

Title: Enterprise Security Management (ESM) - Enterprise Management (EM)

Maintained by: National Information Assurance Partnership (NIAP)

Unique Identifier: 00x

Version: 0.1x

Status: draft

Date of issue:

Approved by:

Supersedes:

Background and Purpose

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

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 presents key aspects that support or guide the TC, and may elaborate on subtleties not apparent in the “bulleted” high level statements.

Use Cases

This section is intended to provide the initial scope/bound of the security problem by providing the reader with concise statements regarding the scenarios in which the technology is being used. The intended usage presented here should lay the groundwork for the identifying the resources to be protected, and what threats must be considered in the drafting of the Essential Security Requirements (ESR) and for the TC to consider when writing the PP.

[USE CASE 1] Detection of Potential Unauthorized Activity The detection of potentially unauthorized activity, software, or users is enabled by the collection of host-based endpoint data to a central ESM where the data is analyzed.

[USE CASE 2] Remediation of Malicious Activity The ability to initiate remediation commands to attempt a cleanup of detected malicious activity is a key use case of ESM.

[USE CASE 3] Discovery The capability to effectively browse, query, and export aggregated host-based endpoint data enables a SOC analyst to discover adversaries in post-compromise scenarios.

Resources to be protected

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

Attacker access

- An attacker is assumed to attempt attacks from the following vantage points:
 - The network across which the application engages in communication, both actively and passively. Including potentially IOT devices and BYOD.
 - The platform on which the application is installed, though as an unprivileged subject.
 - The endpoint (host agent) by planting crafted malicious artifacts on the Endpoint platform to be consumed by the ESM System.
- An attacker has an arbitrary amount of time to analyze the behavior of the application, its interaction with its host device or platform, and/or the data it transmits over the network.

Essential Security Requirements

This is where the authors present an initial set of English requirements that specify security functionality, rather than design and/or implementation characteristics. These requirements will provide the foundation for which the detailed set of requirements is derived. It is important that the requirements captured here make an attempt to fully address the categories (e.g., access control, identification, authentication, management capabilities, roles of administration, secure communications, and audit). That's not to say the requirements are fully specified or detailed enough to simply translate to Common Criteria security functional requirements. The goal is that there is enough information contained here, as well as the other sections of this document, to provide the TC enough information to ensure they have an understanding of what is minimally required in breath.

- 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 ESM settings
 - Heartbeat Interval
 - Reporting Interval
- 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
 - 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 ESM 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

Assumptions

Simply put, this section presents the aspects of the product and its intended environment that can be assumed to hold true. This will provide additional scope on the resulting PP. The following assumptions are made for the ESM product and its operational environment:

- Depending on configuration and capability, the product may or may not be:
 - Bound to directory server or cloud environment to support multi-user login
- The ESM system is connected to a network. For purposes of sending/receiving endpoint agent data. Other entities on the network are not inherently trustable.
- Administrators are not malicious in nature.
- Users are not malicious in nature, though they may inadvertently or intentionally engage in risky behavior.

Optional Extensions

- Policy Management
 - Exceptions for Active Directory (AD) objects
 - Assign rules to AD objects
 - Change mode per process
 - Report or block an event based on process or category of process
- Architecture
 - Resiliency
 - Failover
 - Loadbalanced
 - Local only configurations
 - Compliance
 - Ability to assign separately privileged auditors
 - Collaboration
 - Invite third party or vendor to automatically create rules and import
 - All communication is encrypted and certificate based authentication
 - Customization
 - Allow for custom modules to hook into the architecture based upon client needs
- Vulnerability Assessments
 - Virtual agents or bots can perform tasks using natural language processing (NLP)
 - Automated ticketing, escalation, resolution
- Reporting Capabilities
 - Custom notification message
 - Self-Service Portal
 - Dashboard
 - Display quarantined files that are eligible to be restored to their original location on the endpoint
 - Smart search capabilities to find answers easily and quickly
 - Intelligent analytics enable workflow optimization and automation
 - Metrics can be created from unstructured data and additionally be gathered analyzed efficiently

Outside the TOE's Scope

- Cloud ESM devices – this is not to include a VM running in the cloud running ESM, but ESM cloud specific tool like AWS Security Hub or Azure Sentinel