SentinelOne

DATENBLATT

Singularity™ | IDENTITY

Erkennung und Abwehr von Identitätsbedrohungen in Echtzeit

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

Singularity Identity™ Threat Detection & Response (ITDR), eine Komponente der SentinelOne Singularity XDR-Plattform, schützt die Active Directory- und Azure AD-Domänen-Controller sowie mit der Domäne verbundene Endpunkte in Echtzeit vor Angreifern, die sich Berechtigungen verschaffen und verdeckt agieren wollen. Singularity Identity erweitert die Singularity XDR-Schutzfunktionen mithilfe von Sentinel-Agenten, die Microsoft AD-Domänen-Controller und Endbenutzer-Endpunkte sichern.

Schutz Ihrer Domäne

Erkennen Sie Active Directory-Angriffe von jedem Gerätetyp oder Betriebssystem, einschließlich IoT und OT, und stellen Sie bedingten AD-Zugriff mit MFA-Partnerlösungen bereit.

Keine Chance für Bedrohungsakteure

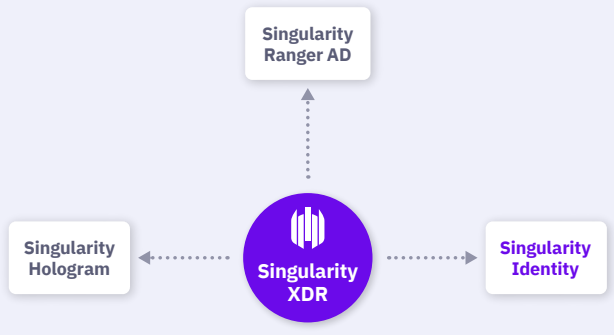
Lenken Sie Angreifer von den AD-Schätzen ab und führen Sie sie in die Irre.

Tarnung, Ablenkung, Schutz

Verstecken Sie Anmelde- und Produktionsdaten und erschweren Sie gleichzeitig laterale Bewegungen.

Erweiterung und Erfassung

Integrieren Sie Singularity Hologram™-Netzwerkköder, um netzwerkinterne Angreifer und Insider-Bedrohungen weiter auszubremsen.



Identitätsschutzkomponenten

Singularity Identity Sentinel-Agenten verhindern, dass Angreifer Zugriff auf die Active Directory- und Azure AD-Schätze erhalten – sowohl lokal als auch in der Cloud.

Weitere Informationen unter **s1.ai/identity**

84 % der Unternehmen haben bereits eine identitätsbezogene Sicherheitsverletzung verzeichnet. Singularity Identity Sentinel-Agenten schützen die Identität in Echtzeit.

WICHTIGE FUNKTIONEN UND VORTEILE

+ Echtzeiterkennung von Active Directory- und Azure AD-basierten Cyberidentitätsangriffen, einschließlich Ransomware
+ Einfache Implementierung mit minimalen Reibungsverlusten; unterstützt lokale Active Directory-, Azure AD- und Multi-Cloud-Umgebungen
+ Schutz vor Identitätsangriffen und für alle verwalteten oder nicht verwalteten Ressourcen in allen Betriebssystemen, einschließlich IoT- und OT-Geräte
+ Tarntechnologie, die Angreifer in die Irre führt und wertvolle Anmeldedaten schützt
+ Verwertbare Erkenntnisse zu Lücken in Ihrer Identitäts-angriffsfläche (einschließlich Konfigurationsfehlern), Zugriffskontrollen, Richtlinien-verletzungen und mehr
+ Integration mit Singularity Hologram-Täuschungs-technologien für den Einsatz von Ködern im Netzwerk und zur Erfassung von Bedrohungsdaten

Anmeldedaten zuverlässig schützen, schnell Mehrwert erzielen

Legen Sie mit den schnellen, reibungslosen und flexiblen Bereitstellungsoptionen sofort los: Singularity Identity ermöglicht die vollständige Abdeckung lokaler AD-, Azure AD- und Multi-Cloud-Umgebungen. Erzielen Sie schnelle Fortschritte bei der Verbesserung Ihrer Sicherheit, indem Sie den Zugriff auf lokale Speicher für Anwendungsanmeldedaten schützen und beschränken, Ihre Identitätsrisiken erkennen und Kontrollen implementieren, um Angreifer abzuwehren.

UNTERSTÜTZUNG UND DURCHSETZUNG VON ZERO TRUST MIT SINGULARITY IDENTITY

+ Beschränkung des impliziten Vertrauens bei Anwendungen und Datenressourcen
+ Identifizierung von Identitätsrisiken von Endpunkten, AD und Cloud
+ Erkennung von Identitäts-angriffen auf Endpunkten und Domänen-Controllern
+ Beschränkung des Zugriffs auf vertrauenswürdige und validierte Anwendungen
+ Unterstützung bedingter AD-Zugriffe über MFA-Partner

Funktionen von Singularity Identity

01 | Identitätsschutz auf dem Domänen-Controller

Der Singularity Identity Sentinel-Agent für AD und Azure AD erkennt Identitätsangriffe aus der gesamten Domäneninfrastruktur. Singularity Identity liefert detaillierte, verwertbare Einblicke, wenn Angriffe von verwalteten oder nicht verwalteten und möglicherweise kompromittierten Geräten – auch aus dem IoT und der OT – ausgehen, und zwar unabhängig von ihrem Betriebssystem oder Standort. Über die Integration mit MFA-Drittanbietern stellt der Sentinel-Agent auch bedingten AD-Zugriff bereit.

02 | Identitätsschutz auf dem Endpunkt

Der Singularity Identity Sentinel-Agent für Endpunkte erkennt Identitätsmissbrauchs- und Erkundungsaktivitäten in Endpunktprozessen, die sich gegen kritische Domänen-Server, Dienstkonten, lokale Anmeldedaten, lokale Daten, Netzwerkdaten und Cloud-Daten richten. Tarn- und Täuschungs-techniken im Agenten bremsen den Angreifer aus und informieren gleichzeitig über die Lage.

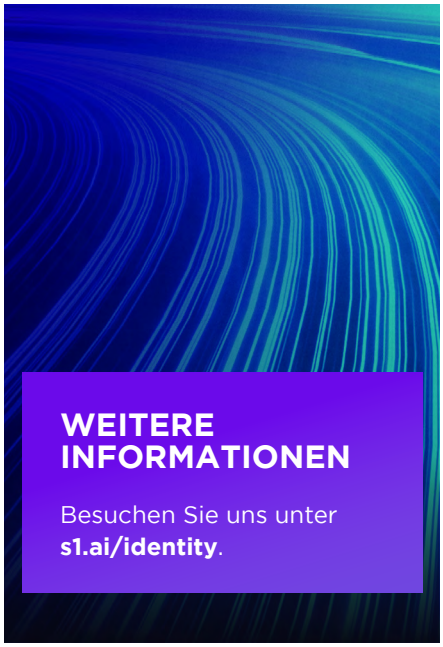
Singularity Identity bildet mit Singularity Hologram™ eine komplette Täuschungs- und Identitätslösung.

03 | Stoppen lateraler Bewegungen

Hindern Sie Angreifer – einschließlich Ransomware – am Vormarsch, indem Sie an jeder Ecke Fallen aufstellen. Mit Singularity Identity können Sie den Diebstahl privilegierter Anmeldedaten (z. B. für wertvolle Benutzer-, Dienst- und Systemkonten) verhindern. Nicht autorisierte Netzwerkerkundung und Fingerprinting verlieren für Angreifer praktisch ihren Sinn, weil legitime Daten durch Köderdaten ersetzt werden. Durch die Integration mit Singularity Hologram können Sie auch laterale Bewegungsversuche zu Netzwerkködern umleiten.

04 | Aufdecken von Angriffspfaden

Singularity Identity hilft Ihnen, verborgene Faktoren zu erkennen und zu verstehen, die Ihre Umgebung für Identitätsangriffe anfällig machen. Dazu gehören gefährdete Angriffsflächen, verwaiste Anmeldedaten und Richtlinienverletzungen. Unterstützt durch grafische topografische Karten zeigt Singularity Identity, wie Angreifer sich in Systemen bewegen könnten, um an die kritischen Ressourcen zu gelangen. Mit diesen Einblicken können Ihre Sicherheits- und IT-Teams den Weg zu den kritischen Ressourcen blockieren und Ihre Abwehr mithilfe von Täuschungstechnologien stärken.



WEITERE INFORMATIONEN

Besuchen Sie uns unter **s1.ai/identity**.

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