Zettaset

SOLUTION BRIEF

BDEncrypt Plus

The Ultimate Protection for Big Data

The increased frequency and sophistication of high-profile data breaches and malicious hacking is putting organizations at continued risk of data theft and significant business disruption. The massive attack surface of big data stores like Hadoop makes them even more vulnerable to unauthorized intrusion.

BDEncrypt Plus (Big Data Encryption+) from Zettaset is an advanced encryption solution that does more than any other existing encryption product to protect Hadoop data stores and prevent unauthorized access to highly-sensitive data, ciphertext, and access control lists.

BDEncrypt Plus provides a high-performance, commercial-grade, standards-based, encryption solution that is optimized for protection, performance, and scalability in big data environments like Hadoop.

Evolving Data Exposures and Risks

There is a common misperception that encrypted data is fully protected, but even data which has been encrypted is exposed to malicious attacks and unauthorized modification. File-based encryption protects data on nodes against attackers reading files, but still is still vulnerable to write attacks on those same encrypted files (ciphertext).

If attacker can write to the ciphertext, he/she can either (1) erase data without detection or (2) mount a chosen ciphertext attack (CCA) to try to obtain the data key. Data-in-motion is an even easier target since attacker can simply modify ciphertext by performing a man-in-the-middle attack.

Zettaset BDEncrypt Plus addresses these vulnerabilities and includes unique features not found in any other data encryption solution.

Ultra-Secure Authenticated Encryption Using Associated Data (AEAD)

Zettaset BDEncrypt Plus uses AEAD architecture (vs. Encryption + MAC) to protect encrypted data from ciphertext modification. This approach ensures that encrypted data is verifiably secure. AEAD enables encryption and authentication to happen concurrently, making it easier to use and optimize than older, commonly-used modes such as CCM.

Authenticated encryption using associated data has additional advantages as part of the BDEncrypt Plus solution.

- AEAD is verifiably secure, while Encrypt + MAC is not
- AEAD using Galois/Counter mode (GCM) protects against an intruder writing to files at-rest by way of a chosen-ciphertext attack (CCA)
- AEAD improves efficiencies because of its ability to concurrently perform encryption and authentication

BDEncrypt Plus

Solution Highlights

- Provides ultra-secure authenticated encryption using associated data (AEAD) to protect data from unauthorized ciphertext modification
- Utilizes Galois/Counter encryption mode (GCM) for enhanced performance and efficiency
- Prevents outside hackers or malicious insiders from surreptitiously modifying access control lists (ACLs)
- Protects against stealthy and highly-damaging chosen-ciphertext attacks (CCAs)
- Optimized for multi-node Big Data distributed-computing architectures like Hadoop

Some otherwise secure encryption schemes, including non-authenticated encryption modes, can allow attackers to discover the encryption keys using a CCA. Non-authenticated encryption only prevents an attacker from reading the plaintext. It does not prevent an attacker from modifying the ciphertext.

The authenticated encryption mode used by BDEncrypt Plus is able to prove that the ciphertext was made by someone who was authorized to possess the encryption. Existing non-authenticated encryption products depend on the user to detect any data modification by noticing plaintext that appears to be wrong, an unreliable approach that exposes organizations to unnecessary risk.

High Performance Encryption with Galois/Counter mode (GCM)

Authenticated encryption will become mandatory due to its more stringent security properties. However, it must not compromise performance and scalability. To ensure optimal performance levels, Zettaset BDEncrypt Plus uses the Galois/Counter mode (GCM) for authenticated encryption. GCM has been identified as the only encryption mode that addresses requirements for high data-rate authenticated encryption. GCM mode encryption can efficiently achieve speeds of up to 10+ gigabits per second, and can be pipelined and parallelized.

Cryptographic Protection for Access Control Lists (ACLs)

Zettaset BDEncrypt Plus cryptographically protects access control lists and prevents an attacker from modifying ACLs and using those changes to gain access to data. Application of ACLs at every layer of access for data is critical to secure a system. An ACL is a list of permissions attached to an object that specifies which users or system processes are granted access to objects and are typically applied to data to restrict access to data to approved entities.

BDEncrypt Plus enforces file access according to policies established by the administrator. Policies can enforce access control as well as encryption. The solution has been designed for interoperability in existing IT infrastructure, and works with Active Directory, LDAP, Kerberos, and UNIX authentication mechanisms. BDEncrypt co-exists with and enhances the Apache Ranger offering by adding ACL integrity to HDFS.

Protection for HDFS Extended Attributes (Xattrs)

Extended attributes (Xattrs) provide a storage place for tags and IVs. Zettaset BDEncrypt Plus cryptographically ties Xattrs to associated files for additional protection against malicious attacks. BDEncrypt Plus uses Xattrs to (1) keep track of authentication tags, and (2) generate unique initialization vectors (IVs) for each block

Zettaset Big Data Encryption Solutions – Feature Comparison

Capability	BDEncrypt Plus	BDEncrypt
Ultra-Secure Authenticated Encryption using GCM	✓	
Cryptographic Protection for ACLs	✓	
HDFS Xattrs (extended attributes) Support	✓	
Selective File-level Encryption	✓	
Bulk Partition-level	✓	✓
Encryption	✓	✓
Compatible with Any Hadoop Distribution	✓	✓
Multiple File System Support	✓	✓
Advanced Encryption (AES) Standard 256-bit	✓	✓
AES-NI Accelerated Performance Support	✓	✓
High Performance Data-at-Rest Encryption	✓	✓
High Performance Data-in-Motion Encryption	✓	✓
Compatible with KMIP Standard Key Managers	✓	✓
Compatible with PKCS #11 Standard HSMs	✓	✓
Encrypts Existing Data	✓	✓

Customers can choose from two Zettaset Big Data Encryption products: BDEncrypt, and BDEncrypt Plus

BDEncrypt is a high-performance, partition-level encryption solution that is ideal for bulk encryption of stored data. Easily deployed via Ambari or CLI, it utilizes Advanced Encryption Standard (AES) 256-bit encryption, the highest level attainable. AES has been adopted by the U.S. government and is now used worldwide. BDEncrypt can be applied to both data-at-rest, and data-in-motion.

BDEncrypt Plus includes all of the capabilities of BDEncrypt, but is designed for selective data encryption down to the file-level. Encrypting and decrypting data at the file-level opens up the possibilities of unauthorized access, and calls for greater levels of data protection. BDEncrypt Plus provides additional protection in two unique ways: (1) Authenticated encryption and protection for cyphertext using associated data (AEAD), and (2) Cryptographic protection for access control lists (ACLs).

Protection that Addresses Compliance Requirements

Zettaset BDEncrypt solutions provide a proven defense for Hadoop in regulated industries such healthcare, financial services, and retail from the accelerating frequency and scope of data breaches. When integrated into a strategic IT security initiative, BDEncrypt can help bring Hadoop big data stores into compliance with corporate and regulatory data protection initiatives including HIPAA, HITECH, PCI, etc.

Function	Zettaset BDEncrypt Plus Capability
Verifiable Data Integrity and Authentication	Provides authenticated encryption using associated data (AEAD). Performs encryption and authentication concurrently. Guarantees data is encrypted and the authenticity of that encrypted data is protected.
Cryptographic Protection for ACLs	Cryptographically secures Access Control Lists (ACLs). Prevents an attacker from modifying the ACL and using those changes to gain unauthorized access to data.
High Performance Encryption Mode	Uses GCM (Galois/counter mode). GCM combines well-known CTR (counter) mode of encryption with the new Galois mode of authentication. Adopted for efficiency and performance in large database environments like Hadoop.
Distribution Compatibility / HDFS Xattrs Support	Compatible with any Hadoop distribution. Works with any HDFS file class including Xattrs (extended attributes) distros such as HDP, PHD, CDH, etc.
High-Granularity Encryption	High granularity. Enables admin to specify a unique key per zone, per directory, and per file. Minimizes the risk of data theft when a single user is compromised.
Multiple File System Support	Designed to support multiple files systems, including HDFS, GPFS, Isilon OneFS. Others file systems are being continually added.
Cluster / Distributed Computing-Aware	Cluster and distributed computing-aware. Optimized for HDFS. Uses distributed policy servers.
Automatic Key Zone Management	Automatically creates and manages zone keys in accordance with Active Directory.
KMIP Standard Compliance (Key Managers)	KMIP-compliant (Key Management Interoperability Protocol). Integrates with KMIP standards-based key managers from leading systems vendors including HP, Thales, IBM, Utimaco, etc. Fits into existing encryption frameworks and provides investment protection.
PKCS#11 Standard Compliance (HSMs)	PKCS#11 compliant (Public Key Cryptography Standard). Integrates with PKCS standards-based HSMs (hardware security modules) from leading vendors. Encryption keys securely stored outside of server, and data is not compromised if storage media is hacked or stolen.
Fast and Easy Deployment	Can be installed and managed with Apache Ambari or commonly-available CLI tools (Ansible, Puppet, Chef).
Additional hardware or software requirements	No additional software or hardware required. Completely self-contained software solution.

About Zettaset

Zettaset is an enterprise software company and the leader in Big Data security and management. Zettaset solutions can be effectively applied in on-premises as well as cloud deployments. Zettaset provides its critical enabling technology through a network of strategic partners. **For more information about Zettaset, contact sales@zettaset.com**

Zettaset
465 Fairchild Drive, Suite 207, Mountain View, CA 94043 // USA: +1.650.314.7920 // Fax: +1.650.314.7950
sales@zettaset.com // www.zettaset.com