LIVRE ÉLECTRONIQUE

Construire l'analyse de rentabilisation d'une stratégie ICP axée sur le cloud

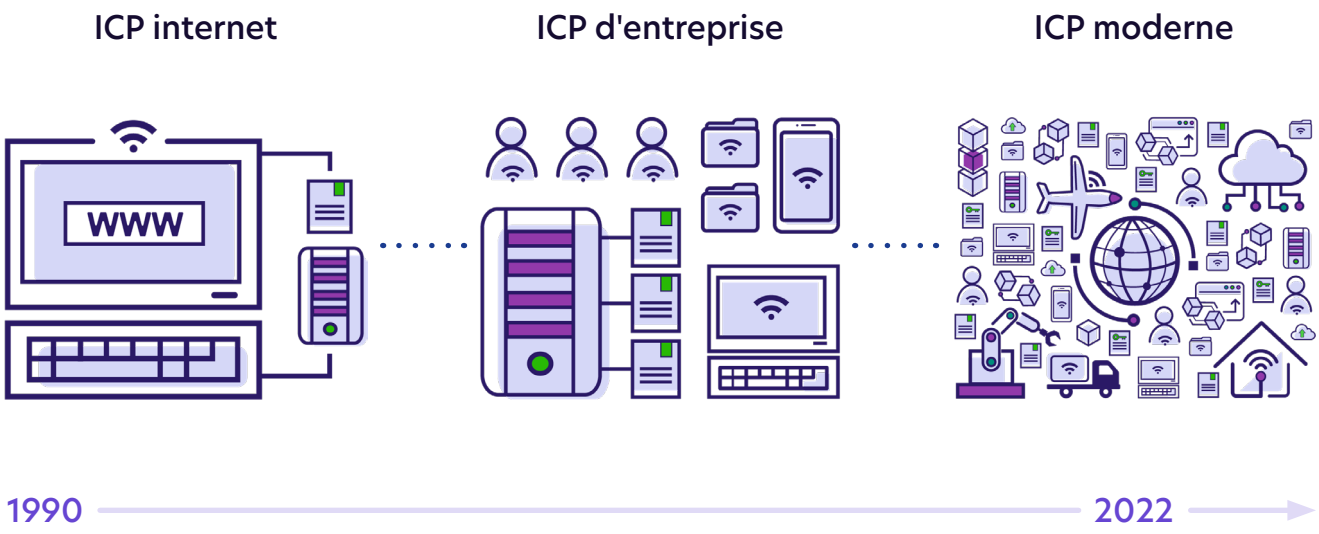
KEYFACTOR

Sommaire

Introduction

Le passage à l'hybride et au multi-cloud est inévitable. Aujourd'hui, les applications doivent fonctionner partout et évoluer rapidement. Que votre organisation ait une stratégie axée sur le cloud ou que vous migriez des applications héritées vers le cloud, les avantages sont bien connus. Dans ce nouveau modèle cloud, les équipes chargées de l'ICP et de la sécurité ont la possibilité d'accélérer leurs propres initiatives et de profiter des avantages de l'infrastructure cloud.

En tant qu'élément essentiel de la sécurité, l'infrastructure à clé publique (ICP) est d'une importance cruciale. Au fil du temps, l'utilisation des certificats ICP et X.509 est devenue synonyme de l'abandon des limites de confiance définies par le réseau à un contrôle axé sur l'identité. Dans l'ensemble, nous avons été témoins de trois époques distinctes d'ICP.



ICP internet

Le premier algorithme asymétrique (RSA) a été introduit en 1977, mais ce n'est que lorsque l'internet s'est établi que l'ICP a vraiment décollé. Dans les années 1990, des autorités de certification (CA) de confiance publique ont été introduites pour établir une confiance généralisée dans l'internet. L'ICP a permis aux organisations d'acheter et de fournir des certificats TLS, principalement pour leurs sites Web et applications destinés au public. Cette période de l'ICP a été marquée par un certain nombre d'autorités de certification (CA) de confiance publique et de certificats à longue durée de vie.

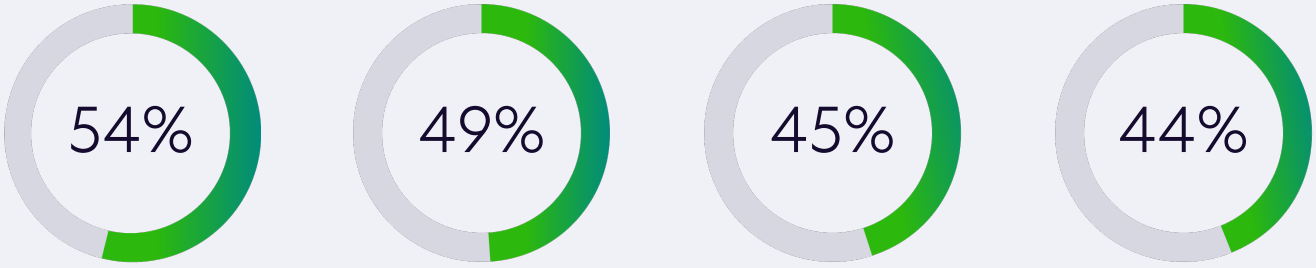
ICP d'entreprise

Dans les années suivant l'introduction de l'ICP, de nombreuses organisations ont réalisé le besoin d'une confiance interne. Les équipes informatiques et de sécurité ont identifié des moyens pratiques de déployer et d'utiliser l'ICP au niveau interne afin de protéger les communications internes, d'authentifier les utilisateurs et les appareils et d'introduire la signature numérique des documents et du code. Cette période de l'ICP a été définie par l'utilisation généralisée d'outils ICP hérités comme Microsoft ADCS pour émettre de plus grands volumes de certificats pour les utilisateurs, les appareils et l'équipement du réseau.

ICP moderne

Aujourd'hui, les organisations tirent pleinement parti de l'ICP pour instaurer la confiance au sein de leurs environnements distribués et connectés. Tout le monde, des architectes de la sécurité aux ingénieurs réseau, en passant par les équipes d'infrastructure et DevOps, s'appuie désormais sur les ICP et les certificats numériques. L'infrastructure à clé publique et les autorités de certification sont déployées dans toute l'organisation pour prendre en charge des cas d'utilisation spéciaux, ce qui rend la gestion et la gouvernance beaucoup plus difficiles. Dans le même temps, les durées de vie plus courtes et les plus grands volumes de certificats posent de nouveaux défis à la gestion.

Les tendances les plus importantes qui promeuvent le déploiement d'ICP, des clés et des certificats



Stratégie de sécurité zéro confiance

Services basés sur le cloud

Télétravail

Internet des objets (IoT ou IdO)

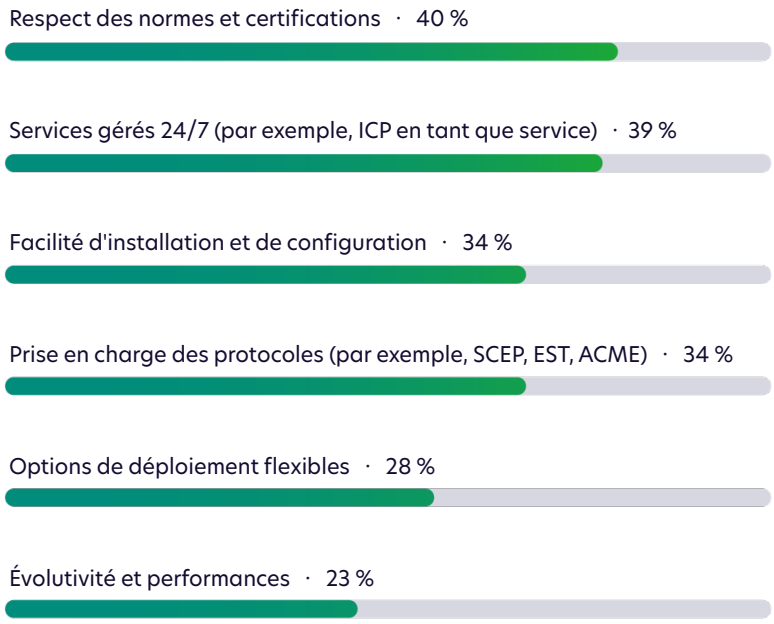
ICP et migration vers le cloud

La migration vers le cloud, les nouveaux cas d'utilisation et un manque général d'expertise en ICP ont forcé de nombreuses équipes à revoir leur stratégie. Au fur et à mesure de l'évolution de la technologie sous-jacente à l'ICP et à la gestion des certificats, de nouveaux modèles de déploiement basés sur le cloud offrent des possibilités de bénéficier de tous les avantages de l'ICP moderne, sans l'empreinte complexe, les contrôles de sécurité et les charges de travail nécessaires pour l'exécution au niveau interne.

Les obstacles à l'utilisation de l'infrastructure à clé publique SaaS s'estompent également rapidement à mesure que les fournisseurs introduisent des fonctionnalités robustes et démontrent leur conformité aux normes réglementaires les plus sévères. Aujourd'hui, de plus en plus d'organisations ont réalisé qu'elles pouvaient atteindre des niveaux de service (SLA) et une conformité aux mandats de sécurité requis plus élevés qu'elles ne pourraient le faire en interne.

Les caractéristiques les plus importantes lors de la sélection de solutions ICP

État de la gestion de l'identité des machines en 2022



L'ICP est de plus en plus complexe

Il est clair que l'ICP est une infrastructure critique, mais de nombreuses organisations ne disposent pas des ressources, de l'expertise ou du temps disponibles pour la gérer. Au regard du nombre croissant de cas d'utilisation et d'intégrations pris en charge par l'ICP, il est parfois difficile de faire face au coût et à la complexité des déploiements ICP.

La complexité croissante entraîne des interruptions du service et des erreurs qui mettent l'entreprise en danger, comme des clés privées non protégées ou une mauvaise configuration de l'autorité de certification. Pour éviter les erreurs fréquentes et une charge inutile pour les équipes, l'idée d'une infrastructure à clé publique en mode SaaS est devenue beaucoup plus intéressante.

Cela dit, il existe de nombreuses façons de migrer l'ICP vers le cloud et plusieurs facteurs importants à prendre en compte pour votre programme ICP, notamment :

Personnel

L'ICP nécessite certaines compétences pour la mise en œuvre de plusieurs composants importants, notamment des règles précises pour la signature de la clé racine, la création d'une PC/DPC, la sauvegarde de la racine de confiance, la configuration des autorités de certification émettrices et de l'infrastructure de révocation, et la maintenance des modèles et des politiques de certificat.

Infrastructure

N'oubliez pas que l'ICP est bien plus qu'un logiciel et des certificats d'autorité de certification. Il s'agit d'un ensemble complet d'infrastructures de serveurs, de bases de données, de HSM, de sauvegarde et de reprise après sinistre, et de politiques de certificat qui nécessitent une diligence constante. Il est important de déterminer si votre centre de données peut répondre à ces exigences de manière rentable et efficace.

Sécurité

En tant que racine de confiance pour votre organisation, l'ICP nécessite des contrôles de sécurité solides. La réalisation de niveaux de sécurité et d'assurance suffisamment élevés avec une infrastructure sur site existante peut s'avérer difficile et onéreuse, surtout si vous n'êtes pas préparé à tout ce que cela implique.

Évaluation des coûts de l'ICP sur site

Au-delà des complexités potentielles de l'exécution de l'ICP en interne, l'hébergement de l'ICP dans votre centre de données peut entraîner plusieurs coûts, attendus et potentiellement inattendus, notamment la mise en œuvre, la main-d'œuvre et l'infrastructure, ainsi que les temps d'arrêt.

Déploiement initial

Que vous reconstruisiez votre ICP ou que vous partiez de zéro, les coûts du déploiement peuvent rapidement dépasser les attentes.

Il peut sembler facile d'installer une autorité de certification Microsoft avec des configurations par défaut, mais la réalité est que l'ICP nécessite beaucoup plus de travail lorsqu'elle est effectuée correctement.

Efforts et dépenses potentiels :

- Architecture ICP et planification des cas d'utilisation
- Configuration initiale du logiciel CA
- Création d'une politique de certification et d'une déclaration des pratiques de certification (PC/DPC)
- Exécution des règles de signature de la clé racine
- Services de consultants ICP pour la mise en œuvre

Travail et soutien continu

Les experts en ICP sont difficiles à trouver et encore plus difficiles à retenir. Même si vous disposez des compétences nécessaires dans votre entreprise, l'évolution des priorités ne permet pas toujours de se concentrer sur l'ICP comme il le faudrait.

Outre le fait que les utilisateurs de certificats ne sont pas des experts, ils ont besoin d'une assistance continue pour demander, renouveler et fournir correctement des certificats pour leurs propres applications.

Efforts et dépenses potentiels :

- Recruter et former du personnel ICP qualifié
- Maintenir la disponibilité CRL et OCSP
- Temps de fonctionnement et renouvellements de l'autorité de certification émettrice et racine
- Maintenance du serveur, tests de sauvegarde et de reprise après sinistre, et résilience
- Formation interne et assistance continue pour les utilisateurs de certificats
- Temps d'arrêt et correction liés aux certificats

Matériel et logiciel

En ce qui concerne l'infrastructure, différents composants sont nécessaires pour prendre en charge un déploiement ICP, notamment les HSM, les serveurs, les bases de données et les plateformes de virtualisation sur lesquelles vous exécutez votre ICP.

Par exemple, l'exécution de votre ICP sur une infrastructure virtualisée avec une sauvegarde et une restauration appropriées entraîne des frais de sécurité élevés.

Efforts et dépenses potentiels :

- Serveur racine de l'autorité de certification hors ligne et isolé
- HSM et enregistrement verrouillable
- Matériel ou infrastructure cloud permettant d'héberger plusieurs serveurs CA
- Licences logicielles pour serveurs, bases de données, logiciels de sécurité et de surveillance
- Contrats d'assistance auprès de plusieurs fournisseurs de matériel et de logiciels

Contrôles de sécurité

Selon les niveaux d'assurance requis par les politiques informatiques de l'entreprise ou les mandats réglementaires externes, les coûts liés à la sécurité de votre infrastructure ICP peuvent rapidement dépasser les prévisions initiales.

Ces contrôles sont nécessaires pour garantir que la racine de confiance derrière votre organisation soit protégée des compromis ou des erreurs de configuration.

Efforts et dépenses potentiels :

- Centres de données hautement sécurisés
- Contrôles de sécurité biométriques et physiques
- Personnel de sécurité et surveillance
- Boîtier hautement sécurisé et/ou ignifuge pour le matériel clé de racine
- Contenants et scellés inviolables
- Considérations environnementales, y compris l'alimentation de secours et le refroidissement

ANALYSE DE RENTABILISATION :

EQ Bank

Equitable Bank

L'Equitable Bank, l'une des plus grandes banques du Canada, s'est aperçue que sa mise en œuvre actuelle de l'ICP ne pouvait pas prendre en charge sa migration vers Azure. Le vice-président de l'infrastructure de sécurité, David Yu, et son équipe ont rapidement élaboré l'analyse de rentabilisation d'une solution ICP basée sur le cloud.

Principaux défis :

- ✗ Les Active Directory Certificate Services (AD CS) hérités ne pouvaient pas prendre en charge les nouvelles exigences du cloud et de DevOps
- ✗ L'utilisation de certificats auto-signés dans les environnements de développement ne répondait pas aux exigences de sécurité
- ✗ Les développeurs se sont heurtés à des obstacles avec les certificats en raison de processus manuels et d'une ICP héritée
- ✗ Une mauvaise visibilité a entraîné des pannes inattendues, causées par des certificats expirés et mal configurés
- ✗ Les dépenses d'exploitation de l'infrastructure ICP effectuées conformément à des normes de sécurité élevées n'étaient pas réalisables en interne
- ✗ L'équipe interne n'avait pas assez de temps ou de ressources pour se consacrer au déploiement de leur ICP

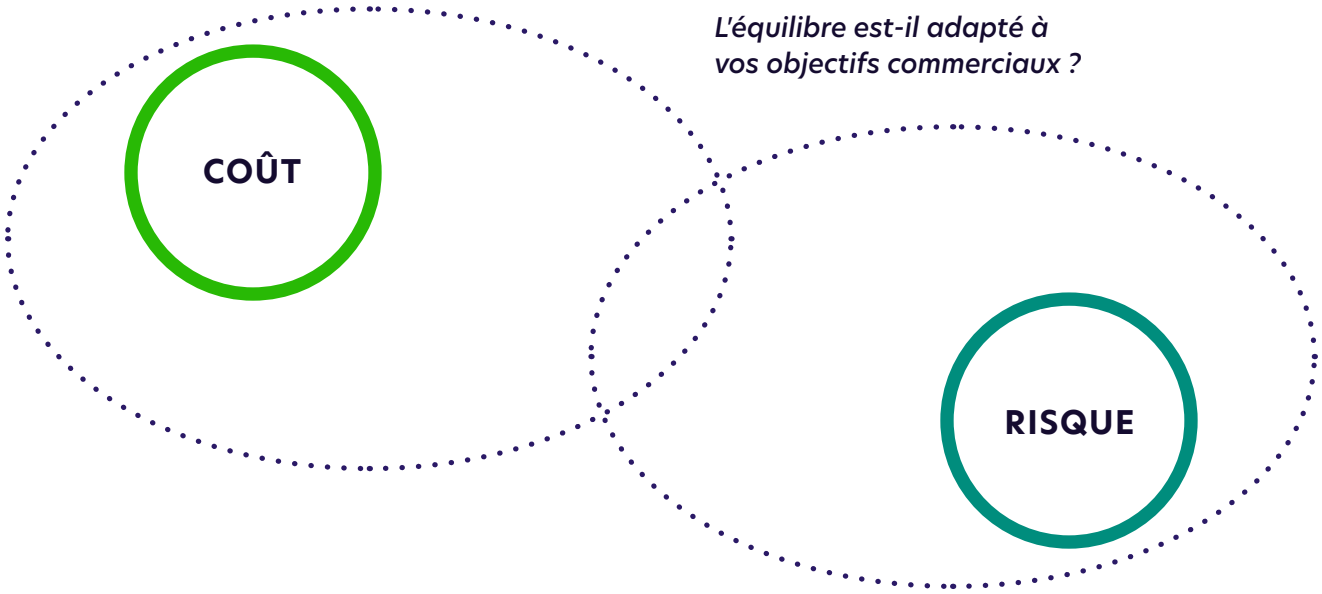
En passant à l'ICP en tant que service, EQ Bank a pu sécuriser sa plate-forme bancaire principale hébergée dans Azure avec une ICP robuste, a réduit le coût et les risques liés à l'exécution de l'ICP en interne et a permis à ses équipes DevOps d'évoluer plus rapidement, en toute sécurité.

Principaux résultats :

- ✓ Migration de l'ancien AD CS vers une infrastructure ICP robuste basée sur le cloud en quelques semaines
- ✓ Réduction de la charge de travail manuelle liée à l'ICP et aux certificats correspondant à l'équivalent de 2 emplois à plein temps (ETP)
- ✓ Élimination complète des pannes liées aux certificats et DevOps pris en charge via les API et l'automatisation

Évaluation du risque vs coûts pour l'ICP

Lors de l'examen des coûts de mise en œuvre de l'infrastructure à clé publique, les organisations visent généralement à réduire ou à minimiser les coûts et à accroître la sécurité. Cependant, assurer simultanément la sécurité et la rentabilité crée un dilemme et nécessite souvent des compromis pour respecter les délais du projet ou des budgets limités.



Les risques de réduction des coûts

L'hébergement de l'ICP peut être coûteux. C'est pourquoi, les équipes cherchent souvent des moyens de réduire les coûts. Malheureusement, ceci entraîne généralement une réduction des principaux contrôles et processus de sécurité.

Les risques de la réduction des coûts

Parallèlement, la sécurité de l'ICP étant essentielle, les équipes souhaitent également éliminer les vecteurs de risque, ce qui augmente inévitablement les frais de mise en œuvre de l'ICP.

Par conséquent, il est très difficile de trouver le bon équilibre entre la sécurité et la rentabilité, en particulier lorsque les équipes s'appuient sur une infrastructure ICP sur site existante et manquent d'expertise pour la mettre en œuvre correctement.

Avantages de la migration de l'ICP vers le cloud

Les solutions ICP basées sur SaaS visent à résoudre le défi consistant à avoir un rapport acceptable entre les risques et les coûts, ce qui permet aux organisations de trouver un équilibre et de tirer parti de l'économie d'échelle. Les organisations peuvent également accélérer le déploiement, répondre aux exigences de sécurité et prendre en charge simultanément les cas d'utilisation Cloud-native et traditionnels sur site.

Haute évolutivité

Permet aux équipes de créer de nouvelles autorités de certification et/ou d'émettre des certificats instantanément en quelques clics

Déploiement plus rapide

Les offres ICP SaaS clé en main réduisent le temps de déploiement de quelques mois à plusieurs jours, voire plusieurs heures

Diminution des coûts

Élimine le besoin d'approvisionner des serveurs, des bases de données, des HSM et autres logiciels et matériels de support

Sécurité améliorée

L'ICP fonctionne sur des installations hautement sécurisées et à la pointe de la technologie, et est exploitée par des fournisseurs conformes et audités

Libère l'informatique

Réduit la charge des équipes internes et élimine les tâches de maintenance de l'ICP répétitives et à faible valeur ajoutée

Facilité d'intégration

De nombreuses solutions ICP basées sur SaaS offrent des intégrations flexibles et une automatisation prêtes à l'emploi

Stratégies pour l'ICP dans le cloud

Il existe de nombreuses raisons pour la mise à niveau de votre ICP, qu'il s'agisse de la migration vers le cloud, de l'expiration de la racine ou de l'autorité de certification émettrice, ou de la nécessité de prendre en charge davantage de cas d'utilisation. Cependant, il n'y a pas qu'un seul chemin vers le cloud. En matière d'ICP, vous avez le choix.

ICP hybride

Une option consiste à créer et à exécuter votre ICP en interne et à l'intégrer à vos services et applications basés sur le cloud dans une architecture hybride. Contrairement aux anciens déploiements ICP basés sur Microsoft, les solutions ICP modernes comme EJBCA prennent en charge les ICP matérielles ou logicielles qui peuvent s'exécuter dans votre centre de données ou votre environnement cloud, mais avec l'extensibilité et l'évolutivité nécessaires aux environnements modernes hybrides et multi-cloud.

ICP SaaS clé en main

Une autre option consiste à tirer parti d'une ICP fournie par SaaS, telle que EJBCA SaaS, qui permet aux organisations d'éliminer les efforts et les dépenses liés à l'exécution de l'infrastructure dorsale requise pour prendre en charge l'ICP. Cependant, les équipes ont toujours la possibilité de lancer et de configurer des autorités de certification et des modèles pour répondre à leurs cas d'utilisation et à leurs exigences. Il s'agit d'un équilibre entre conserver le contrôle et réduire certains des efforts impliqués dans la gestion de l'ICP.

ICP gérée

Les organisations à la recherche d'une approche axée davantage sur une ICP « sans intervention » peuvent opter pour un service d'ICP entièrement géré et hébergé dans le cloud. Souvent appelées ICP en tant que service, ces solutions offrent une approche sans contact, avec un déploiement, une surveillance et une gestion ICP de bout en bout gérés par une équipe d'experts qualifiés. Ces solutions offrent également souvent une autorité de certification racine isolée et hors ligne, protégée par plusieurs mesures de sécurité biométriques et physiques.

ICP par Keyfactor

Chez Keyfactor, nous pensons que les équipes doivent avoir la flexibilité nécessaire pour déployer l'ICP telle qu'elle est nécessaire et partout - dans le cloud ou sur site, entièrement gérées ou auto-hébergées. Cette approche aide les organisations à simplifier leur ICP et à favoriser la confiance numérique dans leur paysage connecté, tel qu'il est aujourd'hui et quelle que soit son évolution future.

Mieux encore, nous combinons nos solutions ICP avec une automatisation du cycle de vie de bout en bout pour les clés et les certificats dans les environnements informatiques de l'entreprise, DevOps et même IoT et IIoT. Il s'agit d'une plateforme unique pour l'ICP et l'automatisation de l'identité des machines.

Pourquoi Keyfactor

✓ Fortes compétences ICP

L'ICP est plus qu'un simple logiciel. Nous avons plus de 20 ans d'expérience en ingénierie, architecture et conception ICP.

✓ Une plateforme

Nos clients bénéficient d'une plateforme unique pour l'ICP et l'automatisation du cycle de vie des certificats. Moins de complexité, plus d'agilité.

✓ Simplicité

La sécurité ne fonctionne que lorsqu'elle est adoptée. Nos solutions visent à simplifier l'ICP et les certificats pour les experts ICP et les utilisateurs non spécialisés.

✓ Flexibilité

Vous avez la possibilité d'exécuter l'ICP tel que vous le désirez et dans l'emplacement voulu, dans le cloud, comme architecture hybride ou sur site.

✓ Évolutivité

Nos solutions ont été testées et éprouvées pour fonctionner sans effort dans des environnements avec des millions, voire des milliards de certificats.

✓ Fiable et conforme

Keyfactor travaille sans relâche pour se conformer aux normes de sécurité industrielles comme ISO 27001, ISO 9001, les critères communs, SOC 2 Type II, etc.

Prêt à migrer votre ICP ?

Vous savez déjà que l'ICP est essentielle à la sécurité, mais la mise en place de l'infrastructure et des ressources nécessaires pour la construire et l'exploiter correctement n'est pas une tâche facile.

Les équipes de sécurité étant soumises à une pression croissante, une stratégie ICP axée sur le cloud peut les aider à simplifier et à échelonner l'émission de certificats à la demande, en fonction de l'augmentation des cas d'utilisation.

PRISE DE CONTACT

Commencez votre voyage vers le ICP sur cloud, demandez une démonstration à un expert Keyfactor

DEMANDER UNE DÉMO

KEYFACTOR

Keyfactor est la plate-forme d'identité machine et IoT pour les entreprises modernes. L'entreprise aide les équipes de sécurité à gérer la cryptographie comme une infrastructure critique en simplifiant l'ICP, en automatisant la gestion du cycle de vie des certificats, et en favorisant l'agilité cryptographique à grande échelle.

Pour en savoir plus, visitez www.keyfactor.com ou suivez-nous sur LinkedIn, Twitter, et Facebook.

Bâti sur la confiance et la sécurité, Keyfactor est un fier employeur garantissant l'égalité des chances, un partisan et un défenseur de la création d'un lieu de travail fiable, sécurisé, diversifié et inclusif.

CONTACTEZ-NOUS

- www.keyfactor.com
- +1.216.785.2946