**Data Security for Big Data**

Big data security is a term used for all collective measures taken to protect both data and analytical processes from theft, attacks or all other malicious activities. Just like other forms of cybersecurity, big data security is about attacks originating from every online or offline sphere. Companies operating on the cloud face multiple challenges including online information theft, DDoS attacks and ransomware. These attacks can get more threatening for companies that store confidential information such as customer data including credit card details, bank accounts, or other contact details. Furthermore, an attack on the organization’s big data can also cause serious losses in terms of reputation, litigation costs or fines.

**The Challenges**

Let’s look at some major big data challenges that define how you should set up your security.

* The incoming data that can be intercepted while in transit.
* The storage data can be stolen while on cloud or data servers
* Data that is being outputted can serve as an access point for cyber criminals
* Advanced tools for nonrelational databases and unstructured big data are comparatively new technology that are still in active development and are hard for security software to protect
* Good security tools can protect data storage but may not do the same for data from several analytics tools to several locations
* Big data installation size is usually very large, ranging from terabytes to petabytes, and cannot fit into regular security audit. Also, as most of the big data platforms are cluster based, they have several vulnerabilities across various servers and nodes.
* The owner of big data needs to update environment security regularly otherwise there can be high-risk of data loss
* Once security tools monitor and alert about any suspicious infection on the database, system or web CMS, big data experts must have the knowledge and skills to efficiently remove the infection.

**Implementing Big Data Security**

There are many ways an organization can implement security measures to protect its big data. Though these tools are not new, but what makes them important is how they are able to keep multiple data secure in different stages.

**Encryption**

Use encryption tools that can secure data at rest and in transit, and across large volumes of data. Encryption should also be applied to all forms of user-generated and machine-generated data. You should also work your encryption tools with various analytical toolsets and the output data, as well as big data formats like Relational Database Management Systems, non-relational DBMS like NoSQL and specialized file systems.

**Access Control**

Access control is a basic measure that must be taken to secure a network, but is often overlooked with only minimal control due to high management overheads. Inadequate access control can turn out disastrous for big data. To avoid a data breach from happening due to this reason, it is always recommended to use a policy-based approach with an [access control application](http://www.cardzgroup.com/ContactLessSmartCard.html) that regulates access according to user job roles. An automated access control based upon a policy helps manage multiple control levels, for instance, multiple administrators - and secure big data platform from inside attacks.

**Intrusion Detection and Prevention Systems**

Intrusion Detection and Prevention Systems are as valuable for big data platform as they are for network security. With its distributed architecture and the value it holds, big data is often subjected to intrusion attempts. This is where Intrusion Prevention Systems stop intruders from accessing the system, and in case an intrusion attempt is successful, Intrusion Detection System quarantines it before it causes severe loss to the data.

**Physical Security**

Physical Security is just as important as everything else. Ensure your or your cloud provider’s data center’s physical security when deploying your big data platform. Physical security ensures that strangers or unrelated staff members are not granted access to the data center. Also keep a record of security logs and video surveillance cameras.

**Firewalls**

Build strong firewalls to filter traffic entering and leaving your servers. Firewalls do an excellent job at preventing attacks by filtering traffic from unknown sources or third parties.

**Assess Your Cloud Service Provider**

If you store our big data in the cloud, ensure that your cloud service provider is keeping your data protected with all adequate mechanisms. Check with them to know that they undertake regular security audits.

**Who Should Have the Responsibility to Keep Big Data Secure?**

Everyone has their part to play in securing big data.

Information Security and IT departments have to formulate security software, policies and procedures to efficiently protect the deployment of big data against user access and malware. Database Administrators need to closely work with the IT and Information Security staff to protect their databases. Compliance staff should work with these departments to ensure that all best practices are being complied with.

While enterprises may focus on one area of security, they often overlook other areas. The best approach to ensure comprehensive big data security is to understand all the challenges and solutions and integrate them into a unified system that can share and correlate threat intelligence, security alerts and all other activities - in real time.