// Whitepaper – EOL & EOS

Strategic End-of-Life & End-of-Support Management

Author: Lawrence Dempsey

Executive Summary

When support expires for hardware or software assets or when these assets reach their End-of-Life, your critical business infrastructure could be left exposed to critical security risks, compatibility issues, and reduced functionality. Your services and processes could be hampered, your business paralyzed.

But with the right solutions and services, strategic End-of-Life & End-of-Support management can give you the visibility you need to protect and even improve your IT infrastructure. In this white paper, we will show you the ins and outs of strategic End-of-Life & End-of-Support management, discuss the risks involved in not doing it, and show you how your business can benefit and grow by gaining IT lifecycle and support visibility.

Table of Contents

Introduction

End-of-Life and End-of-Support are two different things that can lead to similar and overlapping problems. End-of-Life is when the product reaches the end of its sales cycle.
The product has been retired from the OEM's product line and is no longer available through their direct sales. While the product may still be available through resellers or partners, the OEM is no longer focusing on developing that product and has a planned End-of-Support date in sight.

Because of various national regulations, End-of-Life and End-of-Support are not the same. Very often, OEMs are legally required to offer support for a certain period after the product's End-of-Life, usually between 6 and 12 years depending on the kind of product. In this time, the OEM will generally cease offering new feature updates, and instead provide the bare minimum of support to keep the product running and to protect it from new threats and newly discovered vulnerabilities.

What happens when support runs out?

End-of-Support means that the product is no longer supported at all. No new maintenance updates, no security updates, no support whatsoever. You have a few options available to you when your hardware or software asset reaches its End-of-Support:

1) **Negotiate extended support** – If it's available, you might be able to pay extra for technical and security support beyond the product's lifecycle. Keep in mind though that even where this is an option, at some point support will end for good.
2) **Upgrade or find a new solution** – There may be another, newer, and fully-supported product on the market that fills the same need or at least most of the same need.
3) **Go it alone** – There may be reasons for keeping around legacy assets, but if you decide to hold on to them, it will be up to you and your IT security team to track, monitor, and eliminate vulnerabilities and to support the asset when it runs into problems.

What are the risks of not doing End-of-Life & End-of-Support management?

No matter what you decide to do, you need to have the information and the visibility into your environment to make those decisions. There are significant risks to not gaining visibility into your End-of-Life & End-of-Support status.

At first glance, it may appear that End-of-Life for an IT product doesn't necessarily imply any risks. The OEM has simply decided to stop producing the product and to remove it from their portfolio. Sales may continue through partners and resellers, but the OEM no longer takes any responsibility for manufacturing the product and producing new features. But while end of development isn't a risk per se, if you have grown accustomed to new features and rely on those regular feature and performance enhancements as part of your own development or service roadmap, then you may find yourself having to adjust your business goals because of a discontinued product. Enterprises work with and rely on the innovations and enhancements from their software and hardware vendors in planning and forecasting business maintenance and growth. When products reach their End-of-Life, enterprises that rely on them might face serious challenges in meeting their own growth goals. If anything, an End-of-Life announcement should be used as a start signal: now's the time to make some strategic decisions about your infrastructure and the place this product has in it.

End-of-Support, on the other hand, brings with it some clear and present dangers. If you haven't planned and prepared for the End-of-Support, here are some of the risks you'll face immediately.

1) **Security gaps** – Support provides regular and continuous risk and vulnerability monitoring as well as warning and patches whenever a new vulnerability is detected. Instead of having to do the work of monitoring and discovering vulnerabilities as well as then finding solutions for them, the OEM's support offering is your first line of defense in protecting your IT infrastructure. After all, who better to do threat and risk assessment and mitigation than the software vendor?

2) **Compatibility issues** – Compatibility issues emerge regularly whenever the product or some underlying system is updated. Fixing these compatibility issues is a standard and routine part of any support offering. The moment support has expired, your software and hardware will be subject to compatibility issues that could cause severe interruptions to your business processes.

3) **Reduced performance** – If your IT assets aren't kept up to date through regular support, their performance will degrade over time, making your business less agile and less dependable.

4) **Service interruptions** – Out-of-support assets break down more easily and more frequently, disrupting critical business services.

5) **Higher costs** – In order to mitigate some of the problems mentioned above, you may have to divert your own financial resources and development capabilities to maintain and support discontinued products. This increases your costs and puts a strain on resources you'd rather use to grow your business.

6) **Regulatory issues** – Many industries are governed by strict data protection and privacy regulations that restrict and forbid the use of out of support IT assets. Not adhering to these regulations can result in financial penalties, problems with accreditation and insurance, as well as restrictions to your right to operate.

The benefits of End-of-Life & End-of-Support management

You can see from the list above that the risks of not doing End-of-Life & End-of-Support management are significant. And yes, you should do what you can to mitigate these risks as they can have significant, even catastrophic consequences for your business. But there's more to life and IT management than risk avoidance, and the same is true of End-of-Life & End-of-Support management. We do it because it also provides significant benefits for an organization. Here are just some of the reasons why you should actively manage End-of-Life & End-of-Support for your hardware and software assets.

Proactive risk mitigation – There's putting out fires, and then there's making sure they don't happen in the first place. A truly effective risk mitigation strategy is one that anticipates risks and does what it can to prevent them. End-of-Life & End-of-Support management ensures that you're always on the lookout for potential risks and stopping them before they happen, saving you time, resources, and money, and guaranteeing business continuity and reliability.

Cost controls – By knowing and understanding what changes are coming up and whether you need to migrate to new computing resources, you can better plan your costs and keep them from detonating your budget.

Strategic IT asset procurement – While this is also a cost control measure, monitoring End-of-Life & End-of-Support status will help you decide not just whether to purchase new computing resources but also how. Your IT environment is in a constant state of change. Whether it's because your business is expanding and taking on new challenges, legacy software and hardware no longer provide the functionalities you need, you find more cost-effective options for your environment, or some combination of the above, your business is regularly able to take advantage of new options. If you know, for instance, that support will expire for an important business IT asset, and that there you can combine those indispensable functionalities with other more powerful and cost-effective suites, then you can make better purchasing decisions. But without that insight, you risk making unnecessary purchases, squandering time, and resources until you're able to migrate to new solutions.

Deeper IT visibility – Gaining a complete and reliable overview of your environment is an absolute requirement for managing your IT. By adding End-of-Life & End-of-Support data to your arsenal of information, you can better equip IT teams to manage change, mitigate risk, reduce response times, plan resources, and make better, more strategic decisions.

Protected processes – Your value streams depend on reliable, uninterrupted IT services and processes. When support expires, those services and processes are left vulnerable to system failures, compatibility issues, viruses, and cyberattacks.

Ensured reliability – The worst thing that could happen to your brand and your reputation is the perception that your services are unreliable. Service interruptions will send your customers packing, headed for greener, more stable pastures. By managing End-of-Support, you can make sure that your services aren't subject to sudden and unpredictable slowdowns and stoppages by keeping them patched, updated, and protected from attacks, viruses, and compatibility issues.

Strategic End-of-Life & End-of-Support management

Ideally, you should start planning how what to do with a product when an OEM announces End-of-Life. But with so many products in your infrastructure, it can be hard to nearly impossible, to get complete IT visibility without the right solutions and services. Knowing what you have and keeping an accurate record of End-of-Life & End-of-Support is a crucial first step, but it's not the whole strategy. To get from knowledge to strategy, we recommend the following steps:

1) **Find out what's ending** – Keep track of the End-of-Life & End-of-Support status of your assets. You can do this yourself by keeping record of notices that come in from the various vendors, or you can take advantage of a technology catalog that is regularly updated by a team of experts.

2) **Determine whether extended support is available** – Your vendors may reach out to you with an offer for extended support, or you can reach out to them to see if such an arrangement is possible.

3) **Do a risk/benefit assessment** – What are the risks and benefits of keeping the asset as opposed to finding something new when support runs out? Can your team effectively keep the asset running and secure when the OEM ends support? Is the product easily replaceable within your portfolio, or will migrating it cause significant problems and delays? How will migrating/not migrating the product impact your business in the near and long term?

4) **Decide whether to update the asset** – In reviewing your End-of-Support & End-of-Life status, you may discover that you no longer need the asset, or that some other product provides even more value than the expiring product. In that case, you may decide to switch altogether, a process that will require you to understand the dependencies in your environment to ensure an uninterrupted service flow.

5) **Plan for migration to avoid conflicts** – If you do decide to update the asset, this will affect all the underlying dependencies. Make sure to check the dependencies to avoid or mitigate any conflicts before you migrate, so that you can ensure the reliability and continuity of your business services.

6) **Work with security to manage vulnerabilities** – Even if you do decide to migrate to a new product, there may be a period between End-of-Support and when the new product and services are fully integrated into your environment. No matter the decision, work with your cybersecurity team to ensure that your infrastructure is protected from vulnerabilities, data leaks, and attacks.

The expanding importance of a Technology Catalog

A technology catalog is a central database of hardware and software asset information. In most instances, it is run and maintained by third-party providers who do the work of gathering and normalizing asset and market data to provide organizations with a foundation for their IT management activities. From Hardware and Software Asset Management to End-of-Life & End-of-Support management, the technology catalog is the cornerstone for truth and reliability. With it, you can compare, clean, normalize, and enrich data gathered from your own infrastructure to gain value-driven insights into your environment.

Because End-of-Life and End-of-Support data are market and not technology data, they aren't discoverable by traditional means. Press releases, website updates, emails, and updated service terms and conditions will be how an OEM communicates an expiring product or support contract, and this data will, in most instances, need to be manually gathered, entered, and maintained.

According to Gartner, "Gathering and updating End-of-Life data is challenging due to large infrastructure estates and variation in how providers publish this information for hardware and software." They list Raynet's RayVentory Catalog as one of the technology catalogs that "provide vetted End-of-Life data and other product details that can be accessed directly or integrated into other tools used for management activities" along with Flexera's Technopedia and Eracent's IT-pedia. A third-party technology catalog, such as the next generation AI powered catalog that's part of the Raynet Unified Data Platform, can provide you with that and much more data, giving you a trustworthy tool for data enrichment and normalization and providing you a complete overview of your End-of-Life & End-of-Support status.

Conclusion

Not managing your End-of-Life & End-of-Support is taking a calculated but unadvised risk. The barriers to management are low and the benefits are substantial and many.

Protect your IT investment and ensure the reliability and stability of your business with strategic End-of-Life & End-of-Support management.

About the author

Lawrence Dempsey
As Vice President of Solutions at Raynet, Inc., Lawrence is committed to helping clients achieve complete IT visibility, so they can identify savings, lower risks, and realize important business initiatives.

Lawrence offers more than a decade of experience in software procurement, software management, and software reselling. Lawrence's expertise ranges from license eligibility and software deployment reconciliation to contract interpretation and SAM and ITAM process optimization.

[1] "How to Improve Infrastructure Fitness and Sustainably Reduce a Technical Debt". Gartner. Roger Williams, Daniel Stang, and Mark Margevicius. 11 January 2022. ID: G00756218.

Why Raynet

As a global software vendor with market-leading solutions and complementary managed services, we make successful end-to-end management of IT projects and operations possible.

Following the mission **Discover to Manage**, our vision is that all companies worldwide achieve transparency and security as well as optimization of their IT investments by using our technologies..

Get in touch

For more information, call our sales team at **+1 (224) 532-2811** or write to **sales@raynet-inc.com**.