Specops Device Trust : Accès Zero Trust

L'identité à elle seule ne suffit pas. Si l'accès repose uniquement sur « qui vous êtes », une simple attaque de détournement de session peut entraîner une violation, même avec la MFA. Les hackers volent des tokens de session, utilisent des appareils compromis et exploitent les failles des contrôles d'identité traditionnels.

La solution Specops Device Trust : Authentifier et vérifier l'utilisateur et l'appareil à chaque point d'accès, et de manière continue tout au long de la session.

Authentification

- Liaison des identités aux appareils autorisés
- Blocage des identifiants volés sur les appareils de l'attaquant

Vérification

- Contrôle de la sécurité des appareils tout au long des sessions
- Friction minimale pour l'utilisateur, sans MDM invasif

Remédiation

- Remédiation rapide en libre-service, sans tickets IT
- Corrections en un clic et périodes de tolérance pour l'utilisateur

Déploiement et intégration

- **Systèmes d'exploitation :** Windows, macOS, Linux, iOS, Android
- **Intégration IdP :** Okta, Azure AD/Microsoft Entra ID, Ping Identity
- **Modèle de déploiement :** SaaS Cloud (disponibilité > 99,99 %)
- **Impact sur les performances :** Aucun ralentissement pour les utilisateurs
- **Options de déploiement :** Déploiement progressif par groupe d'utilisateurs, type d'appareil ou plateforme OS

Différences avec les solutions MDM

Capacité	Infinipoint	Solutions MDM
Décision d'accès en temps réel lors de l'authentification, plutôt que des contrôles de conformité périodiques	✓	✗
Vérification continue tout au long de la session, et pas uniquement lors de la connexion	✓	✗
Correction des failles par l'utilisateur plutôt que le blocage des accès	✓	✗
Compatibilité avec BYOD sans installation invasive	✓	✗
Intégration directe aux IdPs pour une authentification fluide	✓	✗

Fonctionnalités principales

Fonctionnalités	Avantages
Zero Device Trust Verification	Vérification en continu de la posture des appareils à chaque demande d'accès et tout au long de la session, grâce à des centaines de contrôles granulaires.
MFA résistant au phishing	Association des utilisateurs à leurs appareils de confiance. L'authentification est autorisée uniquement depuis des appareils approuvés et enrôlés afin de prévenir les prises de contrôle de comptes.
Verrouillage utilisateur-appareil	Enrôlement des appareils approuvés et association de chaque utilisateur à son matériel autorisé. Contrôle du nombre, du type (ordinateur, mobile) et de la classification des appareils (entreprise, BYOD) autorisés par utilisateur ou par groupe.
Vérification continue de la posture	Vérification de la posture des appareils à chaque connexion et toutes les 10 minutes pendant la session. Détection des menaces actives, des contrôles de sécurité désactivés et des non-conformités.
Remédiation en un clic	Remédiation par les utilisateurs des problèmes de conformité (« Activation du chiffrement », « Mise à jour du système », « Activation du pare-feu ») avec des périodes de tolérance configurables. Réduction significative des tickets de support IT tout en maintenant la sécurité.
Sécurité des appareils tiers	Identification des appareils accédant à votre réseau, qu'il s'agisse de BYOD ou de dispositifs utilisés par des prestataires. Visibilité complète sur l'ensemble des appareils accédant à votre environnement, qu'ils soient gérés par l'entreprise ou non, y compris le shadow IT.
Politiques basées sur le risque	Définition de politiques granulaires pour chaque utilisateur, type d'appareil, système d'exploitation et état de conformité, avec un accès dynamique adapté à la santé actuelle de l'appareil.

Découvrez comment fonctionne Specops Device Trust

En savoir plus : https://specopssoft.com/fr/produits/specops-device-trust/
Demander une démo : https://specopssoft.com/fr/contact/