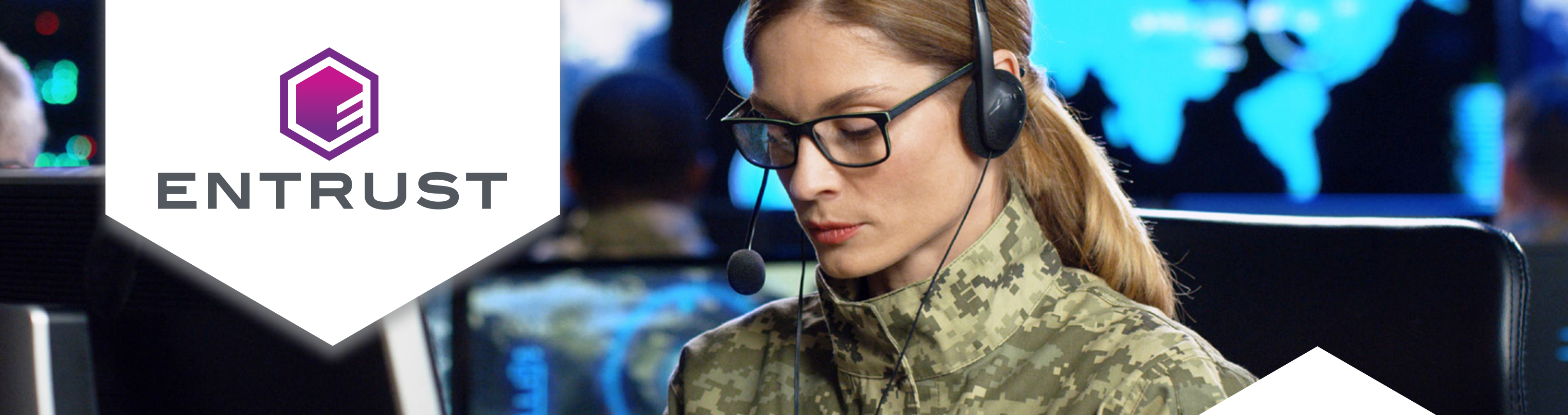
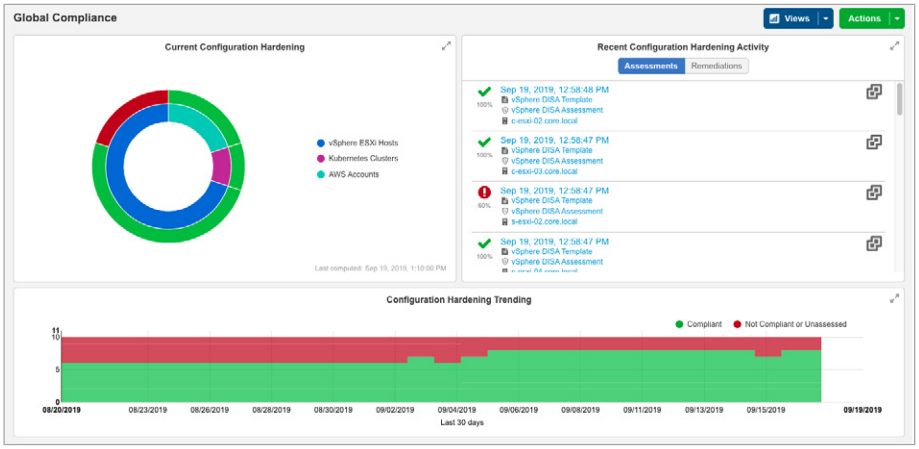


CCRI Solution

Our goal at Entrust is to provide the Department of Defense (DoD) and other Federal Agencies with a Command Cyber Readiness Inspection (CCRI) solution featuring two simple steps: Configuration Hardening and Encryption at Rest.

Step 1. Configuration of VMware to meet DISA STIGs, NIST 800-53, and other compliance standards with Entrust

Both the DISA STIGs and NIST 800-53 standards require significant time and effort from administrators to maintain compliance. When these standards change, administrators must make manual adjustments. When an environment has hundreds of hosts, these manual compliance processes increase risk exposure. Entrust helps to automate and accelerate this process to ensure compliance and reduce risk exposure.



✓ 100% Sep 19, 2019, 12:58:48 PM
vSphere DISA Template
vSphere DISA Assessment
c-esxi-02.core.local

✓ 100% Sep 19, 2019, 12:58:47 PM
vSphere DISA Template
vSphere DISA Assessment
c-esxi-03.core.local

! 60% Sep 19, 2019, 12:58:47 PM
vSphere DISA Template
vSphere DISA Assessment
s-esxi-02.core.local

✓ 100% Sep 19, 2019, 12:58:47 PM
vSphere DISA Template
vSphere DISA Assessment

> “ Our goal at Entrust is to provide the Department of Defense (DoD) and other Federal Agencies with a Command Cyber Readiness Inspection (CCRI) solution featuring two simple steps: Configuration Hardening and Encryption at Rest. ”

Entrust provides compliance configuration templates designed to accelerate and automate compliance for VMware, following DISA STIGs, NIST 800-53, and other regulatory standards. Entrust creates a continuous compliance strategy that offers several core advantages, including:

- Identifying compliance drift when comparing to DISA STIGs or NIST, indicating what is necessary to maintain continuous compliance, and enabling vulnerability remediation with the push of a button.
- Image hardening of VMware environments.
- Rich audit content and robust reporting to support visibility of a compliant infrastructure.

As your organization begins to implement its cloud and container initiatives, Entrust will be able to address those compliance needs as well – and in each case, reduce operator intervention and ensure the agency is in a state of continuous compliance. Organizations who leverage Entrust for continuous compliance also have access to Container Security for Kubernetes and OpenShift.

Learn more at entrust.com

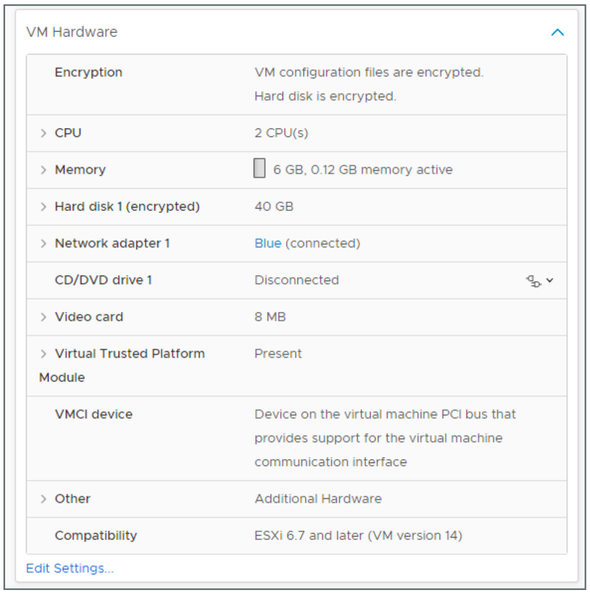
CCRI Solution

Step 2. Encryption at Rest

DISA STIGs and NIST 800-53 are both now requiring encryption at rest as a part of their standard. With vSphere/vSAN 6.5 and greater, customers have the ability to turn on a blanket encryption and vTPM to gain a more compliant state.

If organizations wish to enable vSphere encryption, they will need an encryption key manager – Entrust is the preferred VMware encryption key manager. A key manager is not the only part of the value of the Entrust Data Protection portfolio. Additionally, the following features/functionality are available:

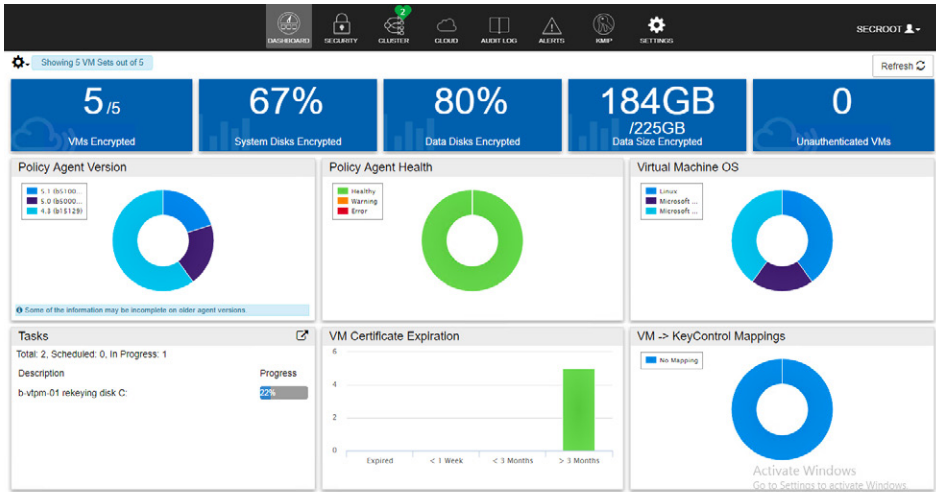
- Automated rekey of encrypted targets, resulting in no downtime or lack of access to data. Threat vectors are reduced with a robust key rotation strategy.
- Multi-cloud data protection. Environments are changing and are not consistent across enterprise resources. Entrust provides central governance of data in multi-cloud architectures and autonomous servers, as well as the legacy data center.
- The foundation to secure privileges from the data at rest, which can be used in conjunction with a more comprehensive ability to secure the entire stack with policy-based security.



VM Hardware

Encryption	VM configuration files are encrypted. Hard disk is encrypted.
› CPU	2 CPU(s)
› Memory	6 GB, 0.12 GB memory active
› Hard disk 1 (encrypted)	40 GB
› Network adapter 1	Blue (connected)
CD/DVD drive 1	Disconnected
› Video card	8 MB
› Virtual Trusted Platform Module	Present
VMCI device	Device on the virtual machine PCI bus that provides support for the virtual machine communication interface
› Other	Additional Hardware
Compatibility	ESXi 6.7 and later (VM version 14)

Edit Settings...



Showing 5 VM Sets out of 5

5 /5 VMs Encrypted

67% System Disks Encrypted

80% Data Disks Encrypted

184GB /225GB Data Size Encrypted

0 Unauthenticated VMs

Some of the information may be incomplete on older agent versions.

Tasks

Total: 2, Scheduled: 0, In Progress: 1

Description	Progress
b-vtpm-01 rekeying disk C:	22%

VM Certificate Expiration
6
4
2
0
Expired
< 1 Week
< 3 Months
> 3 Months
VM -> KeyControl Mappings
No Mapping
Activate Windows
Go to Settings to activate Windows.

Simplifying CCRI

CCRI can be a high-cost, high-risk challenge. The end-to-end Entrust CCRI solution helps organizations ensure audit-readiness, while reducing the cost and time burden. Entrust CCRI is the first solution of its kind to provide both Encryption at Rest and DISA STIG remediation in a highly automated, comprehensive package.

Learn more at
entrust.com

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