Okta, CrowdStrike et Zscaler proposent une solution Zero Trust intégrée, la meilleure du marché, qui offre une sécurité inter-domaines et contextuelle.

Défis

Alors que vous vous efforcez de mettre en œuvre des initiatives de transformation digitale et de soutenir votre personnel distribué, la sécurisation de vos utilisateurs, vos endpoints et vos applications est un défi permanent qui est exacerbé par l'évolution du paysage des menaces.

Les identités des utilisateurs, les endpoints, les applications et les réseaux représentent des vecteurs d'attaque primaires qui élargissent votre surface d'attaque et augmentent les risques. Les solutions de sécurité ponctuelles qui s'adressent à un domaine mais s'intègrent mal à d'autres solutions vous donnent un faux sentiment de sécurité. Une telle approche laisse des failles dans la couverture de sécurité et expose les entreprises à des cyber-risques et à des mesures correctives coûteuses. Cela explique pourquoi nous constatons une augmentation du nombre de cyberattaques en dépit des investissements supplémentaires dans les solutions de cybersécurité.

Ce dont vous avez besoin

Pendant des années, les entreprises ont tenté de surpasser leurs adversaires en multipliant les solutions de sécurité ponctuelles pour combler les lacunes de leur architecture de sécurité. Nous avons désormais atteint un point de rendement décroissant : l'ajout de produits supplémentaires multiplie la complexité, augmente les temps de réponse et, en fin de compte, nous rend moins sécurisés. Il est temps de réimaginer notre approche de la sécurité et d'utiliser la puissance de l'IA pour gagner en rapidité et en évolutivité. Disposer des bonnes solutions de sécurité avancées fonctionnant de concert de manière transparente peut offrir une approche stratifiée de la sécurité dont nous avons grand besoin, contribuer à stimuler l'efficacité opérationnelle et réduire la complexité.

Solution

L'engagement en faveur d'une approche Zero Trust, qui s'appuie sur une vérification continue en temps réel et basée sur les risques de l'identité de l'utilisateur, du contexte du terminal et de la politique commerciale, améliorera la sécurité des entreprises. Cette approche procure une plus grande simplicité, une meilleure sécurité et une plus grande agilité commerciale que les solutions de sécurité existantes ponctuelles et cloisonnées pour permettre la réussite d'une transformation digitale.

La sécurité intégrée est une sécurité puissante

Une architecture Zero Trust repose sur trois piliers fondamentaux :

Identités **Endpoints** **Applications**

Pour les entreprises qui se lancent dans une démarche Zero Trust ou qui élaborent une solution Zero Trust pour maximiser les investissements actuels, les solides partenariats et les intégrations pré-testées des leaders du marché Okta, CrowdStrike et Zscaler fournissent un modèle pour une solution Zero Trust de bout en bout, des utilisateurs aux endpoints et aux applications.

Ces intégrations garantissent aux administrateurs une vue en temps réel du paysage des menaces et de la situation de sécurité de leurs endpoints et applications.

L'accès aux applications critiques peut être modifié de manière dynamique en fonction du contexte de l'utilisateur, du terminal et des politiques d'accès. Et en cas d'attaques, des mesures correctives multiplateformes sont prises rapidement. Les défenses sont davantage renforcées par l'ajout de politiques de prévention dans toutes les intégrations pour contrecarrer de futures attaques similaires.

Le résultat net est une solution Zero Trust de pointe, cloud native et contextuelle, qui simplifie le déploiement en éliminant la complexité des solutions de sécurité bricolées tout en réduisant les risques.

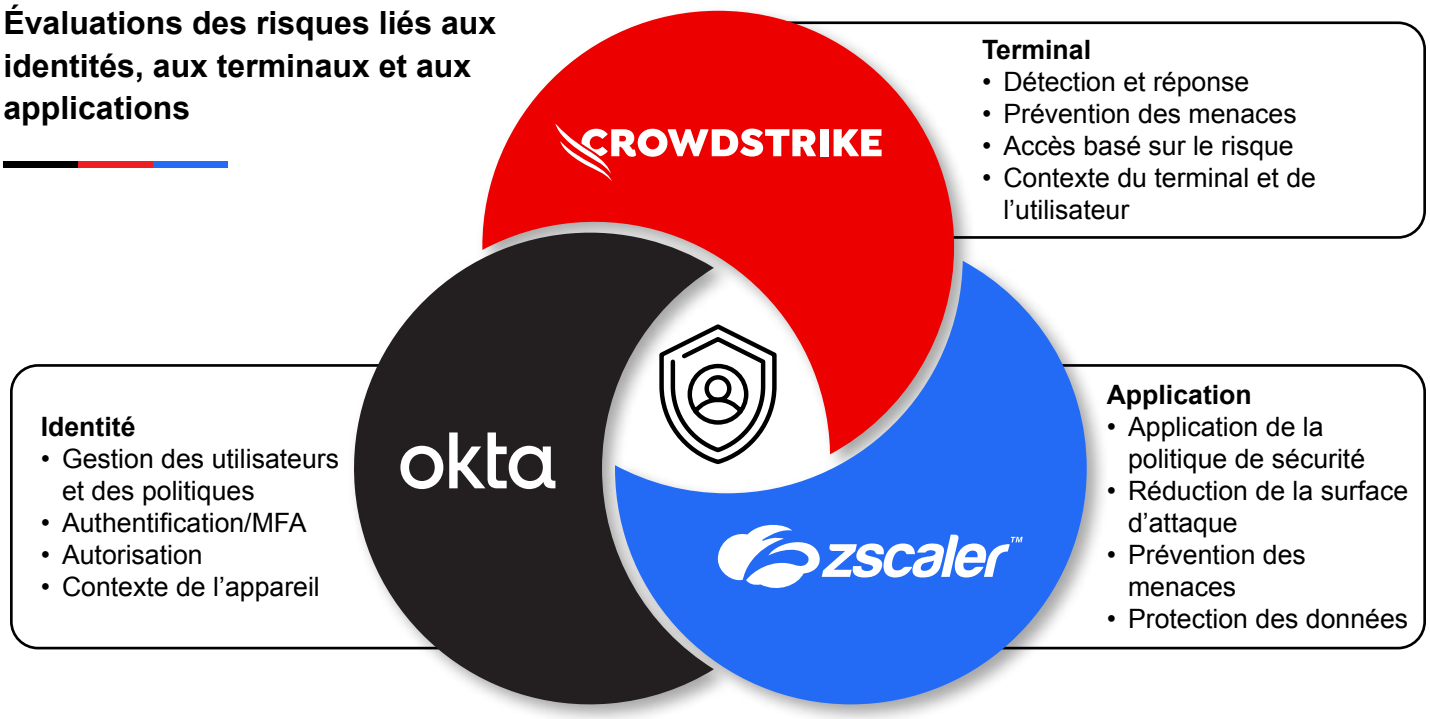
Résultats commerciaux clés

Prévention
Réduire la surface d'attaque et éviter toute compromission grâce au partage d'informations sur les menaces et de télémétrie inter-domaines pour prendre des décisions de contrôle d'accès Zero Trust et mener une vérification continue

Confinement
Assurer le confinement des menaces en temps réel en empêchant les déplacements latéraux grâce à la détection des menaces modernes, telles que la compromission des informations d'identification, les malwares de type « zero-day », les ransomwares ou les menaces internes, et en permettant l'application inter-domaines

Réponse
Accélérer la détection et la réponse aux menaces sur plusieurs domaines grâce au partage de la télémétrie contextuelle pour découvrir, trier et enquêter rapidement sur les incidents, afin de garantir une correction plus rapide et plus précise.

Évaluations des risques liés aux identités, aux terminaux et aux applications



Partage de la télémétrie et des renseignements sur les menaces

Pour en savoir plus sur nos solutions, consultez okta.com, crowdstrike.com et zscaler.fr | ©2024