CENTRIFY SOLUTIONS BRIEF

Centrify Solution for Continuous Diagnostic Monitoring (CDM) and Continuous Monitoring as a Service (CMaaS)

Centrify Server Suite addresses critical requirements within Phase 2 of the CDM Program as defined by the Department of Homeland Security:

- Network Access Controls (NAC)
- Manage Credentials and Authentication (MCA)
- Manage Account Access (MAA)

FA9 - Manage Account Access (MAA)

The Requirement

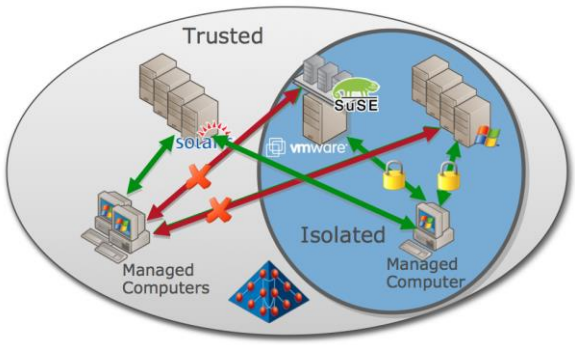
The Manage Account Access (MAA) Function is to prevent access beyond what is needed to meet business mission by limiting account access and eliminating unneeded accounts to prevent attackers from gaining unauthorized access to sensitive data. The Manage Account Access capability will assign access to computing resources based, in part, on their level of trustworthiness (as determined in Functional Area 6, Section 2.2.1.6).

Specific Functional Requirements with Centrify Remediation

- Prevent access beyond what is needed to meet business mission
  - Centrify enforces a centrally managed, locally enforced, least access policy to limit user access to only those resources based on business requirements
- Limit account access to prevent attackers from gaining unauthorized access to sensitive data
  - Centrify eliminates usage of shared accounts which are a primary source of attack, instead providing a centrally managed, locally enforced, fine grained privilege elevation solution to empower administrative staff to perform their job duties without changing their identities.
- Eliminate unneeded accounts to prevent attackers from gaining unauthorized access to sensitive data
  - Centrify eliminates the need for secondary accounts through fine grained privilege management for specific tasks as required by the user's job function as allowed on specific resources.
- Assign access to computing resources based, in part, on level of trustworthiness (as determined in Functional Area 6: TRU)
  - Centrify provides a granular role-based management model that enables granting privileges based on job function and account status as managed within Active Directory.

Centrify Solution Summary

- Centrify Server Suite provides a centrally managed host-based security solution to enforce Role-based management for access to critical servers and applications that serve the Mission.



- Centrify simplifies the management and enforcement of least access and least privilege policies to reduce risk of attacks on sensitive systems and data.

FA8 - Manage Credentials and Authentication (MCA)

The Requirement

The Manage Credentials and Authentication (MCA) Function is to prevent a) the binding of credentials to or b) the use of credentials by other than the rightful owner (person or service) by careful management of credentials, preventing attackers from using hijacked credentials to gain unauthorized control of resources, especially administrative rights. The MCA capability ensures that account credentials are assigned to, and used by, authorized people. This capability will rely on the results of the Manage Account Access capability (Section 2.2.1.9) to ensure that only trusted people receive credentials. This covers credentials for physical and logistical access.

Specific Functional Requirements with Centrify Remediation

- Prevent the binding of credentials to other than the rightful owner (person or device) by careful management of credentials
  - Centrify enforces smart card login on Linux and Mac computers to ensure the proper identification of users at login.
- Prevent the use of credentials by other than the rightful owner (person or service) by careful management of credentials
  - Centrify leverages Active Directory as the sole source of user identity once the user has authenticated using his Smart Card, thus ensuring the identity used on the network

will always represent the user who performed the initial authentication.

- Prevent the use of hijacked credentials to gain unauthorized control of resources, especially administrative rights
  - Centrify enforces the use of Kerberos, which can only be obtained after smart card login, to strongly identify users upon access to servers and applications. This effectively eliminates the use of passwords across the entire environment.
  - Centrify also enables the elimination of secondary Active Directory identities for Windows Administrators which are typically members of the Domain Administrators group typical of environments where the user needs to perform administrative duties with domain admin rights. Centrify provides a granular privilege elevation capabilities for Windows computers to ensure that the least amount of privileges are granted on specific systems where needed without granting full Domain Administrator rights to anyone. This solution will ensure that no user will login to any computing resource with the Domain Administrator rights.
- Ensure that account credentials are assigned to, and used by, authorized people
  - Centrify leverages Active Directory for the authoritative user identity repository, which is typically managed directly through automated feeds from an HR system to ensure that only active employees will have a valid account.
- Rely on the results of the Manage Account Access (MAA) capability to ensure that only trusted people receive credentials
  - The Centrify solution tightly couples the management of user credentials, their Account and privileges to ensure that only authorized users are allowed to access systems they are authorized, that they can only execute privileged commands they are authorized on the systems where authorized and any activity run with privilege is recorded to ensure accurate auditing and accountability.

Centrify Solution

- Centrify provides access and policy management for computer objects, authentication, authorization roles and command level control leveraging Active Directory. The Centrify Agent on UNIX, Linux, Windows and Mac systems enforce this centrally managed policy to ensure compliance with the functional requirements.
- Centrify provides complete account and authorization controls for Unix, Linux and Windows servers and workstations for both access control to sensitive systems and command level control for authenticated users.

FA5 - Network Access Controls (NAC)

Requirement

Function is to prevent, and allow the agency to remove and limit, unauthorized network connections/access to prevent attackers from exploiting internal and external network boundaries and then pivoting to gain deeper network access and/or capture network resident data in motion or at rest. Boundaries include firewalls as well as encryption (virtual private networks). Additionally, the function will prevent, remove, and limit unauthorized physical access.

Specific Functional Requirements with Centrify Remediation

- Prevent unauthorized network connections/access; limit if not preventable; remove if established
  - Centrify provides IPsec-based Server Isolation technology that enables computer systems to locally require authentication prior to communication at the network layer to ensure that only authorized systems are allowed access. This solution provides logical isolation to ensure that sensitive systems can only be accessed from other authorized computers.
- Prevent attackers from exploiting internal and external network boundaries
  - Centrify provides IPsec-based Server isolation to enable definition and enforcement of much more granular network access policies based on mutual authentication of hosts in a peer to peer model across network boundaries as may be required by the Mission. This model works to significantly limit the attack surface for any attack on a workstation as Servers can be configured to refuse all network traffic that is not explicitly allowed both in-bound and out-bound.
- Prevent attackers from pivoting to gain deeper network access
  - Centrify provides policy enforcement to both single sign-on functions for any user who gains access to a server from his workstation to limit risks of further access by an attacker.
- Prevent capture of data in motion
  - Centrify will enforce IPsec policies that require encryption as defined on a port by port basis between authorized computers.
- Prevent capture of data at rest
  - Centrify provides the management to enable usage of FileVault for encryption of Mac computers to prevent access to data stored on these systems.
  - Centrify also provides management of mobile devices and enforcement of storage encryption.
- Prevent unauthorized physical access; limit if not preventable; remove if gained
  - Centrify does not have a solution for this requirement.

Centrify Solution

- Centrify provides Server and Domain Isolation capabilities for UNIX and Linux systems that is interoperable with Microsoft IPsec technologies to enable a much more granular network access from any given system to only those other systems it is authorized to communicate with.
- Centrify leverages Active Directory Group Policy to define and globally enforce common security policies such as firewall policies and disk encryption policies to further secure the environment.

Contact Centrify

Santa Clara, California	+1 (669) 444-5200
EMEA	+44 (0) 1344 317950
Asia Pacific	+61 1300 795 789
Brazil	+55 11 3958 4876
Latin America	+1 305 900 5354
Email	sales@centrify.com
Web	http://www.centrify.com

To get started, try our free version: http://www.centrify.com/express