Big Data Security

Big data security is the process of monitoring and protecting a company's important business data with the goal of ensuring safe and compliant ongoing operation.

- Big data security is a constant concern because Big Data deployments are valuable targets to would-be intruders.
- A single **ransomware attack** might leave a company's big data deployment subject to ransom demands.
- **Even worse**, an unauthorized user may gain access to a company's big data to siphon off and sell valuable information.
- Securing big data platforms takes a mix of **traditional security tools**, **newly developed toolsets**, and **intelligent processes** for monitoring security throughout the life of the platform.

How Big Data Security Works

- **Big data security's mission is clear enough: keep out on unauthorized users** and **intrusions with firewalls**, **strong user authentication**, **end-user training**, and **intrusion protection systems** (IPS) and **intrusion detection systems (IDS)**.
- In case someone does gain access, **encrypt your data** in transit and at rest.
- This sounds like any network security strategy. However, big data environments **add another level of security because security tools must operate during three data stages that are not all present in the network.**
- These are: **data ingress**, which is what's coming in; **stored data**; and **data output going out to applications and reports**.

Stage 1: Data Sources. :

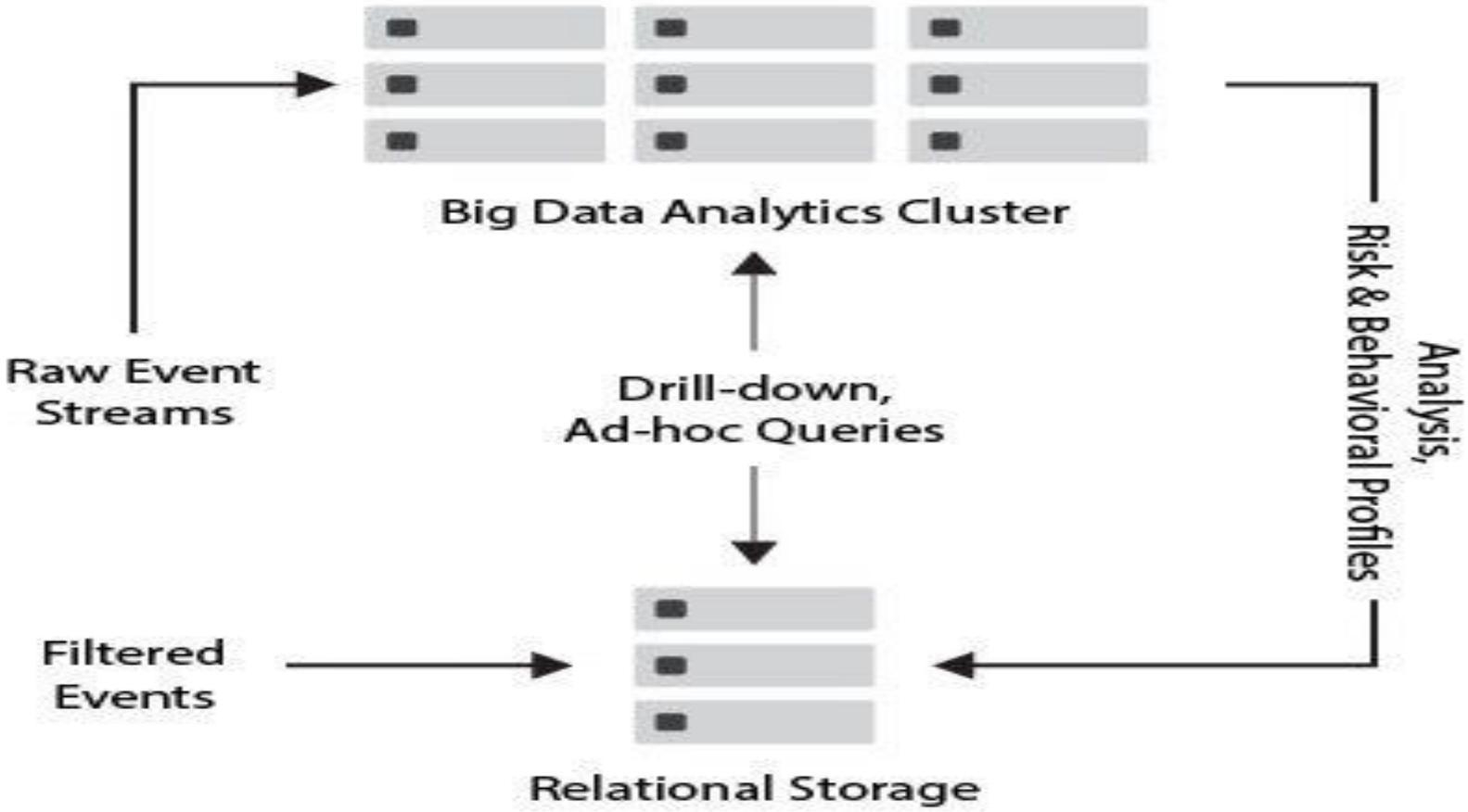
- Big data sources come from a variety of sources and data types.
- User-generated data alone can include customer relationship management (CRM), transactional and database data, and vast amounts of unstructured data such as email messages or social media posts.
- In addition to this, you have the whole world of machine-generated data including logs and sensors.

Stage 2: Stored Data :

- Protecting stored data takes mature security tool sets including encryption at rest, strong user authentication, and intrusion protection and planning.
- A company needs to run its security tool sets across a distributed cluster platform with many servers and nodes.
- In addition, its security tools must protect log files and analytics tools as they operate inside the platform.

Stage 3: Output Data.:

- The entire reason for the complexity and expense of the big data platform is so it can run meaningful analytics across massive data volumes and different types of data.
- These analytics output results to applications, reports, and dashboards.
- This extremely valuable intelligence makes for a rich target for intrusion, and it is critical to encrypt output as well as ingress.
- Also, secure compliance at this stage: make certain that results going out to end-users do not contain regulated data.


Big Data Analytics Cluster
Raw Event Streams
Drill-down, Ad-hoc Queries
Analysis, Risk & Behavioral Profiles
Filtered Events
Relational Storage

Navigating Big Data Security & Trends

- **Two of the biggest trends in the world of big data stand somewhat in opposition to each other:** the proliferation of big data that informs smart technology, and also the growing movement for consumers to own and decide how their personal data is being used.
- **Technologies like IoT**, artificial intelligence, machine learning, and even customer relationship management (CRM) databases collect terabytes of data that contain highly sensitive personal information.
- This personal form of big data is valuable for enterprises that want to better cater their products and services to their audience, but it also means that all companies and third-party vendors are held responsible for the ethical use and management of personal data.

Take a look at some of the top trends happening in the big data world, **the important security points that many companies are missing, and some tips for getting big data security right:**

1) **Update your cloud and distributed security infrastructure:**

- Big data growth has caused many companies to move toward cloud and data fabric infrastructures that allow for more data storage scalability.
- Cloud security is often established based on legacy security principles, and as a result, cloud security features are misconfigured and open to attack.

2) **Set mobile device management policies and procedures**

- IoT and other mobile devices are some of the greatest sources and receivers of big data, but they also offer several security vulnerabilities since so many of these technologies are owned and used for personal life.

- Set strict policies for how employees can engage with corporate data on personal devices, and be sure to set additional layers of security in order to manage which devices can access sensitive data.

3) **Provide data security training and best practices**

- Most often, big data is compromised as the result of a successful phishing attack or other personalized attack targeted at an unknowing employee.
- Train your employees on typical socially engineered attacks and what they look like, and again, set up several layers of authentication security to limit who can access sensitive data storage.

Benefits Of Big Data Security

- **Customer Retention:** With big data security, a company can observe many data patterns, which allows them to better fit their products and services with their clients needs.

- **Risk Identification:** Because of big data security, a company can use big data tools to identify risks in their infrastructure, helping companies create a risk management solution.

- **Business Innovation:** Big data security can help companies update their tools and help transfer products into new secure systems. This innovation can improve business processes, marketing techniques, customer service, and company productivity.
- **Cost Optimization:** Big data security technologies can reduce customer costs by efficiently storing, processing, and analyzing large volumes of data. Big data security tools also will calculate how the product will benefit the company, so companies can pick a company that is better for their infrastructure.

Challenges of Big Data Security

- **Newer technologies can be vulnerable:** Advanced analytic tools for unstructured big data and non-relational databases (NoSQL) are examples of newer big data technologies in active development. It can be difficult for security software and processes to protect these new toolsets.
- **Variable impact:** Mature security tools effectively protect data ingress and storage. However, they may not have the same impact on data output from multiple analytics tools to multiple locations.

- **Access without permission:** Big data administrators may decide to mine data without permission or notification. Whether the motivation is curiosity or criminal profit, your security tools need to monitor and alert on suspicious access no matter where it comes from.
- **Beyond routine audits:** The sheer size of a big data installation, terabytes to petabytes large, is too big for routine security audits. And because most big data platforms are cluster-based, this introduces multiple vulnerabilities across multiple nodes and servers.
- **Requires constant updates:** If the big data owner does not regularly update security for the environment, they are at risk of data loss and exposure.

Big Data Security Technologies

- **Encryption:**
- **Centralized Key Management:**
- **User Access Control:**
- **Intrusion Detection and Prevention:**
- **Physical Security:**