Kentucky Department of
EDUCATION

Office of Education Technology

KETS Endpoint Protection Recommendations

Version 1.6 – 5/6/2025

Document Owner:	Paul Shoemaker	Date Created:	12/11/2024
Approver(s):	OET Leadership	Date Approved:	8/7/2025

Summary: This document will provide recommendations and guidance for the procurement of Endpoint Protection Solutions for district use. This document should be shared with district/school leaders and vendors, so they will understand these guidelines prior to selecting and offering solutions. The goal is to assist in the procurement of Endpoint Protection Solutions that best serve the district and meet all necessary security and operational requirements before financial obligations are established or installation activity begins.

Intended Audience: The audience of these recommendations is District EdTech Staff, school and district leaders, and vendors/service providers. This document is to be shared within this audience to establish the needs of the districts (in terms of design and general uses) while ensuring the Endpoint Protection Solution will operate successfully within the technical and security requirements of the KETS environment.

Purpose and Scope: Endpoint protection solutions should have certain features and characteristics to ensure interoperation with other key parts of the KETS environment and be sustainable.

1. All computing devices managed or provided by districts, that are capable of using endpoint protection software (such as Windows and MacOS devices), should have endpoint protection software licensed, installed and operational.
2. The Endpoint Protection Solution should be capable of centralized management of clients/devices and be capable of enforcing security requirements such as updates to the client, definitions, quarantine efforts, etc.
3. Districts should ensure that Endpoint Protection Solution updates, including clients and any definitions/signature components, are regularly and consistently installed to protect against security vulnerabilities.
4. The Endpoint Protection Solution should include logging of alerts and events, on the device at a minimum and ideally centrally collected, which can be remotely accessed by admin staff for review.
5. The Endpoint Protection Solution should have heuristic scanning capability as well as traditional definition/signature scanning. AI and machine learning capabilities, for example, can improve protection against unknown (behavior based) threats.
6. The Endpoint Protection Solution should have real-time proactive and on-demand scanning capabilities.

7. The Endpoint Protection Solution should have browser activity protection, including protection against phishing attacks and malicious websites.

8. Districts should consider their endpoint environment and include protection coverage for Windows and MacOS operating systems and include Server platforms when selecting an endpoint protection solution.

9. Solutions should consider secure remote management, including secure internal network and external access.

10. Endpoint Protection Solutions should be properly scaled for the district's endpoint population. Districts should work closely with the selected vendors to tailor the solutions for proper scale of use and projected growth over the lifecycle of the proposed systems.

11. Endpoint Protection Solutions should be selected with consideration of their long-term lifecycle and total cost of ownership.

12. The endpoint protection solution should not exhaust the client device CPU/memory/hard drive resources while operating.

13. The districts should consider the solution's capability to create customized configurations/policies to address specific operating environments.

14. The solution should include robust vendor support that can be activated by the district upon request. Consider how a help request can be submitted (Phone, Text, Email) and what response times for a support request is expected.

15. Warranties and support should cover the lifecycle of the Endpoint Protection Solution. Other support arrangements or Software as a Service for Endpoint Protection Solutions should be selected with consideration of total cost of ownership and limited district technical staff. More expensive levels of vendor service may be worthwhile if allowing district edtech staff to focus on higher priorities.

16. Districts should consider any requirements from current or prospective Cyber Insurance providers.

Note that effective endpoint protection may result from multiple services and not just a single product. Several of the capabilities listed above may already be in place at your district and would not need to be included in another, separate product or service.