SentinelOne

DATENBLATT

Singularity RangerAD

Bedrohungen für Ihr Active Directory bewerten, erkennen und stoppen

AD und Azure AD sind häufige Ziele von identitätsbasierten Cyberangriffen. Ihre Kompromittierung kann dazu führen, dass Angreifer ihre Zugriffsmöglichkeiten erweitern, Persistenz erzielen, Zugriffsrechte ausweiten, weitere Ziele identifizieren und sich lateral im Netzwerk bewegen können.

SentinelOne Singularity Ranger AD, eine Komponente der Singularity XDR-Plattform, identifiziert falsche Konfigurationen, Schwachstellen und aktive Bedrohungen für Active Directory (AD) sowie Azure AD und bewertet dadurch die Konfiguration Ihrer Identitätsumgebung. Ranger AD liefert normative, verwertbare Erkenntnisse zu Risiken für Ihre Identitätsangriffsfläche, hilft Ihnen bei der Reduzierung des Kompromittierungsrisikos und gewährleistet, dass Ihre Assets die Best Practices für Sicherheit einhalten.

Kontinuierliche Analyse von Identitätsbedrohungen

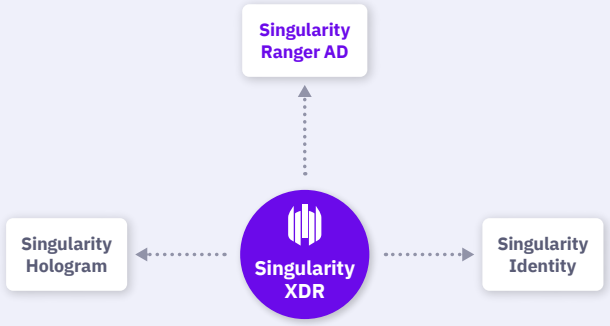
Sie können auf teure und manuelle Audits verzichten. Schwerwiegende Schwachstellen in Active Directory und Azure AD werden auf Domänen-, Geräte- und Benutzerebene automatisch identifiziert.

Reduzierung Ihrer AD-Angriffsfläche

Analysieren Sie Konfigurationsänderungen, um Best Practices einzuhalten, und beseitigen Sie zu umfangreiche Berechtigungen basierend auf praktischen Empfehlungen, um Probleme schnell zu beheben.

Erkennung von Indikatoren für aktive AD-Angriffe

Sie können AD und Azure AD sowohl kontinuierlich als auch bei Bedarf proaktiv auf Aktivitäten überwachen, die auf mögliche aktive Angriffe hindeuten.



Identitätsschutzkomponenten

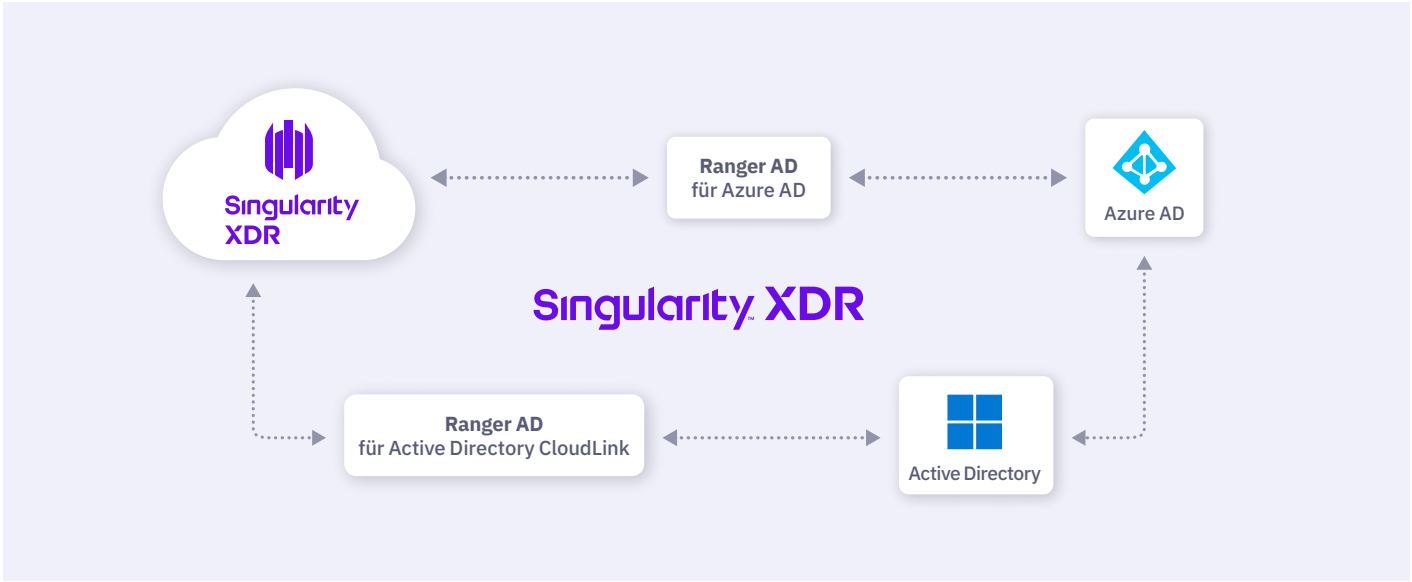
Ranger AD lässt sich einfach bereitstellen, liefert schnelle, verwertbare Erkenntnisse zur Absicherung der Active Directory- und Azure AD-Implementierungen und reduziert dadurch die Angriffsfläche Ihrer Identitätsumgebung.

Weitere Informationen unter **s1.ai/ranger-ad**

84 % der Unternehmen haben bereits eine identitätsbezogene Sicherheitsverletzung verzeichnet. Ranger AD stellt verwertbare Informationen bereit, mit denen Sie diese Risiken reduzieren können.

WICHTIGE FUNKTIONEN UND VORTEILE

+ Proaktive Reduzierung identitätsbasierter Risiken
+ Vergleich Ihrer AD- und Azure AD-Konfigurationen mit Best Practices
+ Erkennung fehlerhafter AD- und Azure AD-Sicherheitskonfigurationen
+ Identifizierung von Risiken auf Domänen-, Geräte- und Benutzerebene
+ Sofortige Benachrichtigungen bei verdächtigen AD-Änderungen
+ Reduzierung der MTTR bei identitätsbasierten Angriffen
+ Mehr Transparenz und Flexibilität durch kontinuierliche und bedarfsbasierte Überwachung auf aktive AD-Angriffe
+ Rollback bei schädlichem Verhalten mithilfe einer Scripting-Engine für Wiederherstellungen



Reduzierung Ihrer AD-Angriffsfläche und Aufbau von Resilienz

Ranger AD analysiert Ihre AD-Konfiguration im Hinblick auf die Best Practices, begleitet Sie bei der schnellen Korrektur übermäßig umfangreicher Berechtigungen im gesamten Unternehmen und verringert dadurch wirksam Ihre Angriffsfläche. Das proaktive Schließen der von Ranger AD identifizierten Lücken kann die langfristige Sicherheitslage Ihres Unternehmens erheblich verbessern.

SCHNELLE EINSATZBEREITSCHAFT

+ Flexible Bereitstellung: lokal und als SaaS
+ Flexible Abdeckung: lokales AD, Azure AD und Multi-Cloud
+ Implementierung mit minimalen Reibungsverlusten und schnellen, verwertbaren Ergebnissen
+ Vollständige Abdeckung lokaler Active Directory-, Azure AD- und Multi-Cloud-Umgebungen
+ Maximale Sicherheit mit minimalen Ressourcen: erfordert nur ein Endgerät und keine privilegierten Anmeldedaten

Hunderte Echtzeitprüfungen

Domänenebene

+ Schwache Richtlinien
+ Erfassung von Anmeldedaten
+ Kerberos-Schwachstellen

Geräteebene

+ Nicht autorisierte Domänen-Controller
+ Betriebssystem-probleme
+ AD-Schwachstellen

Benutzerebene

+ Anmeldedaten-analyse
+ Privilegierte Konten
+ Inaktive Konten
+ Gemeinsam genutzte Anmeldedaten

Innovativ. Vertrauenswürdig. Anerkannt.

Gartner

Führender Anbieter im 2021 Magic Quadrant für Endpoint Protection-Plattformen

MITRE ENGENUITY

Rekordergebnis bei der ATT&CK-Bewertung

- 100 % Schutz. 100 % Erkennung.
- Höchste analytische Abdeckung 3 Jahre in Folge
- 100 % Echtzeit und keinerlei Verzögerungen

Gartner peerinsights 4,9 ★★★★★

99 % BEI GARTNER PEER INSIGHTS™

EDR-Analysten empfehlen SentinelOne Singularity

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

Informationen zu SentinelOne

SentinelOne (NYSE:S) ist ein Vorreiter auf dem Gebiet der autonomen Cybersicherheit und verhindert, erkennt und stoppt Cyberangriffe schneller und genauer als je zuvor. Unsere Singularity XDR-Plattform schützt und stärkt weltweit führende Unternehmen mit einem Echtzeitüberblick über Angriffsflächen sowie mit plattformübergreifender Korrelation und KI-gestützten Reaktionen. Nutzen Sie mehr Optionen mit geringerer Komplexität.

sentinelone.com

sales@sentinelone.com
+ 1 855 868 3733