jamf

LE MODÈLE DE SÉCURITÉ ZERO TRUST:

Adopter une stratégie de sécurité plus moderne

LE MONDE DU TRAVAIL EST EN CONSTANTE ÉVOLUTION

Il est important de concilier efficacité et productivité au quotidien avec les exigences globales des entreprises modernes.

La technologie progresse en même temps que la population active pour connecter les gens et leur donner accès à tout ce dont ils ont besoin, de n'importe où, de n'importe quel appareil. Le monde du travail progresse à une vitesse phénoménale, et les entreprises font tout leur possible pour accompagner leurs employés, où qu'ils se trouvent, et les aider à répondre à leurs besoins professionnels.

Ce soutien exige que les administrateurs informatiques surmontent et s'adaptent au défi supplémentaire que représente la sécurisation des données, tout en laissant aux employés une liberté totale et sans restriction d'accès à tout ce dont ils ont besoin, de n'importe où, pour rester productifs.

Presque du jour au lendemain, le concept de réseau d'entreprise a été jugé insuffisant dans un monde moderne de travail à distance. Il manquait de flexibilité pour des employés internationaux constamment en déplacement, entraînait des coûts supplémentaires sous la forme de tickets de support technique, et augmentait les risques de sécurité des données. D'autres aspects de la technologie ayant fait de nombreux progrès pour s'adapter à cette évolution, il fallait également trouver un meilleur moyen d'assurer un accès sécurisé.

La réponse ? Le modèle Zero Trust : un modèle de sécurité plus efficace avec une approche centrée sur l'identité.

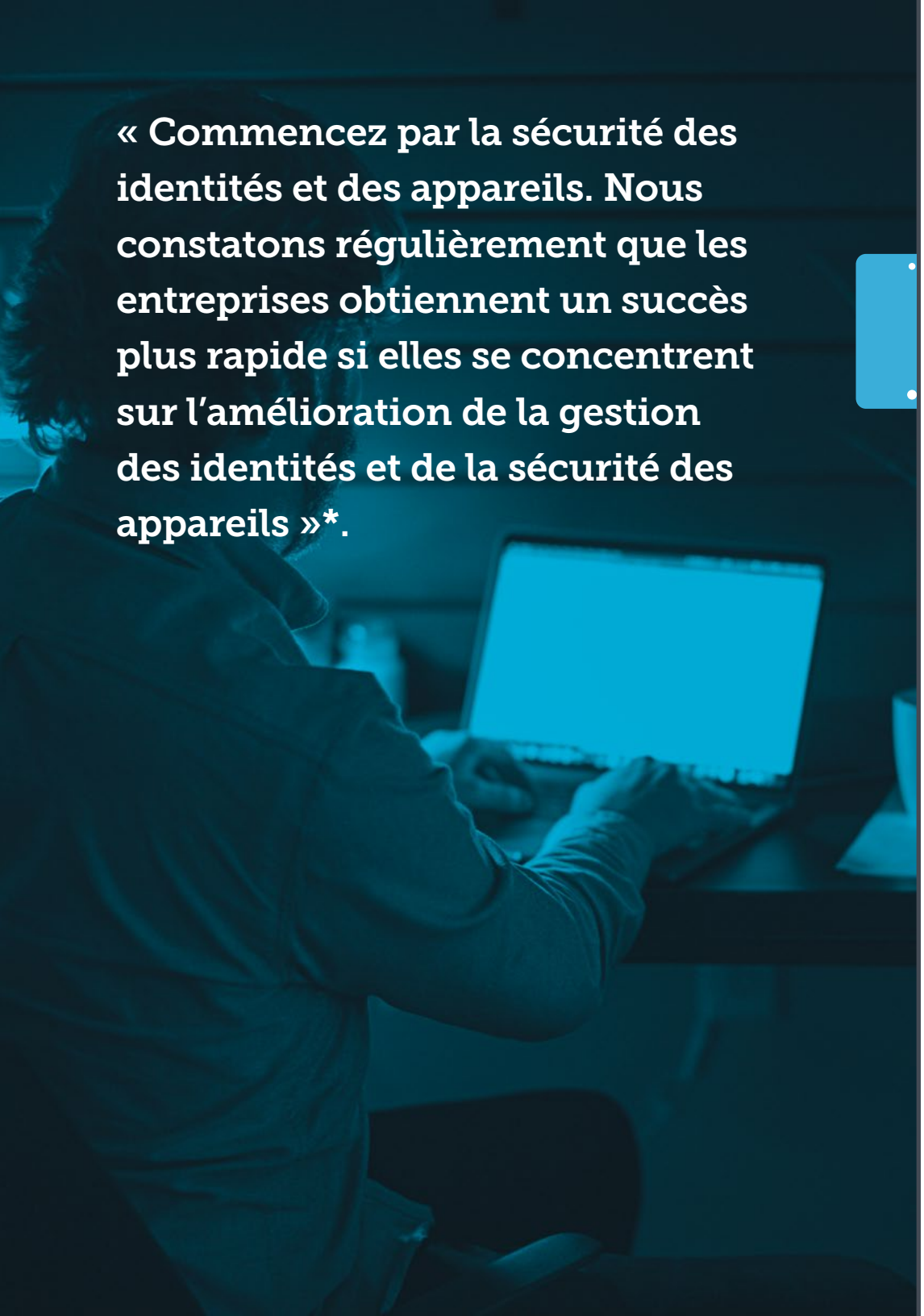
QU'EST-CE QUE LE MODÈLE DE SÉCURITÉ ZERO TRUST ?

Le concept du Zero Trust ne date pas d'hier. En fait, il y a plus d'une décennie que le chercheur Jon Kindervag de Forrester a développé le concept d'origine du modèle Zero Trust qui abandonne les réseaux internes de confiance au profit d'une idée qui considère tout le trafic du réseau comme non fiable, à l'intérieur ou à l'extérieur de ses périmètres. Son concept se résume ainsi : « **NE JAMAIS FAIRE CONFIANCE, TOUJOURS VÉRIFIER.** »

Le concept du modèle Zero Trust s'accompagne de trois principes directeurs en plus de celui de « ne jamais faire confiance » :

- Toutes les ressources doivent être accessibles de manière sécurisée, à partir d'une machine sécurisée, quel que soit l'endroit
- Le contrôle d'accès est corrélé à l'identité d'un utilisateur et à ce à quoi cet utilisateur est autorisé à accéder
- Les entreprises doivent inspecter et enregistrer tout le trafic pour vérifier que les utilisateurs se comportent correctement

Depuis sa création il y a dix ans, ce concept initial a été amélioré et repensé. Chase Cunningham a notamment insisté sur le fait que la sécurité devait être centrée sur les utilisateurs. Cette notion a été transformée en une réalité réalisable grâce aux progrès de l'identité cloud, à la sécurité des appareils, à l'essor de la gestion des identités et des accès et aux solutions de sécurité des terminaux qui servent de base au contrôle d'accès et à la sécurité modernes.



« Commencez par la sécurité des identités et des appareils. Nous constatons régulièrement que les entreprises obtiennent un succès plus rapide si elles se concentrent sur l'amélioration de la gestion des identités et de la sécurité des appareils »*.

En mettant l'accent sur l'aspect « humain » de la sécurité, l'attention se porte sur les personnes qui accèdent à votre système et sur les contrôles d'accès dont elles disposent. C'est là qu'intervient un fournisseur d'identité cloud - comme Okta - qui est très important. L'utilisation de l'identité cloud vous permet de vous assurer que les bonnes personnes ont le bon niveau d'accès aux ressources. Ces utilisateurs ont l'autorisation d'accéder à ce dont ils ont besoin pour être productifs, où et quand ils en ont besoin.

Cette approche garantit à la fois la fiabilité de l'identité de la personne qui demande l'accès et le respect des principes directeurs. Il est essentiel pour le succès de ce modèle de faire appel aux bons partenaires.

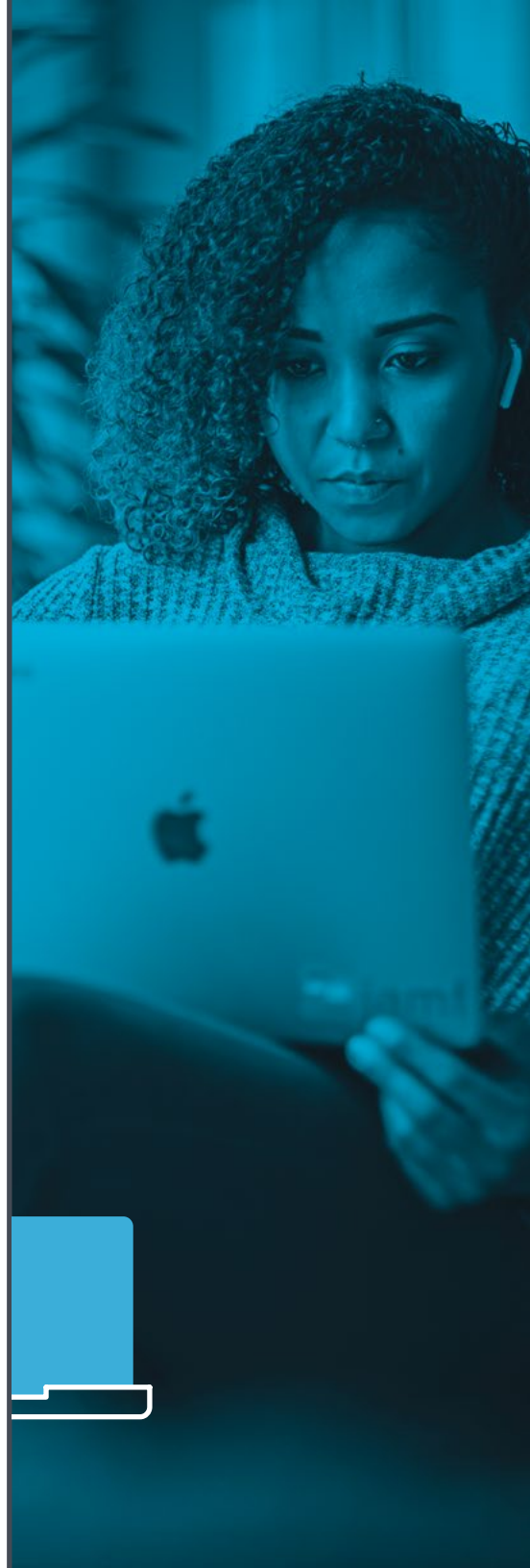
UNE MEILLEURE SÉCURITÉ GRÂCE AU MODÈLE ZERO TRUST

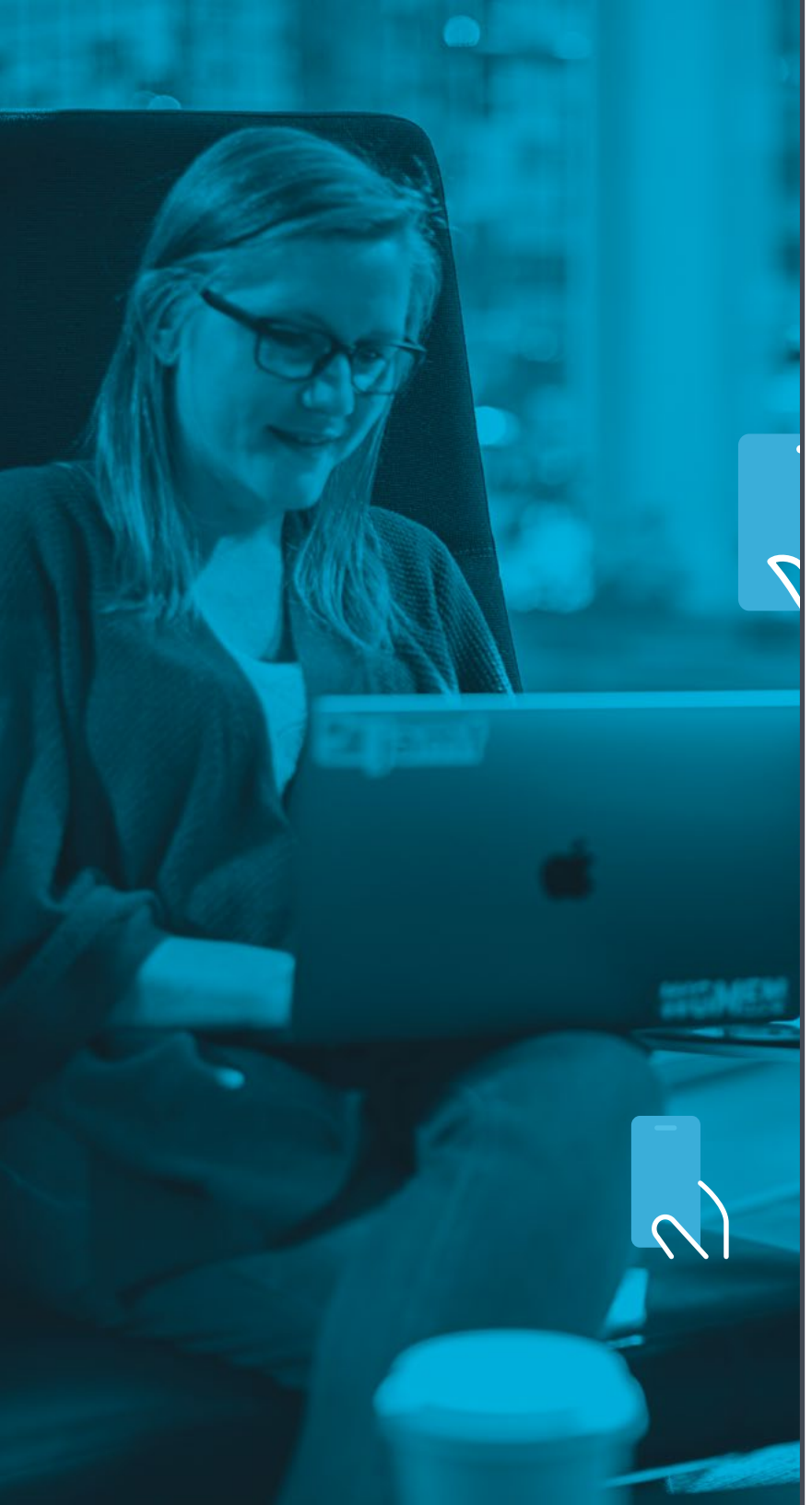
Tout comme les composants du modèle Zero Trust mettent les utilisateurs au cœur du processus, les organisations doivent tenir compte de l'expérience de ces derniers presque autant que de la sécurité elle-même. Les priorités ne sont plus « **1. SÉCURITÉ 2. EXPÉRIENCE UTILISATEUR** » **MAIS PLUTÔT « 1A. SÉCURITÉ 1B. EXPÉRIENCE UTILISATEUR ».**

Malheureusement, dans le passé, les exigences de sécurité accrues représentaient souvent une lourde charge pour les employés, les obligeant à franchir des étapes supplémentaires pour obtenir l'accès - plus maintenant.

Avec Okta Identity Cloud et Jamf Connect, les entreprises peuvent bénéficier d'un niveau élevé de confiance en regroupant les identités des applications et des appareils grâce à une connexion unique et transparente, et en offrant la possibilité de

- Approvisionnement et authentification dès le départ
- Synchroniser les informations d'identification cloud
- Accès sans mot de passe aux applications professionnelles





Jamf Connect est compatible avec la plupart des solutions de gestion des appareils mobiles

mais lorsqu'il est associé à Jamf Pro et Okta Device Trust, il permet d'empêcher un Mac ou un utilisateur non géré et non fiable d'accéder aux applications et aux informations importantes de l'entreprise. Les fonctionnalités d'Okta Device Trust permettent aux administrateurs d'exiger des utilisateurs qu'ils n'utilisent que des appareils connus et sécurisés pour accéder aux ressources et aux données de l'entreprise. La combinaison de ces trois éléments permet aux utilisateurs de se connecter, de faire vérifier leurs identifiants et d'obtenir un accès transparent et sécurisé grâce à une stratégie de sécurité à trois degrés, quel que soit l'endroit où ils se trouvent pour travailler. Au bureau, à la maison ou en déplacement, l'identité d'un utilisateur est vérifiée, il dispose de ce dont il a besoin et les équipes IT sont assurées que tout est sécurisé.

Utiliser un fournisseur d'identités comme Okta signifie que vous pouvez gérer de manière centralisée et à distance les utilisateurs, les groupes, les mots de passe et l'accès aux ressources de manière sécurisée grâce au cloud. Grâce à Jamf Connect et Jamf Pro, votre authentification unique (SSO) peut s'étendre à tous les programmes, applications et ressources de vos utilisateurs qui ont été déployés de manière sécurisée. Cela signifie que le service informatique peut savoir qu'il existe un niveau de sécurité élevé, quel que soit l'endroit d'où un utilisateur accède aux ressources.

jamf | CONNECT

okta

TESTER JAMF CONNECT

EN SAVOIR PLUS SUR OKTA

POUR ALLER PLUS LOIN : LA SÉCURITÉ DE L'APPAREIL

« NE JAMAIS FAIRE CONFIANCE, TOUJOURS VÉRIFIER » comprend également la vérification de l'appareil lui-même. La vérification de l'identité de l'utilisateur est une partie importante des efforts de sécurité, mais la vérification de la machine à partir de laquelle un utilisateur accède aux ressources ajoute une couche supplémentaire de protection. Le rapport 2019 de Symantec sur les menaces à la sécurité sur Internet a révélé qu'un appareil sur 36 utilisés dans les organisations était classé comme à haut risque. Surtout avec la popularité de BYOD. L'approche de « refus par défaut », qui consiste à s'assurer du statut de sécurité d'un appareil avant de lui donner accès à des ressources critiques, est de la plus haute importance dans un modèle Zero Trust.

Comme l'indique Venafi, « dans les environnements Zero-Trust, chaque machine doit avoir sa propre identité et il doit y avoir un moyen de vérifier que l'identité de la machine est valable pour chaque transaction. »

Heureusement, l'intégration de la Trust Protection Platform de Venafi transforme la gestion des certificats TLS et des identités de machines en un processus simple et rationnel grâce à leur nouvelle intégration avec Jamf Pro. Grâce à cette intégration, une multitude de certificats, provenant d'un nombre quelconque d'autorités de certification, peuvent être automatiquement émis ou révoqués pour des milliers d'appareils. Les profils de configuration et leur flexibilité permettent d'appliquer les configurations à des groupes spécifiques d'appareils similaires. En même temps, la plateforme de Venafi permet de gérer des règles spéciales personnalisées, ce qui offre une certaine souplesse pour les cas d'utilisation de certificats uniques. Ainsi, les appareils appartenant à l'entreprise, ou en BYOD, partagent tous le même niveau de sécurité de base avant de pouvoir accéder aux ressources WiFi, VPN ou autres ressources stratégiques. L'intégration de Venafi apporte une sécurité élevée des identités sur vos machines et appareils, complétant ainsi le cercle complet de votre modèle Zero Trust.

VENAFI®

EN SAVOIR PLUS SUR VENAFI

COMMENCEZ DÈS AUJOURD'HUI

Dans un monde mobile, le « réseau d'entreprise » ne peut plus être statique et doit s'adapter à des employés à distance. Pour certains, Microsoft Active Directory hébergé sur place demeure la seule solution qu'ils ont connue par le passé. Active Directory (AD) offre une identité et une authentification, protégeant contre les personnes extérieures à l'annuaire, mais il est restrictif et n'est plus adapté. Ce scénario exige que les utilisateurs soient sur place et dans les murs d'un bureau, mais ne fonctionne plus parce que les utilisateurs et les appareils d'aujourd'hui se trouvent entièrement en dehors de ces murs.

En éliminant le faux sentiment de sécurité derrière un pare-feu ou le périmètre de l'entreprise, les équipes informatiques et de sécurité peuvent évaluer plus fréquemment la sécurité des contrôles d'accès, des appareils et des ressources. Le passage vers des technologies modernes assure une meilleure protection des utilisateurs et des appareils, tout en améliorant la productivité des employés. En examinant les risques liés à l'accès, aux appareils et aux données, on se donne les moyens de donner aux employés à distance les outils dont ils ont besoin pour être productifs. Un accès sécurisé et fluide, de manière rationnelle et intuitive pour les utilisateurs : fidèle à la philosophie d'Apple.

Sources :

Forrester, A Practical Guide To A Zero Trust Implementation, Jan 2020
https://reprints.forrester.com/#/assets/2/53/RES157736/reports

Venafi, Why Zero Trust Requires Machine Identity Protection, May 2019
https://www.venafi.com/blog/why-zero-trust-requires-machine-identity-protection

APPLIQUER LE MODÈLE ZERO TRUST

jamf | CONNECT

ESSAYEZ JAMF CONNECT