

LIVRE BLANC

Protéger l'industrie manufacturière avec une sécurité du plus haut niveau

Passez à l'authentification sans mot de passe, assurez l'intégrité des produits, sécurisez votre chaîne d'approvisionnement et évitez les temps d'arrêt



Sommaire

- 2 Table des matières
- 3 Garantir la résilience dans l'industrie manufacturière : faire face à la double réalité de l'IA
- 6 Modernisez le MFA et passez à l'authentification sans mot de passe pour un accès sécurisé des utilisateurs aux systèmes et données stratégiques
 - 6 Principaux éléments à prendre en compte pour l'authentification dans les environnements IT et OT
 - 9 Inconvénients de l'authentification classique
 - 10 Qu'est-ce que l'authentification résistante au phishing ?
 - 10 Que sont les passkeys ?
 - 11 L'avenir repose sur une authentification sans mot de passe
 - 12 Communication homme-machine sécurisée avec la YubiKey
- 14 Sécurisation de la chaîne d'approvisionnement pour l'industrie manufacturière
 - 14 Protection des accès tiers
 - 14 Assurance d'une intégrité maximale pour les pièces de vos produits
 - 15 Sécurisation du code et des données externes
 - 15 Communication machine à machine sécurisée avec la YubiHSM 2
 - 16 Prise en charge des environnements d'infrastructure à clé publique (PKI)
- 17 Étude de cas : Sécuriser les systèmes et la chaîne d'approvisionnement chez Schneider Electric
- 18 Étude de cas : Mitsubishi Electric renforce la cybersécurité mondiale avec la YubiKey
- 18 Étude de cas : Une chaîne de confiance portative pour EasyMile afin de sécuriser les véhicules autonomes
- 19 Déploiement rapide et fluide des systèmes sans mot de passe à grande échelle
- 20 Résumé

+ de 180 000



systèmes ICS/OT sont exposés
chaque mois à Internet.⁸

72 %



des attaques ciblant les
systèmes OT ont utilisé l'IT
comme point d'entrée.⁹

3 300



organisations industrielles ont
vu leurs données publiées
sur des sites de fuite de
ransomware en 2025.¹⁰

42 %



des intrusions (phishing, malware,
ransomware) ont entraîné des
pannes opérationnelles qui ont
affecté les revenus.¹¹

78 %



des RSSI estiment que les
cybermenaces pilotées par l'IA
ont déjà un impact significatif
sur leur organisation.¹²

Garantir la résilience dans l'industrie manufacturière : faire face à la double réalité de l'IA

Pendant cinq années consécutives, l'industrie manufacturière est restée le secteur le plus ciblé au monde, représentant 27,7 % de tous les cyberincidents mondiaux.¹ Le secteur manufacturier reste la cible principale des attaques sophistiquées de malware, de ransomware, de phishing et de type Man-in-The-Middle (attaque MiTM). Ce ciblage s'explique par le rôle central du secteur dans la chaîne d'approvisionnement mondiale et par sa richesse en informations précieuses et en propriété intellectuelle. Cette pression est encore accentuée par l'émergence de l'intelligence artificielle (IA) : elle constitue un puissant outil de production pour les entreprises, mais est utilisée par des acteurs malveillants pour amplifier les vecteurs d'attaque. Dans ses formes les plus avancées, l'IA est désormais utilisée pour automatiser la communication en temps réel dans les campagnes de phishing. Ainsi, même les employés les plus vigilants ont de plus en plus de difficultés à distinguer les demandes authentiques de celles malveillantes.

Alors que l'informatique (IT) et les technologies opérationnelles (OT) continuent de se rapprocher, les complexités augmentent à mesure que des systèmes autrefois isolés sont intégrés à Internet. L'ampleur de cette exposition est d'ailleurs importante, avec plus de 180 000 systèmes de contrôle industriel (ICS) et environnements OT exposés au Web chaque mois.² Dans cet environnement, une approche sécurisée dès la conception n'est plus facultative : elle est primordiale. L'essor de la puissance définie par logiciel et de l'IA agentique, c'est-à-dire des agents spécialisés qui optimisent la production et gèrent les chaînes d'approvisionnement de manière autonome, introduit des couches de risque qui exigent que chaque point d'entrée potentiel soit protégé contre les accès non autorisés. Plus précisément, les agents d'IA bénéficiant d'un accès privilégié pourraient être manipulés pour provoquer des perturbations physiques ou opérationnelles significatives, et pourraient potentiellement entraîner des dommages matériels ou des pertes humaines.

Les enjeux financiers de toutes les interruptions liées aux cyberattaques sont impressionnants. Les entreprises de l'industrie manufacturière sont confrontées à des coûts de brèche de données de 5 millions de dollars en moyenne³, ainsi qu'à une perte potentielle de propriété intellectuelle et d'intégrité des produits. Les conséquences de l'attaque Colonial Pipeline 2021 rappellent avec force la nécessité d'une résilience opérationnelle et d'une visibilité de la chaîne d'approvisionnement. Le coût estimé des temps d'arrêt imprévus étant de 50 milliards de dollars par an pour l'industrie,⁴ et étant donné que 42 % des intrusions entraînent des interruptions opérationnelles qui ont un impact direct sur les revenus,⁵ la sécurisation des communications homme-machine et machine-machine est essentielle à la continuité de l'activité.

Même si les organisations qui ont signé des contrats avec le gouvernement respectent depuis longtemps des normes strictes telles que FIPS, DFARS et ISO 9001, les récentes attaques de grande envergure ont déclenché un renforcement des exigences réglementaires. En janvier 2026, l'Alliance Five Eyes, l'Allemagne et les Pays-Bas ont publié de nouvelles directives : les Principes de connectivité sécurisée pour l'OT.⁶ Cette orientation conjointe souligne le fait que, bien que la connectivité entre les systèmes IT et OT soit essentielle, elle doit suivre un modèle sécurisé dès la conception, qui privilégie le renforcement de la frontière OT par l'utilisation d'une authentification résistante au phishing.

Pourquoi l'accent est-il si fortement mis sur l'authentification multi-facteurs (MFA) résistante au phishing ? La réalité est que les solutions traditionnelles, en particulier les noms d'utilisateur, les mots de passe et les authenticateurs mobiles, ne sont plus efficaces contre les menaces optimisées par l'IA. Une étude portant sur 350 000 tentatives de piratage en situation réelle a révélé que les mots de passe à usage unique (OTP) basés sur SMS n'ont bloqué que 76 % des attaques ciblées, tandis que les notifications push en ont bloqué 90 %.⁷ Le taux de pénétration minimum est donc de 10 %, ce qui signifie qu'avec le MFA classique, une attaque réussie n'est plus une probabilité, mais une certitude.

Les entreprises de l'industrie manufacturière sont conscientes de l'urgence de moderniser les systèmes d'authentification et de sécurité dans les environnements IT et OT convergés. Cette évolution est essentielle non seulement pour garantir un accès fluide aux données et systèmes critiques, mais également pour protéger l'intégrité et la propriété intellectuelle de chaque composant du cycle de vie de la production. Cependant, la vitesse sans précédent de l'IA et la sophistication croissante des cybermenaces ont entraîné un ensemble unique de défis qui ont un impact sur ce secteur :

Défis rencontrés dans le secteur de l'industrie manufacturière



Infrastructure
existante



IA agentique
et autonomie



Environnements
de postes de
travail partagés



Utilisation intensive,
environnements
imposant le port
de gants



Zones mobiles
restreintes



Gestion de la chaîne
d'approvisionnement



Problèmes de
perturbation
du travail



Intégrité des
composants
du produit



Protection de la propriété
intellectuelle pour l'industrie
manufacturière
et la conception

Les opérations de l'industrie manufacturière s'appuient souvent sur les équipements et applications de production existants, ce qui peut souvent imposer des contraintes sur l'évolutivité et l'interopérabilité des solutions de sécurité modernes. De plus, la séparation traditionnelle entre les systèmes de l'industrie manufacturière et les réseaux informatiques d'entreprise ne correspond plus à la réalité des écosystèmes de fabrication intégrés actuels.

Cette connectivité accrue a ouvert la voie à une transformation plus profonde : la transition des tâches manuelles vers les actions autonomes machine à machine. À cette époque où les agents IA gèrent les chaînes de production et d'approvisionnement sans une intervention humaine constante, les points d'entrée de ces agents deviennent des cibles de cyberattaque de premier plan pour les mouvements latéraux et l'escalade des privilèges. Le renforcement de ces limites autonomes avec des références matérielles est désormais essentiel pour empêcher les actions de contrôle non autorisées, qui pourraient entraîner des dommages physiques ou des pannes générant un impact sur les revenus.

Les environnements de postes de travail partagés sont également courants dans l'industrie manufacturière, où l'on utilise souvent des systèmes d'exploitation non pris en charge avec un minimum de contrôles d'entreprise et un manque de privilèges d'accès définis. Un employé standard dans l'industrie manufacturière peut accéder à plus de 27 000 fichiers sensibles (par exemple, des données financières, des informations sur la chaîne d'approvisionnement, de la propriété intellectuelle) dès son premier jour de travail.¹³ L'authentification peut être une première ligne de défense pour se protéger contre les cybermenaces, mais la dépendance à des méthodes d'authentification classiques telles que le nom d'utilisateur et le mot de passe, ainsi que l'authentification mobile, peut exposer les organisations manufacturières à un risque plus élevé de violation.

70 %

des violations du cloud
proviennent principalement
d'identités compromises,
et non de failles logicielles.¹⁴

60 %



des interactions avec le service
d'assistance informatique sont
associées à la réinitialisation
des mots de passe.¹⁶

Les informations d'identification compromises restent le point d'entrée d'attaque le plus courant : 70 % des brèches de cloud proviennent d'identités compromises, et non de failles logicielles.¹⁴ Les mots de passe peuvent également augmenter les coûts du service d'assistance informatique liés à la réinitialisation des mots de passe. L'idéal est de passer à un avenir sans mot de passe en éliminant complètement ces derniers. Un employé standard doit utiliser et retenir 191 mots de passe, un facteur de complexité et de frustration pour les utilisateurs.¹⁵ À l'heure actuelle, pour une entreprise moyenne, 60 % des interactions avec le service d'assistance informatique sont liées à la réinitialisation des mots de passe.¹⁶ Outre les coûts informatiques, les entreprises perdent en moyenne 5,2 millions de dollars par an en productivité suite au verrouillage des comptes.¹⁷

Dans l'industrie manufacturière, il est essentiel de garantir l'authenticité de tous les composants afin d'éviter toute réplique non sollicitée et tout vol, mais également pour l'assurance qualité. En effet, une chaîne d'assemblage ne doit se composer que de produits d'origine réelle, car l'ensemble est toujours la somme de ses pièces. Les lignes de production de divers composants de produits peuvent provenir de différentes usines de fabrication ainsi que d'installations de fabrication tierces dans le monde entier. Des problèmes d'intégrité des produits peuvent survenir si les micrologiciels des composants ne sont pas signés numériquement ni certifiés, pour garantir l'authenticité et l'intégrité des composants à la fin des lignes de production respectives. Il est également important de s'assurer que seuls des composants authentiques sont utilisés lors de l'entretien ou du remplacement par un revendeur tiers.

Les leaders de l'industrie manufacturière ont besoin de solutions hautement fiables, qui offrent des fonctionnalités de sécurité modernes tout en facilitant la transition vers un flux de travail sans mot de passe. Cette évolution est essentielle non seulement pour optimiser l'expérience utilisateur et l'efficacité globale, mais également pour renforcer l'organisation face à l'évolution rapide des menaces. En outre, ces solutions doivent prendre en charge un déploiement rapide à grande échelle afin de préserver la qualité, l'intégrité et la propriété intellectuelle de chaque composant tout au long du cycle de vie, de la production initiale à l'assemblage, en passant par la réparation et le remplacement en aval. Pour s'assurer qu'une chaîne d'assemblage reste un écosystème fermé de produits issus d'une source réelle, les entreprises doivent établir une racine de confiance cryptographique qui protège l'ensemble de la chaîne de valeur.





Sécurité



Productivité



Fiabilité



Durabilité



Coût

Modernisez le MFA et passez à l'authentification sans mot de passe pour un accès sécurisé des utilisateurs aux systèmes et données stratégiques

Lors de l'étude de solutions d'authentification pour améliorer la sécurité des systèmes informatiques et OT dans l'industrie manufacturière, il est important de prendre en compte l'efficacité de la solution en matière de protection contre les cyberattaques externes, y compris celles basées sur l'IA, et les menaces internes, ainsi que son impact sur la productivité des utilisateurs et sa fiabilité dans des environnements variés.

Principaux éléments à prendre en compte pour l'authentification dans les environnements informatiques et OT

Les cinq exigences d'authentification essentielles que les entreprises de l'industrie manufacturière doivent prendre en compte sont indiquées à gauche :



SÉCURITÉ

Comment vous assurez-vous que seuls les utilisateurs autorisés accèdent à un équipement partagé ?

Comment sécuriser les terminaux et appareils partagés que l'on trouve souvent dans les entreprises de l'industrie manufacturière avec plusieurs utilisateurs en rotation, en s'assurant que les comptes utilisateurs sont sûrs et que les utilisateurs n'ont accès qu'aux applications, services et données auxquels ils doivent avoir accès ?

Actuellement, 44 % des entreprises de l'industrie manufacturière disposent de plus de 1 000 comptes « utilisateur fantôme » liés à des comptes d'utilisateur et de service inactifs.¹⁸

Les comptes administrateurs ou les postes de travail partagés avec accès à des informations privilégiées doivent être protégés par un mécanisme d'authentification qui rend impossible l'usurpation d'identité.

Les postes de travail partagés doivent s'appuyer fortement sur les autorisations des utilisateurs et les contrôles d'accès (pas de connexions partagées, d'invités ou anonymes), et présenter des restrictions empêchant la sauvegarde des mots de passe. Les comptes administrateurs doivent également être individuels et non partagés, afin de permettre un dépannage en personne ou à distance.

En outre, dans le contexte de l'industrie manufacturière, il est important de s'assurer que la solution d'authentification n'introduit pas de nouveaux défis en matière de sécurité. Par exemple, de nombreuses entreprises de l'industrie manufacturière ont dû mettre en œuvre des politiques liées aux appareils portables pour maintenir les téléphones en dehors de l'atelier, en raison des perturbations de la productivité et des dangers potentiels d'une utilisation inappropriée des téléphones portables : en effet, elle peut entraîner une inattention lors d'une tâche à accomplir ou face à l'environnement, ce qui est à la fois dangereux et coûteux dans un environnement de fabrication.



SÉCURITÉ

Comment vous assurez-vous que la personne qui se connecte à une machine est l'utilisateur légitime ?

Lors de l'évaluation des solutions d'authentification, il est crucial de reconnaître que les priorités en matière de cybersécurité diffèrent considérablement entre les environnements IT et OT. Dans l'IT, l'accent est mis sur la triade de la CIA : la confidentialité, l'intégrité et la disponibilité des données. Cependant, au sein de l'OT, la priorité passe au modèle AIC (Availability, Integrity, Confidentiality), où la disponibilité, l'intégrité et la confidentialité sont les piliers essentiels. Une fiabilité et une sécurité accrues sont également primordiales pour l'OT, car bien qu'une violation de l'IT puisse entraîner une perte de données, les pratiques non sécurisées en OT peuvent avoir des impacts physiques dévastateurs.

La sécurité OT exige une protection hautement fiable pour garantir la disponibilité opérationnelle et améliorer les protocoles de sécurité qui protègent directement des vies humaines. Alors que l'IT et l'OT continuent de converger, la surface d'attaque s'élargit. La limite de l'OT est une cible principale pour le mouvement latéral. L'authentification doit être résistante à l'usurpation d'identité pour empêcher les actions de contrôle non autorisées qui perturbent les fonctions critiques.



PRODUCTIVITÉ

Comment s'assurer que l'utilisateur est en mesure de s'authentifier facilement sur plusieurs appareils et applications ?

44 %



des entreprises de l'industrie manufacturière disposent de plus de 1 000 comptes « utilisateur fantôme » liés à des comptes d'utilisateur et de service inactifs.¹⁸

54 %



des employés pensent que les solutions d'authentification à deux facteurs, telles que les mots de passe à usage unique et les codes push, perturbent leur flux de travail quotidien.¹⁹

Tout mécanisme d'authentification adopté doit permettre aux employés de s'authentifier rapidement et facilement, afin d'éviter les perturbations du flux de travail et les solutions de contournement non approuvées, comme le partage de mots de passe. Actuellement, 54 % des employés pensent que les solutions d'authentification à deux facteurs (2FA), telles que les mots de passe à usage unique et les codes push, perturbent leur flux de travail quotidien.¹⁹ De plus, si l'accès aux systèmes est peu fréquent, comme pour les systèmes RH ou de paie, le risque d'oubli des mots de passe et de verrouillage de compte est élevé.

Toutes les formes de MFA n'offrent pas l'équilibre optimal entre une sécurité renforcée et une expérience utilisateur simple et rapide, favorisant une productivité élevée. Les authenticateurs mobiles augmentent le nombre d'étapes du processus d'authentification, ce qui oblige les utilisateurs à attendre le mot de passe à usage unique, les codes d'application push, ou à retirer leurs gants pour interagir avec un appareil. En outre, ces processus sont soumis aux limites des environnements mobiles restreints et aux règles syndicales.

Quel que soit le scénario, il faut tenir compte du temps nécessaire à l'authentification et du nombre de fois qu'un utilisateur devra s'authentifier au cours d'une journée ou d'un quart de travail. Prenez également en compte la taille du service informatique et le temps moyen de traitement des verrouillages de compte, ce qui contribue au temps d'arrêt de la production et aux coûts directs de main-d'œuvre. Lorsque les exigences d'efficacité sont élevées, envisagez une expérience d'authentification sans mot de passe ou l'avantage d'une expérience NFC par simple contact avec des appareils portables, dans la mesure du possible, en particulier dans le cas des postes de travail partagés.



FIABILITÉ

Comment garantir une authentification fiable qui fonctionne en permanence, même dans des environnements difficiles avec différents points de défaillance ?

L'authentification est un service stratégique. Si les employés ne peuvent pas se connecter aux applications ou aux portails qu'ils utilisent, ils ne peuvent pas faire leur travail. Toute solution d'authentification doit être fiable pour chaque utilisateur et exclure les points de défaillance courants, qu'il s'agisse de la connectivité, de la batterie de l'appareil, de la réception cellulaire ou de la batterie de tokens matériels. Les solutions d'authentification doivent également être dotées de fonctionnalités telles que la technologie NFC, adaptées à des environnements tels que la fabrication industrielle, les salles blanches ou les environnements caractérisés par une atmosphère explosive.

Il faut savoir que toute solution d'authentification reposant sur « quelque chose que vous connaissez » (comme un mot de passe) est sujette à l'erreur humaine (perte, oubli ou erreur de frappe) qui alourdit l'expérience d'authentification et risque de bloquer l'accès des utilisateurs à leurs comptes. De plus, les solutions d'authentification mobile ne sont pas toujours fiables dans les environnements à postes de travail partagés, où la couverture cellulaire est irrégulière ou inexistante. C'est le cas par exemple dans les environnements OT, ou lorsque les utilisateurs sont dépendants de la batterie de l'appareil dans le cas de l'authentification mobile.



DURABILITÉ

Comment vous assurez-vous que le produit peut résister aux conditions difficiles de l'atelier ?

Toute solution déployée dans un site de fabrication doit être capable de résister aux rigueurs quotidiennes de cet environnement. La présence d'équipements lourds et mobiles, de surfaces dures et de gants épais de protection augmente le risque d'endommagement des solutions d'authentification sur le lieu de travail. Outre la résistance à l'écrasement et la capacité à résister à un nettoyage régulier, la solution de votre choix doit être certifiée IP68 pour garantir une résistance totale à la poussière et à l'eau.

Il est important de noter que la durabilité doit englober la sécurité humaine. Une solution d'authentification hautement fiable est intrinsèquement sûre. Elle offre une conception sans batterie et résistante aux étincelles, qui réduit les risques physiques au lieu d'introduire de nouveaux dangers dans l'usine. En éliminant les distractions et les failles de sécurité inhérentes au MFA mobile, vous vous assurez que la protection du système ne se fait jamais au détriment de la protection des vies humaines.





COÛT

Comment réduire le nombre de tickets d'assistance liés à l'authentification ?

Toute forme d'authentification classique, comme les noms d'utilisateur et les mots de passe, et l'authentification mobile appliquée et mise en œuvre à grande échelle, nécessitera une mise en œuvre des politiques, une formation des utilisateurs et une assistance informatique permanentes. Même les formes d'authentification mobile 2FA et MFA les plus simples, telles que les mots de passe à usage unique par exemple, créent une charge de travail considérable pour l'assistance si les codes tardent à arriver, si les utilisateurs se voient bloquer l'accès à leur compte ou s'ils doivent enregistrer de nouveaux appareils. En outre, les syndicats peuvent exiger que les entreprises prennent en charge le coût total de l'appareil, y compris les coûts matériels, les coûts de service récurrents, la gestion des appareils d'entreprise et les logiciels de sécurité, ainsi que les coûts de remplacement du téléphone en raison de la casse inévitable qui peut se produire dans les environnements de production.

Chaque fois qu'un utilisateur rencontre des difficultés avec l'authentification mobile, il n'est pas productif. Plus un employé peut s'authentifier et faire son travail rapidement et en toute sécurité, ou même réinitialiser son mot de passe par lui-même si nécessaire, plus le retour sur investissement est élevé.



Inconvénients de l'authentification classique

Fiabilité et sécurité faibles, friction et coûts élevés

Il est important de noter que, même si toute forme de 2FA ou de MFA offre plus de sécurité que les mots de passe seuls, l'authentification classique repose toujours sur les mots de passe comme premier facteur, toujours non sécurisé, inefficace et source de frustration pour les employés. Et cette frustration entraîne des solutions de contournement dangereuses, telles que le partage de mots de passe, la réutilisation de mots de passe sur plusieurs comptes ou l'enregistrement de mots de passe dans le navigateur ou l'application, où ils peuvent être vulnérables.

En outre, dans le cas du MFA mobile (SMS, OTP et application push), le second facteur est lié à l'appareil portable. C'est un signal d'alarme, et ce pour quatre raisons :

1. Il peut y avoir des problèmes de disponibilité lorsque les appareils portables n'envoient pas les codes en temps voulu, en raison d'une mauvaise connectivité ou de services peu fiables.
2. Il n'est pas réellement garanti que la clé privée soit stockée dans une zone sécurisée de l'appareil portable.
3. Le mot de passe à usage unique ou la clé privée peuvent être interceptés par divers moyens, comme un échange de cartes SIM.
4. Il est impossible de garantir la preuve de possession, ou en termes NIST, de prouver qu'elle résiste à l'usurpation d'identité.

L'authentification mobile classique est sujette aux cyberattaques modernes, notamment le phishing, les attaques par force brute, les attaques de type Man-in-the-Middle, les malwares et l'échange de cartes SIM mentionné précédemment. Outre les questions de sécurité, l'authentification mobile classique comporte de nombreux coûts cachés liés à la perte de productivité, au coût des appareils, à une assistance IT accrue et à des frictions au niveau de l'expérience utilisateur. En fait, 43 % des organisations citent l'expérience utilisateur comme le principal obstacle à l'utilisation d'une solution MFA.²⁰ Pour en savoir plus, consultez notre livre blanc :

[Les 5 principales idées reçues concernant l'authentification mobile : déconstruire le mythe par rapport à la réalité du MFA classique.](#)

Le remplacement de l'authentification à facteur unique (nom d'utilisateur et mot de passe) classique par une authentification multi-facteurs (MFA) résistante au phishing est la première étape du renforcement des pratiques de sécurité.

Taux de risque de piratage de compte



0%

Clé de sécurité FIDO (YubiKey)

10 %

Message sur appareil

21 %

Secondaire

24 %

Code SMS

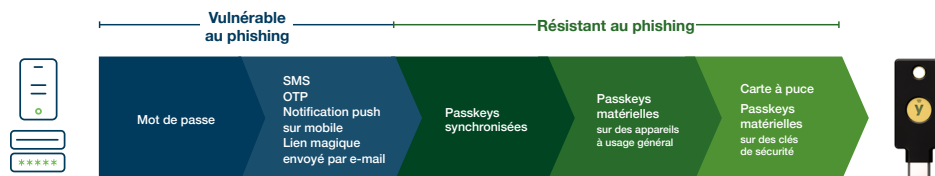
50 %

Numéro de téléphone

Google, [How effective is basic account hygiene at preventing account takeovers](#)

Qu'est-ce que l'authentification résistante au phishing ?

Les processus d'authentification résistante au phishing reposent sur la vérification cryptographique entre des appareils ou entre un appareil et un domaine, ce qui les immunise contre les attaques qui tentent de compromettre ou de perturber le processus d'authentification. D'après la publication spéciale (SP) 800-63 du NIST, seuls deux types d'authentification sont résistants au phishing : les cartes à puce/PIV et le standard d'authentification moderne FIDO2/WebAuthn.



Que sont les passkeys ?

« Passkeys » est le nouveau nom utilisé pour désigner les informations d'identification sans mot de passe FIDO2, une norme qui est en train de remplacer les mots de passe et connexions MFA vulnérables au phishing par des méthodes sans mot de passe plus sécurisées. Il existe différents modes de mise en œuvre des passkeys :

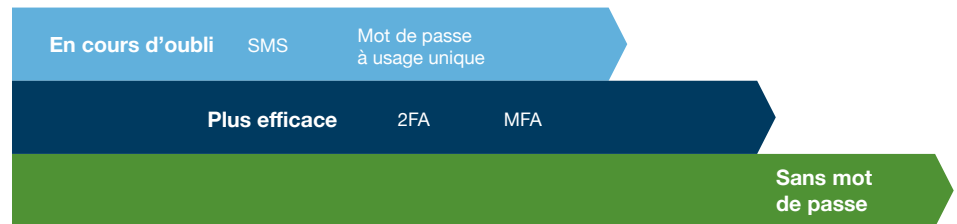
Les **passkeys synchronisées** sont stockées dans le cloud, ce qui signifie que les informations d'identification d'un smartphone, d'une tablette ou d'un ordinateur portable peuvent être partagées entre différents appareils. Si les passkeys synchronisées facilitent la récupération des informations d'identification en cas de perte ou de vol d'un téléphone ou d'un ordinateur portable, les informations d'identification FIDO sont quant à elles plus difficiles à retracer. Elles sont donc adaptées à des contextes ne nécessitant pas une sécurité extrêmement élevée.

Les **passkeys matérielles** offrent aux entreprises un meilleur contrôle de leurs informations d'identification FIDO par rapport aux passkeys synchronisées. Il existe différents types de passkeys matérielles : certaines sont stockées dans des appareils à usage général (smartphones, ordinateurs portables, tablettes), d'autres dans des clés de sécurité matérielles spécialement conçues pour une sécurité renforcée. Les passkeys matérielles intégrées à des clés de sécurité FIDO modernes sont celles qui offrent les meilleures garanties en matière de sécurité. Elles fournissent aux entreprises des capacités fiables d'attestation et de gestion du cycle de vie des informations d'identification. Grâce à ce type de passkeys, les entreprises peuvent offrir l'expérience la plus simple possible d'intégration des utilisateurs et de récupération des informations d'identification sur l'ensemble des appareils et des plateformes, tout en se conformant aux réglementations les plus strictes.



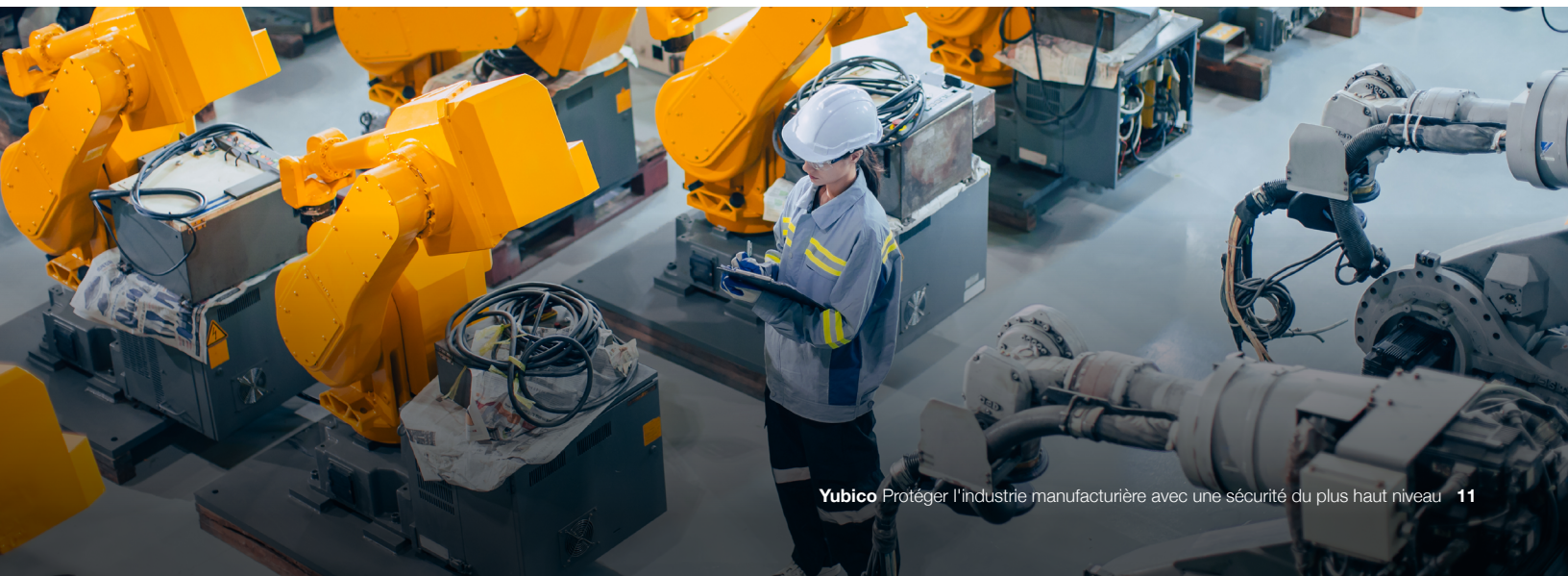
L'avenir repose sur une authentification sans mot de passe

Le passage de l'authentification multi-facteurs (MFA) classique au MFA résistant au phishing est une étape clé dans la sécurisation des environnements OT et informatiques dans l'industrie manufacturière. Mais la prochaine étape du MFA moderne consiste à introduire l'authentification sans mot de passe. Les actions de l'utilisateur étant en fin de compte la plus grande faiblesse de l'authentification classique, et l'authentification en plusieurs étapes contribuant fortement à l'insatisfaction de l'utilisateur, la meilleure pratique mondiale tend vers une authentification sans mot de passe, c'est-à-dire une authentification qui n'exige pas de l'utilisateur qu'il fournisse un mot de passe lors de la connexion.



Les cartes à puce traditionnelles sont une autre forme de cartes sans mot de passe qui offrent une sécurité élevée, mais qui nécessitent généralement des dépenses d'investissement élevées pour les lecteurs de cartes à puce, les cartes et les plateformes de gestion back-end. La technologie de carte à puce est principalement mise en œuvre dans les environnements sur site. En fonction de vos besoins, les cartes à puce peuvent vous convenir. Le secteur dans son ensemble s'oriente vers un flux de connexion sans mot de passe exploitant des normes d'authentification modernes, telles que FIDO2/WebAuthn, qui sont parfaitement compatibles avec le cloud.

La norme d'authentification moderne FIDO (Fast Identity Online) permet une authentification forte à deux facteurs, multi-facteurs et sans mot de passe. La norme FIDO a été créée par la FIDO Alliance, une association industrielle ouverte dont la mission est de réduire la dépendance aux mots de passe. FIDO2/WebAuthn est la norme FIDO la plus récente. Elle fait appel à la cryptographie à clé publique pour une sécurité élevée, les clés privées ne quittant jamais l'authentificateur. Pour les entreprises de l'industrie manufacturière qui disposent de systèmes OT classiques et d'une faible tolérance aux tâches non productives, les clés de sécurité matérielles FIDO2 offrent une authentification multi-facteurs et sans mot de passe avec une sécurité et une expérience utilisateur élevées qui n'étaient pas accessibles jusqu'à présent. Les clés de sécurité matérielles basées sur FIDO2 peuvent fournir une chaîne de confiance portable parfaitement adaptée aux environnements de postes de travail partagés et mobiles restreints.



La clé YubiKey



est la **seule** solution qui offre une résistance élevée au phishing et qui a prouvé qu'elle arrête **100 %** des tentatives de piratage de comptes dans des recherches indépendantes.²¹



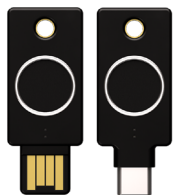
La série YubiKey 5

De gauche à droite : YubiKey 5 NFC, YubiKey 5C NFC, YubiKey 5Ci, YubiKey 5C, YubiKey 5 Nano et YubiKey 5C Nano



La série YubiKey 5 FIPS

De gauche à droite : YubiKey 5 NFC FIPS, YubiKey 5C NFC FIPS, YubiKey 5Ci FIPS, YubiKey 5C FIPS, YubiKey 5 Nano FIPS et YubiKey 5C Nano FIPS



YubiKey Bio Series - FIDO Edition

De gauche à droite : YubiKey Bio - FIDO Edition, YubiKey C Bio - FIDO Edition

yubico

Securing Operational Technology with Yubico

Hardening OT access to protect safety, uptime, and continuity



How expanded connectivity is reshaping cyber risk in operational technology
Operational Technology (OT) supports critical infrastructure including manufacturing, energy, healthcare, and government. These OT environments consist of large-scale machines and Industrial Control Systems (ICS), including Distributed Control Systems and SCADA, to manage physical processes including machine-to-machine and human-to-machine communication. Historically, these environments were designed to prioritize safety and uptime, rather than secure connectivity. By their nature, these systems are often considered shared workstations.

The guidance stresses that OT-IT connectivity is essential but must follow a secure-by-design model. It outlines eight principles to help organizations modernize connectivity while ensuring exploitability risk across industrial environments. Among these, hardening the OT boundary is identified as a strategic priority.
Principle 5: Why hardening the OT boundary is now a strategic imperative
The OT boundary is the critical contact point between these trusted operational systems and external networks.



Découvrez comment renforcer les frontières de l'OT avec Yubico

Communication homme-machine sécurisée avec la YubiKey

Une authentification résistante au phishing et une passerelle vers l'authentification sans mot de passe

Yubico propose la YubiKey, une clé de sécurité matérielle conçue pour offrir une sécurité du plus haut niveau, une grande facilité d'utilisation et une durabilité industrielle. Les passkeys matérielles, comme la [YubiKey](#), offrent la meilleure défense. Avec la YubiKey, les entreprises de l'industrie manufacturière peuvent déployer à grande échelle une authentification multi-facteurs et sans mot de passe résistante au phishing, avec une expérience utilisateur simple et rapide qui favorise une productivité élevée. La YubiKey garantit une résilience maximale en protégeant les secrets privés sur un élément sécurisé qui ne peut pas être exfiltré.

La YubiKey vous permet de sécuriser la communication homme-machine dans une ère de menaces basées sur l'IA, protégeant ainsi les systèmes IT et OT contre tout accès non autorisé. La YubiKey emploie des protocoles d'authentification modernes tels que les normes d'authentification ouvertes FIDO U2F et FIDO2, pour éliminer les attaques par phishing visant les informations d'identification. De plus, les YubiKeys prennent également en charge les protocoles SmartCard, OTP et OpenPGP, ce qui permet l'utilisation d'une seule clé de sécurité dans divers environnements IT et OT modernes et classiques, et avec diverses [solutions IAM tierces](#) telles que Microsoft, Okta, Duo et Ping, ainsi que l'authentification de [milliers d'applications et de services](#). La prise en charge multiprotocole permet aux fabricants d'utiliser la YubiKey comme passerelle vers l'authentification sans mot de passe, et de l'utiliser pour combler le fossé entre la sécurisation de l'infrastructure industrielle existante et les environnements cloud modernes.

Les YubiKeys sont extrêmement portables et simples à utiliser, ce qui permet d'améliorer la productivité des employés. La YubiKey offre une connexion rapide sans mot de passe par un simple appui sur un bouton, 4 fois plus rapide que la connexion par SMS. De plus, une seule YubiKey fonctionne sur plusieurs appareils, notamment les ordinateurs de bureau, les ordinateurs portables, les appareils mobiles, les tablettes et les postes de travail partagés. Elle est disponible dans différents formats, certains pouvant être attachés à un porte-clés, et offre des connecteurs USB-A, USB-C, NFC et Lightning.

Les YubiKeys offrent une sécurité robuste dans tous les ateliers de fabrication



ne nécessitent pas de batterie ni de connexion à Internet.



hautement durables, résistantes à la poussière, à l'écrasement et à l'eau (certifiée IP68).



adaptées aux environnements sans étincelles ou à faible risque d'étincelles.



sans installation de logiciel ni connexion cellulaire requise.

Afin d'améliorer encore davantage l'expérience utilisateur et la rapidité d'authentification, Yubico propose également la YubiKey Bio Series - FIDO Edition, qui prend en charge FIDO U2F et FIDO2. Elle assure la sécurité caractéristique de toutes les YubiKeys, avec une nouvelle expérience sans mot de passe basée sur la biométrie.

Pour les environnements hautement réglementés, les YubiKeys sont également disponibles dans des formats validés FIPS 140-3, qui répondent aux exigences les plus élevées en matière d'authentification de niveau 3 (AAL3) du NIST SP 800-63B.



Nous avons intégré les clés YubiKey dans nos systèmes SCADA de gestion de l'énergie pour renforcer la sécurité grâce au MFA. Ce processus permet à un opérateur d'entrer en service, de s'authentifier rapidement et de prendre les mesures appropriées, sans aucune interruption du système. Le MFA garantit que seuls les utilisateurs authentifiés peuvent accéder au système. »

Chad Lloyd

Directeur de l'architecture de cybersécurité pour la gestion de l'énergie | Schneider Electric



[En savoir plus](#)



Notre objectif était d'éliminer le piratage de compte en adoptant un MFA plus fort. L'adoption des YubiKeys nous a permis de faire progresser en permanence notre stratégie d'authentification. Notre objectif est d'activer l'authentification sans mot de passe pour tous les utilisateurs à l'avenir. »

M. Daisuke Okamoto

Division de la plate-forme IT | Mitsubishi Electric Digital Innovation



[En savoir plus](#)



Les YubiKeys sont rapides, robustes et de qualité supérieure : un matériel d'exception associé à une sécurité d'exception. C'est très simple et cela permet de gagner du temps par rapport aux personnes qui doivent entrer un TOTP, car il faut saisir six chiffres pour chaque compte. C'est beaucoup plus rapide d'appuyer sur une clé. »

Ángel Uruñuela

RSSI du groupe Fluidra

FLUIDRA

[En savoir plus](#)





Accès des tiers



Intégrité de la propriété intellectuelle et des produits



Signature de code sécurisée



Pour protéger de manière proactive notre chaîne d'approvisionnement, nous travaillons en étroite collaboration avec des fournisseurs clés afin de créer un double chiffrement, car le fournisseur et Schneider Electric disposent de modules YubiHSM 2 intégrés au processus de fabrication. »

Chad Lloyd

Directeur de l'architecture de cybersécurité pour la gestion de l'énergie
Schneider Electric

Schneider Electric En savoir plus

Sécurisation de la chaîne d'approvisionnement pour l'industrie manufacturière

Les chaînes d'approvisionnement de l'industrie manufacturière englobent le mouvement de biens et de composants physiques d'un point à l'autre, mais également les autres partenariats et relations commerciales qui soutiennent l'organisation, y compris les intégrations souvent négligées, telles que l'utilisation de ressources ou de code tiers. Lorsqu'elle est définie comme telle, une chaîne d'approvisionnement externe couvre *tout* produit ou service utilisé « en l'état » pour développer le propre produit ou service d'une entreprise.

La sécurisation de la chaîne d'approvisionnement nécessite de sécuriser l'accès et les *entrées* (composants physiques, logiciels ou données) dans le processus de fabrication, afin de garantir la qualité et l'intégrité du produit, et d'assurer la protection contre la perte de propriété intellectuelle ou de temps de production.

Protection des accès tiers

L'attaque Colonial Pipeline n'était que l'un des nombreux incidents très visibles dans la chaîne d'approvisionnement qui ont mis les fabricants en alerte. Les arrêts de production peuvent s'avérer coûteux dans de nombreux scénarios de fabrication, sans parler des problèmes liés à la perte de propriété intellectuelle. Une récente enquête a révélé que jusqu'à 97 % des entreprises ont subi une violation de la cybersécurité en raison d'une faiblesse de la chaîne d'approvisionnement.²² Par exemple, en 2013, le vol d'informations d'identification d'un fournisseur tiers a été à l'origine de la violation de Target, entraînant plus de 18,5 millions de dollars d'amendes.²³

Le principal défi pour les fabricants réside dans la complexité de la protection des chaînes d'approvisionnement en aval, compte tenu des centaines (voire milliers) de points d'entrée qui doivent être surveillés tout au long du processus. Les entreprises de l'industrie manufacturière doivent identifier et authentifier tous les utilisateurs ayant accès aux entrées, à la propriété intellectuelle ou aux systèmes impliqués dans la chaîne d'approvisionnement. Par exemple, le réseau interne de KP Snacks a été piraté, permettant aux pirates d'accéder à des fichiers sensibles et de les conserver, ce qui a entraîné des perturbations de la chaîne d'approvisionnement.²⁴

La solution YubiKey de Yubico fournit une authentification moderne et résistante au phishing à grande échelle sur l'ensemble de la chaîne d'approvisionnement, aidant les entreprises de l'industrie manufacturière et leurs fournisseurs à mettre en œuvre une authentification robuste et facile à utiliser pour tout utilisateur disposant d'un accès en amont au réseau ou lors de transferts critiques de propriété intellectuelle.

En l'associant à YubiKey as a Service (voir ci-dessous), vous pouvez offrir une solution simple et peu coûteuse pour améliorer la sécurité de la chaîne d'approvisionnement.

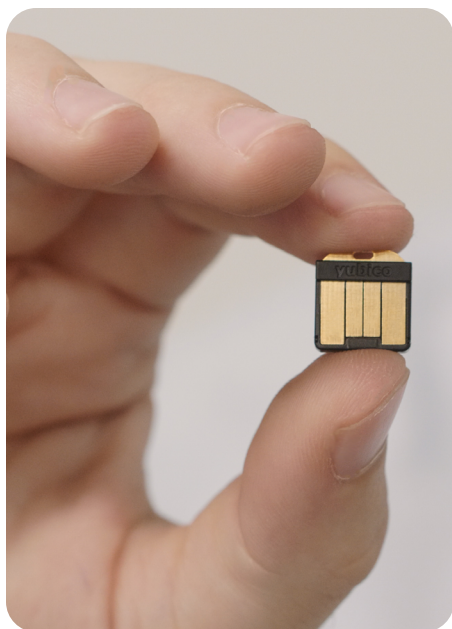
Assurance d'une intégrité maximale pour les pièces de vos produits

Les fabricants savent qu'il est essentiel de s'assurer que tous les composants impliqués dans un processus de bout en bout sont authentiques, afin d'éviter toute réplique et tout vol non sollicités, mais aussi pour l'assurance qualité : en effet, une chaîne d'assemblage ne doit se composer que de produits d'origine authentique. Par conséquent, il faut toujours qu'une solution soit mise en place pour protéger l'intégrité et la propriété intellectuelle de tous les composants, de la production à l'assemblage, en passant par la réparation et le remplacement. De plus, à mesure que l'IA agentique et les fonctions autonomes se multiplient, il est primordial de sécuriser les communications machine à machine et les points d'entrée qui contournent la supervision humaine pour garantir l'intégrité globale du système.

La YubiHSM 2



permet des communications machine à machine, un stockage et des opérations sécurisés et inviolables des clés, en empêchant la copie et la distribution accidentelles des clés cryptographiques, et en empêchant le vol à distance des clés stockées dans le logiciel.



L'approche traditionnelle de la protection de la propriété intellectuelle (PI) et de la prévention de la contrefaçon dans l'industrie manufacturière implique l'utilisation de clés cryptographiques numériques et du chiffrement. Les clés cryptographiques sont stockées dans un logiciel hautement vulnérable ou dans un modèle de sécurité matérielle (HSM). Malheureusement, les HSM traditionnels montés sur rack et sur carte sont volumineux et coûteux, ce qui les rend peu pratiques dans l'atelier, dans les centres de données en cage ou pour les appareils IoT.

Sécurisation du code et des données externes

Les entreprises de l'industrie manufacturière qui utilisent des logiciels dans leurs produits doivent disposer d'une méthode de signature de code sécurisée pour l'ingestion de code ou de données provenant de sources externes. Ces derniers temps, comme en témoigne l'attaque SolarWinds de 2020, le besoin de solutions de signature de code sécurisées a augmenté. Lors de cette attaque, les pirates ont exploité une violation du système de signature de code SolarWinds, qui leur a permis de distribuer frauduleusement du code malveillant sous forme de mises à jour légitimes pour plus de 18 000 installations du produit SolarWinds Orion dans le monde entier.²⁵

De plus, la solidité de la solution cryptographique que vous utilisez dépend de la méthode d'attestation de votre partenaire de la chaîne d'approvisionnement. Il est donc essentiel que ces partenaires puissent montrer une chaîne de traçabilité pour le code qui s'exécute jusqu'à l'ordinateur du développeur d'origine.

Communication machine à machine sécurisée avec la YubiHSM 2

Protection cryptographique pour protéger la propriété intellectuelle et l'intégrité des produits

Grâce à sa collaboration avec plusieurs partenaires du secteur de la fabrication responsables de la production à grande échelle de composants électroniques, Yubico a créé la YubiHSM 2, le plus petit HSM au monde, ultra-portable et économique, au format nano. La YubiHSM 2 permet un stockage et des opérations de clés sécurisés et inviolables, en empêchant la copie et la distribution accidentelles de clés cryptographiques et en empêchant le vol à distance des clés stockées dans le logiciel. La YubiHSM 2 peut être utilisée dans tous les processus où les secrets et l'authenticité des composants doivent être gérés, et où toute tentative de manipulation doit être empêchée.

Elle peut être facilement déployée sur un emplacement USB sur des serveurs, des bases de données, des lignes d'assemblage robotisées, des applications et des appareils IoT.

La YubiHSM 2 est utilisée pour protéger le processus de fabrication en veillant à ce que seules les stations de programmation certifiées puissent interagir avec les composants, ou pour écrire des signatures numériques sur chaque composant afin de garantir son authenticité. Dans les deux cas, la sécurité renforcée de la YubiHSM 2 contribue à préserver la réputation d'une entreprise et lui donne l'assurance que ses produits fonctionneront comme prévu, même après avoir quitté l'atelier de fabrication.

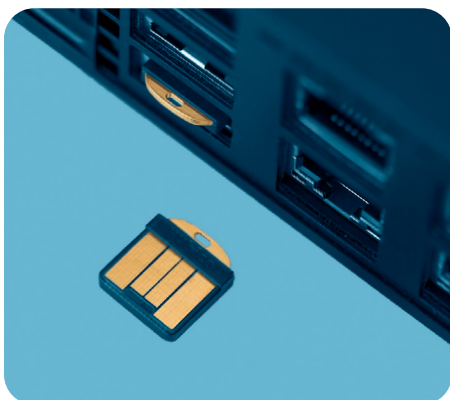
La YubiHSM 2 est parfaitement adaptée pour protéger les clés de signature et les certificats utilisés pour la signature de code, ce qui contribue à sécuriser les secrets partagés au sein de la chaîne d'approvisionnement. Les entreprises qui doivent répondre aux exigences FIPS 140-3 ont la possibilité d'opter pour la YubiHSM 2 FIPS 140-3 validée de niveau 3, afin de garantir les plus hauts niveaux de protection des données.

Il est important de noter que la clé cryptographique utilisée pour signer et/ou certifier des composants n'est jamais exposée en dehors du matériel de la YubiHSM 2, ce qui garantit un niveau de sécurité élevé. Pour illustrer ce point avec un exemple, même si un attaquant à distance est en mesure de compromettre un réseau ou l'ordinateur qui y est connecté, il n'y a toujours aucun vecteur d'attaque évident. D'un autre côté, si le même attaquant est en mesure d'obtenir un accès sous-jacent complet à un logiciel équivalent, il peut au moins exécuter une analyse de la mémoire ou des fichiers locaux à la recherche de faiblesses ou de schémas potentiels.

La YubiHSM 2

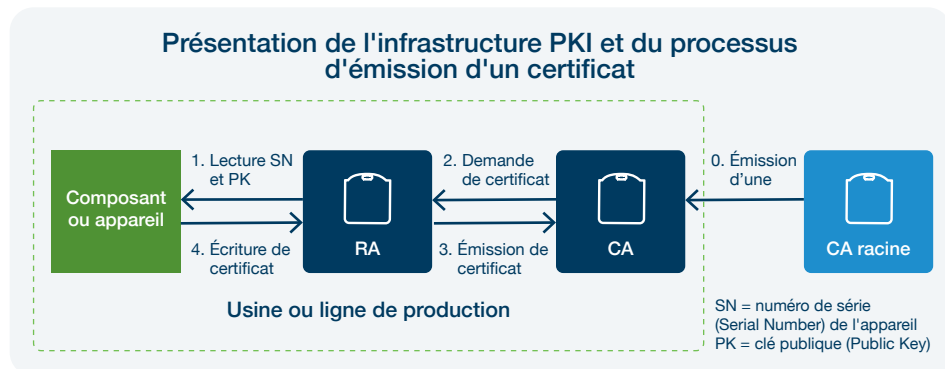


est utilisée pour protéger le processus de fabrication en veillant à ce que seules les stations de programmation certifiées puissent interagir avec les composants, ou pour écrire des signatures numériques sur chaque composant afin de garantir son authenticité.

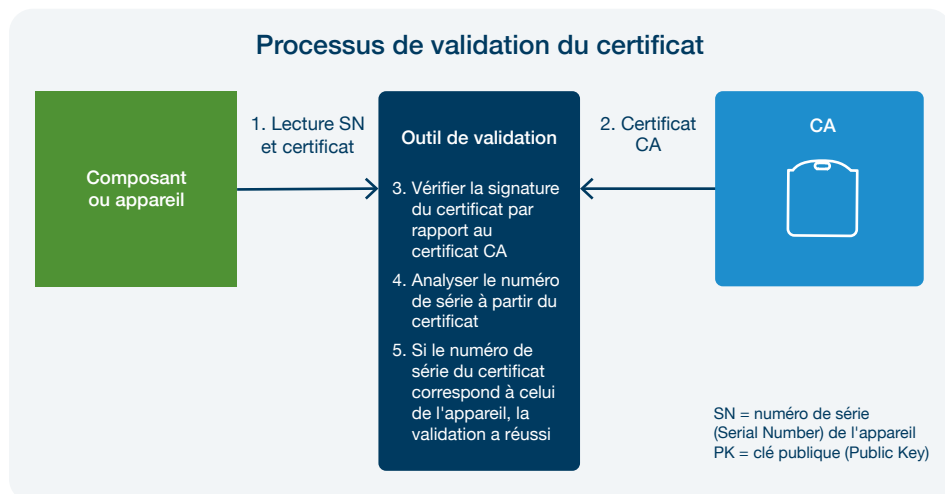


Prise en charge des environnements d'infrastructure à clé publique (PKI)

La YubiHSM 2 étant conçue pour stocker des clés cryptographiques, elle est idéale pour protéger l'infrastructure PKI et son réseau de clés cryptographiques. Le processus d'émission de certificats à l'aide d'une PKI basée sur la YubiHSM 2 pour la fabrication est détaillé ci-dessous :



Dans ce schéma, l'autorité de certification racine (CA racine) utilise une YubiHSM 2 pour héberger sa paire de clés (c'est-à-dire ses clés privées et publiques) en plus de son certificat, sur site ou dans un centre de données hors site. Sur la ligne de production, une autorité de certification (CA) peut être déployée et configurée avec un certificat signé par l'autorité de certification racine en tant que délégué. Avec cette paire de clés et ce certificat, toutes les informations d'identification ultérieures peuvent être signées et également protégées par une YubiHSM 2. Ces informations d'identification supplémentaires sont émises par une autorité d'enregistrement (RA) qui, à son tour, a fait signer son certificat par l'autorité de certification. Enfin, les certificats de composant peuvent être utilisés pour vérifier l'authenticité de chaque composant, produit ou dispositif en cours de production, comme indiqué dans le schéma ci-dessous.



En pratique, cela permet aux fabricants de vérifier l'authenticité de chaque composant produit. La collecte de numéros de série cryptés sur l'unité de contrôle électronique (ECU) peut également faciliter les tests et être utilisée pour le suivi d'audit.

ÉTUDES DE CAS



Sécuriser les systèmes et la chaîne d'approvisionnement chez Schneider Electric



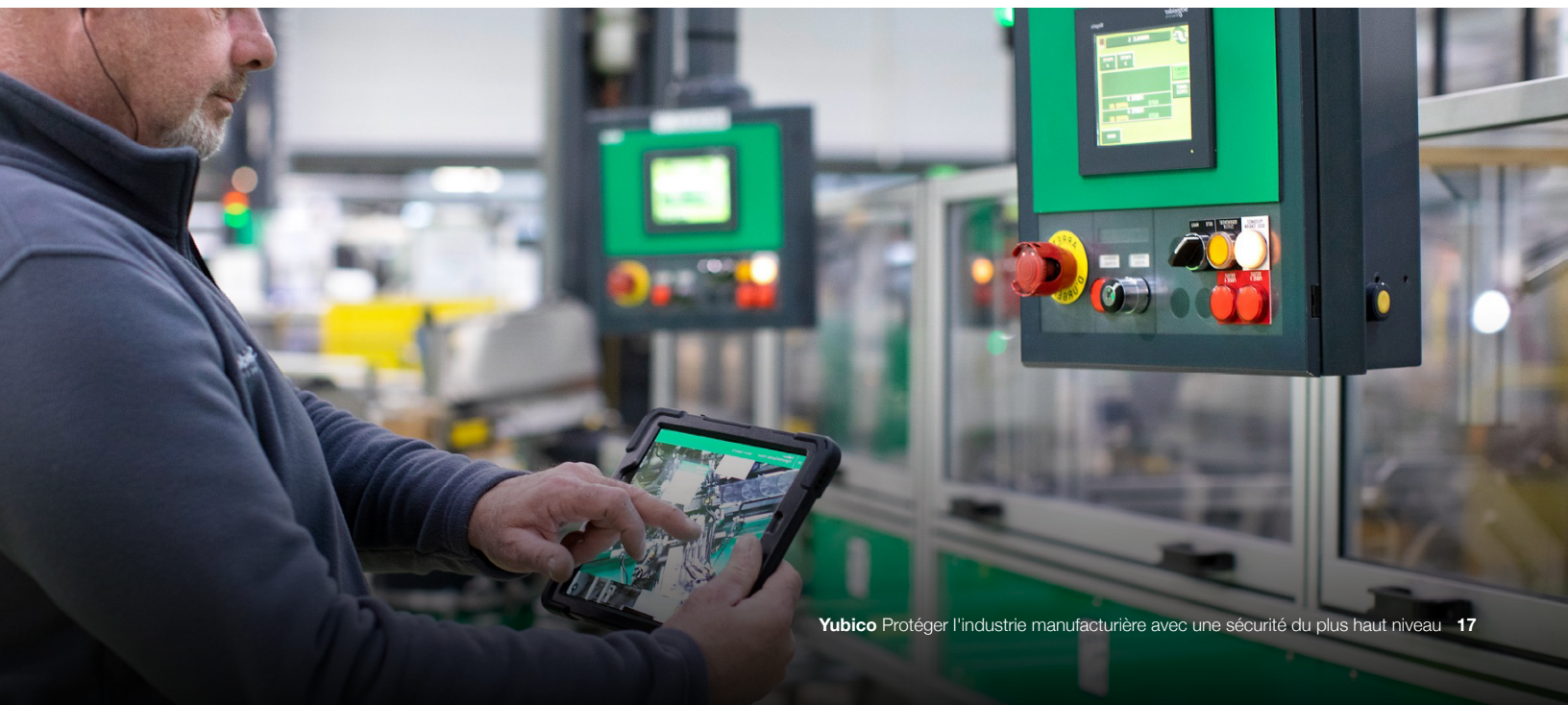
Schneider Electric est un leader dans la transformation numérique de la gestion et de l'automatisation de l'énergie, de la fabrication de pièces électriques et de systèmes de gestion de l'énergie, avec notamment un système SCADA (Supervisory Control and Data acquisition) utilisé pour la gestion à distance d'infrastructures critiques (par exemple, centres de données, hôpitaux, pétrole et gaz).

La YubiKey a permis à Schneider Electric d'intégrer le MFA dans un système isolé sans dépendre d'Internet ni d'une authentification par SMS moins sécurisée, ce qui a permis de rationaliser l'authentification pour les changements d'équipe. La YubiKey est également utilisée dans les situations de contrôle où des actions de dérogation de supervision sont requises. Le MFA moderne par le biais de clés YubiKey a été intégré au processus d'obtention de la certification CEI-62443 SL2.

« La sécurité est une priorité absolue chez Schneider Electric et se reflète dans toutes nos actions », souligne Chad Lloyd, Directeur de l'architecture de la cybersécurité pour la gestion de l'énergie chez Schneider Electric. « Dans le cadre de notre certification CEI SL2, nous avons intégré le MFA à notre système d'alimentation, ce qui nous permet de répondre aux exigences de la norme SL3 à l'avenir. C'est désormais un point de différenciation pour Schneider Electric », a déclaré M. Lloyd.

Outre l'intégration des YubiKeys dans ses systèmes SCADA utilisés par les clients dans les infrastructures critiques, Schneider Electric a pris des mesures pour garantir la qualité et l'intégrité de sa chaîne d'approvisionnement en tirant parti du Hardware Security Module YubiHSM 2 pour s'intégrer aux principaux fournisseurs dans le processus de fabrication. La sécurité matérielle cryptographique de haut niveau de la YubiHSM 2 contribue à soutenir les processus de test et de fabrication rigoureux de tous les produits Schneider Electric authentiques.

Le format nano de la YubiHSM 2 était essentiel pour soutenir un déploiement et une utilisation flexibles dans les ateliers, nécessitant uniquement un simple port USB pour la connexion.



ÉTUDES DE CAS



Mitsubishi Electric renforce la cybersécurité mondiale avec la YubiKey

Mitsubishi Electric est un leader mondial dans le domaine de l'innovation produit et est un fabricant de produits et de systèmes électriques et électroniques, pour les consommateurs, les entreprises et une large gamme d'infrastructures critiques, y compris l'énergie, les transports et les systèmes d'information et de communication. Fondée en 1921, Mitsubishi Electric a établi son siège social à Tokyo, au Japon, et est présente dans plus de 120 pays.

En tant que fournisseur clé de produits et de solutions électriques et électroniques pour les secteurs d'infrastructure critiques dans le monde entier, et en tant que fournisseur majeur de systèmes de défense japonais, Mitsubishi Electric doit impérativement se protéger contre les cyberattaques persistantes.

Afin de garantir que son investissement dans le MFA était bien adapté, Mitsubishi Electric souhaitait s'assurer que la solution répondait aux normes définies par les directives sur l'identité numérique du NIST (National Institute of Standards and Technology) et l'AAL (Authenticator Assurance Level), reconnues dans le monde entier comme des normes équitables pour la gestion des identités. Lors de la mise en œuvre du MFA dans diverses divisions et filiales, Mitsubishi Electric a dû faire face à de nombreux défis, notamment des scénarios en zone mobile restreinte, car la plupart des sites de production limitent l'utilisation de tout appareil mobile.

La YubiKey est apparue comme une solution optimale pour les technologies IT et OT, y compris l'accès aux systèmes de contrôle industriel (ICS), ne nécessitant aucun matériel, logiciel, alimentation externe, batterie ni connexion réseau supplémentaire. En adoptant les solutions Yubico, telles que la YubiKey, Mitsubishi Electric élève considérablement le niveau de sécurité et établit une base solide pour faciliter et protéger sa transformation numérique, en ouvrant la voie à une authentification sécurisée sans mot de passe.



Une chaîne de confiance portable pour EasyMile afin de sécuriser les véhicules autonomes

EasyMile développe des solutions logicielles pour son parc de véhicules autonomes (principalement ceux utilisés pour transporter des personnes et des marchandises) selon les normes de sécurité les plus strictes. Déjà utilisatrice de clés YubiKey de Yubico pour sécuriser les comptes administrateur, EasyMile s'est tournée vers Yubico pour cibler et renforcer son infrastructure PKI. EasyMile a rapidement et facilement déployé la YubiHSM 2 pour sécuriser l'infrastructure PKI X.509 CA, servant à sécuriser son écosystème de véhicules autonomes. Le résultat ? Un gage de confiance pour son écosystème de certificats de sécurité.

La YubiHSM 2 fournit également une chaîne de confiance portable dans la fabrication mondiale. Par exemple, après avoir développé sa propre infrastructure PKI interne, une entreprise du classement Fortune 500 s'est tournée vers Yubico pour trouver une solution plus économique permettant de préserver l'intégrité de ses produits. Cette marque s'est appuyée sur la YubiHSM 2 pour signer et certifier numériquement chaque composant fabriqué sur plusieurs sites, afin de garantir l'authenticité et l'intégrité du produit à la fin des lignes de production respectives.





Déploiement rapide et fluide des systèmes sans mot de passe à grande échelle

Il est prouvé que les passkeys, comme celles utilisées dans les clés de sécurité modernes, telles que YubiKeys, sont efficaces pour arrêter les cybermenaces basées sur l'IA à grande échelle. Elles s'imposent donc comme le système qui permet aux entreprises intelligentes de garder une longueur d'avance sur les cybermenaces. La mise en œuvre du MFA résistant au phishing et d'une infrastructure sans mot de passe vous font peur ? Rassurez-vous.

Pour faciliter la sécurisation des identités numériques à grande échelle grâce à l'authentification résistante au phishing, [YubiKey as a Service](#) offre aux entreprises un moyen flexible et économique de déployer des YubiKeys sur l'ensemble du personnel, de la chaîne logistique et des clients finaux.

Grâce à [YubiKey as a Service](#), les entreprises bénéficient de déploiements simples et évolutifs de YubiKeys à l'échelle mondiale, pour leur personnel, leur chaîne d'approvisionnement et leurs clients finaux. YubiKey as a Service offre aux clients différents formats, un stock de remplacement et une assistance client prioritaire, le tout pour un prix inférieur au prix d'une tasse de café par mois. Les organisations accèdent automatiquement au [Portail client](#), un tableau de bord Web centralisé qui permet aux équipes IT de déployer, de suivre et de gérer efficacement le déploiement de la YubiKey, avec une visibilité en temps réel sur l'inventaire, la progression du déploiement et l'activation des utilisateurs.

Les clients ont également accès aux services clés en main [Enrollment](#) et [Delivery](#) qui aident les équipes IT à équiper rapidement les utilisateurs de YubiKeys pour accélérer la résistance au phishing, puis à expédier les YubiKeys aux utilisateurs finaux dans le monde entier, que ce soit au bureau ou à domicile. Les utilisateurs peuvent même [commander en libre-service](#) des YubiKeys et les faire livrer à l'adresse de leur choix, à tout moment. Les clients YubiKey as a Service bénéficient d'améliorations continues des services existants et nouveaux, ce qui garantit un investissement de sécurité intelligent et pérenne.

Yubico propose également des [services professionnels](#) pour aider les entreprises à déployer les YubiKeys rapidement et à grande échelle. Nous proposons une gamme de services de conseil, notamment une assistance à l'intégration technique, aux développeurs et aux API, ainsi qu'une planification et une mise en œuvre du déploiement.

La [YubiHSM 2](#) est l'un des HSM les plus petits et les plus abordables du marché. Elle est parfaitement adaptée à un large éventail de cas d'utilisation et à tous les types d'organisations et de secteurs, ce qui la rend simple et rapide à acheter, à fournir et à déployer. Grâce à son faible encombrement, la YubiHSM 2 offre une solution accessible, pour une sécurité solide et résistante au phishing, à un grand nombre de clients de l'industrie manufacturière et de la chaîne d'approvisionnement dans le monde entier.





Sécurisez la chaîne d'approvisionnement et protégez l'accès, la propriété intellectuelle et l'intégrité des produits tiers en tirant parti de la YubiKey et de la YubiHSM 2 pour garantir une sécurité du plus haut niveau.

Retour sur investissement élevé, risques et coûts réduits

Dans une [étude commandée](#) et réalisée pour le compte de Yubico, Forrester Consulting a récemment interrogé des responsables de la sécurité de cinq entreprises ayant recours aux clés YubiKey. Il en ressort que, pour une entreprise composite, les résultats sont spectaculaires :

 **99,99 %**

Réduction de l'exposition au phishing et au vol d'informations d'identification

 **90 %**

Moins de tickets d'assistance

 **265 %**

Retour sur investissement sur 3 ans

² Sur la base d'entretiens menés par Forrester auprès de six décideurs de grandes entreprises utilisant les YubiKeys. Les expériences ont été agrégées pour créer une organisation composite : une entreprise mondiale de 5 000 employés avec un chiffre d'affaires de 2,5 milliards de dollars par an qui utilisait auparavant un MFA traditionnel.

[En savoir plus →](#)

Résumé

Construire un avenir cyber-résilient pour l'industrie manufacturière

Les entreprises de l'industrie manufacturière modernes ont besoin de solutions de sécurité modernes pour améliorer l'efficacité et la résilience opérationnelle, à une époque où l'IA agit à la fois comme un catalyseur stratégique et comme un puissant accélérateur de menaces. Pour être efficaces, ces solutions doivent être durables, faciles à utiliser et adaptées à divers environnements, de l'atelier de production à la salle de conférence. Idéalement, ces solutions doivent être conçues pour réduire certains frais coûteux et non productifs liés à l'authentification classique. De plus, alors que l'IA agentique et la puissance software-defined continuent de transformer le secteur, le renforcement de l'authentification et de l'autorisation de ces terminaux autonomes est essentiel pour empêcher les interruptions non autorisées.

Les récentes cyberattaques sophistiquées ont souligné la nécessité urgente de sécuriser la chaîne de production et la chaîne d'approvisionnement dans son intégralité, afin de préserver la continuité des opérations. En conséquence, les grandes entreprises de l'industrie manufacturière déploient un MFA résistant au phishing et une authentification sans mot de passe, de même qu'une protection cryptographique pour se défendre contre les menaces modernes qui ciblent à la fois les écosystèmes IT et OT. La sécurisation de la communication entre les humains et les machines, ainsi que de machine à machine, est un élément clé pour garantir une stratégie complète de cyber-résilience.

L'adoption d'une approche proactive, en sécurisant vos données et vos produits avec la solution de sécurité appropriée, permettra de réussir : limiter les risques de pannes, minimiser les taux de pénétration des attaques et protéger la propriété intellectuelle riche en informations. De plus, cette stratégie offre une transparence et un contrôle cryptographique essentiels sur chaque étape du processus de fabrication de bout en bout.

Les solutions YubiKey et YubiHSM 2 de Yubico sont sécurisées, portables et faciles à utiliser. Elles ont été conçues pour répondre aux besoins des entreprises de l'industrie manufacturière, où qu'elles se trouvent. Elles permettent de prendre en charge de manière fluide les infrastructures existantes ainsi que les systèmes modernes basés sur le cloud.

Grâce à une inscription exclusive et à une livraison clé en main mondiale disponible via YubiKey as a Service, Yubico est là pour vous aider à déployer une sécurité matérielle du plus haut niveau à l'échelle mondiale.

La sécurité n'est pas seulement une mesure défensive, elle constitue la base de l'innovation industrielle. En plus de protéger vos systèmes, le renforcement de vos limites grâce à une sécurité renforcée par matériel soutient votre avenir. La base de vos opérations manufacturières sécurisées est à portée de main avec Yubico.

Approuvé par :

 Schneider Electric

 MITSUBISHI ELECTRIC

 EAS MILE

 FLUIDRA



Contactez-nous
yubi.co/contact



En savoir plus
[Comment vous lancer avec le MFA résistant au phishing](#)

Sources

- ¹ IBM, X-Force Threat Intelligence Index 2026
- ² Industrial Cyber, BitSight warns of surge in ICS/OT Internet exposure, raising critical infrastructure cybersecurity concerns
- ³ IBM, Cost of a Data Breach Report 2025
- ⁴ Emerson, How Manufacturers Can Achieve Top Quartile Performance
- ⁵ Fortinet, 2025 State of Operational Technology and Cybersecurity Report
- ⁶ The Five Eyes Alliance et al., Secure connectivity principles for Operational Technology (OT)
- ⁷ Kurt Thomas, Angelika Moscicki, New research: How effective is basic account hygiene at preventing hijacking
- ⁸ Industrial Cyber, BitSight warns of surge in ICS/OT Internet exposure, raising critical infrastructure cybersecurity concerns
- ⁹ ABI Research and Palo Alto Networks, The State of OT Security
- ¹⁰ Dragos, 2026 OT Cybersecurity Year in Review
- ¹¹ Fortinet, 2025 State of Operational Technology and Cybersecurity Report
- ¹² LandBase, Agentic AI Statistics Every GTM Leader Should Know in 2026
- ¹³ Varonis, 2021 Data Risk Report, Manufacturing
- ¹⁴ SentinelOne, Key Cyber Security Statistics for 2026
- ¹⁵ Amber Steel, LastPass Reveals 8 Truths about Passwords in the New Password Exposé
- ¹⁶ Gartner, 3 Simple Ways IT Service Desks Should Handle Incidents and Requests
- ¹⁷ Ponemon Institute, 2019 State of Password and Authentication Security Behaviors Report
- ¹⁸ Varonis, 2021 Data Risk Report, Manufacturing
- ¹⁹ Ponemon Institute, 2020 State of Password and Authentication Security Behaviors Report
- ²⁰ 451 Research, 2021 Yubico and 451 Research Study
- ²¹ Kurt Thomas, Angelika Moscicki, New research: How effective is basic account hygiene at preventing hijacking
- ²² BlueVoyant, Managing Cyber Risk Across the Extended Vendor Ecosystem 2021
- ²³ Reuters, Target Settles 2013 Hacked Customer Data Breach for \$18.5 Million
- ²⁴ Reuters, Hackers Hold Hula Hoops Hostage in cyber-raid on Britain's KP Snacks
- ²⁵ SEC, Form 8-K SolarWinds Corporation



À propos de Yubico

Yubico (Nasdaq Stockholm : YUBICO) est une entreprise de cybersécurité moderne dont la mission est de rendre Internet plus sûr pour tout le monde. En tant qu'inventeurs de la YubiKey, nous avons établi la norme d'excellence pour une authentification moderne, résistante au phishing et reposant sur du matériel, empêchant les piratages de comptes et simplifiant la connexion sécurisée.

Depuis 2007, nous avons contribué à la mise en place de normes d'authentification globales, co-créé FIDO2, WebAuthn et FIDO U2F, et introduit la passkey originale. Aujourd'hui, notre technologie de passkey sécurise des personnes et des organisations dans plus de 160 pays, transformant la manière dont l'identité numérique est protégée, de l'intégration à la récupération de compte.

Plébiscitées par les marques, les gouvernements et les institutions les plus soucieux de sécurité au monde, les YubiKeys fonctionnent immédiatement avec des centaines d'applications et de services, offrant un accès rapide, sans mot de passe, sans friction ni compromis.

Nous pensons que la sécurité renforcée ne devrait jamais être hors de portée. Grâce à notre initiative philanthropique Secure it Forward, nous faisons don de YubiKeys à des associations soutenant les communautés à risque.

Avec un double siège à Stockholm (Suède) et Santa Clara (Californie), Yubico est fier d'être reconnu parmi les 100 entreprises les plus influentes selon TIME et les plus innovantes selon Fast Company. Pour en savoir plus, rendez-vous sur www.yubico.com.