

Imperva Delivers a Powerful Pre-Processor for Splunk Optimization and Savings

Imperva seamlessly reduces Splunk database monitoring costs by 95%, preserves transparent access to raw data, and provides richer security insights

For many enterprises, Splunk acts as the primary repository for database activity logs generated by native logging and DAM tools. Given that these logs can represent >40% of the data indexed into Splunk, and will only grow in size moving forward, this approach has quickly become very expensive.

At the same time, most SOC teams continue to interact with low-level raw data and do not receive the rich, high-quality data they need to rapidly take appropriate actions. To achieve higher value data, SOC teams require expensive Splunk development efforts and time to more effectively isolate critical events.

Imperva enhances your Splunk integration to provide the best of both worlds: reduce Splunk licensing costs while also optimizing your data security program with the addition of a broad range of new capabilities purpose-built for data security. Imperva pre-processing pushes only the intelligence extracted from raw data into Splunk at a fraction of the cost and enables Splunk to be much more effective at incidence response and enterprise level correlation. Splunk receives only the critical events it needs from data security tools, enabling SOC teams to more easily interpret them without needing to wade through irrelevant raw data. This unprecedented visibility enables SOC teams to easily follow chains of events and in a single view gain real security insights.

Infosec leaders: reduce Splunk database activity indexing costs by 95%

Imperva does all the heavy lifting – capturing and retaining the raw data, analytically reducing this to manageable information and forwarding key events directly to Splunk. Imperva presents security events in an easy to understand format with embedded data enrichment, making the analysts more effective by providing a clear lens into critical events.

SOC teams: Imperva does the mining, you get the gold

Besides the intelligent pre-processing, Imperva's unique bidirectional integration lets Splunk users seamlessly access all the raw data stored in Imperva using the Splunk UI, despite not having indexed this massive data set into Splunk.

Imperva pre-processing optimizes another core benefit of the Splunk platform, the end-to-end correlation of disparate data streams.

The Splunk team can easily correlate events end-to-end from their entire estate of tools into a single view of the event and its interrelated pieces. Security analysts can then triage the issue and run a Imperva workflow or playbook, all without leaving the Splunk UI.

Imperva analytically pre-processes all the raw data to isolate the critical intelligence and push it to Splunk, often enriching the data before it is sent to Splunk so that there is greater context.

This helps dramatically reduce Splunk licensing costs, cost-effectively expand database activity visibility and retention, and enrich key events with context for faster remediation.

Imperva is an analyst-recognized, **cybersecurity leader** championing the fight to **secure data and applications** wherever they reside.

