Bloombase and Entrust protect storage infrastructure to mitigate data breaches

Joint solution secures sensitive information in traditional and next-generation data centers

HIGHLIGHTS

- Discover sensitive information across data-at-rest resources utilizing artificial intelligence
- Provide dynamic access control of structured/unstructured data using machine learning
- Encrypt heterogeneous storage and control access to trusted hosts and applications
- Provide a FIPS 140-2 Level 3 platform on-premises or as a service for centralized key management and securevng FS a-3.4 (g)-itntrseTm[illegible]a)-[illegible]n3 (e)-[illegible]3 (co[illegible]JE[illegible])-11.Intri[illegible](e)-1[illegible]4 (g)-15[illegible](e)waTm[illegible]h)-[illegible]3 (d11.[illegible](a)a

data center (SDDC) technologies, highlights data storage infrastructure as a prime target for attack. Encryption protects data privacy, however the techniques used to encrypt data can vary among software applications and storage technologies. With diverse applications deployed across an increasingly decentralized environment, effectively protecting the growing volume of sensitive data is crucial to ensure secure computing of mission critical applications to achieve business automation.

The challenge: securing heterogeneous storage environments with a holistic protection approach

Enterprises are migrating from on-premises disk systems to cloud-based storage services to better-manage the increasing need of data capacity. The trend has been accompanied by a shift from selective encryption of data classified as sensitive, to a policy that encrypts everything in storage. The degree to which organizations can trust this approach depends directly on the protection of cryptographic keys. Encryption keys underpin security, and safeguarding and managing them is critically important.

As more data gets encrypted, more keys need to be secured and managed to protect data in storage and to ensure it can be decrypted when needed.

The solution: Bloombase and Entrust together deliver high performance and enhanced security to heterogeneous storage infrastructures

Leveraging artificial intelligence (AI) and deep machine learning (ML) technologies, Bloombase StoreSafe provides autonomous discovery, dynamic access control, and lifecycle cryptographic protection of sensitive data-at-rest, both structured and unstructured, managed in on-premises storage systems and off-premises cloud storage services. Its application-transparent and protocol-preserving features enable it to protect the entire spectrum of storage infrastructures from on-premises, to virtualized, big data repositories, and cloud storage services. Bloombase StoreSafe operates as a storage proxy, encrypting data before it is physically stored, and deciphering the stored ciphertext on the fly only when presented to trusted applications and hosts. The schema guarantees [illegible] is astru00[illegible]3.4[illegible]T[illegible]

Encryption keys handled outside the cryptographic boundary of a certified HSM are significantly more vulnerable to attack, which can lead to compromise of critical keys. HSMs offer a proven and auditable way to secure valuable cryptographic material. nShield HSMs integrate with Bloombase StoreSafe to provide comprehensive logical and physical protection of keys.

nShield Connect HSMs enables Bloombase customers to:

- Secure keys within carefully designed