



Ten Hard Facts About Singularity™ EDR/XDR Superiority Versus CrowdStrike Falcon

White Paper



Table of Contents

Executive Summary	3
-------------------	---

10 Hard Facts About Singularity XDR Superiority	4
1. Flexible Deployment Model and Easier Agent Management	4
2. Best-In-Class Prevention and Detection Proven by MITRE ATT&CK	4
3. Cloud Native, Unified and Scalable Native + Open XDR Built on Single Data Lake Platform That Provides Ease of Use and Drives Consolidation	5
4. Superior and Scalable Security Expertise Delivered Using Gen-AI Capabilities	6
5. Straightforward and Easy Platform Management	6
6. A Force Multiplier of Your SoC Team	7
7. Coverage Without Compromise	7
8. Custom Detections Paired With Automated Mitigation Actions	8
9. Offline vs Online Efficacy	8
10. Proud Product and Operational Transparency	9

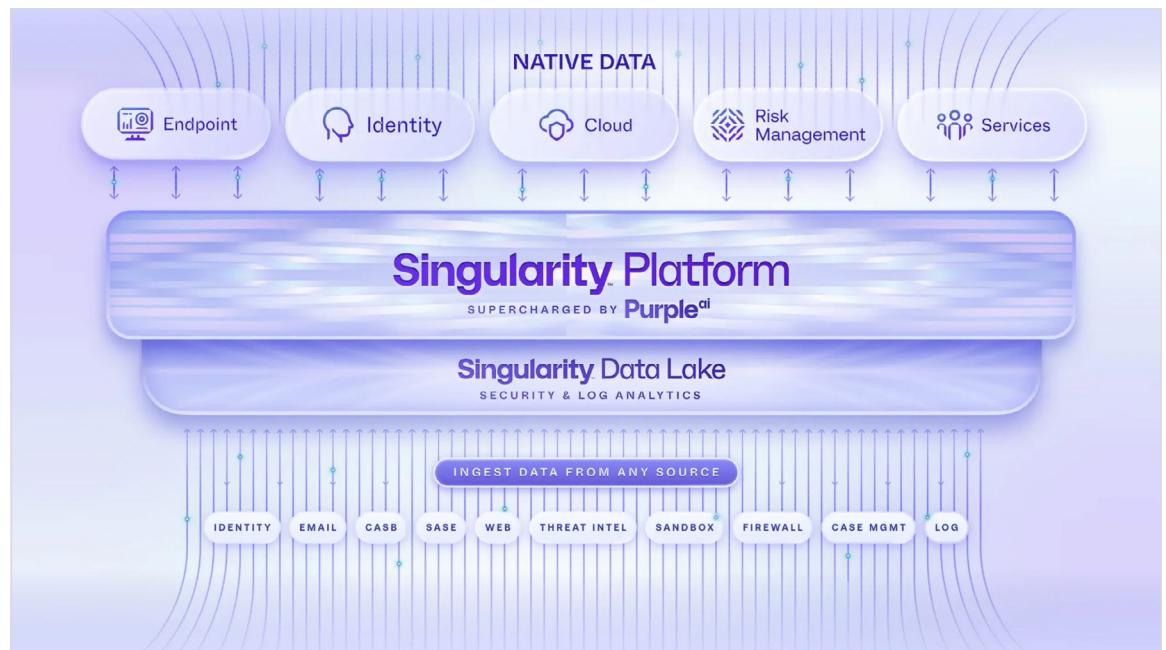
Contact us	10
------------	----

Executive Summary

SentinelOne (NYSE:S) SentinelOne provides a Gen-AI powered Enterprise Security Platform. Built on a single, scalable and unified data lake setting a new standard for SOC modernization and enterprise resilience.

SentinelOne is pioneering autonomous cybersecurity across endpoints, cloud, and identity to prevent, detect, and respond to cyber attacks at faster speed, greater scale, and higher accuracy than human-powered technology alone.

SentinelOne's Singularity Platform empowers enterprises to achieve greater visibility of their dynamic attack surfaces, including endpoints, cloud, containers, identity, and mobile & network-connected devices, and take action in real time with AI-powered automation and cross-platform correlation.



This document intends to highlight many of key differentiators that sets SentinelOne apart from other vendors in the market.

SentinelOne always recommends for organizations to conduct side-by-side proof-of-concepts, ensuring that their success criteria are properly met. Additionally, ensure an analysis of the Total Cost of Ownership (TCO) and Return of Investment (ROI) is also added into the decision equation, given that upfront costs of licensing not always reveal the actual impact of possibly having to use and manage an inefficient and shortcoming security platform, in years to come.

10 Hard Facts About Singularity XDR Superiority

1. Flexible Deployment Model and Easier Agent Management

SentinelOne	CrowdStrike
<ul style="list-style-type: none">• On-Prem (air gapped) and Cloud based (SaaS) deployment• SentinelOne agent is supported for 15 months after the release of the agent before it reaches end of support.(EOS). This means organizations will have less agent upgrades to do in a given year. The agent will continue to receive 'Live Threat Updates' to keep the security levels current.• SentinelOne also provides policy based agent upgradation for different defined asset groups for automated upgradation in line with policy of the organization.	<ul style="list-style-type: none">• Cloud only. No on-prem management console and no support for air-gapped environments.• CrowdStrike agent is only supported for 6 months after the initial release before it reaches the end of life. An organization will have to have more agent upgrades in a given year, making the agent management cumbersome.• Without the set agent upgradation policy, CrowdStrike agent does automated agent upgradation without the management's approval which can lead to non-compliance and unpredictable business disruption.

2. Best-In-Class Prevention and Detection Proven by MITRE ATT&CK

SentinelOne	CrowdStrike
<ul style="list-style-type: none">• SentinelOne has consistently performed at the top since the inception of the MITRE Enterprise Evaluation and demonstrated consistency and commitment towards excellence.• In the 2023 MITRE evaluation, SentinelOne again delivered 100% Protection and Detection with 18/18 steps with 100% Real Time detections (zero delays), 100% Realistic Detections (zero configuration changes), and all the alerts across 2 days of evaluation were consolidated into 22 campaign level alerts. These results are delivered using only the EDR product from SentinelOne.• SentinelOne is the only EDR/XDR vendor to have participated and excelled in all 3 MITRE testing across EDR, Deception and Managed Services.	<ul style="list-style-type: none">• CrowdStrike has been delivering subpar results in MITRE Enterprise Evaluation with results that can't be practically replicated in a real SOC environment.• In the 2023 MITRE Enterprise Evaluation, CrowdStrike had 16 configuration Changes and 27 Delayed Detections with the product running on 'Aggressive Mode' which causes alert fatigue and performance impact in a production environment. Additionally, multiple products (4) were used during the evaluation.• Additionally, CrowdStrike has consistently scored significantly lower than SentinelOne across MITRE Enterprise Evaluations. Please only rely on MITRE Website for the analysis, ATT&CK rounds of evaluations.

MITRE ATT&CK Evaluation Across Year

	2021			2022			2023		
	Configuration Changes*	Delayed Detection*	Number of Products Used*	Configuration Changes*	Delayed Detection*	Number of Products Used*	Configuration Changes*	Delayed Detection*	Number of Products Used*
SentinelOne	0	0	1	2	0	1	0	0	1
CrowdStrike	25	15	3	2	13	3	16	27	4
Microsoft	35	0	3	13	0	4	42	0	2

MITRE Enterprise Evaluation 2023

	Configuration Changes*	Delayed Detection*	Total Sub-Steps Coverage**	Total Steps Coverage**	Number of Products Used*
SentinelOne	0	0	96.18%	100%	1
CrowdStrike	16	27	93.12%	100%	4

*Lower the better

**Excluding config changes, delayed detection and NA

3. Cloud Native, Unified and Scalable Native + Open XDR Built on Single Data Lake Platform That Provides Ease of Use and Drives Consolidation

SentinelOne	CrowdStrike
<ul style="list-style-type: none"> • SentinelOne customers receive longer raw data retention (14 days with Complete and 30 days with Enterprise/ Commercial license) and additionally, 365 days of malicious data retention by default. The raw data retention can be further extended up to 3 years as hot storage. • Threat Hunting can be performed on data for as long as it stored in the Singularity data Lake • Through the Singularity Marketplace or where chosen through API's or Syslogs customers can ingest all types of data including structured, semi-structured, and unstructured data and convert them into an industry agnostic schema, OCSF. This enables easy sharing of data and intelligence sharing across the teams and organizations. 	<ul style="list-style-type: none"> • CrowdStrike offers out-of-the-box 7 days of data retention with only 3 months of malicious data retention. • The data is stored and needs to be purchased in 2 different data storages, i.e. Threat Graph and Falcon Long Term Repository (FLTR) and the data needs to be exported from Threat Graph to FLTR using API. This limits the scope and use-cases e.g.; OverWatch scope will be limited to the data stored in Threat Graph Database only. • Using CrowdStrike Marketplace integration, third party data can be ingested but the data isn't converted into an industry neutral format such as OCSF (Open Cybersecurity Schema Framework) which can lead to vendor lock-in, data left being unportable and difficult to share.

4. Superior and Scalable Security Expertise Delivered Using Gen-AI Capabilities

SentinelOne	CrowdStrike
<ul style="list-style-type: none"> • SentinelOne offers a Security Expert Gen-AI capability called 'Purple AI' which is your 'AI Security Analyst' to help you lower the skill requirements, ease of and scale up security operations. • The efficiency of Gen-AI and LLM depends on a scalable cloud native data backend. The Singularity Data Lake is a cloud native data backend with index-free ingestion, parallel query search engine, column data store and search which results in fast response to natural language queries to data. • Beyond the Threat Hunting, Investigation, Information Synthesization use-cases of the Purple AI can be used for support and troubleshooting related questions too. 	<ul style="list-style-type: none"> • CrowdStrike's Gen-AI alternative 'Charlotte AI' is lacking multiple core features and has a very limited use-case today. • The underlying data lake behind Charlotte AI is not cloud-native and only deployed on cloud which limits the performance and scalability aspects of Charlotte AI. • Charlotte AI's capabilities are limited to just running queries in natural language processing without exposing the query used in the backend to build on the search. Also, does not offer investigation notebooks that can be shared with other SOC analysts, suggested next steps for guided investigation, etc.

5. Straightforward and Easy Platform Management

SentinelOne	CrowdStrike
<ul style="list-style-type: none"> • SentinelOne platform, by default, provides a robust multi-tenancy, multi-site and Role-Based-Access-Control (RBAC) model allowing organizations complete flexibility to maintain individual sites and still have a unified view of the entire organization. • Assets across the tenants can be moved seamlessly without requiring uninstallation and reinstallation. • With 'Network Discovery' customers discover unmanaged devices, including IoT devices. Furthermore, customers are capable of automatically deploying SentinelOne agent, using Peer 2 Peer, for any unmanaged endpoint discovered across Windows, macOS and Linux. Customers have the option to block the traffic to rogue devices in the network. 	<ul style="list-style-type: none"> • Enterprise grade Multi-tenant or sub-tenants within a tenant architecture isn't supported by CrowdStrike by default and requires the customers to open a support case through 'community partner portal'. • Setting up a multi-site and movement of assets across sites are very cumbersome and the agent will have to be uninstalled first and re-installed with a new CID under the new child tenant. • CrowdStrike provides unmanaged device discovery but there is no native way to automatically secure devices, via automatic onboarding like SentinelOne. A third party product such as SCCM, BigFix is required to install the agents in unsecured systems and patch the vulnerabilities discovered.

6. A Force Multiplier of Your SoC Team

SentinelOne	CrowdStrike
<ul style="list-style-type: none"> • SentinelOne Platform delivers out-of-the-box automated response actions for all alerts across Windows, macOS and Linux. • SentinelOne patented automated 1-Click Remediation and 1-Click Rollback restores file to a previously good known state, automatically, without any intervention. • SentinelOne RemoteOps and RemoteOps Forensics delivers unique features and limitless parallelization and scale to empower SOC teams to run scripts across millions of endpoints and collect and parse forensic artifacts. This reduces Mean Time to Response (MTTR) and Attack Containment during remote forensics and incident response, by offering 30 supported artifacts and action scripts out-of-the-box, native data ingestion of DFIR at scale, and more. 	<ul style="list-style-type: none"> • The response capabilities are limited to network containment only. For more response options custom scripts are needed to be built, maintained, and loaded. CrowdStrike pushes customers to use Falcon Fusion however it barely scales operationally. • There is no rollback capability, which increases the cost of a security incident recovery. No 1-click Automated Remediation Capability to revert all the changes made by the attacker to the system such as Registry, malwares, etc. All the changes have to be reversed manually or the system needs to be re-imaged, which ends up increasing the Total Cost of Ownership (TCO) and processing time. • Also, scripts can't be executed across a group of fleet of endpoints at once unless you are using a SOAR capability or install PSFalcon their PowerShell module.

7. Coverage Without Compromise

SentinelOne	CrowdStrike
<ul style="list-style-type: none"> • Full feature parity across Windows, Linux and macOS and additionally support for legacy OS as well. • Consistency policy management and support across supported platforms for consistent experience, but also improved prevention, detection and response across an organization estate. • The Linux agent supports eBPF implementation where the agent sits in the user mode and doesn't hook to the kernel directly. This approach eliminates the risk of kernel panics as well as makes mass roll out of agents easy. 	<ul style="list-style-type: none"> • Inconsistent coverage and lack of feature parity across Windows, macOS and Linux OS. Eg. 'Advanced Remediation', 'Lateral Movement and Credential Access', and even 'Quarantine' missing on non-Windows endpoints. • The coverage for Linux OS is subpar. With every change in kernel version, the CS agents go in 'Reduced Functionality Mode' which disables all the security capabilities and only maintains connection with the management console. The alternate 'user mode' has limited functionality as of today. • Moreover, each linux distro and kernel version require a different CS agent version which makes mass roll out of the agents very difficult.

8. Custom Detections Paired With Automated Mitigation Actions

SentinelOne	CrowdStrike
<ul style="list-style-type: none"> • Storyline Active Response (STAR) provides customers with the ability to create advanced custom detections, using PowerQuery and Purple AI, with support for native automated mitigation actions (including automated rollback and network containment). • STAR has no hidden quotas or limit of executions for each custom detection and there is no need to set frequency, given it runs in near-real time against telemetry that gets ingested into the platform. • STAR works in combination with RemoteOps, customers benefit from automated workflows that take incident response to the next level. • SentinelOne has the capability to upload benign or malicious files to the SentinelOne cloud where they are stored for 30 days and can be used for forensics analysis and additional investigation workflows. There is no pre-requisite for the file to be quarantined first. 	<ul style="list-style-type: none"> • Scheduled Search capability only generates alerts based on custom detection built but unable to take response based on the policy setting. • CrowdStrike has a capability called IOA (Indicators of Attack) for proactive blocking based on rules that are limited in types. • CrowdStrike currently only supports the download of files that have been quarantined first and has no option to upload benign executable files or non-convicted files for analysis.

9. Offline vs Online Efficacy

SentinelOne	CrowdStrike
<ul style="list-style-type: none"> • SentinelOne delivers 100% Detection capabilities without relying on an active internet connection. • Doesn't require cloud connectivity for its efficacy as the Static and Behavioral AI models are available on the agent itself and the threat detection can happen autonomously. This saves the time and bandwidth for to and from between agent and the backend cloud. • Results in Lower TCO, Lower MTTD, MTTR and Improved SecOps. 	<ul style="list-style-type: none"> • CrowdStrike requires cloud connectivity to offer 100% of its threat detection and prevention efficiency. This leads to missed detections when in offline mode. • CrowdStrike Falcon Platform relies on backend processing and the manual Threat Hunters (OverWatch) Team in the backend to detect threats that are missed by the tools (MITRE ATT&CK Eval results demonstrates). This results in delayed detections, translating into longer attack dwell time and higher business impact.

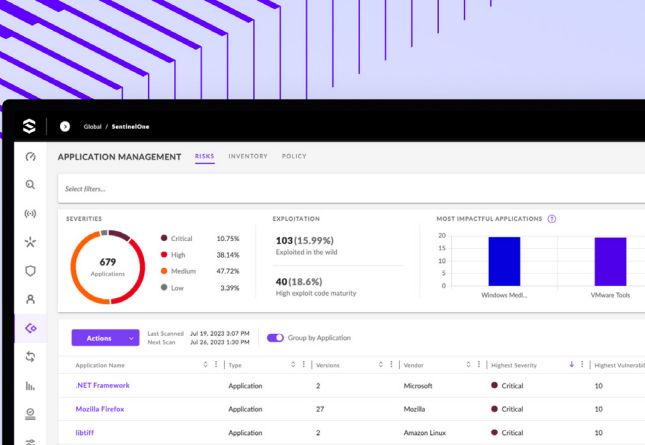
10. Proud Product and Operational Transparency

SentinelOne	CrowdStrike
<ul style="list-style-type: none"> SentinelOne Platform delivers autonomous capabilities by design on the endpoints, cloud and identities. However, in case organizations don't have access to the right skill sets and number of professionals, they can leverage MDR (Vigilance) and Managed Threat Hunting (WatchTower) services to add in/ augment their Security Operations. SentinelOne also offers licensing flexibility to the customers to just buy MDR services or Threat Hunting Services or Threat Intelligence as ala-carte. 	<ul style="list-style-type: none"> CrowdStrike is not transparent about the line between their Product (Falcon) and Services (Overwatch). According to independent reports like MITRE ATT&CK Eval, it is evident that Overwatch services (managed threat hunting) are used alongside to cover the threat detection gap left/unaddressed by the technology. CrowdStrike doesn't offer the flexibility of just buying MDR services, MDR has to be purchased with Threat Intelligence and Threat Hunting Services. This forced bundling ends up increasing the licensing cost and thus the TCO.

Ready for a Demo?

Visit the [SentinelOne website](https://sentinelone.com) for more details, or give us a call at +1-855-868-3733

sentinelone.com



The screenshot shows the SentinelOne console interface. At the top, it displays 'APPLICATION MANAGEMENT' with tabs for RISKS, INVENTORY, and POLICY. Below this, there are several charts and a table. A 'SEVERITIES' chart shows a distribution of 679 applications: Critical (10.75%), High (38.14%), Medium (47.72%), and Low (3.39%). An 'EXPLOITATION' chart shows 103 (15.99%) applications exploited in the wild, with 40 (18.6%) having high exploit code maturity. A 'MOST IMPACTFUL APPLICATIONS' bar chart shows Windows Mail and VMware Tools as the top two. Below the charts is a table of applications:

Application Name	Type	Versions	Vendor	Highest Severity	Highest Vulnerability
.NET Framework	Application	2	Microsoft	Critical	10
Mozilla Firefox	Application	27	Mozilla	Critical	10
libffi	Application	2	Amazon Linux	Critical	10

Innovative. Trusted. Recognized.



A Leader in the 2023 Magic Quadrant for Endpoint Protection Platforms



Record Breaking ATT&CK Evaluation
 + 100% Protection. 100% Detection
 + Outstanding Analytic Coverage, 4 Years Running
 + 100% Real-time with Zero Delays



96% of Gartner Peer Insights™ EDR Reviewers Recommend SentinelOne Singularity





Contact us

sales@sentinelone.com
+1-855-868-3733

sentinelone.com

About SentinelOne

SentinelOne is the world's most advanced cybersecurity platform. The SentinelOne Singularity™ Platform detects, prevents, and responds to cyber-attacks at machine speed, empowering organizations to secure endpoints, cloud workloads, containers, identities, and mobile and network-connected devices with intelligence, speed, accuracy, and simplicity. Over 11,500 customers—including Fortune 10, Fortune 500, and Global 2000 companies, as well as prominent governments—all trust SentinelOne to Secure Tomorrow.

24_MKTG_Product_WhitePaper_006_Ten_Hard_Facts_S1_CrowdStrike_r3_07082024

© SentinelOne 2024

