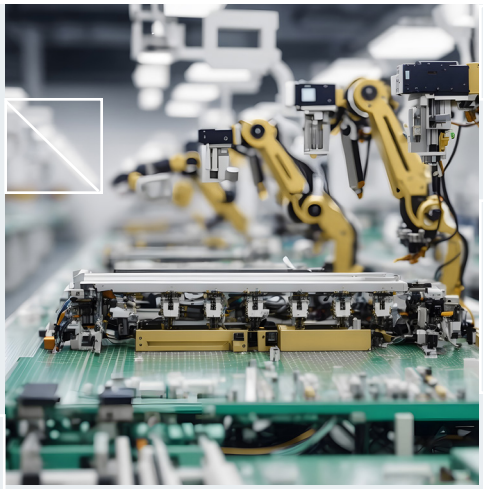
EBOOK



CONFIANCE POUR LES APPAREILS : SÉCURISER LES TECHNOLOGIES CONNECTÉES DE DEMAIN

digicert®

SOMMAIRE

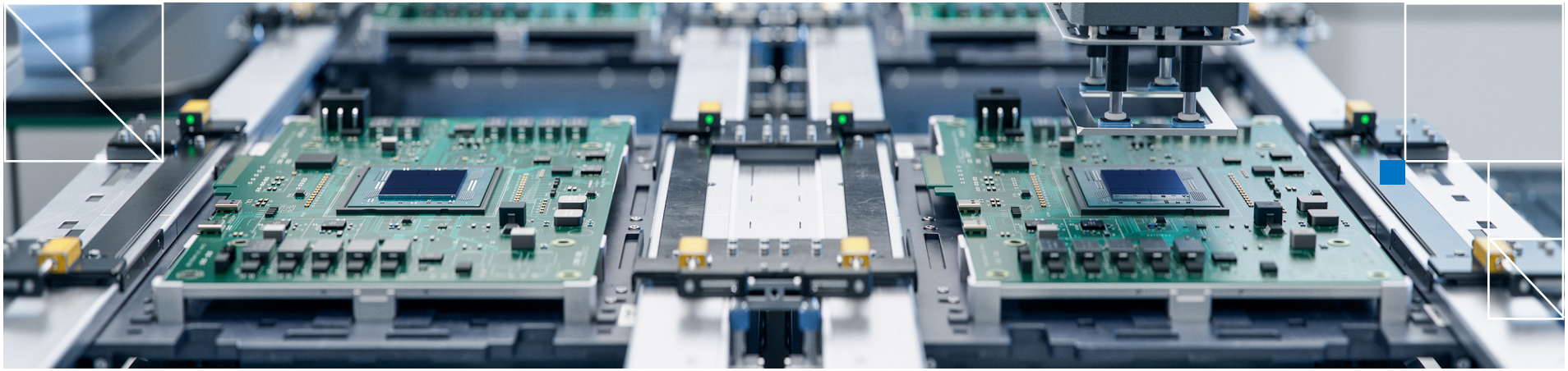
LE TOUT CONNECTÉ, ENTRE PROMESSES ET MENACES

Le monde ultra connecté dans lequel nous vivons fait apparaître chaque jour de nouvelles opportunités… mais aussi des vulnérabilités. En effet, les risques qui planent sur le marché de l'Internet des objets (IoT) évoluent aussi vite que les technologies elles-mêmes. Et ce ne sont pas seulement les utilisateurs qui sont menacés, mais l'intégrité de réseaux entiers.

Qui dit plus d'appareils, dit plus de vecteurs d'attaque. Or, une seule compromission peut avoir des conséquences désastreuses : perte de données, manque à gagner, érosion de la confiance des clients… jusqu'à l'ébranlement des fondements mêmes de l'entreprise.

Le public a soif de connectivité, ce qui n'a pas échappé aux fabricants ni aux développeurs. Mais faute de prioriser la sécurité, certains d'entre eux continuent d'alimenter le boom des compromissions d'appareil, une véritable industrie du crime qui devrait rapporter 10 000 milliards de dollars aux attaquants d'ici 2025.

La question n'est pas de savoir si vous devez investir dans la sécurité de vos appareils, mais quand. La confiance pour les appareils n'est pas accessoire, elle est fondamentale. Voyons comment elle peut vous aider à vous défendre contre les attaquants et à vous démarquer de vos concurrents.



MARKETING « SECURITY-FIRST »

Beaucoup de fabricants IoT font de la sécurité un enjeu essentiel. Ils sont conscients du besoin d'établir un rempart solide contre des menaces toujours plus diverses. Les pierres angulaires de ces défenses ? Identité, inviolabilité et conformité.

Identité numérique immuable

La confiance pour les appareils sécurise l'identité d'un appareil dès sa création. Il conserve ainsi son intégrité tout au long de son cycle de vie. Les identités immuables permettent de se prémunir contre un certain nombre d'attaques et constituent un socle sécurisé sur lequel repose l'ensemble du processus de fabrication.

Écosystème inviolable

Les mécanismes anti-falsification protègent non seulement les appareils individuels, mais aussi l'ensemble du réseau contre les modifications non autorisées. Ils sont donc d'une importance primordiale. La confiance pour les appareils prévoit une sécurité multiniveau, composée d'ancres de confiance et de processus de démarrage sécurisé, pour garantir l'inviolabilité des équipements. Cette approche a l'avantage de dissuader les tentatives d'effraction physique, tout en préservant l'intégrité logicielle de l'appareil, la propriété intellectuelle du fabricant et les données de l'utilisateur.

Conformité aux normes internationales

La confiance pour les appareils aide les fabricants à s'aligner sur les protocoles de sécurité internationaux, par exemple grâce à des modèles prédéfinis axés sur les réglementations en vigueur. Il devient alors facile d'éviter les problèmes de non-conformité.

Le marketing « security-first » dans le monde réel

Nous avons déjà pu constater l'efficacité de ces mesures de sécurité dans le monde réel. En voici quelques exemples concrets :

- La confiance pour les appareils a permis à une entreprise d'électronique d'intégrer des identités immuables à ses produits domotiques. Ainsi, l'origine de chaque appareil et les mises à jour de ses firmwares restent authentifiées et sécurisées tout au long du cycle de vie, de la production à l'utilisation.
- Un fabricant de capteurs industriels a rendu son écosystème inviolable pour protéger les appareils de son infrastructure critique, renforçant par là même la résilience de ses produits.
- Grâce à la confiance pour les appareils, un fabricant international d'électroménager a pu s'y retrouver plus facilement dans les nombreuses réglementations sur la confidentialité. Les profils de sécurité, personnalisés en fonction des marchés, garantissent la conformité de ses appareils aux normes locales, sans besoin de refonte complète. Des économies de temps et de ressources considérables pour le fabricant.

La confiance pour les appareils fournit un framework de sécurité complet, déployé dès la conception de l'appareil connecté. Intégration d'identités immuables, inviolabilité garantie, conformité simplifiée aux normes internationales… la confiance pour les appareils renforce non seulement le processus de fabrication, mais aussi l'authenticité des appareils gravitant dans l'environnement.

CHAPITRE 2

INDUSTRIE AGILE

Dans notre monde ultra connecté, les modes de déploiement flexibles sont la clé de voûte de l'agilité. Ils permettent aux fabricants de s'adapter aux nouveaux environnements et aux nouvelles exigences de façon rapide, fluide et efficace. En se libérant du carcan des modèles standards, les fabricants peuvent moduler leur posture de sécurité en fonction de leurs processus de production, aussi uniques soient-ils. L'enjeu n'est pas seulement de s'adapter aux différentes infrastructures physiques, mais aussi aux environnements technologiques variés qui interviennent dans leurs activités.

Respect des lois locales sur la protection des données

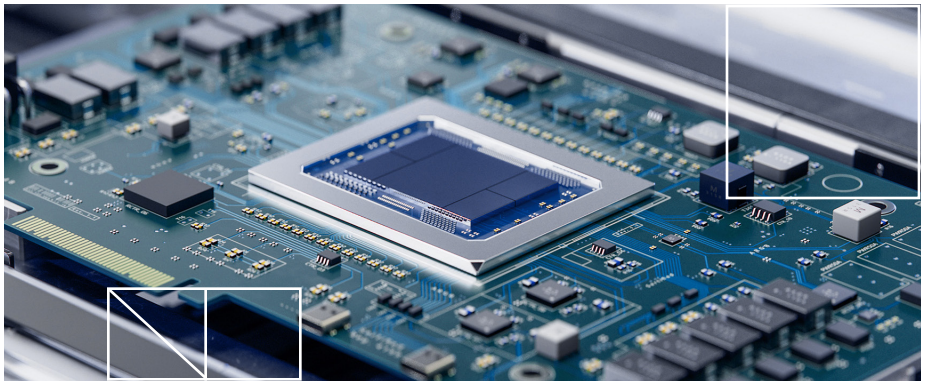
Les fabricants qui souhaitent développer leurs activités à l'international font face à un défi majeur : ils doivent maintenir un framework de sécurité homogène tout en respectant les réglementations locales sur la protection des données, qui varient grandement d'une région à l'autre. Pour ce faire, l'entreprise doit orchestrer méticuleusement ses pratiques de sécurité. Le but est de se conformer aux règlements locaux sans freiner ni entraver le déploiement.

En misant sur une solution de sécurité flexible et scalable, les fabricants peuvent étendre leur présence dans le monde entier, sans compromis sur la sécurité de leurs appareils.

Ressources, mémoire et sécurité : résoudre l'équation par la flexibilité

Les ressources et la mémoire des appareils IoT varient d'un équipement à l'autre. Pour les protéger, les fabricants doivent donc déployer des solutions de sécurité flexibles. De fait, si le système de sécurité est trop gourmand en ressources, les appareils dotés d'une puissance de calcul et d'une mémoire limitées en pâtiront. À l'inverse, un système trop léger risque de ne pas offrir une protection suffisante aux appareils plus puissants.

D'où l'importance d'adopter une approche pondérée qui s'adapte aux ressources de chaque appareil sans alourdir inutilement la charge de travail. Cette adaptabilité est fondamentale : elle garantit une sécurité robuste sur les appareils les plus avancés et une protection légère, mais efficace pour les équipements plus limités.



En adoptant des principes de déploiement flexibles dans leurs processus de fabrication, les entreprises font face avec plus d'assurance à la complexité de l'IoT.

L'industrie agile dans le monde réel

Voici quelques exemples concrets qui prouvent l'efficacité de ces principes dans la fabrication de l'IoT :

- Une entreprise d'électronique grand public a capitalisé sur des solutions de sécurité flexibles et évolutives pour gérer son vaste catalogue de produits, des TV connectées de pointe aux gadgets domotiques IoT les plus basiques. Elle a pu ainsi adapter les mesures de sécurité aux capacités de chaque produit et aux exigences de chaque marché, un avantage primordial pour la réussite de son expansion à l'international.
- Une entreprise industrielle, qui fabrique des capteurs pour l'agriculture connectée, a utilisé ces principes pour la gestion d'appareils déployés dans plusieurs continents. Chacune de ces régions présente des conditions atmosphériques et des exigences réglementaires différentes. La solution s'est adaptée à ces contraintes, permettant aux appareils dotés d'une puissance de calcul limitée de fonctionner en toute sécurité, même dans des environnements isolés où les ressources se font rares.

En adoptant des principes de déploiement flexibles dans leurs processus de fabrication, les entreprises font face avec plus d'assurance à la complexité de l'IoT. Déploiement flexible, évolutivité internationale, sécurité adaptée aux ressources… avec toutes ces cartes en main, les fabricants peuvent construire un écosystème de production résilient, armé pour répondre aux exigences d'aujourd'hui et anticiper les besoins de demain.

CHAPITRE 3

EXCELLENCE OPÉRATIONNELLE

L'excellence opérationnelle des processus de fabrication IoT repose avant tout sur une synergie entre automatisation et sécurité robuste. Au cœur de cette stratégie opérationnelle : la gestion automatisée des certificats, pierre angulaire des identités et de la sécurité des appareils IoT. Émission, renouvellement, révocation… tout au long du cycle de vie des certificats, l'automatisation élimine le risque d'erreur humaine, garantissant ainsi la précision et l'exactitude de l'identité des appareils.

La gestion automatisée des certificats peut également s'étendre aux appareils sur le terrain. Une fois déployés, ces appareils reçoivent des mises à jour et des correctifs de sécurité à distance, une méthode qui limite les interruptions de services et accroît l'efficacité opérationnelle, sans aucune intervention physique. Réduction du nombre de rappels et de mises à jour manuelles, prolongement du fonctionnement des appareils, économies de ressources, gain de temps… les avantages sont nombreux.

La gestion automatisée des certificats dans le monde réel

À l'ère du tout connecté, la confiance pour les appareils peut devenir un véritable levier d'excellence opérationnelle, et ce dans de nombreux secteurs :

- Dans les Smart Cities, des milliers de capteurs et d'appareils collectent et transmettent des données pour gérer le trafic routier, la consommation énergétique et la sécurité des habitants. Intégrée à ces appareils, la gestion automatisée des certificats agit sur deux plans : elle garantit la sécurité des données en circulation et permet d'authentifier l'identité de chaque appareil. Dès lors, les décisions les plus critiques peuvent se fonder sur des informations à la fois fiables et exactes.
- Le secteur médical utilise des appareils IoT très variés, allant des équipements de surveillance aux « wearables » portés par les patients pour suivre leur état de santé. Il est donc absolument vital d'assurer le plus strict niveau de sécurité et de fiabilité opérationnelle pour ces appareils. Grâce à l'automatisation de la gestion des certificats et des identités, les nouveaux dispositifs d'authentification sont installés rapidement sur tous ces équipements. Résultat, les informations sur les patients sont protégées et les soignants peuvent compter sur l'intégrité des données reçues.
- Dans l'industrie, la gestion automatisée des systèmes de protection permet aux appareils de s'ajuster aux évolutions des écosystèmes de sécurité. La posture de sécurité s'adapte ainsi aux menaces en constante évolution, avec un impact minime sur les opérations. Cette flexibilité représente un atout indispensable pour les fabricants, qui peuvent ainsi maintenir la confiance de leurs clients et préserver leur image de marque.

Intégrée aux appareils IoT, la gestion automatisée des identités et du cycle vie des certificats propulse les entreprises vers l'excellence opérationnelle. À la clé : un renforcement de la sécurité, une réduction des risques opérationnels et des écosystèmes IoT plus fiables. Trois avantages essentiels pour répondre aux exigences des infrastructures de demain.

CHAPITRE 4

PÉRENNISATION DE LA PRODUCTION

Le secteur de la sécurité IoT est en constante mutation. Les fabricants ne doivent donc pas seulement tenir compte des enjeux actuels, mais aussi anticiper ceux à venir.

Se préparer à l'informatique quantique

L'informatique quantique crée de nouvelles opportunités, mais aussi de nouvelles menaces. En fragilisant les méthodes de chiffrement traditionnelles, elle risque d'introduire de nouvelles vulnérabilités dans les parcs IoT. La cryptographie post-quantique (PQC) offre une solution à ce nouveau défi. Elle protège les appareils contre les capacités de déchiffrement des ordinateurs quantiques, assurant leur intégrité et la confidentialité de leurs données à long terme.

Adoption de technologies émergentes

Les nouvelles technologies comme le protocole MQTT 5.0 proposent des fonctionnalités avancées de communication entre appareils, notamment la mise en file d'attente des messages. Sécurité renforcée, amélioration de la gestion des données, efficacité des communications entre appareils… leurs avantages sont légion. Autre exemple : le système open source Kubernetes automatise le déploiement, la montée en charge et la gestion des applications containerisées. Il permet d'intégrer l'agilité et la scalabilité à la gestion des appareils.

Pour une gestion IoT plus efficace, les fabricants peuvent adopter le protocole MQTT 5.0, le système Kubernetes ou d'autres technologies émergentes. Ils ont ainsi la garantie d'une infrastructure robuste, réactive et scalable face au rythme effréné des progrès technologiques.

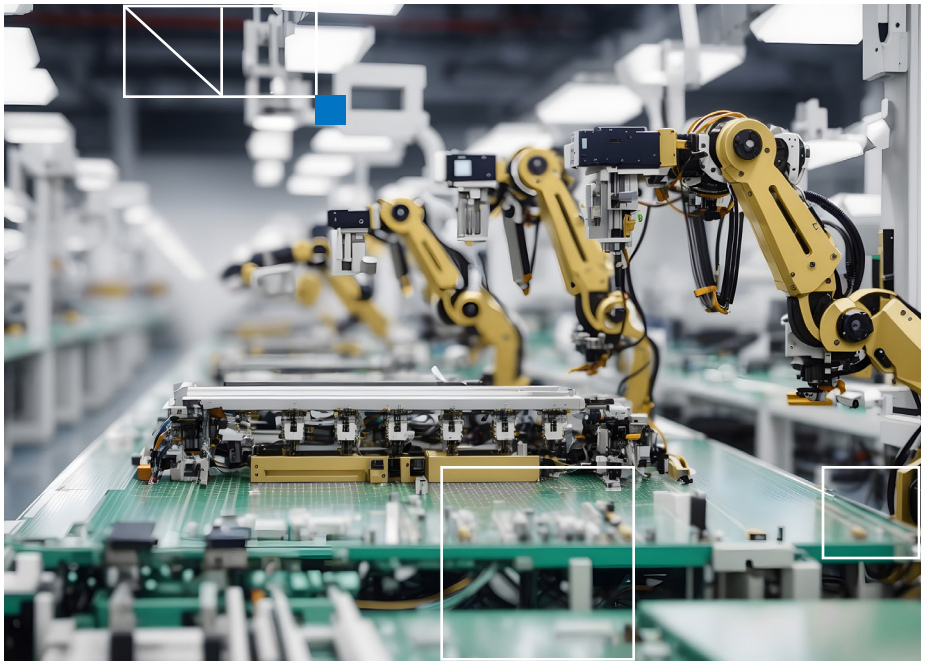
L'informatique quantique crée de nouvelles opportunités, mais aussi de nouvelles menaces. En fragilisant les méthodes de chiffrement traditionnelles, elle risque d'introduire de nouvelles vulnérabilités dans les parcs IoT.

Anticiper les évolutions réglementaires

Les réglementations évoluent constamment pour faire face aux nouvelles menaces. La conformité aux standards sectoriels est donc un défi sans fin. Respecter les normes actuelles ne suffit pas. Pour anticiper ces changements, les entreprises doivent participer activement aux conversations qui façonnent ces réglementations.

Les fabricants doivent donc se rapprocher des organismes de normalisation et des groupes de travail techniques pour s'informer des évolutions juridiques à venir et mettre à jour leurs produits. La proactivité est la clé d'une transition fluide vers ces nouvelles normes. En évitant les refontes, les fabricants réalisent des économies significatives, tout en s'assurant que leurs produits restent à la pointe des pratiques de sécurité.

En anticipant les évolutions réglementaires, les fabricants peuvent également se hisser au rang de leaders du secteur. Ils sont ainsi prêts à répondre aux exigences des consommateurs les plus soucieux de la sécurité, à braver la complexité des marchés internationaux et à se conformer aux diverses réglementations en vigueur dans le monde entier. Enfin, cette approche envoie un message fort aux autres acteurs du secteur : l'entreprise met un point d'honneur à respecter les normes de sécurité les plus élevées, renforçant ainsi la confiance de ses clients et son image de marque.



Industrie de l'IoT : la clé de la pérennisation

Anticipation des menaces émergentes, intégration des technologies innovantes, conformité proactive… toutes ces pratiques aideront les fabricants à sécuriser leurs produits, mais aussi à les préparer aux enjeux futurs. En adoptant cette approche prospective stratégique, ils s'imposeront en tant que leaders du secteur IoT, capables de livrer des produits de pointe sécurisés, fiables et pérennes à l'épreuve des technologies de demain.

CHAPITRE 5

CONFIANCE POUR LES APPAREILS : DES AVANTAGES CONCRETS

Quoi de mieux que l'expérience de clients réels pour se rendre compte des avantages d'un framework de sécurité robuste ? Les études de cas ci-dessous illustrent la puissance transformatrice de la confiance pour les appareils et les méthodes pour appliquer cette approche. Elles présentent en termes concrets l'impact de ces pratiques pour les entreprises afin de mieux vous éclairer sur leurs avantages stratégiques.

Étude de cas n° 1

Client : fabricant d'appareils domotiques

Solution : mise en place d'un framework de sécurité pour une gamme complète de produits

Résultat : réduction significative des cas de compromission, accompagnée d'un renforcement de la confiance des clients et d'une consolidation de son image de marque, comme en témoigne l'accroissement considérable de sa part de marché. Après calcul, le fabricant a pu quantifier son retour sur investissement (ROI), qui s'est avéré nettement supérieur aux projections initiales.

Étude de cas n° 2

Client : multinationale spécialisée dans les appareils IoT industriels

Solution : optimisation des processus de conformité

Résultat : l'entreprise a capitalisé sur une solution avancée de sécurité des appareils pour optimiser ses processus de conformité, avec à la clé des économies et un TTM (Time-to-Market) accéléré pour les nouveaux produits. Grâce à ce framework, elle a pu automatiser des volets essentiels de la gestion de la sécurité des appareils, réduisant la charge de travail des équipes IT et le risque d'erreur humaine dans la gestion des certificats.

Étude de cas n° 3

Client : grand constructeur automobile

Solution : développement d'une solution de sécurité personnalisée

Résultat : la solution de sécurité sur mesure a permis au constructeur de créer une plateforme automobile connectée hautement sécurisée. La réussite de ce partenariat confirme le statut de leader de l'entreprise, véritable force d'innovation dans le secteur des technologies automobiles. Il souligne également toute la détermination et l'expertise du fournisseur de solution face à des enjeux industriels uniques.

À l'heure où les compromissions de données et les vulnérabilités font la une de l'actualité, il est indispensable d'adopter une approche proactive et exhaustive de la sécurité.

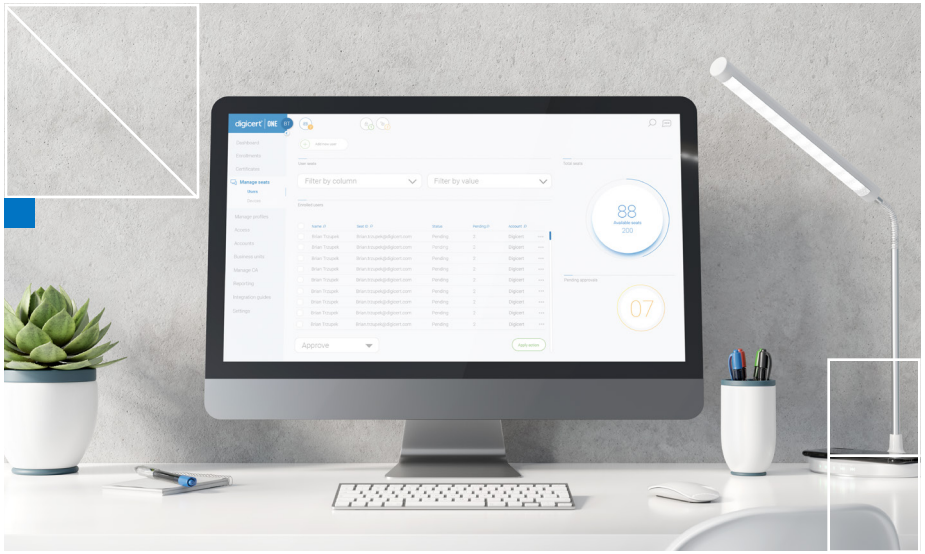
Des solutions de sécurité à l'impact durable

L'impact des solutions déployées dans ces études de cas s'étend bien au-delà du simple volet opérationnel : leurs répercussions stratégiques vont jusqu'à influencer la façon dont l'entreprise est perçue dans son secteur. À l'heure où les compromissions de données et les vulnérabilités font la une de l'actualité, il est indispensable d'adopter une approche proactive et exhaustive de la sécurité.

LA SÉCURITÉ DES APPAREILS, REMPART DES ENTREPRISES

La sécurité des appareils, rempart des entreprises

La sécurité des appareils et l'excellence opérationnelle sont devenues des enjeux décisifs. Face à des menaces toujours plus complexes, une seule solution : adopter une approche proactive de la sécurité des appareils.



DigiCert® IoT Trust Manager vous simplifie la tâche. Rendez-vous sur digicert.com/fr/contact-us pour en savoir plus sur la confiance pour les appareils. Vous découvrirez comment cette approche sécurise l'IoT, vos données et toute votre entreprise contre les menaces d'aujourd'hui et de demain.

À propos de DigiCert

Leader de la confiance numérique, DigiCert apporte aux entreprises, aux particuliers, aux pouvoirs publics et aux consortiums les outils qui leur permettront d'échanger et de communiquer de façon sereine et sécurisée dans l'univers du digital.

Sa plateforme DigiCert® ONE assure aux organisations une visibilité centralisée et un contrôle inégalé sur leurs besoins de confiance numérique pour sécuriser tout leur environnement : site web, accès et communications d'entreprise, logiciels, identités, contenus et appareils. Son logiciel de premier plan, associé à une parfaite maîtrise des standards, des services de support et des opérations, fait de DigiCert le garant de la confiance numérique des entreprises dans le monde entier.