BLOOMBASE®

OVA MEMBER
OPEN VIRTUALIZATION ALLIANCE

Solution Brief

# Bloombase Secure Computing for KVM Virtual Data Center

Bloombase at-rest data security software platform provides turnkey, agentless, non-disruptive, application-transparent encryption of storage data for enterprise virtual datacenters powered by KVM. The solution can help to:

- Secure your KVM virtual machines (VM) and disks (VMDK)
- Provide multi-tenancy encryption protection of KVM-based virtual desktop infrastructure (VDI)
- Protect your business critical and time sensitive data in virtually all kinds of enterprise scale storage systems from SAN, NAS, tape library, VTL, virtual storage, cloud and beyond
- Mitigate outbound threats and data leakage caused by insiders and managed services providers (MSP)
- Quickly and securely retrieve your secret cipher-data for various trusted and authorized applications as-if they are in plain-text
- Immediately meet various stringent data confidentiality and secrecy regulatory compliance requirements
- Maximize your return on investment (ROI) with easy-to-implement, scalable security-hardened KVM platform for multi-tenancy, mixed operating system, and heterogeneous vendor private cloud applications
- Easily manage security rules and encryption policies of your business critical data

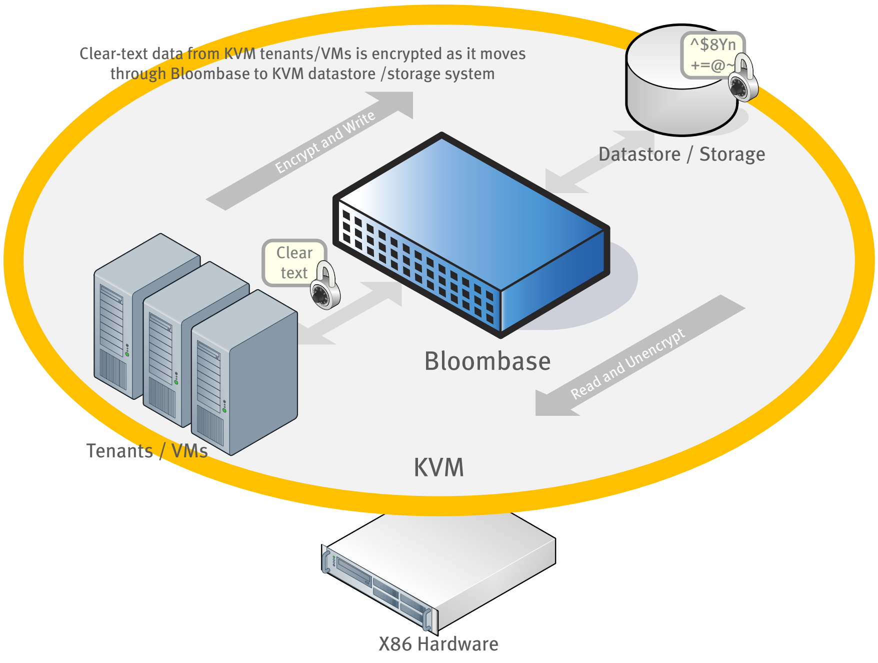
Enterprise data breaches have seen on the sharp increase in terms of spread and scale, despite the numerous IT security measures and best practices implemented. Various studies pointed out data exposure is caused by a range of threats: hardware theft, backup tape loss, viral attacks, malwares or insider threats. The paradigm shift of core data to virtual data center and cloud could open up new kinds of attacks which may lead to catastrophic business secret leakage.

Traditional Information Technology security measures regard outsiders as the originators of cyber-attacks. Technologies such as firewalls, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), content filters, anti-virus, anti-malware, anti -spyware, SSL-VPN, Unified Threat Management (UTM), all sit at the frontline defending the perimeter of core IT infrastructure.

The fact that insider threats, targeted attacks and unknown attacks are on the rise, sensitive data residing on core enterprise storage in plain-text leaves computing systems with huge vulnerabilities. Data encryption is technically recognized as the last line of defense as mandated by numerous industry best practices to combat data exposure. Nevertheless, enterprises choosing application-specific encryption usually have to put forth unbalanced effort on implementation and as a result push the mission-critical applications towards degraded performance and increased risks.

Bloombase at-rest data encryption solution enables transformative data privacy and operational efficiency over and above what was previously achievable only with drastic application changes requiring tremendous second development at hosts and applications that are costly and risky.

With Bloombase transparent storage encryption, even the most complex and throughput demanding data services will benefit from the privacy and integrity assurance


Clear-text data from KVM tenants/VMs is encrypted as it moves
through Bloombase to KVM datastore /storage system
^$8Yn
+=@~
Encrypt and Write
Datastore / Storage
Clear
text
Bloombase
Read and Unencrypt
Tenants / VMs
KVM
X86 Hardware

capabilities for data availability, security and scalability.

Bloombase empowers KVM organizational customers to securely encrypt virtual machines and virtual storage systems that is hardly achievable by traditional hardware encryption products, accelerating transition from physical to virtual data center infrastructure without having the tradeoff between virtualization and security.

Bloombase agentless encryption security solution can flexibly be deployed as a physical appliance or a virtual appliance on KVM as a separate tenant. It works as a storage proxy providing transparent encryption and un-encryption of KVM data stores securing virtual disk drives in form of VMDK files.

Rather than as closed and proprietary hardware appliances, Bloombase assumes an entirely software-based approach in providing real-time encryption of enterprise storage systems which is platform portable, scalable and extensible.

Riding on KVM the industry proven rock-solid, small foot-print, fast I/O and efficient process technologies, Bloombase data encryption virtual appliance sets a record-breaking and new level in virtual data center information encryption security.

Authorized hosts and trusted applications leverage virtual storage resources provided by Bloombase for encryption and un-encryption of at-rest data stored at backend storage services. When host applications, tenants or KVM hypervisor write plain-text data to backend storage via Bloombase, the encryption engine extracts plain payloads and converts them as cipher-text in real-time before they get persisted at the actual storage media. Reversing the process, as storage hosts read from actual storage through Bloombase, the unencryption engine is triggered to retrieve cipher-text from storage and converts them to virtual plain-text on-the-fly before getting recomposed as plain payloads and presented to hosts and applications. Storage data in the KVM-powered virtual data center stays naturally encrypted and permanently locked, therefore, it is private and safe.

OS-dependent data encryption tools require drastic and potentially risky platform changes which is difficult to manage and maintain over time. Encryption at storage is impossible without the expense of costly hardware replacement. Bloombase provides easy to deploy, effortless and cost-effective at-rest data encryption software that works to secure data moving within KVM virtual data center infrastructure in a fully open, scalable and naturally virtualized architecture.

Bloombase transparent data security solution supports the open and industry standard KVM technology that will persist over time. Not only does it protect virtual machines, but Bloombase is designed to secure virtual desktop infrastructure, virtual storage, physical storage and host, thereby providing cost efficiency and manageability. Bloombase brings a rich selection of security features that meet multiple and heterogeneous security requirements from a range of industry verticals and geographies. It scales easily with the resources allocated on KVM it runs on, ensuring emerging encryption requirements are fulfilled dynamically and efficiently. Bloombase clustering option is fault-tolerant and highly available to ready large enterprise scale customers for mission critical secure data services.

Bloombase enables you meet various stringent data privacy regulatory compliance with a low-cost, turnkey approach that delivers critical information protection at the last line of defense in your KVM virtual data center environment.

## What is KVM

KVM (Kernel-based Virtual Machine) is the leading open source complete virtualization solution on X86 hardware and it supports all major operating systems including Linux and Windows. KVM enables organizations to be agile by providing robust flexibility and scalability that fit their specific business demands. KVM converts the Linux kernel into a bare metal hypervisor and it leverages the advanced features of Intel VT-X and AMD-V X86 hardware, thus delivering unsurpassed performance levels. In addition, KVM incorporates Linux security features including SELinux (Security-Enhanced Linux) developed by the US Security Agency to add access controls, multi-level and multi-category security as well as policy enforcement. As a result, organizations are protected from compromised virtual machines which are isolated and cannot be accessed by any other processes.

## What is Open Virtualization Alliance (OVA)

The mission of the Open Virtualization Alliance (OVA) is to foster the adoption of KVM as an open virtualization alternative, accelerate the emergence of an ecosystem of third-party solutions around KVM, increase overall awareness and understanding of KVM, encourage interoperability, promote best practices and highlight examples of customer successes. Founding members of the Open Virtualization Alliance include HP, IBM, Intel, and Red Hat. For more information about the Open Virtualization Alliance and its members, visit http://www.openvirtualizationalliance.org.

Bloombase is a member of Open Virtualization Alliance since 2011.

## Learn More

To learn more about Bloombase transparent data security solutions, contact your Bloombase sales representative, or visit http://www.bloombase.com

BLOOMBASE®

**Bloombase** - Next Generation Data Security **email** info@bloombase.com **web** http://www.bloombase.com