Entrust CloudControl

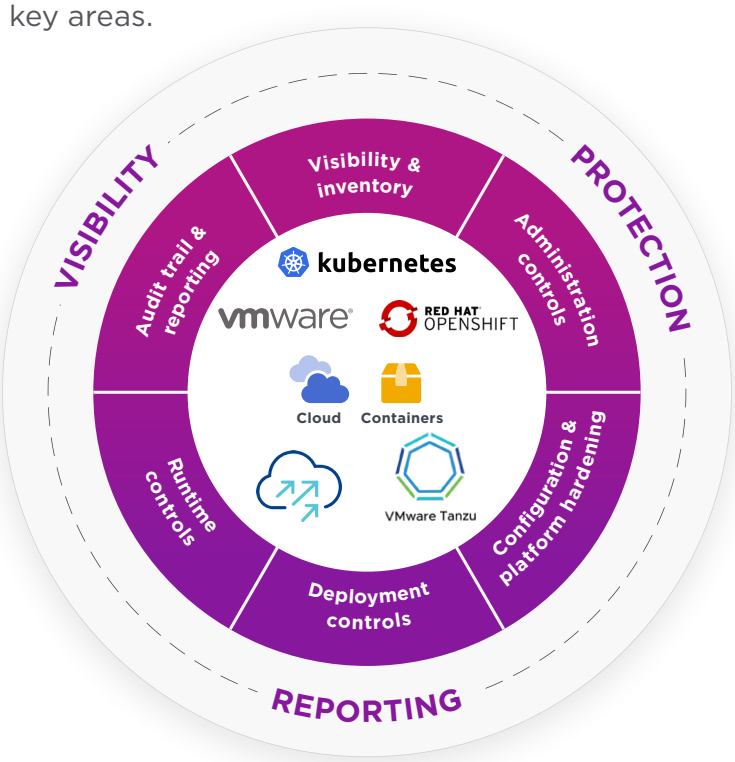
Comprehensive security for hybrid multi-cloud environments including centralized authentication, authorization, and audit control

HIGHLIGHTS

- Comprehensive security controls help meet compliance requirements across virtualization, public cloud, and containers
- Provides automation with real-time compliance and security features
- Unified policy, visibility, and administrative guardrails, establishing a baseline that can constantly monitor deployments
- Built-in compliance templates for hardening virtual machine and containerized environments
- Secure separation of workloads
- "Security as code" automation for DevSecOps
- Seamless integration with and support for VMware Cloud Foundation (VCF) environments

Comprehensive capabilities

Entrust CloudControl drives security, compliance, and availability across six key areas.



Protect applications and data

Prevent disruption due to administrator errors

Helps meet compliance requirements with low operational overhead

Produce audit-quality logs to support incident response

Leverage hardening templates for virtual machine and containerized environments

Learn more about CloudControl at entrust.com

Entrust CloudControl

Reducing IT risks through a unified security framework

As IT environments transition to hybrid cloud, security architectures must undergo a corresponding transformation. Entrust CloudControl (formerly HyTrust CloudControl) addresses the need for a comprehensive solution by providing a unified framework for security and compliance across the hybrid cloud – reducing both risk and operational overhead.

Comprehensive risk management

CloudControl offers a wide range of capabilities that can be customized to meet any organization's desired risk posture and control activity requirements. Supporting VMware Cloud Foundation, the centralized solution enables organizations to achieve authentication, authorization, and audit control for UI and API access to critical infrastructure resources in the ecosystem – including ESXi hosts, vCenters, NSX-T Managers, vSAN, and SDDC and associated workload and management domains.

Visibility and inventory	Administration controls	Configuration and platform hardening	Deployment controls	Runtime controls	Audit trail and reporting
• vSphere, VCF and NSX-T, Red Hat OpenShift, and VMware Tanzu containerized environments • Discovery • Inventory and security context	• RBAC (role-based access control) • ABAC (attribute-based access controis) • Secondary approval • Multi-factor authentication and IAM integration	• Configuration best practices • Compliance templates including NIST 800-53, CMMC, PCI-DSS, HIPAA, DISA STIG	• Workload placement and segregation • Security best practices • Image assurance • CI/CD integration	• Continuous policy enforcement • Real-time alerts • Automatic remediation	• Forensic-quality change log • Cross-platform logging and search • Recommendation and executive summary reports • SIEM integration

Learn more about CloudControl at entrust.com

Entrust CloudControl

KEY FEATURES & BENEFITS

- **Decreased risk of security or availability failures.** Gain full-stack multi-dimensional policies and industry-leading administration controls to protect against insider threats and human errors that cause downtime.
- **Improved agility for virtualized data centers, public and private clouds.** Acquire "create once, apply anywhere" policies that support consistent controls and eliminate manual efforts.
- **Lower operational overhead.** Eliminate multiple consoles and inconsistent security constructs, and gain security policies that support "security as code" automation.
- **Automated approach to help support efficient full-stack compliance.** Provides built-in templates for:
  - Cybersecurity Maturity Model Certification (CMMC)
  - Payment Card Industry Data Security Standard (PCI DSS)
  - National Institute of Standards and Technology (NIST) 800-53
  - Health Insurance Portability and Accountability Act (HIPAA)
  - Federal Risk and Authorization Management Program (FedRAMP)
  - Defense Information Systems Agency Security Technical Implementation Guides (DISA STIGs)
  - And more

The solution also provides workload placement controls, logical segmentation, and robust audit trail and reporting that supports control validation.

- **Improved visibility and operational awareness.** You gain insight with forensic-quality logs for incident response root cause analysis and intent context.
- **Authentication, authorization, and audit control for VCF.** Achieve authentication, authorization, and audit control (AAA) security for VMware Cloud Foundation (VCF). CloudControl provides role-based access controls (RBAC) for VCF that provides visibility into who is accessing resources in the VCF SDDC Manager and down to the ecosystem infrastructure components including ESXi hosts, vCenters, NSX-T Managers, and vSAN.

Entrust CloudControl

Automate operations

Automate operational best practices to lower risk and drive availability:

- Highly granular attribute- and role-based administrator authentication and authorization
- Environmental hardening
  - Virtual environments
  - Containerized environments including Red Hat OpenShift and VMware Tanzu
- Privileged Access Management for vSphere

Accelerate digital transformation

Unlock agility in multiple dimensions.

- Security policies can be written independently of underlying infrastructure and translated into actual controls based on workload location
- Logical segmentation automatically enforces workload placement policies based on multiple attributes
- Policies can be integrated into DevOps-style CI/CD environments using "security as code"

Proven, scalable risk management

As architectures have evolved from virtual to software-defined data center (SDDC) private cloud/hybrid multi-cloud, CloudControl continues to be the leading option for lowering risk of data loss or downtime due to compromise or abuse of the control/management plane. Entrust also continuously innovates broader capabilities across multiple dimensions while maintaining unified policy and visibility.

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	LICENSING/DEPLOYMENT
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