okta

Webinar 1 minute : Le Zero Trust en pratique

Pas le temps de visionner le webinar Le Zero Trust en pratique ? Rassurez-vous, nous allons tout vous expliquer.

La sécurité Zero Trust fait beaucoup parler d'elle, certes, mais elle ne relève pas seulement de la théorie.

La confiance se résumait jusqu'ici à une décision binaire déterminée par le réseau, mais face à l'engouement des entreprises pour les services cloud et mobiles, le périmètre tel que nous le connaissions n'existe plus. La confiance ne dépend plus du réseau et n'est plus une décision binaire.

Les familiers des concepts du Zero Trust cherchent désormais à savoir si ce modèle tient réellement ses promesses sur le terrain en termes de sécurité. Où que vous en soyez dans votre parcours Zero Trust, vous vous demandez probablement comment intégrer ces notions et architectures au sein de votre entreprise.

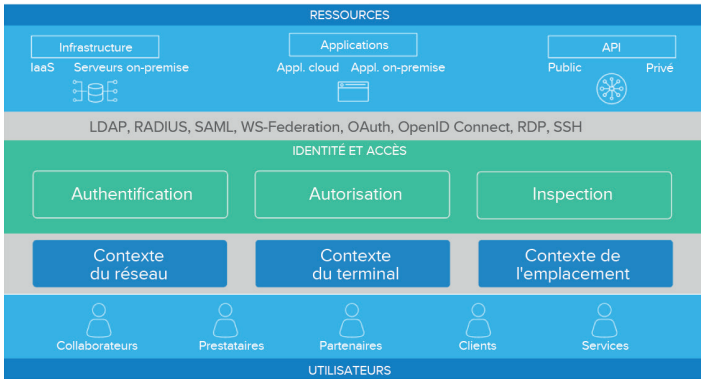
Pourquoi commencer par les identités ?

Une couche d'identités unifiée s'impose pour créer des contrôles d'accès plus élaborés, élaborer des politiques évoluant au fil du temps et aider vos systèmes à gagner en intelligence. L'accès repose sur la confiance, qui est déterminée par le contexte.

Lier confiance et contexte

Étape 1 : cartographiez vos ressources et l'identité de vos utilisateurs. Font-ils partie d'un groupe à haut risque ? Quelles sont les ressources auxquelles ils tentent d'accéder ? S'agit-il d'un outil à faible risque ou d'une infrastructure à haut risque ?

Étape 2 : examinez le contexte de l'événement d'authentification. Quel est le contexte lié au réseau, au terminal et à l'emplacement ? S'agit-il d'une nouvelle adresse IP ? L'utilisateur se connecte-t-il depuis une zone IP de l'entreprise ? S'agit-il d'un terminal géré ou nouveau ? L'authentification a-t-elle lieu dans une nouvelle ville, une nouvelle région, voire une zone géographique sur liste noire ?



Étape 3 : combinez les deux premières étapes pour créer une réponse contextuelle : faut-il demander un deuxième facteur d'authentification, autoriser/refuser l'accès ou émettre une alerte de sécurité ?

Étape 4 : dépassez le cadre des politiques d'accès basées sur le contexte, et évaluez le risque global associé à la connexion, elle-même évaluée en continu.

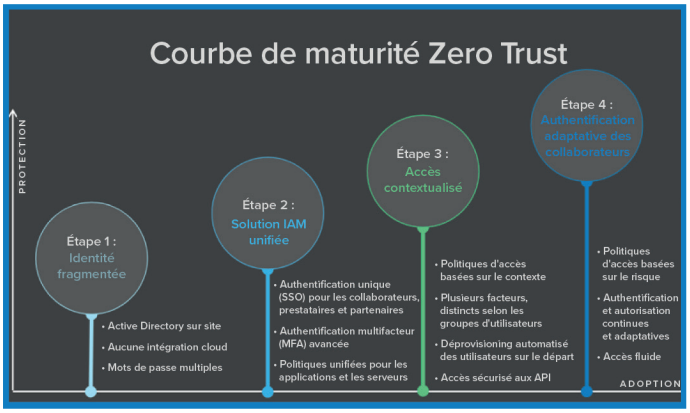
Si tout est correctement implémenté, vous récolterez les fruits du Zero Trust : les bonnes personnes disposeront du bon niveau d'accès aux bonnes ressources, dans le contexte adéquat, évalué en continu. L'objectif est, bien sûr, de limiter au maximum les points de friction. La sécurité doit être un moteur et non un frein obligeant les utilisateurs à jongler avec plusieurs réseaux ou à saisir différents mots de passe.

Difficultés

Le Zero Trust permet de déjouer certaines des grandes difficultés que rencontrent les équipes IT et sécurité : gestion de plusieurs référentiels d'utilisateurs sans aucune source fiable, prolifération des mots de passe dans toute l'entreprise, gestion manuelle des PKI et des clés, et absence de solution pour appliquer le principe de moindre privilège. Faute de visibilité sur le comportement des utilisateurs, seul le trafic réseau était auparavant contrôlable. Résultat : des brèches étaient parfois découvertes au bout de plusieurs semaines, plusieurs mois, voire plusieurs années.

Étapes à suivre pour atteindre le Zero Trust

Que le Zero Trust soit une initiative organisationnelle générale ou un projet ascendant, cette courbe de maturité, que nombre de nos clients ont suivie, peut vous guider dans votre propre parcours.



Points à retenir

Bien qu'il n'y ait pas de recette miracle pour implémenter le Zero Trust, votre parcours doit commencer par les identités, qui servent de fondement, contribuent à la sécurité et pilotent les expériences. Avec une solide couche d'identités, les utilisateurs gagnent la confiance de l'entreprise sur la base d'un contexte qui est évalué en continu.

Okta est une plateforme Zero Trust de pointe, mais aussi un tremplin. Le cabinet d'analystes Forrester Research, qui a récemment inclus Okta dans son étude du marché Zero Trust, The Forrester Wave™: Zero Trust eXtended (ZTX) Ecosystem Providers, 4e trimestre 2018, a déclaré :

> « Okta sait parfaitement comment protéger les utilisateurs finaux et sécuriser leur accès au réseau, ce qui constitue un atout majeur pour toutes les stratégies et entreprises orientées Zero Trust. La société a consacré énormément de temps et de ressources au déploiement d'un système de sécurité simple pour les utilisateurs finaux et les entreprises, et grâce à sa croissance exponentielle et à son développement fulgurant, elle s'est constitué une solide base de clients conquis par sa solution. »

Vous souhaitez en savoir plus ? Visionnez le webinar complet ici.

Qui sommes-nous ?

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.

www.okta.com/fr