SentinelOne

SCHEDA TECNICA

Singularity RangerAD

Valutate, intercettate e risolvete le minacce rivolte ad Active Directory

AD e Azure AD sono obiettivi comuni degli attacchi informatici basati sulle identità. La loro compromissione può fornire agli hacker la possibilità di ampliare privilegi e opportunità di accesso, stabilire la persistenza, identificare altri obiettivi e spostarsi lateralmente.

SentinelOne Singularity Ranger AD, un componente della piattaforma Singularity XDR, è una soluzione di valutazione delle configurazioni relative alle identità che identifica le configurazioni errate, le vulnerabilità e le minacce attive rivolte ad Active Directory (AD) e ad Azure AD. Fornendovi informazioni prescrittive e fruibili sulle esposizioni della superficie di attacco relativa alle identità, Ranger AD vi aiuta a ridurre il rischio di compromissione e a garantire che le vostre risorse siano in linea con le best practice di sicurezza.

Analizzate in modo continuo l'esposizione delle identità

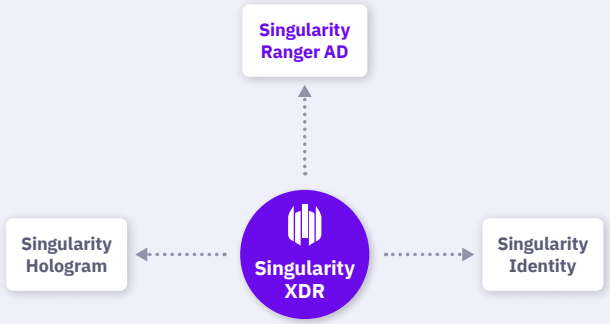
Evitate i costosi audit manuali. Individuate automaticamente le esposizioni critiche a livello di dominio, dispositivo e utente in Active Directory e Azure AD.

Riducete la superficie di attacco di AD

Analizzate le modifiche della configurazione per garantire la conformità alle best practice e sfruttate indicazioni operative fruibili per applicare correzioni rapide ed eliminare i privilegi eccessivi.

Rilevate gli indicatori di attacchi attivi rivolti ad AD

Monitorate in modo proattivo AD e Azure AD per rilevare attività che indichino attacchi potenzialmente attivi, sia su base continuativa che on-demand.



Componenti dell'identità

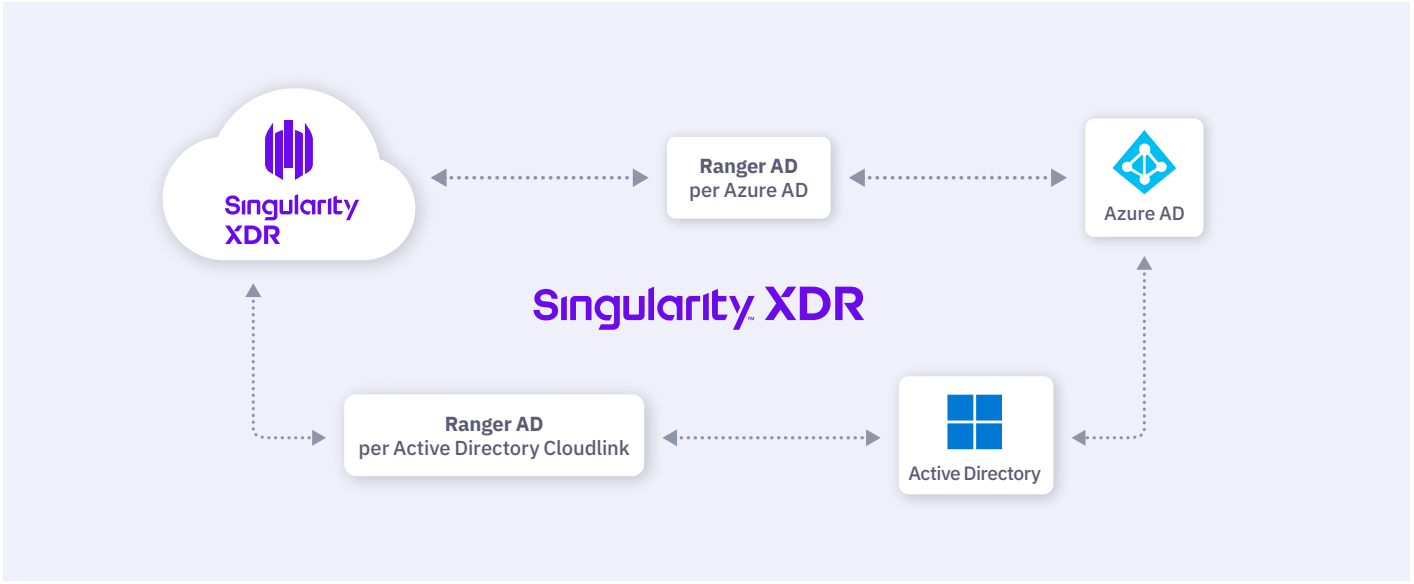
Ranger AD è semplice da implementare e fornisce informazioni rapide e fruibili su come rafforzare la sicurezza delle implementazioni di Active Directory e Azure AD, riducendo la superficie di attacco delle identità.

Per maggiori informazioni, visitate **s1.ai/ranger-ad**

L'**84%** delle organizzazioni ha subito una violazione delle identità. Ranger AD fornisce informazioni utili per ridurre tale esposizione.

FUNZIONALITÀ E VANTAGGI PRINCIPALI

+ Affrontate in modo proattivo il rischio basato sulle identità
+ Confrontate le configurazioni di AD e Azure AD con le best practice
+ Rilevate le configurazioni di sicurezza errate di AD e Azure AD
+ Scoprite le esposizioni a livello di dominio, dispositivo e utente
+ Ottenete informazioni su modifiche sospette ad AD
+ Riducete il tempo medio di correzione (MTTR) degli attacchi basati sulle identità
+ Ottenete visibilità e flessibilità grazie al monitoraggio continuo e on-demand degli attacchi attivi rivolti ad AD
+ Eseguite il ripristino della versione precedente in caso di comportamento dannoso utilizzando un motore di script di correzione



Riducete la superficie di attacco di AD e create un ambiente resiliente

Ranger AD analizza la configurazione di AD per verificarne la conformità alle best practice e vi offre indicazioni per la correzione rapida di eventuali privilegi eccessivi all'interno dell'organizzazione, consentendovi di ridurre in modo concreto la superficie di attacco. Colmare o correggere in modo proattivo le lacune identificate da Ranger AD può migliorare il profilo di sicurezza a lungo termine del vostro team.

Centinaia di controlli in tempo reale

Livello del dominio

+ Criteri deboli
+ Raccolta di credenziali
+ Vulnerabilità di Kerberos

Livello del dispositivo

+ Controller di dominio inaffidabili
+ Problemi del sistema operativo
+ Vulnerabilità di AD

Livello dell'utente

+ Analisi delle credenziali
+ Account con privilegi
+ Account obsoleti
+ Credenziali condivise

TIME-TO-VALUE RAPIDO

+ Implementazione flessibile: on-premise e SaaS
+ Copertura flessibile: AD on-premise, Azure AD e multi-cloud
+ Implementazione a basso impatto e risultati rapidi e fruibili
+ Ottenete la copertura completa per ambienti Active Directory, Azure AD e multicloud on-premise
+ Ottenete la massima sicurezza con risorse minime: è necessario un solo endpoint e non sono richieste credenziali con privilegi

Innovazione. Affidabilità. Reputazione.

Gartner

Leader nel 2021 Magic Quadrant per le piattaforme di protezione degli endpoint

MITRE ENGENUITY

Valutazione record di ATT&CK

- 100% di protezione. 100% di rilevamento.
- Copertura analitica eccellente per 3 anni consecutivi
- 100% dei rilevamenti in tempo reale, senza alcun ritardo

Gartner peerinsights. 4,9 ★★★★★

99% in Gartner Peer Insights™

I recensori di EDR consigliano SentinelOne Singularity

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

Informazioni su SentinelOne

SentinelOne (NYSE:S) è all'avanguardia nella sicurezza informatica automatizzata e previene, rileva e risponde agli attacchi informatici in modo più rapido e preciso che mai. La nostra piattaforma Singularity XDR protegge e supporta le aziende leader a livello mondiale offrendo loro visibilità in tempo reale sulle superfici di attacco, correlazione tra piattaforme e risposte basate sull'intelligenza artificiale. Ottenete più funzionalità e meno complessità.

sentinelone.com

sales@sentinelone.com
+ 1 855 868 3733