SentinelOne

Get More Out of Your Splunk Investment

Pair Splunk With the Advantages of a Modern Data Lake That Can Deliver High Performance at a Fraction of the Cost.

Organizations need centralized visibility to security events so they can identify and automate response to threats and vulnerabilities. Often, security data is only visible in point solutions in their unique format, forcing companies to duplicate and move data to traditional SIEM solutions. These solutions were developed in the pre-cloud era, and when used as a data lake, they quickly become cost prohibitive and perform poorly.

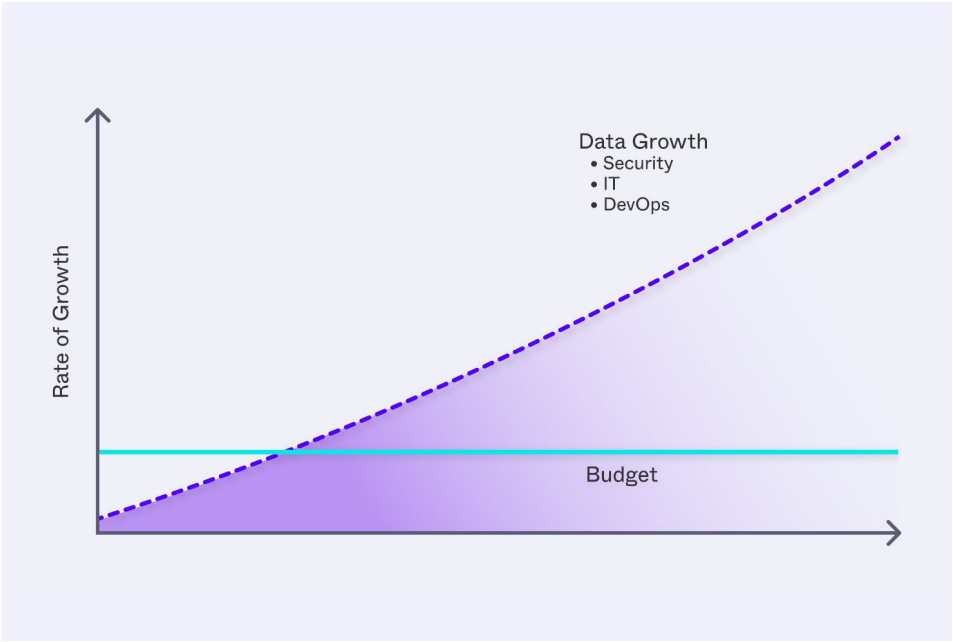
Splunk Challenges

High Licensing Cost

Splunk has a single-tenant architecture built for a pre-cloud, on-premises world. Splunk is not designed to auto-scale, resulting in either over-provisioned or underperforming environments. By not leveraging the innovations available in the cloud, Splunk passes the inefficiency burden to its customers, resulting in a very high cost of ownership.

Workarounds Are Expensive And Complex

Budgets have not kept pace with growing data volume. To contain their Splunk bill, companies have built workarounds, including sampling, creating roll-ups, increasing cluster size, or using tiered storage. However, these workarounds create new complexities such as operational overhead and data loss, which in turn result in even higher costs and blind spots due to the missing data.



Key Benefits

+ Massive Cost Savings
  Efficient cloud-native architecture allows us to pass savings to our customers.
+ All Data is Hot. Always.
  There is no need for tiered storage, rehydrating, or re-indexing data. All of the data is readily available for querying instantly.
+ Effortless Scalability
  True cloud autoscaling results in scaling to petabytes without any effort from your operations team.
+ Unified Security and Observability
  One data lake platform for your teams across all use cases—Security and IT.
+ No Data Left Behind
  Capture and retain all of your data. No sampling or dropping data to cut costs. Achieve compliance with confidence that no data is missing.
+ Long-term Data Retention at a Fraction of the Cost
  Retain data for multiple years and pay a fraction of the cost only when you query the data.

The Solution

01. Augment Splunk with SentinelOne Singularity Data Lake

Singularity Data Lake centralizes event data across all sources and use cases from hybrid, multi-cloud, or on-premises environments. Customers use Singularity Data Lake as a critical foundation of the security stack and to augment their SIEM by sending only low-volume data for high-value alerts to Splunk Enterprise Security, while retaining all data in the Singularity Data Lake where it's available to search directly inside of Splunk.

02. Keep Your Splunk Workflows

We have built seamless integrations with Splunk so our customers get more from their existing investments without changing their Splunk experience. If you use SentinelOne for your endpoint, cloud, or identity protection, you are already using Singularity Data Lake. Reduce costs by eliminating data duplication. Query any data stored in Singularity Data Lake natively from Splunk. Build your Splunk dashboards, alerts, reports, and workflows just as you always have in Splunk—it just works!

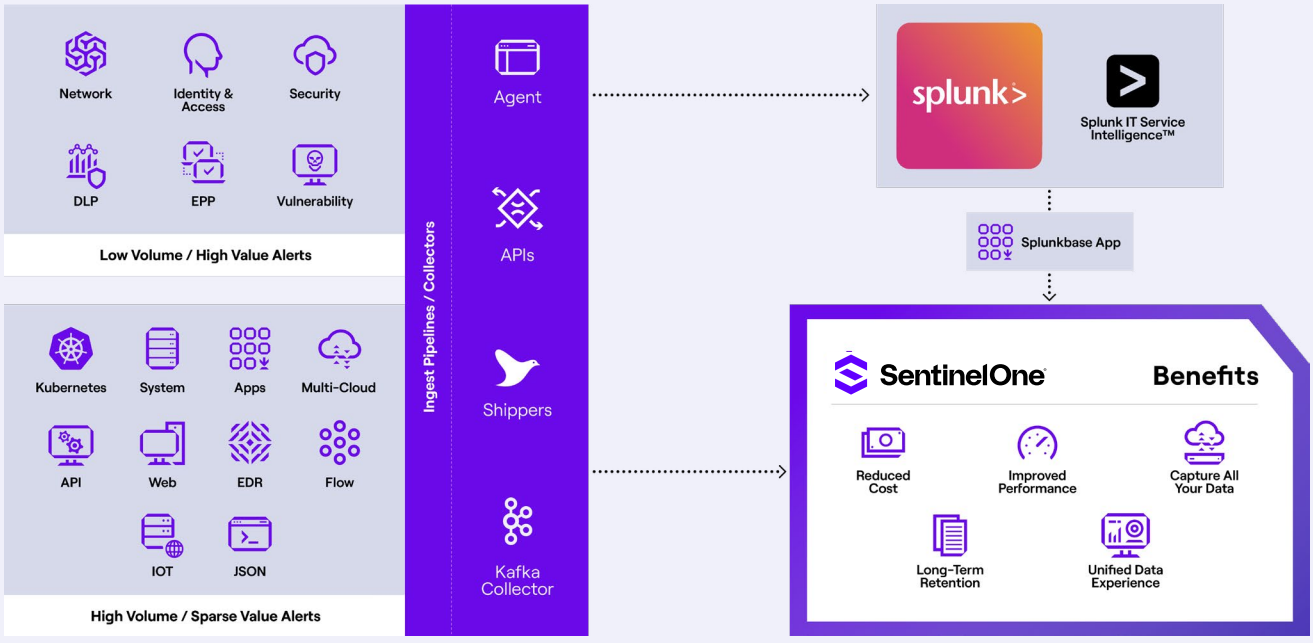
03. Hundreds of Supported Event Data Sources

Simple, easy-to-use ingestion mechanisms with all major data sources save 100s of hours needed to manually set up and configure data ingestion.

04. Data Normalization for Faster Investigations

Memorizing field names and matching schema across multiple vendors are a thing of the past. Singularity Data Lake can also normalize the incoming data to Open Cybersecurity Schema Framework (OCSF), an open standard so customers can quickly get value from their data.

> "With SentinelOne, our security, DevOps, and IT teams have one single source of truth to make data-driven decisions. We no longer have to stitch context across teams and use cases.
>
> Kevin Vuong
> CISO, COPART



05. Positive ROI in Weeks

Delivering on our commitment to customer success, we include a white-glove joint success plan so customers achieve positive ROI within weeks without any heavy lifting from their teams.

Gartner
Peer Insights™

“

All in all, the solution is the easiest solution I have ever had for fighting threats and one of the easiest software deployments I have done. Their service is exceptional.

Security And Risk Manager
CONSTRUCTION

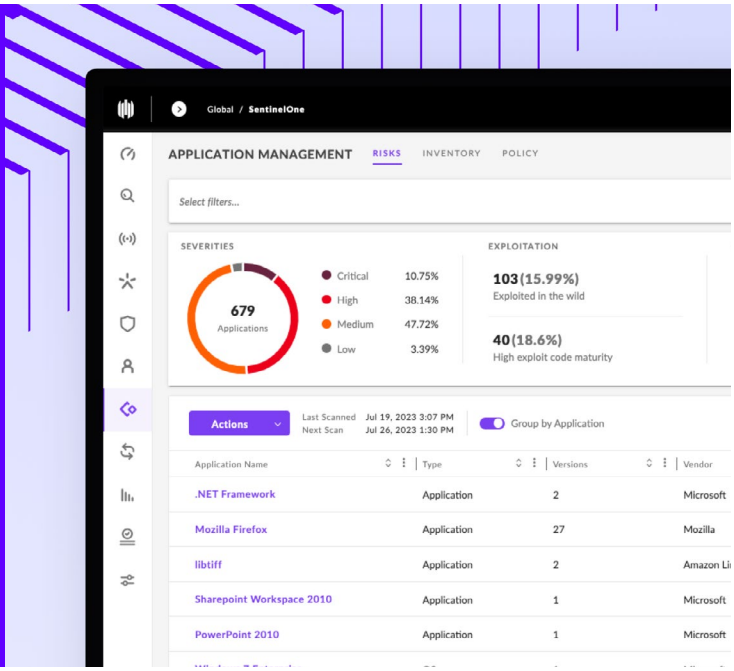
Singularity Platform

Proactively resolve threats in real-time at the site of the cybersecurity battle: the computing and cloud edge.

Ready for a Demo?

Visit the SentinelOne website for more details, or give us a call at +1-855-868-3733

sentinelone.com



Innovative. Trusted. Recognized.

Gartner

A Leader in the 2022 Magic Quadrant for Endpoint Protection Platforms

MITRE ENGENUITY

Record Breaking ATTACK Evaluation

+ 100% Protection. 100% Detection
+ Top Analytic Coverage, 3 Years Running
+ 100% Real-time with Zero Delays

Gartner
Peer Insights™

96% of Gartner Peer Insights™

EDR Reviewers Recommend SentinelOne Singularity

FedRAMP · TEVORA PCI DSS Attestation HIPAA Attestation · AICPA SOC · STAR LEVEL ONE · VB100 VIRUS · SE Labs Innovator WINNER 2021 · SE Labs · Trusted Cloud Provider CSA

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.

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

© SentinelOne 2024