Asset Armageddon Survival Guide

Devices past the Last Date of Support (LDoS) can cripple your network. Are you prepared or blind to the threat?

orange™

Business Services

The hidden threat

A time bomb is lurking in your infrastructure, ticking away, waiting for the most inopportune moment to explode. Everything seems to be running smoothly, but hundreds of devices may not be supported. If one fails, what was smooth seconds ago becomes chaos.

Large enterprises depend on their technology infrastructures, complex networks containing hundreds or even thousands of devices. Every device has a latent risk: someday its manufacturer will no longer support it. For many devices, that critical date may be drawing near.

What does this mean in practice? Extended outages, unbudgeted expenses, security vulnerabilities, angry tweets, the call you don't want to get from your boss. Or worse, finding your company's name 'above the fold' in USA Today because of a hack. In short, Asset Armageddon.

No time for complacency and 'I don't know' is definitely NOT the right answer to the question, "How many devices are near or past their Last Date of Support (LDoS)?"

This whitepaper provides a step-by-step survival guide for companies currently facing this challenge, even if they are unaware of the threat. It explains in detail how products get to LDoS and how you can avoid Asset Armageddon before it becomes reality.

> **'I don't know' is definitely NOT the right answer to the question, "How many devices are near or past their LDoS date?"**

Myth busting – know the risks behind unsupported devices

Assets past LDoS is no big deal, right? After all electronic devices don’t break much. Read the list and ask yourself, ‘Do I feel safe with my current LDoS plan?’

Security

Security is the number one problem for unsupported devices. It exposes companies to imminent financial and intellectual property losses, and reputational damage. A product past its last day of support can easily land an organization in the headlines, making it the next Target or Home Depot.

The software and firmware on obsolete products cannot be updated. This makes it easier for attackers to exploit new vulnerabilities found in older systems, leading to some grievous security holes. In one case, an Orange client was using almost 850 devices that were so old they were unable to close off the Telnet port (a common ingress point for attackers).

The IT department was effectively operating with hundreds of open doors in its network that it had no way of closing, because the devices were unsupported, meaning that their code could not be updated.

Compliance

If devices aren’t supported, then it may affect your compliance position. The PCI-DSS Standard specifically advises companies to review their hardware and software technologies annually to ensure that they are supported[1].

Reliability

Unsupported equipment with non-standard configurations that cannot be upgraded make infrastructures unstable, increase error rates and prolong outage periods. This makes it more difficult and time-intensive to track down and fix operational problems.

Eventually, even solid state devices begin to degrade in performance or fail altogether. This hardware may support critical functions and cause cascading failures when it stops working, leading to service disruptions that affect infrastructure services and business applications.

Failed equipment can lose a company its customers, and regaining that business is a long and costly process.

Continuity

If you are unaware that a device is no longer supported, then when it fails you may find yourself struggling to find a replacement, or tracking down a third party who can support the equipment. You may be unable to substitute another model without first evaluating it against your standards, or rashly appointing a service contractor without the necessary procurement processes. That all takes time, which could disrupt your services.

Cost

Companies caught unprepared with unsupported devices face unbudgeted expenses, higher support costs, longer outages, expedite charges and exorbitant time and materials rates. Beyond hard dollars, there’s lost productivity and the potential for worse – lost revenue and reputation.

[1] https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2.pdf

Infrastructures out of control

In today's time-starved, budget-compressed world, the tidy infrastructures of the past easily go haywire.

Planning for a device's obsolescence is more challenging than it seems, especially with acquisitions, divestitures, and hybrid platforms. In one LDoS Assessment we found that one of the world's largest consumer products companies had purchased more than 10,000 pieces of Cisco equipment from over 250 suppliers with 350 separate maintenance contracts. Sixteen percent (16%) of their equipment becomes obsolete in early 2017. Ten years earlier, it was a 'tidy network' – today, borderline unmanageable. In another example Orange found approximately $50 million of LDoS equipment in a global infrastructure assessment for a financial services company client.

Some organizations disable competent support resources with complex technical and organizational structures. In some cases, the people responsible for managing the assets aren't involved in all stages of the lifecycle, leading to gaps in their knowledge. For example, a global petroleum exploration company recently asked Orange Business Services to quote a price for renewing support on 850 devices in its network. They asked Orange not to include maintenance contracts for their access points, explaining that they did not buy support for access points. When Orange audited their network, we found that 250 of their access points had five-years of prepaid maintenance contracts. The manager asking for the quote was responsible for the assets, but had not purchased them, and was completely unaware that the maintenance contracts existed.

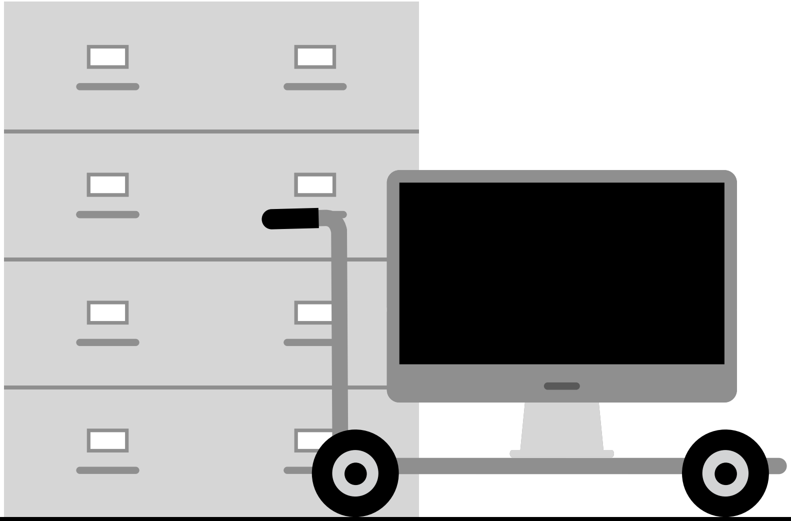
No wonder such disparities occur. The array of devices in today's enterprise infrastructure are often sourced by different teams, and typically from different suppliers, through various channel partners. They are managed by different departments in multiple business units and subsidiaries.

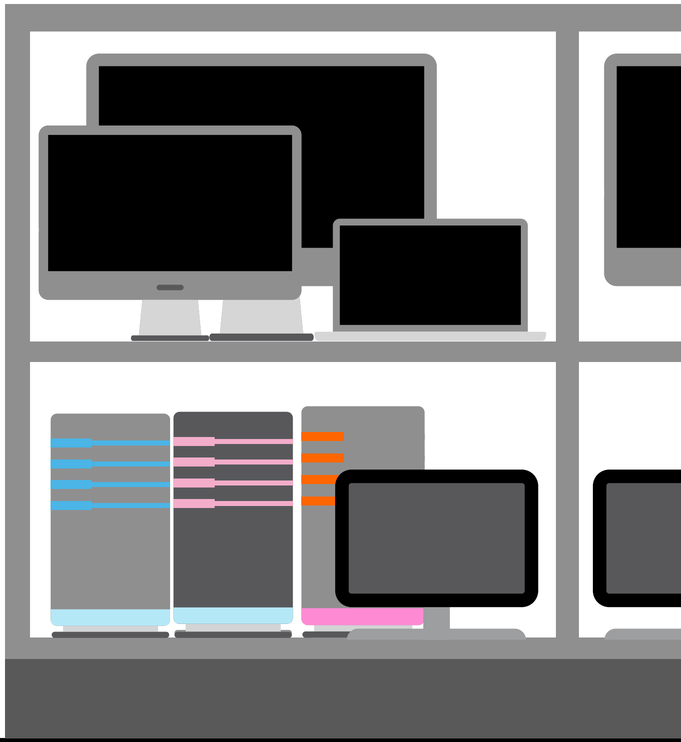
Unless companies take the time and effort to uncover their LDoS exposure, they face the security, compliance, reliability, continuity and cost risks listed in the prior section. Prevention starts with understanding the LDoS cycle which we cover next.

The road to obsolescence

Planning for LDoS may seem daunting, but it need not be difficult if you follow a defined plan. Products progress through several steps before they reach their official last day of support.

1. **The end of life date is announced.** Vendors typically announce the end of life date years before it occurs, allowing the product to move through several stages along the road to obsolescence. These typically include:
2. **The last date of sale.** The product is no longer sold.
3. **The last ship date.** This is typically a few months after the last date of sale.
4. **The end of software maintenance.** Bug fixes and software patches cease.
5. **The end of routine failure analyses.** The vendor no longer determines the cause of product hardware failures.
6. **The last new service contract.** This represents the last opportunity to order a new service and support contact for the device.
7. **The final service contract renewal.** Existing service contracts cannot be renewed from this point forward.
8. **The last date of support:** The product is officially obsolete.





The road to obsolescence

Below is a sample schedule for the Cisco ISR2800 router. While other vendors may use different language, the process is usually similar across OEMs.

Milestone	Definition	Date
End-of-Life Announcement	The date the document that announces the end of sale and end of life of product is distributed to the general public.	Nov 1, 2010
End-of-Sale Date	The last date to order the product through Cisco point-of-sale mechanisms. The product is no longer for sale after this date.	Nov 1, 2011
Last Ship Date: HW	The last-possible ship date that can be requested of Cisco and/or its contract manufacturers. Actual ship date is dependent on lead time.	Jan 30, 2012
End of SW Maintenance Releases Date: HW	The last date that Cisco Engineering may release any final software maintenance releases or bug fixes. After this date, Cisco Engineering will no longer develop, repair, maintain, or test the product software.	Oct 31, 2014
End of Routine Failure Analysis Date: HW	The last-possible date a routine failure analysis may be performed to determine the cause of hardware product failure or defect.	Oct 31, 2012
End of New Service Attachment Date: HW	For equipment and software that is not covered by a service-and-support contract, this is the last date to order a new service-and-support contract or add the equipment and/or software to an existing service-and -support contract.	Oct 31, 2012
End of Service Contract Renewal Date: HW	The last date to extend or renew a service contract for the product.	Jan 30, 2016
Last Date of Support: HW	The last date to receive service and support for the product. After this date, all support services for the product are unavailable, and the product becomes obsolete.	Oct 31, 2016

LDoS playbook: gather the data

You have two choices: the ‘Ostrich approach’, hoping the issue goes away or the ‘Proactive approach’, tackling the issue head on. (Head on is easier than you think.)

Getting your arms around LDoS in your environment is easy to understand, but tedious to actually accomplish. In this section we outline the key elements in the plan from discovery through decision along with insights for on-going operation post LDoS.

Get the necessary data

To start, you need to quantify the LDoS exposure in your environment. Do you have tens, hundreds or (hopefully not) thousands of devices past or near their LDoS dates? The process starts with data. Beyond LDoS, you should also understand every device’s maintenance status. Here are the data collection steps:

- **Get a contract download**
  Existing support contracts and purchase records are good sources to help build a picture of your existing asset/coverage base. Ideally, you will get these details from your own central purchasing department, but this may not be reliable because equipment is often purchased outside of the main procurement function. Also, purchasing departments typically don’t maintain support contracts so moves and decommissioning aren’t captured beyond the initial purchase/renewal.

  As an alternative, you can approach your manufacturer/maintenance provider directly. Many, like Cisco, maintain a database of all equipment purchased by a customer. If manufacturers don’t support this process, or if you’re dealing with many different suppliers, then another option is to use a third party assessment service, which will typically blend on-site and remote asset identification techniques.

- **Find what’s not installed**
  Compare the list from the contract download step with your online install base. This requires an up-to-date asset database. If you don’t have an accurate asset database, you should consider an infrastructure assessment which compares purchase and maintenance records to what is actually online in your network. You may find yourself having to conduct a second sweep for equipment not on the contract list, during which you will find those contracts and reconcile them. Obsolete and uncovered equipment becomes an immediate priority.

- **Organize the data**
  After reconciling the list, clear it of any irrelevant data. This means eliminating everything that doesn’t have an impending LDoS. You can then use this subset of data to create a pivot table listing equipment by supplier and by LDoS, enabling you to prioritize your devices.

LDoS playbook: evaluate your options

Evaluate your network and your options

At this point, your assessment team has a prioritized list of devices to work through. They can choose from several options when preparing each device for its LDoS.

- **Categorize your response by device class**

  All devices are not the same in relationship to business and operational criticality, users effected, security or compliance risk. A data center switch effects more users and carries far more security risk than an IP phone. Categorize effected equipment and build your plan for LDoS according to:

  - business and operational criticality
  - numbers of users effected by a potential failure
  - compliance risk
  - security exposure

  Unless a device is ranked "low" according to these criteria, then planning for replacements is the priority. Devices ranked "low" fall to the bottom of the priority list and can be considered for running past LDoS or taking advantage of manufacturer's "replace on failure" programs.

  Avoiding Asset Armageddon means having a plan for every device for LDoS and maintenance coverage – including these options:

- **Self-manage**

  Maintaining the device in-house requires a sufficiently skilled support team that can meet internal service level agreements. This requires a degree of process maturity in the in-house team, and could involve some inventory overhead (spares), which will increase cost and have an effect on the balance sheet.

- **Third party support**

  If you are unable or unwilling to manage your own obsolete assets, then you can turn to third-party maintenance services. This requires managing external SLAs and will also require a service provider with an adequate sparing policy. Internal teams must devote resources to managing these relationships.

- **Prepare to replace the asset**

  "Replace on failure", self-manage and third party support solutions are temporary measures. If you adopt this approach, then you should budget for a planned upgrade at a later date. In many cases, the asset may need replacing before the LDoS because it is critical to operations and the risk of failure is simply too great.

  In these instances, budget for the hardware refresh and begin the procurement process early so that the hardware can be swapped without disruption to normal business operations. Be sure to consider the implications on the rest of your infrastructure while planning this process.

- **Eliminate/consolidate the asset**

  There may be some assets that simply aren't necessary anymore or could be consolidated. Perhaps they support an infrastructure area that is destined for an IaaS solution in the cloud. These assets present opportunities for elimination and cost savings.

LDoS playbook: further steps

Further steps

Avoiding asset armegeddon isn't the only benefit to come from your LDoS assessment. After evaluating and choosing the right options for devices approaching LDoS, you can use the data you've accrued as a valuable tool for refining your supplier relationships and contracts, especially around maintenance. Here are some further steps to take:

- **Consolidate maintenance contracts**

  The data gathering process will have created a list of products and supplier maintenance contracts. Examining those contracts may present opportunities to rationalize some of them and save valuable dollars that can be used elsewhere.

- **Consolidate suppliers**

  Some suppliers may be surplus to requirements if appropriate equipment can be sourced from other suppliers and supported more effectively or for lower fees. Concentrating your procurement power on a smaller number of suppliers may also generate savings in capital expenditure by giving you more leverage for volume discounts. The LDoS data already compiled will enable you to identify these opportunities and revise your procurement program accordingly.

- **Refresh your own asset database**

  A comprehensive asset database is a linchpin in any well-run IT department, forming a foundation for effective change management. Use the data gathered during the LDoS assessment to refresh your own asset database, updating the support status of each serial number currently in use within your infrastructure. This can then be fed into the configuration management database and used to help plan for change management in the future.

- **Clean up your maintenance supplier's database**

  Manufacturers and maintenance providers keep centralized records of products sold to their customers and will have a list of where they believe the equipment is installed. This can be incorrect, leading to service problems when support teams are working to tight SLA deadlines. This is your chance to refine your support procedures with the supplier, creating opportunities for better service in the future.

Surviving to thriving

A complete LDoS assessment propels your company beyond Asset Armageddon to maximizing your infrastructure around uptime, productivity and higher return on assets. Taken further, it provides a solid foundation for maintaining control of your infrastructure.

Planning

A complete LDoS assessment is a powerful tool. Knowing which products are nearing their end of life enables you to plan more effectively in three areas:

- **Finance**

  IT departments can earmark their replacement budget ahead of time rather than pushing themselves into a deficit with emergency purchases. This makes financial planning easier, which helps with governance.

- **Tech refresh prioritization**

  IT departments are constantly refreshing devices, whether or not they are nearing their last date of support. Sometimes, the refreshes are discretionary, based on the desire for more functionality or a changing vendor relationship. Product transitions based on impending obsolescence may take priority, but decision makers can only make those determinations if they have full visibility into their equipment LDoS status and related support contracts.

- **Change management**

  Knowing in advance which devices must be replaced or consolidated enables IT departments to schedule them ahead of time and align them with other changes. This can lead to smoother, less risky change management processes.

A platform for good governance

An LDoS assessment is something that you should do to protect your organization from burdensome and costly unplanned problems, but it also brings some additional benefits.

One of the biggest advantages of an LDoS assessment is the groundwork it lays for inventory and asset management. The assessment will naturally highlight IT assets in your infrastructure, including those that you didn't know existed. This gives you several key benefits:

- Full asset visibility helps you to use them more efficiently, putting greater workloads onto assets that can support them.
- Properly documenting IT assets enables you to populate a configuration management database (CMDB), which can in turn form the backbone for an IT service management strategy. This strategy can include the automation of repetitive administration tasks through IT workflows.
- Documenting asset configuration enables IT teams to weed out non-standard products and improve operational stability.
- Proper asset and inventory management can drive risk management and compliance programs, enabling administrators to document and verify that device configurations meet the appropriate standards.

Properly documenting your support contract portfolio enables you to refine your supplier list and your maintenance contracts, which in turn creates opportunities for cost savings. It also enables you to enhance your technical planning, making informed decisions about which infrastructure functions will move to the cloud, for example.

Look at this procedure as a foundational process for change management, budgeting and technology planning strategies. Consider working with a third party provider to help get you through this project, especially if this is your first time embarking on a LDoS analysis.

About us

Orange Business Services, the Orange entity for business, is both a telecommunications operator and IT services company dedicated to businesses in France and around the world. Our 20,000 employees support companies, local government bodies and public sector organizations in every aspect of their digital transformation. This means we're at hand to orchestrate, operate and optimize: mobile and collaborative workspaces; IT and cloud infrastructures; connectivity (fixed and mobile networks, private and hybrid systems); applications for Internet of Things, 360° customer experience and big data analytics – as well as cybersecurity, thanks to our expertise in the protection of information systems and critical infrastructures. More than 2 million businesses in France and 3,000 multinationals place their trust in us. See why at: **orange-business.com** or follow us on Twitter **@orangebusiness.**

Contact us at: **http://www.orange-business.com/en/any-request**

orange™ Business Services

October 2016