AUTHENTIFICATION MULTIFACTEUR CONTEXTUELLE

Livre blanc

Okta France
Paris

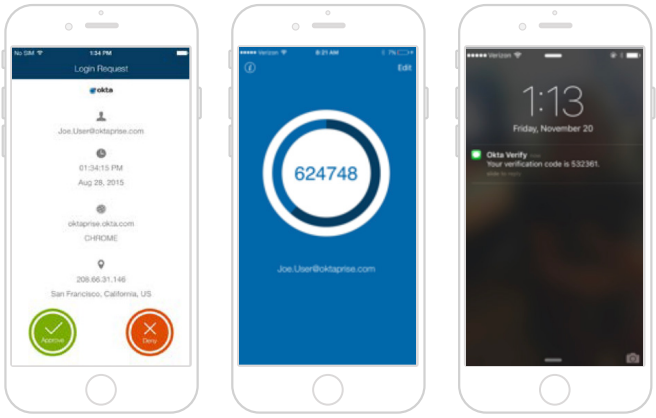
paris@okta.com
01 85 64 08 80

Résumé

Ce livre blanc présente Okta Adaptive Multi-Factor Authentication (MFA), une solution complète destinée aux entreprises qui, soucieuses de leur sécurité, souhaitent protéger leurs applications et leurs données. À la fois simple et robuste, elle assure une gestion contextualisée des accès en fonction de politiques, prend en charge un grand nombre de facteurs avancés, tire parti des big data de plusieurs milliers d'entreprises, et s'intègre avec les applications et les VPN dont les entreprises ont besoin. Okta Adaptive Multi-Factor Authentication garantit aux entreprises une sécurité optimale doublée d'une expérience utilisateur de qualité.

La sécurité est l'affaire des cadres dirigeants

Les failles de sécurité ne sont plus seulement une problématique IT. Protéger les entreprises contre l'impact d'un vol de données confidentielles en termes de coût et d'image est désormais la préoccupation majeure des cadres dirigeants. Il faut en moyenne 205 jours à une entreprise pour détecter une brèche[1]. Or, son impact peut être profond et durable. L'entreprise est tenue responsable des dommages occasionnés, mais cela ne s'arrête pas là : son chiffre d'affaires peut aussi en pâtir dans la mesure où le consommateur hésitera avant de faire un achat ou de lui confier ses données personnelles.



Les systèmes d'authentification classiques ne suffisent plus

Les VPN et les applications sont généralement sécurisés au moyen d'un système d'authentification à un seul facteur : le mot de passe. Mais en plus d'être difficiles à gérer, les mots de passe sont vulnérables à un certain nombre d'attaques courantes. Pour subtiliser les mots de passe des applications bancaires, grand public et d'entreprise, les pirates ont recours à des techniques de plus en plus sophistiquées, comme le phishing et l'ingénierie sociale. Face à la prolifération de ces attaques, les professionnels de l'informatique et de la sécurité doivent renforcer les contrôles.

[1] http://www.itsecurityguru.org/tag/breach

Pourcentage d'augmentation annuel du coût des failles de sécurité[2].

Pourcentage d'individus qui ouvrent les e-mails de phishing. Ils sont 11 % à cliquer sur les pièces jointes[3].

Pourcentage des attaques d'applications web perpétrées à l'aide d'identifiants volés[3].

Dans le cas du vol de données subi par le grand groupe d'assurance américain Anthem, des pirates ont dérobé des dossiers personnels dans les bases de données de l'entreprise à l'aide d'identifiants administrateurs compromis. Si une authentification multifacteur avait été en place, les pirates n'auraient pas pu se contenter des mots de passe administrateurs pour accéder aux données. Cette couche de vérification supplémentaire aurait évité la perte des données de près de 78,8 millions d'individus, dont 8,8 à 18,8 millions ne sont même pas des clients d'Anthem.

L'impact de la mobilité

La multiplication des collaborateurs nomades amène les entreprises à revoir les modes d'accès aux applications et aux données. Les utilisateurs accèdent à leurs applications chez eux, dans un café ou à l'hôtel, et sur leurs terminaux mobiles. Ils veulent donc pouvoir se connecter partout, ce qui oblige les équipes IT et sécurité à s'adapter de façon à sécuriser les accès depuis des réseaux et équipements inconnus.

Les avantages de l'authentification multifacteur

L'authentification multifacteur protège les entreprises d'un certain nombre d'attaques reposant sur le vol d'identifiants de connexion. Les utilisateurs doivent fournir un élément d'information en plus de leur mot de passe principal : quelque chose qui les définit, qu'ils détiennent ou qu'ils connaissent. Ainsi, même si le mot de passe est dérobé, le pirate ne pourra pas se connecter sans ce facteur supplémentaire.

[2] Ponemon Institute. 2015 Global Cost of Data Breach.
[3] Verizon. Data Breach Investigations Report.

Les limites des solutions d'authentification multifacteur d'ancienne génération

Expérience utilisateur médiocre

Malgré des avantages certains, l'authentification multifacteur peut impacter l'utilisateur final de multiples manières. Les solutions basées sur des jetons matériels sont difficiles à gérer et leur maintenance coûte cher. Le coût du suivi et du remplacement des jetons est significatif. Sans parler de l'inconvénient pour l'utilisateur final d'avoir à transporter ces jetons matériels et à saisir des codes. Quand une politique d'authentification multifacteur stricte est mise en place, les utilisateurs doivent s'authentifier plusieurs fois par jour, ce qui est source de frustration et nuit à leur productivité.

Gestion complexe

Les produits d'authentification multifacteur indépendants qui existent actuellement sont difficiles à implémenter, car ils doivent être intégrés avec chaque application et chaque système séparément. Il est également compliqué d'étendre la protection multifacteur aux nouvelles applications et d'ajouter des utilisateurs, ce qui rend l'évolutivité difficile. Et l'inconvénient des intégrations ponctuelles est que les administrateurs peuvent oublier d'activer la protection multifacteur ou ne pas savoir qu'elle est nécessaire pour les nouvelles ressources.

Évolutivité difficile

Les produits d'authentification multifacteur indépendants obligent les entreprises à utiliser des applications et systèmes compatibles avec des intégrations d'éditeurs spécifiques. Cette protection multifacteur ne peut donc être étendue à l'ensemble des applications et ressources. À l'heure où les applications cloud sont en plein essor, les entreprises réalisent que nombre d'entre elles ne gèrent pas les intégrations de leur fournisseur d'authentification multifacteur. Soit ces applications ne prennent pas en charge l'authentification multifacteur, soit elles utilisent un mécanisme natif, comme les codes envoyés par SMS et les questions de sécurité. Autant de processus qui ajoutent à la confusion des utilisateurs finaux, puisque ces derniers doivent jongler entre différents identifiants et facteurs d'authentification pour accéder à leurs services et applications.

Impossibilité de protéger tous les types d'utilisateur

Le nombre et les catégories d'utilisateurs en entreprise ne cessant d'augmenter, un seul type de facteur d'authentification ne permettrait pas de gérer les collaborateurs nomades ou internationaux, ni même certains groupes d'utilisateurs qui n'ont pas accès à un smartphone du fait de leurs fonctions. Nombreux sont par exemple les centres d'appel qui n'autorisent pas leurs employés à utiliser un terminal mobile personnel.

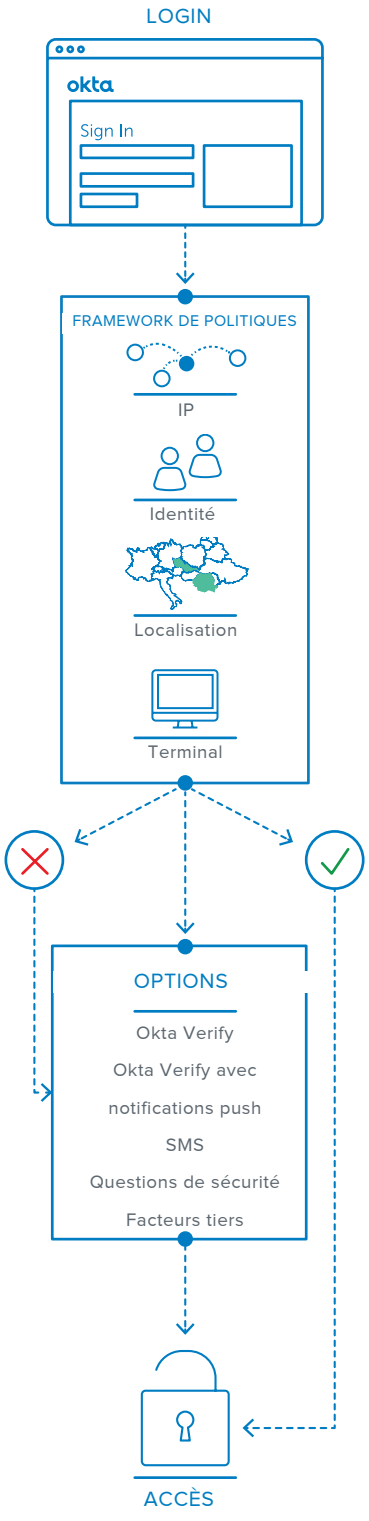
Une nouvelle approche de la sécurité : plus intelligente, plus simple et plus complète

Okta Adaptive MFA comble les lacunes des produits d'authentification multifacteur indépendants actuels en proposant une sécurité optimale et une expérience utilisateur de qualité grâce à la gestion des accès contextualisée basée sur des politiques, la prise en charge d'un grand nombre de facteurs modernes, l'analyse des big data et les intégrations avec l'ensemble des applications et VPN à protéger dans l'entreprise.

La gestion des accès contextualisée réduit les risques

La gestion des accès contextualisée d'Okta aide les entreprises à réduire les risques en examinant quand, où et comment les utilisateurs accèdent aux applications et aux données. Libre à elles d'autoriser l'accès, d'exiger une authentification renforcée, de restreindre les champs d'application, ou encore de refuser l'accès en fonction de l'identité de l'utilisateur, du réseau ou du pays depuis lequel il se connecte, et du terminal qu'il utilise. Les administrateurs pourront même ajuster les accès en fonction des facteurs de vérification sélectionnés par l'utilisateur et du mode d'authentification principal.

Les politiques d'accès contextuel d'Okta Adaptive MFA permettent de protéger facilement davantage de ressources avec un second facteur, sans perturber les activités de l'utilisateur. Le second facteur n'est pas demandé à chaque tentative de connexion, mais uniquement en cas de nécessité.



Une couverture complète des utilisateurs grâce à un ensemble de facteurs secondaires avancés

Grâce à l'intégration avec un grand nombre de facteurs secondaires et à des politiques d'enregistrement flexibles, les équipes IT n'ont plus à se demander si les utilisateurs sont équipés des derniers smartphones, voire d'un téléphone tout court pour ceux situés à l'étranger. Okta Adaptive MFA sécurise les accès de tous les utilisateurs à l'aide de facteurs choisis en fonction du rôle, des privilèges et de l'environnement de travail de chaque individu. Les options nécessitant un smartphone, comme Okta Verify avec notifications push, offrent aux utilisateurs un moyen simple et rapide de confirmer leur identité. Pour ceux qui ne disposent pas de smartphones, Okta Adaptive MFA prend en charge d'autres facteurs, comme les codes envoyés par SMS. Okta gère aussi des intégrations avec plusieurs facteurs tiers comme Yubikey, afin de faciliter la migration d'un facteur à l'autre, par exemple de RSA à Okta Verify. Les politiques d'enregistrement d'Okta permettent aux administrateurs de sélectionner les facteurs obligatoires, facultatifs et désactivés pour certains utilisateurs ou groupes d'utilisateurs, et peuvent justifier la configuration de facteurs redondants afin de réduire les coûts de support IT.

Sécurité proactive et authentification adaptative basée sur les risques

Les fonctions d'analyse des big data d'Okta calculent des scores de risque sur la base de profils utilisateurs détaillés, afin de limiter les faux positifs et de sécuriser les données et applications de façon proactive. Les équipes de sécurité peuvent utiliser les informations d'Okta provenant de millions d'utilisateurs, de terminaux et de demandes d'authentification pour identifier les attaques potentielles et empêcher les accès non autorisés. Contrairement aux produits d'authentification multifacteur autonomes, qui n'offrent pas une vision complète, Okta Adaptive MFA a accès aux données d'authentification unique (SSO) et de gestion de la mobilité en entreprise (EMM) d'Okta. Cette combinaison de données contextuelles tirées de l'ensemble des activités d'authentification d'un utilisateur renforce la sécurité en augmentant le nombre d'éléments à usurper pour les pirates.

Plus important encore, Okta Adaptive MFA ne se contente pas de générer des alertes. Comme Okta centralise le contrôle des accès à toutes les applications, lorsqu'une demande d'authentification suspecte est détectée, le pirate potentiel est automatiquement stoppé et les administrateurs peuvent bloquer totalement l'accès.

Des déploiements simples avec intégrations aux applications et aux VPN

Okta Adaptive MFA est une solution 100 % cloud qui permet le déploiement dans les entreprises d'un système d'authentification forte pour toutes les applications et les infrastructures stratégiques. Les administrateurs peuvent choisir parmi plus de 500 intégrations SAML et RADIUS dans le réseau d'applications d'Okta (OAN) pour protéger rapidement des applications et des VPN. La gestion centralisée des utilisateurs, des terminaux et des politiques de sécurité multifacteur permet de couvrir sans aucune exception l'ensemble des individus et des ressources à mesure qu'ils sont ajoutés, modifiés et supprimés.

Disponible pour les développeurs

En règle générale, les solutions d'authentification multifacteur sont difficiles à implémenter pour les développeurs qui créent leurs propres applications et portails. Okta Adaptive MFA est disponible sous forme d'API et de widget (Okta Sign-On) afin de simplifier l'inscription, la révocation et l'authentification. Les développeurs peuvent ainsi facilement ajouter un système d'authentification forte dans tout type d'application personnalisée. Grâce aux API d'Adaptive MFA d'Okta, ils peuvent aussi personnaliser entièrement l'expérience multifacteur pour offrir aux utilisateurs les avantages et la simplicité d'Okta Adaptive MFA dans une interface sur mesure.

Conclusion

Okta Adaptive MFA permet aux administrateurs IT et sécurité de déployer des mesures efficaces pour protéger les applications et infrastructures, sans nuire à l'expérience utilisateur. Okta offre une solution multifacteur intelligente, reposant sur les données contextuelles relatives aux utilisateurs, aux terminaux et aux comportements, ainsi que sur un grand nombre de facteurs avancés pour répondre aux besoins de tous les utilisateurs. L'ajout d'applications et d'utilisateurs est simple. Par conséquent, les entreprises peuvent bénéficier d'un retour sur investissement rapide et passer plus facilement de leurs produits multifacteurs on-premise à la solution cloud plus rentable d'Okta. Grâce à l'authentification unique (SSO) intégrée et à la gestion de la mobilité en entreprise (EMM), Okta simplifie la protection des utilisateurs, des terminaux et des applications.

Pour en savoir plus, consultez notre site :
okta.com/learn/Adaptive-MFA