Method for enhancing the cybersecurity of an endpoint computer includes configuring an endpoint agent so that it resides on the endpoint computer to communicate with a cybersecurity device, configuring the endpoint agent to monitor and collect data on operating system events of the endpoint computer associated with each file from a set of files being executed on the endpoint computer, configuring the endpoint agent to send the collected operating system event data via a communication module to a cybersecurity device installed on a network selected from a group consisting of: i) an information technology network; ii) an operational technology network; iii) a cloud infrastructure, where the cybersecurity device contains a machine learning model for analyzing operating system event data from the endpoint computer received from each endpoint agent connected via an application programming interface to the cybersecurity device. While collecting data on operating system events, a set of real-time file content snapshots is taken, where each file content snapshot in the set corresponds to each operating system event on the endpoint computer, the resulting set of file content snapshots is uploaded via an endpoint agent to a cybersecurity device, where each file content snapshot in the set is time-stamped, and determine changes in the file contents by comparing the file content snapshots from the set using the cybersecurity device's machine learning model, followed by determining the time of the operating system event that poses a potential cybersecurity threat to the endpoint computer.