KuppingerCole Report

EXECUTIVE VIEW

By Alexei Balaganski

May 19, 2020

SentinelOne Singularity Platform

Die integrierte Sicherheitsplattform von SentinelOne kombiniert Präventions-, Erkennungs-, Analyse- und Mitigierungsfunktionen mit dem autonomen KI-Agenten und ermöglicht so tiefe Einblicke und konsistenten Schutz für On-Premises-Endgeräte, virtualisierte Umgebungen und Cloud-Workloads.

By **Alexei Balaganski**
ab@kuppingercole.com

Content

1 Einleitung

Das Antivirus wurde vor Jahren und bei mehreren Gelegenheiten für tot erklärt. Hinter diesen Behauptungen steckt eine gewisse Wahrheit - angesichts der massiven Zunahme von Größe und Komplexität der IT-Infrastrukturen haben sich alte, auf Signaturen basierende Antivirenlösungen seit langem als ungeeignet erwiesen, um gegen das Ausmaß und die Raffinesse moderner Cyber-Angriffe zu schützen. Und obwohl Endgeräteschutzlösungen (Endpoint Protection, EPP), die sie ersetzt haben, zusätzliche Funktionen wie Anwendungs-Whitelisting, Gerätekontrolle und Firewalls bieten, versagen sie immer noch oft bei ihrer Hauptaufgabe: der Erkennung von Malware vor oder während ihrer Ausführung, um Schäden zu verhindern.

Die enorme Anzahl an externen und internen Bedrohungsvektoren, mit denen sich digitale Unternehmen konfrontiert sahen, führte schließlich zu der Erkenntnis, dass der Schutz vor bekannten Bedrohungen allein keine praktikable Sicherheitsstrategie mehr ist. Ein bedeutender Paradigmenwechsel in der Cybersicherheit brachte eine neue Klasse von Endpoint Detection and Response (EDR)-Produkten hervor, die sich auf die Erkennung und Untersuchung verdächtiger Aktivitäten an Endgeräten (und verschiedener Artefakte und Spuren, die von Malware nach einem Angriff hinterlassen werden) konzentrierten. EDR-Lösungen erfassen in der Regel verschiedene Telemetriedaten von Endgeräten mit Hilfe von Software-Agenten und ermöglichen es Sicherheitsanalysten, betroffene Endgeräte aus der Ferne zu untersuchen, um die Grundursache eines Sicherheitsvorfalls zu identifizieren und zu beheben.

Eine Zeit lang wurden EDR-Lösungen als perfekte Alternative zu den alten Antiviren vermarktet, aber leider wurden ihre großen Mängel schnell erkannt. Erstens hat sich die Definition eines Endgerätes selbst weiterentwickelt - heutzutage sind verschiedene Desktops, mobile Geräte, virtuelle Maschinen, sogar Container und andere Cloud-Workloads direkt mit Unternehmensnetzwerken verbunden, und das macht die Aufgabe, eine konsistente Sichtbarkeit über diese Netzwerke hinweg aufrechtzuerhalten, zu einer Herausforderung. Wichtiger war jedoch die Erkenntnis, dass mehr Sicherheitstelemetrie nicht unbedingt zu mehr Sicherheit führt (dasselbe Problem haben die Anbieter von SIEM-Produkten fast ein Jahrzehnt zuvor bereits erkannt).

Die wachsende Zahl von Alarmen, die durch eine EDR-Lösung erzeugt werden, kann selbst ein großes Team von Sicherheitsexperten schnell überfordern, so dass nur sehr wenig Zeit bleibt, einen Vorfall zu untersuchen und darauf zu reagieren, bevor er sich zu einer größeren Störung ausweitet. Viele Unternehmen lösen das Problem, indem sie ihren Sicherheitsbetrieb an einen Managed Service auslagern. Ein alternativer Ansatz, der in letzter Zeit an Popularität gewonnen hat, ist der Einsatz von KI-basierten Methoden und anderen Automatisierungswerkzeugen, um die Produktivität der Analysten zu verbessern und die für die Entscheidungsfindung benötigte Zeit zu

verkürzen. Da diese Lösungen jedoch auf menschliches Eingreifen angewiesen sind, sind sie noch weit davon entfernt, eine echte Echtzeit-Reaktion auf erkannte Cyber-Bedrohungen zu ermöglichen.

SentinelOne ist ein Anbieter von Endgerätesicherheit mit Sitz in Mountain View, Kalifornien. Das Unternehmen wurde 2013 von einem Team von Veteranen der israelischen Cyber-Intelligence-Community gegründet.

Die strategische Vision des Unternehmens ist eine integrierte Endgerätesicherheitsplattform, die mehrere unzusammenhängende Sicherheitstools durch eine einzige Lösung ersetzen soll, um Cyber-Bedrohungen über alle IT-Assets des Unternehmens, sowohl vor Ort als auch in der Cloud, zu verhindern, zu erkennen, zu analysieren und darauf zu reagieren. Das Unternehmen befindet sich in Privatbesitz und wird durch Investitionskapital unterstützt. Auch wenn es sich technisch gesehen noch in der Startup-Phase befindet, hat eine Reihe erfolgreicher Investitionsrunden SentinelOne bereits zu einem Einhorn-Unternehmen mit einer Marktbewertung von über 1,1 Milliarden Dollar gemacht. Es bedient derzeit über 3.500 Unternehmenskunden weltweit.

2 Produktbeschreibung

Das aktuelle Flaggschiff von SentinelOne ist die SentinelOne Singularity Platform - eine einheitliche Lösung für Endgeräteschutz, -erkennung, -reaktion und -minderung, die auf einer autonomen KI-Technologie basiert. Dieses kürzlich erfolgte Rebranding vereinheitlicht mehrere Varianten der Kernplattform, die zuvor als eigenständige Produkte angeboten wurden.

Die Kerntechnologie, die die Singularitätsplattform antreibt, ist der universelle, vollständig autonome Agent, der auf Endgeräten eingesetzt wird: Unterstützt werden Windows-, Mac- und Linux-Plattformen, darunter nicht nur physische Geräte, sondern auch virtualisierte und Cloud-Workloads. Der Agent verfolgt alle auf dem Gerät stattfindenden Aktivitäten in Echtzeit, wie ausgeführte Prozesse, geöffnete Dateien und viele andere Datenpunkte - all diese Informationen können dann dazu verwendet werden, bösartige oder verdächtige Aktivitäten zu erkennen, ihre Art zu analysieren und auf identifizierte Bedrohungen zu reagieren.

In dieser Hinsicht kann die Technologie mit vielen derzeit auf dem Markt erhältlichen EDR-Lösungen verglichen werden, jedoch mit einigen bemerkenswerten Unterschieden, durch die sich SentinelOne von der Mehrheit der Wettbewerber abhebt.

Erstens unterscheidet die Plattform nicht zwischen gutem und schlechtem Verhalten. Sie erfasst und analysiert alle Aktivitäten auf dem Gerät und ordnet sie verschiedenen Szenarien zu. Dieser Ansatz ermöglicht es dem Unternehmen, denselben Software-Agenten zu verwenden, um mehrere Funktionen von klassischem EDR bis hin zu verschiedenen Endgeräteschutzfunktionen (EPP) zu betreiben oder sogar die Überwachung von IoT-Geräten zu ermöglichen, indem die Telemetrie vom lokalen Gerät auf seine Netzwerk-Peers ausgeweitet wird.

Zweitens enthält der SentinelOne-Agent zusätzlich zu der verhaltensbasierten KI-Engine, die während der Ausführungsphase die Prozessüberwachung durchführt und so Muster und Anomalien in ihrem Laufzeitverhalten erkennt, auch eine statische KI-Engine. Diese zweite Engine wird zum Scannen von Dateien vor der Ausführung verwendet und ersetzt einen signaturbasierten Antivirus durch eine moderne, ML-basierte statische Code-Analyselösung. Kombiniert mit zusätzlichen Schutzfunktionen wie Firewall und Gerätesteuerung macht dies den Agenten zu einer leistungsfähigen EPP-Lösung.

Nicht zuletzt verlässt sich die SentinelOne AI-Engine bei ihrer Analyse nicht auf die Cloud. Seine autonome Natur erlaubt es ihm, lokale Analysen in Echtzeit ohne die Latenzzeit durchzuführen, die durch die Kommunikation mit der Cloud entsteht.

Tatsächlich bleibt die volle Funktionalität auch auf einem Gerät erhalten, wenn es überhaupt nicht mit dem Internet verbunden ist. Sobald die Verbindung wiederhergestellt ist, sendet der Agent

natürlich wieder seine Telemetrie zur Speicherung und forensischen Analyse an die Management Cloud.

Diese einzigartige Kombination von Sicherheitsfunktionen ermöglicht es SentinelOne, ein Endgeräteschutzprodukt vollständig zu ersetzen und es mit einer breiten Palette von Verhaltenserkennungs- und Reaktionsfähigkeiten einer typischen EDR-Lösung zu ergänzen - und das alles in einem einzigen autonomen Agenten, der weder auf die Cloud angewiesen ist noch menschliches Eingreifen erfordert. In diesem Szenario bietet der Agent allein sowohl proaktiven Schutz gegen eine Reihe bekannter und unbekannter Bedrohungsvektoren als auch Echtzeit-Reaktion auf böswillige Verhaltensweisen wie Ransomware-Angriffe.

Sie ist in der Lage, bösartige Binärdateien, Skripte, Makros und dateifreie Malware zu neutralisieren, indem sie betroffene Prozesse beendet, Dokumente unter Quarantäne stellt oder sogar mit Ransomware verschlüsselte Dateien aus Volume-Shadow-Copies wiederherstellt. Je nach den von Administratoren festgelegten Richtlinien können diese Aktionen manuell oder vollautomatisch durchgeführt werden. Im letzteren Fall erfolgen sie für Endbenutzer völlig transparent, selbst auf einem Gerät ohne Verbindung zum Internet.

Die Erkennungs- und Reaktionsfähigkeit der Plattform endet hier jedoch nicht. Wie bei einer traditionelleren EDR-Lösung empfängt und speichert die zentrale Verwaltungskonsole von SentinelOne die gesamte Telemetrie von verwalteten Geräten und stellt sie forensischen Analysten zur Verfügung. Die Standarddauer der Datenspeicherung beträgt 30 Tage, kann aber gegen eine zusätzliche Gebühr auf ein ganzes Jahr verlängert werden. Der Umfang der gesammelten Telemetrie-Informationen stellt sicher, dass Analysten einen tiefen Einblick in jedes kleinste Detail der Endgeräte-Aktivitäten haben. Dies ist nicht auf Sicherheitsereignisse beschränkt: Andere Anwendungsfälle sind möglich, z.B. ein zentralisiertes Inventar der installierten Anwendungen.

Die patentierte Storylines-Technologie weist jedem aufgezeichneten Ereignis eindeutige, aber konsistente Identifikatoren zu, so dass verwandte Ereignisse verfolgt werden können. Dadurch wird sichergestellt, dass Analysten die ursprüngliche Abfolge der Ereignisse und die Beziehungen zwischen den betroffenen Prozessen und Artefakten schnell rekonstruieren können. Eine vollständige Timeline kann visualisiert werden, was den Forensikexperten hilft, die Ursache des Angriffs zu ermitteln und die erforderlichen Abhilfemaßnahmen zu bestimmen.

Selbstverständlich bietet die Plattform auch eine voll funktionsfähige Suchmaschine, um eine proaktive Bedrohungsjagd (Threat Hunting) zu ermöglichen. Mithilfe einer Storyline-ID, die einer Gruppe verwandter Ereignisse zugeordnet ist, können Analysten nach bestimmten potenziellen Bedrohungen suchen oder Auslöser einrichten, um über künftige Erkennungen benachrichtigt zu werden. Von derselben Administrator-Benutzeroberfläche aus können Änderungen an Endgeräten zu einem bekannten sicheren Zustand zurückgesetzt werden.

Natürlich bietet die Verwaltungskonsole von SentinelOne einen vollständigen Satz von Sicherheits- und Datenschutzfunktionen, inklusive starker Authentifizierung, Identity Federation mit SAML, feinkörnigem Rollenmodell sowie Anonymisierung sensibler Benutzerinformationen.

Die gesamte Plattform ist von ihrer Konzeption her mandantenfähig, und Kundendaten können innerhalb einer bestimmten geografischen Region isoliert und sowohl bei der Speicherung als auch bei der Übertragung verschlüsselt werden. Dadurch wird die Compliance für Unternehmen in stark regulierten Branchen sowie auch für Behörden gewährleistet.

Eine der neueren Erweiterungen der Plattform ist SentinelOne Ranger. Diese Lösung ergänzt das Standardangebot der Endgeräte-Telemetrie durch Netzwerk-Scanning. Derselbe Agent kann jedes verwaltete Gerät in einen Sensor umwandeln, der das lokale Netzwerk sondiert und alle bisher unbekannten angeschlossenen Geräte identifiziert. Mithilfe einer Geräte-Fingerabdruck-Technologie kann SentinelOne Ranger die Gerätekonfiguration und die Plattform erkennen, IoT- und andere intelligente Geräte identifizieren und eine allgemeine Unterscheidung zwischen verwalteten, nicht verwalteten und nicht unterstützten Geräten vornehmen.

Dieses Live-Geräteinventar steht zur Analyse in der zentralen Konsole zur Verfügung und bietet einen globalen Einblick in die Sicherheitslage des Netzwerks. Geräte, die noch nicht von SentinelOne verwaltet werden, können mit wenigen Klicks schnell übernommen werden; nicht unterstützte Geräte können je nach konfigurierten Richtlinien gemeldet oder automatisch isoliert werden. Die gesamte Lösung erfordert keine zusätzliche Hardware oder Software und auch keine Änderungen an der Netzwerkinfrastruktur.

Die SentinelOne Singularity Platform unterstützt eine Reihe von Integrationen mit Sicherheitswerkzeugen von Drittanbietern. Derzeit werden über 15 Integrationen für Anbieter wie Splunk, Okta oder Tanium angeboten, zusätzlich zu einem allgemeinen SIEM-Konnektor. Für Kunden, die nicht über die erforderlichen Sicherheitskenntnisse verfügen, bietet das Unternehmen den Managed Vigilance Service an. Dieser umfasst eine 24/7-Reaktion auf Alarme, Expertenempfehlungen zum Umgang mit Vorfällen und optionale aktive Abhilfemaßnahmen.

3 Strengths and Challenges

Das einzigartige agnostische Datenmodell der SentinelOne-Plattform ist das, was sie von den meisten Konkurrenten unterscheidet. Tiefe Einblicke in alle (nicht nur böswillige) Aktivitäten über eine breite Palette von unterstützten Endgerät-Plattformen, ob physisch oder virtualisiert, die sogar durch entfernte Telemetrieerfassung von IoT- und eingebetteten Geräten erweitert werden können, machen SentinelOne nicht nur zu einer EDR-Plattform mit vollem Funktionsumfang, sondern ermöglichen mehrere Anwendungsfälle, die über die Cybersicherheit hinausgehen.

Die Fähigkeit, autonom und ohne die durch die cloudbasierte Analyse verursachte Latenzzeit zu arbeiten, ermöglicht es SentinelOne, verschiedene bekannte und unbekannte Cyber-Bedrohungen in Echtzeit zu erkennen und zu entschärfen, ohne dass ein menschlicher Analyst hinzugezogen werden muss. Dadurch wird nicht nur der Endgeräteschutz verbessert, sondern auch die Belastung der Sicherheitsteams drastisch reduziert.

Auch wenn es die Einstufung der Lösung in eine bestimmte Produktkategorie etwas schwierig macht, so kann ihre breite Palette an Schutz-, Erkennungs-, Analyse- und Mitigierungsfunktionen über lokale und Cloud-Umgebungen hinweg in einer einzigen integrierten Lösung eine beeindruckende Ergänzung der Sicherheitsinfrastruktur jedes Unternehmens darstellen, die auch einfach zu implementieren und zu bedienen ist.

Strengths

- Integrierte Sicherheitsplattform mit einem einzigen universellen Endgerät-Agenten
- Unterstützng für Windows-, Mac- und Linux-Plattformen, virtualisierte Geräte, Cloud-Workloads und sogar IoT-Geräte
- Vollständig autonomer Schutz mit mehreren KI-Engines
- Tiefe Einsicht in Geräteaktivitäten dank des erweiterbaren Telemetrie-Datenmodells
- Mehrere Funktionen zur Verbesserung der Privatsphäre in der Verwaltungskonsole

Challenges

- Begrenzte Anzahl von 3rd-Party-Partnerschaften und -Integrationen
- Die Architektur macht sich nicht die externe Bedrohungsintelligenz und die "Weisheit der Menge" der anderen Kunden zunutze

4 Weitere relevante Dokumente

Buyer's Compass: Endpoint Detection & Response (EDR) – 80213
Leadership Compass: Enterprise Endpoint Security: Anti-Malware Solutions – 71172
Leadership Brief: Do I Need Endpoint Detection & Response (EDR)? – 80187
Leadership Brief: Artificial Intelligence in Cybersecurity – 70278
Advisory Note: Real-Time Security Intelligence – 71033

Copyright

KuppingerCole Analysts support IT professionals with outstanding expertise in defining IT strategies and in relevant decision-making processes. As a leading analyst ompany, KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

KuppingerCole, founded back in 2004, is a global, independent analyst organization headquartered in Europe. We specialize in providing vendor-neutral advice, expertise, thought leadership, and practical relevance in Cybersecurity, Digital Identity & IAM (Identity and Access Management), Cloud Risk and Security, and Artificial Intelligence, as well as for all technologies fostering Digital Transformation. We support companies, corporate users, integrators and software manufacturers in meeting both tactical and strategic challenges and make better decisions for the success of their business. Maintaining a balance between immediate implementation and long-term viability is at the heart of our philosophy.
For further information, please contact clients@kuppingercole.com.