Zettaset

SOLUTION BRIEF

Zettaset Encryption Suite

Data-Centric Protection for Big Data Environments

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. Complicating this scenario is the unbounded growth of Big Data and petabyte-scale data storage, new open source database and distribution schemes like Hadoop and NoSQL, and the continued adoption of cloud services by enterprises. This momentum is breaking down the traditional perimeter, forcing organizations to look at security differently, with the focus shifting from the perimeter to the data that needs to be protected.

Big Data Security Challenges

The massive attack surface of big data stores makes them highly vulnerable to unauthorized intrusion. However, much of the encryption technology that exists today was not designed for deployment in Big Data's distributed computing architectures such as Hadoop and NoSQL which consist of multiple servers that are networked together into a server array known as a cluster.

For example, distributed data systems like Hadoop require a distributed policy server, with secure policy replication to prevent unauthorized modifications to policies. Distributed systems also require automated mechanisms for secure node removal when a server is removed from a cluster, encryption for both data-at-rest and in-motion, as well as rapid and secure encryption key rotation. All of these functions must perform efficiently without requiring the re-encryption of any files or downtime during normal operation.

When it comes to securing big data in the enterprise, open source and legacy encryption solutions are compromised in many ways. For example, open source transparent data encryption (TDE) lacks basic standards-interoperability with existing KMIP-compliant key managers and PKCS#11-compliant hardware security modules (HSMs), making open source encryption difficult to fit into existing enterprise security infrastructures, and leaving encryption keys exposed. Most legacy encryption products were designed for static relational databases, and lack the ability to scale and perform well in highly-dynamic, petabyte-scale, distributed computing architectures. Very few are optimized for big data distributed file systems like HDFS.

Encryption That is Optimized for Big Data

The Zettaset Big Data Encryption Suite has been designed from the ground up for optimal performance and scalability in distributed Big Data systems like Hadoop and NoSQL, as well as the latest generation of Relational databases. The Zettaset solution delivers data-centric security utilizing advanced encryption and access control technologies to ensure the highest levels of protection of critical data.

Protection that Addresses Compliance Requirements

The Zettaset Big Data Encryption Suite provides a proven defense in regulated industries such as healthcare, financial services, and retail from the accelerating frequency and scope of data breaches. When integrated into a strategic IT security initiative, the Big Data Encryption Suite can help bring Hadoop, NoSQL and Relational big data stores into compliance with corporate and regulatory data protection initiatives including HIPAA, HITECH, and PCI.

Customers can choose from two different encryption products in the Zettaset Big Data Encryption Suite: (1) BDEncrypt, and (2) BDEncrypt Plus.

Zettaset BDEncrypt

Zettaset BDEncrypt is a high-performance, partition-level encryption solution which 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.

Zettaset BDEncrypt Solution Highlights:

- **Works in Hadoop, NoSQL, and Relational** database environments
- **Performance optimized** to meet big data scalability in distributed computing architectures (approx. 3% impact on Data-at-Rest, 7% on Data-in-Motion)

- **Selected by IBM Power Systems** to protect and secure IBM Power8 Linux Scale-out servers
- **KMIP-compliant:** Certified interoperability with existing key manager solutions from HP/Atalla, Thales, and others
- **PKCS#11-compliant:** Certified interoperability with existing Hardware Security Modules (HSM) from Utimaco, Gemalto, and others

Zettaset BDEncrypt Plus

Zettaset BDEncrypt Plus is designed for selective data encryption down to the file-level. File-based encryption protects data on nodes against attackers reading files, but still has exposure to write attacks on those same encrypted files (cipher text). If attacker can write to the cipher text, he can either (1) erase data without detection or (2) mount a chosen cipher text attack to obtain the data key. Data-in-motion is an even easier target: An attacker can simply modify cipher text by performing a man-in-the-middle attack.

BDEncrypt Plus provides additional protection against this threat in two unique ways: (1) Authenticated encryption and protection for cypher text using associated data (AEAD), and (2) Cryptographic protection for access control lists (ACLs).

Zettaset BDEncrypt Plus includes many of the capabilities associated with BDEncrypt, including performance-optimization for distributed computing systems, and KMIP/PKCS#11 compliance for interoperability with existing key managers and HSMs.

Zettaset BDEncrypt Plus Solution Highlights:

- **Distribution and database transparent**: works on any HDFS installation that supports extended attributes
- **Detects unauthorized modifications** to encrypted data, protects data integrity
- **Provides authenticated encryption** using associated data (AEAD) with Galois/Counter mode (GCM)
- **Cryptographically secures Access Control Lists (ACL)**: Prevents an attacker from modifying ACLs and using those changes to gain access to data
- **Automated key management:** Integration with HSMs via PKCS#11 and key management servers via KMIP
- **Granular crypto keys:** Can be assigned with unique keys per-zone, per-directory, or per-file
- **Multiple file system support**, including HDFS, GPFS, Isilon OneFS (others in development)
- **Kerberos integration**

Zettaset Big Data Encryption Suite - Solution Comparison

Capability	BDEncrypt Plus	BDEncrypt
Protects Integrity of Encrypted Data	✓	
Authenticated Encryption using Galois/Counter Mode	✓	
Cryptographic Protection for Access Control Lists	✓	
HDFS Extended Attributes (Xattrs) Support	✓	
Selective File-level Encryption	✓	
Bulk Partition-level Encryption		✓
Compatible with Any Hadoop Distribution	✓	✓
Multiple File System Support	✓	✓
Advanced Encryption Standard (AES) 256-bit encryption	✓	✓
AES-NI Accelerated Performance Support	✓	✓
Data-at-Rest Encryption	✓	✓
Data-in-Motion Encryption	✓	✓
Compatible with KMIP-compliant (Key Management Interoperability Protocol) Key Managers	✓	✓
Compatible with PKCS-compliant (Public Key Cryptography Standard) #11 HSMs	✓	✓
Manageable via Ambari or CLI	✓	✓

Strategic Partnerships and Interoperability Certifications

The Zettaset Big Data Encryption Suite technology provides proven interoperability between enterprise key managers, cryptographic devices and range of storage, security and cloud products. It has been tested and certified for interoperability with our strategic systems and security partners, including:

- **Hortonworks Distribution Platform** for Hadoop (HDP), and Ambari management.
- **Gemalto (SafeNet)** - key management systems
- **HPE Security** – Enterprise System Key Manager
- **IBM** - Power Linux Scale-out Systems
- **Thales e-Security** - key management systems
- **Utimaco** - hardware security modules