White Paper

National Institute of Standards and Technology (NIST) 800-53 and Entrust

ENTRUST

SECURING A WORLD IN MOTION

Introduction

In this paper, we will explore background topics around Federal Information Security Modernization Act (FISMA), NIST, and NIST Special Publication 800-53. We will then examine specific security controls called out by 800-53 and we will map how those controls are addressed by Entrust.

Background

The U.S. Government has recognized the importance of information and data security, codified in FISMA 2002. FISMA requires government agencies to develop and enforce policies around secure configuration and deployment of information systems with the understanding that securely configured systems are more secure and present fewer opportunities for compromise. These requirements are captured in Federal Information Processing Standards (FIPS) Publication 200, Minimum Security Requirements.

With the goals of reducing cost and risk in complying with FISMA directives captured in FIPS 200, NIST has produced a number of documents and guidelines, among them NIST SP 800-53. NIST 800-53 "provides a catalog of security and privacy controls for federal information systems and organizations and a process for selecting controls to protect organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation from a diverse set of threats, including hostile cyber-attacks, natural disasters, structural failures, and human errors. The controls are customizable and implemented as part of an organization-wide process that manages information security and privacy risk."

The current revision, R4, was published in April 2013 and is is the most comprehensive rework of the piece since initial publishing in 2005. One of the biggest changes was an increased emphasis on a holistic approach to security, including a "build it right" strategy of baking security into the fabric of the network as well as underscoring the importance of continuous monitoring to provide organizations with necessary real-time data to take appropriate steps with regard to security.

"...Through the process of risk management, leaders must consider risk to U.S. interests from adversaries using cyberspace to their advantage and from our own efforts to employ the global nature of cyberspace to achieve objectives in military, intelligence, and business operations..."

— National Strategy for Cyberspace Operations
Office of the Chairman, Joint Chiefs of Staff U. S. Department of Defense White Paper

Security controls

NIST 800-53 groups security controls into 18 families, listed below. Of these, six focus on controlling and tracking infrastructure access or ensuring configuration or system integrity. These are the controls where Entrust can help with compliance.

ID	Family	ID	Family
AC	Access Control	MP	Media Protection
AT	Awareness and Training	PE	Physical and Environmental Protection
AU	Audit and Accountability	PL	Planning
CA	Security Assessment and Authorization	PS	Personnel Security
CM	Configuration Management	RA	Risk Assessment
CP	Contingency Planning	SA	System and Services Acquisition
IA	Identification and Authentication	SC	System and Communications Protection
IR	Incident Response	SI	System and Information Integrity
MA	Maintenance	PM	Program Management

"...Leaders at all levels are accountable for ensuring readiness and security to the same degree as in any other domain..."

—National Strategy for Cyberspace Operations
Office of the Chairman, Joint Chiefs of Staff U. S. Department of Defense White Paper

Entrust enables access control (AC) compliance

Entrust Access Control can, in general, extend and enhance compliance for virtualized platforms. Specifically, we support two-factor authentication (2FA) and multifactor authentication while preventing the sharing of root accounts, disabling default passwords, and enabling Role-Based Access Control (RBAC) in addition to highly granular authorization.

AC Control	NIST requirement for FISMA compliance	Virtualization platform constraints/gap	Entrust requirement fulfillment for virtual environments
Account Management (AC-2)	Specify access privileges and grant access to the system based on: (i) a valid access authorization; (ii) intended system usage; and (iii) other attributes as required by the organization or associated missions/ business functions.	• Supports single-factor authentication only • Allows root account sharing • Allows default passwords • Defaults to admin privileges for all operations	• Supports multi-factor authentication • Prevents root account sharing • Prevents use of default passwords • Enables limited access privileges based on intended system usage and other attributes
Access Enforcement (AC-3)	Enforce approved authorizations for logical access to the system in accordance with applicable policy.	Enables broad access privileges based on roles only	Enforces authorization policy defined by granular role-based and attribute-based access privileges
Information Flow Enforcement (AC-4)	Enforce approved authorizations for controlling the flow of information within the system and between interconnected systems in accordance with policy.	Allows unfiltered VM- to-VM communications, unconstrained by policy	Enforces trust zone policies that constrain users' ability to change information flows
Separation of Duties (AC-5)	Implement separation of duties through assigned information system access authorizations.	• Provides limited ability to enforce access policies separating duties • Provides no pre-defined roles besides administrator	• Provides the authorization granularity needed for effective separation of duties • Provides 17 pre-defined, customizable roles
Least Privilege (AC-6)	Employ the concept of least privilege, allowing only authorized accesses for users which are necessary to accomplish assigned tasks in accordance with organizational mission.	Defaults to super user privileges	Allows only the operations and access to virtual resources users need to do their jobs

(Continued from previous page)			
AC Control	**NIST requirement for FISMA compliance**	**Virtualization platform constraints/gap**	**Entrust requirement fulfillment for virtual environments**
Security Attributes (AC-16)	Support the binding of security attributes to information in storage, in process, and in transmission.	Provides no mechanism to tag virtual objects with security attributes	Enables object tagging with security attributes that enable robust and flexible access control

Entrust enables audit and accountability (AU) compliance

With Audit and Accountability, Entrust enables richer, better logging than the stock virtualization platform does on its own, enabling easier compliance and better forensics.

AU Control	NIST requirement for FISMA compliance	Virtualization platform constraints/gap	Entrust requirement fulfillment for virtual environments
Audit Review, Analysis, and Reporting (AU-6)	Analyze and correlate audit records across different repositories to gain organization-wide situational awareness	Provides basic virtualization event data to SIEM solutions that may not be detailed enough for correlation with physical data center audit records	Provides the thorough, fine-grained virtualization event data needed by SIEM solutions for correlation with similarly detailed physical data center records
Non-Repudiation (AU-10)	Protect against an individual falsely denying having performed a particular action.	Allows admin anonymity via sharing of root account	Associates unique user ID with every event logged
Audit Generation (AU-12)	Provide audit record generation capability for the list of auditable events defined in AU-2. Produce audit records in a standardized format.	• Creates separate log files for vCenter and each host server • Uses different log formats for vCenter vs. hosts	• Consolidates and centrally manages logs covering vCenter and all hosts • Uses a single, uniform format for combined vCenter and host log data

Entrust enables security assessment and authorization (CA) compliance

For Security Assessment and Authorization Compliance, control CA-7 stipulates establishing continuous monitoring for configuration changes as well as a way to determine the security impact of changes to systems.

CA Control	NIST requirement for FISMA compliance	Virtualization platform constraints/gap	Entrust requirement fulfillment for virtual environments
Continuous Monitoring (CA-7)	Establish a continuous monitoring strategy and implement a continuous monitoring program that includes: • A configuration management process for the information • A determination of the security impact of changes to the information system	• Does not provide functionality to continuously monitor and manage the hypervisor configuration • Does not provide functionality to determine the security impact of changes to the hypervisor configuration • Can only implement permissions on virtual objects in a hierarchical fashion; cannot implement meaningful permissions in a dynamic environment	• Continuously monitors hypervisor configurations for drift and policy violations in vCenter and all hosts • Determines the security impact of configuration changes by continuously comparing configuration states to baselines such as CIS Benchmark standards, VMware Best Practices, and other frameworks • Can establish permissions and policies that can follow the virtual machine regardless of where it resides in the environment

Entrust enables configuration management (CM) compliance

With Configuration Management Compliance, the control calls out the need to have central management over hypervisor configuration, including the ability to monitor, manage, and apply settings. While these capabilities are not native to the hypervisor, with Entrust it is possible to monitor, verify, and control hypervisor configuration while also centrally enforcing access to the hypervisor.

CM Control	NIST requirement for FISMA compliance	Virtualization platform constraints/gap	Entrust requirement fulfillment for virtual environments
Configuration Settings (CM-6)	Monitor and control changes to configuration settings in accordance with organizational policies and procedures. Employ automated mechanisms to centrally manage, apply, and verify configuration settings. Employ automated mechanisms to respond to unauthorized changes to organization's configuration settings. Demonstrate conformance to security configuration guidance (i.e., security checklists), prior to being introduced into a production environment.	• Does not provide functionality that verifies, monitors, or controls hypervisor configurations • Does not provide means to generate alerts for unauthorized configuration changes • Is not able to check if a configuration conforms with policy or checklist	• Verifies, monitors, and controls hypervisor configuration changes • Provides configuration change request logs to SIEM solutions that can be used to trigger alerts • Enables organization to check if a configuration conforms with a customized configuration policy or with guidance such as Center for Internet Security (CIS) Benchmark standards, VMware Best Practices, or other frameworks
Least Functionality (CM-7)	Configure the information system to prohibit or restrict the use of specified functions, ports, protocols, and/or services.	Enables some configuration of access restrictions on individual hosts	Centrally enforces hypervisor access policy via protocol (Secure Shell (SSH), vSphere client, Simple Object Access Protocol (SOAP)) and hypervisor IP address controls on all hosts

Entrust enables identification and authentication (IA) compliance

The native capabilities of the hypervisor fall short of requirements of IA controls in a couple of areas. One is that it is possible to share root passwords and the other is a lack of support for multifactor authentication. With Entrust, both of these areas are addressed. All users have unique IDs which are tied to user actions in the logs. Additionally, Entrust supports two-factor authentication, providing a more secure environment.

IA Control	NIST requirement for FISMA compliance	Virtualization platform constraints/gap	Entrust requirement fulfillment for virtual environments
Authentication (Organizational Users (IA-2)	Uniquely identify and authenticate organizational users, including organizational employees or individuals the organization deems to have equivalent status of employees (e.g., contractors, guest researchers, individuals from allied nations). Use multifactor, replay-resistant authentication for network and local access to privileged accounts. For network accounts, one of the factors is provided by a device separate from the information system being accessed. Allow the use of group authenticators only when used in conjunction with an individual/ unique authenticator.	• Permits root account sharing, enabling anonymous access • Requires password for access; does not support multi-factor authentication	• Requires a unique ID for access by an organizational user and associates the unique ID with every operation performed by the user • Supports multifactor, replay-resistant authentication such as RSA SecurID and hardware tokens for network and local access to privileged accounts
Identification and Authentication (Non-Organizational Users) (IA-2)	Uniquely identify and authenticate non-organizational users.	Permits potential root account sharing by non-organizational users, enabling anonymous access	Requires a unique ID for access by a non-organizational user and associates the unique ID with every operation performed by the user

Entrust enables system and information integrity (SI) compliance

With the System and Information Integrity Control, we deal most closely with SI-9, which calls for restrictions on who can input information into the system. The native virtualization platform has only very coarse-grained ability to control input. Entrust augments these capabilities with role-based authorization, enabling fine-grained control.

SI Control	NIST requirement for FISMA compliance	Virtualization platform constraints/gap	Entrust requirement fulfillment for virtual environments
Information Input Restrictions (SI-9)	Restricts the capability to input information to the information system to authorized personnel. Restrictions may extend beyond the typical access controls employed by the system and include limitations based on specific operational/ project responsibilities.	Does not restrict the ability to input information based on specific operational/ project responsibilities	Restricts the capability to input information, via any access method, using role-based authorization sufficiently fine-grained to distinguish between users' operational/project responsibilities

Conclusion

Virtualization has brought many changes to the way IT is run. Beyond the well-understood benefits in cost savings and business and mission agility though, virtualization has also concentrated power over many, if not most, of the systems run by an organization in the hypervisor and special accounts with administrative power over the hypervisor.

One could then reasonably expect that these high-value accounts as well as the hypervisor itself to be targeted for attack. From the adversary's point of view, the game has become far simpler. Capture the right account and you have keys to the kingdom. In the past there was considerably less centralization, but now he who owns the hypervisor owns the kingdom.

Beyond the very real risks of external adversaries such as APT1, etc., there are also internal risks that need to be taken into account. Consider the rogue insider. Or, consider the well-intended but fat-fingered hyper admin who fat fingers the draining of the wrong VM(s). We have seen both scenarios in the field and they can both result in compromise of data, systems, and ultimately mission.

In the end, while everything has changed, many things remain the same. Generally speaking, a well-designed, well-secured network will do well with compliance and, if security fundamentals are kept in mind when designing the network, then the end product will be better and more secure.

While guidelines and white papers can be helpful, every network and every mission are different. We would be happy to discuss your particular scenario and share some ideas that have worked well in similar scenarios.

For more information

888 690 2424
+1 952 933 1223
sales@entrust.com
entrust.com

ABOUT ENTRUST CORPORATION

Entrust is dedicated to securing a world in motion by enabling trusted identities, payments, and data protection. Today more than ever, people demand seamless, secure experiences, whether they're crossing borders, making a purchase, accessing e-government services, or logging into corporate networks. Entrust offers an unmatched breadth of digital security and credential issuance solutions at the very heart of all these interactions. With more than 2,500 colleagues, a network of global partners, and customers in over 150 countries, it's no wonder the world's most entrusted organizations trust us.

Learn more at
entrust.com

Entrust and the Hexagon logo are trademarks, registered trademarks, and/or service marks of Entrust Corporation in the U.S. and/or other countries. All other brand or product names are the property of their respective owners. Because we are continuously improving our products and services, Entrust Corporation reserves the right to change specifications without prior notice. Entrust is an equal opportunity employer.
© 2021 Entrust Corporation. All rights reserved. HS22Q1-dps-nist-800-53-entrust-wp

ENTRUST

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