Entrust DataControl

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

HIGHLIGHTS

- Complete workload lifecycle encryption management
- Enterprise Key Management Server (KMS)
- Strong and granular virtual machine (VM) encryption: live boot (OS) and data partition encryption
- Access controls for separation of duties among administrators
- 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

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.

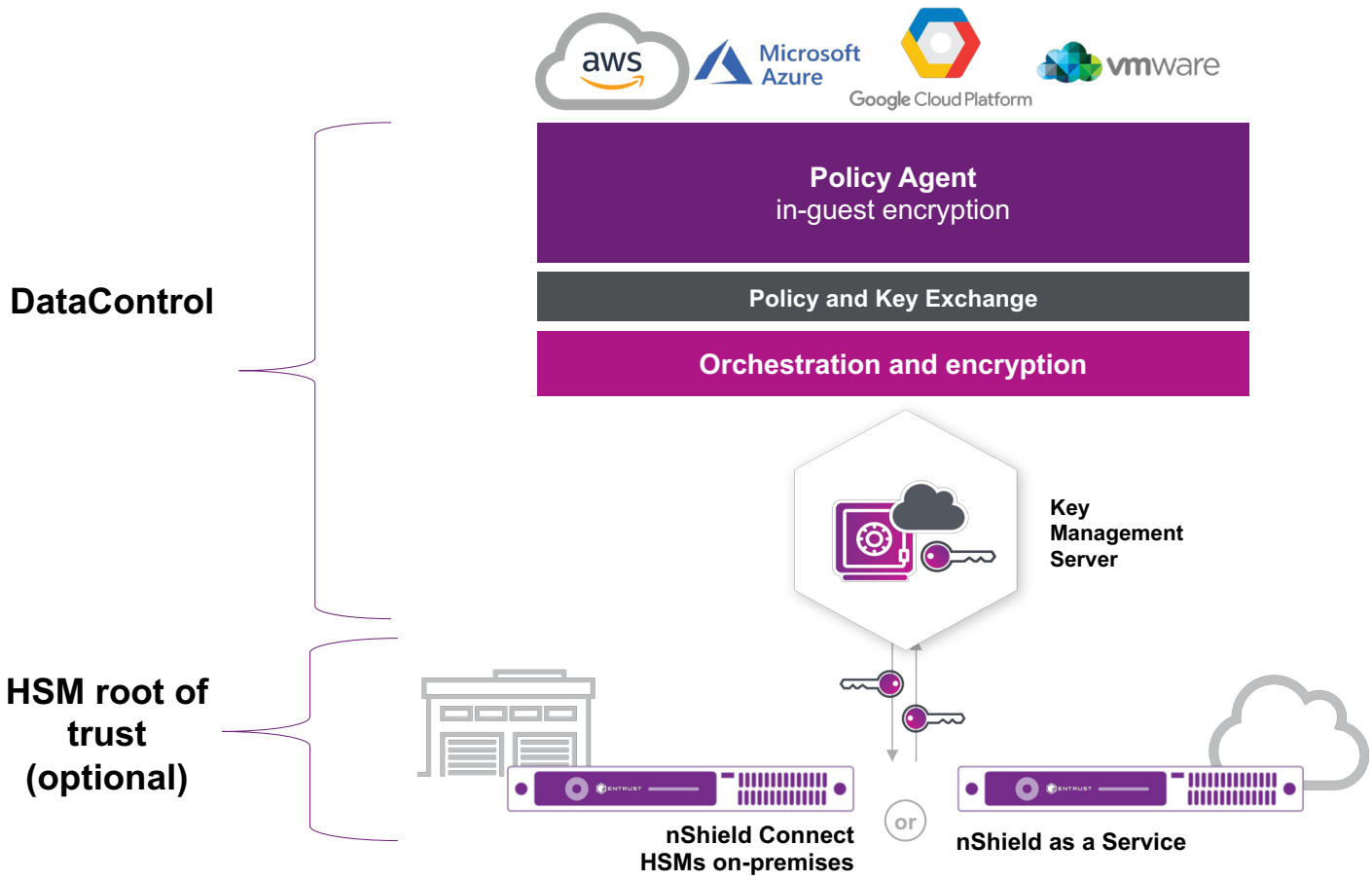
Workload encryption is not a deploy once and forget operation

It is critical to frequently rotate data encryption keys. Managing workload encryption from each cloud vendor's platform is complex and increases the risk of inconsistent policies and human mistakes. Built-in key management policy reduces complexity and ensures consistency.

Entrust DataControl (formerly HyTrust) 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.

Learn more about DataControl at entrust.com

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)
- Amazon Machine Image (AMI) available via Amazon marketplace
- Virtual Hard Disk (VHD) available via Microsoft Azure marketplace

Learn more about DataControl at entrust.com

Entrust DataControl

KEY FEATURES & BENEFITS

Managing encrypted workloads in a multi-cloud infrastructure

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

Deep workload protection

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.

- Superior user experience
- Zero downtime encryption
- High-availability clustering ensures disaster recovery capabilities

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.

Deduplication support

Previously, the concern existed that encryption and deduplication could not co-exist, given that encrypting data makes every block different. DataControl's unique approach offers AES 256-bit encryption while maintaining 91% of storage deduplication benefit.

Platform support

- **Private cloud platforms:**
  - vSphere
  - OVHCloud
  - 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

Learn more about DataControl at entrust.com

Entrust DataControl

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
- 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

DataControl is part of a suite of data encryption, multi-cloud key management, and virtual machine and containerized workload security policy compliance products. See table below for details.

ENTRUST PRODUCT	DESCRIPTION	ADDITIONAL INFORMATION
KeyControl BYOK	For generating and bringing your own cryptographic keys to AWS, Microsoft Azure, or Google Cloud Platform	Licensed standalone or can be deployed with KeyControl and/or DataControl
KeyControl	Enterprise encryption key management for KMIP enabled workloads	Licensed standalone or can be deployed with KeyControl BYOK and/or DataControl
DataControl	For fine-grained, agents based control and encryption key management of virtual machine encryption in multi-cloud environments	Licensed standalone or can be deployed with KeyControl and/or KeyControl BYOK
CloudControl	For automated workload security policy enforcement and compliance in virtualized and containerized environments protecting sensitive data against misconfigurations in the cloud.	

Learn more at
entrust.com

ENTRUST

Global Headquarters
1187 Park Place, Minneapolis, MN 55379
U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223