Meeting the Demands of Securing Big Data

THE CHALLENGE

Big Data is changing the way businesses and organizations make critical decisions. Of course, we have always had data, but now we can compile vast amounts of data at incredible speeds, from multiple platforms and products. Thanks to business intelligence and analytics software, data that is collected in the normal course of business can now be mined and correlated to find relationships and meaning. We have actionable intelligence.

This ability was made possible by the cloud, which created a practical and cost-effective place for immense data to live (as opposed to massive on-site servers). But cloud storage introduces a security risk:

- A large aggregated data store is an attractive target for hackers and malicious insiders.
- Big Data stored in a public or hybrid cloud environment has a larger attack surface, virtual environment has its own security issues.
- Sensitive data is being ported from mature and secure relational databases into NoSQL data stores that inherently lack compatible security controls.

THE SOLUTION

There are many ways to address these concerns, which presents its own challenge with so many products and platforms available. Because Kaizen Approach does not sell software or products, we can offer unbiased recommendations. For a particular customer in the Intelligence Community, we recommended the Hadoop suite of tools as the foundation of a NoSQL database.

A NoSQL database is ideal for huge quantities of data, especially unstructured or non-relational data; but security is not built into Hadoop (nor any NoSQL database). It was never built for enterprise security but for publically available data. For this customer, we initiated the following steps (among others that were specific to the customer).

- Determined which data should be in a NoSQL database given the immaturity of Big Data products/implementations

- Firewalled off the Big Data clusters from rest of network
- Hardened and secured machines (virtual and physical) where a database cluster is distributed
- Limited who can access the databases with authentication
- Recognized the target of and power of consolidated data to attackers and malicious insiders
- Acknowledged that compliance/regulatory issues are the same for NoSQL databases as for relational databases: backup, auditing, monitoring, and securing data is still required

THE RESULTS

The tools to secure Big Data are new or being developed, but the concepts behind securing the data are not. Our experienced professionals are steeped in security concepts, risk management, technology and principles of data processing. For this customer, we were able to analyze which add-on security products would best meet their needs and best reduce the risk of a security breach in their Big Data environment. This gave them the confidence to take full advantage of the benefits that cloud-housed Big Data and its resulting analytics can bring to their organization.

Are you concerned about the security of your data in the cloud?

CONTACT US