As businesses turn to elastic cloud services like Microsoft Azure to run their critical applications, security and compliance remain top concerns; SafeNet ProtectV solves this challenge in Microsoft Azure by delivering an easy way to protect sensitive, highly-regulated data in the cloud. SafeNet ProtectV encrypts entire virtual machine instances and attached storage volumes, so Microsoft Azure customers can separate security administration duties, enforce granular controls and establish clear accountability with audit trails to achieve regulatory compliance as they take advantage of the cloud.

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 to 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.

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.

KEY BENEFITS

The tools that customers need to stay compliant on Microsoft Azure:
> Encryption of entire virtual machines and their associated storage volumes
> Undisputed command and proof of ownership for data and keys
> Only authorized individuals can launch VMs
> Prevents unauthorized data exposure or super-user abuse

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.

Separate Security Administration Duties
With SafeNet ProtectV, customers can separate security and storage duties amongst administrators – both internal and external to their organization. Encrypted virtual machines are only accessible to the customer or authorized key holder. Cloud administrators - or anyone with access to the cloud environment - can perform their job responsibilities without ever having access to the cleartext data on the virtual machine. By bringing these operations fully under their control from a single management point, they can ensure that privileged users in the cloud pose no threat to sensitive data.

Retain and Demonstrate Data Control
Data retrieval and digital shredding remain the enterprise’s responsibility when their data are hosted by cloud service providers such as Microsoft Azure. SafeNet ProtectV renders stolen or hidden data copies useless to unauthorized users wherever they are located. By centralizing key management and
policy enforcement with SafeNet solutions, customers simplify and streamline security oversight to reduce the risk of errors and improve their ability to demonstrate data control and regulatory compliance.

Encrypting virtual machines individually allows organizations to implement more finely tailored security and control in multi-tenant environments. For example, HR and finance teams can access the virtual machines unique to their business units containing their sensitive, regulated data without having access to any other machine and data in their cloud. All of the policies for these secured machines are managed from the SafeNet ProtectV Manager and SafeNet KeySecure (or SafeNet Virtual KeySecure).

**Establish Clear Accountability**
SafeNet ProtectV encrypts entire virtual machines and bare metal servers at the volume level to secure all of the data residing on the server. Once encrypted, all instance archives, snapshots and backups remain secure regardless of their location. SafeNet ProtectV’s Startguard pre-boot authentication makes it impossible to instantiate virtual machines without appropriate authorization. This requirement allows customers to track all encrypted instances even when copied or archived leaving an audit trail for all copies of the customers’ 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 (SafeNet Virtual KeySecure) from the Microsoft Azure marketplace. From either of these approaches, administrators can use SafeNet ProtectV to secure their cloud stored data while ensuring full - and sole - control of their encryption keys.

**Conclusion**
SafeNet ProtectV, available in the Microsoft Azure Marketplace, allows Microsoft Azure customers to encrypt and protect their most sensitive data and applications on Microsoft Azure while maintaining compliance requirements and achieving high levels of data protection.

Get started today with a 30-day free trial of SafeNet ProtectV in the Microsoft Azure Marketplace.

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

**About Gemalto’s SafeNet Identity and Data Protection Solutions**
Gemalto offers one of the most complete portfolios of enterprise security solutions in the world, enabling its customers to enjoy industry-leading protection of digital identities, transactions, payments, and data – from the edge to the core. Gemalto’s portfolio of SafeNet Identity and Data Protection solutions enable 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

**Follow Us:** blog.gemalto.com/security

©Gemalto 2017. All rights reserved. Gemalto, the Gemalto logo, are trademarks and service marks of Gemalto and are registered in certain countries. SB (EN)-date 13Dec2017 - Design: RM