SentinelOne

SOLUTION BRIEF

SentinelOne Data Retention

Enterprises take an average of **280 days** to identify and contain a breach[1]. While there could be many reasons for a lengthy mean time to detect (MTTD), one of the key factors is the lack of availability of historical EDR data. As Gartner pointed out in one of its blogs, "if you typically detect compromised assets in 60 days after the attacker gets in...and you store... for 30 days, why the hell are you doing it?" A question worth considering! The recent SUNBURST attack is yet another instance that has highlighted how critical it is to have a longer "look back" capability, typically needed to investigate and validate IOCs in the environment.

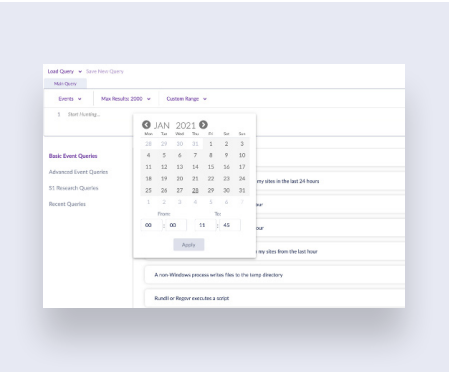
Whether you are proactively looking to uncover advanced adversaries, retroactively looking to respond to a threat, or conduct a post-incident investigation, long term data and visibility is the key. Without long term visibility, it is hard to understand the root cause analysis and answers to questions such as:

- How were we breached? What were the circumstances that led to this event?
- Did this threat actor ever exist in my environment?
- Did we know we had this threat in our environment?
- Did it morph? Is it still lurking in our environment?

These questions offer insight into understanding the root cause of an incident. To answer them, however, you need to have access to all the relevant data.

Get unparalleled visibility into your environment

SentinelOne provides access and visibility into your environment for 365 days and beyond to let your team analyze incident activities and conduct historical analysis. The ability to look back into any point in time allows analysts to see if the threat has targeted your organization in the past and view the full stream of information on how that attack occurred, including the entire process tree, timeline, and related activities.



KEY BENEFITS

Unmatched Visibility

Benign data retention of 365 days and beyond, for full historical analysis of any attack - no matter how long the dwell time.

Hunt with Ease

Easily query, pivot, and drill down into suspicious activities using the same language, same UI your team is familiar with.

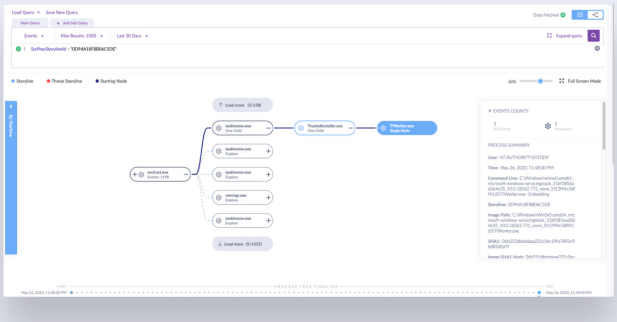
Proven at Scale

Reduce operational and storage costs and maintain high performance.

1 2020 Cost of Data Breach, Ponemon

Investigate with speed and accuracy

Having access to the right data is needed but it is not necessarily sufficient. Any analysts will tell you that sifting through the sheer volume of raw logs to find artifacts and evidence is like finding the proverbial needle in the haystack. SentinelOne not only provides you with historical data, but the patented StorylineTM technology provides real-time actionable correlation and context that lets your security team understand the full story of what happened in your environment. This gives them the full picture of what happened on a device and what caused it to happen, letting analysts visualize the attack chain, understand the root cause and see lateral movements to accelerate investigations.



Hunt with confidence and ease

Leverage the powerful and intuitive SentinelOne Deep Visibility threat hunting capabilities to perform historical hunts to investigate specific indicators of compromise, indicators of attack, or MITRE-based Tactics, Techniques, and Procedures (TTPs) in your environment. Analysts can use the same user-friendly Deep Visibility query language, the same management console resulting in no additional learning curve for your security team.

Meet compliance requirements

SentinelOne data retention capability also provides the answer to your compliance needs across different data retention and audit requirements. Be ready for audits including PCI DSS, HIPAA, NIST, and more, by leveraging connected data insights across multiple endpoints.

USE CASES FOR LONGER DATA RETENTION

+ Detect low and slow attacks
+ Self-audit to search and validate that an IOC was not present in the environment
+ Data storage for Incident response and audit as needed

SentinelOne is a Customer First Company

Continual measurement and improvement drives us to exceed customer expectations.

Gartner peerinsights customers' choice™

97% Of Gartner Peer Insights™ 'Voice of the Customer' Reviewers recommend SentinelOne

97% Customer Satisfaction (CSAT)

FedRAMP

ISO 27001 CERTIFIED by schellman

EU GDPR COMPLIANT

SE Labs AAA Enterprise Endpoint Protection

TEVORA PCI DSS Attestation HIPAA Attestation

Gartner peerinsights 4.9 ★★★★★

About SentinelOne

More Capability. Less Complexity. SentinelOne is pioneering the future of cybersecurity with autonomous, distributed endpoint intelligence aimed at simplifying the security stack without forgoing enterprise capabilities. Our technology is designed to scale people with automation and frictionless threat resolution. Are you ready?

sentinelone.com

sales@sentinelone.com
+ 1 855 868 3733