okta

S’initier au Zero Trust

Ne jamais faire confiance, toujours vérifier

Okta France
Paris

paris@okta.com
01 85 64 08 80

S’initier au Zero Trust

Résumé

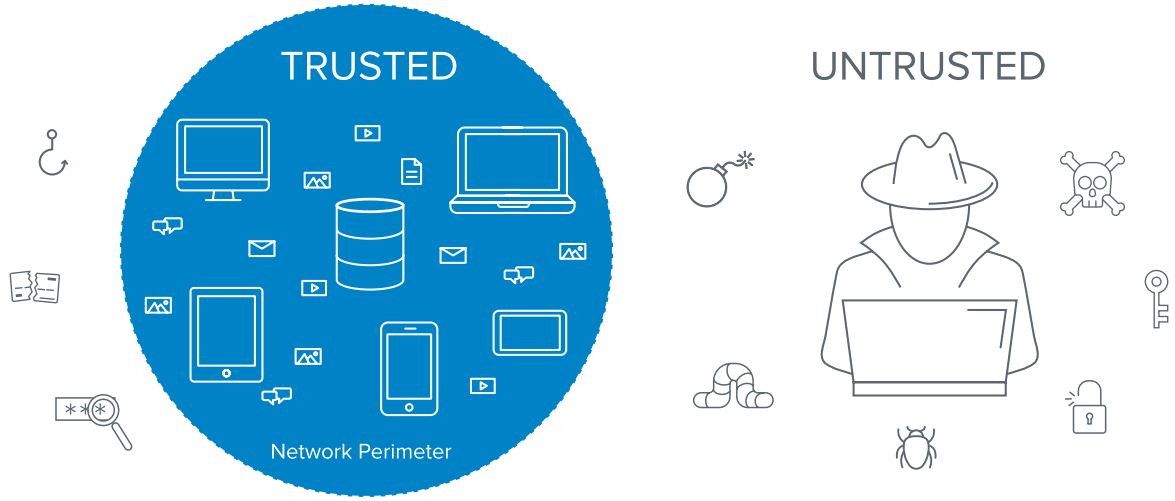
L’approche Zero Trust de la sécurité rejette l’idée selon laquelle le monde serait divisé en deux catégories : les réseaux internes « fiables » et les réseaux externes « non fiables ». Face à l’adoption des solutions cloud et mobiles, nous ne pouvons plus nous permettre d’adopter une perspective de la sécurité centrée sur le périmètre du réseau. Nous devons en effet garantir un accès sécurisé aux différents utilisateurs (collaborateurs, partenaires, prestataires, etc.), où qu’ils se trouvent et quels que soient le terminal et le réseau utilisés. S’il n’existe aucune solution miracle pour mettre en place une architecture de sécurité Zero Trust, la gestion des identités et des accès constitue néanmoins une technologie essentielle, sur laquelle les entreprises en quête de sécurité Zero Trust doivent s’appuyer.

Dans ce document, nous allons étudier les transformations du contexte de sécurité qui ont conduit à la création du Zero Trust, l’état actuel du framework ZTX (Zero Trust Extended Ecosystem), et la manière dont les entreprises peuvent utiliser Okta pour établir une appproche Zero Trust pérenne et efficace.

Problématique : la disparition du bouclier qui protège vos données

Les architectures de sécurité classiques reposent sur une vision dichotomique : d’un côté, les personnes dignes de confiance, autorisées à accéder à l’ensemble des données de l’entreprise ; de l’autre, les personnes suspectes, tenues à l’extérieur. Les équipes IT et sécurité investissent dans des systèmes défensifs qui protègent la frontière séparant ces deux groupes, en veillant particulièrement à sécuriser le périmètre du réseau, généralement à l’aide de pare-feux. Cette approche permet en effet d’ériger un mur virtuel entre les menaces potentielles et l’écosystème de l’entreprise. Malheureusement, ce modèle entièrement basé sur la confiance pose problème, car en cas de violation du périmètre, le pirate a assez facilement accès à tout ce qui se trouve sur l’intranet — sans parler des dégâts qu’une personne malveillante en interne pourrait causer, sans même enfreindre le périmètre.

Approche binaire de la sécurisation des entreprises



Face à l'adoption croissante des technologies cloud et mobiles, qui incitent à travailler hors du périmètre de sécurité des réseaux d'entreprise, ce périmètre est toujours plus difficile à renforcer. Dans ce contexte, aucun bouclier ne protège plus les ressources sensibles de l'entreprise : l'ensemble des collaborateurs, des prestataires, des partenaires et des fournisseurs ont accès aux données au sein du périmètre traditionnel.

Dans un monde cloud et mobile, davantage de personnes ont accès, où qu'elles soient, à toujours plus de ressources et de données à partir d'un plus grand nombre de terminaux. Il suffit d'une cyberattaque agressive pour que l'écosystème tout entier soit mis à mal. Les entreprises ne peuvent donc plus se reposer sur le principe de confiance en matière d'IT.

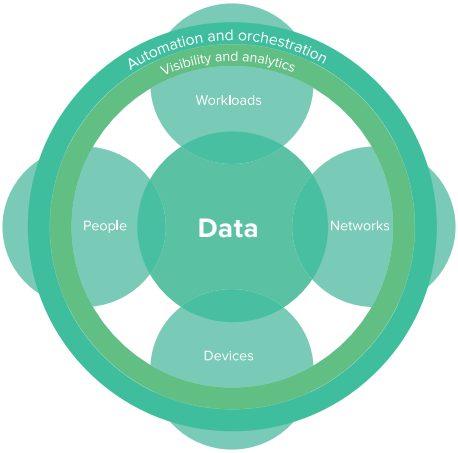
Prochaine étape : l'évolution du Zero Trust

Cette évolution du contexte de sécurité a donné naissance au concept du Zero Trust. Le Zero Trust est un framework de sécurité développé en 2009 par Jon Kindervag, analyste chez Forrester Research, qui rejetait l'idée opposant un réseau interne fiable à un réseau externe non fiable. Selon lui, il fallait considérer l'ensemble du trafic comme non sécurisé. Dans la version initiale du framework, Jon Kindervag cherchait surtout à revoir le périmètre du réseau et conseillait aux entreprises d'inspecter la totalité du trafic en temps réel, ce qui nécessitait une gateway de segmentation du réseau. Son approche du Zero Trust reposait essentiellement sur les trois principes suivants : 1) l'accès à toutes les ressources, où qu'elles se trouvent, doit être sécurisé ; 2) le contrôle des accès repose sur un principe de nécessité absolue et est strictement appliqué ; et 3) les entreprises doivent inspecter et enregistrer l'ensemble du trafic pour vérifier si les utilisateurs se comportent normalement.

Depuis 2009, l'essor des solutions cloud et mobiles a joué un rôle de catalyseur dans l'évolution du modèle Zero Trust initial. En 2017, l'approche CARTA de Gartner[1] faisait ainsi écho au framework de Jon Kindervag. Elle préconisait l'authentification et l'octroi des accès non plus seulement au point d'entrée principal, mais tout au long de l'expérience utilisateur, moyennant une évaluation contextuelle basée sur les risques destinée à identifier les menaces potentielles. L'étude BeyondCorp de Google, publiée en 2014[2], présente un exemple particulièrement réussi de déploiement à grande échelle du Zero Trust.

[1] Use a CARTA Strategic Approach to Embrace Digital Business Opportunities in an Era of Advanced Threats, Gartner, Inc., 22 mai 2017
[2] BeyondCorp: A New Approach to Enterprise Security, Google, 2014

L'évolution du framework Zero Trust de Forrester, l'écosystème ZTX (Zero Trust Extended Ecosystem) dirigé par l'analyste Chase Cunningham, traduit également cette tendance à s'éloigner de la segmentation du réseau. Dans la version de Chase Cunningham, le Zero Trust passe des « pare-feux de nouvelle génération » à une « gestion des accès de nouvelle génération ». Cette nouvelle perspective renforce l'aspect humain du modèle et fait du contrôle de l'identité des personnes ayant accès au réseau et aux données, la clé de la réussite. L'équipe de Forrester insiste sur l'intérêt stratégique de fonctionnalités telles que l'authentification unique (SSO), et observe une « réduction exponentielle des menaces liées à l'accès » grâce à l'authentification multifacteur[3].



Malgré l'évolution du modèle, le concept de base du Zero Trust est resté le même : dans le contexte de sécurité actuel, l'attention ne se concentre plus sur le réseau, mais sur les personnes qui ont accès aux systèmes et sur les contrôles d'accès auxquels elles sont soumises. C'est là qu'intervient la gestion des identités — et Okta.

2009 2011 2013 2015 2017 2019

2009: Naissance du framework Zero Trust de Forrester

2018: Lancement du framework TX

2014: Publication de l'étude BeyondCorp de Google

- La connexion depuis un réseau spécifique ne doit pas déterminer les services accessibles.
- L'accès aux services est octroyé en fonction de l'identité et du terminal de l'utilisateur.
- L'accès aux services doit être entièrement authentifié, autorisé et chiffré.

2017: Publication du modèle CARTA de Gartner

Continuous Adaptive Risk and Trust Assessment

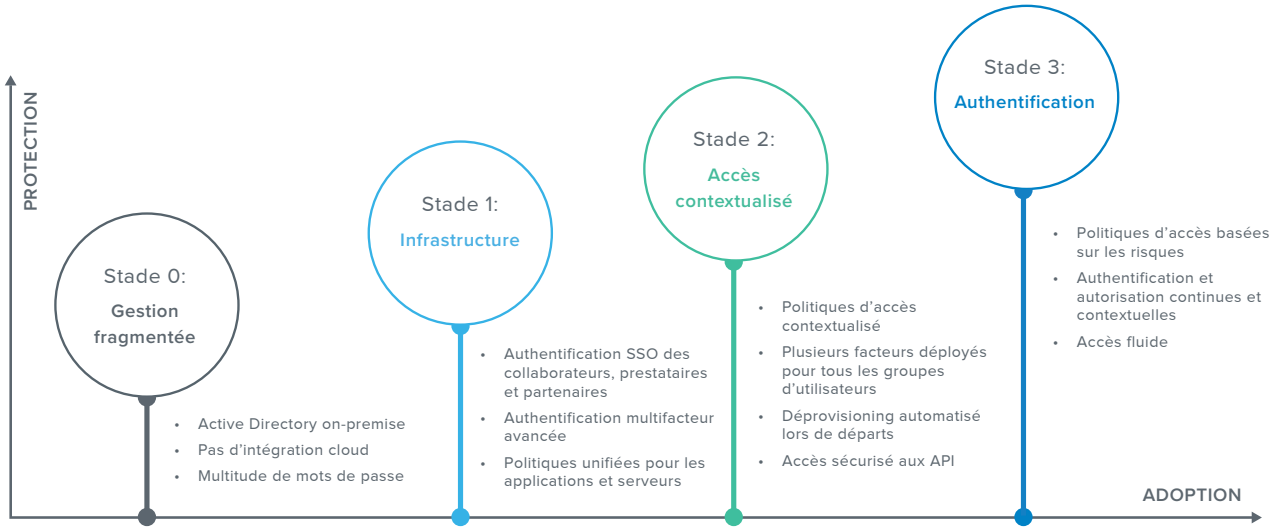
[3] The Zero Trust eXtended (ZTX) Ecosystem, Forrester Research, Inc., 19 janvier 2018

Forrester a récemment publié une nouvelle étude Zero Trust[4] qui insiste davantage encore sur l'importance de la gestion des accès et désigne Okta comme l'un des acteurs majeurs (Strong Performers) du marché de la sécurité Zero Trust. Parmi les différents fournisseurs cités dans cette étude publiée au 4e trimestre 2018 et intitulée The Forrester Wave™: Zero Trust eXtended (ZTX) Ecosystem Providers, Okta obtient la note maximale dans trois catégories : sécurité des collaborateurs, vision et stratégie ZTX, et approche du marché. Selon les propres termes du cabinet, « alors que les notions traditionnelles de "systèmes" et d'"infrastructure" disparaissent, l'identité, sous ses multiples formes, joue un rôle de plus en plus important. » Forrester considère l'identité comme « un pilier essentiel du Zero Trust » en raison de sa nature stratégique[5].

Baser la sécurité Zero Trust sur la gestion des identités

Pour dire les choses simplement, le principe de base du Zero Trust est de « ne jamais faire confiance, toujours vérifier ». Cette approche garantit à chaque utilisateur un niveau d'accès adapté aux ressources dont il a besoin, dans le contexte qui convient, et une évaluation continue de cet accès — le tout sans créer de points de friction. Cet objectif ultime ne s'atteint pas du jour au lendemain, et lorsqu'une entreprise met en œuvre une architecture Zero Trust, l'infrastructure passe par différents stades de maturité :

Courbe de maturité



Stade 0 : **Gestion fragmentée des identités**

Au début de leur parcours de sécurité Zero Trust, la plupart des entreprises se retrouvent avec différentes applications on-premise et cloud non intégrées, ou avec des annuaires on-premise de type Active Directory. Cela oblige les équipes IT à gérer des identités disparates dans plusieurs systèmes, ainsi que les nombreux services et applications utilisés sans connaissance des enjeux informatiques. Côté utilisateur, on assiste à une multiplication des mots de passe, généralement vulnérables. Sans visibilité ni maîtrise de ces identités fragmentées, les équipes responsables de l'IT et de la sécurité se retrouvent avec des fenêtres de vulnérabilité potentiellement larges, que les pirates mettent à profit pour accéder aux systèmes.

[4] Future-Proof Your Digital Business With Zero Trust Security, Forrester Research Inc., 28 mars 2018
[5] The Forrester Wave™: Zero Trust eXtended (ZTX) Ecosystem Providers, 4e trimestre 2018

Stade 1 : **Gestion des identités et des accès (IAM) unifiée**

Pour corriger les failles de sécurité créées par cette multitude d'identités fragmentées, la première étape consiste à faire appel à un système IAM (Identity and Access Management) commun à l'ensemble des applications cloud et on-premise. Cette consolidation opérée au stade 1, via l'authentification unique (SSO), est essentielle pour gérer les accès et ne doit pas se limiter aux seuls clients. Elle doit en effet concerner tous les utilisateurs ayant besoin d'accéder à un service, ce qui inclut l'ensemble des collaborateurs, des prestataires et des partenaires de l'entreprise au sens large. L'ajout d'un second facteur d'authentification à ce point d'accès centralisé permet de limiter les attaques visant les identifiants. Par ailleurs, il est indispensable d'unifier les politiques d'accès aux applications et aux serveurs, pièces maîtresses de l'infrastructure IT, afin de centraliser la gestion des identités et des accès dans un espace sûr et facile à administrer par l'équipe informatique.

Des milliers d'entreprises utilisent Okta SSO pour unifier les identités de leurs utilisateurs, souvent en l'associant à Okta Universal Directory. Cet annuaire cloud, qui peut être utilisé comme une source fiable et unique, fait office de point d'intégration des multiples annuaires Active Directory et autres annuaires on-premise. Okta SSO simplifie la gestion et la sécurisation de l'entreprise étendue par l'équipe IT, et évite la multiplication des mots de passe qui pénalise les utilisateurs. Avec Okta Advanced Server Access, les équipes IT peuvent étendre le contrôle des accès à la couche serveur, en généralisant ainsi la gestion des accès sécurisée à toutes les ressources on-premise et cloud placées sous leur responsabilité.

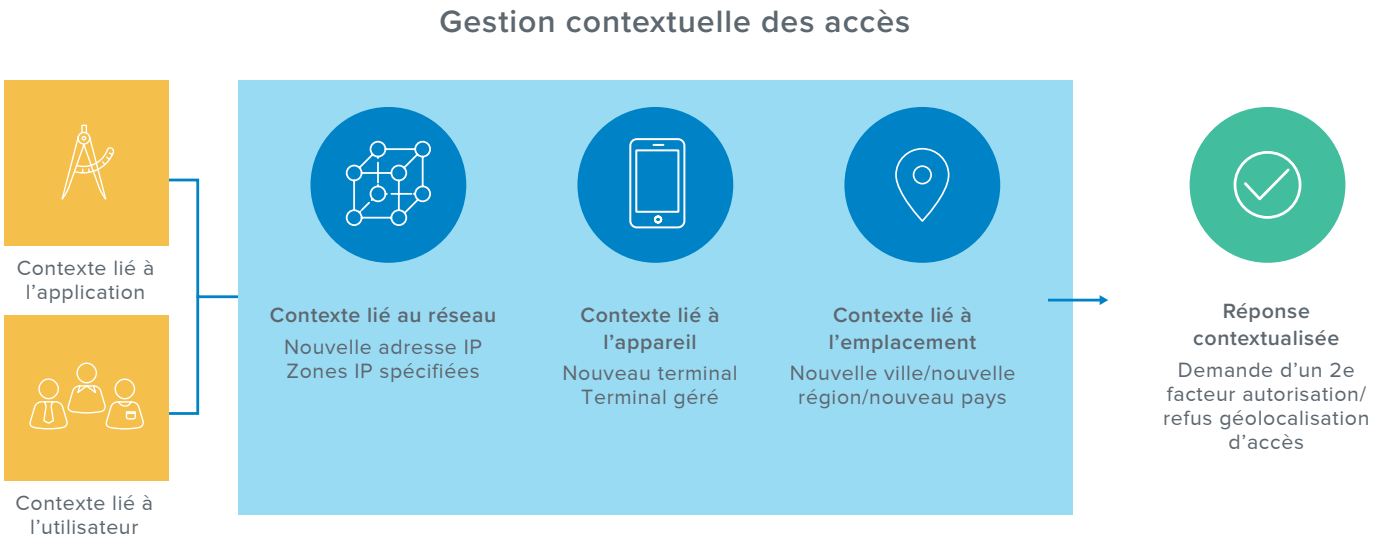
Stade 2 : **Accès contextualisé**

Une fois la gestion des identités et des accès (IAM) unifiée, l'étape suivante vers la sécurité Zero Trust consiste à superposer les politiques d'accès contextualisé. Il faut pour cela recueillir des informations contextuelles sur les utilisateurs (Qui sont-ils ? Font-ils partie d'un groupe à risque ?), les applications (À quelle application l'utilisateur essaie-t-il d'accéder ?), les terminaux, la localisation et le réseau, et appliquer des politiques d'accès sur la base de ces informations. Par exemple, il est possible de définir une règle pour fluidifier l'accès aux terminaux gérés depuis le réseau de l'entreprise, et de demander une authentification multifacteur pour les terminaux non gérés qui cherchent à se connecter à partir de nouveaux sites. Les entreprises peuvent également imposer plusieurs facteurs pour l'ensemble des groupes d'utilisateurs, afin d'instaurer un dispositif d'authentification renforcée basé sur l'analyse des tentatives d'authentification. Ainsi, les utilisateurs à faible risque et non équipés de smartphone peuvent se servir de mots de passe à usage unique, tandis que les collaborateurs à plus haut risque sont tenus d'utiliser des jetons avec clé cryptographique pour s'authentifier en toute sécurité auprès d'un service.

D'autre part, si un utilisateur change de poste, le provisioning automatisé permet de s'assurer qu'il a uniquement accès aux outils dont il a besoin (ou, si le collaborateur quitte l'entreprise, de révoquer automatiquement ses droits d'accès, en réduisant ainsi le risque de comptes orphelins ou d'accès latent après son départ). Enfin, ces contrôles d'accès sophistiqués doivent être étendus à toutes les technologies utilisées par le personnel, et prévoir un accès sécurisé aux API, piliers des applications actuelles, mais susceptibles d'exposer les données sensibles aux dangers du Web.

Aujourd'hui, nombre d'entreprises utilisent déjà la fonctionnalité de gestion des accès contextualisée intégrée à la solution Okta Adaptive MFA. En traitant diverses informations contextuelles sur l'utilisateur, le terminal, le lieu, le réseau et l'application ou le navigateur employé pour accéder à une ressource, le framework de politiques d'Okta peut apporter une réponse contextualisée. Cette dernière repose sur la tolérance au risque de l'entreprise, qui constitue sa première ligne de défense. Par exemple, l'entreprise peut établir une politique qui exige un simple mot de passe à l'utilisateur qui cherche à s'authentifier sur le réseau de l'entreprise depuis son ordinateur portable professionnel habituel. Mais si l'utilisateur essaie de s'authentifier sur son ordinateur portable depuis l'étranger, sur un réseau Wi-Fi public, la politique pourrait imposer un second facteur en plus du mot de passe.

Ce type d'accès contextualisé offre des avantages aussi bien pour l'utilisateur que pour les équipes en charge de l'IT et de la sécurité, puisqu'il n'impose un second facteur qu'en cas d'authentification à risque, et non de manière systématique.



Stade 3 : **Authentification adaptative**

La dernière étape d'une implémentation Zero Trust consiste à renforcer les efforts de l'entreprise en matière d'authentification et d'autorisation d'accès. Cela signifie que l'authentification n'est plus cantonnée au point d'entrée principal, mais généralisée à toute l'expérience utilisateur en continu, moyennant une évaluation contextuelle basée sur les risques destinée à identifier les menaces potentielles. À première vue, cette approche se résume à ajouter un moteur intelligent d'analyse des risques aux réponses contextualisées du 2e stade, pour aller au-delà des politiques définies au cas par cas à l'étape précédente. Les équipes IT peuvent alors établir une tolérance de risque et autoriser l'évaluation des risques en fonction de ces signaux contextuels, afin de déterminer le niveau de risque d'un événement d'authentification donné et d'imposer un second facteur sur la base de ces renseignements. D'autre part, la « confiance » n'est plus accordée de manière définitive : l'authentification contextuelle fait l'objet d'un suivi continu destiné à repérer tout changement de l'un de ces signaux. Une nouvelle vérification de l'authentification et de l'autorisation est par conséquent demandée en cas de changement de l'un des aspects du contexte de l'utilisateur. Enfin, si ces contrôles d'accès intelligents avec analyse des risques renforcent la sécurité, ils simplifient aussi l'expérience de l'utilisateur final, ce qui se traduit par un accès plus fluide et, si les politiques établies par l'équipe IT le permettent, une authentification sans mot de passe.

Okta permet aux administrateurs d'utiliser des politiques pour transformer l'expérience d'authentification des utilisateurs et élimine totalement les mots de passe du flux d'authentification. En remplaçant les mots de passe par un autre facteur (comme Okta Verify ou une clé YubiKey), qui devient alors le premier facteur d'authentification, Okta offre davantage de liberté aux administrateurs informatiques. Ces derniers peuvent établir des politiques d'authentification basées sur les risques, qui imposent une authentification renforcée reposant sur la tolérance de risque liée aux différents signaux reçus. Si son identité laisse peu de doute, l'utilisateur est uniquement invité à fournir ce premier facteur, qui n'est pas un mot de passe.

Même si Okta dispose déjà d'une approche performante basée sur les politiques et intégrant des signaux contextualisés, nous ne cessons de développer l'intelligence de notre moteur de politiques pour lui donner une dimension plus comportementale.

Aujourd'hui, la plupart des entreprises n'en sont encore qu'au stade 0 de la courbe de maturité Zero Trust, mais à mesure qu'elles se rapprochent du principe « ne jamais faire confiance, toujours vérifier », Okta leur offre de nouvelles fonctionnalités pour les aider à simplifier et à renforcer la gestion des accès.

Étendre le Zero Trust à un écosystème de sécurité plus vaste

Okta offre une solution de gestion des identités servant de base à l'architecture Zero Trust, tout en s'intégrant étroitement à l'ensemble des solutions de sécurité pour vous permettre d'unifier votre approche. Avec Okta Integration Network, Okta gère des intégrations étroites avec toutes les composantes de l'écosystème Zero Trust :

netskope	McAfee Together is power.	Sécurité des données
paloalto NETWORKS	CISCO	Sécurité réseau
vmware	Carbon Black.	Sécurité des équipements
CYBERARK	BOMGAR	Sécurité de la charge de travail
splunk>	IBM QRadar	Analyse
servicenow	splunk>	Orchestration

Ce large éventail d'intégrations soutient une stratégie de pointe indépendante, emblématique d'Okta Identity Cloud.

Si le suivi comportemental repose sur un contrôle intelligent de l'accès aux ressources des entreprises, il est toutefois difficile d'identifier la cause première d'une brèche — surtout si le problème est d'en identifier l'auteur plutôt que la nature des données visées. Grâce à l'intégration de solutions d'analyse de sécurité et de gestion des événements de sécurité (SIEM), Okta permet aux entreprises d'exploiter toute la richesse de sa gestion contextualisée des identités et de l'activité des utilisateurs pour prendre des mesures de réhabilitation des comptes compromis. Okta s'intègre également avec des CASB, comme Netskope et McAfee, ce qui lui permet d'offrir une visibilité et des alertes détaillées pour un contrôle continu des événements à risque lors des sessions authentifiées. À l'instar de ses partenaires SIEM, Okta peut fournir de précieuses données d'authentification pour mieux détecter les anomalies, ce qui permet aux services CASB de renvoyer une réponse à Okta, qui peut alors révoquer l'accès au niveau de la couche de gestion des identités. Ce ne sont là que quelques exemples de dispositifs de sécurité Zero Trust parmi d'autres offerts aux entreprises par Okta Integration Network.

Étude de cas : 21st Century Fox

Depuis toujours, la sécurité est l'une des principales préoccupations de 21st Century Fox, le géant mondial de la production de films et de programmes par câble, radiodiffusion, télévision payante et satellite. L'entreprise, qui s'adresse chaque jour à plus de 1,8 milliard d'abonnés dans près de 50 langues, est à la tête d'un portefeuille mondial de réseaux câblés et de radiodiffusion mais aussi de biens, comme des studios de cinéma et de télévision. Il y a quelques années, l'attaque d'un autre grand studio a convaincu l'entreprise de renforcer ses pratiques de sécurité.

Étape 1 : Prise en main du Zero Trust

21st Century Fox disposait de tous les éléments classiques d'un périmètre protégé, des pare-feux aux logiciels antivirus. L'un des premiers projets confiés à l'équipe IT par Melody Hildebrandt, responsable de la sécurité des systèmes d'information, visait à regrouper tous les utilisateurs internes de la Fox dans un même environnement. Il s'agissait notamment de renforcer l'authentification, d'identifier plus facilement les utilisateurs ayant accès à telle ou telle application, et de simplifier les processus de gestion des identités. Une fois l'infrastructure centrale de gestion

> « Okta était le socle dont nous avions besoin pour mener notre projet Zero Trust à maturité. C'était la solution de gestion des identités à laquelle nous pouvions intégrer les moyens de contrôle nécessaires pour évaluer l'identité d'une personne. Elle nous a aidés à mûrir notre réflexion autour du Zero Trust. »
>
> **– Melody Hildebrandt, CISO, 21st Century Fox**

des identités et des accès unifiée, Melody Hildebrandt a cherché à concevoir une nouvelle architecture Zero Trust capable de contrer les tentatives de vol d'identifiants et les attaques par phishing, aujourd'hui à l'origine de la plupart des brèches qui font les gros titres. Ces changements n'ont pas nui à l'expérience utilisateur des collaborateurs, prestataires et partenaires qui composent le réseau de la Fox.

Étape 2 : Adoption d'une solution de gestion des accès dynamique et contextualisée au sein de 21st Century Fox, dans son ensemble étendu

21st Century Fox a fait appel à Okta Identity Cloud pour étendre cette approche du Zero Trust à l'ensemble de ses effectifs, en utilisant les produits Okta de gestion de l'identité des collaborateurs pour ses employés, et ses produits API pour son réseau de partenaires et de prestataires. L'entreprise, qui utilisait déjà les produits Okta SSO, Universal Directory et Lifecycle Management, a décidé d'y ajouter les solutions Adaptive MFA et API Access Management.

Une fois l'infrastructure centrale mise en place, il était indispensable pour Melody Hildebrandt et son équipe d'adopter un modèle dynamique de gestion des accès. Ils ont donc déployé les produits Okta Lifecycle Management et Universal Directory. Au moindre changement de statut d'un utilisateur dans Workday (le système RH de la Fox), Universal Directory examine ses attributs et replace l'utilisateur dans le groupe approprié. Ensuite, la solution Lifecycle Management se charge du provisioning des outils et du niveau d'accès dont l'utilisateur a besoin pour travailler.

Au final, les utilisateurs ont instantanément accès à tout ce dont ils ont besoin, et il n'y a aucun risque qu'une personne ait accidentellement accès à des informations qui ne lui sont pas destinées. Qui plus est, en cas de compromission des identifiants, il y a moins de risques qu'une personne extérieure puisse accéder à du contenu ou des données sensibles. Et lorsqu'un collaborateur de 21st Century Fox quitte l'entreprise ou que le contrat d'un partenaire prend fin, les mesures nécessaires sont prises presque immédiatement. L'accès est révoqué dès le déprovisioning du compte dans Universal Directory, et il ne subsiste aucun compte « fantôme ». Avec l'Adaptive MFA, l'entreprise peut également prendre des décisions d'authentification avisées, sur la base de facteurs tels que l'identité de l'utilisateur, le type de terminal dont il se sert, l'endroit où il travaille et l'application à laquelle il souhaite accéder. Elle peut ainsi maintenir des niveaux de sécurité élevés, tout en épargnant à ses collaborateurs des étapes inutiles lors du processus d'authentification. Lors du déploiement de la solution Adaptive MFA, 21st Century Fox est resté très à l'écoute de ses collaborateurs et partenaires, et leur a proposé un maximum d'options d'identification, notamment Okta Verify, YubiKey, Okta Verify avec notifications push, appels vocaux, SMS, jetons USB U2F, etc.

La formule Zero Trust idéale pour 21st Century Fox : sécurité + convivialité

Pour 21st Century Fox, la réussite se mesure à la capacité à offrir du contenu aux consommateurs de manière simple et sécurisée. Hotstar, une application mobile proposée aux consommateurs indiens, qui a récemment dépassé les sept millions de vues simultanées en direct, en est une excellente illustration. « C'est un résultat assez surprenant pour une application lancée il y a à peine deux ans, la première à proposer du cricket aux utilisateurs mobiles indiens, avec une protection contre les attaques DDoS et le piratage des identifiants, dont le risque était extrêmement élevé », explique Melody Hildebrandt.

Avec Okta, les collaborateurs et partenaires de 21st Century Fox peuvent se recentrer sur leur cœur de métier, c'est-à-dire proposer d'excellents contenus aux clients de l'entreprise, sans avoir à se préoccuper des menaces extérieures. Ils peuvent en substance combler une importante faille de sécurité, tout en simplifiant la tâche des équipes IT et des utilisateurs. De quoi réjouir les spectateurs de la Fox, car le contenu ne cesse de s'améliorer.

Que vous réservent Okta et le Zero Trust ?

Il n'existe aucune solution miracle pour parvenir au Zero Trust, quoi qu'affirment certains fournisseurs. Les entreprises sont en quête de technologies de pointe qui leur offrent un maximum de flexibilité et d'efficacité. C'est la raison pour laquelle elles se tournent actuellement vers Okta et la gestion des identités pour entamer leur parcours Zero Trust, en inscrivant Okta Identity Cloud au cœur de leur stratégie de gestion des accès de nouvelle génération — et en veillant à ce que chacun ait accès aux informations appropriées en temps voulu. Ne jamais faire confiance, toujours vérifier.

Gestion innovante des accès

Chaque utilisateur **a le** niveau d'accès adapté **aux** ressources dont il a besoin **dans le** contexte qui convient **avec une** évaluation continue de cet accès

Maximum de fluidité

Okta ne cesse d'investir pour accompagner les entreprises tout au long de ce parcours. Suivez-nous et ne manquez pas nos articles de blogs sécurité (okta.com/blog et www.okta.com/security-blog/) pour vous tenir informé des mises à jour déployées sur notre plateforme.

À propos d'Okta

Okta est un éditeur indépendant spécialisé dans la gestion et la protection des données d'identification, leader du secteur. La plateforme Okta Identity Cloud connecte et protège les collaborateurs des plus grandes entreprises au monde, en plus d'assurer une connexion sécurisée avec leurs partenaires, fournisseurs et clients. Grâce à son intégration avancée à plus de 6 500 applications, Okta Identity Cloud permet à n'importe quel utilisateur de se connecter facilement et en toute sécurité, tous terminaux confondus.

Des milliers de clients, dont 20th Century Fox, Adobe, Dish Networks, Experian, Flex, LinkedIn et News Corp, font confiance à Okta pour améliorer leur productivité, doper leur chiffre d'affaires et préserver leur sécurité. Grâce à Okta, ils peuvent accéder facilement et sans risque aux technologies dont ils ont besoin pour accomplir leurs missions stratégiques.

Pour en savoir plus, rendez-vous sur www.okta.com/fr