

Les angles morts des certificats: une panne en attente de se produire

Selon le rapport DigiCert 2026 Global PKI Research Report, seules 34% des entreprises disposent d'un inventaire complet de leurs certificats.



Les organisations sont moins bien préparées qu'elles ne le pensent. De nouvelles conclusions d'Omdia et de DigiCert expliquent pourquoi.

Les organisations exploitent des environnements PKI dont elles n'ont pas une visibilité complète, tout en restant responsables des interruptions de service, des failles de sécurité et des manquements à la conformité.

La PKI n'est plus un simple système. C'est un écosystème complet qui s'est fragmenté trop rapidement pour que les organisations puissent suivre le rythme.

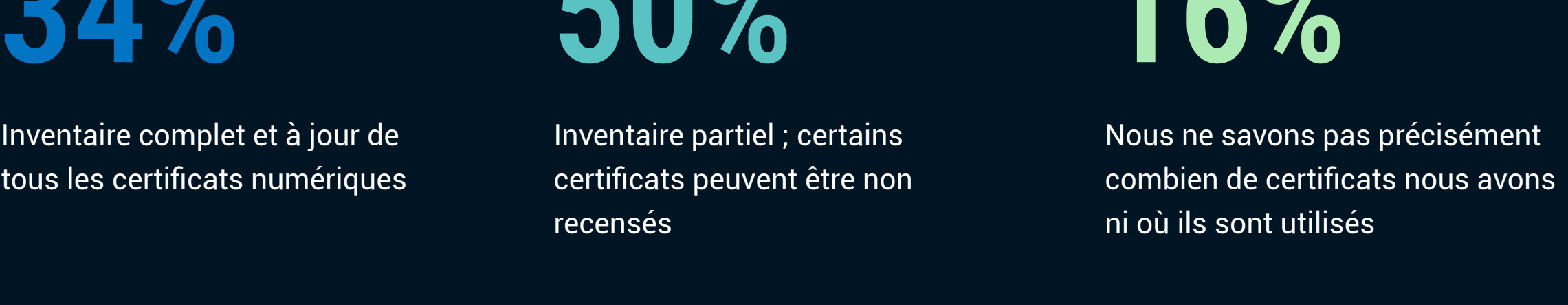
La modernisation de la PKI ne peut plus attendre. L'IA et le quantique accélèrent la nécessité de passer de la prise de conscience à l'action.

On ne peut pas gérer ce que l'on ne voit pas.

Le risque lié à la PKI commence par un manque de visibilité. De nombreuses entreprises exploitent des environnements de certificats dont elles n'ont pas une connaissance exhaustive, créant ainsi une exposition systémique.

Près de 2 entreprises sur 3 ne disposent pas d'un inventaire complet et à jour de leurs certificats numériques.

Quelle proposition décrit le mieux la situation actuelle de votre organisation en matière de suivi des certificats numériques ?



Le risque lié à la PKI est compris. Mais il n'est pas maîtrisé.

Il existe un écart manifeste entre la prise de conscience et la mise en œuvre. Les organisations reconnaissent le risque, mais leurs modèles opérationnels n'ont pas évolué au même rythme.

Entreprises très ou extrêmement préoccupées par:

73%

Risque de pannes ou d'interruptions de service dues à des certificats expirés

74%

Prolifération des certificats à mesure que le nombre de systèmes ou d'identités augmente

La PKI a évolué. Sa gestion n'a pas suivi.

Le suivi manuel et les feuilles de calcul restent la méthode de gestion des certificats la plus utilisée.

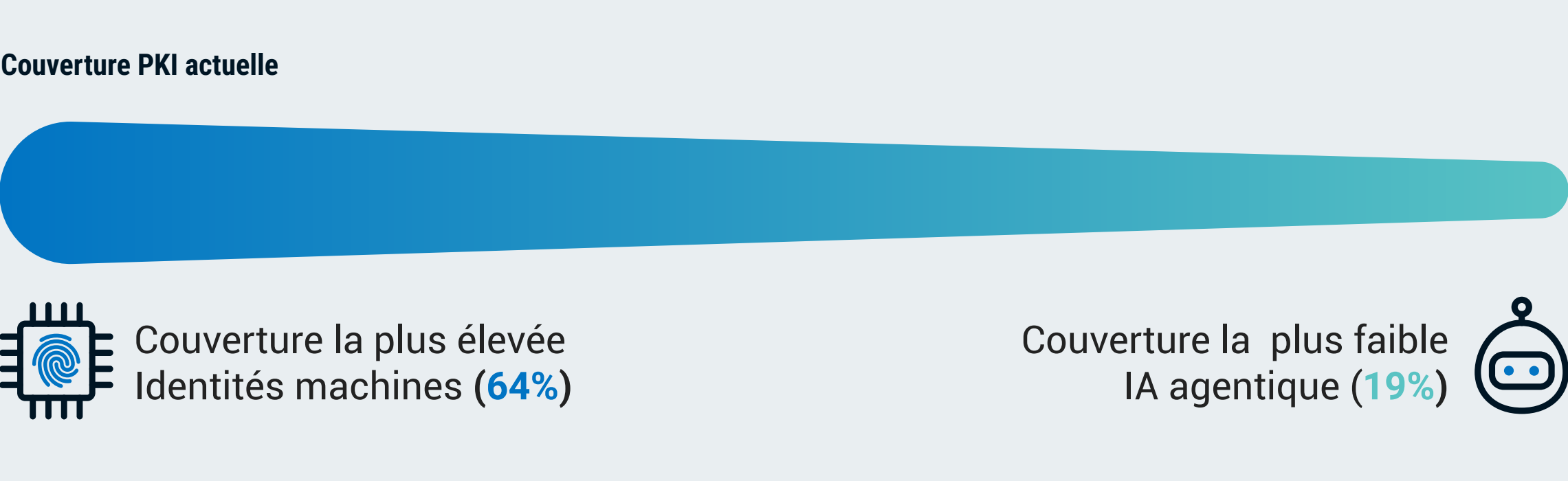
La complexité est l'ennemie de la PKI moderne.

La PKI est devenue structurellement complexe, et pas seulement techniquement. Les difficultés d'intégration et les frictions organisationnelles constituent désormais les principaux freins au progrès.



L'explosion des identités représente à la fois un défi et une opportunité pour la PKI.

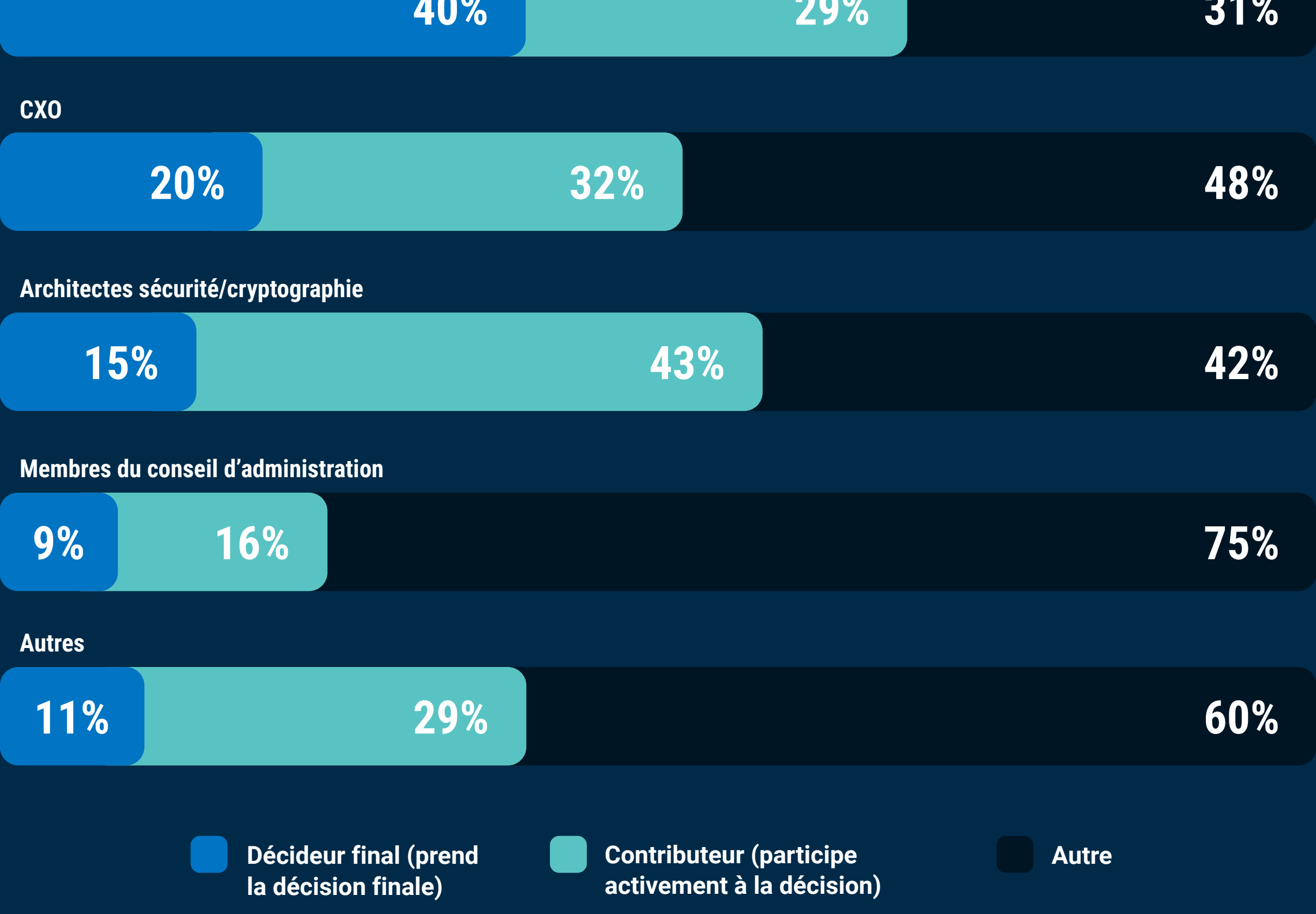
Le passage à grande échelle aux identités non humaines (NHI) met à rude épreuve les approches PKI traditionnelles, en particulier avec l'IA agentique. Les organisations doivent redoubler d'efforts pour répondre aux besoins de couverture.



Tout le monde utilise la PKI. Personne n'en est véritablement responsable.

La dilution des responsabilités ralentit les progrès. La modernisation de la PKI n'est pas seulement un défi technique: c'est aussi un enjeu de gouvernance et de responsabilité.

Quel est le niveau d'implication de chaque partie prenante dans les décisions relatives à la PKI au sein de votre organisation?



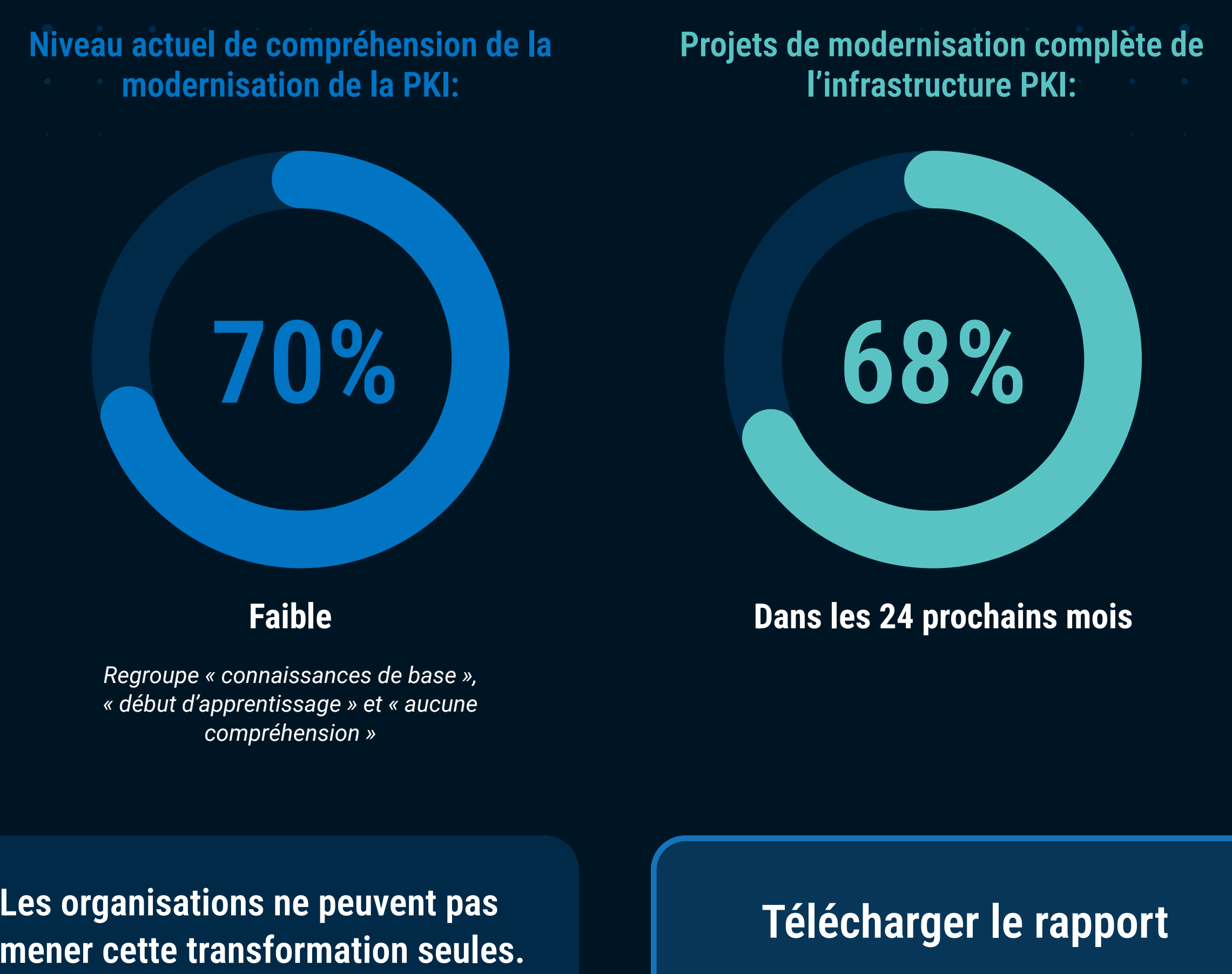
Dans 40% des organisations, le RSSI est le principal décideur en matière de PKI.

Les DSI, les CTO et les équipes de sécurité contribuent à la prise de décision, mais un soutien accru du reste de l'équipe dirigeante est nécessaire.

Seulement 9% des décisions relatives à la PKI sont prises au niveau du conseil d'administration.

L'avenir de la confiance est déjà là. Les organisations ne sont pas prêtes.

La prochaine vague de besoins, portée par l'IA, le risque quantique et le Zero Trust, progresse plus vite que le niveau de préparation des organisations.



Les organisations ne peuvent pas mener cette transformation seules. L'expertise et l'accompagnement des fournisseurs de confiance numérique et de leurs partenaires les aideront à réussir cette transition.

Les organisations ayant engagé la modernisation de leur PKI constatent une réduction de plus de 60% des interruptions de service.

Télécharger le rapport

