Managing Software Obsolescence: A Critical Requirement

Managing obsolescence for physical assets and components has been a no-brainer for years. What hasn't been as obvious is the growing need to manage obsolescence around software that powers increasingly smarter devices and equipment.

Just as components have a service life, so does software. Developers regularly offer new enhancements or provide patches and older software versions may no longer be compatible with newer hardware. In more extreme cases, code may be vulnerable to hackers, leading to potential cybersecurity breaches or service interruptions to mission critical or even lifesaving medical systems.

An obsolescence and patch management program can be very effective in preventing these issues. Product lifecycle data is a key element: general availability, end-of-life, and end-of-support dates can drive automated processes. N-1 version reporting can ensure that software remains current. Finally, up-to-the-minute vulnerability data for software – from trusted sources like the NIST CVE, GitHub Advisory and Maven – can ensure that potential threats can be addressed before they become a real problem.

Having this information available from a continuously curated source like IT-Pedia® supports proactive planning.

To learn more, contact info@eracent.com.

Terry Divelbliss, Sr. Vice President, Eracent