# L’authentification forte : un must pour tous les utilisateurs

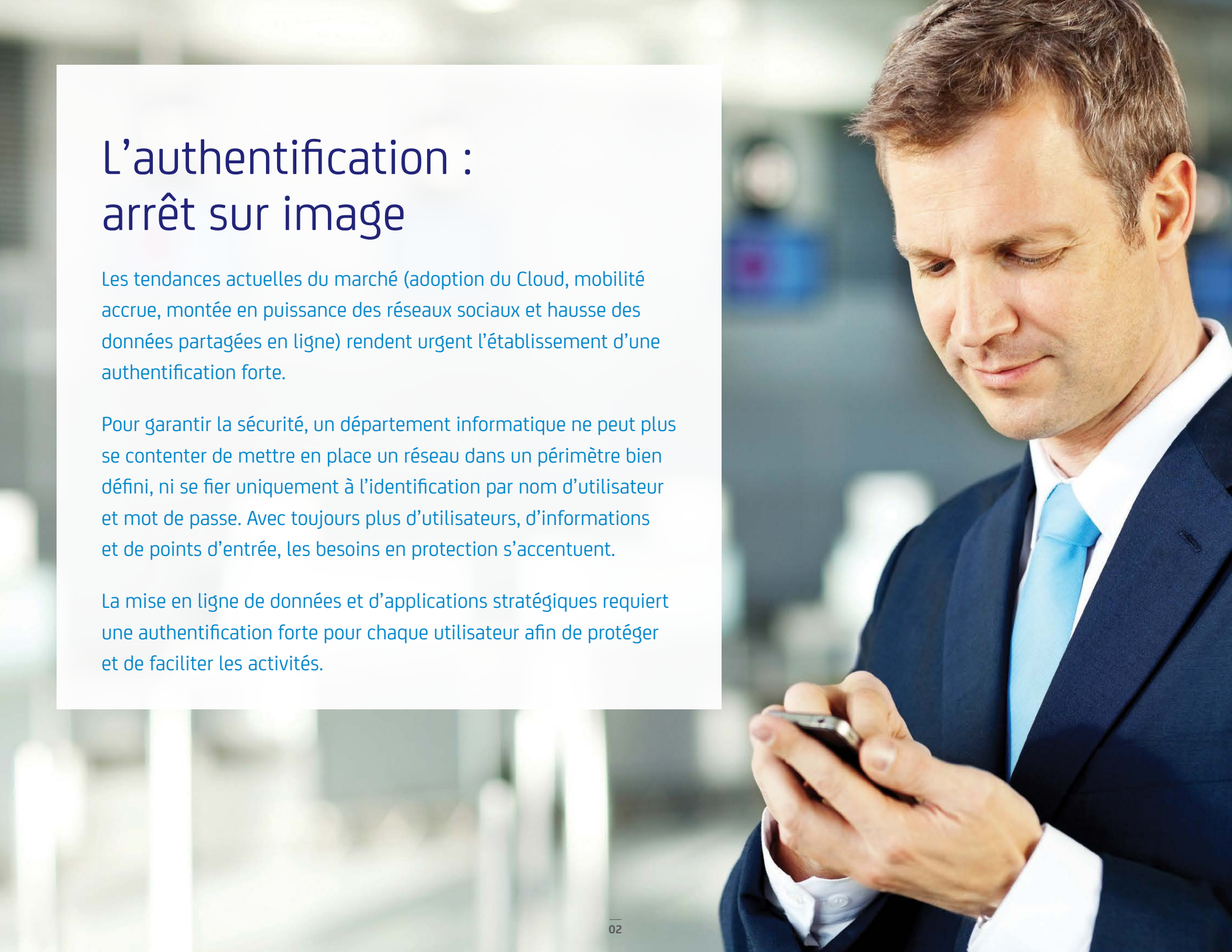
ca technologies

# L’authentification : arrêt sur image

Les tendances actuelles du marché (adoption du Cloud, mobilité accrue, montée en puissance des réseaux sociaux et hausse des données partagées en ligne) rendent urgent l’établissement d’une authentification forte.

Pour garantir la sécurité, un département informatique ne peut plus se contenter de mettre en place un réseau dans un périmètre bien défini, ni se fier uniquement à l’identification par nom d’utilisateur et mot de passe. Avec toujours plus d’utilisateurs, d’informations et de points d’entrée, les besoins en protection s’accentuent.

La mise en ligne de données et d’applications stratégiques requiert une authentification forte pour chaque utilisateur afin de protéger et de faciliter les activités.



« De nombreuses entreprises (près de 70 %) autorisent une certaine forme de BYOD pour les smartphones. Cette proportion va certainement augmenter pour atteindre plus de 80 % d'ici 2020. »

Gartner, « Tracking Changes in Enterprise Smartphone Preferences », Ken Dulaney, David A. Willis et Heather Keltz, 22 novembre 2013

# Évolution des tendances, évolution des menaces

Pour garantir une sécurité appropriée contre les risques à l'échelle de l'entreprise, ses responsables doivent comprendre l'importance d'une authentification forte dans le contexte des tendances technologiques majeures :

**Explosion du nombre et des types d'utilisateurs**

Dans la plupart des entreprises, la base des utilisateurs finaux a été étendue aux employés, aux sous-traitants, aux partenaires et aux clients ; le département IT doit donc prendre en compte l'éventail complet des situations d'utilisation, des scénarios d'accès et des privilèges.

**Réseaux sociaux**

L'utilisation des identifiants de connexion aux réseaux sociaux pour faciliter le processus d'inscription ou de connexion constitue une stratégie désormais répandue permettant d'augmenter la fidélisation des utilisateurs et de simplifier leur expérience. Cela dit, il est possible de compléter cette stratégie au moyen de méthodes conviviales d'authentification forte pour protéger les données et transactions plus sensibles.

**Mobilité**

Avec l'avènement des ordinateurs portables, des tablettes et des smartphones, les utilisateurs peuvent désormais accéder aux données à tout moment, où qu'ils se trouvent.

**Cloud**

L'utilisation croissante du Cloud et des services Web rend obsolète la notion même de « périmètre réseau ».

**Accroissement des menaces**

Les fraudes, le vol d'identités et les attaques ciblées sur différents secteurs d'activité sont de plus en plus fréquents et sophistiqués.

# Les nombreux défis de sécurité

Les entreprises doivent affronter de nombreux défis de sécurité, dont les suivants :

**Contrôler l'accès aux applications Web**

**Garantir la sécurité sur les appareils mobiles**

**Ne pas se laisser déborder par l'évolution des atteintes à la protection des données**

**Se conformer à la réglementation du secteur**

**Déployer une solution de sécurité évolutive tout en maîtrisant les coûts**


## L'ère du mot de passe est-elle révolue ?

« Même si votre mot de passe apparaît sous forme obscurcie et hachée, il reste vulnérable aux pirates qui parviennent à le convertir en texte brut. Ce risque est particulièrement élevé pour les mots de passe faibles, mais nous avons pu constater qu'il est possible de déchiffrer même des mots de passe relativement forts. Si des pirates parvenaient à décoder un mot de passe que vous utilisez sur plusieurs sites, ils pourraient accéder à votre messagerie, à vos relevés de compte et à vos profils de réseaux sociaux. »

– Jon Brodkin
« The secret to online safety: Lies, random characters, *and* a password manager »
*Ars Technica*, 3 juin 2013

# Le maillon faible

Il suffit de regarder les actualités pour constater que les attaques visant les données en ligne sont fréquentes. La combinaison « nom d'utilisateur/mot de passe » pose désormais problème, car elle représente le maillon faible de la stratégie de sécurité d'une entreprise. Ainsi, les experts du secteur constatent :

- des attaques par hameçonnage de plus en plus fréquentes et sophistiquées ;
- des vols et publications de mots de passe ininterrompus (plus de 100 millions de mots de passe ont été publiés en ligne sous forme de texte brut ou chiffré) ;
- une augmentation de la réutilisation des mots de passe.

Selon le groupe d'experts APWG (Anti-Phishing Working Group, groupe de travail contre l'hameçonnage), la durée de vie moyenne des attaques par hameçonnage a augmenté d'environ 70 % au premier semestre 2013[1], ce qui indique clairement que les pirates continuent à cibler les noms d'utilisateur et les mots de passe en raison de leur vulnérabilité.

S'il est vrai que rapidité et simplicité sont deux raisons valables qui expliquent pourquoi les entreprises restent attachées au système « nom d'utilisateur/mot de passe », un nombre croissant d'organisations s'intéressent aux nouvelles méthodes d'authentification pour renforcer leurs défenses.

## Que signifie l'expression « dommage collatéral » ?

À l'ère de la connectivité tous azimuts, il est indispensable de limiter les dégâts causés par le vol de noms d'utilisateur et de mots de passe. Un utilisateur Web lambda gère 25 comptes avec seulement 6,5 mots de passe pour les protéger.[3] Sans protocoles de sécurité adaptés, en cas de vol, ces mots de passe peuvent être utilisés pour compromettre des douzaines d'autres comptes.

En mai 2013, l'Allemagne est devenue le principal pays au monde pour l'hébergement de chevaux de Troie et de programmes de téléchargement basés sur l'hameçonnage, détrônant ainsi les États-Unis. C'était la première fois que l'Allemagne arrivait en tête de ce classement ; en juin 2013, les États-Unis sont revenus à la première place.[2]

En savoir plus >>

1 « Global Phishing Survey: Trends and Domain Name Use in 1H2013 », APWG, 16 septembre 2013
2 « Phishing Activity Trends Report: Q2 2013 », APWG, 5 novembre 2013
3 Ars Technica, « Why passwords have never been weaker—and crackers have never been stronger », 20 août 2012

# La sécurisation des identités : le nouveau périmètre

Les expressions du type « dans le réseau » ou « en dehors du réseau » sont de moins en moins pertinentes étant donné que le réseau est désormais partout. Aujourd'hui, assurer la protection des points faibles signifie axer la sécurité de l'entreprise sur les *identités*. Cette approche présente différents avantages :

- Le niveau d'authentification est déterminé et demandé en amont, même s'il est différent de celui que l'application exige.
- Les professionnels IT peuvent autoriser l'accès à des applications spécifiques et contrôler l'activité des utilisateurs sur l'ensemble de ces applications.
- Savoir quelles sont les informations d'authentification requises en fonction du niveau de risque aide à bloquer les activités suspectes.

La détection et le blocage des activités frauduleuses avant qu'elles ne se produisent, sans impact négatif sur les utilisateurs légitimes et les coûts d'exploitation, revêtent une importance capitale.

# Cinq clés pour une authentification forte réussie

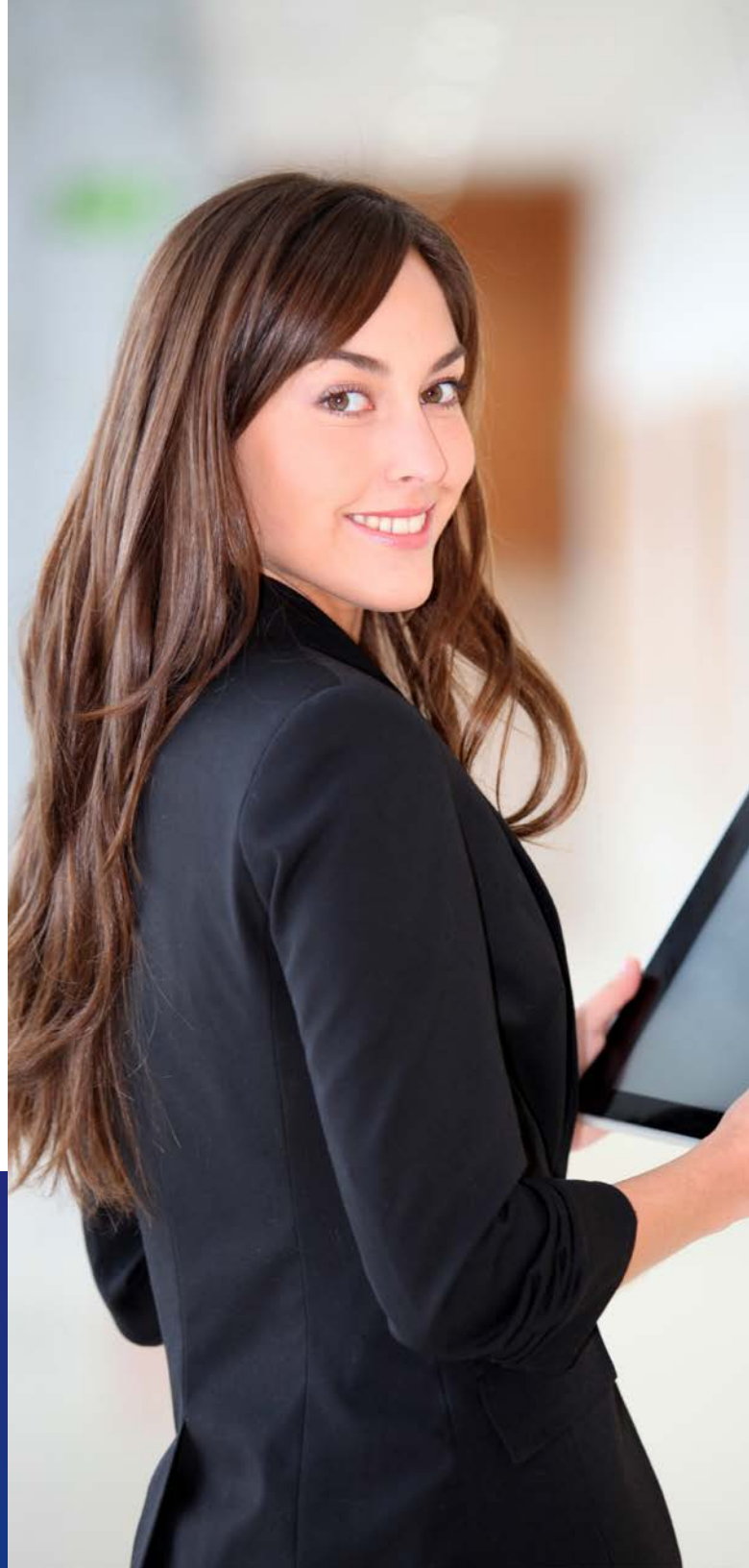
En plus d'accorder la priorité aux identités, une authentification forte doit être omniprésente, transparente et basée sur les risques. Pour répondre à ces critères, les organisations recherchent des méthodes d'authentification efficaces et économiques qui offrent aux utilisateurs une expérience conviviale.

Pour être sûres de leur méthode d'authentification, les organisations doivent :

1. **savoir qui sont les utilisateurs** (employés, sous-traitants, partenaires, clients), et comprendre les critères et niveaux d'accès de chaque groupe ;
2. **fournir le niveau adapté de sécurité par authentification** selon les risques inhérents à la situation ou à l'activité ;
3. **protéger les identités et les données sensibles dans des applications liées** sans alourdir inutilement l'expérience des utilisateurs ;
4. **garder à l'esprit** qu'il peut être nécessaire de protéger aussi bien les applications basées sur le Cloud que celles déployées sur site ;
5. **rechercher des moyens de protéger les transactions** contre les nouvelles menaces, par exemple les attaques par interception.

## Les départements IT doivent également être conscients des aspects suivants.

- **Il n'existe aucune approche universelle :** les départements informatiques doivent donc évaluer de façon approfondie les besoins en authentification, et développer des protocoles adaptés aux utilisateurs concernés ou à la situation spécifique de l'entreprise.
- **La quantité n'est pas toujours synonyme de qualité :** un processus d'authentification à plusieurs étapes peut certes renforcer la sécurité, mais également se révéler frustrant pour un utilisateur et avoir des conséquences négatives, comme la perte d'un client.

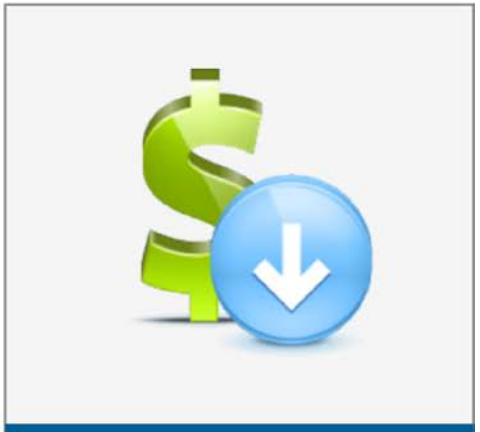


# L’authentification basée sur les risques : le juste équilibre

Les actions des entreprises visant à mettre en place une politique d’authentification entendent généralement réaliser trois objectifs :

**Sécurité adaptée aux risques**

**Expérience utilisateur simplifiée**



**Réduction des coûts d’admin./de support**

Associés correctement, ces trois paramètres peuvent aider les entreprises à verrouiller l’accès à leurs données sensibles tout en simplifiant l’expérience des utilisateurs qui pourront accéder à des informations et à des applications où qu’ils se trouvent.

# L’authentification basée sur les risques : sécurité et transparence

L’authentification basée sur les risques (également connue sous le nom d’authentification adaptative) intervient au niveau du serveur ; elle offre aux utilisateurs une expérience simplifiée tout en assurant la sécurité.

Cette pratique consiste à évaluer un grand nombre d’informations contextuelles, dont les suivantes :

- Identification des périphériques
- Géolocalisation
- Adresse IP
- Règles basées sur les périphériques

L’authentification basée sur les risques a, de bien des manières, évolué en même temps que le paysage informatique pour devenir plus disponible, flexible et puissante. Elle est également plus rentable que d’autres méthodes d’authentification forte, car elle renforce la sécurité avec un coût de déploiement moins élevé.

# Zoom sur l'authentification basée sur les risques

L'authentification basée sur les risques est, dans ses fondements mêmes, différente des autres formes d'authentification forte fondées sur les identifiants. Plus besoin de demander à l'utilisateur de fournir des informations pour vérifier son identité, car avec l'authentification basée sur les risques, ce sont de multiples informations contextuelles qui permettent d'effectuer cette vérification :

## Où l'utilisateur se trouve-t-il ?

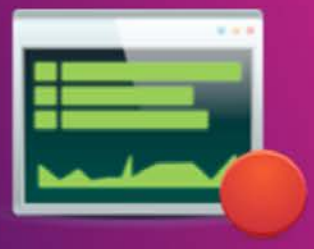
Le lieu d'accès est un facteur essentiel dans l'évaluation de l'identité. Les méthodes basées sur les risques utilisent les adresses IP pour vérifier si l'utilisateur accède aux données depuis un lieu suspect ou si le périphérique employé ne correspond pas avec le type de connexion utilisé pour l'accès.

## Quel est le système ou périphérique utilisé ?

L'authentification basée sur les risques permet également de reconnaître le type du périphérique employé. Si l'utilisateur tente un accès sur un appareil non reconnu ou jamais utilisé auparavant, le système évalue le risque potentiel.

## Que tente l'utilisateur ?

L'authentification basée sur les risques permet également d'évaluer chaque demande particulière. Un département informatique peut ainsi définir des règles associées à différentes actions des utilisateurs (par exemple, l'accès à une base de données spécifique) pour renforcer la protection des données sensibles. Si la demande d'un utilisateur semble inhabituelle ou déclenche une règle spécifique, le système peut refuser l'accès et marquer cette interaction pour l'examiner de façon plus approfondie.



## Le comportement est-il cohérent ?

Les activités des utilisateurs sont un autre facteur clé. Tout comportement incompréhensible de la part d'un utilisateur (connexions très fréquentes, tentatives d'accès à de grandes quantités de données, etc.) déterminera la manière dont le système d'authentification traitera la demande.

## Authentification hors bande à deux facteurs

Dans les cas où une authentification renforcée est requise en raison d'un risque accru (par exemple, des tentatives d'accès sur un ordinateur non reconnu), il est possible d'envoyer hors bande un mot de passe à usage unique sur le téléphone de l'utilisateur (via SMS, courriel ou message vocal) pour vérifier son identité et réduire le risque de fraude.

# L'authentification basée sur les risques : résumé de ses avantages

Dans la plupart des cas, les solutions d'authentification basée sur les risques permettent de réaliser le juste équilibre entre sécurité, expérience utilisateur et coût.

### Convivialité

L'authentification basée sur les risques s'exécute en arrière-plan, ce qui signifie que les utilisateurs n'ont pas besoin de passer par des étapes supplémentaires pour s'identifier.

### Simplicité de déploiement

Les solutions d'authentification basée sur les risques s'exécutant côté serveur, elles sont faciles à déployer et ne nécessitent l'installation d'aucun client sur un téléphone portable, une tablette ou un ordinateur.

### Souplesse

Ces solutions peuvent être adaptées aux besoins immédiats de l'entreprise et à son niveau de tolérance aux risques. Elles sont aussi facilement ajustables en fonction de l'évolution des menaces cybernétiques.

### Support multicanal

Les méthodes d'authentification basée sur les risques sont personnalisables pour différents canaux d'interaction, par exemple les équipements mobiles ou le Web.

### Modélisation des règles et du comportement

Grâce à l'authentification basée sur les risques, un département informatique peut mettre en œuvre des règles destinées à répondre à différents profils et comportements utilisateur.

### Compatibilité multipériphérique

Ces solutions permettent de protéger les demandes d'accès et les transactions provenant d'équipements et de systèmes d'exploitation variés, notamment les tablettes, les téléphones portables et les PC.

### Rentabilité

La plupart des méthodes d'authentification basée sur les risques sont moins onéreuses que les méthodes classiques basées sur les jetons matériels.

# L’authentification basée sur les risques : évaluation des risques

La mise en œuvre du niveau d’authentification adapté exige d’évaluer soigneusement les risques inhérents aux utilisateurs et à leurs activités dans leur globalité.
Les organisations doivent donc s’efforcer de répondre aux questions suivantes :

- À quel groupe l’utilisateur appartient-il ?
- Où se trouve l’utilisateur lorsqu’il accède à des informations/applications ?
- De quels périphériques l’utilisateur va-t-il se servir ?
- Quels types de données sont concernés ?
- Quels types d’activités/transactions sont possibles ?

# Les solutions d'authentification forte de CA Technologies

Flexible et évolutive, la solution CA Advanced Authentication incorpore à la fois des méthodes d'authentification basée sur les risques, telles que l'identification du périphérique, la géolocalisation et la détection de l'activité de l'utilisateur, et un grand nombre de données permettant une authentification multifacteur forte.

Grâce à cette solution, qui inclut CA AuthMinder™ et CA RiskMinder™, les organisations peuvent créer le processus d'authentification adapté à chaque application ou transaction. Disponible sous forme de logiciel à déployer sur site ou en tant que service Cloud, elle permet de protéger l'accès aux applications depuis une multitude de points d'extrémité, notamment tous les appareils mobiles les plus courants. Grâce à cette solution, les organisations peuvent appliquer de manière rentable la méthode appropriée d'authentification forte sur différents environnements, sans alourdir l'expérience des utilisateurs finaux.

Pour plus d'informations sur les solutions d'authentification forte de CA Technologies, rendez-vous sur le site http://www.ca.com/fr/multifactor-authentication.aspx.



CA Technologies (NASDAQ : CA) est un éditeur de logiciels et de solutions intégrées de gestion des systèmes d'information, dont l'expertise couvre tous les environnements informatiques, du mainframe au Cloud Computing et des systèmes distribués aux infrastructures virtuelles. CA Technologies gère et sécurise les environnements informatiques et permet à ses clients de fournir des services informatiques plus flexibles. Grâce aux produits et aux services innovants de CA Technologies, les organisations informatiques disposent de la connaissance et des contrôles nécessaires pour renforcer l'agilité métier. La majorité des sociétés du classement « Fortune 500 » s'appuient sur CA Technologies pour gérer leurs écosystèmes IT en constante évolution.

ca technologies