HYTRUST

Solution Brief

CJIS compliance with HyTrust, VMware, and Intel

The Criminal Justice Information Systems (CJIS) Compliance Specification v5.3 prescribes "Access Controls", "Configuration Management", and "Sys- tems Protection and Data Integrity" as critical control objectives. This document summarizes how HyTrust software can simplify CJIS compliance, by automating VM encryption and administrative controls in a virtualized datacenter running VMware vSphere on Intel processors.

At a glance

This solution brief is a companion document to the HyTrust Product Applicability Guide for CJIS Compliance, to be authored by an independent auditor, Coalfire. Coalfire will validate the extent to which HyTrust's solution will simultaneously satisfy numerous CJIS control requirements, when properly deployed.

About HyTrust

HyTrust is the Cloud Security Automation company, founded in 2007 to help organizations, including federal, state, and local governments, and service providers, to understand and solve the challenges of securing virtualized environments.

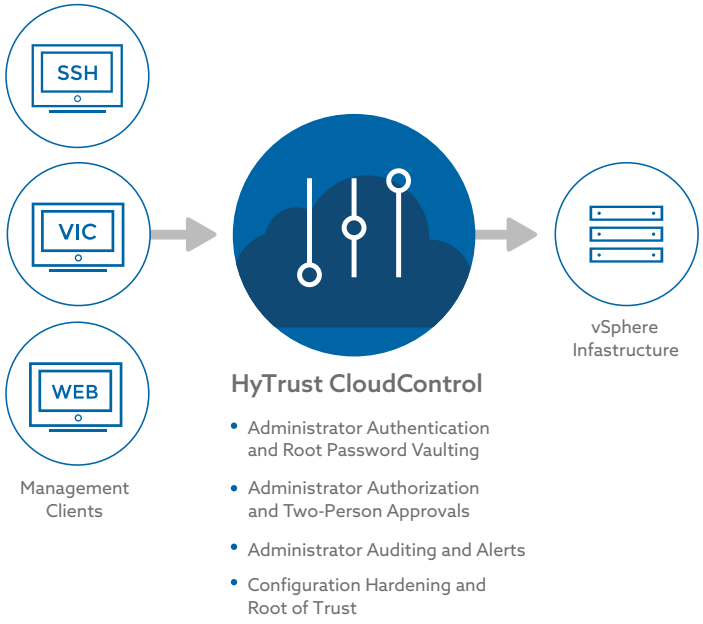
HyTrust is the world's only software company that is both technologically and financially backed by VMware, Intel, Cisco, and In-Q-Tel (the technology investing arm of the US Government Intelligence Community). As a result of these technology partnerships and more than 100 successful customer deployments, HyTrust has become the de facto solution for automating and securing the world's most uptime-sensitive, security-sensitive, and compliance -sensitive virtualized datacenters and cloud infrastructures.

HyTrust CloudControl™

HyTrust CloudControl enables enterprises and service providers to virtualize mission critical applications and deploy multi-tenant private clouds without taking on unacceptable risks. It establishes visibility and accountability, defeats sophisticated attacks, and limits the impact of administrative mistakes by providing:

- Real time monitoring, threat detection, and alerting of suspicious vCenter account activity
- Fine-grained role-based and resource-based authorization, enforcing separation of duties, least privilege, and need-to-know access
- Audit-quality logs that enable complete audit trails tied to individual users' activity

- Strong, multi-factor authentication to protect access to the virtualization platform
- Hypervisor configuration hardening to ensure platform integrity.



HyTrust DataControl™

HyTrust DataControl software provides strong encryption and integrated key management optimized for virtualized and cloud infrastructure. The CJIS specification prescribes both encryption and access controls on encryption keys. HyTrust DataControl can help simplify the CJIS compliance process by enabling auditors to validate that data will be kept secure even in the event of a breach, and that access to encryption keys is well-managed.

HyTrust DataControl excels in several ways:

- DataControl is easy to manage, provides a full API to support automation, and enables initial encryption and re-keying with zero downtime
- DataControl works with all virtualized infrastructure, and is transparent to applications
- DataControl provides integrated key management that is highly-available, fully multi-tenant and makes it possible for end users to keep control of their encryption keys

Intel Trusted Execution Technology (TXT) and Intel Advanced Encryption Standard New Instructions (AES-NI)

A feature of the Intel® Xeon® processor, Intel TXT establishes a root of trust through measurements when the hardware and pre-launch software components are in a known good state. Utilizing the result, in combination with HyTrust CloudControl software, virtual infrastructure administrators can set policies for sensitive data and workload placements to occur only on trusted hypervisors and servers. This helps satisfy the CJIS requirement for Access Control, Systems Protection, and Data Integrity.

A second feature of the Intel® Xeon® processor is the Intel AES-NI circuitry, which is automatically detected and utilized by HyTrust DataControl software, without any configuration or modification require in the hardware or software. AES (Advanced Encryption Standard) is an encryption standard adopted by the U.S. government starting in 2001. Where present, Intel AES-NI is used to accelerate the performance of HyTrust DataControl encryption and decryption, thereby addressing the performance issues of software-only encryption solutions.

How HyTrust CloudControl and HyTrust DataControl help organizations achieve CJIS compliance

Many of the 100+ controls that are prescribed in CJIS specification v5.3 pertain to controls on processes and procedures for hiring and training datacenter operators, system administrators, etc. Of the remaining CJIS controls that deal with virtual infrastructure administrator access management, separation of duties, least privilege enforcement, and logging of virtual infrastructure administrator activity, HyTrust's encryption, workflow automation, and logging software has been explicitly architected to satisfy more than a dozen controls.

It is unusual for a single software solution to satisfy so many compliance controls simultaneously. Much of this is because HyTrust CloudControl is deployed as an in-line transparent proxy between all virtual infrastructure administrators and the virtual infrastructure itself. The depth of controls in the HyTrust solution enables organizations to greatly simplify the task of architecting, testing, and deploying an audit-ready, CJIS compliance-capable virtualized infrastructure. The level of technology integration between HyTrust's solution and solutions from partners such as VMware, Cisco, and Intel also helps simplify the integration work required of organizations.

A matrix of the CJIS controls that HyTrust software can help satisfy is listed in Appendix A.

HyTrust - Cloud Under Control.
1975 W. El Camino Real, Suite 203
Mountain View, CA 94040, USA
Phone: 1-844-681-8100
International: 1-650-681-8100

CJIS v5.3	Subsections supported by HyTrust and Intel		
Policy area	**HyTrust CloudControl (Hypervisor Controls)**	**HyTrust DataControl (VM Encryption and Key Management)**	**Boundry Controls using CloudControl, DataControl, Intel TXT, and Intel AES-NI**
4: Auditing and accountability	5.4.1, 5.4.1.1(4), 5.4.1.1.1		
5: Access control	5.5.2, 5.5.2.1, 5.5.2.2	5.5.2, 5.5.2.2, 5.5.2.3, 5.5.2.4	5.5.2.3
7: Configuration management	5.7.1, 5.7.1.1		
8: Media protection		5.8.1, 5.8.2.1	5.8.1
9: Physical protection		5.9.2	
10: Systems protection and data integrity	5.10.3.2	5.10.1.2(3), 5.10.1.2(4), 5.10.1.5	5.10.1.1(5)