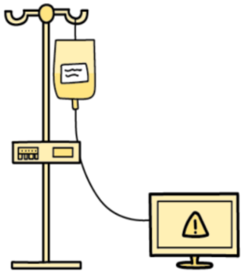
End-of-Life Software

Definition and Risks of using End-of-Life Technology

Botsford ASSOCIATES

What is End-of-Life Software?



End-of-life (EOL) software refers to software that is no longer being supported or maintained. This means the vendor will no longer release updates and security patches to protect against new vulnerabilities or provide technical service. Therefore, using EOL software comes with inherent risks that will only get worse as time passes. Organizations will need to decide whether to keep using the EOL software, upgrade it, or migrate to a new solution.

Cybersecurity Threats Intensified with Outdated Software

The financial sector is the one most commonly targeted by cybercriminals due to the sensitivity of it's data as well as the financial implications and tarnishing of reputation associated with a data breach. According to Palo Alto research, nearly half of ransomware attacks are caused by hackers exploiting system vulnerabilities such as unpatched or outdated software. Outdated software may result in higher risks of data breaches, disruption of services, DDoS attacks, and ransomware which could cause huge financial impacts for an organization.

Risks Involved with Continuing to Use End-of-Life Technology Past its Support Date

Many large software companies will continue to offer critical software support to its products even past its expiration date. However, these products will most likely not be prioritized as the company shifts its attention to its more up-to-date product offerings. As time continues past its end-of-support date, there will be more vulnerabilities that hackers can exploit, leaving potentially confidential data and systems at risk. The following are key risks that EOL software may pose:

Key Risks	Description
Compromised Security	When patches, bug fixes, and security upgrades are no longer available it presents a higher risk that hackers could breach application through an unpatched vulnerability. Older technologies also may be incompatible with modern encryption standards or two-factor authentication requirements.
Incompatibility with Latest Solutions	Software built on obsolete technology architecture may result in incompatibility when trying to integrate with the most recent hardware and software configurations.
Increased Maintenance Costs	Organizations often will need to purchase third-party support as the vendor no longer offers technical support. This support is typically more expensive, and if an outage were to occur there may be added cost to additional downtime as the technical support is limited.
Lack of Technical Support	After end-of-support date vendors often withdraw bug reporting, and no longer offer phone or internet support for inquiries. The remote assistance and escalation processes as well as community support for troubleshooting are typically lacking.
Poor Performance	Older technology typically lacks speed and performance, especially when comparing to the leading-edge product.
Regulatory Noncompliance	Continuing to use EOL software may expose an organization to regulatory noncompliance with regulations and standards like General Data Protection Regulation (GDPR), Payment Card Industry Data Security Standard (PCI DSS), Sarbanes–Oxley Act (SOX) and may result in hefty fines.

End-of-Life Software

EOL Options and Planning Strategies

Botsford
ASSOCIATES

Options Available to Organizations Facing End-of-Life Technology

As the end-of-support (EOS) date nears organizations need to develop an end-of-life plan. After the EOS date the software will still work but it will be more vulnerable to security risks as patches are unavailable for any vulnerabilities. Organizations will ultimately need to decide whether to keep using the EOS software past EOS date, upgrade it to a new version, or to find alternative solutions in-house or externally.

Option 1: Keep Using EOS Software

After the EOS date passes and the software still works, organizations may choose to keep using the EOS software in the interim with risk mitigation such as purchasing third-party support. However, as the software gets further away from the EOS date it will be more vulnerable to security risks.

Option 2: Update Software to Latest Version

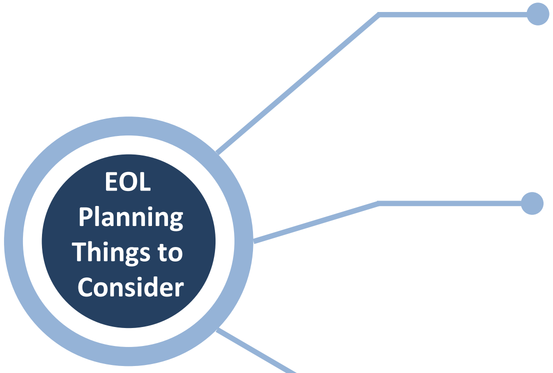
Often the easiest and most effective solution is to update to the latest version of the software as it will allow the organization to take advantage of the most cutting-edge functionality, speed, and security without the cost, complexity, and risk of trying to rebuild or switch to a different platform.

Option 3: Rebuild or Switch to New Platform

Migrating to a different platform may provide new opportunities such as new features and functionalities that were not available on the prior platform, or may operate on a more powerful technical stack. However there is often trade-off this option of added time, cost, and training.

End-of-Life Planning: Things to Consider to Mitigate the Risks with End-of-Life Technology

The best way to mitigate the risk associated with end of life technology is to be proactive, and stay aware of technology changes before they become out of date. This will provide time to research new technologies or versions available, and to develop and execute on end-of-life transition plans



EOL Planning Things to Consider

Track the end-of-life status for all software used in the company

Organizations should have an inventory of all software being used to identify, catalog, and track all software that is installed and in-use. Within this inventory there shall be tracking of the end-of-support dates to allow the organization time to plan and transition to newer products.

Conduct a Risk Assessment to Evaluate Risks with EOL Software

When assessing EOL options available, the existing software shall be evaluated to determine criticality to business operations, likelihood of vulnerabilities and their potential impacts. The outcome of this assessment may indicate whether replacement or update is necessary, or if compensating controls can be established such as security monitoring and incident response plans.

Keep Existing Software Updated During Upgrade or Migration

While planning the transition to newer products, organizations shall not forget about staying up-to-date on the latest software patches and updates, and stay informed about any vulnerabilities. Critical updates must be prioritized to address critical bugs or vulnerabilities.

End-of-Life Software

Best Practices for Dealing with EOL Software

Strategies to Minimize Risks When Operating End-of-Life Software

Look For Alternative Support Options

If third-party support is available, this may be a good way to extend the useful life of end-of-life (EOL) software. Third-party vendors may offer services such as security updates, bug fixes, and technical support. This is more often available for popular software and software where you have access to the source code.

Network Segmentation

Isolating EOL software restricts access and limits the number of entry or exit points to protect from vulnerabilities. Organizations should consider sandboxing or virtualization to keep the systems secure. Also EOL applications are often kept online to access historical records, which it should be assessed if the records can be exported and system shut down.

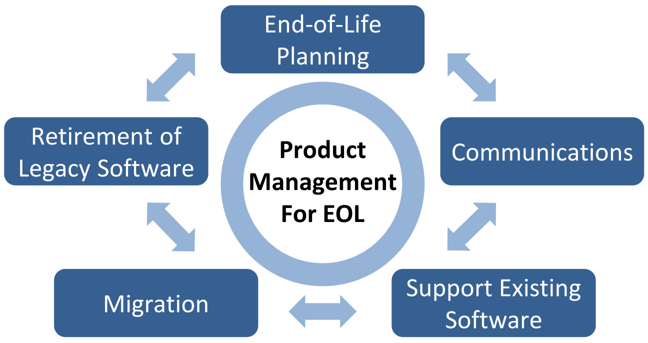
Regular Security Assessments

Performing regular security assessments, including vulnerability scanning and thread-led penetration testing should help identify risks or vulnerabilities to the infrastructure. In addition, incident response testing can help prepare organizations for potential outages and attacks.

Limit Technical Debt

Continuing to use software past its EOL date can increase the chance of system issues and outages. So keeping the code base as efficient as possible is important to limit the likelihood of issues arising. Development teams shall focus on the most critical codebase areas, and look to structure the code into smaller, more manageable pieces.

Important Processes to Follow When Migrating to a New Technology Solution



Product Management For EOL

End-of-Life Planning

Communications

Support Existing Software

Migration

Retirement of Legacy Software

When organizations decide to migrate to a new technology solution they will need to follow key change management processes:

Planning involves identifying and assessing the best options available to phase out or discontinue a legacy product.

Communication is required to inform end users, and other technology leaders that have integrated with the legacy product and may be impacted by a product approaching end-of-life.

Supporting Existing Software involves ongoing support and maintenance for the product during the transition period and may include software updates and bug fixes to the existing software that is being phased-out. Organizations cannot afford to forget continued maintenance while planning to migrate to the new solution.

Migration involves all activities related to the transition to the new or upgraded product such as training, documentation, testing, and other activities.

Retirement includes decommissioning the product, removing access and taking it off the network

End-of-Life Software

Botsford Team Contacts

For additional information about this Regulatory brief or Botsford Associates Financial Services Regulatory Practice, and how we can help you, please contact:

Jon Block
Managing Partner
Financial Services
NYC: 917.647.3434 / TOR: 416.915.0438
jblock@botsford.com

Andrew Moreira
Managing Director - Consulting
Financial Services
NYC: 917.722.0939 / TOR: 647.361.4404
amoreira@botsford.com

Gordon Wong
Managing Director - Advisory
Financial Services
NYC: 917.722.1200 ext 319 / TOR: 437.253.4933
gwong@botsford.com