Entrust CloudControl

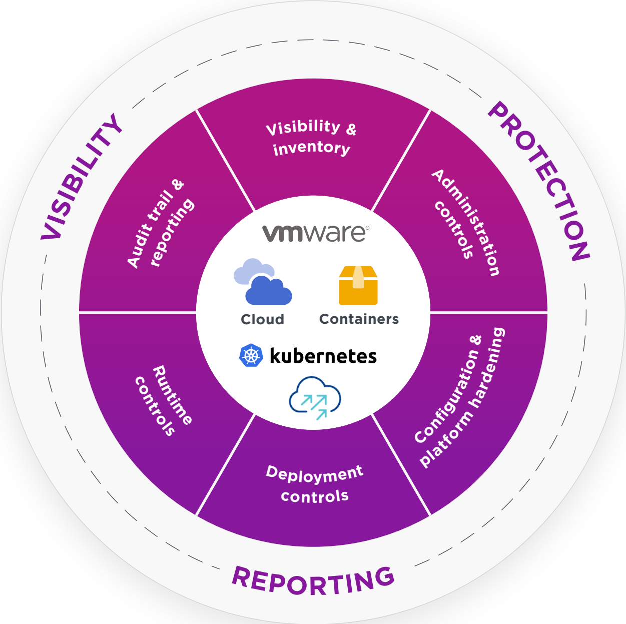
Comprehensive security for hybrid multi-cloud environments including centralized authentication, authorization, and audit control

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) 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 capabilities

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



HIGHLIGHTS

- Comprehensive security and compliance across virtualization, public cloud, and containers
- More than 20 capabilities in a single solution
- Unified policy, visibility, and administrative guardrails
- Built-in compliance templates and robust reporting
- Secure separation of workloads
- “Security as code” automation for DevSecOps
- Support for VMware Cloud Foundation
- Seamless integration with VMware Cloud Foundation (VCF) environments

Protect applications and data

Prevent disruption due to administrator errors

Meet compliance requirements with low operational overhead

Produce audit-quality logs to support incident response

Learn more about CloudControl at entrust.com

Entrust CloudControl

Comprehensive risk management

CloudControl offers more than 20 capabilities which 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 & NSX-T, public cloud, containers, and Kubernetes • Discovery • Inventory and security context	• RBAC • ABAC • Secondary approval • Root password vaulting • Two-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 • Boundary control • CI/CD integration	• Policy re-scan • Real-time alerts • Automatic remediation	• Forensic quality change log • Cross-platform logging and search • Recommendation and executive summary reports • SIEM and ITSM integration

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, spear phishing against IT staff, and human errors that cause downtime.
- **Improved agility for virtualized datacenters, public and private clouds.** Acquire "write once, apply anywhere" policies that support consistent controls and eliminate manual efforts.
- **Lower operational overhead.** Eliminate multiple consoles and inconsistent security constructs, and gain Trust Manifests that provide "security as code" automation.
- **Efficient full-stack compliance.** Provides built in templates for: Payment Card Industry Standard (PCI), 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.

Feature spotlight: Automate operations

Automate operational best practices to lower risk and drive availability:

- Highly granular attribute and role-based administrator authentication and authorization
- Environmental hardening
- Privileged Access Management for vSphere

Learn more about CloudControl at entrust.com

Entrust CloudControl

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 – and now 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 administration interface. Entrust also continuously innovates broader capabilities across multiple dimensions, while maintaining unified policy and visibility.

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