Common Criteria Evaluation and Validation Scheme
National Information Assurance Partnership (NIAP)

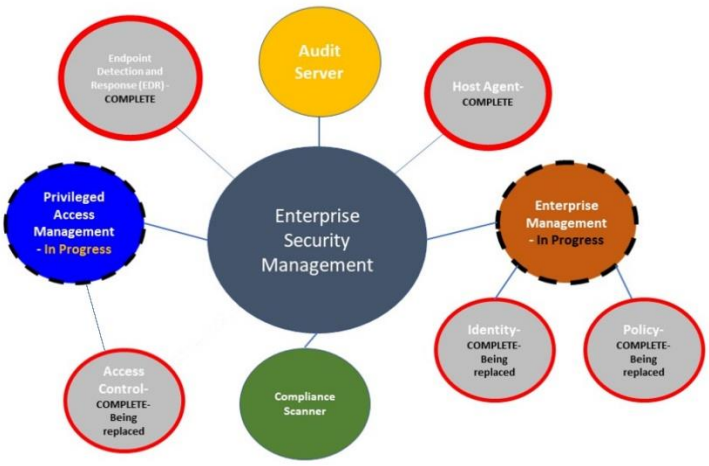
Title: Enterprise Management (EM)
Maintained by: National Information Assurance Partnership (NIAP)
Unique Identifier: 00x
Version: 2.3x
Status: Draft
Date of issue: 05/15/2024
Approved by:
Supersedes:

Background and Purpose

This document describes a core set of security requirements for Enterprise Management systems. These requirements cover basic security characteristics and behaviors for an EM server.

Enterprise Management (EM) systems are used to deploy software and manage systems in an enterprise. EM systems typically consist of a host, and may include endpoint host agents to allow for the discovery, reporting and remediation of IT policy and security issues.

The diagram below is to provide context of the previous ESM suite and how it is evolving. Specifically, Enterprise Management PP will be replacing Identity and Policy while PAM will be replacing Access Control. Audit Server and Compliance Scanner will be future efforts.



The intent is that the remaining sections provide succinct statements that highlight the relevant aspects to be addressed by the Technical Community (TC) constructing the PP. Here, the authors provide a narrative that introduces the reader to the problem being solved, and present key aspects that support or guide the TC, and may elaborate on subtleties not apparent in the "bulleted" high level statements.

Use Case(s)

[USE CASE] **Monitoring and Management**

[USE CASE 1] **Event Management**

The ability to handle event management and monitoring across server and workstation endpoints.

[USE CASE 2] **Standard Services and Alerts**

The ability to monitor multiple system services across endpoints, such as alerting for low disk space, high memory usage alerts, account creations, accounts being added or removed from groups, services stopping.

[USE CASE 3] **Patching**

The ability to collect patching levels and deploy updates.

[Use Case 4] **Policies**

The ability to deploy policies to server and workstation endpoints, in addition to deploying instructions to network configurable infrastructure devices.

[USE CASE 5] **Discovery**

The capability to browse, query, and export aggregated host-based endpoint data through a management dashboard query interface, in addition to automatically add newly discovered endpoints to a monitored database.

[USE CASE] **Expandability**

[USE CASE 1] **Vendor Expansion**

The ability to integrate with additional vendor packages for monitoring and configuration of varying physical and virtual hardware.

[USE CASE 2] **Resource Expansion**

The capability to generate performance and analysis to estimate when a monitored resource will be exhausted.

[USE CASE] **Security**

The ability to function in any configuration of endpoints with or without agents in the following ways.

Agent

[USE CASE 1] **Detection of Potential Unauthorized Activity**

The ability for agents to detect potentially unauthorized activity, software, or users by collection of host-based endpoint data and reporting back to the management server for further analysis.

[USE CASE 2] **Remediation of Malicious Activity**

The ability for the management server to instruct agents to perform remediation activities on the endpoints to cleanup detected malicious activity and report back through secured channels.

Agentless

[USE CASE 1] **Detection of Potential Unauthorized Activity**

The detection of potentially unauthorized activity, software, or users is enabled by remote collection of host-based endpoint data by the management server.

[USE CASE 2] **Remediation of Malicious Activity**

The ability to perform remediation activities on the endpoint remotely from the management server to cleanup detected malicious activity.

Resources to be Protected

- Sensitive data stored by the EM system.
- Credentials for authentication to or from the EM system.
- Cryptographic key material used to perform secure communications with host agents.
- Sensitive data in transit to or from the EM system.

Attacker Access

Here the author provides the threat paths that the requirements need to address and mitigate. This includes the type of access an attacker may have to target. This would include whether there is a concern regarding remote or local access to the target, or whether there are special concerns regarding physical access.

- An attacker can arbitrarily update and deploy policies and/or applications to endpoints.
- An attacker can exploit the lack of an established standard for communication between the EM server and host agents or endpoints.
- An attacker with access to the EM server can view or change authentication credentials to the management interface.
- An attacker can impersonate the Enterprise Management server on the network.

Essential Security Requirements

- Patch Management
    - Scanning and updating patches is important enterprise security and requires management at all phases: QA, development, staging, production, etc. and maintaining strict policies to avoid any unexpected events.

- Policy Management
    - Exception creation and policy configuration
    - View protected processes
    - Agent and EM settings
        - Heartbeat Interval
        - Reporting Interval
    - Content updates

- Vulnerability Assessment
    - Import unknown hashes and set policy for them based on rules
        - Ability to administratively override previous policies
    - Scanning hosts for missing patches, configurations, security policies
        - Scanning file executions and running files
- Architecture
    - Resiliency
        - Failover
        - Load balanced
    - Endpoint and Tenant Management
        - Role-based access control
        - Agent revocation

    - Permission Segregation
        - Role based Tier model, protecting privileged accounts and resources from non-privileged.
    - Compliance
        - Auditing capabilities
    - Confidentiality
        - Encrypted communication between EM host and clients
- Risk Management
    - Behavior Detection/Threat Modeling
    - Network Virtualization
    - Ties into architecture with custom defense strategies based on the capabilities of the architecture
    - Zero Trust
- Reporting Capabilities
    - Log forwarding (SIEM, Syslog, Email, etc.)
    - Security events search criteria

Threats

T.NETWORK_ATTACK
An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may engage in communications with applications and services running on or part of the OS with the intent of compromise. Engagement may consist of altering existing legitimate communications.
T.NETWORK_EAVESDROP
An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may monitor and gain access to data exchanged between applications and services that are running on or part of the OS.
T.LOCAL_ATTACK
An attacker may compromise applications running on the OS. The compromised application may provide maliciously formatted input to the OS through a variety of channels including unprivileged system calls and messaging via the file system.
T.LIMITED_PHYSICAL_ACCESS
An attacker may attempt to access data on the OS while having a limited amount of time with the physical device.

Assumptions

The following assumptions are made for the EM software product and its operational environment. The Enterprise Management Software is not expected to provide any assurance in any of these areas, and as a result, requirements are not included to mitigate the associated threats.

- A.PLATFORM

The TOE relies upon a trustworthy computing platform with a reliable time clock for its execution. This includes the underlying platform and whatever runtime environment it provides to the TOE.

- A.PROPER_ADMIN
  The Administrator of the software solution is not careless, wilfully negligent or hostile, and administers the OS within compliance of the applied enterprise security policy.
- A.PROPER_USER
  The user of the application software is not wilfully negligent or hostile, and uses the software in compliance with the applied enterprise security policy.
- A.PHYSICAL_PROTECTION
  The Enterprise Management Software is physically protected in it's operational environment and not subject to physical attacks that compromise the security or interfere with the host device's physical interconnections or ability to operate at full capacity. This protection is assumed to be sufficient to protect the data contained within the Enterprise Management Software solution.
- A.REGULAR_UPDATES
  The Enterprise Management Software is assumed ot be updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities

Operational Environment

Security Objectives for the Operational Environment

- OE.PLATFORM
  The TOE relies upon a trustworthy computing platform for its execution. This includes the underlying operating system and any discrete execution environment provided to the TOE.
- OE.TRUSTED_ADMIN
  Security Administrators are trusted to follow and apply all guidance documentation in a trusted manner. For Enterprise Management Software, this includes the Administrator responsible for configuring, deploying, and updating the primary software solution.
- OE.PROPER_USER
  The user of the application software is not willfully negligent or hostile, and uses the software within compliance of the applied enterprise security policy.
- OE.PHYSICAL
  Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.
- OE.UPDATES
  The TOE firmware and software is updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.