Les 10 principaux indicateurs ICP à suivre

Obtenez les indicateurs dont vous avez besoin pour analyser l'état de chaque identité de machine.

KEYFACTOR

EBOOK

Contenus

KEYFACTOR

Introduction

Si vous exécutez des opérations d'infrastructure à clé publique (ICP) dans votre entreprise ou si vous êtes responsable de la gestion de milliers de clés et de certificats, ce livre électronique est exactement ce qu'il vous faut.

Soyons réalistes. Il y a beaucoup à prendre en compte lorsqu'il s'agit de l'état de l'infrastructure à clé publique et des identités des machines.

Obtenir un inventaire précis de chaque clé et certificat est le point de départ, mais ce n'est vraiment que la pointe de l'iceberg. Il existe de nombreux indicateurs d'activité, d'efficacité, d'efficience qui se prêtent à un suivi, mais si vous êtes dans la même situation que la plupart des organisations avec du temps et des ressources limités, vous devez vous concentrer sur l'essentiel.

C'est pourquoi, nous avons défini les 10 principaux indicateurs à utiliser pour gérer efficacement la cryptographie dans votre entreprise.

Ce guide vous aidera, vous et votre équipe, à créer une base de référence pour éviter les pannes évitables, les risques de sécurité et les frustrations causées par des identités de machine inconnues ou non suivies.

Les 10 principaux indicateurs ICP

#1: État d'expiration

Qui doit être informé ?

- Propriétaires d'applications
- Gestionnaires
- Administrateurs ICP

Pourquoi devriez-vous vous en soucier ?

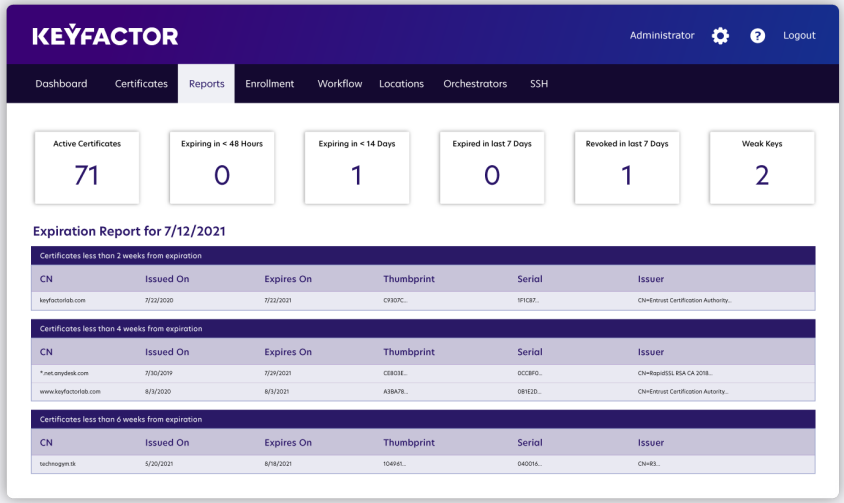
Sans une visibilité adéquate sur chaque clé et chaque certificat, vous ne saurez pas quand ils expireront. Pire encore, si vous ne savez pas à qui transmettre les informations, le risque de panne de réseau continuera d'augmenter au fur à mesure que vous ajoutez des identités dans votre entreprise.

Ces pannes entraînent des temps d'arrêt coûteux, qui finissent par reposer sur les pieds de l'exécutif lorsqu'ils se produisent.

Exemple de rapport

Ce rapport fournit une vue des expirations à venir ainsi que le laps de temps restant jusqu'à l'expiration.

Ceci vous permet de planifier les certificats à renouveler en premier et de voir qui est responsable du renouvellement.



#2: Taille et importance de la clé

Qui doit être informé ?

- Administrateurs ICP
- Auditeurs
- Équipes de sécurité

Pourquoi devriez-vous vous en soucier ?

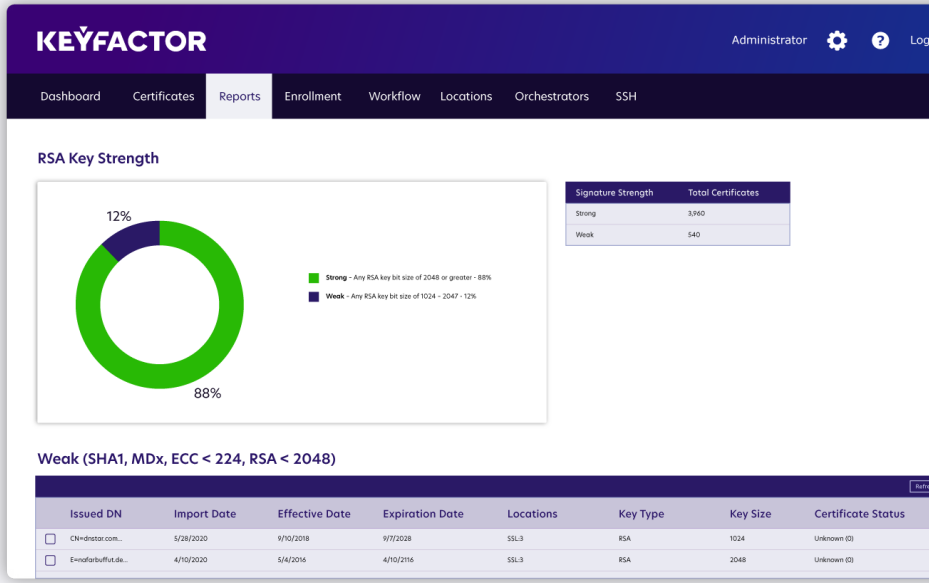
Les algorithmes évoluent avec les progrès de l'informatique et, comme eux, vous devez être en mesure de vous adapter rapidement et avec un minimum de perturbations pour les applications et l'infrastructure existantes.

Ce rapport permet aux équipes de voir les certificats vulnérables dans leur environnement et de commencer à les remplacer par des certificats plus solides et conformes.

De plus, la révocation en bloc et la réémission de certificats via une plate-forme automatisée peuvent aider à réduire considérablement le temps nécessaire pour résoudre les problèmes et l'impact sur vos opérations.

Exemple de rapport

Ce rapport affiche un graphique à secteurs pour chaque autorité de certification sélectionnée indiquant les certificats actifs par taille de clé (par exemple, 1 024 bits, 2 048 bits). Il fournit également des informations détaillées sur les lignes pour localiser les certificats faibles.



#3: Algorithmes de signature

Qui doit être informé ?

- Administrateurs ICP
- Auditeurs
- Équipes de sécurité

Pourquoi devriez-vous vous en soucier ?

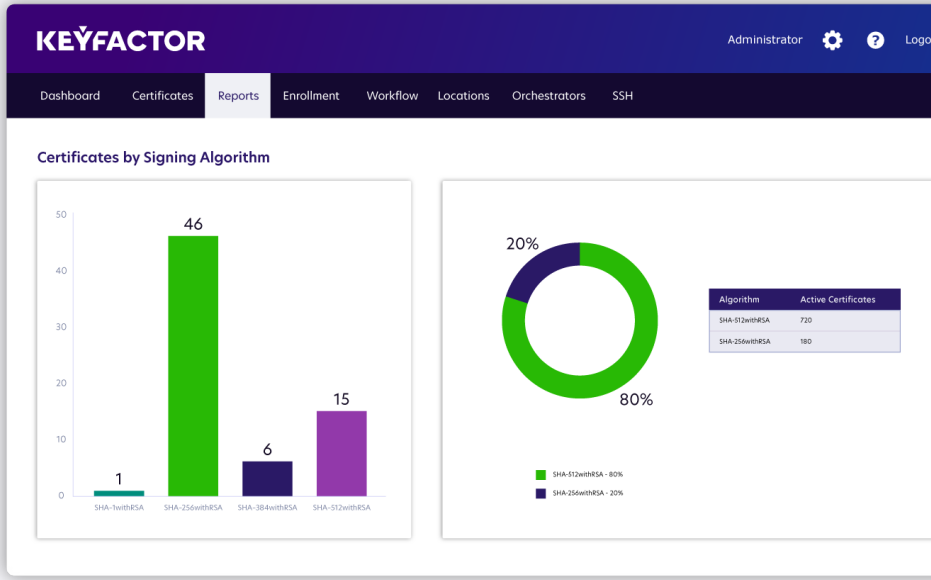
Les algorithmes de signature clés sont le fondement de la confiance et de la sécurité de votre ICP. Comme pour la taille et l'importance de la clé, il est essentiel de suivre les algorithmes de signature et de se préparer à la migration si - ou plus précisément quand - l'algorithme est obsolète.

Un exemple bien connu est la migration de SHA-1 vers SHA-2, une transition qui a été beaucoup plus longue et perturbatrice qu'elle n'aurait dû l'être pour de nombreuses organisations.

Les hachages plus grands sont généralement plus sûrs car ils sont moins vulnérables aux attaques par collision. Cependant, la définition de « plus grand » est en constante évolution dans le monde de la cryptographie.

Exemple de rapport

Ce rapport vous montrera où vous pouvez augmenter la robustesse de vos signatures numériques en voyant l'algorithme de hachage (par exemple, SHA-1, SHA-256) utilisé pour créer le hachage utilisé dans la signature.



#4: Émission d'autorité de certification (CA)

Qui doit être informé ?

- Administrateurs ICP
- Équipes de sécurité

Pourquoi devriez-vous vous en soucier ?

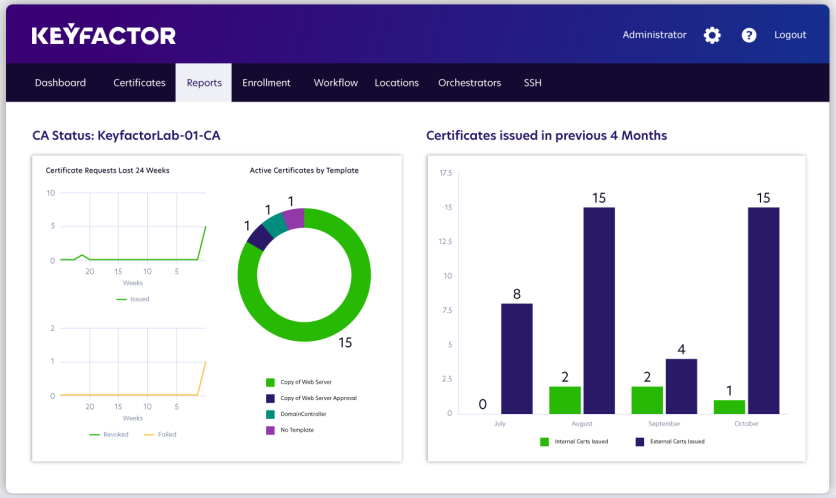
Pour les administrateurs ICP travaillant avec plusieurs CA, vous avez besoin d'une vue d'ensemble de l'activité qui se déroule sur la CA à un moment donné. Cela peut être utile pour détecter une activité anormale.

Par exemple, un GPO mal configuré peut émettre des certificats alors qu'il ne le devrait pas. Ceci entraîne le déploiement d'identités de machine dans votre environnement dont vous n'avez pas besoin. Les identités inutiles offrent davantage de portes qu'un attaquant peut essayer d'utiliser.

Exemple de rapport

Ces diagrammes circulaires et graphiques linéaires indiquent le nombre de certificats émis, refusés et révoqués pour une période de temps sélectionnée pour la ou les autorités de certification (CA) sélectionnées.

Les équipes peuvent définir des alertes qui sont déclenchées si une autorité de certification émet des certificats à un rythme extrême. Cela aide les administrateurs à comprendre si une émission anormale de certificats se produit sans qu'ils le sachent.



#5: Demandeurs et propriétaires de certificats

Qui doit être informé ?

- Propriétaires d'applications
- Gestionnaires de certificats

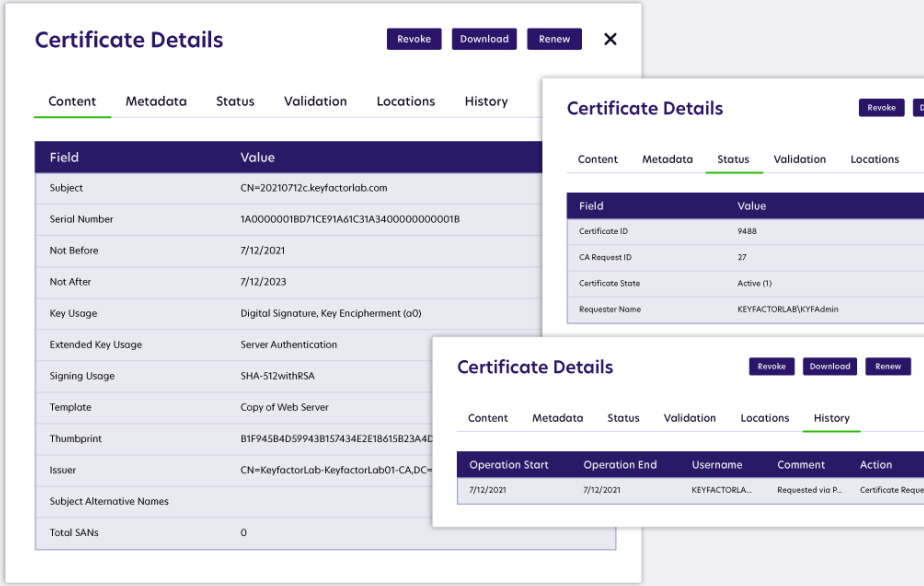
Pourquoi devriez-vous vous en soucier ?

Lorsqu'un certificat arrive à échéance ou est en panne, la première question qui est habituellement posée est : « À qui appartient le certificat ? » Sans savoir qui est le titulaire du certificat, le temps d'arrêt de l'entreprise se prolonge jusqu'à ce que quelqu'un soit avisé du renouvellement du certificat.

Savoir exactement à qui appartiennent les certificats vous permet d'envoyer des rappels et des alertes au propriétaire direct pour éviter toute panne imprévue.

Exemple de rapport

Voir qui demande des types de certificats spécifiques peut permettre aux administrateurs de prévoir les tendances d'émission de certificats dans le temps et d'afficher les coordonnées des demandeurs.



#6: Certificats auto-signés

Qui doit être informé ?

- Administrateurs ICP
- Équipes de sécurité
- Propriétaires d'applications
- Gestionnaires de certificats

Pourquoi devriez-vous vous en soucier ?

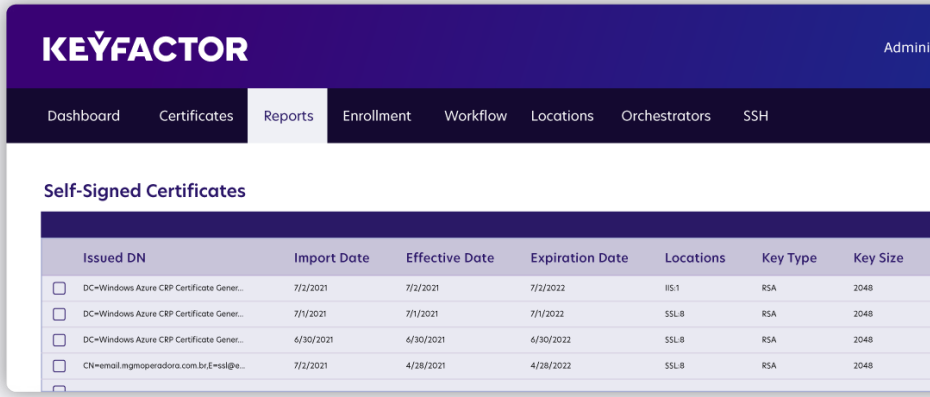
La vitesse de DevOps a rapidement augmenté l'utilisation de certificats auto-signés au sein des équipes d'ingénierie. Bien qu'ils se déploient extrêmement rapidement, un certificat auto-signé est un certificat qu'une autorité de certification ne signe pas du tout - ni privé ni public.

C'est pourquoi il est recommandé d'intégrer des gestionnaires de secrets avec des émetteurs conformes à la politique (autorités de certification publiques ou privées). Ainsi, vous pouvez configurer la surveillance de l'émission de certificats à volume élevé à partir de ces gestionnaires de secrets. Sans cette intégration, l'audit du cycle de vie des certificats devient presque impossible.

Exemple de rapport

Ce rapport affichera le nombre de certificats auto-signés par environnement avec des paramètres de surveillance des seuils de certificat. Si le seuil de certificat est atteint, l'administrateur ICP sera alors conscient du nombre élevé de certificats auto-signés utilisés.

En comparant le nombre de certificats auto-signés aux certificats soutenus par une autorité de certification, les équipes peuvent comprendre où réside le risque dans l'organisation.



#7: Certificats génériques

Qui doit être informé ?

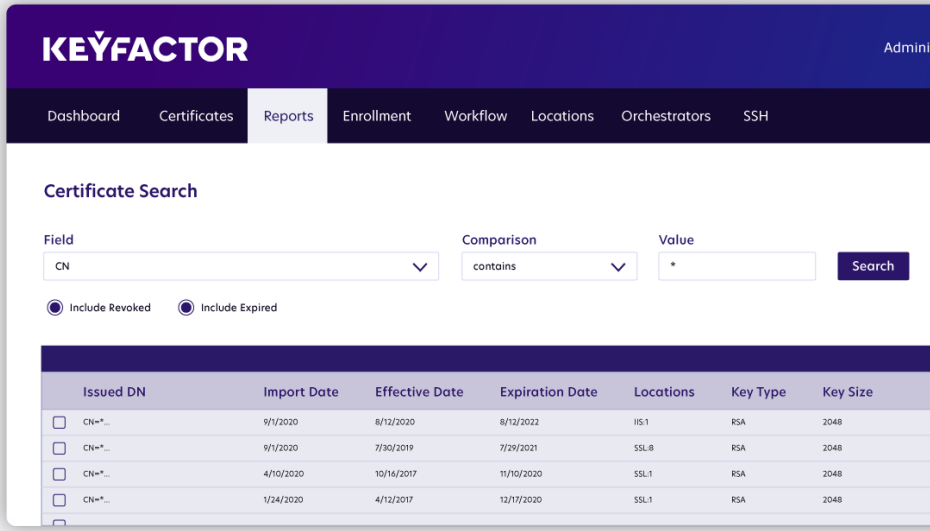
- Administrateurs ICP
- Équipes de sécurité

Pourquoi devriez-vous vous en soucier ?

Les certificats génériques SSL peuvent présenter un avantage pour les organisations qui souhaitent déployer et sécuriser un grand nombre de sous-domaines. En revanche, alors qu'ils offrent des économies de coûts et de la flexibilité, leur recours à la même clé privée augmente le risque d'un compromis à l'échelle de l'organisation.

Exemple de rapport

Ce rapport indique le nombre de certificats génériques dans l'inventaire et chaque point de terminaison utilisé avec chaque certificat. La recherche de « * » aide l'administrateur ICP à comprendre la portée de l'utilisation des certificats génériques et à remédier à tout point de défaillance unique.



#8: Certificats automatisés vs manuels

Qui doit être informé ?

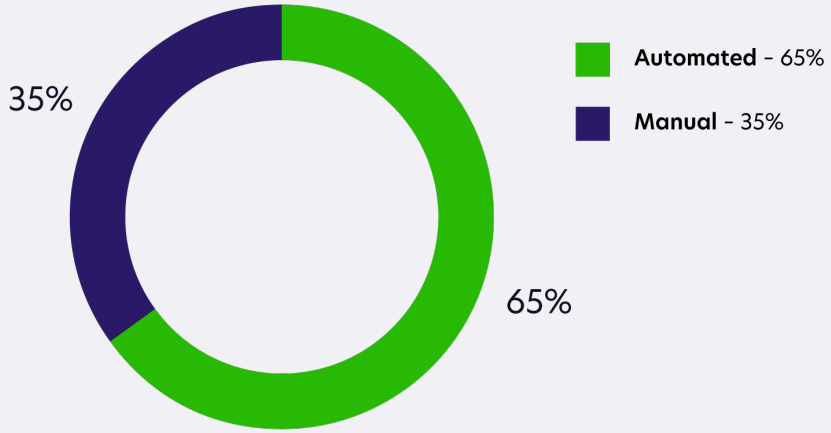
- Administrateurs ICP
- Équipes de sécurité
- Cadres

Pourquoi devriez-vous vous en soucier ?

Votre objectif doit être d'obtenir autant d'automatisation du cycle de vie des certificats que possible pour les certificats sous votre contrôle. Cependant, sans comprendre la quantité de processus de gestion de certificats ad hoc et manuels que vous avez en place, il est difficile de définir des objectifs d'automatisation.

Exemple de rapport

Ce rapport comparatif indique le nombre de certificats automatisés par comparaison aux certificats gérés. Il surveillera activement les certificats qui ont lancé les renouvellements et les déploiements automatisés sur les charges de travail et les terminaux.



#9: État CRL

Qui doit être informé ?

- Administrateurs ICP
- Équipes de sécurité

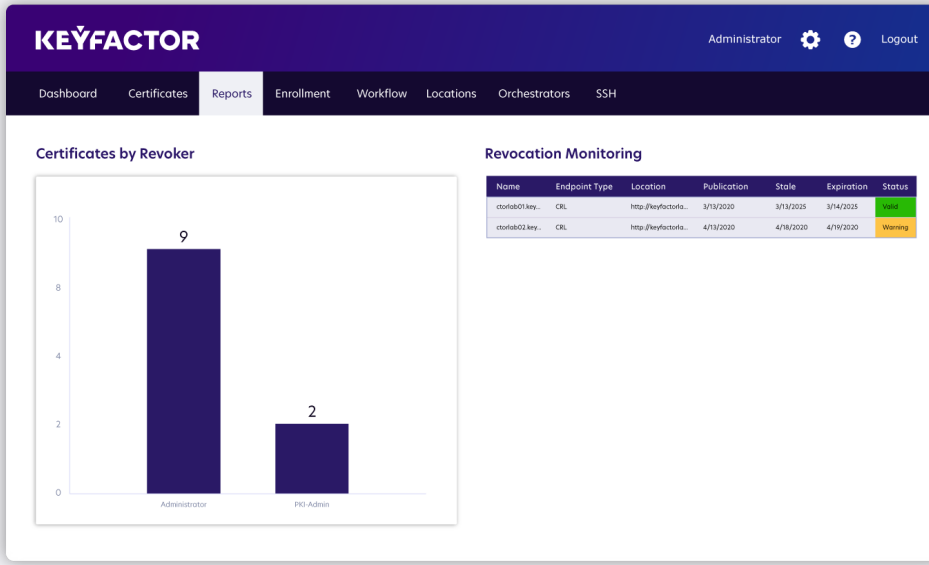
Pourquoi devriez-vous vous en soucier ?

Les certificats sont révoqués pour diverses raisons : compromission de la clé ou de l'autorité de certification, certificat devenu inutile ou certificat remplacé. Voir qui révoque les certificats permet à un administrateur ICP de procéder à un suivi afin de déterminer si des applications ou des points de terminaison connexes pourraient nécessiter une correction similaire.

Par exemple, si une clé est compromise, l'administrateur de la sécurité peut souhaiter contacter le responsable de la révocation pour déterminer l'origine du problème. Ceci lui permet de comprendre les processus pour éviter un futur compromis qui pourrait permettre à un attaquant d'accéder au système.

Exemple de rapport

Ce rapport affiche un graphique à barres du nombre de certificats révoqués à partir d'une plage de dates sélectionnée pour des autorités de certification spécifiques. Ce rapport peut en outre décomposer quel utilisateur effectue la révocation.



#10: Certificats inconnus

Qui doit être informé ?

- Administrateurs ICP
- Équipes de sécurité

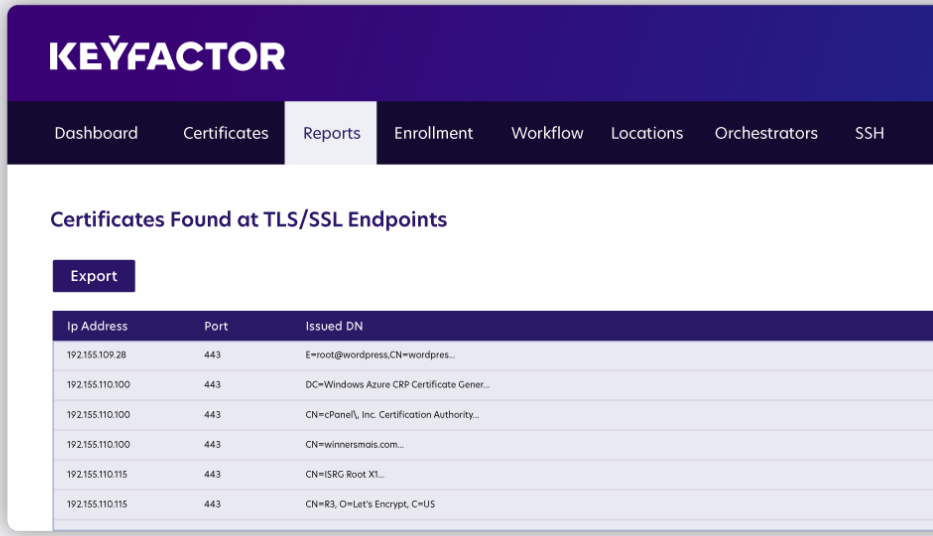
Pourquoi devriez-vous vous en soucier ?

Quoi de pire que de ne pas gérer un certificat connu ? Ce n'est pas gérer un inconnu. Ces certificats anonymes sont ceux qui proviennent d'autorités de certification que vous ne connaissez pas. Ce sont des certificats qui se trouvent sur des terminaux inconnus.

Sans savoir où se trouve chaque certificat, vous êtes vulnérable aux pannes imprévues, aux temps d'arrêt coûteux et à une exposition accrue aux risques.

Exemple de rapport

Ce rapport affiche le résultat d'une analyse planifiée ou à la demande des terminaux TLS/SSL. En analysant vos points de terminaison, votre équipe peut surveiller en permanence tous les certificats inconnus afin que vous puissiez les mettre sous gestion du cycle de vie.



Tout rassembler avec les tableaux de bord Keyfactor

L'examen de ces indicateurs peut aider à analyser l'état de votre ICP. Cependant, il est difficile de déterminer précisément où vous devez vous concentrer sans les voir ensemble dans une vue holistique et pratique.

C'est là que Keyfactor peut vous aider.

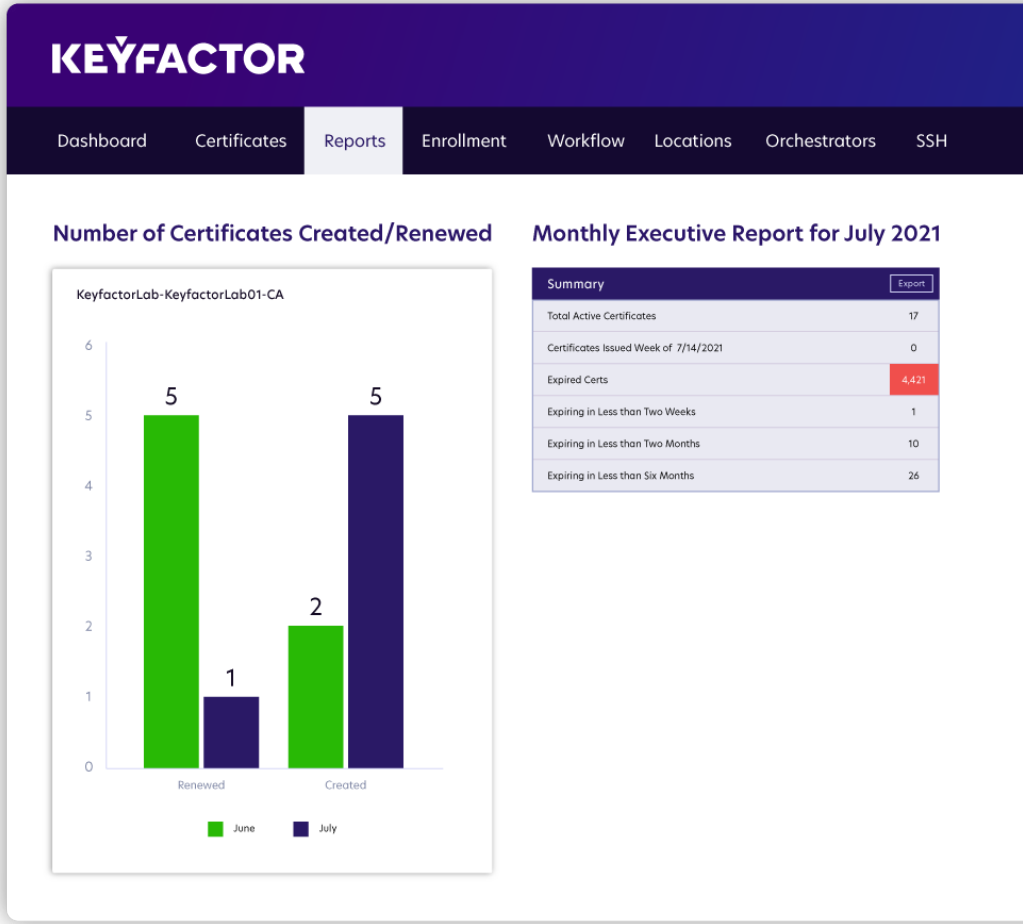
En combinant ces mesures dans des tableaux de bord exécutifs et d'équipe, Keyfactor vous permet de mieux visualiser les points sur lesquels vous devez vous concentrer pour améliorer vos pratiques de gestion et d'automatisation des certificats.

Rapport exécutif mensuel

Ce tableau de bord offre aux dirigeants un aperçu de l'activité d'émission au cours du mois écoulé, par rapport au mois précédent. Ceci leur permet également de voir le nombre de certificats qui arriveront à expiration dans les 30 prochains jours et le nombre de certificats en cours d'émission par l'autorité de certification.

Ce rapide aperçu de l'état de l'autorité de certification permet à un cadre de voir en quelques secondes s'il existe des drapeaux de haut niveau indiquant un problème éventuel.

Par exemple, un grand nombre (voire aucun !) de certificats devant expirer dans les 16 à 30 prochains jours pourrait indiquer qu'il existe un risque de panne et une enquête rapide pour faire remplacer le certificat avant que cela ne se produise.

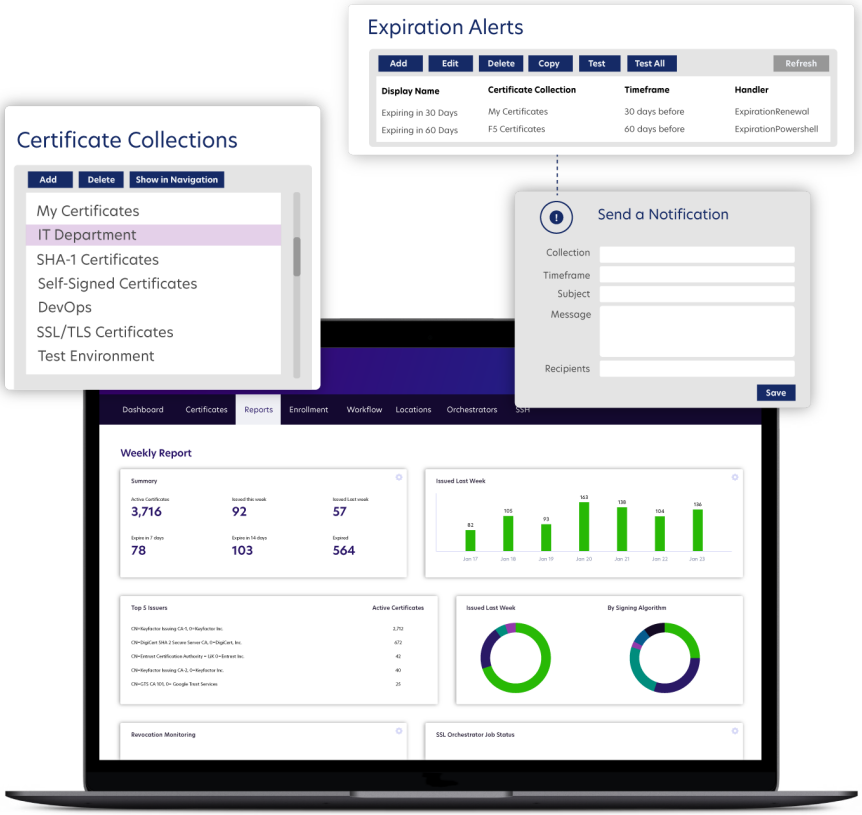


État de santé de l'état de l'ICP

Pour les cadres disposant d'une formation plus technique, ainsi que pour les administrateurs ICP et les propriétaires d'applications, ce rapport fournit une vue du tableau de bord avec tous les types d'indicateurs de l'état de l'ICP en liaison avec les certificats concernés par les rapports.

En un coup d'œil, le rapport montre, entre autres, les émissions, les expirations, l'importance des clés, les émetteurs et l'activité de l'autorité de certification.

Avoir une vue d'ensemble de l'état de l'ICP peut être un bon point de départ pour déterminer, le cas échéant, les secteurs de l'environnement qui ont besoin d'attention pour corriger les pannes, les GPO mal configurés, etc.



KEYFACTOR

Il est temps d'améliorer les rapports.

Reprenez le contrôle de votre cryptographie avec Keyfactor.

Keyfactor fournit une fenêtre unique sur plusieurs identités de machine, telles que les clés et les certificats utilisés dans les environnements hybrides et multicloud des organisations.

Demandez une démonstration sur la façon dont vous pouvez améliorer la visibilité, le contrôle et l'automatisation pour chaque identité de machine.

DEMANDER UNE DÉMO

KEYFACTOR

Keyfactor est le leader des solutions ICP en tant que service et de crypto-agilité basées sur le cloud. Notre plate-forme Crypto-Agility permet aux équipes de sécurité d'orchestrer de manière transparente chaque clé et chaque certificat dans l'ensemble de l'entreprise.

Nous aidons nos clients à appliquer correctement la cryptographie, des entreprises modernes multi-cloud aux chaînes d'approvisionnement IoT complexes. Avec des dizaines d'années d'expérience dans la cybersécurité, Keyfactor bénéficie de la confiance de plus de 500 entreprises à travers le monde.

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