okta

5 façons d'accélérer l'adoption du Zero Trust grâce à l'identité

De plus en plus, les responsables sécurité et les experts IT se tournent vers le modèle de sécurité Zero Trust axé sur la gestion des identités et des accès. Découvrez comment celui-ci aide les entreprises à sécuriser le mode de travail hybride, à se protéger à long terme contre les cybermenaces croissantes et à adopter la technologie cloud à grande échelle.

99 %

des entreprises considèrent l'identité comme une composante importante, voire décisive dans leur stratégie de sécurité Zero Trust

Source : The State of Zero Trust Security 2021, Okta

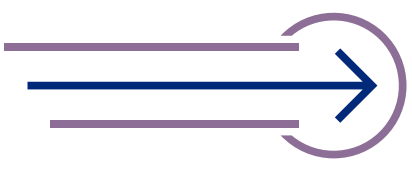
1 Optimisation de la transformation digitale

Si les entreprises accélèrent leur transition vers le cloud, fournir des accès sécurisés n'en demeure pas moins un processus long et laborieux. Optimiser la sécurité et déployer les outils et plateformes nécessaires aux collaborateurs moyennant un minimum de friction nécessite de disposer d'une plateforme moderne de gestion des identités, qui propose aux responsables IT des intégrations prêtes à l'emploi pour les applications métiers stratégiques.

97 %

des décideurs considèrent que la pandémie a accéléré la transformation digitale de leur entreprise

Source : COVID-19 Digital Engagement Report, Twilio



2 Sécurisation du mode de travail hybride

Aujourd'hui, les collaborateurs veulent être libres de travailler partout où ils se sentent à l'aise et productifs. Unifiant le contrôle des accès à toutes les applications dans le cloud et on-premise pour l'ensemble des utilisateurs, les solutions modernes de gestion des identités permettent d'offrir aux utilisateurs un accès instantané et sécurisé aux bonnes ressources, où et quand ils en ont besoin.

89 %

des collaborateurs sont partisans du télétravail au moins en temps partiel

Source : Global Workforce Hopes and Fears Survey 2022, PwC

3 Protection contre les cybermenaces les plus fréquentes

Mis sous pression par les exigences posées par des effectifs hybrides et en télétravail, les entreprises ont souvent sacrifié la sécurité au profit de la continuité de leurs activités. L'adoption d'outils modernes de gestion des identités, comme l'authentification multifacteur (MFA) et l'authentification unique (SSO), élimine rapidement les frictions liées à l'usage de mots de passe, tout en renforçant la résilience au niveau de la couche d'identités.

61 %

des cyberattaques enregistrées en 2021 impliquaient des identifiants volés ou trop faibles

Source : 2022 Data Breach Investigations Report, Verizon

4 Automatisation des processus manuels de provisioning

Alors que la technologie cloud tend à améliorer la cyber résilience, le déploiement manuel d'applications augmente le risque de brèches de données liées à l'erreur humaine. L'automatisation du provisioning grâce à l'identité fait disparaître bon nombre de ces risques, et décharge les équipes IT qui peuvent se concentrer sur le renforcement de la sécurité dans d'autres domaines.

88 %

des brèches de données de 2021 ont été causées par l'utilisation abusive d'identifiants

Source : Why Do People Make Mistakes?, Tessian

5 Protection des API et des applications

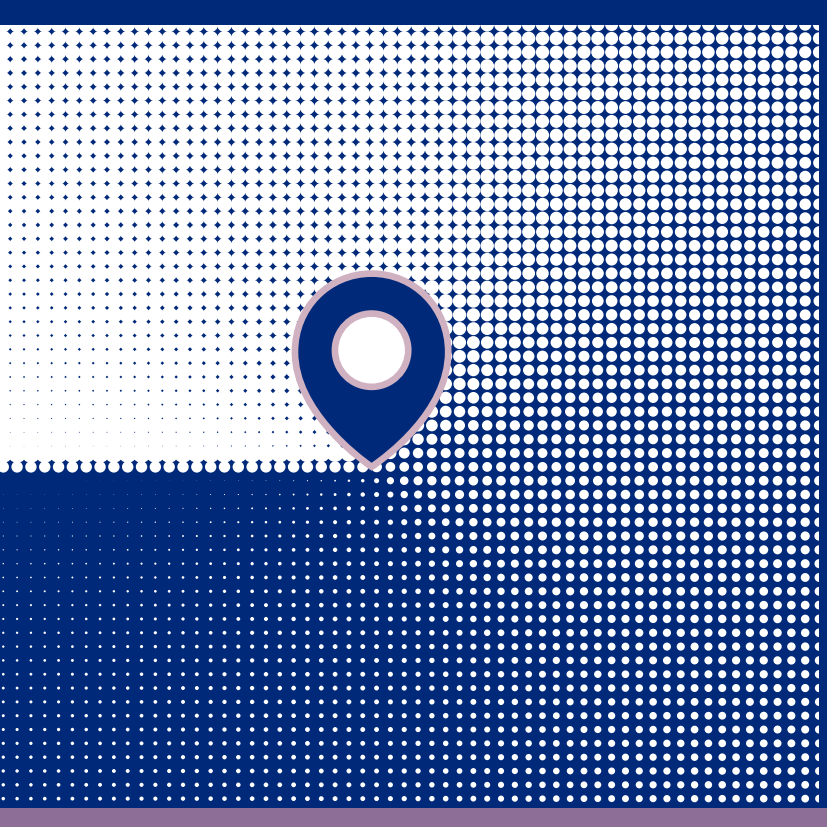
En plus de protéger vos applications, un bon fournisseur d'identité doit étendre ses contrôles d'accès sophistiqués à toutes les technologies utilisées par les collaborateurs. Il doit notamment prévoir un accès sécurisé aux API, piliers des applications actuelles mais susceptibles d'exposer les données sensibles aux dangers du Web.

Les attaques d'API ont augmenté de

681 %

au cours des 12 derniers mois

Source : State of API Security Report 2022, Salt



Par où entamer votre parcours Zero Trust ?

Si vous souhaitez en savoir plus sur la manière dont l'identité peut accélérer votre adoption du Zero Trust, ou si vous souhaitez vous positionner dans ce parcours et connaître la direction à prendre, regardez le podcast vidéo avec Brian Glick, rédacteur en chef de Computer Weekly, et Ian Lowe d'Okta.

Regarder le podcast vidéo