

SentinelOne Ranger®

Cloud-basierte Netzwerktransparenz und -kontrolle

Die Verbreitung von IoT in Unternehmen, laxe BYOD-Richtlinien und eine große Anzahl an Mitarbeitern, die von unterwegs oder im Homeoffice arbeiten – all diese Faktoren führen dazu, dass zahlreiche nicht verwaltete internetfähige Geräte mit der Unternehmensinfrastruktur verbunden werden. Es bedarf nur eines kompromittierten Druckers, der von einem Kriminellen als Ausgangspunkt für Spionage, laterale Bewegungen und Breaches missbraucht wird.

Zur Minimierung dieses Risikos bietet SentinelOne die Agentenkomponente Ranger® an, die als Bestandteil unserer Singularity-Plattform implementiert wird und jeden Endpunkt in einen Netzwerksensor verwandelt. Mit den Sentinel Ranger-Sensoren können Sie die Angriffsfläche des Unternehmensnetzwerks kontrollieren, indem Sie alle gerätebasierten Bedrohungen in Echtzeit erkennen, identifizieren und eindämmen. Ihre Endpunkte können die Computing-Infrastruktur jetzt autonom vor IoT-Angriffen, kompromittierten Geräten und Schwachstellen schützen – ganz ohne Hardware und ohne Netzwerkänderungen. Sie müssen lediglich Ranger® in der Endpunktrichtlinie aktivieren. Die Sentinel-Agenten übernehmen den Rest.

Wichtigste Vorteile

- + Für Großunternehmen geeignete Netzwerkkontrolle und Inventare
- + Erkennung neuer Geräte in sensiblen Umgebungen – einschließlich Warnmeldung
- + Kontrolle der Netzwerk-Angriffsfläche durch Isolierung gerätebasierter Bedrohungen
- + Suche nach verdächtigen Netzwerkgeräten im gesamten Unternehmen

Erhebliches Problem – praktisch reibungslose Lösung

SentinelOne Ranger® bietet Transparenz und zentrale Kontrolle für das gesamte Netzwerk, bei minimalen Reibungsverlusten. Ranger® ist eine Komponente unseres Sentinel-Agenten, die Sie lediglich aktivieren müssen. Dank Ranger® gehören zusätzliche, spezialisierte Agenten, SPAN- und TAP-Ports und Netzwerkgeräte und Tools für Netzwerktransparenz zum alten Eisen. Auch die mühsame manuelle Erfassung des Datenverkehrs und das Hochladen zur Analyse entfallen. Ranger® führt diese Schritte automatisch durch.



RANGER

Ranger® ist Netzwerktransparenz und -kontrolle mit einem Klick

WICHTIGE UNTERSCHIEDSMERKMALE VON RANGER®

- + Netzwerktransparenz mit einem Mausklick
- + Kontrolle über unbekannte und IoT-Netzwerkgeräte mit einem Mausklick
- + Keine zusätzliche Software
- + Keine neue Hardware
- + Keine Netzwerkänderungen
- + Aktive und passive Scans
- + Pro Subnetz detailliert konfigurierbar



“

Die Konfiguration und Implementierung waren extrem einfach. Das Cloud-Dashboard lässt sich leicht bedienen.

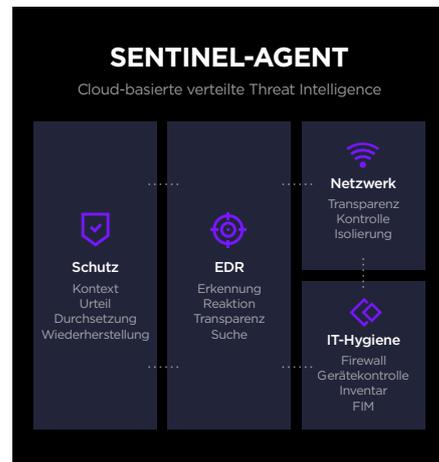
250 Mio. bis 500 Mio. USD

2. Juli 2020

Cloud-basierte Netzwerkkontrolle

Die SentinelOne Singularity-Plattform bietet über die Cloud verwaltete verteilte Threat Intelligence. Unsere hervorragenden Funktionen für Endpunkt-Sicherheit, Endpoint Detection and Response, Cloud-Workload-Sicherheit und IT-Abläufe konsolidieren mehrere bestehende Technologien zu einer zentralen Lösung. SentinelOne Ranger® ergänzt diese Lösung mit einem einzigen Agenten für Netzwerk- und IoT-Kontrolle. Ranger® erfüllt diese Kundenanforderungen:

- Echtzeit-Überwachung der Datenbank für das Konfigurationsmanagement (CMDB) auf Änderungen
- Untersuchung der Geräte und Geräteaktivitäten
- Wechsel von verdächtigen Geräten und Suche nach lateralen Bewegungen
- Isolierung gerätebasierter Bedrohungen mit einem Mausklick
- Identifizierung von Lücken innerhalb der SentinelOne-Bereitstellung



Singularity Complete + RANGER®	<p>Suche nach nicht autorisierten und IoT-Geräten in Deep Visibility™</p> <p>Überwachung auf verdächtiges Verhalten mit Storyline™ Active Response-Watchlisten</p>	RANGER® ADD-ON-FUNKTIONEN
Singularity Control + RANGER®	<p>Isolierung gerätebasierter Bedrohungen aus dem Infrastrukturnetzwerk</p> <p>Umfassendes Live-Asset-Inventar zur Verwaltung der IT-Hygiene</p> <p>Sofortige vollständige unternehmensweite Transparenz mit flexiblen Funktionen für aktive und passive Scans</p>	
Rogues™	<p>Identifizierung von Lücken in der Agentenbereitstellung Cloud-basiert durch SentinelOne</p> <p>Verständnis des Netzwerks durch automatische Netzwerk-Scans</p>	ROGUES™ BASIS-FUNKTIONEN

WO LIEGT DER UNTERSCHIED ZWISCHEN ROGUES UND RANGER®?

Rogues und Ranger® sind beide in den Agenten integriert. Die Funktionen sind von der erworbenen Lizenz abhängig. Rogues ist eine kostenlose Funktion, die in den Produktpaketen Singularity Complete und Singularity Control enthalten ist. Ranger IoT ist ein Add-on-Produkt, das zahlreiche Zusatzfunktionen für Netzwerktransparenz und -kontrolle bietet.

 2020 MITRE ATT&CK <ul style="list-style-type: none"> • Geringste False-Negative-Rate • Meiste Korrelationen • Umfassendste Datenanreicherung 	 2020 GARTNER MAGIC QUADRANT FÜR EPP <ul style="list-style-type: none"> • Als „Leader“ eingestuft • Höchste Bewertung für „wichtige Funktionen“ bei allen drei von Gartner definierten Kundenprofiltypen 	 2020 FORRESTER WAVE™ EDR „Strong Performer“	 2020 KUPPINGERCOLE MARKET COMPASS Hervorragender EPDR-Innovator
---	---	---	---

Bei SentinelOne haben Kunden höchste Priorität

Durch kontinuierliche Auswertung und Verbesserung können wir die Erwartungen unserer Kunden übertreffen.

 97 % der Gartner Peer Insights™ „Voice of the Customer“-Bewerter empfehlen SentinelOne	97 % Kundenzufriedenheit (CSAT)	 BASE Labs AAA BASE Labs BASE Labs	 ISO 27001 CERTIFIED by schellman	 EU GDPR COMPLIANT
		 TEVORA PCI DSS-Bestätigung HIPAA-Bestätigung		 Gartner peerinsights. 4,9 ★★★★★

Informationen zu SentinelOne

Mehr Funktionen, weniger Komplexität: SentinelOne ist ein innovativer Anbieter für Cybersicherheit mit autonomer, verteilter Endpunkt-Threat Intelligence, der das Sicherheitskonzept vereinfacht, ohne Kompromisse zu verlangen. Unsere Technologie lässt sich automatisieren und ermöglicht die reibungslose Behebung von Bedrohungen. Sind Sie bereit?

sentinelone.com

sales@sentinelone.com

+ 1 855 868 3733