies dans les entreprises, David Kennedy affirme qu'il est de plus en plus en plus difficile d'assurer une visibilité et un contrôle réseau complets. « Les entreprises modernes sont plus exposées et les menaces internes augmentent », précise-t-il. Cette situation est d'ailleurs aggravée par l'afflux des tablettes, smartphones et autres terminaux mobiles dans l'environnement de travail industriel. Il ajoute que dans un tel contexte, il est difficile de garantir un « contrôle granulaire » des identités opérant sur le réseau.

David Kennedy explique que Diebold a analysé les stratégies de ses concurrents, mais « aucune n'est aussi efficace que celle de Cisco ISE. Cisco ISE est une solution complète et ça a été pour nous un grand avantage. » La solution, intégrée avec le client pour la mobilité sécurisée Cisco AnyConnect, a permis à Diebold d'examiner tous les appareils du réseau et de rationaliser les accès des invités et des sous-traitants. « Elle a considérablement simplifié et sécurisé le processus dans son ensemble », explique le responsable de la sécurité. « [Les sous-traitants] ne peuvent accéder qu'aux informations, ports et protocoles dont ils ont besoin », explique-t-il. Il ajoute que le processus est entièrement automatisé et transparent pour l'utilisateur. Enfin, Diebold est désormais capable de gérer efficacement le risque que représentent les terminaux mobiles sur les sites industriels. « La mobilité est une préoccupation majeure pour nous, mais depuis que nous avons Cisco ISE, ce n'est plus un problème », affirme David Kennedy. « Cisco ISE révolutionne complètement notre réseau. »

Une protection complète grâce aux zones démilitarisées (DMZ) industrielles

Aucun produit, aucune technologie, aucune méthodologie ne peut sécuriser seul les opérations industrielles. La protection des ressources industrielles stratégiques requiert une approche de sécurité globale et complète qui utilise plusieurs couches de défense (physique, procédurale et électronique) pour répondre à différents types de menaces.

C'est pourquoi de plus en plus d'entreprises combinent des services d'identification complets avec des zones tampons avancées situées en périmètre des réseaux (les DMZ industrielles) qui appliquent des politiques de sécurité des données entre un réseau fiable (zone industrielle) et un réseau non sécurisé (zone de l'entreprise). Ces DMZ industrielles forment un réseau séparé situé entre les deux zones. Les DMZ industrielles sont généralement formées de nombreux appareils d'infrastructure, y compris de pare-feu, de serveurs VPN, d'hôtes d'applications IACS et de serveurs proxy inverses, en plus des appareils d'infrastructure réseau tels que les commutateurs, les routeurs et les services virtualisés.

Si vous souhaitez vraiment assurer la sécurité de votre réseau IACS, nous vous conseillons la gamme de solutions de DMZ industrielles pour les environnements CPwE (Converged Plantwide Ethernet) proposée par Cisco et Rockwell Automation.

Global Aluminum Company utilise les DMZ pour optimiser et protéger son réseau industriel

Les DMZ industrielles jouent un rôle important dans la sécurisation et l'optimisation de l'un des plus grands sites de production d'aluminium du monde. La fondeuse à 6 milliards de dollars construite par Emirates Aluminium Company Ltd (EMAL, filiale d'Emirates Global Aluminium) à Abu Dhabi produit 1,4 million de tonnes d'aluminium par an. La fonderie est divisée en plusieurs zones industrielles indépendantes (avec leurs réseaux IT) qui correspondent à différentes étapes du processus de fabrication de l'aluminium. Le challenge : faire converger ces réseaux disparates et partager des informations importantes pour optimiser la production sans compromettre la sécurité ni la résilience.

L'EMAL a déployé une solution de DMZ industrielle basée sur Cisco pour permettre aux informations de circuler entre chaque zone via le réseau IT de l'entreprise, sans compromettre la sécurité. Chaque zone a sa propre DMZ, avec des pare-feu jumeaux, qui fournit une « zone neutre » où le trafic suspect peut être identifié et isolé avant qu'il ne s'infiltre dans les réseaux, les serveurs et les systèmes. L'entreprise a efficacement fusionné ses réseaux d'entreprise et de production en utilisant une DMZ comme pont, permettant le partage des données entre les deux réseaux, sans se heurter aux problèmes liés aux interfaces propriétaires. « Les DMZ sont généralement utilisées pour protéger les réseaux d'entreprise contre les menaces venant d'Internet », explique Sylvain Boily, gestionnaire de l'automatisation chez BBA, consultant sur le projet. « Cette application des DMZ dans un environnement de production est révolutionnaire. »

Le fabricant d'aluminium recherche actuellement d'autres solutions et envisage notamment un système de surveillance IP capable d'intégrer la surveillance vidéo aux autres techniques, comme le traitement analytique et le contrôle d'accès, pour offrir une solution de sécurité pérenne à l'échelle de l'entreprise. « Nous avons créé un réseau répondant aussi bien aux besoins présents et futurs », indique Sylvain Boily. « Il offre toutes les fonctions nécessaires au transfert des informations. Redondance, sécurité, contrôle du trafic ; tout est là. »

Cisco Secure Ops : une solution de sécurité complète à un coût raisonnable

Le nombre de menaces ne cesse d'augmenter. L'Internet des objets accroît l'efficacité des usines, mais la hausse du nombre de connexions aux systèmes de contrôle industriels rend ces derniers plus vulnérables aux cyberattaques. Les industriels ont besoin d'une solution sécurisée plus robuste pour protéger leurs réseaux des cyberattaques. Ils cherchent des solutions alternatives aux solutions classiques qui nécessitent des investissements importants en équipement et personnel. Ils veulent des solutions nativement flexibles et capables de s'adapter rapidement pour répondre aux besoins de l'entreprise.

C'est pour ces raisons que de plus en plus d'entreprises adoptent Cisco Secure Ops, un service de sécurité hébergé qui protège les systèmes de contrôle industriels et les réseaux SCADA (système de contrôle et d'acquisition de données), améliore l'efficacité et réduit les pannes sur le site. C'est un système global et complet qui offre aux industriels une vue centralisée de ce qui se passe sur leurs sites distants. Il peut détecter et signaler les anomalies, déclencher le processus de gestion des incidents et protéger les systèmes d'usine les plus critiques. Il repose sur une approche modulaire des contrôles de sécurité, offrant la flexibilité nécessaire pour s'adapter à de nouveaux vecteurs d'attaque à mesure que l'entreprise se développe et que les exigences de sécurité évoluent. En outre, les industriels peuvent implémenter Secure Ops sur site.

La solution interagit avec la plupart des principales entreprises d'automatisation pour la détection et l'inventaire des ressources, la sécurisation des accès, etc. Certains des fournisseurs de solutions d'automatisation sont des partenaires communs de distribution. En s'appuyant sur cet écosystème de partenaires, la solution Secure Ops fournit à la fois les avantages des systèmes de sécurité Cisco, une expertise en matière de réseau, la sécurisation des systèmes de contrôle industrialisés, ainsi que des informations opérationnelles.

Avec Secure Ops, les fournisseurs distants disposent d'une approche unique et optimisée pour accéder de manière sécurisée aux systèmes des ateliers de production. L'approche comprend un outil d'audit puissant doté de fonctionnalités de conformité, qui accède au système et offre une plus grande efficacité opérationnelle.

Un fournisseur d'énergie leader protège son infrastructure critique et réduit ses dépenses grâce à Secure Ops

Les cyberattaques, les risques opérationnels et la conformité sont des préoccupations majeures pour ce fournisseur d'énergie leader, qui produit plus de 3 milliards de barils de pétrole et de gaz naturel par jour dans 70 pays. La croissance et la complexité du système de contrôle industriel de l'entreprise exigeaient une solution de sécurité novatrice, capable de protéger les infrastructures stratégiques (les anciennes comme les nouvelles) tout en garantissant la conformité et en maîtrisant les coûts.

« Que ce soit dans les raffineries, les puits ou les usines de lubrifiant, nous devons protéger notre infrastructure stratégique », explique le directeur informatique de l'entreprise. « Nous avons sollicité Cisco pour créer une solution complète. » La solution Cisco Secure Ops repose sur les logiciels et le matériel réseau déployés sur le terrain pour surveiller à distance plus de 50 sites en amont comme en aval. Nous disposons ainsi d'un « tunnel » sécurisé depuis l'infrastructure jusqu'à une console de gestion centralisée. Des ingénieurs et des experts en informatique postés dans un bureau de services globaux réagissent au plus vite à toutes les menaces à la sécurité.

En collaboration avec des partenaires spécialisés dans les systèmes de contrôle industriels et dans les questions de santé et de sécurité sur les sites industriels, Cisco a fourni une solution de bout en bout sous la forme d'un service complet, avec à la clé une réduction considérable des dépenses d'investissement de départ pour l'entreprise. Une étude du ROI menée par l'entreprise a indiqué que la solution Secure Ops a permis de réduire les coûts de 700 000 dollars par site, en cinq ans. En accélérant la gestion et en maîtrisant les menaces, l'entreprise a gagné en agilité, réduit ses coûts liés aux opérations et à la sécurité et limité considérablement les pannes.

« Aujourd'hui, nous consacrons beaucoup moins de temps à la gestion des événements liés à la sécurité et des malwares. En fait, depuis l'adoption de la solution cloud Cisco de sécurisation du web, plus aucun client n'a été infecté et nous n'accédons plus que rarement au portail d'administration. »

– Peter Kersting, responsable de la sécurité informatique, Arup

Avec Secure Ops, les industriels s'appuient sur leurs personnels, processus et technologies pour :

- automatiser l'identification des ressources et de la procédure de gestion de stock au niveau 1 du modèle industriel de Purdue ;
- renforcer la sécurité en mettant à jour les systèmes, en limitant l'accès à distance et en surveillant la conformité ;
- automatiser le processus de téléchargement et de distribution des correctifs système et des mises à jour d'antivirus ;
- obtenir des informations opérationnelles grâce aux techniques d'apprentissage automatique et d'analyse comportementale pour signaler les erreurs système et humaines ou les incidents causés par des malwares ;
- augmenter le taux de rendement global et la productivité par une réduction des pannes ;
- augmenter la visibilité et le contrôle des coûts avec moins de complexité et plus de cohérence ;
- gérer plus facilement la cybersécurité et la conformité, site par site ;
- résoudre les problèmes liés au manque de personnel qualifié pour gérer et contrôler la cybersécurité.

La sécurité physique, votre première ligne de défense

Les attaques les plus sérieuses auxquelles les industriels sont confrontés sont celles impliquant des cybercriminels qui parviennent à entrer dans les usines et qui causent des dommages de l'intérieur. Qu'il s'agisse d'éviter les vols de ressources ou les pertes de données, les entreprises peuvent bénéficier d'une solution de sécurité physique complète intégrée à un réseau industriel filaire et sans fil sécurisé.

Les préoccupations liées à la sécurité physique ont poussé Del Papa Distributing, un distributeur régional de bière situé au Texas, à implémenter des systèmes de sécurité et de surveillance Cisco basés sur l'IP dans l'architecture de son nouveau siège de 10 hectares près de la côte du Golfe du Mexique. « Nous voulions que notre nouveau centre de distribution dispose d'un réseau simple et sécurisé pour assurer la sécurité physique, la communication, la collaboration et même la surveillance de la température de notre stock », indique Steve Holtsclaw, responsable des systèmes de données chez Del Papa.

En collaboration avec Zones, un partenaire de Cisco, le distributeur a établi un réseau IP sécurisé incluant des solutions Cisco pour la vidéosurveillance, le contrôle des accès physiques, les panneaux numériques, les capteurs de température et plus encore. Des caméras IP surveillent le périmètre de la propriété, un entrepôt de 9 290 mètres carrés, les couloirs du bureau et toutes les portes où s'effectuent les livraisons. Le système alerte les collaborateurs lorsque la porte d'une zone restreinte est ouverte et fournit un lien vers la vidéo en direct. Les portes peuvent être ouvertes et fermées en appuyant sur le bouton d'un téléphone IP.

La sécurité physique et le système de surveillance ne sont qu'une partie de l'architecture réseau convergée globale de Del Papa, qui comprend également des solutions de communications unifiées et de collaboration Cisco qui ont permis d'améliorer la sécurité et l'efficacité de l'entreprise. « L'Internet des objets fait partie intégrante de notre monde moderne », explique Stephen Lurie, vice-président et responsable de l'Internet des objets, chez Zones. « En misant sur la connexion de son architecture, Del Papa Distributing a pu améliorer sa sécurité physique et ses processus commerciaux. »

La traduction d'adresses réseau : plus de flexibilité et de sécurité

Les industriels doivent relever des défis spécifiques dans les environnements d'usine connectés à Internet. L'un de ces défis est dû au fait que les machines industrielles et les composants des machines utilisent souvent la même plage d'adresses IP. Cela complique la réplication des équipements sur site, car il arrive souvent qu'une adresse IP se retrouve en double et génère une erreur dans l'architecture IACS. Les industriels sont alors contraints d'engager d'importants frais de développement et de mise en service de machine pour y pallier.

Cisco et Rockwell Automation ont résolu ce problème ensemble (tout en améliorant la sécurité) avec une solution de traduction d'adresses réseau (NAT) spécialement conçue pour les environnements d'usine convergés par Ethernet. Basée sur les normes du secteur, l'architecture de Cisco et de Rockwell offre à ces industriels un avantage de taille, à savoir la possibilité de réutiliser leur nombre fini d'adresses IP. Étant donné que plusieurs machines et porte-palettes peuvent avoir les mêmes adresses IP, la solution facilite le dépannage et le maintien en conditions opérationnelles du matériel. La durée de la mise en service peut également être considérablement réduite en mappant rapidement et facilement les adresses IP en double.

Les solutions NAT peuvent également améliorer la sécurité quand elles sont configurées pour ne présenter au monde extérieur qu'une adresse pour le réseau entier, ce qui permet de masquer efficacement le réseau interne de l'industriel. Les industriels les plus avancés utilisent de plus en plus les solutions NAT à la fois pour la conservation d'adresses et la sécurité, en particulier dans les environnements distants.

La protection de la périphérie

Une partie stratégique d'un réseau d'une usine est la périphérie d'Internet, où le réseau de l'entreprise rencontre le réseau Internet public. La périphérie d'Internet fonctionne comme une passerelle entre les industriels (et autres entreprises) et le reste du cyberespace. Elle dessert aussi à d'autres éléments des réseaux d'entreprise. Étant donné que les utilisateurs des réseaux accèdent à des sites web et utilisent la messagerie pour les communications interentreprises (B2B), les ressources du réseau doivent demeurer à la fois accessibles et sécurisées.

Cisco offre une approche modulaire de la périphérie d'Internet, permettant d'adapter et de personnaliser la conception du réseau pour répondre aux besoins de chaque client et aux modèles commerciaux, quelles que soient leur taille et leurs exigences. Les industriels se tournent vers Cisco pour obtenir une sécurité « à la périphérie » et limiter les nombreuses menaces qui visent cette zone essentielle du réseau. Cisco propose des solutions et des conceptions validées comprenant les fonctions suivantes :

- **Pare-feu et prévention des intrusions.** Protège l'infrastructure réseau et les données contre les menaces Internet telles que les vers, les virus et des attaques ciblées.
- **Accès à distance et VPN.** Offre un accès sécurisé et homogène aux ressources du réseau depuis des sites distants.
- **Sécurité de la messagerie.** Fournit des services de filtrage des spams et des malwares, qui permettent d'éviter les pertes de données et les baisses de productivité des utilisateurs du réseau.
- **Sécurisation du web.** Surveille et contrôle l'utilisation acceptable tout en gérant l'augmentation des risques associés à la navigation sur Internet.

Connexion sécurisée des machines

Parmi les directeurs et responsables d'usine interrogés lors d'un récent sondage au sujet des éléments qu'ils connectaient et prévoyaient de connecter à leur réseau, 62 % ont déclaré que les équipements de production figuraient au sommet de leur liste. Et le nombre d'équipements à connecter est faramineux. Selon certaines estimations, on compterait 60 millions de machines réparties dans les usines du monde entier, et 90 % d'entre elles ne sont pas connectées.[4] Ce nombre de connexions est voué à augmenter, car de plus en plus d'industriels tirent parti des technologies IoT pour connecter leurs machines et robots au-delà de leurs ateliers de production, jusqu'aux constructeurs des machines.

Cisco montre la voie en matière de sécurisation de la connexion des machines sur les sites de production du monde entier. Conçue pour permettre une connexion rapide et répétable des machines, la solution Cisco Connected Machine est une gamme de solutions numériques qui améliore le taux de rendement global, la maintenance prédictive et l'optimisation des processus. Elle fournit aux constructeurs de machines et aux industriels qui utilisent ces machines des technologies de commutation, de sécurité et de traitement intégrées aux machines ou liées à celles-ci. La solution intègre par ailleurs des fonctions d'analyses du cloud et de la périphérie qui prennent en charge la surveillance et la maintenance prédictives des machines.

Synthèse

Les industriels entrent dans l'ère des usines connectées. Les opérateurs industriels ne sont plus isolés des autres usines, fournisseurs ou sièges sociaux et atteignent des niveaux de productivité, de qualité et de visibilité jusqu'à présent inédits. Malheureusement, ces réseaux plus vastes et plus complexes sont aussi plus vulnérables aux cyberattaques et aux failles de sécurité, contre lesquelles il est toujours plus difficile de se défendre. L'essor de l'IoT se poursuit et dans son sillage s'est formé un plus large écosystème de machines connectées qui ajoute une nouvelle dimension au challenge que représente la sécurité.

Les industriels relèvent ce challenge et en retirent même un avantage concurrentiel, en mettant en œuvre la nouvelle génération de solutions de sécurité intégrées conçues pour l'IoT. Ces solutions réunissent plusieurs couches de défense pour protéger la propriété intellectuelle et les ressources physiques contre les failles involontaires et le cybervol, tout en accélérant la résolution des menaces, en réduisant les risques de panne et en augmentant l'efficacité de tous les équipements.

Les solutions de sécurité Connected Factory de Cisco et de ses partenaires définissent les normes dans ce nouvel environnement, offrant aux industriels tels que Diebold, DG, Air Liquide et des milliers d'autres une solution de sécurité efficace et robuste pour leurs usines, qui protège également la réputation de leurs marques et ouvre la voie vers une croissance future.

[4] IHS 2014 Machines Report for Cisco, PWC Internet of Things in Manufacturing 2015, McKinsey Disruptive Technologies 2013 Report

Évaluez la cybersécurité de votre environnement industriel

Vos systèmes industriels sont-ils vulnérables aux attaques ? Cisco vous propose d'effectuer une évaluation des vulnérabilités et des risques de cybersécurité. Nous commencerons par examiner l'infrastructure de votre système de contrôle industriel, vos réseaux et vos processus pour comprendre les risques et les vulnérabilités. Ensuite, nous vous aiderons à justifier auprès de vos supérieurs les futurs investissements en matière de cybersécurité en quantifiant les risques financiers pour l'entreprise et en rationalisant des solutions de cybersécurité spécifiques capables de réduire les risques majeurs de cybersécurité identifiés. En élaborant une justification commerciale et un plan d'action, Cisco vous aide à protéger vos systèmes contre les menaces actuelles et futures.

Êtes-vous satisfait de l'architecture de sécurité et de la conception de votre système de contrôle industriel ? Cisco peut vous aider à concevoir une architecture de cybersécurité industrielle de référence au niveau d'un seul site ou à l'échelle de toute l'entreprise pour vos réseaux OT. Nous nous proposons d'examiner les capacités de votre infrastructure réseau industrielle à protéger les ressources critiques de l'entreprise, et de vous offrir une évaluation complète et indépendante basée sur les bonnes pratiques de l'architecture et de la conception de votre réseau. Nos résultats et l'architecture de cybersécurité industrielle de référence qui en découlera vous fourniront un plan pour le renforcement de la sécurité du réseau, qui indiquera notamment où mettre en œuvre des contrôles de sécurité spécifiques et comment classer les systèmes en zones de sécurité spécifiques. Notre évaluation est conforme au modèle ISA-95 et à l'infrastructure de sécurité ISA-99/IEC-62443 et prend en compte tous les contrôles de sécurité nécessaires, y compris les produits et solutions déjà mentionnés dans ce livre blanc.

Pour en savoir plus : rendez-vous sur cisco.com/go/factorysecurity ou contactez-nous à l'adresse inquire-factorysecurity@cisco.com.