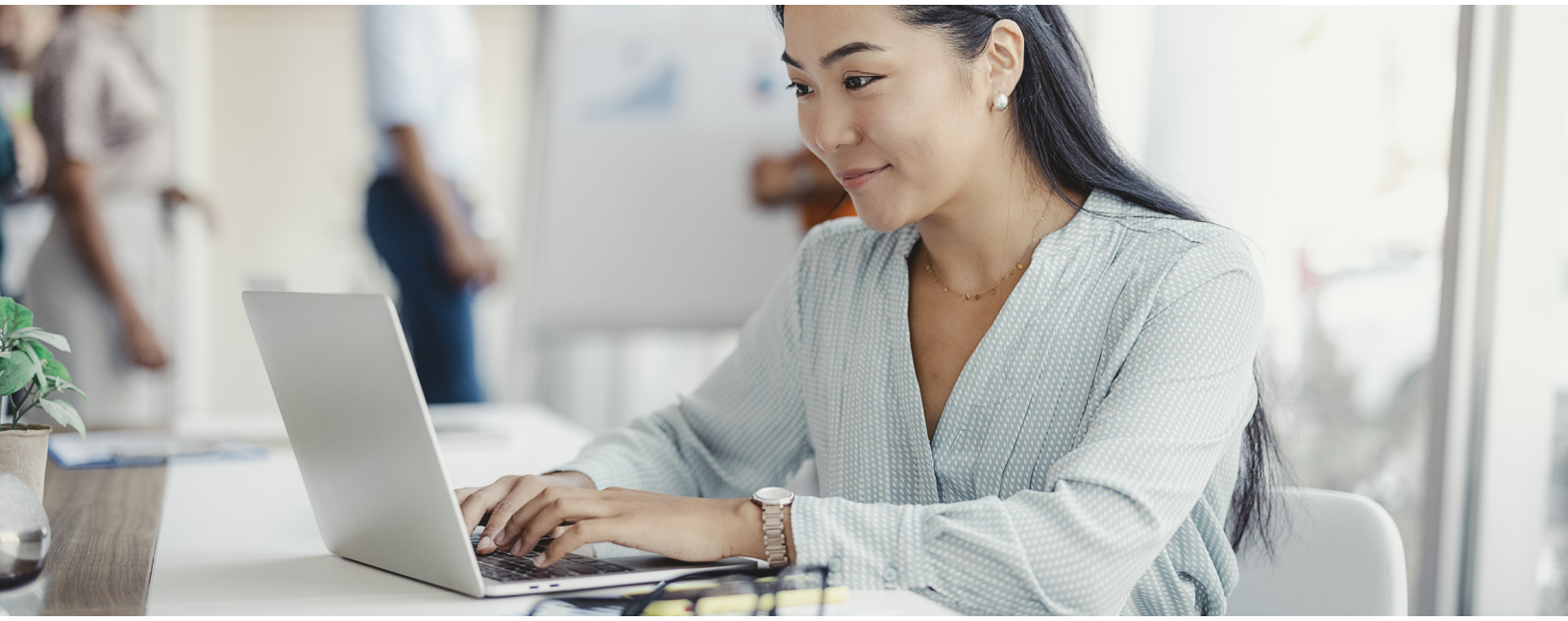
SOLUTION BROCHURE

Backup and Recovery With Commvault & Entrust Cryptographic Security Platform

Commvault®

ENTRUST
SECURING A WORLD IN MOTION

Contents



The Need for Comprehensive Data Management

Data is now 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. Because of this threat, there's now a critical need for robust backup and recovery solutions in the data protection domain. These solutions ensure that data is not only preserved but recoverable in the event of data loss – which can occur during hardware failures, cyber threats, 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.

Comprehensive data management platforms provide reliable data protection, seamless recovery, and simplified administration. Commvault, a leading data management provider, offers a suite of solutions designed to manage and protect data across various environments, including:

Data Protection: Offering backup and recovery solutions for on-premises, hybrid, and multi-cloud environments to ensure data availability and integrity

Information Management: Facilitating data governance, compliance, and eDiscovery to help organizations manage their information lifecycle effectively

Cyber Resilience: Providing cybersecurity solutions against ransomware and other threats to assist companies in reducing risk, controlling costs, and maintaining business continuity

With Commvault, businesses gain peace of mind knowing their data is secure, always available, and easily recoverable.

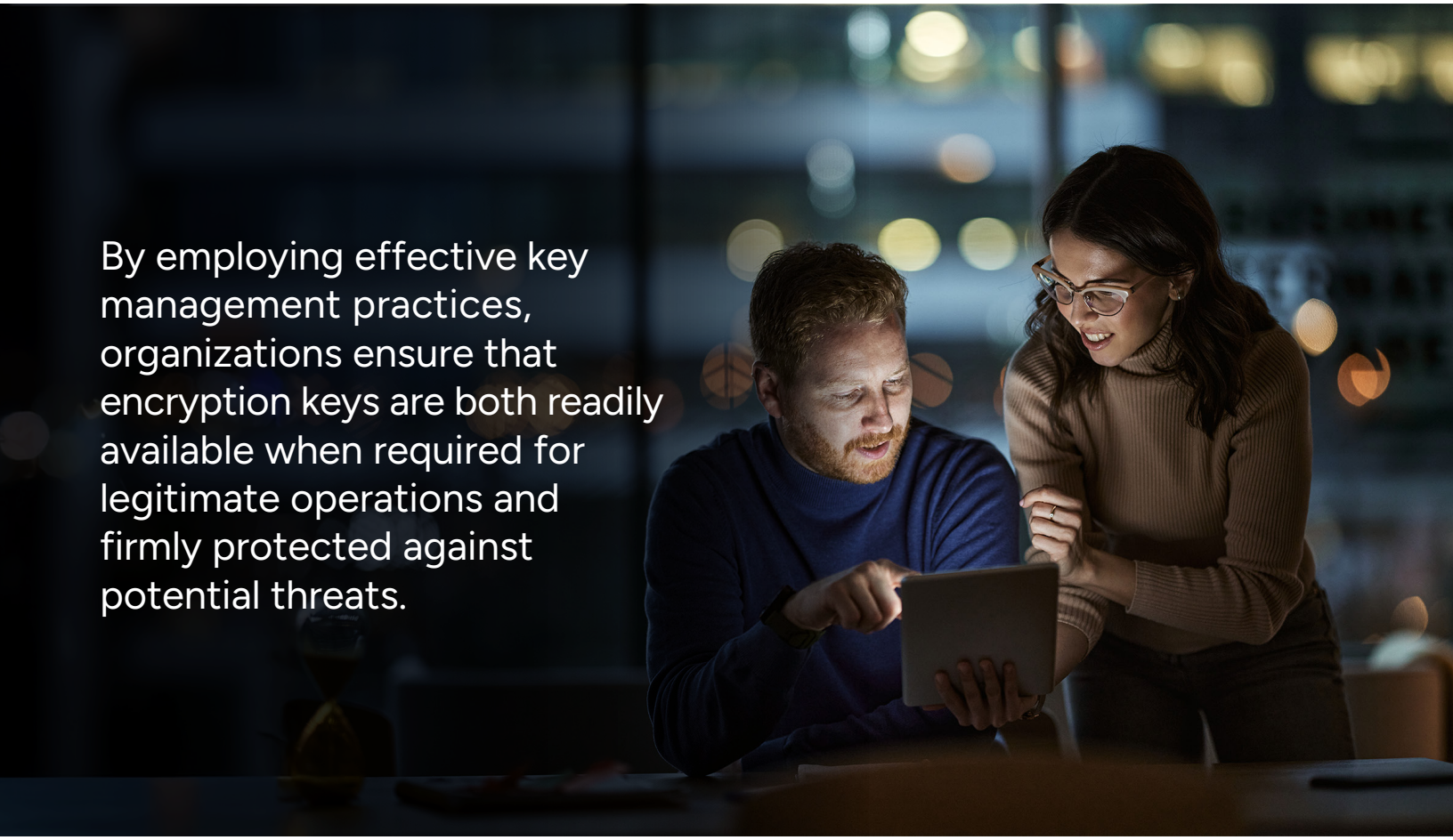
The Importance of Protecting Backups

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 to ensure that if 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 management of cryptographic keys. Keys used to secure and decrypt data, particularly backup data, must be handled with the care.

This is where a strong key management system (KMS) comes 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.



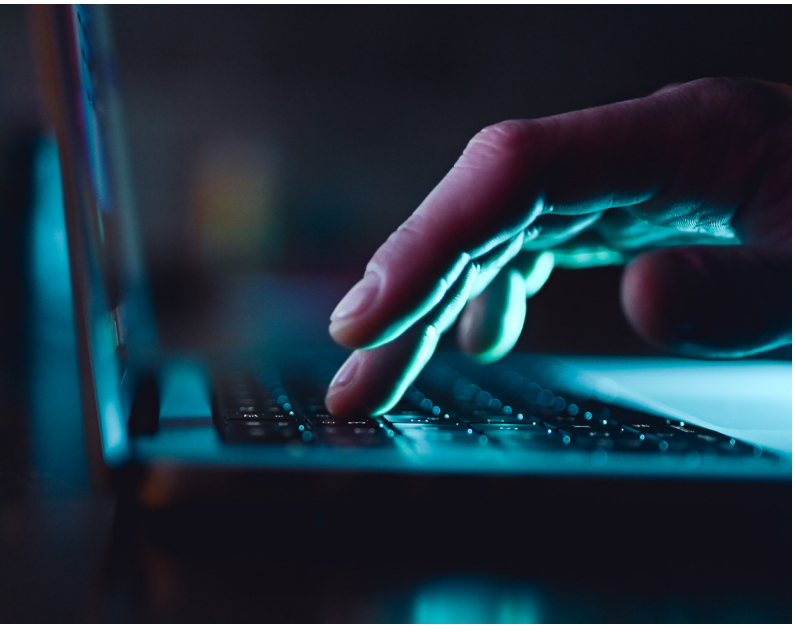
How KMSs Enhance the Security of Backups

Separation between backup operations and key management

By clearly delineating the responsibilities of backup teams and those in charge of managing cryptographic keys, a KMS ensures that no single party controls both data and the keys that protect it. This separation mitigates the actions of insider threats and adds an extra layer of security to your backup environment.

Strict access controls to keys

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, 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 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 Cyptographic Security Platform KMS Solution

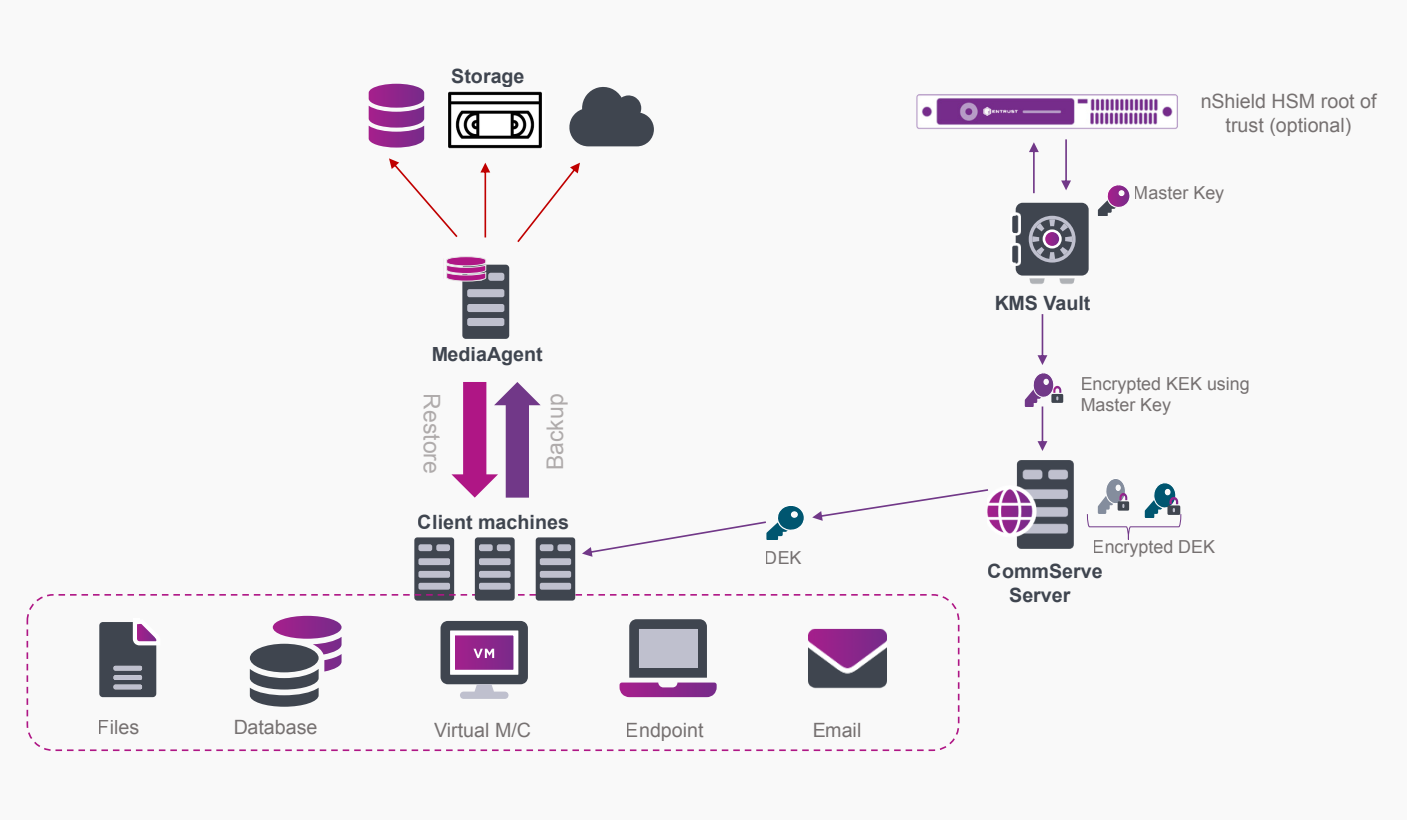
The Entrust Cryptographic Security Platform Key Management Solution integrates with Commvault, providing a key management server in the Commvault environment via the KMIP open standard.

For organizations requiring higher levels of assurance, Entrust's Key Management Solution (KMS) 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 key management vault(s). It's also used when generating cryptographic keys, ensuring high-quality entropy from the HSM's random number generator is used in keys created and managed by the platform key management vaults irrespective of which vault type is deployed.

How Does Entrust KMS Strengthen the Protection of Backup Data?

Commvault protects data by installing agent software on physical or virtual hosts called client machines. These agents use native operating system or application APIs to ensure data remains in a consistent state. Production data is processed on client machines, then transferred through a MediaAgent to disk, tape, or cloud storage. All backup operations are orchestrated by the CommServe server, which also provides an administrative interface for configuration and monitoring. Backup data can be encrypted by the agents on client machines, ensuring confidentiality in transit and at rest.

The Entrust platform's independent vault provides an additional layer of security around encryption keys, ensuring that backup data remains protected against unauthorized access throughout its lifecycle.



Key Components of a Key Management Solution

CommServe Server

A CommServe server is a central management system that coordinates all backup tasks and maintains configuration, security, and operational history.
For each client machine, the CommServe server creates a data encryption key (DEK) and encrypts it with a key encryption key (KEK), then stores the encrypted DEK in its database.

MediaAgent

A MediaAgent is a data transmission manager responsible for moving data and controlling storage libraries. Multiple MediaAgents can be deployed for scalability.

Client Machines

Client machines are servers (physical or virtual) with Commvault software components installed. They may also include specialized solutions for file systems or applications like databases.

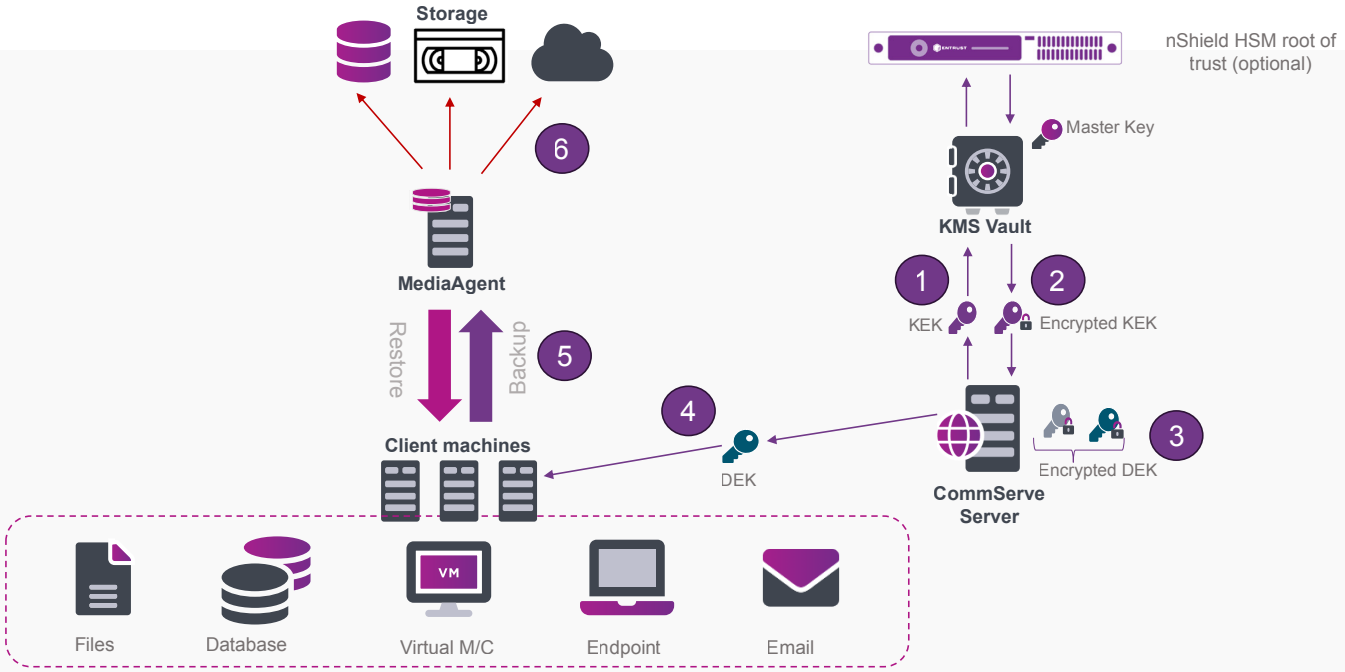
Key Management Vault

Generates the master key and encrypts the KEK. Entrust's KMS augments the security Commvault data protection by providing an independent vault that generates and manages master keys. The master key is used to encrypt the KEK. In turn, the KEK encrypts the DEKs used to secure backup data. This layered encryption prevents unauthorized access to keys – even if storage or other infrastructure components are compromised – dramatically enhancing overall backup security.

Backup Workflow

Backup Workflow

1. **Generate KEK**
   The CommServe server generates a KEK and requests that the Key Management vault encrypt it with the master key.
2. **Store KEK**
   The Key Management vault returns the encrypted KEK and master key ID to the CommServe server, which stores them in its database.
3. **Encrypt DEK**
   For each client, the CommServe server creates a DEK and encrypts it with the KEK, then stores the encrypted DEK in its database.
4. **Distribute DEK**
   The CommServe server sends the DEK to the client.
5. **Encrypt Backup Data**
   The client uses the DEK to encrypt its backup data and sends the encrypted data to the MediaAgent.
6. **Write to Storage**
   The MediaAgent writes the encrypted data to the designated storage target (disk, tape, or cloud).



Restore Workflow

Restore Workflow

1. **Retrieve Encrypted Keys**
   The CommServe server fetches the encrypted KEK and DEK from its database.
2. **Request Master Key**
   The CommServe server requests the master key from the Key Management Vault.
3. **Decrypt KEK**
   The CommServe decrypts the KEK using the master key.
4. **Decrypt DEK**
   The CommServe decrypts the DEK with the KEK.
5. **Provide DEK**
   The CommServe sends the DEK to the client.
6. **Fetch Encrypted Data**
   The MediaAgent fetches and sends the encrypted backup data to the client.
7. **Decrypt Data**
   The client decrypts the data using the DEK.

The Entrust Difference

The Entrust Cryptographic Security Platform, deployed on premises or as a service, 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.

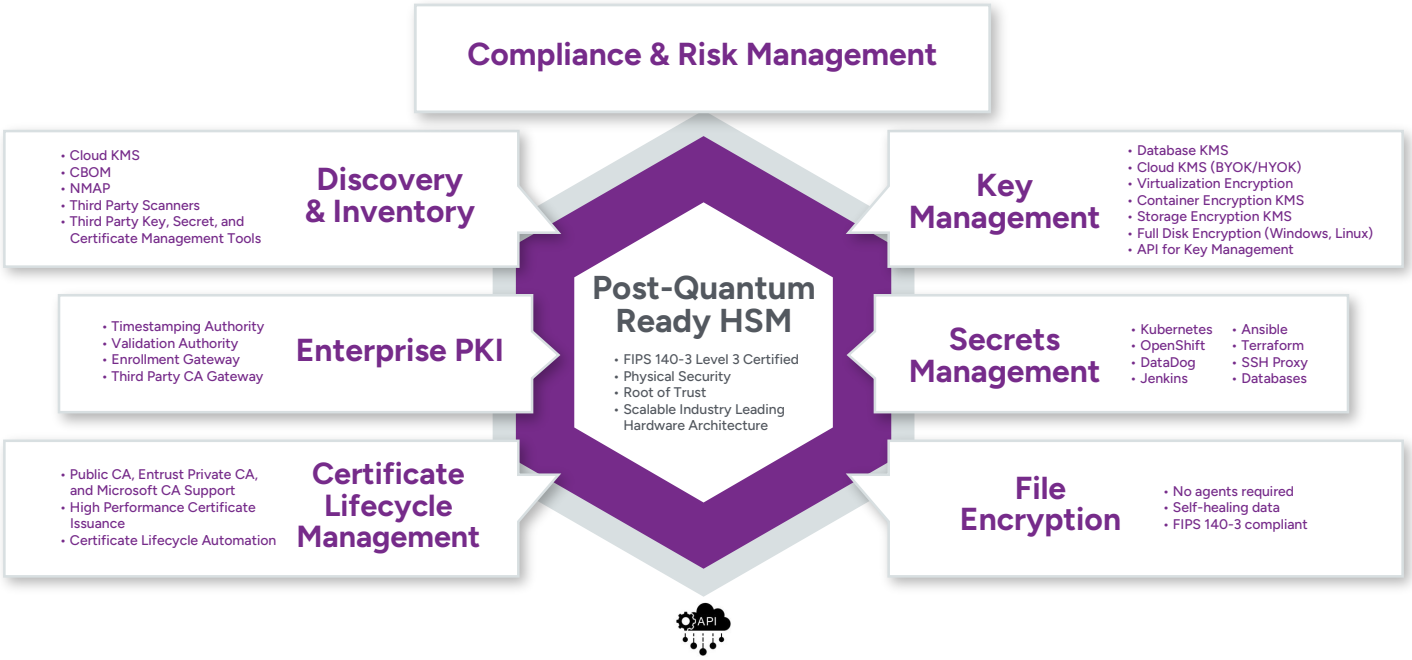
The concept of decentralized security refers to a system where an organization's cryptographic assets are not confined to a single, central repository. Instead, these assets are distributed and located wherever the organization deems appropriate.

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.

Entrust Cryptographic Security Platform

Entrust's Cryptographic Security Platform is an innovative solution that unifies cryptographic management by combining the rich capabilities to operate PKI, Certificate Lifecycle Management, Key and Secrets Management, and HSMs all from a single, cohesive system.

This platform addresses the growing need for comprehensive cryptographic asset management in an increasingly complex digital landscape. By integrating these critical components, the Cryptographic Security Platform offers unparalleled security, compliance, and operational efficiency for organizations dealing with securing an increasing number of machine identities, protecting sensitive data and navigating complex cryptographic requirements.



Benefits and Features of Entrust Cryptographic Security Platform KMS With Commvault

BENEFITS

- **Enhanced Data Security**
  Integrating the platform KMS adds an extra layer of protection to Commvault's backup solutions, ensuring encryption keys are managed securely and minimizing the risk of data breaches.
- **Regulatory Compliance**
  By leveraging the platform KMS, organizations can more easily meet stringent data security and privacy regulations (e.g., GDPR, HIPAA), confidently maintaining compliance with industry standards.
- **Simplified Key Management**
  The integration streamlines key handling within the Commvault 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 ensures key management scales effortlessly to meet evolving data demands.
- **Improved Recovery Times**
  Efficient, secure key retrieval ensures rapid access to encrypted data during disaster recovery, significantly shortening restoration times.

FEATURES

The platform KMS integration offers support for Commvault backup and replication. Some key features of this integration include:

- Data at rest encryption
- Rekeying with zero downtime
- Use with multiple vaults, allowing security administrators to isolate different KMIP environments for security and compliance
- Each KMIP vault has its own KMIP objects, client certificates, access policies, audit logs, local user accounts, Active Directory settings, and HSM settings
- The HSM provides an extra layer of security by encrypting the Commvault master key
- A KEK is created in HSM for each KMIP vault and wraps all keys within the vault

ABOUT ENTRUST

Entrust fights fraud and cyber threats with comprehensive identity-centric security that protects people, devices, and data. Our solutions help enterprises and governments safeguard critical systems from every angle, enabling secure onboarding and issuance, providing everyday identity protection, and empowering them with 360-degree visibility and orchestration across keys, secrets, and certificates so they can transact and grow with confidence. Building on our decades as a pioneer and innovator in establishing trust, Entrust has a global partner network and supports customers in over 150 countries.

For more information, visit www.entrust.com.

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

ENTRUST
SECURING A WORLD IN MOTION