LeMagIT
L'informatique pour et par les pros
TechTarget
E-handbook
Contenu PRO+

L'IAM en pleine transformation à l'heure du cloud et de la mobilité

Dans ce guide

Introduction.

La gestion des identités et le contrôle des accès n'a jamais été un sujet mineur. Mais sous l'effet d'ouvertures et d'interconnexions croissantes, les deux sujets ont considérablement gagné en importance et en complexité au fil du temps. L'adoption des infrastructures et applications en mode cloud, ainsi que celle de la mobilité, n'ont fait qu'amplifier le phénomène.

Jusqu'à faire émerger des questions sur des sujets longtemps considérés comme des acquis tels que les mots de passe ou encore l'authentification à facteurs multiples, la mobilité apportant là son lot de défis autant que de promesses.

Face à ces changements, le domaine autrefois vu comme largement monolithique de l'IAM (*Identity and Access Management*) s'oriente durablement vers une dissociation nette entre gestion des identités et de leur cycle de vie, d'une part, et contrôle des accès et de l'authentification, de l'autre.

Dans ce guide

Car les deux domaines évoluent, le second, notamment, jouant la carte de l'intelligence pour trouver dynamiquement le meilleur compromis entre confort de l'utilisateur – et sa productivité – et sécurité des ressources, en fonction de leur criticité et du contexte des requêtes. Jusqu'à laisser entrevoir la possibilité de processus d'authentification largement transparents.

Dans ce guide

Les pour et les contre de la fédération d'identité

Robert Sheldon, journaliste et consultant

La fédération d'identité est une technologie relativement nouvelle dans le monde de la mobilité, et elle ne manque pas de s'accompagner de défis. Voici quelques points clés pour simplifier les déploiements.

A mesure que la gestion de l'identité est étendue à de nouveaux domaines, il convient de penser à mettre en place la fédération. Mais il faut être bien conscient des difficultés.

Il fut un temps où la gestion des identités se limitait au contrôle d'accès aux ressources au sein d'un seul domaine de sécurité. Mais les utilisateurs internes accèdent désormais à des ressources externes et des utilisateurs externes accèdent à des ressources internes. Les approches traditionnelles de la gestion d'identité montrent leurs limites.

Dans ce contexte, de nombreuses organisations se tournent vers la fédération d'identité pour faciliter le travail des utilisateurs sur plusieurs systèmes, tout en réduisant la charge administrative liée à la gestion de l'accès à ces systèmes.

Dans ce guide

Introduction à la fédération d'identité

La fédération d'identités lie l'identité d'un utilisateur à travers plusieurs domaines de sécurité, chacun doté de son propre système de gestion des identités. Lorsque deux domaines sont fédérés, l'utilisateur peut s'authentifier sur un domaine, puis accéder aux ressources de l'autre domaine sans avoir à s'authentifier une seconde fois.

Par exemple, un groupe d'organisations qui travaillent ensemble sur un projet pourrait vouloir former une fédération d'identité afin que les utilisateurs de chaque organisation puissent plus facilement accéder et partager les ressources entre les membres participants. Avec la fédération d'identité, les utilisateurs n'ont besoin d'être authentifiés qu'une seule fois pour accéder aux ressources de tous les domaines, tandis que les administrateurs peuvent toujours contrôler les droits d'accès dans leurs domaines respectifs.

Une composante importante de la fédération d'identité est le Single Sign-on (SSO), un mécanisme qui permet aux utilisateurs de ne s'authentifier qu'une fois pour accéder à plusieurs systèmes ou applications. La fédération d'identité et le SSO sont parfois, et par erreur, appréhendés comme un seul et même système. La fédération d'identité s'appuie fortement sur les technologies SSO pour authentifier les utilisateurs à travers les divers domaines couverts.

Dans ce guide

La fédération d'identité viser à lever les obstacles qui empêchent les utilisateurs d'accéder facilement aux ressources dont ils ont besoin quand ils en ont besoin. Sans sacrifier pour autant la sécurité des ressources.

Le rôle de la gestion des fédérations d'identité

La fédération d'identité permet ainsi aux administrateurs de résoudre de nombreux problèmes liés l'accès à des ressources distribuées sur plusieurs domaines. Par exemple, il n'est pas nécessaire de mettre en place un système spécialisé pour faciliter l'accès aux ressources externes à l'organisation.

La fédération d'identité peut également bénéficier aux applications qui ont besoin d'accéder à des ressources réparties dans plusieurs domaines de sécurité.

Pour profiter de ces bénéfices, il est nécessaire de mettre en œuvre une gestion complète de la fédération d'identité. Ce terme générique recouvre le processus d'administration de tous les éléments associés à une plateforme complète de fédération d'identité. Cela comprend non seulement les technologies qui rendent la fédération possible, mais aussi les accords, politiques, normes et autres éléments qui définissent la façon dont le service est mis en œuvre.

Dans ce guide

Pour que la fédération fonctionne, toutes les parties impliquées doivent s'entendre sur ces éléments. Elles doivent ainsi s'accorder sur les attributs d'identification à inclure, comme le courriel, le nom et l'intitulé de fonction, sur la manière de représenter ces attributs en interne, et sur la norme à utiliser pour échanger des données d'authentification et d'autorisation. En la matière, la norme Security Assertion Markup Language (SAML) est couramment utilisée.

Parvenir à un accord sur tous ces éléments peut être la partie la plus difficile de la mise en œuvre d'une fédération d'identité, à moins de souscrire à une plateforme de fédération existante, comme celles établies par des entreprises comme Microsoft et Facebook.

Les organisations qui se regroupent pour créer leur propre fédération ont plus de difficultés parce que tous les participants doivent s'entendre sur toutes les composantes. Et les systèmes locaux de gestion d'identité, les lois et règlements régionaux applicables aux organisations impliquées peuvent ajouter une complexité non négligeable au processus. En outre, l'une des organisations devra servir d'autorité centrale, ce qui n'est pas une légère responsabilité.

La gestion de la fédération d'identité peut également s'appliquer à une seule organisation qui gère plusieurs domaines de sécurité. Il s'agit d'une technologie relativement jeune, et sa signification exacte est encore en évolution, de sorte que les particularités peuvent varier d'une source à l'autre.

Dans ce guide

Comment déployer une fédération d'identité

Malgré les défis que pose la gestion de la fédération d'identité, de nombreuses organisations estiment ses promesses méritent les efforts. Mais avant de se lancer, il convient d'avoir un aperçu clair et concis des objectifs du projet afin que toutes les personnes concernées comprennent exactement ce qu'elles essaient d'accomplir.

Les participants doivent aussi en apprendre le plus possible sur leurs pairs au sein de la fédération et ce qu'ils doivent en attendre. Si une organisation rejoint une fédération existante, son équipe informatique doit comprendre les règles qu'elle accepte, les normes auxquelles elle doit se conformer et les informations qu'elle doit partager.

Une fois que les informations nécessaires ont été rassemblées, il est possible de commencer le processus de planification. À moins que les participants ne se joignent à une fédération existante, ils doivent parvenir à un consensus sur la mise en œuvre de la fédération d'identité, en matière de logiciels et de matériel, de politiques de configuration, de types d'attributs et de normes, mais aussi de règles d'adhésion et de résiliation, et d'innombrables autres considérations.

A charge ensuite, pour chaque équipe informatique concernée, de planifier son propre déploiement en tenant compte des standards et des accords de la fédération.

Dans ce guide

L'aspect le plus important du processus de planification est d'aborder correctement toutes les questions liées à la sécurité. Les participants doivent établir des normes minimales de sécurité sur lesquelles tous peuvent s'entendre. Et cela recouvre notamment l'audit et la collecte de données de journalisation, dans le respect de la vie privée, ainsi que la sécurisation de ces données.

Bien sûr, tout au long de ce processus, il convient de tenir compte des besoins des utilisateurs finaux. La fédération d'identité devrait améliorer leur expérience, pas alourdir leurs activités professionnelles au quotidien.

Il faut pour cela fournir aux utilisateurs des instructions claires sur la façon de configurer leurs comptes, ainsi que des détails sur la confidentialité et l'utilisation de leurs identifiants. Les messages d'erreur, d'avertissement et d'information doivent en outre être concis et utiles.

Enfin, si authentification fédérée et locale doivent coexister, les options doivent être claires et les procédures doivent être intuitives et faciles à comprendre.

Dans ce guide

Les outils de gestion des identités et des accès jouent la carte de l'intelligence

Erica Mixon, journaliste

Le fonctionnement en mode service et l'intelligence artificielle permettent de réduire la charge administrative. Mais l'adoption n'en est qu'à ses débuts et beaucoup s'interrogent sur ce que l'avenir réserve à l'IAM.

Les outils de gestion des identités et des accès deviennent de plus en plus automatisés. L'administration s'en trouve simplifiée et allégée, mais il n'est pas encore possible de laisser les outils fonctionner en roue libre.

La mobilité est à l'origine de nombreuses innovations dans le domaine de la gestion des identités et des accès (IAM), au cours des deux dernières années. Aujourd'hui, des technologies telles que l'apprentissage automatique, les microservices et le cloud font leur entrée dans les outils d'IAM, afin de les rendre plus transparents, accessibles et automatisés pour les utilisateurs finaux et les administrateurs.

Dans ce guide

Exécuté en mode cloud

Face De fait, la gestion d'identités en mode service est de plus en plus répandue. Mary Ruddy, vice-présidente de la recherche chez Gartner, souligne sans surprise l'élasticité de cette approche.

L'éditeur ThoughtWorks est passé d'un produit open source sur site à l'offre cloud d'Okta en 2013 pour gérer l'identité et les accès de ses employés. Depuis, Phil Ibarrola, directeur technique de ToughtWorks, souligne à quel point ce choix a permis de réduire la charge liée aux activités d'IAM : « de temps en temps, un utilisateur oublie son mot de passe ou son système d'authentification à facteurs multiples ne fonctionne plus correctement, et il faut procéder à des réinitialisations. Mais ces incidents sont rares ».

Phil Ibarrola ne regrette donc pas de perdre une certaine granularité dans la gestion des identités au profit d'un rôle plus informel : « au moment de faire cette transition pour le cloud, il y avait une certaine anxiété à l'idée d'abandonner le contrôle de certaines choses dans notre infrastructure. Mais avec le temps, on réalise que cela fait partie du transfert de risque et du fait de placer sa confiance dans un fournisseur de services ».

Néanmoins, tous les outils de gestion des identités et des accès n'ont pas besoin de passer au cloud. Produactivity, un éditeur guatémaltèque qui propose une application permettant aux entreprises de suivre l'utilisation des terminaux

Dans ce guide

mobiles de leurs collaborateurs, utilise les outils d'IAM en mode cloud (ou IDaaS) d'Auth0. Mais son directeur technique, Mercedes Wyss conserve un certain niveau de contrôle sur les données – qui incluent des informations personnelles et géolocalisées – en les stockant dans sa propre base de données, en local, plutôt que dans celle d'Auth0.

Sur la voie de l'intelligence

Les menaces de sécurité étant toujours plus complexes, les fournisseurs doivent rendre leurs outils d'IAM plus intelligents et plus sophistiqués. Grâce à des analyses avancées qui s'appuient sur l'apprentissage automatique, ces outils peuvent surveiller le comportement des utilisateurs pour établir des prédictions et mieux détecter des anomalies. Pour Mary Ruddy, cette tendance n'est encore qu'émergente et les organisations n'en sont qu'aux premiers stades de l'adoption.

Microsoft propose ainsi Azure Active Directory (AD) Identity Protection, qui utilise l'apprentissage automatique pour détecter les comportements suspects des utilisateurs. Les administrateurs n'ont pas besoin de savoir comment mettre en œuvre des techniques d'apprentissage automatique pour bénéficier de la protection de l'identité et ils peuvent signaler à Microsoft tout faux positif que le système détecte pour participer à l'amélioration des algorithmes et des modèles qu'ils génèrent.

Dans ce guide

D'autres produits, comme Oracle Adaptive Access Manager et RSA Adaptive Authentication, permettent de modifier ces modèles – une souplesse qui plaît généralement aux grandes entreprises qui subissent déjà des cyberattaques spécifiques. Les administrateurs expérimentés peuvent ainsi ajuster les modèles établis par apprentissage automatique pour réduire les taux de faux positifs et obtenir un niveau de contrôle plus granulaire.

Les outils d'IAM peuvent également recourir à l'analytique pour déterminer avec plus de précision quand il est pertinent de demander des facteurs d'authentification supplémentaires afin d'éviter d'alourdir continuellement l'expérience utilisateur. Par exemple, le système d'IAM peut évaluer des attributs tels que l'emplacement de l'utilisateur, l'empreinte numérique de l'appareil et l'adresse IP pour accorder automatiquement l'accès si la combinaison est considérée comme à faible risque. Une compagnie d'assurance qui a déployé cette fonctionnalité a réduit de 90 % l'utilisation de l'authentification à facteurs multiples et des mots de passe par ses employés, indique ainsi Mary Ruddy.

Car tout à la fois, la mobilité complique et simplifie l'authentification à facteurs multiples. Les terminaux mobiles peuvent être utilisés comme support de vérification dans l'authentification à facteurs multiples, par jeton, authentification implicite, etc.

L'application mobile Produactivity permet aux managers de suivre l'activité de leurs collaborateurs sur les terminaux mobiles, et il n'est pas systématiquement

Dans ce guide

nécessaire de saisir un mot de passe pour accéder à l'application : une fois qu'Auth0 reconnaît que l'utilisateur se sert d'un terminal propriété de l'entreprise, un simple lien envoyé par e-mail permet de finaliser le processus d'ouverture de session, une fois pour toutes.

Dans ce guide

Avantages et inconvénients d'une application mobile d'authentification à facteurs multiples

Valéry Marchive, journaliste

L'authentification à facteurs multiples peut améliorer la sécurité d'une application en arrêtant de se reposer sur un simple mot de passe. Reste à savoir si c'est justifié, et quels sont les avantages et les travers de l'approche.

L'authentification à facteurs multiples (MFA) est essentielle pour toute application d'entreprise qui stocke, traite ou permet d'accéder à des données sensibles ou à des informations personnellement identifiables. Mais son adoption présente des défis qui vont bien au-delà de ceux qui accompagnent une approche nom d'utilisateur/mot de passe.

Une application mobile d'authentification à facteurs multiples exige que les utilisateurs fournissent plusieurs identifiants indépendants pour utiliser l'application ou accéder à ses données. Il s'agit de rendre plus difficile l'accès à des informations sensibles pour les personnes non autorisées.

Dans ce guide

De quoi s'agit-il exactement ?

Les informations d'identification acceptables pour une application d'authentification à facteurs multiples sont généralement divisées en quatre catégories : ce que l'utilisateur sait, ce qu'il possède, ce qu'il présente, ou ce qu'il fait.

La première catégorie renvoie à des éléments mémorisés, comme des mots de passe, des codes PIN, ou des réponses à des questions secrètes. Dans la seconde catégorie, on peut trouver les cartes d'identité, les porte-clés, les jetons de mot de passe à usage unique ou le terminal mobile lui-même. La troisième catégorie fait référence à des caractéristiques spécifiques à l'individu susceptibles d'être contrôlés par un dispositif dédié, comme les empreintes digitales, la rétine ou la morphologie faciale, notamment. La dernière, plus récent, touche à la biométrie comportementale, aussi appelée authentification continue ou implicite.

L'authentification à double facteur (2FA) est généralement appréhendée comme un type de MFA, bien que les deux soient parfois considérées comme des approches différentes. Quoi qu'il en soit, une stratégie d'authentification à facteurs multiples efficace devrait recouvrir plusieurs des catégories mentionnées plus haut. Par exemple, une application qui requiert un haut degré de sécurité peut nécessiter un mot de passe et un jeton de sécurité, en plus d'un smartphone enregistré.

Dans ce guide

Parce qu'une application mobile d'authentification à facteurs multiples permet d'aller au-delà d'un mot de passe seul, que des pirates peuvent assez facilement compromettre, elle permet de gagner en sécurité. Même un mot de passe stocké de manière chiffrée peut être vulnérable aux attaques en force brute.

Chaque facteur ajouté au processus d'authentification se traduit par un niveau de protection supplémentaire. Si un facteur est compromis, les autres sont toujours en place pour protéger les données sensibles. L'activation d'une application mobile d'authentification à facteurs multiples peut en outre aider à résoudre des problèmes de conformité réglementaire.

Les défis de l'authentification à facteurs multiples

Chaque facteur d'authentification additionnel est susceptible d'impliquer un effort supplémentaire de la part de l'utilisateur final. Il peut être déjà assez difficile de se rappeler et de gérer les mots de passe, mais l'ajout de tâches telles que la gestion des applications d'authentification peut affecter la productivité et entraîner de la frustration, en particulier lorsque les utilisateurs se heurtent à des difficultés ou doivent répéter plusieurs étapes chaque fois qu'ils accèdent à leurs applications.

Dans ce guide

Et ce n'est pas une mince tâche que d'intégrer l'authentification à facteurs multiples à une application, du côté des développeurs, et notamment pour les applications patrimoniales.

Malgré tout, une organisation qui prend la sécurité au sérieux n'a pas d'autre choix que de prendre cette direction. Pour l'instant, c'est la pratique de référence acceptée pour l'authentification des utilisateurs et la protection des données sensibles.

Dans ce guide

Tous les systèmes d'authentification à facteurs multiples ne se valent pas

Valéry Marchive, journaliste

L'utilisation des SMS pour véhiculer un code à usage unique est officiellement déconseillée depuis deux ans. Mais leur transfert par applications dédiées ne protège pas forcément non plus contre le phishing.

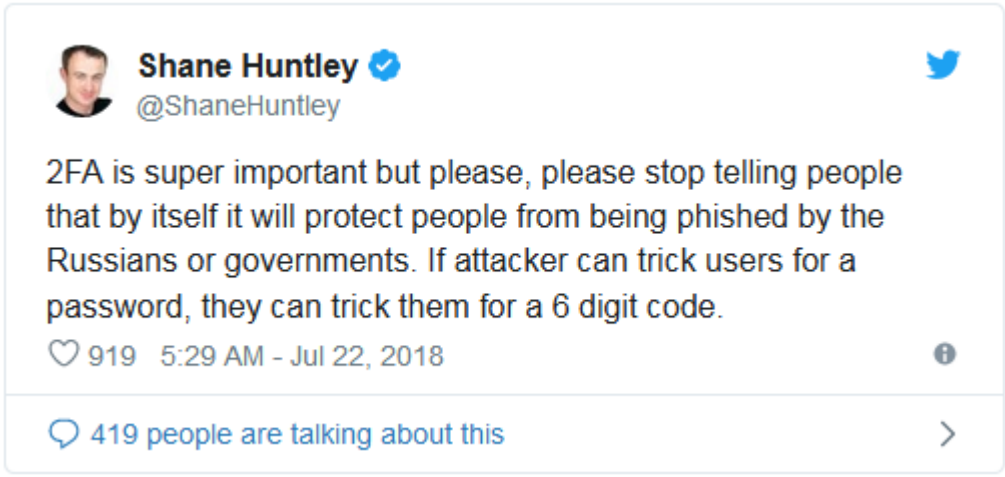
C'était au mois de septembre dernier : nos confrères du *Guardian* révélaient que Deloitte avait été victime d'une attaque informatique partie d'un compte administrateur du serveur de messagerie du cabinet, protégé par un simple mot de passe, sans authentification à facteurs multiples. Le cas est loin d'être isolé : fréquemment, l'utilisation de facteurs d'authentification supplémentaires, au-delà du mot de passe même le plus robuste, est recommandée comme un élément de sécurisation nécessaire, voire indispensable. Mais ce n'est pas une panacée.

Le SMS est déconseillé depuis l'été 2016 par le Nist américain pour véhiculer des codes à usage unique utilisés comme second facteur d'authentification, en raison des faiblesses connues du système de signalisation SS7, mais

Dans ce guide

également du risque de détournement de cartes SIM – une situation déjà rencontrée par Cloudflare en juin 2012.

Face à cela, de plus en plus de services proposent des alternatives basées sur des applications mobiles, telles qu'Authy, notamment. Mais là encore, la solution n'est pas parfaite. Et c'est ce que vient de rappeler Shane Huntley, directeur de la division analyse des menaces de Google.



Dans ce guide

Sur Twitter, il souligne que l'authentification à double facteur (ou 2FA, pour *2 Factors Authentication*) peut protéger contre des attaques touchant au vol de mots de passe, notamment lorsqu'ils ont été réutilisés. « Mais n'importe quel système 2FA qui implique la saisie d'un code par l'utilisateur peut être *phishé* ». Et de détailler le processus : « l'utilisateur saisit son mot de passe sur le site des attaquants ; les attaquants tentent de s'authentifier et le code SMS est envoyé à l'utilisateur ; l'attaquant voit que le code est nécessaire et affiche une page demandant le code à l'utilisateur ; l'utilisateur saisit le code ; l'attaquant a gagné ».

Fin 2016, le spécialiste du paiement en ligne Stripe avait lancé une campagne de hameçonnage interne, en utilisant les codes graphiques d'AWS. La page Web frauduleuse était là particulièrement élaborée, allant jusqu'à demander un second facteur d'authentification. Malgré une campagne de formation organisée trois mois plus tôt, le taux de conversion a atteint plus de 25 %, depuis l'ouverture de l'e-mail de phishing jusqu'à la saisie d'identifiants complets permettant de détourner effectivement les comptes d'utilisateurs.

Dès lors, Shane Huntley recommande vivement l'utilisation d'appareils physiques comme second facteur d'authentification, à commencer par les clés USB au standard U2F, porté par l'alliance Fido (pour *Fast Identity Online*), comme celles de Yubico. Mais il existe également des appareils Bluetooth Low Energy certifiés, ainsi que des cartes sans contact, comme Gemalto, Infineon ou encore Safran en proposent. Certains terminaux mobiles peuvent également

Dans ce guide

faire office aussi de jeton – Nok Nok Labs produit ainsi un client logiciel pour iOS qui tire profit de l'enclave sécurisée et de TouchID. Les navigateurs Chrome, Firefox et Opera supportent nativement U2F. Des projets indépendants visent à son support pour Safari, sous macOS et iOS.

Dans ce guide

Ce qui différencie la gouvernance des identités de la gestion des accès

Matthew Pascucci, security architect

De nombreux acteurs sont présents sur les deux domaines et l'ensemble a longtemps été appréhendé au travers de la notion générique d'IAM. Mais les différences sont marquées et appellent à une dissociation des concepts.

La gouvernance des identités (IGA) et la gestion des accès (AM) servent un même objectif : garantir qu'un utilisateur peut accéder à des ressources du système d'information – systèmes, applications, données – avec des droits appropriés à sa fonction dans l'entreprise et ses besoins métiers, sans plus ni moins. Mais IGA et AM s'avèrent complémentaires et apportent chacun une partie de la réponse au problème : le premier recouvre l'établissement des droits, tandis que le second s'applique à en assurer le respect.

Ainsi, les systèmes de gouvernance des identités doivent tout d'abord permettre de gérer le cycle de vie de ces identités numériques, depuis leur création jusqu'à leur suppression – ou leur archivage à des fins de traçabilité. Par exemple, un système d'IGA doit permettre de fermer rapidement et aisément tous les accès d'un utilisateur au moment où il quitte l'organisation.

Dans ce guide

Vient ensuite la gestion des droits, établis sur la base d'un éventail de rôles, de groupes, déterminés eux-mêmes en lien étroit avec les métiers. L'adhérence est là particulièrement forte avec les processus et l'organisation interne de l'entreprise puisqu'il s'agit de produire un référentiel permettant de traduire en termes techniques des autorisations qui relèvent de l'organisationnel. Et des politiques peuvent également venir définir des ajustements contextualisés des droits en fonction des circonstances entourant les tentatives d'accès, du comportement connu du demandeur, et de la criticité de la ressource.

Qu'il s'agisse de la création d'une nouvelle identité à l'occasion d'un recrutement, par exemple, ou de l'octroi temporaire de droits exceptionnels, ou d'une délégation pour un remplacement, le système doit pouvoir supporter la gestion de nombreuses situations d'exception. Pour cela, un outil de gestion de workflows doit permettre de soumettre des requêtes, d'un côté, et de les accepter ou rejeter, de l'autre.

Surtout, un système d'IGA vise à industrialiser le contrôle de l'adéquation des droits accordés aux utilisateurs avec leurs missions dans l'entreprise, dans le cadre des processus de revue de droits internes. De quoi valider en continu la conformité de ceux-ci avec les politiques de l'entreprise ou encore ses impératifs réglementaires, mais également répondre à des demandes d'audit, interne comme externes.

Les systèmes de gestion des accès sont quant à eux là pour contrôler l'accès aux ressources du système d'information, en lien avec les droits gérés dans le

Dans ce guide

système d'IGA. Il s'agit donc tout d'abord d'offrir une couche globale d'authentification – aussi consolidée (SSO) que possible en fonction des capacités d'intégration offertes par les différentes ressources du système d'information visées –, et de gestion des sessions.

A cela peuvent s'ajouter des fonctions de base de gestion de l'identité, comme l'enrôlement et la gestion de mot de passe en self-service, ou encore l'ajustement adaptatif des conditions d'authentification en fonction du contexte de la requête.

Le contrôle d'accès et la gouvernance des identités ne s'appliquent pas uniquement aux collaborateurs des entreprises, ou à leurs partenaires. Ils peuvent également être utilisés pour leur clients consommateurs, ou pour des entités sans la moindre composante humaine, comme des ressources du SI (ou de celui d'une organisation tierce) nécessitant un accès à d'autres ressources du système d'information.

Dans ce guide

Accéder à plus de contenu exclusif PRO+

Vous avez accès à cet e-Handbook en tant que membre via notre offre PRO+ : une collection de publications gratuites et offres spéciales rassemblées pour vous par nos partenaires et sur tout notre réseau de sites internet.

L'offre PRO+ est gratuite et réservée aux membres du réseau de sites internet TechTarget.

Profitez de tous les avantages liés à votre abonnement sur: http://www.lemagit.fr/eproducts

Images; Fotolia

©2018 TechTarget. Tout ou partie de cette publication ne peut être transmise ou reproduite dans quelque forme ou de quelque manière que ce soit sans autorisation écrite de la part de l'éditeur.

Dans ce guide

Le document consulté provient du site www.lemagit.fr

Cyrille Chausson | *Rédacteur en Chef*
TechTarget
22 rue Léon Jouhaux, 75010 Paris
www.techtarget.com

©2018 TechTarget Inc. Aucun des contenus ne peut être transmis ou reproduit quelle que soit la forme sans l'autorisation écrite de l'éditeur. Les réimpressions de TechTarget sont disponibles à travers The YGS Group.

TechTarget édite des publications pour les professionnels de l'IT. Plus de 100 sites qui proposent un accès rapide à un stock important d'informations, de conseils, d'analyses concernant les technologies, les produits et les process déterminants dans vos fonctions. Nos événements réels et nos séminaires virtuels vous donnent accès à des commentaires et recommandations neutres par des experts sur les problèmes et défis que vous rencontrez quotidiennement. Notre communauté en ligne "IT Knowledge Exchange" (Echange de connaissances IT) vous permet de partager des questionnements et informations de tous les jours avec vos pairs et des experts du secteur.