Hortonworks and Protegrity

Hortonworks Data Platform (HDP) is a pure open source Apache™ Hadoop® distribution. HDP combines the power and cost-effectiveness of Hadoop with the advanced services and reliability required for enterprise deployments. Together with Protegrity's Big Data Protector, they provide the most reliable and secure enterprise-ready Big Data solution available.

WHAT IS BIG DATA?

Large organizations are flooded by data from transactions, websites, emails, medical devices – the list goes on. This is **Big Data**: The endless accumulation of data that defies traditional means of intake, storage, and analysis. These issues with extremes of the "4 V's" – **Velocity**, **Volume**, **Variety**, and **Veracity** – have led to the development of a highly available, distributed computing framework called Hadoop, designed to efficiently take in, store, and analyze vast amounts of data for transformative insights.

HORTONWORKS DATA PLATFORM

Hortonworks Data Platform (HDP) is the most stable and reliable Hadoop distribution, and the only 100% open source data management platform for Hadoop. HDP allows organizations to capture, process, and share data in any format and at scale. Built and packaged by the core architects of Hadoop, HDP includes: **Data Services** to store, analyze and access data; **Operational Services** to manage and operate Hadoop; and **Platform Services** such as high availability and snapshots - required for enterprise implementations of Hadoop. These services allow enterprises to manage a Hadoop cluster at scale and uncover business insights from new and existing Big Data sources.

KEY FEATURES

- **End-to-end, complete protection for HDP**
- **Protection in HDFS, MapReduce, Hive, and Pig**
- **Utilize Vaultless Tokenization for field-level sensitive data protection**
- **High-performance, infinitely scalable**
- **Security during business analysis with minimal performance impact**
- **Platform protection easily integrates HDP protection into enterprise security solution**
- **Comprehensive security for multi-vendor, heterogeneous enterprises**

PROTEGRITY BIG DATA PROTECTOR

Protegrity is the first vendor to deliver a comprehensive data security solution for Big Data platforms. Utilizing volume-level strong encryption for files, patent-pending Vaultless Tokenization on the node for individual data elements, and central Policy control for access management, the **Protegrity Big Data Protector** secures all sensitive data in HDP – at rest in HDFS; in use during processing and analysis; and in transit to and from enterprise data systems. The actual data in Big Data systems can now be tokenized and protected from external and internal threats, including privileged users.

VAULTLESS TOKENIZATION

Granular data protection is essential to any comprehensive data security solution, and recently many companies are turning to technologies such as masking and **Vaultless Tokenization** to secure the data itself. Masking provides sufficient security, but is irreversible and not viable if the original data is ever needed. Vaultless Tokenization provides the same benefits of masking with the additional advantage of reversibility for situations that require data in the clear.

PROTECTING NEW DATA ENTERING HADOOP

Protegrity's file encryption minimally impacts the rate at which data can be loaded into HDFS. As data enters, individual data elements can also be tokenized with the MapReduce program on the node, and then distributed to the clusters inside encrypted files.

PROTECTING DATA TO AND FROM THE ENTERPRISE

As enterprise data enters or leaves HDFS, including monetized data, the same policy-level protection, file encryption, and data tokenization can be applied. This continuous protection ensures security of sensitive data throughout the enterprise and beyond.

PROTECTING DATA DURING ANALYSIS

The API available to each MapReduce, Hive, or Pig task is extended with policy-driven data protection functions, such as Vaultless Tokenization. This allows sensitive data to remain secure during analysis, while retaining the visibility critical to deep business insights.

ENTERPRISE DATA SECURITY

The **Protegrity Data Security Platform** delivers protection to a rich set of multi-vendor, heterogeneous technologies, securing files, applications, databases, Big Data, and Cloud environments. Protegrity's **Enterprise Security Administrator** provides central policy and key management, auditing, and reporting across the enterprise. In addition, all audit logs can be fed into Hadoop for intelligence-based security analysis. This holistic approach allows seamless security across all systems, without disruption to business processes.

Protegrity's award winning and innovative software is backed by over 30 pending or granted industry patents, all of which provide superior protection unique to the Protegrity Data Security Platform. The Platform is comprised of the Enterprise Security Administrator (ESA) and a suite of Database, File, and Application Protectors with advanced Vaultless Tokenization, format-preserving encryption, strong encryption, masking, hashing, and monitoring software.

VAULTLESS TOKENIZATION

Protegrity's industry-first, patent-pending **Vaultless Tokenization** process that eliminates the challenges associated with standard, vault-based tokenization. Greatly reduced bottlenecks in performance and scalability caused by latency, no more fear of collisions, and no more sensitive data or tokens residing in your token server. In the event of a breach, tokens hold no value to a potential thief. Tokens can also be embedded with business intelligence, allowing for seamless analytics and business processes without the need to detokenize data.

DATA PROTECTION METHODS

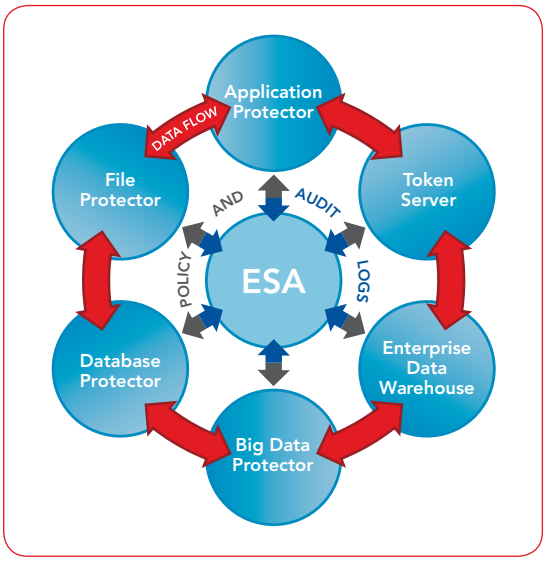
An effective data security strategy is defined by matching the risk associated with any particular type of data (e.g. credit card numbers, PII, etc.) with a specific data protection method. Protegrity supports a comprehensive range of **Data Protection Methods**, including Vaultless Tokenization, format-preserving encryption, strong encryption, masking, hashing, and monitoring.

ENTERPRISE COVERAGE

Protegrity has a proven record of successfully implementing data security solutions in complex, heterogeneous environments. The **Protegrity Data Security Platform** has extensive interoperability with the variety of databases, operating systems, applications, and platforms inherent in all large enterprises, including Oracle, DB2, SQL Server, IBM Mainframe, Hadoop, Teradata, and more.

DATA PROTECTORS

To help organizations implement a truly end-to-end data security strategy, Protegrity provides a collaborative set of Data Protectors, including the **Database Protector**, **File Protector**, and **Application Protector**. These Data Protectors can be combined as needed to provide flexible security for sensitive data in all forms across an entire enterprise.



BIG DATA

Protegrity is the first vendor to deliver a comprehensive data protection path to Apache™ Hadoop®, including Hortonworks, and other **Big Data** platforms. For the first time in Big Data platforms, data protection is no longer solely reliant on access controls. The actual data can be protected from external and internal threats while at rest in HDFS; in use during MapReduce, Hive, and Pig processing; and in transit to enterprise systems such as an Enterprise Data Warehouse.

CENTRAL POLICY & KEY MANAGEMENT

Protegrity's **Policy** level approach enables Security Officers to determine and specify *what, when, where* and *how* data will be protected, *who* is allowed access, and to record all attempts to access sensitive data. Protegrity also provides integrated, comprehensive **Key Management** capabilities, with an easy-to-use system.

SEPARATION OF DUTIES

The Protegrity Security Platform provides a **Separation of Duties**, isolating security administration to security officers. Database and application administrators and users are unable to access sensitive data in the clear, or grant security access to others. Since the data itself is protected, technologists – DBAs, programmers, or system engineers – can continue administering different aspects of the enterprise IT environments without disruption to business processes.

CENTRAL REPORTING

Protegrity's **Central Reporting** capability enables Security Officers to monitor the continuous enforcement of Policy throughout all protection points, while giving compliance assessors the information they need to certify compliance with applicable legal and regulatory requirements, such as PCI, HIPAA/HITECH, and PII.

protegrity

Corporate Headquarters
Protegrity USA, Inc.
5 High Ridge Park, 2nd Floor
Stamford, CT 06905
Phone: **203.326.7200**

United Kingdom
3 Regius Court
Church Road
Penn
Buckinghamshire
HP10 8RL
Phone: **+44 1494 857762**

Germany
Am Hehsel 38
22339 Hamburg
Phone: **+49 40 538 89260**

www.protegrity.com