Au cœur de RSA: Déploiement à grande échelle de solutions FIDO et sans mot de passe

Le défi

Lorsqu'une organisation vend des solutions d'authentification, elle doit se poser cette question difficile : **utilise-t-elle réellement ce qu'elle fournit comme solution ?**

En 2024, la direction de RSA s'est fixé un objectif : arrêt total de l'utilisation des mots de passe pour tous ses employés. RSA est une entreprise de sécurité mondiale dont les employés sont répartis dans le monde entier, une situation qui reflète celle de nombreuses entreprises. La motivation pour arrêter l'utilisation des mots de passe était double : réduire les risques liés au détournement de ces mots de passe et renforcer la sécurité de RSA, et enfin utiliser et évaluer en interne ses propres solutions. RSA s'est mis à la place de ses clients pour appréhender chaque défi d'intégration, chaque décision stratégique et chaque frein au changement auxquels les entreprises sont confrontées lors du déploiement à grande échelle d'une solution sans mot de passe et de la technologie FIDO.

Voici ce que RSA a appris lorsque la théorie s'est confrontée à la réalité.

Position de départ de RSA

Pour RSA, la solution était evidente. RSA® ID Plus est une plateforme d'identité et gestion des accès (IAM) prenant en charge l'authentification multi facteur sans mot de passe, l'accès, l'authentification unique (SSO) et d'autres fonctionnalités dans les environnements cloud, hybrides et sur site.

RSA développait activement les fonctionnalités nécessaires aux entreprises pour un déploiement sans mot de passe (flux d'inscription, procédures de récupération et règles d'accès), alors même que les employés de RSA utilisaient encore des mots de passe. Les équipes de sécurité et de R&D de RSA avaient mené des expérimentations préliminaires avec les clés de sécurité matérielles FIDO, confirmant ainsi les propriétés de sécurité de cette technologie. Ces expérimentations ont également mis en lumière les réalités opérationnelles du déploiement de l'authentification FIDO : difficultés d'interopérabilité entre les plateformes, complexité de la distribution à l'échelle mondiale et un certain écart à résoudre entre une preuve de concept fonctionnelle et un déploiement à l'échelle de l'entreprise. La décision de déployer RSA ID Plus afin de prendre en charge l'authentification sans mot de passe au sein même de l'organisation RSA n'était pas une opération marketing. C'était le seul moyen honnête de valider l'efficacité de la solution RSA ID Plus pour tous les utilisateurs, dans tous les environnements et pour tous les cas d'utilisation.

Auteurs de l'étude : Shauna Pettit-Brown, Robert Hughes, Jean-Christophe Laurent, Kenn Chong, and Philip J Corriveau

À propos de RSA Security

RSA fournit les fonctionnalités de gestion des identités, d'authentification, de contrôle d'accès, de gouvernance et de cycle de vie nécessaires pour prévenir les menaces, sécuriser l'accès et garantir la conformité. Plus de 9 000 organisations, dont la sécurité est une priorité absolue, font confiance à RSA pour gérer plus de 60 millions d'identités dans des environnements sur site, hybrides et multicloud. Pour plus d'informations, consultez RSA.com.

Ce que le déploiement interne a révélé

Déployant sa propre plateforme, RSA en a tiré un enseignement crucial : ID Plus fonctionnait comme prévu. La complexité résidait dans son intégration avec l'écosystème d'identité de la compagnie au sens large.

Lors de cette mise en place, RSA a découvert des scénarios reposant par défaut sur l'utilisation de mot de passe. Dans le cadre de la mise en œuvre d'une authentification 100 % sans mot de passe. Ce qui suit détaille ces scénarios, et comment RSA les a résolues afin de garantir une authentification sans mot de passe pour chaque utilisateur, dans chaque environnement et tout au long du cycle de vie de son identité.

Le dilemme architectural

L'un des premiers cas d'utilisation identifiés par RSA concernait l'enrôlement des nouveaux utilisateurs et l'enregistrement de leur premier authentificateur. Le portail libre-service RSA exigeait un authentificateur pour l'authentification sans mot de passe, mais les nouveaux employés avaient besoin d'un mot de passe pour accéder au portail et enregistrer leur premier authentificateur. Il ne s'agissait pas d'une limitation du produit, mais d'une dépendance architecturale antérieure qui supposait que les utilisateurs auraient besoin d'un mot de passe.

Correction apportée par RSA (fin 2024) :

- Inscription des nouveaux utilisateurs ⟶ Point d'entrée dédié ne nécessitant aucun mot de passe
- Récupération de compte ⟶ Processus distinct ne dépendant pas de la réinitialisation du mot de passe
- Authentification quotidienne ⟶ Règles définissant l'authentification sans mot de passe par défaut

Ce que RSA a appris : ayant mis en œuvre ces changements, RSA pose désormais des questions différentes à ses clients lors de la planification.

Non pas « quels authentificateurs souhaitez-vous ? » mais « où les mots de passe sont-ils encore requis ? »

Sécuriser les interactions avec le service d'assistance

Alors que RSA déployait l'authentification sans mot de passe et simplifiait l'enrôlement des nouveaux utilisateurs, l'entreprise s'est penchée sur un problème de sécurité connexe : la vérification auprès du service d'assistance. Les méthodes de vérification traditionnelles basées sur des connaissances (identifiant de l'employé, nom du responsable) peuvent être exploitées par des attaquants, pour ensuite manipuler le personnel d'assistance afin qu'il réinitialise les identifiants, ou inciter les employés à divulguer leurs identifiants.

L'approche RSA: RSA a mis en œuvre une vérification bidirectionnelle en temps réel pour les interactions avec le service d'assistance. Lorsqu'un employé contacte l'assistance, l'agent lance une session de vérification. L'employé s'authentifie à l'aide d'une méthode enregistrée (clés d'accès, code QR, biométrie), et le système génère un code à usage unique que l'employé communique à l'agent. Ceci permet de vérifier l'identité des deux parties, confirmant ainsi que l'utilisateur est légitime et que l'agent est un représentant autorisé.

Ce que RSA a appris: une infrastructure sans mot de passe a rendu cette solution possible. RSA a pu exploiter les mêmes méthodes que ses employés utilisaient déjà pour l'authentification quotidienne, ce qui élimine les secrets partagés au niveau du point de contact du service d'assistance, cible privilégiée des attaques d'ingénierie sociale.

Complexité des règles et de la gestion de groupe

La plateforme ID Plus dispose de fonctionnalités robustes en matière de gestion des règles de sécurité. Cependant, son déploiement interne a révélé la complexité organisationnelle liée à la définition et à la mise en œuvre coordonnée de ces règles. RSA a dû répondre aux questions suivantes lors du déploiement de l'authentification sans mot de passe :

- Quels sont les premiers groupes à bénéficier des nouvelles règles ?
- Comment les règles devraient-elles être mises en œuvre progressivement entre les départements ayant des profils de risque différents ?
- Quel est le plan de repli pour les cas particuliers imprévus ?

Ce que RSA a appris : il ne s'agit pas d'un problème technologique que les clients peuvent résoudre avec un logiciel. C'est un problème de prise de décision organisationnelle. Cela exige du temps, l'adhésion des parties prenantes et des itérations. RSA ne pouvait pas se permettre de raccourcir le processus, et RSA ne peut pas non plus le faire pour ses clients ; mais RSA peut partager son expérience sur ce qui a fonctionné et ce qui n'a pas fonctionné.

La percée de la clé d'accès FIDO 'mobile'

Grâce à l'architecture de la plateforme ID Plus, RSA a pu relever le défi de la distribution matérielle auquel ses équipes de R&D étaient confrontées.

Début 2025, RSA a intégré le support des clés d'accès FIDO ("Passkeys" en Anglais) liées à l'appareil dans son application d'authentification mobile, qui est désormais certifiée FIDO2. Cela a permis à RSA de distribuer des clés d'accès s'adaptant facilement aux méthodes de travail existantes de ses employés.

L'avantage de l'adoption : les employés utilisaient déjà l'application mobile de RSA pour s'authentifier. L'ajout de l'utilisation des clés d'accès ne nécessitait donc aucune nouvelle application, aucune inscription séparée et aucune nouvelle configuration par l'utilisateur.

Résultat : L'adoption des clés d'accès n'a pas été difficile, mais une extension naturelle des comportements existants. RSA a éliminé le problème lié à la distribution de clés de sécurité physiques rencontrés par les équipes de R&D tout en maintenant la résistance au phishing inhérente à l'authentification FIDO.

Pourquoi c'est important pour les entreprises : Les organisations évaluent généralement les clés d'accès synchronisées par rapport aux clés de sécurité matérielles.

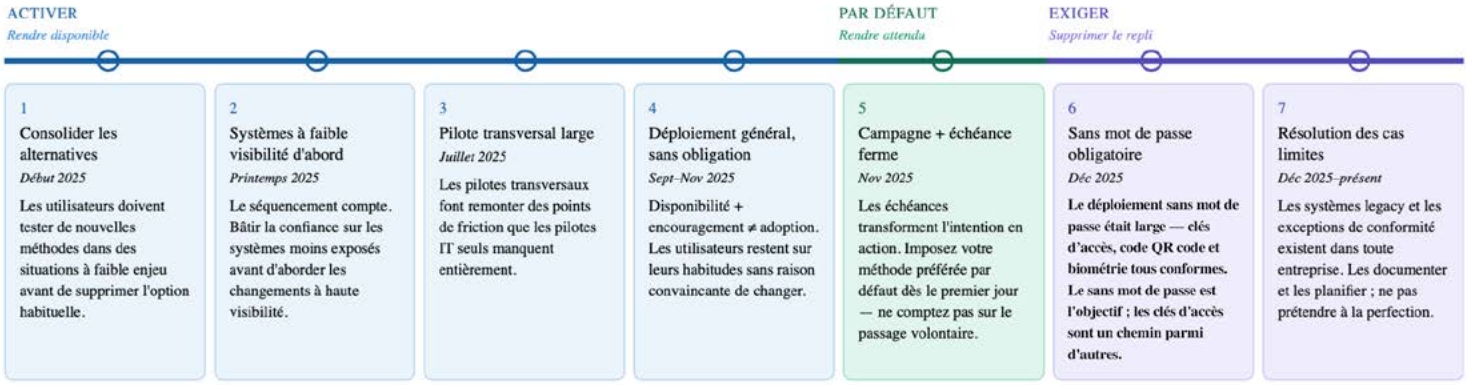
Elles oublient souvent l'existence d'une troisième option : les clés d'accès liée à l'appareil, intégrées à une application d'authentification mobile d'entreprise existante. Cette solution offre aux organisations une meilleure sécurité, avec une expérience utilisateur améliorée et sans les coûts inhérents à la distribution de matériel.

Le parcours de déploiement : quand la technologie rencontre le comportement humain

Avec une plateforme prête et des clés d'accès 'mobile' disponibles , RSA a commencé le déploiement interne, et **à alors découvert que la préparation technique n'est pas forcément synonyme de préparation organisationnelle.**

La technologie a été déployée en quelques semaines. Modifier les habitudes des employés a pris plus de temps, jusqu'à un an pour certains. Ce processus s'est déroulé en trois étapes importantes : rendre l'authentification sans mot de passe disponible **(Activation)**, en faire la méthode par défaut **(Par défaut)** et supprimer complètement l'option mot de passe **(Obligation)**. Les étapes ci-dessous correspondent à cette évolution.

FIGURE
Le parcours sans mot de passe : Activer → Par défaut → Exiger



ACTIVER
Étapes 1 à 4 : Rendre l'accès sans mot de passe disponible

Avant de demander à leurs employés de changer leurs habitudes, les organisations doivent créer un climat de confiance propice à l'expérimentation. La phase de test consiste à lever les freins psychologiques à l'adoption de la nouveauté, non pas en la forçant, mais en veillant à ce que les méthodes familières restent accessibles pendant que les employés s'habituent aux nouvelles. Les études sur la gestion du changement montrent régulièrement que les individus ont besoin d'une exposition progressive à un nouveau comportement avant de l'adopter volontairement en remplacement d'une habitude bien ancrée.

L'objectif ici n'est pas de créer une dynamique, mais d'être prêt.

ÉTAPE 1 :
Renforcer les solutions alternatives avant de supprimer les mots de passe (début 2025)

Authentifications sans mot de passe ajoutées. Authentifications avec mots de passe encore disponibles . Objectif : familiarisation, pas adoption.

Ce que RSA a appris : il est nécessaire d'essayer de nouvelles méthodes dans des situations à faible enjeu avant des supprimer les anciennes.

ÉTAPE 2 :
Supprimer d'abord les mots de passe des systèmes à faible enjeu (Printemps 2025)

Les accès VPN et SSO sont devenus sans mot de passe avant la connexion sur le poste de travail. Cela a normalisé le fait que les mots de passe ne soient pas toujours nécessaires avant le changement le plus visible.

Leçons tirées par RSA : L'ordre des changements est crucial. Il est important de se familiariser avec les changements sur les systèmes moins utilisés avant de s'attaquer à ceux que les employés utilisent le plus fréquemment.

ÉTAPE 3 :
Pilote de déploiement de l'agent MFA pour poste de travail (Juillet 2025)

50 employés réparties dans tous les services — pas seulement le service informatique — ont testé l'authentification par clé d'accès sur poste de travail, tout en pouvant continuer à utiliser leur mot de passe..

Décision clé : La crédibilité repose sur la diversité des rôles, et pas seulement sur des utilisateurs techniques.

Leçons tirées par RSA : Les projets pilotes transversaux font ressortir des difficultés différentes de celles rencontrées par les projets pilotes exclusivement informatiques. RSA a constaté des problèmes d'expérience utilisateur et des lacunes de communication qui seraient autrement passées inaperçues.

ÉTAPE 4 :
Déploiement pour tous, sans obligation pour le moment (sept.-nov. 2025)

L'authentification sans mot de passe du poste de travail est désormais accessible à tous. Les mots de passe fonctionnent toujours.

Résultat : L'adoption a été très modeste. Malgré la disponibilité de l'authentification sans mot de passe et les incitations, la plupart des employés ont continué à utiliser leur mot de passe.

Leçons tirées par RSA : La disponibilité et les incitations ne suffisent pas à garantir l'adoption. Cette expérience directe a permis à RSA de mieux comprendre les difficultés rencontrées par ses clients. Les utilisateurs conservent leurs habitudes à moins d'avoir une bonne raison de changer. Ils peuvent craindre de ne plus pouvoir accéder à leurs systèmes et accomplir leur tâche lorsque les méthodes d'authentification changent.

ÉTAPE PAR DÉFAUT 5 :
Faire de l'authentification sans mot de passe la norme

La disponibilité ne signifie pas l'adoption. Lorsqu'on a le choix entre une voie familière et une nouvelle, on a tendance à choisir le chemin le plus familier. Les recherches comportementales sur les effets par défaut le démontrent clairement : l'option qui demande le moins d'effort l'emporte, même si une autre est objectivement meilleure. La phase par défaut correspond au moment où une organisation cesse de compter sur le changement volontaire et conçoit son système pour que l'absence de mot de passe devienne la norme. Une échéance fixe concrétise ce choix de conception.

ÉTAPE 5 :
Campagne + Date limite claire (novembre 2025)

Programme intensif de 3 semaines combinant :

- Ludification (chasse au trésor, prix, classements)
- Preuve sociale (participation de la direction, parrainage par les pairs)
- Date limite claire : « L'accès sans mot de passe devient obligatoire le 1er décembre »

Résultat : L'utilisation des nouvelle méthodes a triplé en trois semaines.

Ce que RSA a appris : les échéances transforment « je devrais essayer ça un jour » en « je dois le faire maintenant ». L'adoption volontaire stagne, mais les campagnes assorties d'échéances entraînent un véritable changement de comportement – une tendance que RSA prévoit que ses clients rencontreront également.

Autre leçon : si les organisations souhaitent que leurs employés adoptent une méthode d'authentification particulière, il faut la présenter comme la méthode par défaut dès le premier jour. Demander aux utilisateurs de changer activement de méthode de leur propre initiative est une tâche ardue : la plupart resteront sur la voie qui demande le moindre effort. Privilégiez par défaut l'authentificateur de votre choix ; ne comptez pas sur un changement volontaire pour obtenir des résultats.

ÉTAPES 6 À 7 :
Supprimer la solution de secours

Le changement de comportement s'installe durablement lorsque l'ancien comportement n'est plus envisageable. La suppression du mot de passe en tant que solution de repli transforme la situation en un changement permanent. C'est la différence entre une expérience temporaire et une nouvelle norme organisationnelle.

C'est également là que la distinction entre « sans mot de passe» et « clé d'accès » prend toute son importance opérationnelle : les employés peuvent se conformer aux exigences via une clé d'accès, un code QR ou la biométrie. Dès le départ, RSA s'est attaché à respecter l'exigence d'authentification sans mot de passe, mais sans dicter la méthode. Cela a permis de réduire les frictions et d'éviter l'impression d'un choix technologique imposé.

ÉTAPE 6 :
Accès sans mot de passe obligatoire pour tous les postes de travail (décembre 2025)

Les mots de passe sont désactivés pour l'authentification des postes de travail. La plupart des employés ayant déjà effectué la transition en novembre, cette échéance a permis de limiter les perturbations

Ce que RSA a appris : grâce à un groupe de test élargi, l'équipe de mise en œuvre avait déjà identifié et résolu certains problèmes. Le volume d'appels au service d'assistance a augmenté, mais restait gérable.

Une distinction importante qu'il convient de préciser : l'échéance portait sur **l'authentification sans mot de passe**, et non spécifiquement sur des clés d'accès. Les employés s'authentifiant par code QR, biométrie ou autres méthodes basées sur des clés d'accès FIDO étaient pleinement conformes. RSA souhaitait privilégier l'authentification FIDO autant que possible, mais à ce stade, une solution mixe sans mot de passe valait mieux que rien, et le risque d'hameçonnage était réduit dans ces cas d'utilisation spécifiques par rapport à l'authentification par mot de passe. L'objectif est de parvenir à une authentification sans mot de passe, les clés d'accès constituant une des voies possibles. Cette distinction est importante lors des échanges avec les clients : les entreprises confondent souvent les deux, et bien définir les attentes dès le départ permet d'éviter toute confusion lors du déploiement. Autre avantage : RSA proposait toutes ces options dans une seule et même application, ce qui permet d'utiliser la méthode la plus adaptée au bon moment, avec une expérience utilisateur quasi identique, et ainsi de ne pas complexifier le processus d'authentification.

ÉTAPE 7 :
Identifier les cas d'usage particuliers (décembre 2025 à aujourd'hui)

RSA continue d'identifier et de résoudre les cas particuliers qui nécessitent encore une authentification par mot de passe. Cela inclut les intégrations tierces nécessitant une reconfiguration; les systèmes existants ne prenant pas encore en charge le l'authentification FIDO; et les systèmes où l'authentification FIDO est impossible en raison d'exigences de conformité. RSA identifie également d'autres silos d'identité susceptibles de nécessiter une attention particulière.

Ce que RSA a appris : même avec une planification rigoureuse, les entreprises découvrent des exceptions en production. RSA résout ces problèmes grâce à des solutions alternatives, des plans d'action et des exceptions documentées, ce qui est tout à fait normal : d'autres organisations qui s'efforcent de mettre en place des politiques similaires sont également confrontées à la même situation.

Ce que RSA sait désormais — par l'expérience, et non par la théorie

Les résultats sont sans équivoque sur tous les paramètres mesurés par RSA. Le nombre de tickets d'assistance liés aux mots de passe a chuté une fois le déploiement entrée en vigueur - le pic de volume observé pendant la transition a été temporaire et gérable. RSA a atteint une adoption quasi totale de l'authentification sans mot de passe sur l'ensemble des ordinateurs gérés dans les douze mois suivant le lancement du déploiement. Ce délai inclut la phase initiale, initialement volontaire, et la campagne imposant l'authentification sans mot de passe, qui a permis de franchir un cap. La surface d'attaque par hameçonnage et par usurpation d'identité a été sensiblement réduite. Enfin, le déploiement lui-même, de la préparation de la plateforme à l'application complète de la nouvelle politique, a pu être réalisé en un seul exercice budgétaire, même en tenant compte du travail de transformation organisationnelle, rarement intégré dans les budgets des projets technologiques.

Ce qui a fonctionné : les recommandations de RSA pour un déploiement sans mot de passe en entreprise

RSA recommande les bonnes pratiques suivantes pour la mise en œuvre d'un système sans mot de passe à l'échelle de l'entreprise :

Meilleures pratiques technologiques

L'architecture de la plateforme est primordiale. Supprimez toutes dépendances aux mots de passe lors de l'enrôlement, de la récupération et des règles d'accès avant de déployer les authentificateurs. Sinon, l'authentification FIDO devient un complément et non un substitut, créant ainsi des failles dans la chaîne d'identité de l'organisation.

L'absence de mot de passe permet des améliorations de sécurité connexes. La vérification par le service d'assistance constituait une vulnérabilité de longue date. L'infrastructure a rendu possible la vérification bidirectionnelle en temps réel, éliminant ainsi les secrets partagés.

Les clés d'accès liées à l'appareil dans les applications mobiles offrent une troisième option. Au-delà des « clés d'accès synchronisées » et des « clés de sécurité physique », cette approche renforce le contrôle de l'entreprise, améliore l'expérience utilisateur et élimine les frais généraux liés à la distribution du matériel.

Meilleures pratiques de déploiement

Tirez parti des comportements existants des utilisateurs. RSA a progressé plus rapidement car les employés disposaient déjà de l'application mobile. Les organisations devraient identifier et prioritiser leurs points d'ancrage existants en matière d'authentification.

Procédez par ordre d'importance : alternatives ⟶ enjeux moindres ⟶ enjeux importants. Ne commencez pas par le système le plus utilisé. Privilégiez d'abord le confort.

Déployez à grande échelle, imposez ensuite. Laissez aux employés le temps de l'adopter à leur rythme. Identifiez les sources de confusion. Constituez un réseau de testeurs volontaires dans toute l'entreprise et des ambassadeurs.

Les campagnes et les échéances sont plus performantes que l'une ou l'autre prise individuellement. L'adoption volontaire atteindra un plateau, quelle que soit la qualité de l'expérience utilisateur. Pour cela, la preuve sociale est importante, mais l'urgence l'est tout autant. RSA a constaté une augmentation de l'utilisation de l'authentification sans mot de passe trois fois supérieure lorsqu'elle a combiné ces deux éléments avec une date limite claire.

Bonnes pratiques en matière de redondance

Prévoyez les imprévus tels qu'une défaillance de méthode ou la perte d'un appareil, car cela peut arriver. L'authentification sans mot de passe exige une redondance délibérée, tant au niveau des méthodes que des appareils. C'est pourquoi l'alliance FIDO recommande à chaque utilisateur d'enregistrer au moins deux clés d'accès si possible. Dans le cadre du déploiement RSA, certains groupes d'utilisateurs ont reçu à la fois une clé d'accès logicielle liée à l'appareil via l'application mobile RSA et une clé de sécurité matérielle, de sorte que la perte d'accès à l'une ou l'autre n'entraîne jamais une perte d'accès totale.

Meilleures pratiques de RSA en matière de changement organisationnel

Prévoyez suffisamment de temps pour impulser le changement de comportement. Le déploiement technologique prend quelques semaines. Changement des habitudes organisationnelles peut prendre des mois.

Fixez-vous des objectifs ambitieux, puis soyez transparent sur leur portée. L'équipe dirigeante de RSA a imposé un système 100 % sans mot de passe — et cet objectif ambitieux a permis à l'organisation d'aller bien plus loin qu'un objectif plus vague comme « améliorer l'authentification ». RSA a supprimé les mots de passe de tous les terminaux gérés et des principaux flux d'authentification. Des cas particuliers subsistent dans des systèmes existants; RSA les documente et élabore des plans pour les résoudre, plutôt que de prétendre à la perfection. Toute entreprise sera confrontée à cette réalité.

« Qu'est-ce qu'une clé d'accès? » est une question légitime. En dehors du service ingénierie, les employés avaient besoin d'une formation. RSA a développé des analogies claires et une documentation mise à jour pour relier la technologie aux modèles mentaux familiers.

Centralisez les méthodes d'authentification dans une seule application. Les employés pourront ainsi s'authentifier par clé d'accès, code QR ou la biométrie via la même application qu'ils utilisent déjà, la conformité ne nécessite aucun changement de comportement ; il suffit d'un clic différent. La capacité de RSA à proposer la bonne méthode au bon moment, sans changer d'application ni ajouter de frictions, a considérablement réduit les résistances lors du déploiement.

Ce que cela a prouvé à RSA (et à ses clients)

L'adoption d'un système sans mot de passe en interne a permis à RSA d'acquérir une expérience qu'elle ne pouvait pas obtenir via des projets pilotes chez les clients ou des tests en laboratoire : une expérience concrète liée à la complexité de la mise en œuvre d'un système sans mot de passe pour tous.

Expérience RSA :

- L'adhésion de la direction était essentielle pour démarrer.
- Intégration de la plateforme à l'infrastructure existante
- Complexité multiplateforme, scénarios hors ligne, appareils hétérogènes
- Amélioration continue des politiques en fonction des réalités du déploiement
- Gestion du changement s'étalant sur plusieurs mois, et non quelques semaines
- Volume d'appels au service d'assistance pendant la transition
- Écart entre adoption volontaire et obligation légale
- Cas particuliers que les organisations ne peuvent pas prévoir lors de la planification

Lorsque les clients demandent : « Combien de temps cela va-t-il vraiment prendre ? », « Qu'en est-il des employés qui résistent ? » ou « Que faisons-nous des systèmes existants ? », RSA répond en s'appuyant sur son expérience, et non sur la théorie.

RSA est passée de clés de sécurité matérielles, initialement utilisées à titre expérimental en R&D, à une approche sans mot de passe par défaut pour les environnements gérés. L'entreprise a validé sa plateforme en production dans des conditions réelles d'exploitation, notamment le processus d'intégration d'un an que la plupart des études résument en un seul paragraphe.

Cette authenticité, aucun environnement de démonstration ne peut la fournir.

Ce processus a façonné la manière dont RSA contribue à la communauté de l'Alliance FIDO. RSA continuera de travailler avec les autres membres. Élaborer des plans de déploiement, des guides d'implémentation et partager les enseignements tirés afin d'aider les entreprises à suivre le même parcours. Car plus les organisations réussissent avec les clés d'accès, plus la sécurité de toutes les organisations est renforcée.

Les normes techniques sont établies.
Il s'agit maintenant d'aider les entreprises à les déployer avec succès, ensemble.

