Secure your Enterprise with Hadoop

As security breaches are becoming more frequent and sophisticated, traditional security solutions are not able to protect company assets. Organizations realize that just putting up walls around data is no longer enough protection. CIOs are trying to avoid security related incidents from impacting service level agreements (SLAs). It is estimated that 92 percent of security breaches go undetected.1

What’s needed today is deeper insight into the data being generated every day, to identify threats by monitoring and analyzing all events across the network in real time. However, this results in the generation of large amounts of security-related data that must be stored and analyzed. In addition, increased regulations require storing and archiving security event data for longer time periods to comply with more stringent regulations.

It’s no wonder that the information security function needs better analytics to proactively identify threats and reduce risk. Leading analysts estimate that by 2016 nearly 25 percent of global companies will have adopted big data analytics for security use cases, with a positive return on investment within six months.

Key benefits of security analytics include reduced likelihood of fines and lawsuits, greater levels of automation to meet compliance and audit mandates, and minimal maintenance overhead for IT.

The MapR Distribution including Hadoop enables organizations to analyze unlimited amounts and types of data in real time, widen the scale/reach, and accelerate the speed of threat analysis.

1 Gartner SIEM Market Overview
Real-time Analytics on Security Event Data

The key capabilities of the MapR solution include:

- **Data archival.** The MapR Distribution enables archival and storage of security event and other related log data going back several months and years that enables historical search and analysis.

- **Search and discovery.** Indexing and search capabilities from Elasticsearch and Lucidworks that integrate with MapR can aggregate security logs and provide a feature-rich UI that delivers valuable insight. This enables real-time search against a large repository of data.

- **Easy data ingestion.** Copying data to and from the MapR cluster is as simple as copying data to a standard file system using Direct Access NFS™. Applications can therefore ingest data into the Hadoop cluster in real time without any staging areas or separate clusters just to ingest data.

- **Scalability.** Scalability is key to bringing all data together on one platform so the analytics are much more granular and accurate. MapR is the only Hadoop Distribution that scales all the way to a trillion files without compromising performance.

- **High performance.** The MapR Distribution was designed for high performance with respect to both high throughput and low latency. In addition, a fraction of servers are required for running MapR versus other Hadoop distributions, leading to architectural simplicity and lower capital and operational expenses.

MapR delivers on the promise of Hadoop with a proven, enterprise-grade platform that supports a broad set of mission-critical and real-time production uses. MapR brings unprecedented dependability, ease-of-use and world-record speed to Hadoop, NoSQL, database and streaming applications in one unified distribution for Hadoop. MapR is used by more than 500 customers across financial services, government, healthcare, manufacturing, media, retail and telecommunications as well as by leading Global 2000 and Web 2.0 companies. Investors include Google Capital, Lightspeed Venture Partners, Mayfield Fund, NEA, Qualcomm Ventures and Redpoint Ventures.