Entrust DataControl

Data encryption, multi-cloud key management, and workload security

HIGHLIGHTS

- Complete workload lifecycle encryption management – from boot to decommissioning
- Key Management Server (KMS)
- Strong and granular VM encryption: live boot (OS) and data partition encryption
- Access controls for separation of duties among admins
- Easy to deploy and manage
- Seamless integration with Entrust nShield® HSMs for FIPS 140-2 Level 3 certified root of trust

Managing encrypted workloads can get complex, especially in a multi-cloud environment

Many workloads contain critical data, which has to be protected. Your company's reputation is at stake, and after a data breach, lawsuits and loss of revenue are a serious concern.

Workloads go through many lifecycles, from staging to deployment, to backup and eventual decommissioning. Each stage poses different risks of potential data theft or other misuse.

Workload encryption is not a deploy once and forget operation

It is critical to frequently re-key the data, increasing the complexity of key management. Managing workload encryption from each cloud's management platform is complex and increases the risk of inconsistent policies and mistakes. Migrating workloads between clouds means they are first decrypted, then migrated in clear-text, and then re-encrypted, introducing new risk factors.

Learn more about DataControl at entrust.com

Entrust DataControl

KEY FEATURES & BENEFITS

Entrust DataControl secures multi-cloud workloads throughout their lifecycle and reduces the complexity of protecting workloads across multiple cloud platforms. This provides greater protection of your organization's critical and sensitive information while enabling compliance with data privacy regulations.

Managing encrypted workloads in a multi-cloud infrastructure

DataControl allows you to manage your encrypted workloads across different infrastructures. It works on-premises and with the leading public cloud platforms, as well as with hyperconvergence and storage solutions. With DataControl, you get a centralized and scalable solution to control all your encryption keys. DataControl includes the VMware-certified Entrust KeyControl Key Management Server (KMS).

Deep workload protection

Apply strong security and protection for workloads throughout their lifecycle, from boot to backup, and final decommissioning stage.

DataControl provides granular encryption for better security. The protection boundary does not stop at the hypervisor or at the data store; VMs are individually encrypted. Inside the VM, unique keys can be assigned to encrypt each partition, including the boot (OS) disk and swap partitions.

Easy to deploy and manage

DataControl provides deployment flexibility with a single interface for all workload encryption, which eliminates the complexity of using each platform's own encryption feature separately. DataControl offers administrators a superior user experience, and zero downtime encryption allows for frequent and more secure re-keying while the workload remains accessible. High availability clustering ensures your disaster recovery is not impaired by losing access to the critical key management system.

Access controls

DataControl allows for robust policy-based access controls to enforce separation of duties across different user personas. Prevent root users or system administrators from accessing sensitive data by enforcing access controls on encrypted volumes. For hybrid cloud deployments, prevent your cloud service providers' administrators, often responsible for patching and other operational upkeep, from ever accessing encrypted data. Entrust DataControl allows for custom controls across a variety of use cases to enable greater security across multi-cloud deployments.

Deduplication support

Previously, the concern existed that encryption and deduplication could not co-exist, given that encrypting data makes every block different. DataControl has now solved this problem so that customers can enjoy the data security afforded by encryption along with the cost savings offered by the deduplication capabilities of different storage platforms, including VMware vSAN storage. With this unique approach, DataControl offers AES 256-bit encryption while maintaining 91% of the storage benefit of vSAN deduplication.

Platform support

- Private cloud platforms: vSphere, vCloud Air (OVH), VxRail, Pivot3, NetApp, Nutanix
- Public cloud platforms: Amazon Web Services (AWS), IBM Cloud, Microsoft Azure, VMware Cloud (VMC) on AWS, Google Cloud Platform (GCP)
- Hypervisor support: ESXi, AWS, Azure, KVM, GCP

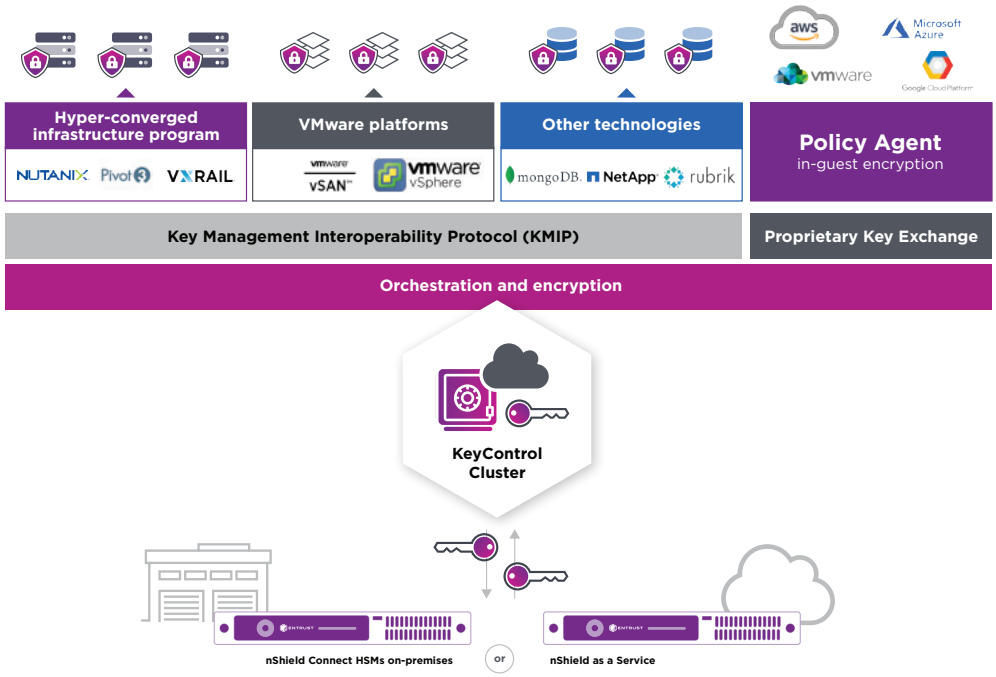
Entrust DataControl

Deployment platform support

CentOS; Red Hat Enterprise Linux; Ubuntu; SUSE Linux Enterprise Server; AWS Linux; Windows Server Core 2012 R2, 2016, and 2019; Windows Server 2012, 2012 R2, 2016, and 2019; Windows 8.1 and 10.

Deployment media

ISO, OVA (Open Virtual Appliance), AMI (Amazon Web Services marketplace), or VHD (Microsoft Azure marketplace)



Technical specifications

- Encrypt boot (OS), swap and data partitions
- Support for encrypting Windows GPT boot drives, including UEFI Secure Boot drives
- Individual keys per partition
- Strong AES (128/256 bit) encryption with Intel hardware acceleration support
- FIPS 140-2 compliant Level 1 encryption key management. Seamless integration with Entrust nShield FIPS 140-2 Level 3 hardware security modules
- Zero downtime encryption with automatic re-keying
- Dynamic partition resizing for Windows VMs
- Supports KMIP v1.1 - 1.4 (Key Management Interoperability Protocol) clients
- High availability (HA) support with active-active cluster (up to 8 KMS servers per cluster)
- Single encryption key for deduplication support
- Certified for VMware vSphere and vSAN encryption
- REST-based API integration for DevOps
- Protect encrypted workloads against unauthorized access with boot and clone protection

Learn more at
entrust.com

ENTRUST

Ergonomics AG
Uetlibergstrasse 132
8045 Zürich
www.ergonomics.ch - 058 311 1000