SentinelOne

FICHE TECHNIQUE

Singularity RangerAD

Évaluer, détecter et corriger l'exposition aux menaces d'Active Directory

Active Directory et Azure AD sont fréquemment la cible de cyberattaques visant les identités. Et pour cause : leur compromission permet aux attaquants de se positionner dans l'environnement de l'entreprise de manière à élargir leurs accès, s'implanter de façon persistante, élever leurs privilèges, identifier d'autres cibles et se déplacer latéralement.

SentinelOne Singularity Ranger AD est une solution d'évaluation de la configuration des identités. Composant de la plateforme Singularity XDR, elle identifie les vulnérabilités et les problèmes de configuration d'Active Directory (AD) et d'Azure AD, ainsi que les menaces actives qui ciblent ces annuaires. Ranger AD fournit des informations prédictives et exploitables sur l'exposition des identités au sein de votre organisation, et vous aide ainsi à réduire le risque de compromission et à mettre vos ressources en conformité avec les bonnes pratiques de sécurité.

Analyse continue de l'exposition des identités

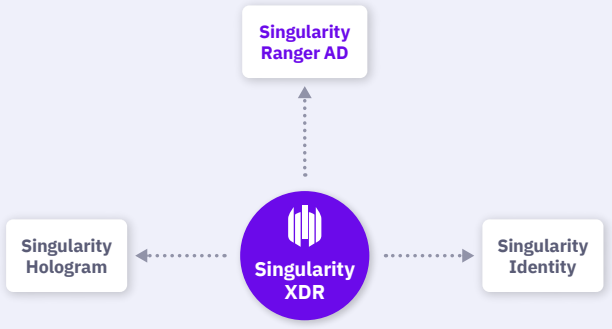
Oubliez les audits onéreux et manuels. Identifiez automatiquement les expositions critiques au niveau de vos utilisateurs, de vos ressources et de vos domaines dans Active Directory et Azure AD.

Réduction de la surface d'attaque d'Active Directory

Analysez les modifications de configuration pour vérifier si elles sont conformes aux bonnes pratiques et supprimez les privilèges excessifs grâce à des recommandations directement exploitables, afin de corriger rapidement les risques.

Détection des indicateurs d'attaques actives ciblant Active Directory

Surveillez de façon proactive AD et Azure AD pour détecter les activités indiquant des attaques potentiellement en cours, à la fois en continu et à la demande.



Composants de la solution ITDR

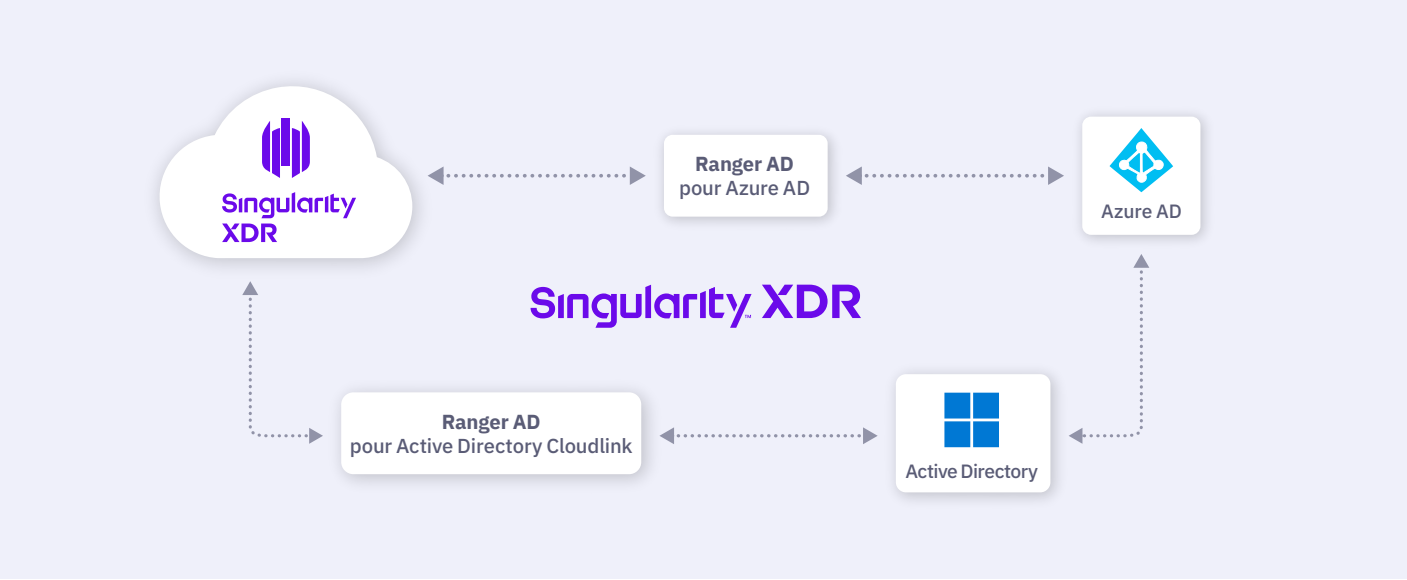
Simple à déployer, Ranger AD fournit rapidement des pistes pour renforcer la sécurité des implémentations Active Directory et Azure AD, réduisant ainsi la surface d'exposition de vos identités.

Pour plus informations, consultez **s1.ai/ranger-ad**.

84 % des entreprises ont été victimes d'une compromission liée aux identités. Ranger AD vous procure les informations exploitables nécessaires pour réduire l'exposition de vos identités.

PRINCIPAUX AVANTAGES ET FONCTIONNALITÉS

+ Éliminez proactivement les risques liés aux identités.
+ Analysez la conformité aux bonnes pratiques de vos configurations Active Directory et Azure AD.
+ Identifiez les erreurs de configuration préjudiciables à la sécurité d'Active Directory et d'Azure AD.
+ Détectez les expositions au niveau du domaine, des ressources et des utilisateurs.
+ Soyez averti de toute activité suspecte de modification d'Active Directory.
+ Réduisez les délais de détection des attaques ciblant les identités.
+ Bénéficiez de la visibilité optimale et de la flexibilité offertes par une fonction de surveillance en continu ou à la demande destinée à détecter les attaques en cours.
+ Annulez les effets des comportements malveillants automatiquement, grâce au moteur basé sur des scripts de correction automatisés.



Réduction de la surface d'attaque d'Active Directory et renforcement de la résilience

Ranger AD analyse votre configuration AD pour vérifier sa conformité aux bonnes pratiques et vous recommande les mesures à prendre pour corriger rapidement tout privilège excessif à l'échelle de l'organisation. La solution contribue ainsi à réduire efficacement votre surface d'attaque. Gérer ou corriger de manière proactive les failles de sécurité identifiées par Ranger AD permet à votre équipe d'optimiser son approche de la sécurité à long terme.

RETOUR SUR INVESTISSEMENT PLUS RAPIDE

+ Déploiement flexible : on-premise ou SaaS
+ Couverture flexible : Active Directory sur site, Azure AD et environnements multicloud
+ Implémentation qui ne bloque pas l'efficacité opérationnelle, produisant des résultats rapides et immédiatement exploitables
+ Couverture de protection complète pour Active Directory sur site, Azure AD et environnements multicloud
+ Sécurité maximale avec un minimum de ressources : la solution ne nécessite qu'un seul endpoint et aucun accès à privilèges

Des centaines de contrôles en temps réel

Au niveau du domaine

+ Stratégies trop laxistes
+ Collecte d'identifiants
+ Vulnérabilités Kerberos

Au niveau des équipements

+ Contrôleurs de domaine non approuvés
+ Problèmes liés au système d'exploitation
+ Vulnérabilités Active Directory

Au niveau des utilisateurs

+ Identifiants
+ Comptes à privilèges
+ Comptes obsolètes
+ Identifiants partagés

Innovation. Fiabilité. Reconnaissance.

Gartner

Leader du Magic Quadrant 2021 consacré aux plateformes de protection des endpoints

MITRE ENGENUITY

Résultats exceptionnels à l'évaluation ATT&CK

- 100 % de protection. 100 % de détection
- Couverture analytique exceptionnelle 3 ans de suite
- 100 % en temps réel, 0 retard

Gartner peerinsights 4,9 ★★★★★

99 % des évaluateurs de Gartner Peer Insights™ pour les solutions EDR recommandent SentinelOne Singularity

FedRAMP · AICPA SOC · TEVORA PCI DSS Attestation HIPAA Attestation · VB 100 VIRUS · AAA · SE Labs BEST Innovator WINNER 2021

À propos de SentinelOne

SentinelOne (NYSE : S) propose une cybersécurité autonome de pointe, capable de prévenir, détecter et neutraliser les cyberattaques plus rapidement et plus précisément que jamais. Sa plateforme Singularity XDR protège les grandes entreprises mondiales en leur offrant visibilité en temps réel sur les surfaces d'attaque, corrélation entre plateformes et réponse aux incidents optimisée par l'intelligence artificielle. Vous disposez ainsi de plus de fonctionnalités, tout en réduisant la complexité de votre écosystème de sécurité.

fr.sentinelone.com

sales@sentinelone.com
+ 1 855 868 3733