State of California

California Department of Technology

Office of Information Security

Endpoint Protection Standard

SIMM 5355-A

January 2019

REVISION HISTORY

REVISION	DATE OF RELEASE	OWNER	SUMMARY OF CHANGES
Initial Release	**January 2019**	**California Information Security Office**	**New Standard in support of SAM Section 5355, Endpoint Defense**

TABLE OF CONTENTS

I. INTRODUCTION

To counter the increasingly sophisticated threat to state data and networks, state entities must ensure that they abide by this standard and have all required capabilities. If the entity has an existing platform that only partially covers the capabilities listed below, it is required to seek out an additional or replacement technology to ensure that any associated gaps are addressed.

II. MINIMUM ENDPOINT SECURITY REQUIREMENTS

Endpoint security technologies deployed by the State must have the following required and recommended capabilities for protection, detection, investigation, containment and remediation.

A. Detection and Protection Capabilities

Endpoint security technologies used by the State shall:

1. Utilize both signature and signature-less detection and prevention techniques (solution should not require manual scanning of endpoints as its sole detection and prevention technique).
2. Provide real-time on-agent prevention and detection, without the need for constant remote connectivity or updates.
3. Utilize artificial intelligence designed to prevent and detect abnormalities and attempted exploits including "zero day" (never-before seen malware) attacks, and use indicators of compromise to identify abnormalities.
4. Detect and prevent memory-based and/or "file-less" attacks.
5. Support common Security Information and Event Management (SIEM) integrations via open Application Programming Interface (API), which can be utilized by the California Department of Technology (CDT) Security Operations Center (SOC) to perform integrations.
6. Provide a centralized software distribution process for updates or integration with an existing distribution solution.
7. Support endpoints located off-premise and agents deployed in a Cloud Platform as a Service and Infrastructure as a Service environment (common resources within cloud infrastructures should be capable of having the solution deployed to it) as well as virtualized machine environments.
8. Support a tiered management structure with multi-tenancy options for sub-allocated management teams (State, Agency) and support Role Based Access Control (RBAC) and delegated access options.
9. Detect user access levels on endpoints, including administrative access, and provide additional search and analytic capabilities with this data.
10. Provide a means to see a near real-time endpoint inventory, and online reports for system application, including versions of applications.
11. Detect rogue endpoints (endpoints on the entities network not covered by the selected endpoint solution).
12. Support current releases of Windows and Linux and be continually updated by the vendor to new versions as they are released.

Additionally, the following detective and protective features are desirable and highly recommended:

1. As enterprise network environments are highly virtualized it is imperative to keep system resources low. Specifically, agent should utilize below 50 MB of memory and 3% CPU while agent is active and 1.5% while idle.
2. Install/Update/Upgrade on-endpoint agent without system reboot.
3. Provide support for current releases of Apple OS X and other Linux/UNIX based operating systems as required by the entity to adequately protect their environment.
4. Provide on-premise and/or off-premise device protection for non-traditional endpoints such as Internet of Things (IoT) and mobile devices.
5. Provide integrations with common/popular business system remediation ticketing systems.

B. Investigative Support Capabilities

The investigate functions of the endpoint security technologies and processes must:

1. Include a historical timeline of all primary endpoint events across all monitored endpoints to determine the technical changes that occurred (e.g., file, registry, network, driver and execution activities) and the business effect (e.g., loss of customer data and transaction fraud). Continuous recording of events on the endpoint is a critical capability.
2. Provide the following investigative scanning capabilities:
    a. RegEx, File, Hash, and value search across all endpoints.
    b. Malicious activity review and validation including analysis, tagging, notes, and workflows.
    c. Hunting via integrated event collection and analysis for defensive investigation / review of potential indicators of compromise.
3. Support root cause assessments via integrated forensic capabilities to include memory analysis, disk analysis, user and entity behavior analysis, and historical process mapping.
4. Provide pre-made analysis and reporting tools or queries (as well as the ability to customize reporting tools and searches).

Additionally, the following investigative features are desirable and highly recommended:

1. Have a centralized management console for determining the status of and issues with all managed endpoints.
2. Offer a visual, browser-based interface.
3. Provide virtual asset tagging.
4. Provide timeline threat graphic views to deliver guided investigations for analysts of a wide range of skillsets.

C. Containment Capabilities

The endpoint security technologies and processes used by state entities shall (at a minimum) contain the incident at the endpoint via automated actions which can be triggered by the local system manager and/or a security analyst (e.g. isolate, remediate, remove, restore to operation). The system must be capable of manually or automatically, via APIs, quarantining the system from the rest of the enterprise network, as well as killing and quarantining specific processes and malicious artifacts.

D. Remediation Capabilities

The endpoint security technologies and processes used by state entities shall (at a minimum) provide functionality allowing for a state agency's Security Operation Center (SOC) to remediate endpoints to a pre-infection state and should remove malicious files, roll back and repair other changes, or create Windows Microsoft Installer (MSI) files to be deployed by system management tools.

Additionally, solutions should have the capability to provide complete remediation instructions for security and IT groups to implement with their own toolsets.

E. DEFINITIONS

For the purposes of this standard:

Endpoints include:

- Workstations and Personal Computers: Any computational devices that run Windows, Linux variants, or Apple Operational Systems (OS).
- Servers: Physical, virtual and cloud-based computational servers that run Server OS variants of Windows, Linux or Apple.

Internet of Things (IOT) devices include:

- Non-traditional computational or "smart" devices, owned or authorized for use by the State, which do not fit the Endpoint definition above and have a network connection to state networks or the internet.

Mobile devices include:

- Handheld computational devices, owned or authorized for use by the State, which run a mobile Operating Systems such as Android and iOS.

File-less attacks include:

- Malicious malware attacks that exclusively exist as a memory-based artifact (i.e. in Random Access Memory) and do not write any part of its activity to the hard drive, and thus is resistant to traditional defenses such as whitelisting, signature detection, hardware verification, etc.

F. QUESTIONS

Questions regarding the implementation of this standard may be sent to:

California Department of Technology
Office of Information Security
Security@state.ca.gov