Empowering Big Data in a Data-driven Economy

Fewer things have been more transformational in IT than the rise of Big Data. Some may argue that the shift to cloud computing or the rampant increase in storage capabilities are just as transformational but it's the ability to use our data, monetize our data, and learn from our data that Big Data has made commonplace. More than being transformational, Big Data has transcended the boundaries of typical IT investment and its applicability to every human. The analytics that Big Data offers is astounding – from the seemingly mundane of retail inventory analysis and feeding JIT manufacturing to the exotic of real-time fraud detection at the Point of Sale and the (potentially) scary of presence-based mobile advertising and monitoring.
Like any technology, understanding how to use it and what is appropriate are key. With regulations like GDPR, HIPAA and NYDFS coming into scope, privacy and data security have never been more important. Understanding how to leverage the power of Big Data while maintaining both regulatory compliance and everyday corporate responsibility is key.

Protect Data, Don't Blame It

Whether it be employee data, customer data, IoT sensor data, or random statistical data, the initial reaction amongst many is that data itself is the problem and it should be limited, not collected, or purged. But, in a truly data-driven economy, not collecting or retaining data just isn't realistic. However, bad actors also know the value of data in the underground economy so the threats to data are real. External threats aside, often the threat is internal, through a 3rd party, or even by mistake. The data itself isn't criminal regardless. The answer is to provide strong protection to data while not affecting its usability. The answer is to provide regulatory compliance while unleashing the power of the data. The answer is to protect the "crown jewels" of your organization with data-centric security. As organizations turn to Big Data to leverage the cost savings and distributed compute, the data risks have made this move more of a challenge than ever. comforte offers you the ability to enable those Big Data projects to move forward, realize the power of the Hadoop, and truly benefit from your data – all while securing your data everywhere it goes – intentionally or unintentionally.

Data-Centric Security Makes Data Happy

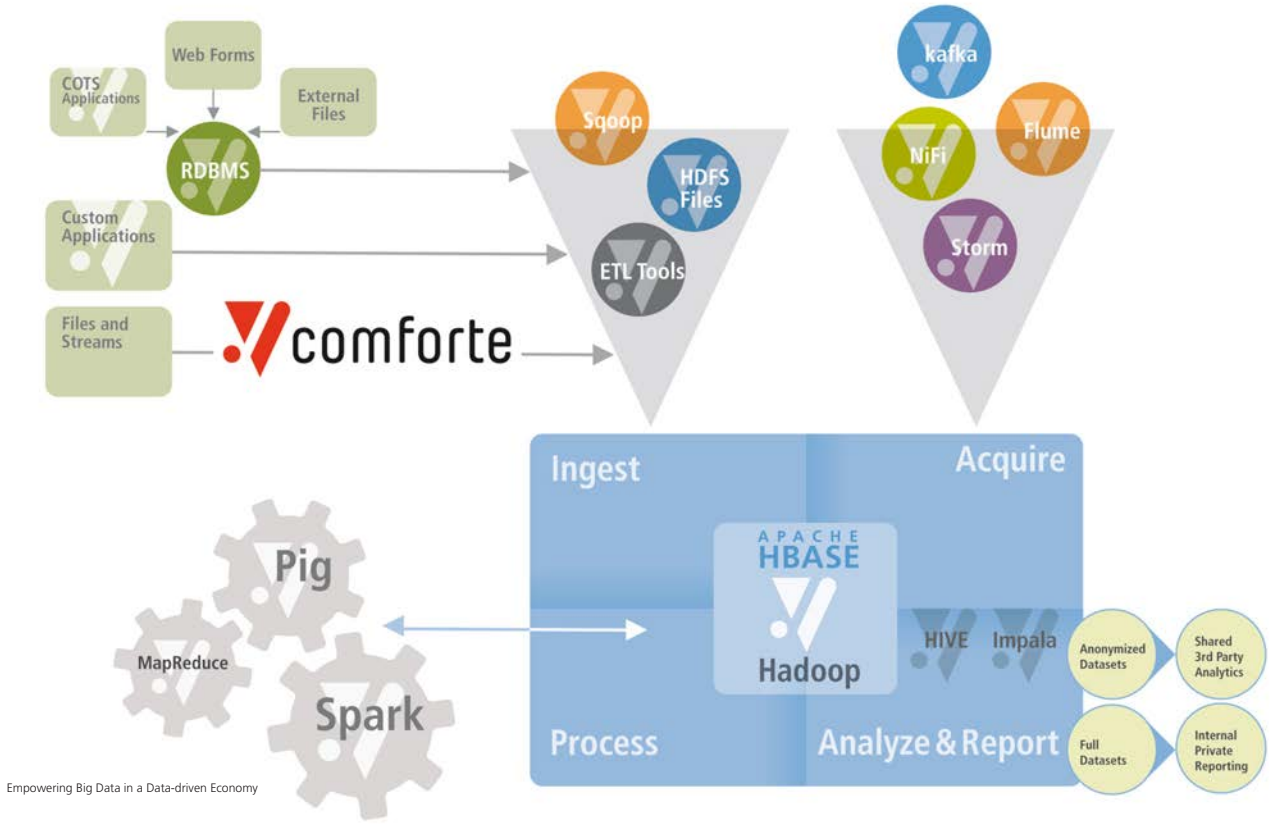
Tokenization replaces sensitive values with non-sensitive values.

A data-centric security model protects the individual data elements wherever possible. That means, if a dataset contains a mix of sensitive data such as Personally Identifiable Information (PII) and data that is not sensitive or regulated, you protect the data at the individual element level using a technology like tokenization. comforte's SecurDPS solution securely tokenizes data to replace elements with tokens that will then represent the original element. What's important about that is that it adheres to the ANSI X9 Tokenization standard so it's proven secure and the tokens generating are format-preserving and offers a 1-to-1 correlation with the original data – maintaining something called referential integrity. That all boils down to a dataset that is the same size that is now full of tokens instead of sensitive data but still has the exact same statistical distribution as the original data. SecurDPS works along-side your existing perimeter, network, and storage security solutions while adding significant value because the data is always protected, wherever it goes or whomever sees it.

Your data is happy because it's still meaningful and relevant. Your databases are happy because schemas don't have to change. Your Hadoop cluster is happy because it doesn't have to worry about containing sensitive data – just tokens. Your data scientists and analysts are happy because they can still get their work done due to referential integrity. Your auditors and regulators are happy because they know that real data can't be exposed.

comforte's Big Data Protection is Organic

comforte SecurDPS was meant for Big Data environments. It is "organic" because the solution scales just like Hadoop scales to meet compute workloads. SecurDPS Protection Nodes are lightweight, can run on VMs or commodity hardware, and scale with the size of your need. No matter if you have one data node or 10,000 data nodes, comforte's fault-tolerant, highly available solution can provide the throughput your workloads require – all without changing your workflows. Need to protect data in a Hadoop ingestion framework, an ETL tool outside your cluster, or flat files in a landing zone on an edge node? Want to manipulate data in HBASE or process data in MapReduce, Pig, or Spark? Need to acquire new data via frameworks like Kafka, Storm, or Flume or a NiFi cluster? Need to perform analysis using Hive or other frameworks? Thinking about comforte has you covered with SecurDPS. No matter how you use Hadoop, comforte can seamlessly integrate both transparently and actively as part of your job to allow you to tokenize data as you ingest it, know that it is protected as it is replicated and stored in HDFS, and still be able to perform analytics and reporting. comforte is truly and organic solution that snaps in that was built from the ground up with Hadoop in mind. Hadoop security through existing measures like Ranger and Knox can help secure your Hadoop cluster but really the goal is to secure the data in your cluster and throughout your Enterprise.



Empowering Big Data in a Data-driven Economy

With more than 20 years of experience in data protection on truly mission-critical systems, comforte is the perfect partner for organizations who want to protect their most valuable asset: data.
comforte's Data Protection Suite, SecurDPS, has been built from the ground up to best address data security in a world that is driven by digital business innovations, empowered customers and continuous technology disruptions.
We are here to enable your success by providing expertise, an innovative technology suite and local support.
To learn more, talk to your comforte representative today and visit www.comforte.com.

Why Data-Centric Security Works for the Enterprise

Protecting data in Hadoop is significant but a corporate data lake is always a part of a bigger operation. As data is ingested into your Hadoop cluster, comforte can help you to protect it so that as it lives and works in HDFS it is secure and, thanks to the data-centric model, still is just as analytically powerful since referential integrity is maintained. But, with comforte you can also protect data in the entire Enterprise that sits around your Hadoop cluster. Applications that acquire data can also use comforte to protect data upsteam and then let that data flow into Hadoop and from Hadoop into any RBMS, report, or other applications. That's part of the power of data-centric security – the security moves with the data.
At comforte, we believe that protecting data upstream as far as possible will give you the most protection because the data can then travel anywhere in your Enterprise and be protected. Point solutions, vendor-specific solutions, network or storage layer protection, or any other solution can't offer you that level of security. In fact, over 90% of workloads can be done on protected data without revealing any sensitive data – giving you the ability to protect the entire Enterprise.