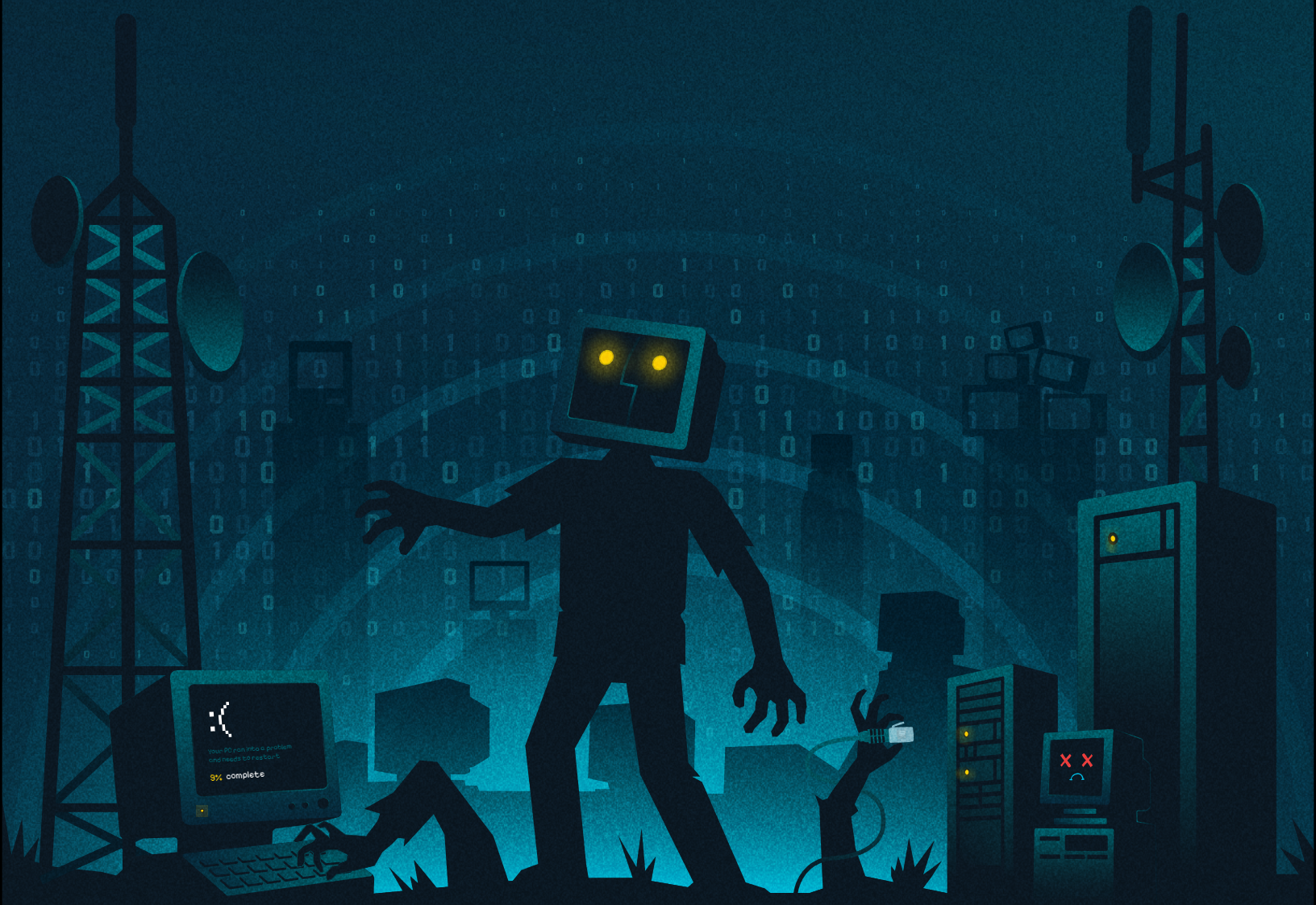
runZero

UNDEAD BY DESIGN

Benchmarking end-of-life operating systems



Executive summary

End-of-life (EOL) operating systems remain an underestimated risk for enterprise networks. This study analyzes millions of assets across hundreds of U.S.-based enterprises to quantify how prevalent unsupported OSes are today, how different industries fare, and what lies ahead as major platforms enter the Sunless Lands.

Across all enterprises studied, **8.56% of assets are running an EOL OS**, with **5% of all observed assets already beyond security support** unable to receive timely, critical patches. These "undead" systems are disproportionately visible to threat actors, provide unique opportunities for routine exploitation, and often indicate broader gaps in maintenance and IT hygiene.

Industry-level analysis highlights that certain sectors consistently struggle with EOL exposure. General retail, machinery and electronics manufacturing, professional services, and chemical/biotech industries carry above-average concentrations of unpatchable systems, raising systemic supply chain risk and public health concerns. Healthcare and social services, in particular, face elevated risks involving patient safety due to the critical nature of medical industry applications that require legacy OSes.

The stakes are about to rise sharply as **Windows 10 reaches end of life on October 14, 2025**. After this date, roughly one-third of Windows assets in enterprise networks will become unsupported almost overnight. Our data suggest that this "Winpocolyse" event will effectively triple the enterprise-wide EOL population, with healthcare and social services most exposed.

Urgent action is required to tackle this situation. OS vendors must guide application developers and end-users through upgrade lifecycles, ensuring post-upgrade compatibility and secure-by-design practices. IT and security teams must advocate for budget and resources, pressure vendors for updated applications capable of running on modern OSes, and prioritize decommissioning unsupported OSes. Security researchers should shine a light on these vulnerable machine populations, raising awareness before threat actors exploit them.

Undead OSes are already on your network, and it's likely to get worse, very soon. Proactive management today is the best defense against tomorrow's breaches.

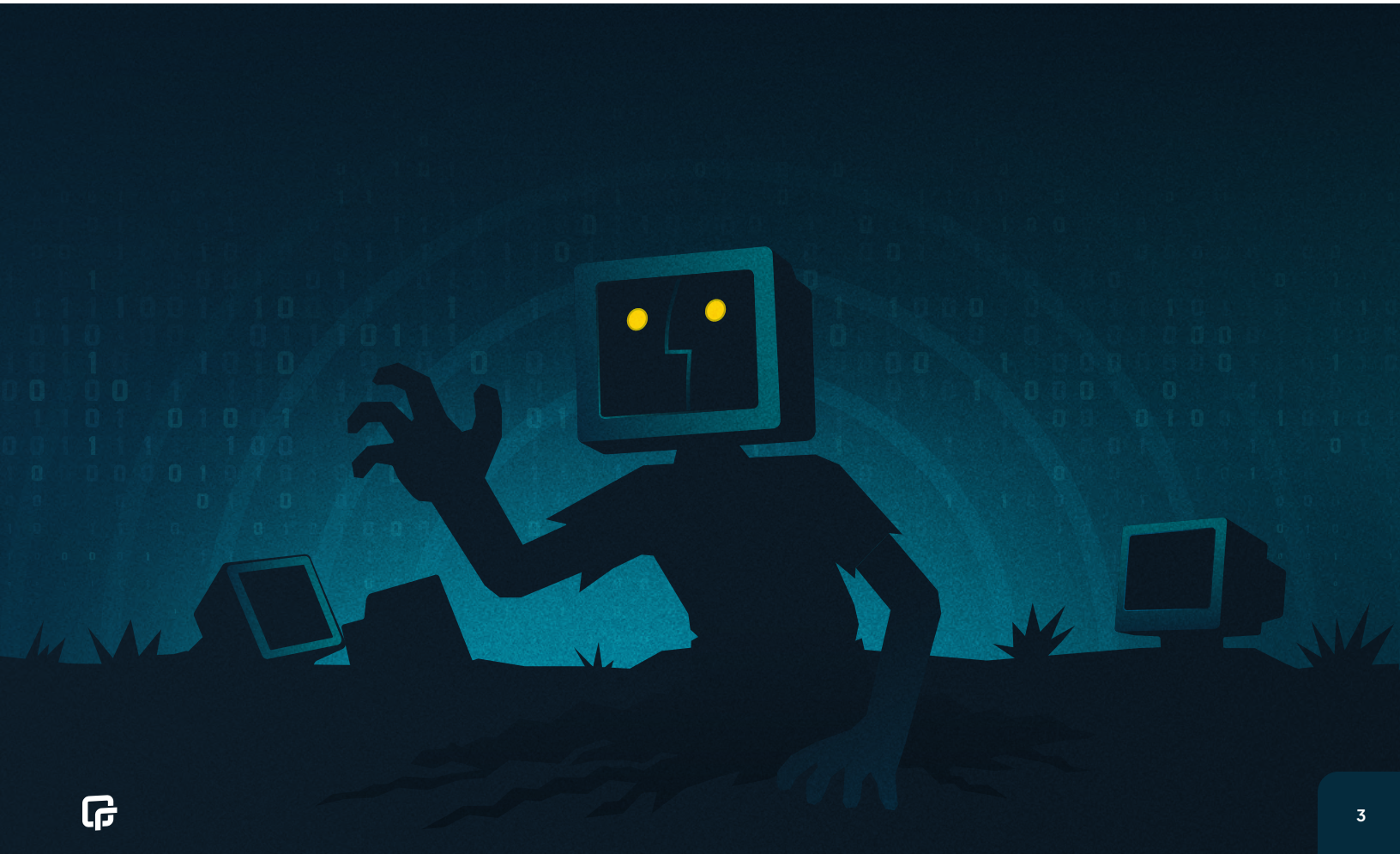
Introduction

Operating systems, or OSes, are purely imaginary. They are collections of ephemeral data and non-physical application programming interfaces (APIs) which allow applications to interact with the physical properties of the computer it runs on. Notably, operating systems have no moving parts and experience no chemical reactions, so they don't wear out due to friction, heat, and other real-world stressors that afflict machines made of silicon and metal, meat and bone.

And yet, these abstract operating systems inevitably face the day when they are designated as "end of life," or EOL, by their producers. Microsoft decides when a version of Windows is at the end of its effective life, Canonical decides when Ubuntu versions are retired, and Apple decides when iOS or MacOS is no longer worthy enough for regular use.

Before that grim day, OSes are described as "supported." During this period of the operating system's shipping life, users of that OS can expect to see new features, functionality, fixes, and most importantly, security patches and updates, on a somewhat regular basis. If you're getting popups from your desktop or your phone bugging you to reboot, you're using a supported operating system.

However, the term "end of life," which is common enough in manufacturing, is misleading, particularly in our digital realm. Unlike people, products that reach the end of their life do not truly die the way mortals do. Instead, they linger, in a state that's not quite dead, but certainly not healthy. Early in their EOL period, OSes are often indistinguishable from their properly supported counterparts. Things continue to operate normally and nothing much has changed. However, for software, and particularly operating systems, this is a particularly risky state of being.



The patchless dead

Attackers who prey on under-defended networks are particularly attracted to unsupported operating systems. For starters, EOL OSes are unlikely to be able to defend themselves against more modern attack techniques, including fresh zero-day exploits, nor provide robust post-exploitation compartmentalization. After all, new security patches aren't available, new defensive architectures are absent, and the pace of exploitation tactics and techniques continues to march on. These are the usual reasons why security professionals advise getting a handle on your population of EOL OSes before they give up the ghost.

It goes beyond mere lack of patches, though. EOL OSes also don't tend to change much after support ends, making them, over time, increasingly easy to fingerprint remotely. This makes them stick out in a reconnaissance probe of a targeted network; as an attacker, I would much rather focus my efforts on the 5% of EOL OSes I'm likely to find in a given network than the vast majority of otherwise "normal" and more-likely-maintained OSes.

Finally, their presence implies a lack of regular maintenance. This implication signals that even if an attack is noisy or disruptive, it's unlikely to attract the notice of an incident responder – after all, if someone was paying attention, they would have upgraded before EOL took hold. Again, as an attacker, if I see that a bunch of my target space is populated by walking dead systems, I'm likely to interpret it as a particularly attractive target space where the lights are on but nobody's home.

But wait just a minute – where did that 5% figure come from? Is it really true that one in twenty operating systems are running without hope of patches on today's networks? Dear reader, that is the very purpose of this paper! It turns out that here at runZero, we were unable to find any quality literature that describes what's a "normal" population of EOL OSes in a given enterprise, much less what normal looks like across industries, or even if that "normal" level is acceptable in today's hostile networking environments.

Unearthing EOL OSes

At runZero, we have access to a rather stupendous set of enterprise network data, composed of both internal and externally exposed assets (and heavy on the internal). We have hundreds of enterprise customers with millions of assets subscribed to our hosted attack surface and exposure management platform. In order to get to the bottom of this EOL mystery of what's typical in a given network, we selected a subset of those hosted enterprises, representing a cross-section of industries and network sizes. What follows is a study of a few hundred US-homed enterprises with a total asset count of about 8 million distinct assets, conducted over two and a half months of observation via weekly snapshots. For more on how the study was conducted, please see the Methodology section at the end of this paper.

Gradations of EOL

For most vendors which advertise EOL dates, there are generally two milestones at the end of a product's journey. The first is the end of active support, where users should not expect new features or low-impact bugfixes. Usually, a product enters this phase when a newer, more technically sophisticated product from that vendor enters the market. There is still staff dedicated to this now-legacy product, but the real development effort is being dedicated to the new operating system. The second, and usually final, phase of support is when the operating system enters the "extended" EOL phase. This is the time when only security fixes are provided, and even then, the security fixes tend to be only those determined to be sufficiently critical to address. All other development and improvement of the operating system ceases. In some cases, these two milestones are passed on the same day, with no extended grace period.

There is a secret third option for EOL support, which is paid, sometimes third-party provided, support. Some larger enterprises pay for ultra-extended support contracts, specifically to avoid the application upgrade and business process upgrade pains of moving properly to a supported operating system. On paper, the cost rarely works out in the user's favor, but the hidden costs of updating and retooling can outweigh annual service contract costs. If you're in the business of scanning and attacking internal networks, you may occasionally run into an obviously ancient server that, frustratingly, refuses to fall before your mighty decade-old exploits. These systems are quite likely hardened with aftermarket patches, produced and procured at great expense. They're rare systems, wildly expensive to maintain, and virtually impossible to distinguish from actual-EOL systems without tossing exploits at them.

Of course, these shambling corpses of computers might also just be honeypots, designed to bait interlopers into an attack. This is a risky, but sometimes effective, defense tactic to identify and then box out attackers, especially in enterprises with excellent intrusion detection monitoring. That said, for the purposes of this study, we're discounting their existence, as they're (probably) rare enough to not move our numbers around too much.

Just how many zombies are too many?

As we've learned from popular media, like the seminal Night of the Living Dead, one or two zombies scraping at your door is troubling, but more of a nuisance than anything. As we see in Left 4 Dead or Zombieland, things start getting worrisome when there are dozens, hundreds, or thousands of the walking dead in your immediate vicinity. So, we must consider, at what point are EOL OSes a pressing problem, demanding attention and effort from CISOs and ITOps?

Across the entire corpus of studied enterprises for the entire window of study, we found that about 8.56% of all assets are at some level of end of life, and just about 5.00% of assets are currently beyond the advertised extended end of life as of September 30, 2025. If you stop reading here, you can confidently know that if less than 5% of your total asset population in your enterprise is unpatchable, you're doing better than average. Good job?

I'm not entirely convinced that this should be a comforting revelation. For all the reasons stated above, unpatched – and unpatchable – EOL operating systems handling critical business functions are a ticking time bomb for your enterprise. In 2021, the United States Cybersecurity and Infrastructure Security Agency stated rather starkly in advisory AA21-287A[1] that "[t]hreat actors likely seek to take advantage of perceived weaknesses among organizations that either do not have — or choose not to prioritize — resources for IT/OT infrastructure modernization." CISA reiterated this warning in 2023 in their Bad Practices blog[2], with, "unsupported (or end-of-life) software in service of Critical Infrastructure and National Critical Functions is dangerous and significantly elevates risk to national security, national economic security, and national public health and safety."

EOL OSes over time

Because the study was conducted over two and a half months, we can look at the week-to-week changes in total EOL asset counts. For the purposes of this study, we picked September 30, 2025 as "today," and backtested our observations with this date in mind.

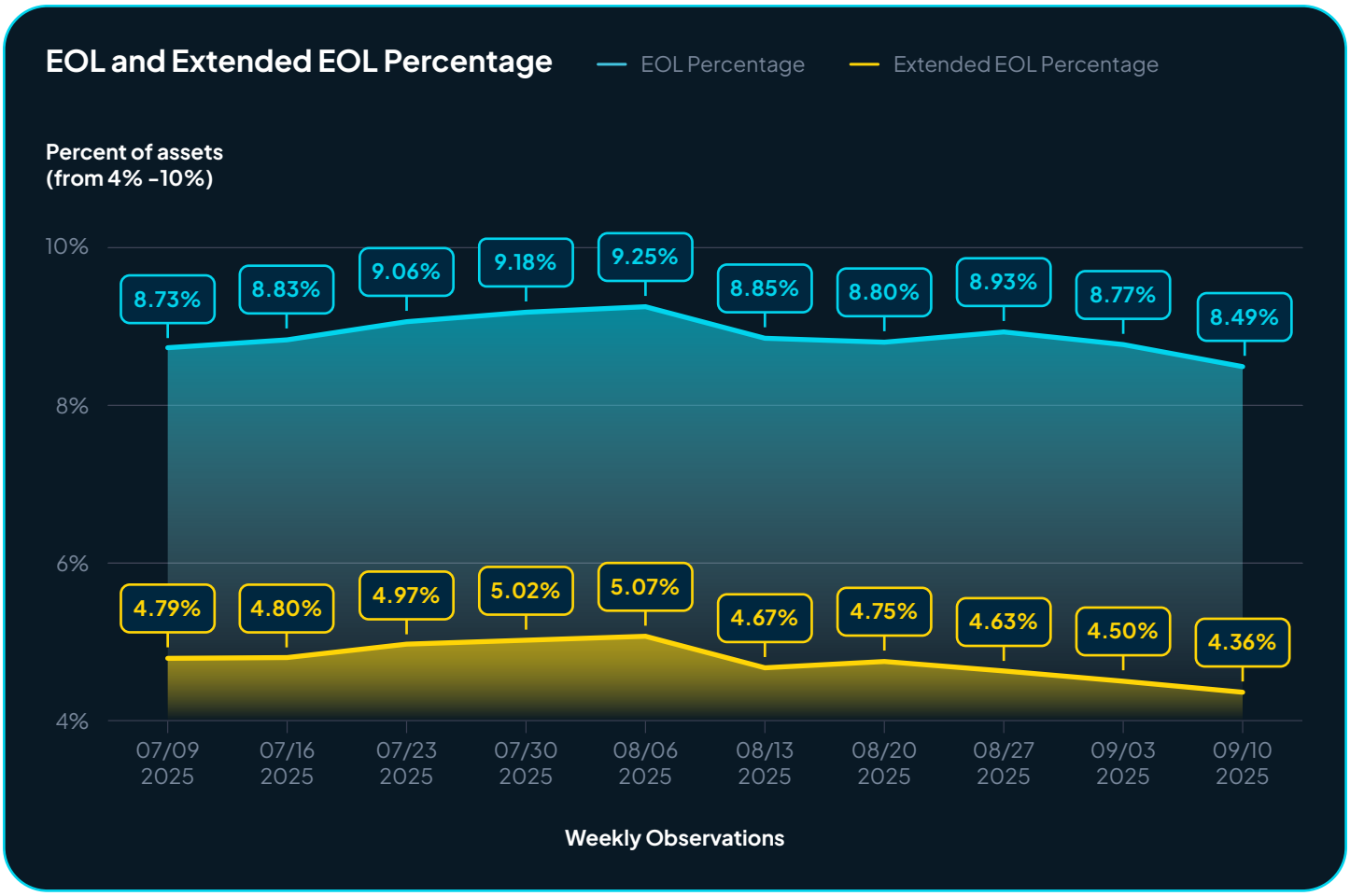


Chart 1: Observed EOL and Extended EOL percentages in networks over time

As we can see from the chart above, from week to week, EOL populations range from 8.49% of total assets to 9.25%, while extended EOL populations range from 4.36% to 5.07%. The good news with this view of the data is that the trend line is at least going in the right direction – there are fewer EOL assets in enterprise networks today than there were at the beginning of July of 2025.

[1] https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-287a
[2] https://www.cisa.gov/news-events/news/free-cybersecurity-services-and-tools-bad-practices

EOL by industry sector

Because we have industry categorizations for all enterprises in the analytic sample, we can take a look to see which industries, in general, are doing better or worse than this 5% overall average for extended EOL OS prevalence. (For this and all other industry comparisons, only 15 of the 24 North American Industry Classification System (NAICS) defined industries are considered for sample size reasons – see Methodology for details.)

Industry (NAICS 2-Digit Prefix)	EOL Percentage	Extended EOL Percentage
Specialized Retail Trade (45)	1.40%	0.94%
Consumer Products Manufacturing (31)	3.87%	2.18%
Transportation and Warehousing (48)	5.77%	2.49%
Wholesale Trade (42)	5.13%	2.83%
Public Administration (92)	4.78%	2.84%
Other Services (81)	11.48%	3.06%
Information (51)	7.61%	3.16%
Finance and Insurance (52)	7.60%	3.59%
Health Care and Social Assistance (62)	6.13%	3.94%
Utilities (22)	7.91%	4.00%
Educational Services (61)	6.26%	4.36%
ALL	8.58%	5.00%
General Retail Trade (44)	13.59%	5.15%
Machinery and Electronics Manufacturing (33)	10.72%	7.23%
Professional, Scientific, and Technical Services (54)	12.84%	7.66%
Wood, Paper, and Chemicals Manufacturing (32)	17.17%	9.05%

Table 1: EOL and Extended EOL Percentages observed, by industry

This table is stacked by least-to-most extended EOL percentage, with ALL serving as the red line, beneath which industries are faring worse than average. As we can see, four industries are struggling to hit the average rate of OSes that are able to be patched against new threats: retail, machinery and electronics, professional services, and chemical manufacturing. This industry also represents biotech and pharmaceutical companies, so this outsized level of EOL and extended EOL OSes is particularly troubling from a public health perspective.

The "Other services" industry sector also rises above the baseline level of feature EOL support expiration, which brings up an important consideration to the EOL story: Just because an operating system has not quite reached the extended EOL milestone **doesn't** mean that everything is fine. As an IT practitioner and a cybersecurity researcher, I've noticed that when operating systems are nearing end of life, especially those OSes based on proprietary software, responsiveness to security events for those operating systems tends to degrade fairly linearly. After all, the vendors of these OSes are focused on shipping the newer, more exciting operating system, and the individual engineers working there will find that their bonuses, career advancement opportunities, and other incentives are tilted toward the new hotness rather than the less glamorous legacy support.

It's not just the vendors guilty of this favoritism. Researchers and academics studying what's out in the world for security implications will also tend toward the more recent, better supported operating systems. This is done in the hope of catching new issues early, their expensive and time-consuming research remains relevant, and because the old stomping grounds for exploits become commonplace and kind of boring. In other words, while we use these bright-line dates to distinguish between "can get patches" and "out of luck" operating systems, the reality (as with most things) is fuzzier, with fewer resources dedicated to both discovering and fixing security issues in older systems.

EOL OSes by industry sector, over time

Over the ten week observation period, how are particular industries faring with their efforts to decommission and upgrade their EOL OS infrastructure?

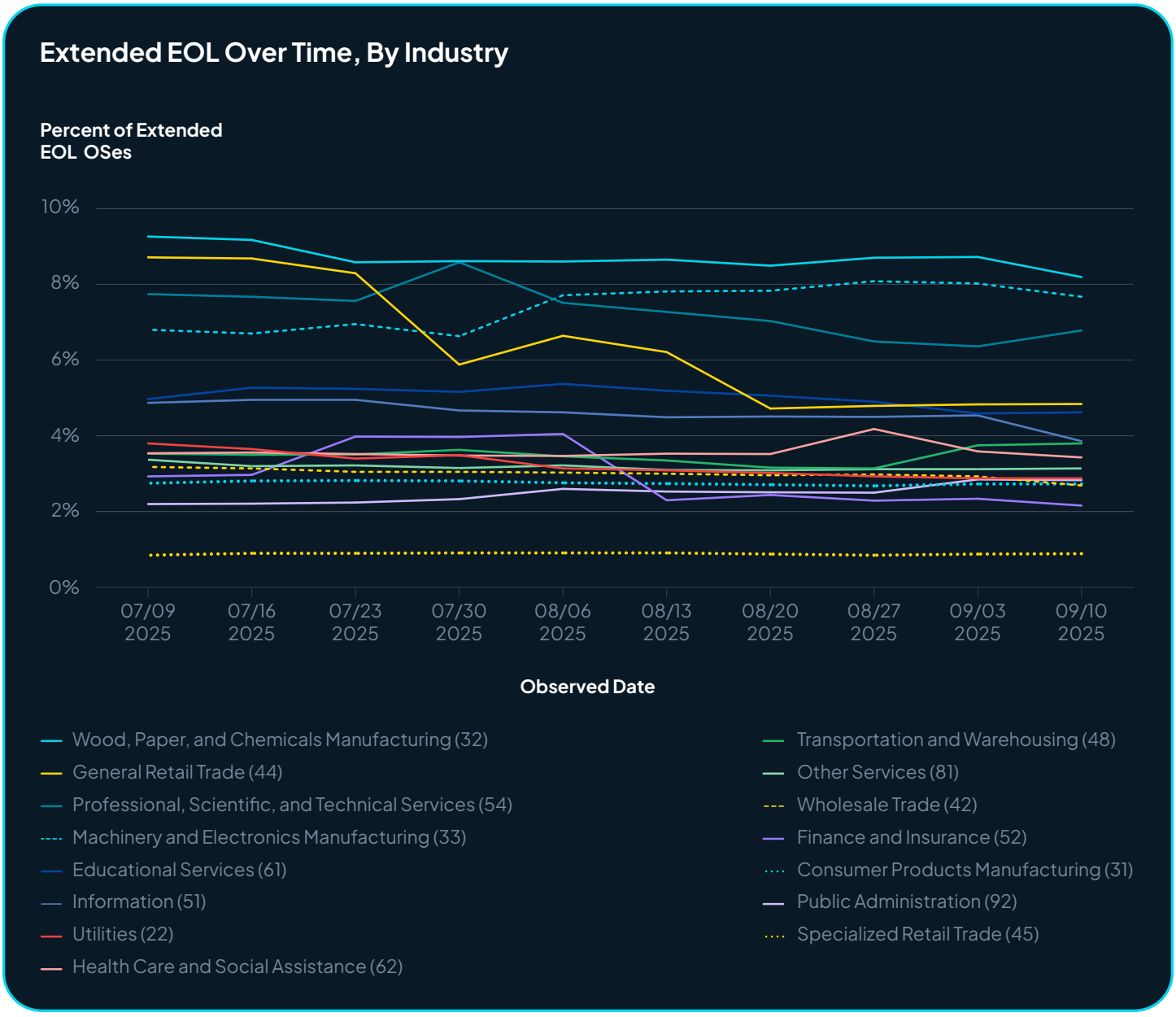


Chart 2: Extended EOL OS percentages, by industry, over time

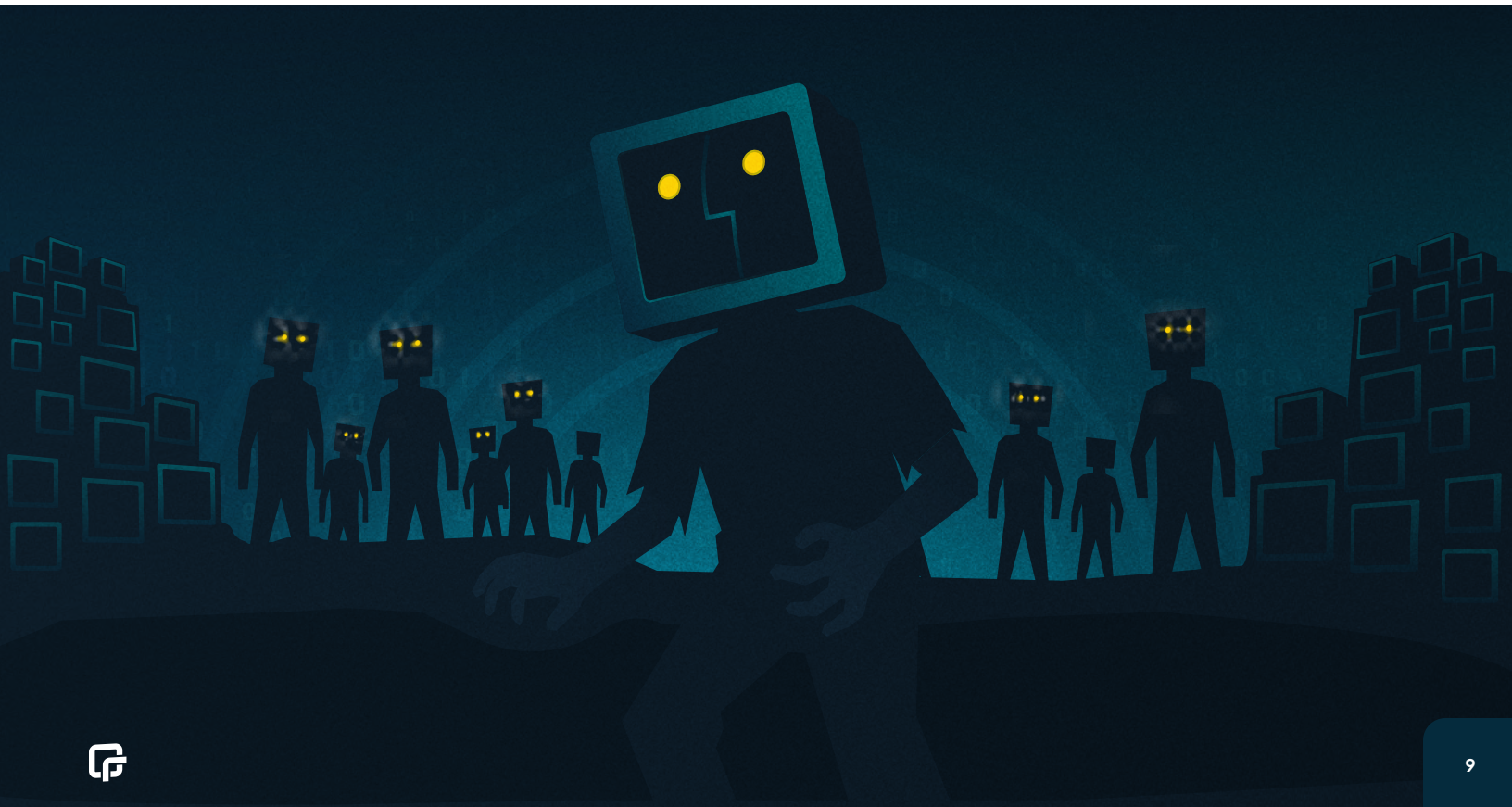
Looking at this time series, while most industries are trending toward fewer EOL OSes, they do not appear to be making concerted efforts to whittle down their EOL OS populations. The general retail sector, though, has made some notable progress, cutting their EOL OS by half, from 8.70% down to 4.84% by the end of the study period. However, both machinery and electronics manufacturers and public administrations appear to be going in the wrong direction with respect to a September 30, 2025 EOL date. Both appear to have **gained** EOL OS populations, rising from 6.8% to 7.7% and 2.2% to 2.8%. At least the public sector is still comfortably below the overall average of 5% of extended EOL OSes.

It's important to note that the analytic sample did not change over the observation period – all enterprises which began in the study in July remained in the study throughout, and no new enterprises joined the analytic sample. Also, the target EOL date remains fixed on September 30, 2025 (we are not considering EOL dates that may have occurred between July and September). This leaves the internal considerations for data collections, which definitely could have changed over time.

As individual enterprises continue to deploy runZero explorers and wire up new data integrations with other survey products to extend visibility across more networks (internal, external, mobile, and cloud), naturally the total population of observed EOL systems should also move around. So, the pollyanna view for these industries is that they may be merely building awareness of newly detected EOL operating systems, rather than adding large numbers of "new" EOL OSes to their enterprises. (Of course, this interpretation cuts both ways – it's entirely possible that some enterprises in general retail merely turned off visibility into EOL-ridden networks, rather than decommissioning and upgrading.)

The truth likely lies somewhere between these two explanations. There does not appear to be an aggressive hunt of EOL OSes (except possibly in the general retail sector), nor do there seem to be massive outbreaks of EOL systems as new internal detection capabilities come on line.

However, this situation will change, rather significantly, on October 14, 2025.



World War W

Microsoft has been warning for well over two years of the eventual sunsetting of Windows 10 on October 14, 2025, starting in April of 2023 according to Forbes[3]. Since then, there have been occasional news articles and support updates, including an early appearance by this author on the runZero Hour[4] webcast (skip to 18m59s for the EOL discussion). At that point, we warned that enterprises are edging into the "almost too late" period for updating off of Windows 10.

The lack of panic around the end of security patches for Windows 10 is both puzzling and troubling. Windows 11 only recently edged out Windows 10 as the most popular Windows desktop version, according to StatCounter:

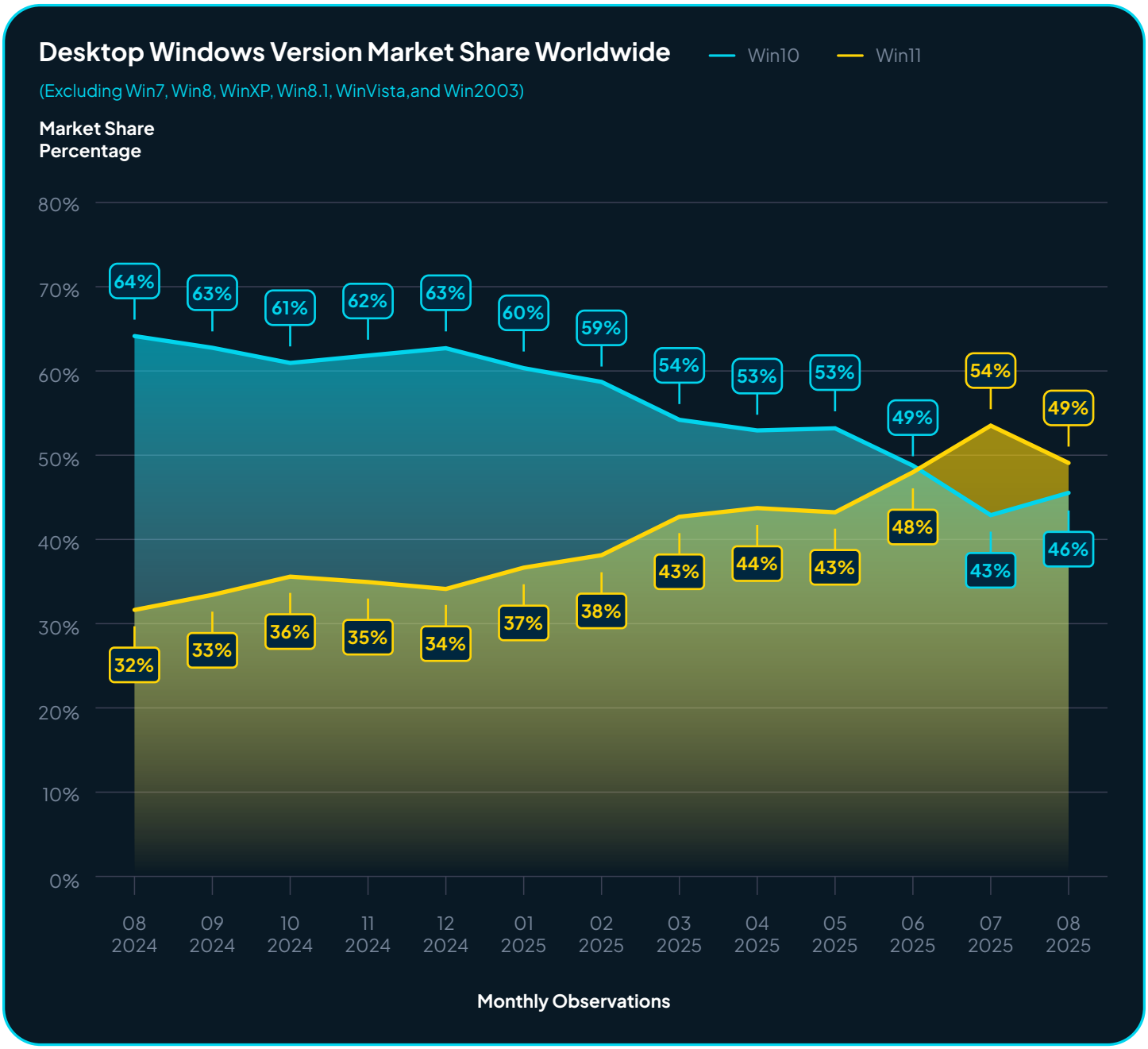


Chart 3: Prevalence of Windows Desktop operating systems as reported by StatCounter.com[5]

[3] https://archive.ph/FtNSK
[4] https://www.runzero.com/resources/runzero-hour-16/
[5] https://gs.statcounter.com/os-version-market-share/windows/desktop/worldwide/

No version of Windows accounts for more than 50% of all desktop operating systems – there is enough Windows 7, Windows 8, and Windows XP, out there to push Windows 11's total market share to a mere plurality of 49% as of August of 2025, according to StatCounter, and runZero's own data confirms this (and provides a more bleak view of old Windows):

OS	Percentage of EOL-detectable Microsoft OSes
All Supported Microsoft OSes (excluding Windows 11)	39.08%
Windows 11 (Versions supported through 2025)	29.00%
October 14 EOL Windows (including Windows 10 and 11)	26.63%
Older Windows 10 Releases (Currently EOL)	3.07%
All Other Currently EOL Microsoft OSes	2.22%

Table 2: Observed prevalence of Windows operating systems

We can expect that after October 14, 2025, about 68% of the total, EOL-detectable Windows operating systems in enterprise networks will remain supported for security fixes (at least until January 1, 2026) without any special considerations made for paid, extended support.

This means that about 32% of Windows OSes will, by default, not be capable of receiving security fixes. That includes the current Windows EOL population of about 5.29% (again, of all Windows systems where runZero can determine EOL status).

Given the millions of systems at stake across industries, it's a little baffling that this isn't being treated like a looming catastrophe, akin to Y2k.

At runZero, we're usually pretty skeptical of doom-and-gloom prognostications. After all, major versions of Windows have gone end-of-life before. Every time this happens, it's definitely painful, it contributes to the lingering EOL OSes we're seeing today, but it's never truly been an apocalyptic event. So it's reasonable to believe that Windows 10's coming EOL isn't likely to be as disastrous as an unmitigated Y2k.

But the world is even more connected today, a quarter century past Y2k. We can see from recent events that any time Windows experiences a global hiccup, major drama results. When a buggy Crowdstrike update was delivered to about 8 million of their Windows-based Endpoint and Detection and Response (EDR) customers in July of 2024, it caused some pretty severe chaos, including grounding most air traffic[6] in and around the US.

Windows today commands about a billion and change[7] monthly active users. If that's true, the Crowdstrike crash only really affected about 0.8% of the world population of Windows.

As mentioned at the start of this paper, EOL status does not mean instant crashes, breaches, and ransom demands. But, if I were in the business of international espionage and cyberwar, I would be sitting on my killer Windows 10 exploit until I could be reasonably sure it couldn't be blocked by routine updates.

[6] https://www.edgarindex.com/2025/06/19/us-court-dismisses-class-action-lawsuit-related-to-crowdstrike-outage-that-disrupted-air-travel/
[7] https://www.tomshardware.com/software/windows/windows-seemingly-lost-400-million-users-in-the-past-three-years-official-microsoft-statements-show-hints-of-a-shrinking-user-base

With that cheery outlook, let's take a closer look at which industries are setting up for some serious EOL headaches.

The Winpocolypse

The chart below is the same weekly time-series view of EOL assets by industry as seen in *Chart 3* above, but considering only Microsoft-sourced assets which will be EOL as of October 14, 2025. This includes those Microsoft OSes that are currently EOL as well.

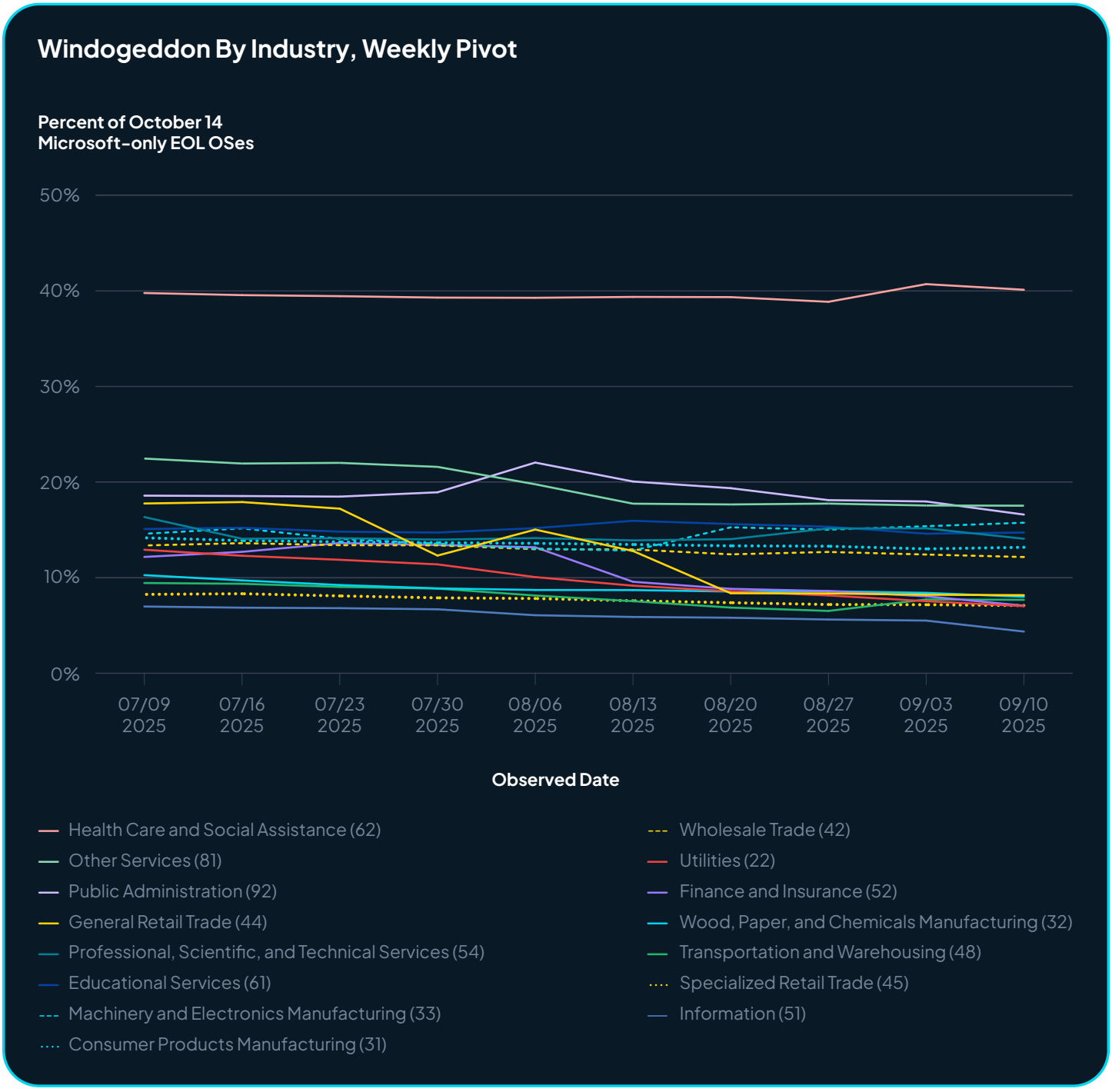


Chart 4: Observed percentages of Microsoft OSes entering EOL on October 14, 2025

This sobering chart shows a clear outlier, healthcare and social services, that's going to have to act pretty quickly to start knocking down their suddenly-turned EOL population. Windows is a pretty "sticky" end-of-life operating system, and anyone who has been to a doctor's office in the last few years no doubt has noticed that today, Windows 7 is not all that unusual to find, even though it went EOL for security fixes in January of 2020.

For the other industries included in this study, the below is the chart excluding healthcare.

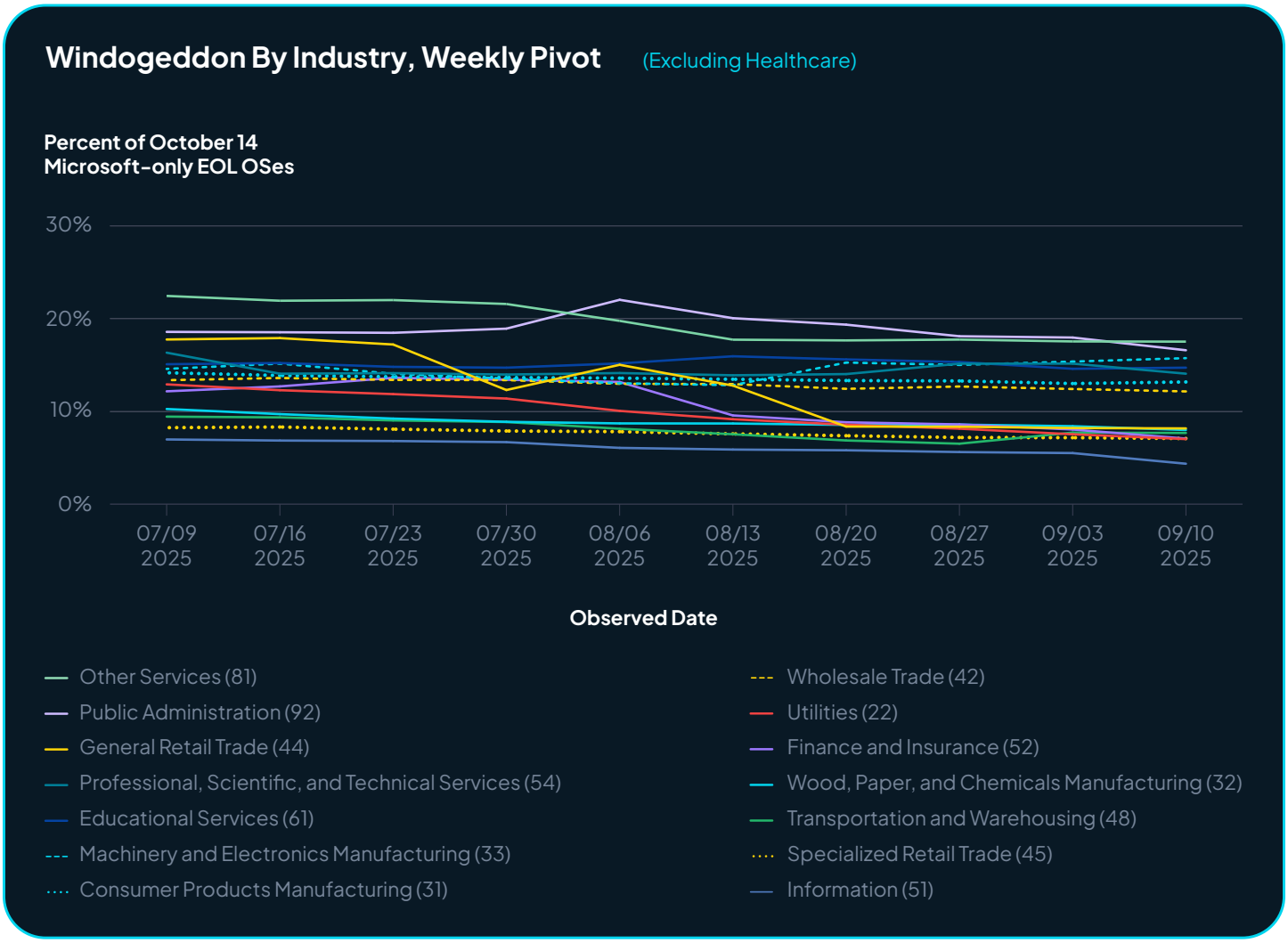


Chart 5: Observed percentages of Microsoft OSes entering EOL on October 14, 2025, excluding Healthcare and Social Assistance industry percentages

Other industries face an EOL outbreak in their enterprises, though not to the outsized effect of healthcare. The least affected industry is information technology, which has relatively little Windows running day-to-day operations (good job, UNIX nerds!). But, where extended EOL percentages were averaging around 5% overall, most industries are going to double – or more – their respective EOL loads. The data today suggests that the new-normal level of EOL in an enterprise will triple, from 5% to about 16%.

Unless urgent action is taken, we're likely to see similarly increased risk of directed attacks involving these older operating systems. Will Microsoft blink? How serious is this October 14, 2025 deadline? After all, this EOL status isn't handed down as some kind of divine punishment or anything – it's a choice by Microsoft. It's driven by economic and business realities, but a choice nonetheless.

Conclusions

This study of end-of-life operating systems across hundreds of U.S.-based enterprises and millions of assets reveals a persistent, if somewhat overlooked, cybersecurity risk. Today, approximately 8.56% of enterprise assets operate on EOL OSes, with 5% already beyond extended support and unable to receive critical security patches. While these numbers may be manageable with careful network segmentation and a concerted effort to decouple EOL OSes from legacy applications, the reality is that these systems represent a concentrated, visible attack surface for threat actors inside and out. Even assets that have not reached extended EOL yet are increasingly under-resourced for security monitoring and patch responsiveness, illustrating the motivational and economic risks of pre-EOL neglect.

Industries vary in exposure to EOL-based risks. Retail, machinery and electronics manufacturing, professional services, and chemical/biotech sectors consistently exhibit above-average concentrations of EOL OSes. For sectors like healthcare, where critical services depend on legacy systems, the risks are particularly acute.

The impending Windows 10 EOL on October 14, 2025 dramatically amplifies this continuing EOL-based risk. Our data suggest that approximately one-third of Windows assets will transition to unsupported status almost overnight, effectively tripling the enterprise-wide EOL population. While merely being EOL is not in and of itself a vulnerability, and while previous major Windows EOL events did not precipitate global crises, the modern connected enterprise's continued dependence on legacy Windows raises the stakes for this EOL deadline more than ever before. Healthcare and social services are particularly and acutely at risk, and EOL OS maintenance is quite likely to crowd out other IT priorities for at least the next year.

End-of-life operating systems are never truly dead, but undead – lingering in a cursed state of half-life, vulnerable, and increasingly dangerous to those assets around them. Enterprises that fail to proactively manage and ultimately reduce EOL operating system populations are providing attractive targets for thieves, spies, and other assorted chaos agents. Strategic prioritization of the rapid decommissioning of unsupported OSes, and continued attention to industry-specific risks are essential steps to mitigate these looming threats.

Grab your Twinkies™ and a shovel!

While the data clearly shows that EOL operating systems are an enduring risk that is only going to get worse, fast, mere awareness alone is not enough. The undead OSes lurking in enterprise networks require decisive action from vendors, IT teams, and researchers alike. What follows are concrete steps each of these groups can take to reduce exposure, prevent exploitation, and avert disaster.

Recommended vendor actions

OS vendors must take a more assertive role in guiding both application developers and customers through the upgrade lifecycle. Application developers which build niche B2B software must prioritize post-upgrade compatibility in a secure-by-design manner, reducing the friction that leaves enterprises trapped on unsupported systems. After all, OS vendors tend to take the reputational hit for releasing OSes that aren't backwards compatible with their necessary enterprise applications, so these vendors can and should communicate more assertively with customers about upcoming EOL events. Normal users are clearly failing to truly grasp the implications of a major Windows version sunset. Application developers often dodge blame for not updating against the new APIs by crying foul over the lack of backwards compatibility, despite the fact that more modern operating systems tend to be faster, more efficient, and more secure.

Recommended IT operations actions

Ask for budget. Articulate the risk with real, data-backed stories (like this paper). When it's license renewal time, you have the most power to pressure your application vendors to update. After all, it's ultimately their fault you're stuck on Windows 7 / Windows 2012 here in 2025. Be ready to seek alternatives to applications that steadfastly require EOL OSes. This is easier said than done, especially in niche markets like healthcare, education, and industrial software, or any industry where an oligopoly persists due to customer lock-in and a lack of true competition in the marketplace.

Victim-blaming for failing to update is much more likely in breach events where the initial access vector was running an end of life operating system. Investigators and commenters alike tend to discount application lock-in issues that force lingering on EOL OSes. CISOs, be extremely wary of letting this EOL hand grenade sit in your lap. In many regulated environments, this victim-blaming can take the form of fines and compliance actions. NIST 800-53 Rev 5, SA-22[8] (important for FISMA and FedRAMP), HIPAA Title 45 CFR § 164.308(a)(1)(ii)(B)[9] (important for healthcare providers), and PCI DSS requirement 6.2[10] (important for credit card processors) are often cited when investigators determine that EOL OSes, and their lack of patches against known vulnerabilities, are implicated in breaches.

Recommended researcher actions

Shine a light on these lurking risks. Tracking EOL systems may not be glamorous, but it is crucial. Researchers can alert enterprises to outsized exposure before threat actors exploit it. The International Institute for Obsolescence Management[11] exists for precisely this reason, and is gaining traction worldwide.

Keep in mind that reporting vulnerabilities in unsupported systems may encounter resistance from vendors and receive muted attention from traditional threat feeds. Nonetheless, raising awareness now can prevent disasters later, even if the CVEs issued for EOL systems get less traction than those for supported software.

[8] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf#page=317
[9] https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-C/section-164.308
[10] https://listings.pcisecuritystandards.org/documents/PCIDSS_QRGv3_1.pdf#page=17
[11] https://www.iiom.global/

Appendix (delicious!): methodology

Data sources

The data analyzed in this paper depends on two primary sources: the database provided by the open source project endoflife.date, and data collected and aggregated by runZero as it's run in client enterprises.

Determining EOL dates

The community collaboration of https://endoflife.date is an enormously valuable resource for determining EOL dates for operating systems, applications, frameworks, and languages, and became such an essential resource for both this paper and general EOL management thanks to the heroic efforts of open source legend captn3m0 (https://github.com/captn3m0). runZero bases much of its EOL intelligence on this resource. From time to time, runZero also conducts EOL research on asset types that aren't otherwise covered by endoflife.date.

Asset data

Asset counts come directly from a proprietary dataset collected and maintained by runZero.

The analytic sample for this study was drawn from a subset of the runZero customer base and consists of enterprises that (1) opted into generalized, anonymized data analyses, (2) held an enterprise license during the study period, (3) were not on-premises installations, and (4) had data residency in the United States. All enterprises in air-gapped environments or with European data residency were excluded.

All members of the analytic sample were present in the customer set as of the July 9, 2025 snapshot and remained present in all subsequent weeks, in order to control for the effect of new customers entering the analyzable set of networks and assets, and the effect of any enterprise customers leaving the analytic sample. Applying these criteria for selection resulted in a sample of a few hundred enterprises, collectively comprising approximately eight million assets across 24 NAICS two-digit prefix coded categories. This sample is a representative fraction of the total customer and asset population available to runZero.

NAICS 2-Digit Prefix	Common Industry Name	Enterprise %	Asset %
33	Manufacturing (Machinery and Electronics)	10.2%	29.0%
52	Finance and Insurance	10.2%	17.8%
51	Information	15.3%	11.9%
45	Retail Trade (Specialized)	1.7%	10.0%
54	Professional, Scientific, and Technical Services	15.8%	9.6%
61	Educational Services	9.3%	7.1%
92	Public Administration	8.2%	2.8%
31	Manufacturing (Consumer Products)	2.8%	2.7%
44	Retail Trade (General)	1.7%	2.4%
62	Health Care and Social Assistance	2.8%	1.4%
81	Other Services (except Public Administration)	6.2%	1.0%
32	Manufacturing (Wood, Paper, and Chemicals)	2.3%	< 1.0%
22	Utilities	2.8%	< 1.0%
48	Transportation and Warehousing (General)	1.7%	< 1.0%
42	Wholesale Trade	2.0%	< 1.0%
11	Agriculture, Forestry, Fishing and Hunting	< 1.0%	< 1.0%
21	Mining, Quarrying, and Oil and Gas Extraction	< 1.0%	< 1.0%
55	Management of Companies and Enterprises	< 1.0%	< 1.0%
71	Arts, Entertainment, and Recreation	1.4%	< 1.0%
56	Administrative and Support and Waste Management and Remediation Services	< 1.0%	< 1.0%
23	Construction	1.1%	< 1.0%
53	Real Estate and Rental and Leasing	< 1.0%	< 1.0%
49	Transportation and Warehousing (Specialized)	< 1.0%	< 1.0%
72	Accommodation and Food Services	< 1.0%	< 1.0%

Table 3: NAICS 2-Digit Prefix codes to industry descriptions mapping

For general statements and observations that do not compare industries, runZero data skews toward Machinery and Electronics Manufacturing (NAICS 2–digit prefix 33), Finance and Insurance (52), Information (51), Specialized Retail Trade (45), and Professional, Scientific, and Technical Services (54).

To enable meaningful comparisons across industries, we focused on sectors with sufficient representation in this dataset. Industries were included for comparison only if they had at least a baseline minimum of distinct enterprises, and at least more than the 25th percentile of unique assets seen across all industries.

This technique of winnowing down industries for comparison purposes, while retaining the whole corpus for the analytic sample, filters out sparsely represented sectors that could skew inter-industry comparisons, while preserving a more complete, industry-agnostic dataset that reflects the broader enterprise landscape. Specifically, the following industries are not represented in inter-industry comparisons: Agriculture (NAICS 11), Mining, Quarrying, and Oil and Gas Extraction (21), Construction (23), Specialized Transportation (49), Real Estate (53), Company Management (55), Administrative Support and Waste Management (56), Arts and Entertainment (71), and Accommodation and Food Service (72).

Data collection

Individual enterprises were able to choose which networks to collect data on, and not all networks are production. We recommend running runZero everywhere, of course, in order to have visibility of enterprise-wide exposures and threats. In that sense, while these numbers are essentially self-reported, they're automatically collected based on each client's own specific criteria. That said, most clients will skew toward production and desktop environments first, and later start adding development, test, cloud, and mobile networks.

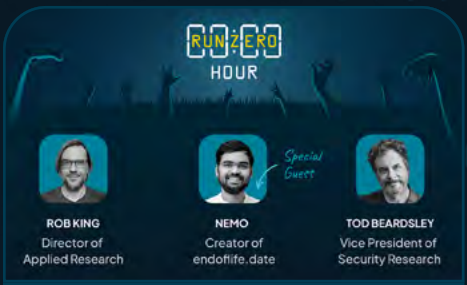
Finally, this dataset reflects passive and active scanning by runZero Explorers in customer environments, as well as data those customers integrate from other sources. Notably, passive scanning and data imports can be less specific than direct scanning, so EOL data for those systems may be unknown.

Determining EOL status

For the purpose of this study, the EOL date chosen was September 30, 2025. By fixating on a static, slightly future date, we can simplify analysis and presentation, removing spikes that would have been caused by EOL dates passing during the observation period, and allows us to see a clearer picture of general EOL trends.

Overall, runZero is generally accurate at identifying specific asset models and versions through active scanning, and tying those specific versions to an EOL date, but there are cases where we cannot make an accurate enough determination of the nature of a detected asset to determine if it is EOL or not. This can be due to limitations in passive scanning, data integration from other sources, or a lack of sufficiently detailed fingerprinting for some less-common asset types. Additionally, not all vendors are forthcoming with EOL dates for their products.

In these cases, when an EOL date cannot be determined, it's set to "0," and we default to presuming these devices are, in fact, still supported. Therefore, comparisons of EOL versus "not EOL" are going to treat these unknown status devices as "not EOL." The subject of truly unknown EOL, and the risks to enterprise security therein, will be addressed more specifically in a future paper.



Beyond the veil with EOL OSes

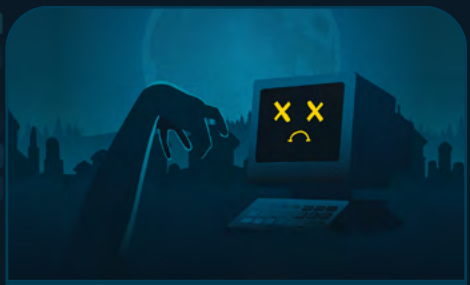
A spooky campfire chat about this report with special guest Nemo.

Watch the Episode

Great research sparks smarter defense

Stay ahead of the curve in exposure management with cutting-edge insights.

Explore runZero Research



Wondering what lurks on your network?

Uncover the unknowns with runZero – start your free trial in minutes.

Try runZero Free

runZero provides a single source of truth for exposure management across your total attack surface: internal, external, IT, OT, IoT, mobile, and cloud.

Providing the most complete and accurate visibility into every asset and exposure, runZero helps you mitigate risks faster, meet compliance requirements, and ensure you continuously discover the assets and exposures that others miss.