Bloombase and Entrust protect storage infrastructure to mitigate data breaches

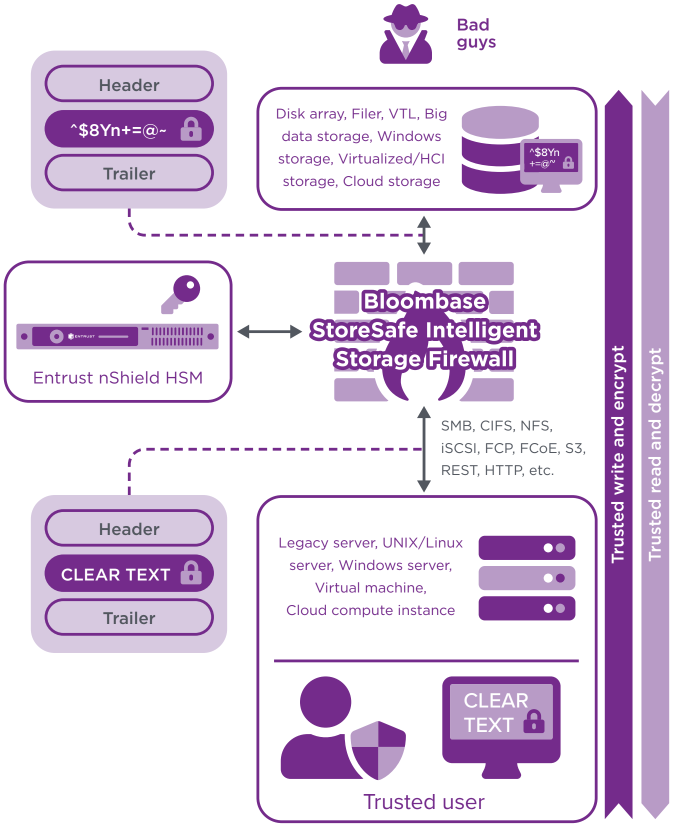
Joint solution secures sensitive information in traditional and next-generation data centers

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 security-hardened key protection
- Facilities compliance with data privacy and security regulations

The problem: sensitive big data is a prime target for cyber attacks and data breaches

Organizations capture and store increasing volume of data, including private and sensitive data, for advanced analytics and business intelligence purposes. This big-data trend, combined with the growing amount of data generated by Internet of things (IoT) smart devices, backed by software-defined


Bad guys
Header
^$8Yn+=@~
Trailer
Disk array, Filer, VTL, Big data storage, Windows storage, Virtualized/HCI storage, Cloud storage
^$8Yn +=@~
Entrust nShield HSM
Bloombase StoreSafe Intelligent Storage Firewall
SMB, CIFS, NFS, iSCSI, FCP, FCoE, S3, REST, HTTP, etc.
Header
CLEAR TEXT
Trailer
Legacy server, UNIX/Linux server, Windows server, Virtual machine, Cloud compute instance
CLEAR TEXT
Trusted user
Trusted write and encrypt
Trusted read and decrypt

Bloombase StoreSafe secures sensitive information in traditional and next generation datacenters with Entrust nShield® HSMs deployed on-premises or as a service.

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 operational transparency and maximum interoperability, while ensuring that unauthorized parties are unable to access the sensitive information without breaking encryption.

Bloombase customers can leverage trusted cryptography solutions from Entrust to facilitate compliance with regulatory requirements. Depending on the deployment environment, customers can integrate Bloombase StoreSafe with nShield hardware security module (HSM). nShield HSMs provides a FIPS 140-2 Level 3 environment for tamper-evident and tamper-resistant protection of cryptographic keys. Customers can deploy nShield Connect HSMs on-premises or as a service to enable compliance with regulatory requirements for multi-national business and government agencies.

Why use Entrust nShield with Bloombase StoreSafe?

Bloombase StoreSafe data-at-rest security technology coupled with the nShield HSMs offer an unprecedented combination of a turn-key, non-disruptive, and application transparent stored data encryption solution with a powerful and centralized key management system for traditional and next-generation data center environments.

Bloombase and Entrust protect storage infrastructure to mitigate data breaches

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 cryptographic boundaries that use robust access control mechanisms, so keys are only used for their authorized purpose
- Ensure key availability by using sophisticated management, storage, and redundancy features to guarantee they are always accessible when needed by the encrypted storage systems and services
- Deliver superior performance to support real-time high-bandwidth storage cryptographic applications

nShield Connect HSMs provide a hardened, tamper-resistant environment for performing secure cryptographic processing, key protection, and key management. With Entrust HSMs you can:

- Provide a tightly controlled tamper resistant environment for safekeeping and managing encryption keys
- Enforce key use policies, separating security functions from administrative tasks
- Interface with applications using industry-standard APIs (PKCS#11, OpenSSL, JCE, CAPI, CNG, nCore, and nShield Web Services when used in conjunction with Web Services Option Pack)

Entrust HSMs

Entrust nShield HSMs are among the highest-performing, most secure and easy-to-integrate HSM solutions available, facilitating regulatory compliance and delivering the highest levels of data and application security for enterprise, financial and government organizations. Our unique Security World key management architecture provides strong, granular controls over access and usage of keys.

BLOOMBASE

Bloombase StoreSafe delivers data-at-rest security for sensitive information managed in traditional data centers and hybrid cloud environment. The purpose-built scalable architecture:

- Protects on-premises storage systems including SAN, NAS, DAS, tape library, and virtual tape library (VTL), regardless of complexity and heterogeneity of the storage infrastructure and protocol
- Secures data in RESTful cloud storage service endpoints, hypervisor datastores, content addressable storage (CAS), and object stores
- Helps organizations mitigate data exfiltration threats and meet data privacy regulatory mandates

www.bloombase.com

Learn more

To find out more about Entrust nShield HSMs visit **entrust.com/HSM**. To learn more about Entrust's digital security solutions for identities, access, communications and data visit **entrust.com**

To find out more about
Entrust nShield HSMs

HSMinfo@entrust.com

entrust.com/HSM

ABOUT ENTRUST CORPORATION

Entrust keeps the world moving safely by enabling trusted identities, payments and data protection. Today more than ever, people demand seamless, secure experiences, whether they're crossing borders, making a purchase, accessing e-government services or logging into corporate networks. Entrust offers an unmatched breadth of digital security and credential issuance solutions at the very heart of all these interactions. With more than 2,500 colleagues, a network of global partners, and customers in over 150 countries, it's no wonder the world's most entrusted organizations trust us.

Learn more at
entrust.com/HSM

ENTRUST

Contact us:
HSMinfo@entrust.com