SOLUTION BROCHURE

Backup and Recovery With Veeam & Entrust KeyControl

veeam

ENTRUST
SECURING A WORLD IN MOTION

Overview

In today's digital age, data is one of the most valuable assets for individuals and organizations. Destructive malware, such as ransomware, is an increasing concern due to its potential to cause irreversible loss, corruption, or unauthorized modification of critical data. The need for robust backup and recovery solutions in the data protection domain is more important than ever. These solutions ensure that data is not only preserved but also recoverable in the event of data loss due to hardware failures, cyber threats such as ransomware attacks, human errors, or even natural disasters. Without effective backup and recovery strategies, the consequences for an organization can be dire, including significant financial losses, reputational damage, and operational disruptions.

Vendors like Veeam provide comprehensive data management platforms that ensure reliable data protection, seamless recovery, and simplified administration. As a central component of the Veeam Data Platform, Veeam Backup & Replication™ protects, backs up, and restores a broad range of workloads – including virtual machines, physical servers, and cloud-based environments. With features like incremental backups, disaster recovery replication, and fast, granular restores, it ensures that critical data and systems remain secure, recoverable, and continuously accessible.

The Importance of Protecting Backups

When it comes to data security, one often-overlooked area is the protection of backups. Even if your primary systems are well-secured, any copies of your data – whether stored on external drives, in the cloud, or on network-attached storage – must also be safeguarded. Encrypting backups is critical because it ensures that, if those secondary storage locations are compromised, the attacker only gains access to unreadable, encrypted data rather than fully visible, valuable information.

Implementing encryption for backups is more than simply choosing an encryption algorithm. It involves a strategic and well-structured approach, including the management of cryptographic keys. The keys used to secure and decrypt data, particularly backup data, must be handled with utmost care.

This is where robust key management systems (KMSs) come into play. A KMS provides a secure environment for creating, storing, distributing, and retiring cryptographic keys. By restricting key access to authorized systems and individuals, a KMS significantly reduces the risk of unauthorized decryption, helping maintain the confidentiality and integrity of sensitive data in complex IT environments.

At the core of their functionality, KMS solutions streamline the entire key lifecycle – from initial generation and secure storage to controlled usage and timely revocation. By employing effective key management practices, organizations ensure that encryption keys are both readily available when required for legitimate operations and firmly protected against potential threats.

How a KMS Enhances Backup Security

Separation of Duties

A KMS separates backup operations from key management, ensuring no single party controls both data and the keys that protect it. This separation reduces insider threats and adds an extra layer of security to your backup environment.

Strict Access Controls

Robust authentication and authorization measures ensure that only authorized personnel, systems, and applications can access or modify encryption keys. Such controls help prevent unauthorized access and strengthen the overall security posture.

Regular and Automated Key Rotation

The backup solution can be configured to automatically rotate encryption keys at predetermined intervals or in response to specific triggers. The rotation is performed using the Key Management Interoperability Protocol (KMIP) interface of the KMS. This approach reduces the window of opportunity for attackers and mitigates the impact of a potential key compromise.

Comprehensive Auditing and Compliance

A KMS provides detailed audit logs for every key-related operation, enabling organizations to track key usage, demonstrate adherence to regulatory requirements, and quickly identify any suspicious activities.

Audit logs can be automatically forwarded to a third-party Security Information and Event Management (SIEM) platform for centralized analysis, enabling faster threat detection, streamlined incident response, and more effective overall security oversight.

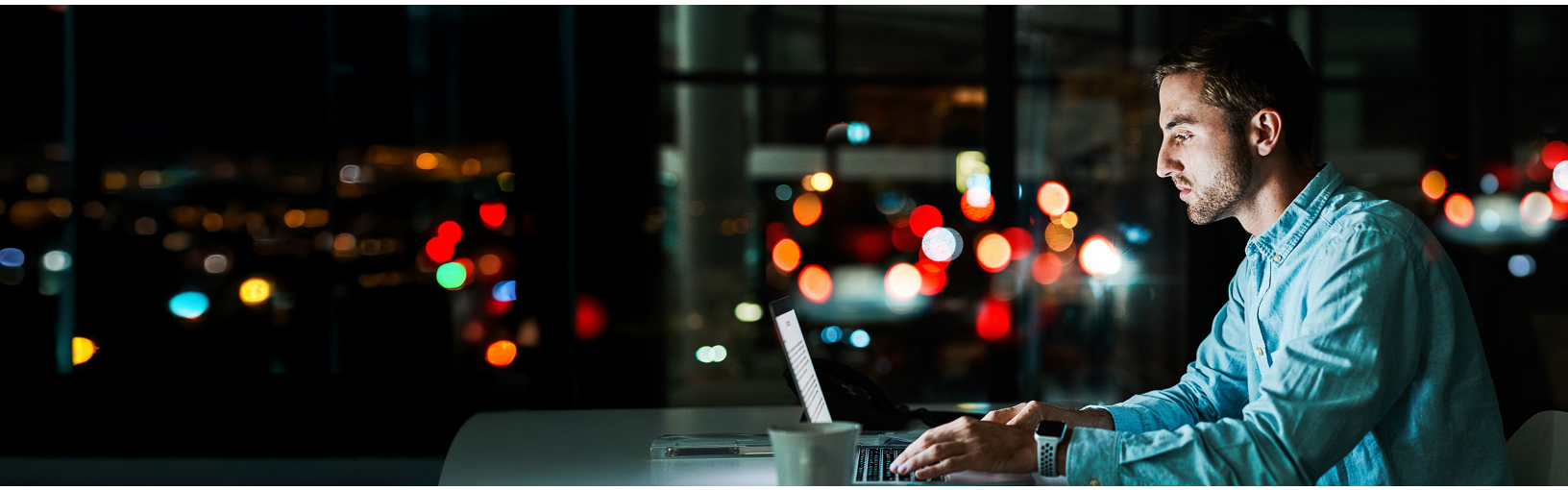
Secure Storage and Distribution of Keys

Leveraging strong encryption and secure communication protocols, a KMS ensures that keys remain confidential and protected from unauthorized access – whether at rest or in transit – throughout their entire lifecycle.

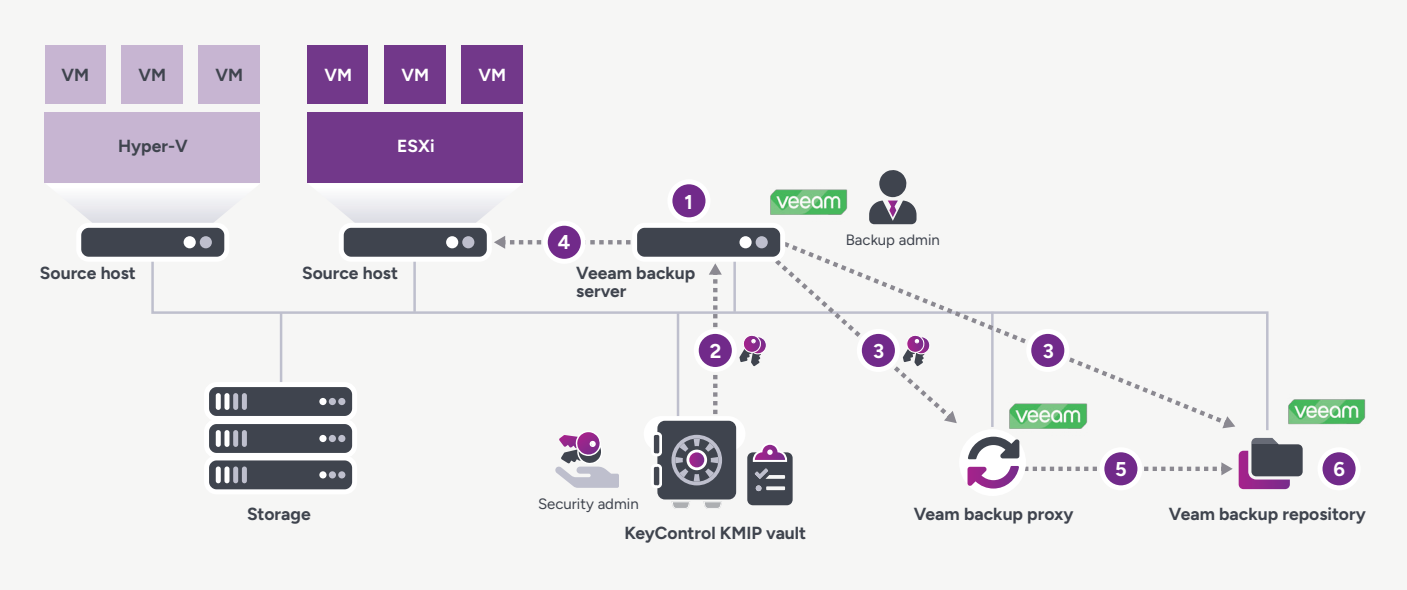
The Entrust KeyControl KMS Solution

The Entrust KeyControl KMS integrates with Veeam Backup & Replication, providing a key management server in the Veeam Backup & Replication environment via the KMIP open standard.

For organizations requiring higher levels of assurance, KeyControl can be seamlessly integrated with a FIPS 140-3 Level 3 Entrust nShield® hardware security module (HSM). The optional HSM is used to protect the master key for the KeyControl virtual appliance. It is also used in the process when generating cryptographic keys, ensuring high-quality entropy from the HSM's random number generator is used in keys created and managed by KeyControl vaults irrespective of which vault type is deployed. See details on the final page where the role of the key encryption key (KEK), protected by the HSM, is described in more detail.



How Does the Encryption of VM Backup Work?



1. At the start of a backup job, the backup manager running on the Veeam Backup server retrieves job settings and creates tasks for all VM disks to backup. The job settings indicates whether backup needs to be encrypted.
2. The Backup Manager communicates with the external KMS (Entrust KeyControl) to request the appropriate cryptographic keys. Following best practice and separation of duties principles, these keys are never stored directly in the Backup Manager's configuration.
3. The Veeam Backup Manager establishes a connection with the target backup repository and the backup proxy. The backup proxy and backup repository establish a connection with each other for data transfer.
4. The Veeam Backup Manager requests a snapshot from the vCenter Server or the ESXi host. VM disks are set to read-only, and all changes the user makes to the VM during backup are written to Delta files.
5. The backup proxy reads VM data from the read-only disk and sends it to the backup repository. While transporting VM data, the backup proxy performs additional processing. It filters out zero data blocks, compresses VM data, uses the retrieved keys to encrypt the data, and transports it to the target Veeam Data Mover.
6. The encrypted VM data is stored in the backup repository.

The Entrust KeyControl Difference

Entrust KeyControl redefines cryptographic key management by combining traditional key lifecycle management and a decentralized vault-based architecture with a comprehensive central policy and compliance management dashboard. The platform offers decentralized security with centralized visibility across your enterprise's cryptographic ecosystem.

The concept of decentralized security refers to a system where an organization's cryptographic assets are not confined to a single, central repository. Instead, these assets are distributed and located wherever the organization deems appropriate.

This approach not only meets network segmentation and data sovereignty requirements, but also ensures that keys are stored within easily manageable and maintainable distributed vaults.

The Compliance Manager feature provides a single, unified dashboard that allows you to view and monitor your organization's cryptographic assets related to your backup and recovery solution deployments. These can be located in one or many vaults to suit architectural needs and can scale to millions of keys.

BENEFITS

Integrating KeyControl KMS with Veeam Backup & Replication

Enhanced Data Security
Integrating the KeyControl KMS adds an extra layer of protection to Veeam's backup solutions, ensuring encryption keys are managed securely and minimizing the risk of data breaches.

Regulatory Compliance
KeyControl helps organizations meet stringent data security and privacy regulations (e.g., GDPR, HIPAA), confidently maintaining compliance with industry standards.

Simplified Key Management
Integration streamlines key handling within the Veeam environment, reducing complexity and operational overhead for IT teams.

Scalability and Flexibility
As businesses grow and adopt diverse infrastructure models – including multi-cloud and hybrid environments – the KMS integration scales effortlessly to meet evolving data demands.

Improved Recovery Times
Secure, efficient key retrieval ensures rapid access to encrypted data during disaster recovery, significantly reducing restoration times.

KeyControl Integration Features

Key Encryption Key (KEK)
Adds an extra layer of security by encrypting all individual KMIP objects within each KMIP vault.

HSM-Generated KEK
Each KMP vault is assigned a KEK generated in the HSM, which wraps all KMIP objects in the vault.

ReKeying With Zero Downtime
Allows cryptographic keys to be replaced seamlessly without disrupting operations.

Multiple Vault Support
Enables security administrators to isolate different KMIP environments for enhanced security and compliance.

Independent KMIP Vault Configuration
Each KMIP vault maintains its own objects, client certificates, access policies, audit logs, local user accounts, Active Directory settings, and HSM root key label for KEK wrapping.

ABOUT ENTRUST

Entrust is an innovative leader in identity-centric security solutions, providing an integrated platform of scalable, AI-enabled security offerings.

We enable organizations to safeguard their operations, evolve without compromise, and protect their interactions in an interconnected world – so they can transform their businesses with confidence. Entrust supports customers in 150+ countries and works with a global partner network. We are trusted by the world's most trusted organizations.

entrust.com Toll-Free: 888.690.2424 | International: +1.952.933.1223 | sales@entrust.com

ENTRUST

SECURING A WORLD IN MOTION