Entrust CloudControl

Comprehensive security for hybrid multi-cloud environments

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

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
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.

<table>
<thead>
<tr>
<th>Visibility and inventory</th>
<th>Administration controls</th>
<th>Configuration and platform hardening</th>
<th>Deployment controls</th>
<th>Runtime controls</th>
<th>Audit trail and reporting</th>
</tr>
</thead>
<tbody>
<tr>
<td>vSphere &amp; NSX, public cloud, containers, and Kubernetes</td>
<td>RBAC</td>
<td>Configuration best practices</td>
<td>Workload placement and segregation</td>
<td>Policy re-scan</td>
<td>Forensic quality change log</td>
</tr>
<tr>
<td>Discovery</td>
<td>ABAC</td>
<td>Compliance templates</td>
<td>Security best practices</td>
<td>Real-time alerts</td>
<td>Cross-platform logging and search</td>
</tr>
<tr>
<td>Inventory and security context</td>
<td>Secondary approval</td>
<td>Image assurance</td>
<td>Boundary control</td>
<td>Automatic remediation</td>
<td>Recommendation and executive summary reports</td>
</tr>
<tr>
<td></td>
<td>Root password vaulting</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Two-factor authentication and IAM integration</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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.** Get built-in templates for first mention and needs to be defined: 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.

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
- Root password vaulting

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, 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.