KuppingerCole Report

EXECUTIVE VIEW

By Alexei Balaganski
January 12, 2022

SentinelOne Singularity Platform

SentinelOne Singularity Platform is a security analytics platform for unified protection, detection, response, and remediation across heterogeneous IT environments powered by an autonomous AI technology.

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

Content

1 Introduction 3

2 Product Description 5

3 Strengths and Challenges 8

4 Related Research 10

Endnotes 11

Copyright 12

1 Introduction

The sheer number of threat vectors, both external and internal, that organizations are facing are a direct consequence of the continuously increasing size and complexity of modern IT infrastructures. It has long become commonplace that traditional perimeter-focused security tools no longer can provide adequate protection in the era of distributed networks, hybrid cloud architectures, and employees working from home. This realization has led to a major paradigm shift in cybersecurity: modern tools focus primarily on quickly detecting, analyzing, and remediating threats before they manage to cause significant damage.

Almost a decade ago, this gave birth to a new class of Endpoint Detection and Response (EDR) products that focused on detecting and investigating suspicious activities on endpoints (and various artifacts and traces left by malware after an attack). In their basic form, EDR solutions collect various telemetry from endpoints using software agents, store that data for a period of time, and enable security analysts to examine affected endpoints remotely to identify and mitigate the root cause of a security incident.

Retaining a sufficient time span of historical data is more critical than ever since adversaries now commonly craft slow and stealthy attacks that might remain dormant for weeks or months before triggering. For example, the Sunburst attack was designed to trigger after 15 days and is but one example of why organizations increasingly seek several months of historical look back.

Originally emerging as an alternative to traditional Endpoint Protection (EPP) tools, these products have evolved into comprehensive, combined protection, detection, and response platforms for desktops, laptops, and servers. In addition, modern EDR/EPDR solutions use machine learning to identify anomalies in security telemetry, map them to known attack tactics and techniques (such as MITRE ATT&CK), and help security analysts make decisions faster and avoid alert fatigue.

Unfortunately, although such tools offer a substantial improvement both in quality and usability over legacy security technologies, monitoring endpoints alone does not provide sufficient coverage for modern, highly distributed, and heterogeneous IT environments. A classic example of convergent evolution, other classes of detection and response tools have emerged in parallel, focusing on the networking layer or cloud infrastructures (NDR) or specifically on cloud-native workloads like virtual machines and containers (CWPP).

The latest development in the security analytics and incident response market is XDR (eXtended Detection & Response). XDR solutions are designed to consolidate and replace multiple security tools for endpoints, networks, and clouds and provide a modernized take on traditional Security Information and Event Management. As opposed to SIEMs, telemetry is pushed into XDR platforms in real-time, not pulled from logs, allowing for much more rapid correlation and analysis. Just like EDR, XDR solutions rely heavily on AI and ML methods to reduce false positives, improve detection and categorization of anomalous activities, and provide a high degree of automation of threat hunting, forensic analysis, and remediation workflows.

SentinelOne is a security vendor headquartered in Mountain View, CA. Founded in 2013, the company's

strategic vision is an integrated endpoint security platform to replace multiple disjointed security tools with a single solution to prevent, detect, analyze, and respond to cyberthreats across all enterprise IT assets, on-premises and in the cloud. Powered by an autonomous AI engine built directly into its endpoint agent, the solution aims to respond to a wide range of threats in real-time without the latency of the cloud.

In early 2020, KuppingerCole had already reviewed the company's flagship product, the SentinelOne Singularity Platform[1]. However, since that time, the company has introduced several major changes in its solution's architecture that enables an expansion of its detection and response capabilities across multiple security layers and beyond just endpoints. These developments warrant an updated look at the SentinelOne Singularity Platform's capabilities.

2 Product Description

SentinelOne Singularity Platform is a security data ingestion and analytics platform for unified protection, detection, response, and remediation across heterogeneous IT environments powered by an autonomous AI technology. Marketed until recently as a next-generation endpoint detection solution, the platform is expanded to cover networks, cloud resources, and IoT devices to provide consistent real-time security capabilities in a true XDR fashion.

At the core of the platform is the single, fully autonomous agent that's deployed on endpoints: Windows, Mac, and Linux platforms are supported, including physical devices, virtualized OSes within customer data centers and cloud service providers, and Kubernetes cloud workloads. The agent keeps track of all activities happening on the device, such as processes being executed, files being opened, and many other data points -- all this information is analyzed in real time by behavioral AI models and can then be used to detect malicious or suspicious activities, analyze their nature, and respond to identified threats.

In contrast to traditional EDR solutions, SentinelOne captures and analyzes all activities - good and bad - on each managed device and using AI, maps these to many different suspicious and risky scenarios. This approach allows the company to use the same agent to power multiple solutions beyond just endpoint security. In addition to several behavioral AI engines that perform process monitoring during the execution phase, SentinelOne includes a static AI engine as well. It is used to scan files before execution, thus replacing a signature-based antivirus with a modern, ML-based static code analysis solution to predict whether executable code is risky even if it's never been seen before. These aforementioned functions are available across all supported OSes.

For years, the biggest differentiator of the SentinelOne platform was its autonomous nature. The agent can perform local AI analysis in real-time without the latency introduced by communicating with the cloud. In fact, it retains full functionality even on a device not connected to the Internet at all. Of course, as soon as the connection is restored, the agent will resume sending its pre-contextualized telemetry to the management cloud for storage and on-demand forensic analysis. Since the scope of the collected telemetry is not limited just by malicious or anomalous activities observed on endpoints, SentinelOne is able to offer a whole range of specialized solutions based on this technology, including observability, analytics, and management use cases.

In February 2021 SentinelOne announced the acquisition of a data analytics vendor Scalyr, which provides a massively scalable event ingestion and storage technology combined with a real-time cloud-native analytics platform. Integrating Scalyr into SentinelOne's cloud-based data platform enables the company to eliminate any potential challenges and limitations for ingesting telemetry data at a massive scale from a multitude of sources, including the data provided by technology partnerships.

While the company's previous EDR solution is still offered as **SentinelOne ActiveEDR®**, an advanced

detection, threat hunting, and response solution that delivers real-time visibility into endpoint activities, this offering now represents just a single facet of the company's overall Singularity Platform.

In last year's report, we covered the company's patented Storyline technology that automatically tracks and links related events and ensures that analysts can quickly understand the original sequence of events and relationships among the affected processes and artifacts without having to spend the time doing this manually. A full attack storyline can be visualized in seconds, helping the forensic experts to trace to root cause and determine the necessary mitigation actions. EDR benign and malicious data retention is available for up to 365 days, enabling an incredibly long historical view into the history of each device and workload for investigatory purposes.

Since August 2021, **SentinelOne Storyline Active Response (STAR)** is available as a complement to their EDR and enables security teams to create custom rulesets that operate in real-time on any kind of security telemetry, helping automate both detection and response to various threats. Essentially, this solution replaces manual proactive threat hunting with a highly automated, extensible alternative that can work autonomously, improving analyst productivity and reducing potential errors. STAR features full MITRE ATT&CK integration to make custom rules easier to create and more accurate.

SentinelOne's agents already had the ability to reach beyond endpoints by scanning the networks that managed devices are connected to and identifying other, unmanaged devices located nearby. With the newly implemented cross-workload correlation capabilities, this network-level telemetry can be used for a variety of advanced observability and security scenarios without the need to deploy additional network monitoring tools.

The **SentinelOne Singularity Ranger®** solution is a component of the EDR agent code that provides network visibility, the push of new agents directly to devices that need to be managed, and even isolation of device-based threats from other managed network devices. As a part of the overall XDR platform, Ranger provides network-level telemetry to detect, analyze and respond to advanced cyber threats even outside of corporate networks, as well as a number of tools to maintain security restrictions and compliance rules.

SentinelOne Singularity Cloud expands the platform's coverage to cloud workloads running in VMs and containers across all major public cloud service providers and private clouds. For Kubernetes-managed workloads, a single agent protects the host OS of the worker node, its pods, and containers, delivering resource efficiency at scale, and avoiding the overhead of sidecars. The solution is available both as a standalone CWPP product and as an integral part of SentinelOne's Singularity security platform. Since the same agent technology is used for on-prem monitoring, hybrid deployments are transparently supported as well.

The most recent addition to the company's portfolio, released in December 2021, is **SentinelOne Singularity Mobile**, a new mobile threat defense solution that expands SentinelOne's coverage to iOS, Android, and Chrome OS devices. Architected according to the Privacy by Design principle, Singularity Mobile is filling the remaining functional gap between existing XDR platforms, which primarily focus on monitoring and protecting workstations and servers, and mobile device management solutions that usually target company-owned mobile devices.

Although Singularity Mobile can work together with most leading MDM solutions, it does not rely on nor aims to replace them. In fact, the product can seamlessly work with both managed and BYOD devices and offers a number of privacy-enhancing controls to prevent snooping into the private activities of device owners. This Managed Threat Defense (MTD) solution is powered by an on-device behavioral AI engine, and thus does not rely on cloud connectivity - a plus considering that mobile connectivity can be spotty at times. Singularity Mobile detects a broad range of mobile malware, exploits, malicious apps, and phishing attacks, both known and zero-day. In addition, it covers other attack vectors like identifying untrusted networks, detecting system tampering (jailbreak), and performing behavioral monitoring.

A conscious design decision was made to not compete with existing MDM solutions, but instead complement and integrate with them, as well as collect additional security telemetry from mobile devices to facilitate cross-platform analytics and correlation.

Altogether, all these solutions power the company's new flagship product: **SentinelOne Singularity XDR**, which unifies previously available detection and response capabilities across endpoints, networks, and cloud workloads in a single cloud-native universal data analytics platform that is open to many third-party integrations.

This approach allows organizations to migrate from a traditional siloed approach to security (with separate products for monitoring different parts of their infrastructure) to an open platform with all the data available for investigation and response in a single management console. By cross-correlating findings from different sources, advanced persistent threats can be more easily identified and mapped to known attack tactics and techniques.

Currently, over 25 technology partnerships have been established with vendors like Zscaler, Mimecast, Azure AD, and others to incorporate their additional security events into the XDR platform. Additionally, threat intelligence feeds from companies like AT&T Alien Labs OTX and Recorded Future can be integrated to provide additional contextual information for threat analysis and incident response. Exporting incidents into external SIEM platforms like IBM QRadar or Splunk is supported as well. SentinelOne has recently launched **Singularity Marketplace**, where customers can choose from a broad range of supported integrations and incorporate them into their XDR deployments with a single click.

The whole platform can be licensed as one of several packages with capabilities ranging from the core next-generation antivirus functions to the full-featured open XDR platform. Standalone capabilities (EDR, NDR, CWPP, Mobile) are also available as separate platform products, along with a range of optional features (e.g., long-term data retention a-la traditional SIEM platforms) and managed services (e.g., managed detection and response, digital forensics & incident response, and threat hunting).

3 Strengths and Challenges

The unique vector-agnostic data model of the SentinelOne Singularity platform is what sets it apart from most of its competitors. Visibility into all activities (not just malicious ones) and the open architecture that allows real-time integrations with third-party sources of security telemetry not only allows the company to address the changing market requirements so quickly and to offer a feature-complete XDR platform in such a short time frame. It also gives its customers unprecedented flexibility in choosing only the capabilities they currently need and then expanding their coverage as necessary.

The ability to function autonomously without the latency introduced by the cloud-based analysis enables SentinelOne to detect and mitigate various known and unknown cyber-threats in real-time without the involvement of a human analyst thereby lowering the mean time to remediate threats. Even though this capability no longer defines the primary marketing strategy for SentinelOne (after all, their new flagship product is a cloud-based XDR platform), the company's strong investment into AI-powered detection and response still translates into major improvements for security analysts' productivity and earlier detection of security breaches.

In the end, SentinelOne not only managed to address all the shortcomings we have identified in our previous review but also introduced major improvements in the platform's scope and coverage. Despite retaining the same name, the new SentinelOne Singularity Platform is a completely new, much more capable security analytics and incident response solution with an open ecosystem.

Strengths

- Fully integrated endpoint, network, mobile, and cloud security platform with a single universal agent
- Flexible XDR architecture with an open marketplace for third-party integrations
- Support for all major desktop, server, and mobile endpoint platforms, VMs, cloud workloads, and IoT
- Autonomous AI engine for real-time analysis without the latency of the cloud
- Strong focus on automation and workflows to improve analysts’ productivity

Challenges

- XDR threat remediation actions are available to a limited but growing set of third-party integrations
- Integration of mobile threat management into the platform is still a work in progress
- Lower-tier packages are too limited in capabilities

4 Related Research

Executive View: SentinelOne Singularity Platform - 80139
Leadership Brief: Do I Need Endpoint Detection & Response (EDR)? - 80187
Leadership Brief: Artificial Intelligence in Cybersecurity - 70278
Market Compass: Endpoint Protection, Detection, and Response - 80508
Leadership Compass: Enterprise Endpoint Security - 71172
Analyst Chat #88: What (and why) is XDR?
Blog: What is XDR?

Endnotes

1 Executive View: SentinelOne Singularity Platform -- 80139, published on May 19, 2020

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 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.