

HUNTSMAN®

Smart Archive



Access to logs in time

Collection of event log data is vital for security and compliance, but log volumes are growing exponentially: the more you collect, the more you have to store and the harder it is to find what you need in the event of incident.

But it's not just access that matters: it's access and analysis of complete logs, in sufficient time to make a difference.

Creating larger log analysis solutions is possible but is commercially difficult to justify. Archiving logs onto tape or DVD storage isn't practical in larger environments, because it slows down access to relevant data for audits, forensic analysis or internal investigations later on.

In the event of an e-discovery exercise, the onus of availability is on you: your organisation must be able to access complete, admissible logs in a timely manner.

An intelligent solution

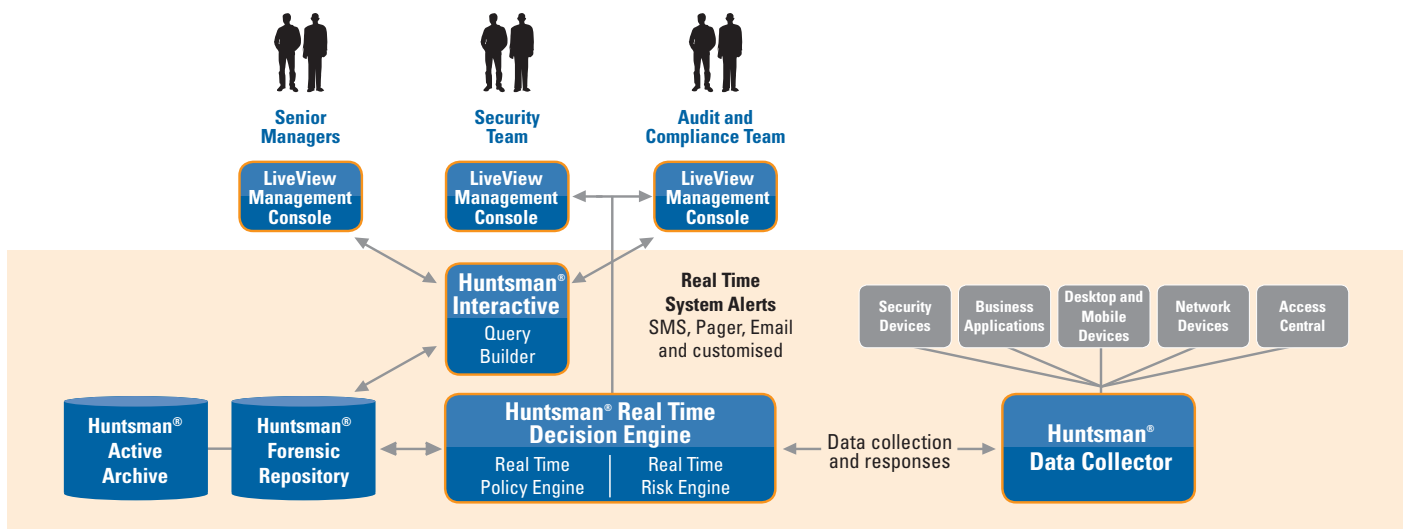
Tier-3 has addressed all these aspects of the problem with Huntsman® Smart Archive which:

- Captures and stores all logs in their entirety;
- Lets you divide them into active or passive archive;
- Automatically moves logs between the two, according to preset parameters;
- Compresses passive archives to reduce storage needs, without loss of integrity; and
- Ensures location and retrieval of any log archive in real time.

'Striking a balance between the resources available for storage and analysis and the continuous supply of log data is critical.'

'Technology briefing: Log management and SIEM' – SC Magazine UK, October 29, 2009

Huntsman® Smart Archive



Intelligent Security. We invented it.

Tier-3 
www.tier-3.com

HUNTSMAN®

Smart Archive

As a centralised platform, Huntsman® aggregates logs from any system and in any format into a single repository. This means that every complete log is captured, rather than purging 'unnecessary' data to save storage and finding later that vital, admissible detail has been lost. It also means that full log data are accessible long after the initial capture or period of currency, so you can find the log you need quickly, regardless of when the event actually occurred.

Active Archive:

- Allows an expanded data set to be incorporated into the reporting windows, and query management and report building to be managed by Huntsman®;
- Reduces audit e-discovery costs, as Huntsman® knows where the data resides and makes it available via a query from the LiveView Console;
- Gives your IT security staff a single integrated view of all data, including multiple archives, and lets them run relevant queries from LiveView;
- Is an economical and logical extension to existing Huntsman® installations;
- Reduces IT expenditure by delivering significant capital savings and operational efficiencies.

Passive Archive:

- Enables event log data to be moved from the reporting repository and stored as a Data Indexed Archive;
- Reduces storage requirements by 90% or more, by using compressed flat files;
- Allows queries from the LiveView console to locate any file quickly, because Huntsman® knows where it is; and
- Allows data to be auto-imported for analysis* with Huntsman's® Intelligent Data Management Engine, including non-sequential data. This ensures that real-time analysis is not compromised.

Integration and visibility

Huntsman® Smart Archive gives you visibility across all your system logs, breaking down the barriers of business intelligence silos so you can find and retrieve data that were previously inaccessible. Through the easy-to-use LiveView console, you can schedule regular reports or investigate data over extended timeframes. You can also create reports based on a broader operational context than just security or compliance incidents, delivering unique insight.

By generating reports that directly compare one time period to another, you can identify slow trends that are only perceptible over long periods, and easily highlight the effectiveness of operational policy changes over time. Moreover, you can translate volumes of discreet, unrelated events into an operational view in context with the end user and use. This way, by looking at data from multiple perspectives, Huntsman® Smart Archive extends the value and usability of collected data, in a cost effective and controllable manner.

Consistent with our flexible adoption model, Huntsman® Smart Archive is designed as an integrated extension to existing Huntsman® deployments. Huntsman® Smart Archive is available either as a Turnkey Archive, balanced with the Huntsman® Forensic Repository to suit varying data volume and reporting requirements, or as Software Only, ready for your virtualised environment.

'Log analysis can help identify security incidents, fraud, policy violations and operational issues, while correctly archived logs simplify auditing, forensic analysis and supporting internal investigations.'

'Technology briefing: Log management and SIEM' – SC Magazine UK, October 29, 2009

*Subject to sufficient capacity being available in the deployed licence.

AUSTRALIA

Tier-3 Pty Limited

L2, 11 Help Street
Chatswood, NSW, 2067
info@tier-3.com
+61 2 9419 3200

UNITED KINGDOM

Tier-3 Pty Limited

No. 1 Cornhill
London EC3V 3ND
info@tier-3.com
+44 203 178 3338

JAPAN

Monet

Ishikawa-Kosan Building 4F 4-7-5
SotokandaChiyoda-ku
Tokyo Japan 101-0021
info@tier-3.com
+81 3 5256 5171

