SOLUTION BRIEF

Virtual Machine Encryption for Microsoft Azure with SafeNet ProtectV™

Cloud services from Microsoft Azure provide the agility, elasticity, capacity, and redundancy required for organizations to maintain a competitive advantage in the market. On-demand delivery of these IT resources, with pay-as-you-go pricing, has convinced many organizations to adopt Microsoft Azure—with substantial cost and efficiency benefits.

Some applications and data require additional security due to rigorous contractual or regulatory requirements. Until now, companies had to store sensitive data (and/or the encryption keys protecting it) in on-premises data centers. Unfortunately, this either prevented migration of these applications to the cloud or significantly slowed their performance.

The Gemalto and Microsoft Solution

Microsoft and Gemalto have teamed up to protect virtual machines and storage volumes in Microsoft Azure so organizations can securely adopt the cloud.

With SafeNet ProtectV™ and SafeNet KeySecure or Virtual KeySecure organizations can place sensitive workloads in Microsoft Azure—no matter what level of security is needed. Best of all, the entire solution set is available for purchase on the Microsoft Azure Marketplace.

SafeNet ProtectV: Virtual Machine, Cloud Instance and Bare Metal Server Encryption

SafeNet ProtectV™ provides volume-level encryption of bare metal servers, virtual machine instances in the Microsoft Azure cloud so organizations can securely run sensitive workloads containing highly regulated data off-premises. SafeNet ProtectV's StartGuard™ pre-boot authentication prevents any protected virtual machine from booting unless the appropriate credentials are provided by the SafeNet ProtectV Manager. Such a requirement prevents copied or stolen virtual machines from being booted in unauthorized environments. Additionally, it means that all virtual machines are administered from a central point – the SafeNet ProtectV Manager – to improve oversight and reduce the likelihood of errors or abuse.

KEY BENEFITS

Complete virtual machine and storage encryption:

- Encrypt entire virtual machines and their associated storage volumes
- No data is written to system partition or storage volume disk without first being encrypted
- Even data stored in the OS partition is secured

The tools customers need to stay compliant in the cloud:

- Undisputed command and proof of ownership for data and keys
- Only authorized individuals can launch VMs
- Prevents unauthorized data exposure or super-user abuse
- Helps meet a range of regulations, such as PCI and PAA

SafeNet KeySecure: Robust, Centralized Enterprise Key Management

SafeNet KeySecure is a FIPS 140-2 (level 1 or 3) validated encryption and key management appliance (available as a hardware or as a virtual appliance – SafeNet Virtual KeySecure) that streamlines encryption management across the enterprise – from either on-premises or the Microsoft Azure cloud. SafeNet KeySecure integrates with SafeNet ProtectV, the SafeNet Data Protection portfolio, native encryption (TDE) from database vendors, Linux Unified Key Setup (LUKS), and a broad portfolio of third-party partners via the Key Management Interoperability Protocol (KMIP) standard to eliminate silos within an organization. SafeNet KeySecure puts administrators in full control of their data to ensure that it is used only as authorized and is protected from a variety of threats both known and unforeseen.

Together with SafeNet KeySecure, SafeNet ProtectV provides a convenient cloud-ready encryption solution that secures data and addresses numerous industry security standards and government regulations to make the cloud feasible for the enterprise. Regardless of where an organization's workloads reside – whether on-premises or in the Microsoft Azure cloud – you can separate security administration duties, enforce granular controls and establish clear accountability with audit trails and detailed compliance reporting.

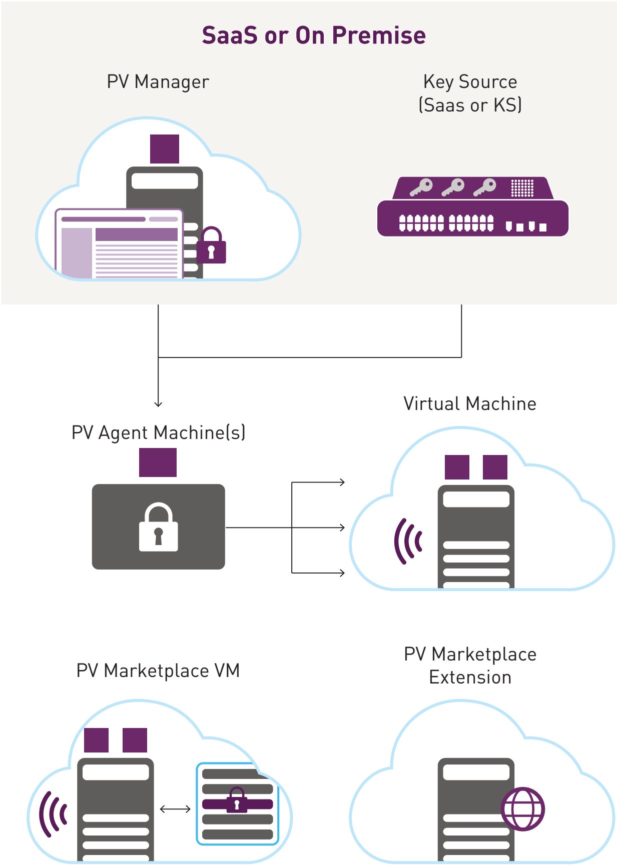
KEY BENEFITS

Save money with subscription pricing:

- SafeNet ProtectV is available in the Microsoft Azure Marketplace as a pay-as-you go subscription and the first 30-days are free!
- Subscriptions are cheaper and better suited for operating expenditure (op-ex) models compared to capital expenditure (cap-ex) models where hardware is purchased with upfront payment.

Maintain Full Data Control Throughout Migration to the Cloud

By encrypting the entire virtual machine, SafeNet ProtectV also encrypts all of the data residing in the instance. Once encrypted, all archives, snapshots and backups of these instances remain secure regardless of where they're copied, stored, or archived. Additionally, SafeNet ProtectV's StartGuard makes virtual machines impossible to instantiate without authorization. Through SafeNet ProtectV's pre-boot authentication requirement customers can track all encrypted instances even when copied or archived, ultimately providing an audit trail of all actions and copies of the customer's data.



Separate Duties Among Administrators

SafeNet ProtectV's encryption obfuscates data rendering it unreadable to the administrators managing the storage environment. SafeNet ProtectV integrates with SafeNet KeySecure and Virtual KeySecure, to place control of the encryption keys in the customer's hands. Deployed together, customers have the ability to separate security and storage duties amongst administrators – both internal and external to the customer's organization. By bringing these operations fully under their control from a single management point, customers can ensure that privileged users in the cloud pose no threat to the sensitive data.

Flexible key management options

SafeNet ProtectV integrates with SafeNet KeySecure and SafeNet Virtual KeySecure for key and policy management so customers can retain full control of their data and ownership of their encryption keys and the surrounding policies - even as everything resides with the cloud service provider.

Depending on assurance needs, customers can deploy a physical key management server (SafeNet KeySecure) on-premises, or a virtual appliance. From either of these models, administrators can use SafeNet ProtectV to secure their cloud stored data while ensuring full - and sole - control of their encryption keys.

Conclusion

SafeNet ProtectV makes migrating and storing sensitive data on Microsoft Azure safer and easier for enterprises while enabling them to preserve full control of their data through the effective and secure management of encryption and the encryption keys securing that data.

To learn more, visit https://safenet.gemalto.com/partners/microsoft/

About Gemalto's SafeNet Identity and Data Protection Solutions

Through its acquisition of SafeNet, Gemalto offers one of the most complete portfolios of enterprise security solutions in the world, enabling its customers to enjoy industry-leading protection of data, digital identities, payments and transactions – from the edge to the core. Gemalto's newly expanded portfolio of SafeNet Identity and Data Protection solutions enables enterprises across many verticals, including major financial institutions and governments, to take a data-centric approach to security by utilizing innovative encryption methods, best-in-class crypto management techniques, and strong authentication and identity management solutions to protect what matters, where it matters. Through these solutions, Gemalto helps organizations achieve compliance with stringent data privacy regulations and ensure that sensitive corporate assets, customer information, and digital transactions are safe from exposure and manipulation in order to protect customer trust in an increasingly digital world.

Contact Us: For all office locations and contact information, please visit safenet.gemalto.com/contact-us

Follow Us: blog.gemalto.com/security

GEMALTO.COM

gemalto
security to be free