

EXECUTIVE PAPER · LEGACY SYSTEMS

End-of-Life Software Is an Unpriced Liability

Every operating system, database, runtime and network appliance has a published date after which its vendor stops fixing it. CFOs and CIOs should track those dates in one register and fund each retirement before it arrives.

AUTHOR

Chris Watkins

SERVICE

Legacy Systems

FOR

CFO, CIO, CEO · 12 min read

AT A GLANCE

The problem. Vendors publish end-of-support dates years in advance. After that date, newly found flaws stay open for good. Attackers know this: state and criminal groups have spent 2024 through 2026 building botnets from retired routers and breaking into retired VPN appliances that can never be patched. In 2026 the US government ordered its civilian agencies to rip out unsupported edge devices within 18 months.

Why it persists. The date sits in a vendor document nobody owns. Replacement competes with feature work and has no line in the budget, so the decision gets made late, under pressure, at the highest price. Paid extended support is bought as a reprieve and renewed until it runs out.

The recommendation. Keep one register of every operating system, database, runtime and appliance with its vendor end date, an owner, and a funded plan. Decide 18 to 24 months ahead whether each item will be retired, upgraded, or carried on paid extended support, and put that cost in the budget year it falls in. Report the register to the audit committee each quarter.

The Decision in Front of You

Windows 10 left support on October 14, 2025. After that date Microsoft stopped shipping security fixes to any business that had not paid for Extended Security Updates [1]. SQL Server 2016 followed on July 14, 2026 [2]. Red Hat Enterprise Linux 7 left standard maintenance on June 30, 2024 [3]. Each date was published years ahead.

The decision is whether those dates are managed as a financial obligation with a schedule, or discovered as a security finding after they pass. Every piece of software in the company will reach one. The cost of reaching it unprepared is set by the vendor's price list, the regulator's expectations, and whoever finds the next unpatched flaw.

This paper concerns lifecycle planning and budgeting. A separate paper in this series covers the operational work of patching software that is still supported.

What's Happening

Vendors publish the dates, and the extensions cost more each year

Software vendors follow fixed lifecycle policies. Microsoft's Windows 10 page states that after October 14, 2025 it no longer provides technical support, feature updates, or quality updates, including security fixes [1]. Businesses can buy Extended Security Updates at $61 per device for the first year, and the

price doubles each year for a maximum of three years [1]. The program is cumulative: an organization that joins in year two pays for year one as well [1]. It covers critical and important security fixes only, with no new features and no general technical support [1].

Databases and operating systems work the same way. Microsoft's lifecycle page shows SQL Server 2016 extended support ending July 15, 2026, with three paid security-update years running to July 2029 [2]. Red Hat offers Extended Life Cycle Support for RHEL 7.9, limited to Important and Critical security fixes, through May 31, 2029 [3]. Runtimes move faster. The PHP project lists security support for PHP 8.2 ending December 31, 2026, and for 8.3 a year later [4].

Exhibit 1. End dates arrive on a calendar the vendor publishes years ahead

Product	End of standard support	Paid extension available	Extension ends
Windows 10 (22H2)	October 14, 2025 [1]	Yes, $61 per device in year one, doubling yearly [1]	Three years after end of support [1]
SQL Server 2016	July 14, 2026 [2]	Yes, Extended Security Updates [2]	July 2029 [2]
Red Hat Enterprise Linux 7.9	June 30, 2024 [3]	Yes, Extended Life Cycle Support [3]	May 31, 2029 [3]
PHP 8.2	December 31, 2026 (security fixes) [4]	No vendor extension from the project [4]	Not applicable
Pulse Connect Secure 9.1x VPN	December 31, 2024 [11]	None; vendor advises migration [11]	Not applicable

Source: vendor lifecycle documentation as cited.

A meaningful share of every estate is already past its date

runZero studied about 8 million assets across a few hundred US enterprises in 2025 and found 8.56% running an end-of-life operating system, with about 5% beyond even extended support [15]. It estimated that Windows 10's retirement would make roughly one third of enterprise Windows assets unsupported at once, tripling the share beyond support from about 5% to about 16% [15].

Open-source platforms show the same pattern. Perforce's 2025 State of Open Source report, produced with the Eclipse Foundation and the Open Source Initiative, found 40% of large enterprises still running CentOS Linux after its end of life [16]. Organizations running end-of-life platforms such as CentOS or AngularJS were nearly three times as likely to report a failed compliance audit as the 14% of all respondents who did [16].

Regulators and standards now name unsupported software directly

CISA lists "use of unsupported (or end-of-life) software" first in its catalog of Bad Practices, and says the risk is especially serious for technology reachable from the internet [5].

In February 2026 CISA went further. Binding Operational Directive 26-02 orders federal civilian agencies to inventory every end-of-support edge device within three months, remove those already past support within 12 months, remove all of them within 18 months, and within 24 months run a continuous process that retires such devices by their end dates [6]. CISA cited "widespread exploitation campaigns by advanced threat actors targeting EOS edge devices" and noted that lifecycle management is already required by OMB Circular A-130 [6]. CISA called the risk "disproportionate and unacceptable" and encouraged every network defender to follow the accompanying guidance [7]. The directive binds only federal agencies, but it sets the standard an auditor or insurer will reach for.

Payment card rules already require the register this paper recommends. PCI DSS v4.0 requirement 12.3.4, mandatory since March 31, 2025, requires a review at least every 12 months of the hardware and software in use [8]. The review must confirm vendors still ship security fixes promptly, document any announced "end of life" plans, and record a plan approved by senior management to remediate outdated technology [8].

Attackers go after what cannot be fixed

Volt Typhoon's router botnet, 2024. In January 2024 the Justice Department announced it had disrupted a botnet that a Chinese state-sponsored group used to hide its intrusions into US critical infrastructure. Most of the hijacked devices were small-office Cisco and NetGear routers that had reached end of life and no longer received security updates [10]. The routers' owners had done nothing beyond leaving retired equipment plugged in.

Criminal proxy networks, 2025. In May 2025 the FBI warned that criminals were infecting end-of-life routers with a variant of TheMoon malware and renting them out as proxies to hide fraud and cryptocurrency theft [9]. The malware needed no password; it scanned for open ports and sent commands to a vulnerable script [9]. The FBI's first recommendation was to replace the routers [9].

Pulse Connect Secure, 2025. Ivanti disclosed a critical remote code execution flaw, CVE-2025-22457, on April 3, 2025, after exploitation that began in mid-March [11]. Supported appliances had a fix from February. The older Pulse Connect Secure 9.1x line had reached end of support on December 31, 2024 and would never receive one [11]. Some of the compromised customers were running it, and Ivanti's advice to them was to migrate [11]. A Shadowserver scan days later found 5,113 vulnerable instances and said a large share were the unpatchable 9.x appliances [12].

SonicWall SMA 100, 2024 to 2025. Google's Threat Intelligence Group reported in July 2025 that a financially motivated group had been attacking end-of-life SonicWall SMA 100 remote access appliances since at least October 2024, including fully patched ones [13]. The attackers used stolen administrator

credentials to plant a rootkit that hid its own files and erased logs, and Google assessed the activity may support data theft, extortion and ransomware [13]. Google's hardening advice ended with one line: replace end-of-life SMA 100 appliances [13].

South Staffordshire Water, 2026. In May 2026 the UK Information Commissioner's Office fined the water company's parent £963,900 over a breach that began with a phishing email in September 2020 and went undetected for about 20 months [14]. Attackers took more than 4.1 terabytes of data affecting 633,887 people, including bank details and National Insurance numbers [14]. The ICO's findings listed unsupported software, including Windows Server 2003, alongside monitoring that covered 5% of the environment [14].

Why the Usual Approach Fails

Most companies learn about end of support from a scanner, an auditor, or an incident, after the decision has been made by default.

The date belongs to nobody. A server's end date sits in a vendor document. The application owner assumes infrastructure tracks it, infrastructure assumes procurement does, and procurement tracks contract renewals, which are different dates.

Retirement has no budget line. Replacing a database or an appliance is a project. It competes with revenue features and loses until the deadline makes it urgent.

Extended support is treated as a solution. Paid extensions buy time, and the vendor prices them to end. Windows 10 Extended Security Updates double each year and stop after three [1]. They cover security fixes only [1][3]. A company that buys the extension without funding the exit has moved the deadline and raised the price.

Appliances get forgotten. Firewalls, VPN concentrators and routers run vendor firmware that does not show up in desktop or server inventories. They sit on the internet edge, which is where CISA, the FBI and Google's investigators found attackers working [6][9][13].

The Framework: The Lifecycle Register

Run end of support the way finance runs debt maturities. Each item has a principal, a maturity date, and a plan to refinance or repay, reviewed on a fixed schedule.

The register holds one row per product version in use, across five categories: operating systems, databases, language runtimes and frameworks, network and security appliances, and commercial applications. Each row records the version, count of instances, internet exposure, business owner, vendor end date, any paid extension with its price and final date, the chosen path, and the budget year that pays for it.

Set the decision point by lead time. Internet-facing appliances and anything holding regulated data need a decision 24 months before the vendor date. Databases and server operating systems need 18 months, since migration testing is slow. Desktops and runtimes need 12. A row that reaches its decision point without a funded plan goes to the audit committee as an exception.

Choose one of four paths. Upgrade in place when the vendor offers a supported version and the application tolerates it. Replace when the product line is ending. Buy paid extended support only with a dated exit plan funded in the same budget. Isolate and accept, removing internet exposure and recording the risk with an executive signature, only when the first three are impossible and the system holds nothing regulated.

Price the late decision. The cheapest moment to act is before the date. Exhibit 2 shows how the bill grows when the decision slips.

Exhibit 2. Illustrative cost of deciding late on 400 Windows 10 devices

Scenario	Year one	Year two	Year three	Three-year total
Replaced before October 2025	$0 ESU	$0 ESU	$0 ESU	Replacement cost only
Enrolled in ESU from the start, then retired	$24,400	$48,800	$97,600	$170,800 plus replacement
Ignored, then enrolled in year two	$0	$73,200 (years one and two together)	$97,600	$170,800 plus replacement, with a year unpatched

Source: author's illustrative estimate using Microsoft's published commercial price of $61 per device for year one, doubling each year, and cumulative enrollment [1]. Year two is $122 and year three $244 per device. Excludes volume discounts, cloud-managed discounts and hardware. Replacement is required in every scenario; ESU only delays it.

Replacement happens in every row, so the extension only changes when it happens and how much is spent first. Waiting saves nothing either, because late enrollment charges for the missed year while the devices sat exposed.

Costs, Risks, and Tradeoffs

Exhibit 3. Tradeoffs of running a funded lifecycle register

Area	Cost or risk	Mitigation
Capital timing	Replacements land in budget years chosen by vendors	Plan 18 to 24 months ahead and smooth spend across years
Inventory effort	Building the first register takes weeks, and appliances and embedded runtimes hide from scanners	Start with internet-facing devices and regulated data stores; add categories quarterly
Forced upgrades	Some upgrades break applications or require licensing changes	Test early; budget a paid extension for the few systems that cannot move in time
Extended support	Annual price rises and security-only coverage [1][3]	Buy only with a dated, funded exit in the same approval
Accepted risk	Isolated legacy systems still fail audits and can still be reached internally	Require executive signature, remove internet exposure, review each quarter
When this is wrong	A small firm on SaaS with few owned servers or appliances has little to register	Track the handful of owned devices and rely on vendor contracts for the rest

Source: author's analysis.

Industrial and medical equipment is the hardest case. Some controllers and devices are certified on an old operating system and cannot change without recertification. For those, isolation, monitoring and a replacement schedule tied to the equipment's capital plan are the honest answer. CISA's directive itself excludes operational technology for this reason [6].

How to Act

Exhibit 4. A one-year roadmap

Window	Actions	Owner	Milestone
First 30 days	Inventory every internet-facing appliance and its firmware version. Check each against its vendor's end-of-support list.	Network or security lead	100% of edge devices listed with vendor end date
First 30 days	Name an owner for the register and one business owner per system.	CIO	Register owner named; owners assigned for every edge device
First 90 days	Extend the register to server operating systems, databases, runtimes and commercial applications. Record end dates, extension options and prices.	Infrastructure and application leads	Register covers all production systems; every row has a date and owner
First 90 days	Decide a path for everything already past support or reaching it within 24 months. Remove or replace any end-of-life edge device.	CIO with CFO	Zero end-of-life devices on the internet edge; every near-term row has a chosen path
First 365 days	Put retirements and extensions into the annual budget by year. Report the register to the audit committee quarterly. Align evidence with PCI DSS 12.3.4 where cards are in scope.	CFO with CIO and compliance	Budget lines for every retirement in the next two years; four quarterly reports delivered
First 365 days	Make end-of-support review part of every purchase: record the vendor's published support term before signing.	Procurement	Support term recorded on 100% of new technology contracts

Source: author's recommendation, informed by CISA BOD 26-02 milestones [6] and PCI DSS v4.0 requirement 12.3.4 [8].

Questions to Ask Your Team

1. Which of our internet-facing devices are past their vendor's end-of-support date today?
2. What reaches end of support in the next 24 months, and is each one in a budget?
3. Who owns the end date for each production database and operating system?
4. Where are we paying for extended support, what does it cost next year, and when does it stop?
5. If an auditor asked for our annual technology review and the remediation plan management approved, what would we hand over?
6. Which systems have we decided to isolate and accept, and who signed for that risk?
7. Does every new technology contract record the vendor's support term?

Closing

Unsupported software is a liability with a known maturity date and a rising carrying cost. The vendor publishes the date, the regulator expects you to have seen it, and attackers look for the equipment that missed it. Keep one register, decide each retirement 18 to 24 months ahead, fund it in the year it falls, and report the balance to the audit committee every quarter.

Sources

[1] Microsoft. "Extended Security Updates (ESU) program for Windows 10." Microsoft Learn. 2025. https://learn.microsoft.com/en-us/windows/whats-new/extended-security-updates.

[2] Microsoft. "SQL Server 2016: Microsoft Lifecycle." Microsoft Learn. 2025. https://learn.microsoft.com/en-us/lifecycle/products/sql-server-2016.

[3] Red Hat. "Announcing up to 4 years of Extended Life Cycle Support (ELS) for Red Hat Enterprise Linux 7." 2024. https://www.redhat.com/en/blog/announcing-4-years-extended-life-cycle-support-els-red-hat-enterprise-linux-7.

[4] The PHP Group. "Supported Versions." 2026. https://www.php.net/supported-versions.php.

[5] Cybersecurity and Infrastructure Security Agency. "Bad Practices." https://www.cisa.gov/stopransomware/bad-practices.

[6] Cybersecurity and Infrastructure Security Agency. "BOD 26-02: Mitigating Risk From End-of-Support Edge Devices." Binding Operational Directive 26-02. 2026. https://www.cisa.gov/news-events/directives/bod-26-02-mitigating-risk-end-support-edge-devices.

[7] BleepingComputer. "CISA orders federal agencies to replace end-of-life edge devices." 2026. https://www.bleepingcomputer.com/news/security/cisa-orders-federal-agencies-to-replace-end-of-life-edge-devices/.

[8] PCI Security Standards Council. "Payment Card Industry Data Security Standard: Self-Assessment Questionnaire D for Merchants." PCI DSS v4.0, Requirement 12.3.4. 2022. https://listings.pcisecuritystandards.org/documents/PCI-DSS-v4-0-SAQ-D-Merchant.pdf.

[9] Federal Bureau of Investigation. "Cyber Criminal Proxy Services Exploiting End of Life Routers." Public Service Announcement I-050725-PSA. 2025. https://www.ic3.gov/PSA/2025/PSA250507.

[10] U.S. Department of Justice, Southern District of Texas. "U.S. Government Disrupts Botnet People's Republic of China Used to Conceal Hacking of Critical Infrastructure." 2024. https://justice.gov/usao-sdtx/pr/us-government-disrupts-botnet-peoples-republic-china-used-conceal-hacking-critical.

[11] Ivanti. "Security Update: Pulse Connect Secure, Ivanti Connect Secure, Policy Secure and Neurons for ZTA Gateways." 2025. https://www.ivanti.com/blog/security-update-pulse-connect-secure-ivanti-connect-secure-policy-secure-and-neurons-for-zta-gateways.

[12] Cybersecurity Dive. "Over 5K Ivanti VPNs vulnerable to critical bug under attack." Citing Shadowserver Foundation scans. 2025. https://www.cybersecuritydive.com/news/5k-ivanti-vpns-vulnerable-critical-flaw-under-attack/744748/.

[13] Google Threat Intelligence Group. "Ongoing SonicWall Secure Mobile Access (SMA) Exploitation Campaign using the OVERSTEP Backdoor." 2025. https://cloud.google.com/blog/topics/threat-intelligence/sonicwall-secure-mobile-access-exploitation-overstep-backdoor.

[14] Help Net Security. "Poor security left hackers inside water company network for nearly two years." Coverage of the ICO penalty against South Staffordshire. 2026. https://www.helpnetsecurity.com/2026/05/11/ico-south-staffordshire-cyberattack-fine/.

[15] runZero. "Undead by Design: End-of-Life Report." 2025. https://www.runzero.com/resources/undead-by-design-report/.

[16] TFiR. "2025 State of Open Source Report: Skills Gaps and EOL Software Jeopardize Big Data Initiatives." Coverage of Perforce OpenLogic report with the Eclipse Foundation and Open Source Initiative. 2025. https://tfir.io/2025-state-of-open-source-report-skills-gaps-and-eol-software-jeopardize-big-data-initiatives/.

The views in this paper are the author's own and do not represent any employer. Scenarios are hypothetical. This paper is not legal, financial, or compliance advice.