

BLOOMBASE STORESAFE INTELLIGENT STORAGE FIREWALL

Safeguarding Crown Jewels from Data Breach for Virtual Data Center and Hybrid Cloud

The Increasing Complexity of Mitigating Catastrophic Data Exposure Vulnerabilities

For any large-scale organization, data leakage remains a critical, yet unresolved problem. The causes can be both intentional (hardware theft, cyberattack, espionage and so on) and unintentional (media loss, buggy application, and so on). The unbridled rate at which businesses are taking advantage of cloud computing is only going to exacerbate the problem: Increased risk of information exfiltration regardless the number of network defenses in place.

A paradigm shift in the approach to data storage management is evident: There has been a move away from structured to unstructured data, resulting in spreading out of crown jewels to virtually every dataset. There is also a concomitant change in the way stored data is managed: from on-premises storage systems to datasources in virtualization and cloud storage services. Despite encryption of data-at-rest as an effective measure assuring the last line of defense in event of data breach, the increased sophistication of cyberattacks targeting at the heterogeneous datacenter environment renders traditional database encryption tools and encryption hardware inadequate, if not useless.

Bloombase StoreSafe for VMware Cloud on AWS Simplifies Data-at-Rest Protection for High Security Cloud Computing

Bloombase StoreSafe intelligent storage firewall provides automatic protection of data-at-rest for workloads running on VMware Cloud on AWS enabling business-critical applications and invaluable crown jewels to be migrated to the cloud seamlessly and securely. The solution addresses intensifying cyberattack challenges, supports evolving datacenter transformation, and helps accelerate adoption of cloud computing model for mission-critical applications.

VMware Cloud on AWS enables customers to run, manage and secure applications in a production-ready, simple and consistent hybrid IT environment. The service enables organizations to continue using existing VMware tools to manage VMware Cloud on AWS environments without having to purchase custom hardware, rewrite applications, or modify their operating model. With access to the broad range of AWS services, and the functionality, elasticity, and security customers have come to expect from the AWS Cloud, the service lays the foundation to run, manage and secure production applications across vSphere®-based private, public and hybrid cloud environments with access to innovative AWS services.

VMware Cloud on AWS Key Benefits

- Unified and operationally consistent hybrid cloud experience across vSphere-based private clouds and VMware Cloud on AWS
- Workload portability and flexible consumption options with single support owner and attractive TCO
- Familiar management tools eliminate the need to retrain staff (vCenter, vSphere

Bringing together best-of-breed technologies and capabilities that create a seamless and flexible hybrid cloud future for customers, VMware and AWS enable services that easily grow and evolve as enterprise needs change. Whether expanding services on-premises or in the public cloud, the VMware Cloud on AWS eliminates the need to make changes to operating models or architectures. The result is the most flexible approach to evolving enterprise cloud strategies to keep pace with digital transformation in business environments.

PARTNER SOLUTION BENEFITS

Security Hardened Cloud Computing

Automates security protection of data to lower the risk and impact of data breach with a unified line of defense from virtual datacenter to the cloud

Platform Agnostic and Open

Offers multi-tenancy security of data-at-rest for any software applications, OSes, storage protocols and datacenter infrastructure technologies requiring no proprietary hardware

Operational Transparent

Provides scalable and flexible application-transparent data-at-rest security protection with zero workflow change to administrators, operations and end users

Security Proven

Mitigates data leakage vulnerabilities by delivering cryptographic services certified at NIST FIPS 140-2 industry standard

Centralized Key Management

Integrates with optional OASIS KMIP key managers, PKCS#11 HSMs, Amazon CloudHSM and KMS for centralized lifecycle key management

Simplified Compliance

Protects sensitive data-at-rest, and helps enable compliance with data privacy and security regulations with clear audit visibility

LEARN MORE

For more information, visit

<https://marketplace.vmware.com/vsx/solutions/bloombase-storesafe-security-server>

and

<https://www.bloombase.com>

API, PowerCLI and modern HTML5-based vSphere Client)

- VMware-delivered service creates zero lifecycle management while enabling customers to retain control of application management and operation
- Lays the foundation for integration of 3rd party tools from leading ecosystem partners.

Partner Solution Overview

Bloombase StoreSafe is an agentless, turnkey, application-transparent, high performance unified stored data security solution which automatically discovers crown jewels and locks them down proactively with a non-disruptive deployment approach: protocol preserving with no operational change to application infrastructure nor daily operations. Bloombase StoreSafe works almost like a firewall in the storage network environment for trusted hosts in form of virtual machine (VM) or cloud compute instance providing encryption as software applications write, and un-encryption as they read. Unlike traditional data encryption tools which require hardware retrofitting and expensive software upgrades, the Bloombase solution operates as a holistic security virtual appliance with an expansive reach over heterogeneous storage protocols (FCP, iSCSI, NFS, SMB, CIFS, S3, REST, and so on) for both on-premises VMware vSphere and off-premises VMware Cloud on AWS.

Leveraging optional Amazon CloudHSM and KMS for centralized key management, not only Bloombase StoreSafe secures VM disks and vSAN-backed datastores, but also cloud storage services including Amazon Elastic File System (EFS), Simple Storage Service (S3) and Elastic Block Store (EBS). Bloombase's software-defined architecture is future-proofed to meet infrastructure changes through scalability and flexibility to deliver secure data services for hyperconverged infrastructure (HCI), private, hybrid and public cloud. As an independent add-on software, Bloombase

delivers security, integrity and helps maintain true separation of duties, enabling organizations to meet data privacy regulatory compliance mandates (GDPR, PCI DSS, HIPAA, PDPL, and so on) easily and cost-effectively.

Figure 1: Bloombase StoreSafe for VMware Cloud on AWS data-at-rest security solution provides turnkey encryption to help organizations meet data confidentiality regulatory compliance requirements

