



CDR Log Analytics and Retention

Hexis Makes Compliance with CDR Data Retention Directives Easy

Communications providers generate hundreds of millions of event records daily. Every phone call placed, connected, disconnected, etc. creates potentially critical event log data. Because of this, regulatory and business drivers now require telecommunications providers to capture and retain years of this data. Hexis helps communications organizations around the world to quickly implement CDR log analytics and retention solutions that uniquely deliver actionable results from massive amounts of log and event data.

High Performance Analytics and Efficient Storage

Telecommunications providers capture and retain years of CDR data for multiple purposes:

- Operations troubleshooting and root-cause analysis
- Fraud detection
- Forensics and investigations
- Anti-terror information requests
- Regulatory compliance

As an example, the EU Retention Directive specifies that the following data elements be captured and retained in an accessible repository for 6 - 24 months:

- Wireline/wireless Call Detail Records (CDRs)
- SMS Logs
- Email Logs
- Proxy Server Logs
- DHCP Assignment Logs

In many cases, this results in billions of records, and terabytes of total data, to maintain and manage. In addition, telecommunication providers must implement the capability to perform pin-point searches over the full repository to retrieve specific records.

The Hexis Approach

To effectively manage these requirements, an entirely new approach is required. Hexis combines enterprise-class software with regulatory and security proficiency, to provide organizations the most efficient and cost-effective means of collecting, analyzing and storing massive amounts of event data regardless of the type or number of data sources to be monitored. This translates to more accurate and efficient security monitoring, investigations, digital forensics and field-proven regulatory compliance. Hexis offers the following benefits:

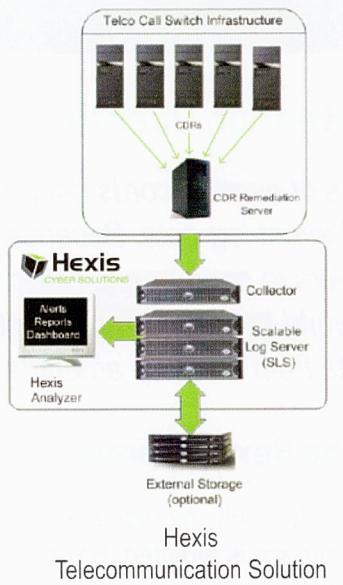
- Captures all CDR and log records from relevant sources
- Stores years of data online with immediate access to all data
- Provides full data analysis capability - easy to extract the exact records of interest
- Offers exceptional data loading and querying performance

Hexis dramatically reduces the cost of deployment and ongoing management associated with security monitoring, investigation and compliance. Hexis's patent-pending technology yields a robust, high-speed, extensible CDR retention and analysis solution.

The Hexis Solution

Hexis provides telecommunication providers with the most scalable means to centrally aggregate, efficiently analyze, dynamically monitor and cost-effectively manage high-volumes of event log data. Hexis is built upon a modular architecture that takes full advantage of parallel processing, and a clustered repository – assuring consistent event collection, analysis and availability. This modular approach allows for appliance-like deployment, distributed configuration, and high performance.

Hexis captures a broad range of event log sources spanning CDRs, email systems, web proxies, network devices, security applications, host operating systems and applications. Event log data is collected supporting flexible batch and streaming protocols for real-time correlation and complete, long-term historic data analysis. The core of the Hexis system is the Scalable Log Server (SLS). It provides a scalable, high-speed analytic repository that parses, compresses and executes built-in and user-supplied queries against stored event log data. Hexis achieves a 10:1 raw log compression rate, while maintaining full access to all the data for ad-hoc and scheduled analysis. Overall alert monitoring, reporting, investigation and administration are provided by the Analyzer through an intuitive web-based interface. The solution is complemented by analytics packages of pre-defined rules and reports, mapped to common security monitoring guidelines and compliance standards.



Convert Years of Data into Actionable Reports - Within Minutes

Hexis eliminates the need for organizations to make operational and compliance compromises with regard to which systems to monitor, which data to collect, and how long to utilize and retain event data online. Hexis's purpose-built data store does not rely on relational database management system (RDBMS) technology. This results in more cost-effective data retention, as well as high performance reporting and analysis. Hexis customers analyze years and gigabytes worth of information considerably faster, and with more precision and consistent results than do their counterparts relying on RDBMS-based systems. Hexis's optimized data store also avoids the high administrative costs associated with managing an RDBMS architecture. Finally, having access to years of data online also eliminates tedious sub-dataset queries and labor-intensive archive restoration processes. Hexis benefits include:

- Leverage content addressed storage to yield enterprise-class security analytics
- Manage volumes of event data to reduce threat, violation and privacy risks
- Streamline operational reporting and automate audit processes
- Accelerate compliance efforts and address data retention guidelines
- Reduce log management storage, archive, administration and growth costs
- Readily expand capacity, performance and availability with appliance-like deployment convenience

Copyright © 2013 Hexis Cyber Solutions, Inc. All rights reserved. Hexis Cyber Solutions and HawkEye are protected by U.S. and international copyright and intellectual property laws. Hexis Cyber Solutions and HawkEye are registered trademarks or trademarks of Hexis Cyber Solutions Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.