TuxCare

Enterprise Linux & Open-Source Landscape Report 2025

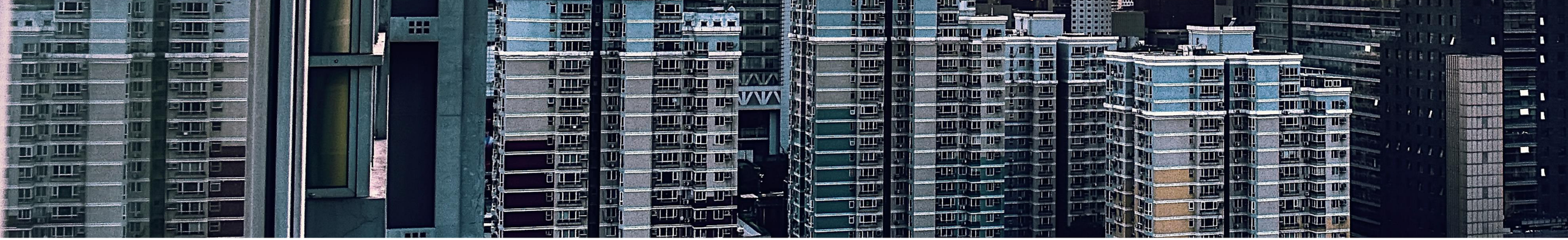


Table of Contents

Dear Colleagues,

The TuxCare Team is thrilled to present the second annual Enterprise Linux and Open Source Landscape Report. Our 2025 report, the result of our yearly industry survey for which many Enterprise Linux users contributed their knowledge, uncovers a fascinating breakdown of the current state of this space.

As we journeyed through a year of significant innovation, disruption, and growth, our survey was designed to encapsulate the insights and opinions of the very people that work with open source and Enterprise Linux as part of their jobs. We achieved this with our standard attention to what matters most to these users and their organizations, with an added focus on the fallout of wide-reaching events.

By navigating through the preferences, behaviors, predictions, and more, of the experts that use open-source products on a daily basis, we have discovered trends that have held strong since last year's report – as well as some patterns that will certainly surprise you.

This report covers several critical areas:

Trends in Enterprise Linux Distribution & Cloud Service Provider Preferences: With CentOS 7 officially in its end-of-life stage, we examine the current preferences of Enterprise Linux users, aiming to understand how these professionals view the software and tools that they depend on.

Linux Patch and Vulnerability Management: This section explores how organizations address security and stability challenges within the Enterprise Linux ecosystem, highlighting key strategies and best practices for patch and vulnerability management.

The CrowdStrike Incident: As we look back on this massive security incident, caused by a flawed testing process, we gain an understanding as to how it impacted organizational software release policies, testing processes, and rollback plans.

The XZ Incident: In this section, we investigate the main causes of exposure to this vulnerability, how it sparked changes in open-source patch management processes, and whether organizations have taken measures to protect themselves from a similar incident in the future.

Open-Source Supply Chain Security: In an environment where open-source software supply chain incidents, like the XZ backdoor incident, are happening, our report examines their impact on supply chain management strategies – outlining key challenges and the responses to these evolving threats.

Plans and Status of AI Adoption: Moving beyond the AI hype, we present a realistic view of how companies are integrating AI-powered software into their operations, exploring their motivations and expectations from these technologies.

The insights generated from the analysis of this year's survey offer a compelling snapshot of an industry that is rolling with the punches, where organizations are developing increasingly sophisticated strategies to navigate the sometimes-choppy waters of open-source software and Enterprise Linux. We truly hope that you find the contents of this report as fascinating as we do!

We greatly appreciate everyone who contributed to this research. Your insights not only deepen our understanding but also drive the collective progress of this space.

Looking ahead, we are eager to see how these emerging trends will continue to shape the future. We encourage you to explore the findings, reflect on their implications, and join the conversation as we work toward a more informed and resilient open-source world.

Sincerely,
Your Friends at TuxCare

Enterprise Linux users aren’t just keeping up.

They’re adapting to every update – and every disappointment.

SECTION 1

Trends in Enterprise Linux Distribution & Cloud Service Provider Preferences

- How many Linux distributions are enterprises using and which ones?
- With CentOS 7 now End of Life (EOL), what does CentOS usage look like today?
- What paths are organizations taking when – and if – they move away from CentOS?
- Which Cloud Services Providers are enterprises using today?

What Linux distributions are enterprise users working with?

Ubuntu

Ubuntu is the most widely used distribution, with 40.75% of respondents indicating its use.

RHEL

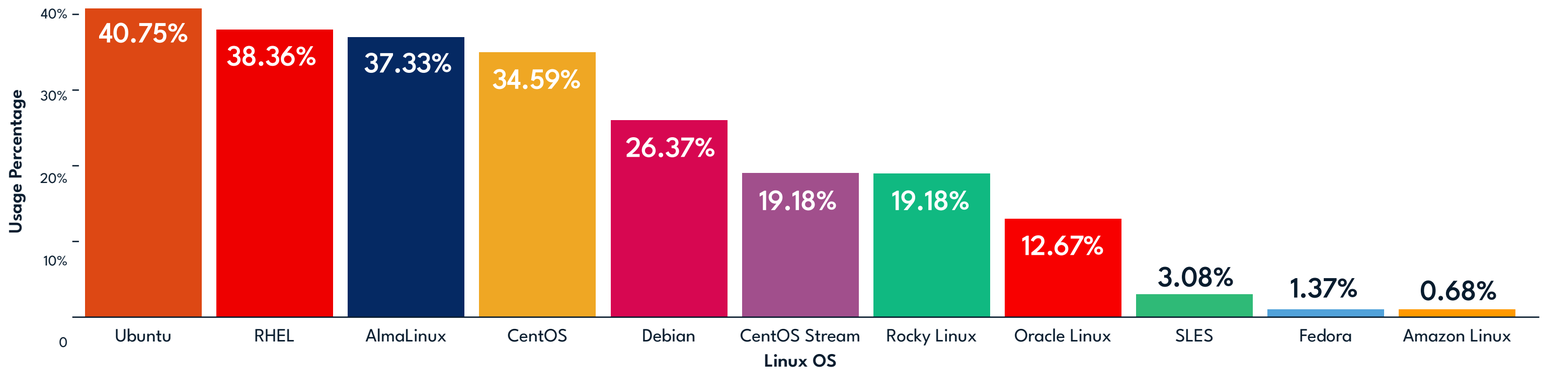
Red Hat Enterprise Linux closely follows, used by 38.35% of respondents (compared to 28.06% last year).

The (Light) Impact of the End of Life of CentOS 7

Despite CentOS 7 reaching End of Life (EOL) in June of 2024, and all other versions of stable CentOS having already reached EOL before that, CentOS usage remains strong, with just a marginal decrease from last year.

34.59% of respondents use CentOS – down from 39.80% in the previous year.

Linux Operating System Usage Percentage



Other noticeable trends:

Debian is rising in popularity
going from 14.8% last year to 26.03% this year.

Like a Rock: Rocky Linux usage has remained stable
at 19.18% compared to last year's 20.58%.

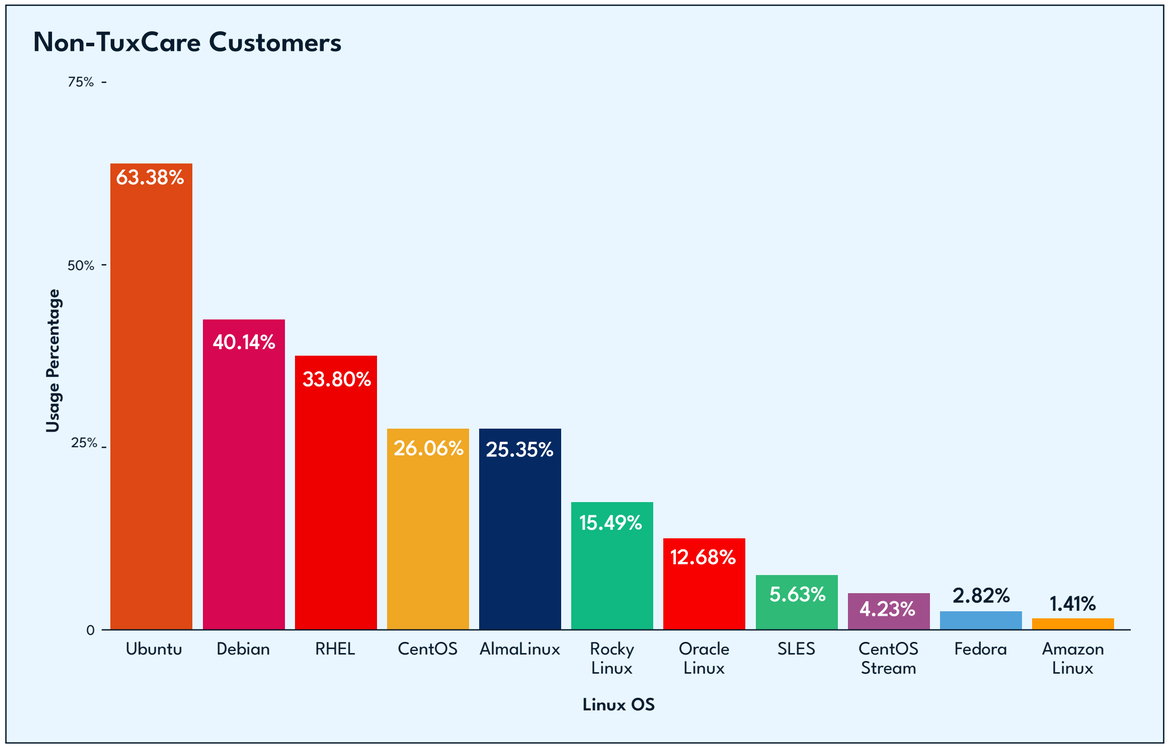
CentOS Stream has drastically diminished in usage
dropping from last year's 34.69% to 19.18% this year.

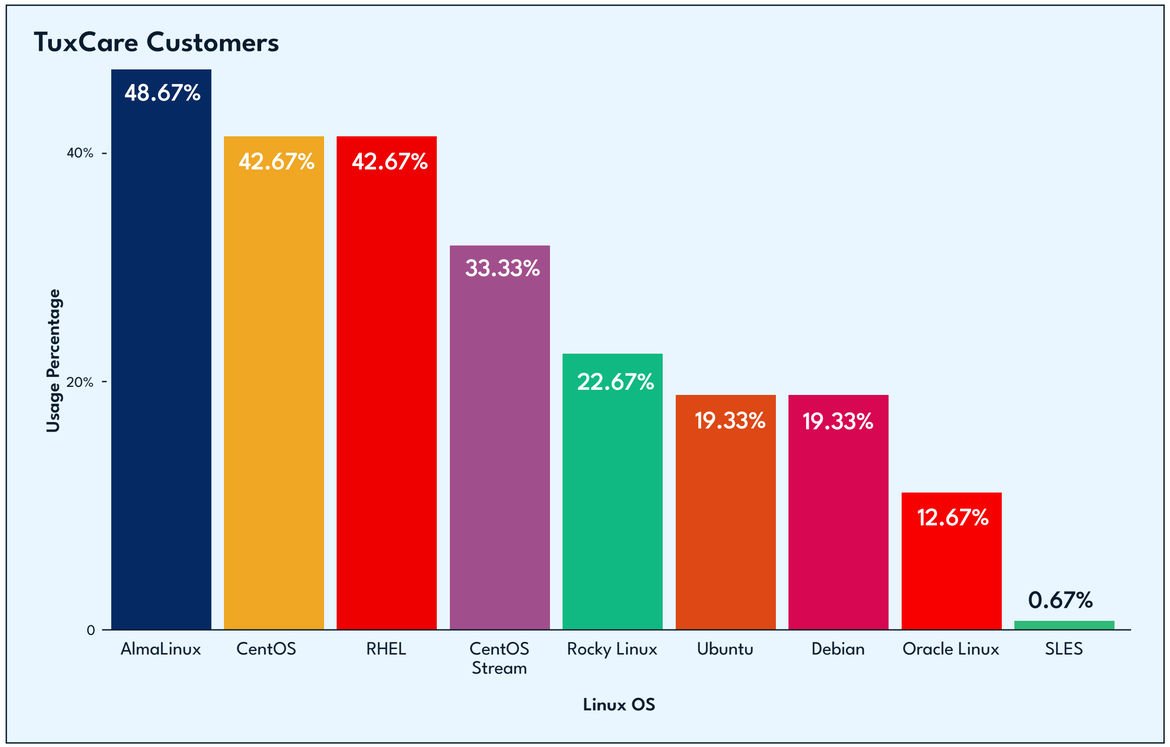
Oracle Linux usage has also remained largely the same
with 14.8% last year and 12.67% this year.

A closer look at Linux distribution usage

TuxCare customers made up about half of this year's survey respondents. Because TuxCare delivers enterprise support services for AlmaLinux and security patching for several distributions as well, the likelihood of some distributions being more popular among TuxCare customers is higher.

To prevent unwanted bias, we are showing the distribution usage data for both TuxCare customers and non-customers separately.





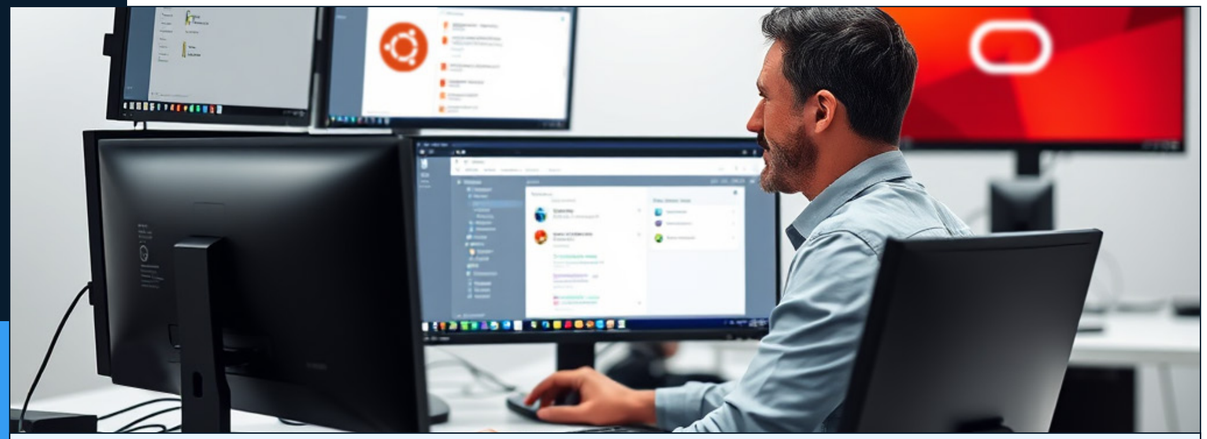
Multi-distro environments are prevalent

On average, enterprises work with

2.33
Linux distributions

...which is more than in the previous year.

Last year, the average number of Linux distributions being used simultaneously together was 1.97. The slight year-over-year increase could be attributed to a number of factors, but one likely explanation is the End of Life (EOL) of CentOS 7. For many organizations, this EOL shift compelled a migration to a non-CentOS Linux distribution, with some enterprises likely implementing multiple non-CentOS distributions to experiment with different options in their environment before making a final decision to commit to just one CentOS replacement.



A Growing Need for Multi-Distribution Security Tools?

Many Enterprise Linux distribution vendors offer security tools that are designed to work exclusively with their own distributions. However, our research indicates that organizations largely utilize more than one Enterprise Linux distribution, often across different ecosystems (one or more distributions within the RHEL ecosystems simultaneously alongside distributions outside of the RHEL ecosystem, for example).

This renders single-distribution tools insufficient for securing their entire Linux landscape. Thankfully, there are multi-distribution security solutions available that provide coverage across various distributions, regardless of whether they belong to the same distribution 'family.' As enterprises continue to diversify their Linux environments, it's likely that the demand for these multi-distribution security tools will increase.

The CentOS Sunset

What the End of Life (EOL) of stable CentOS means for enterprise users

With the end of support of CentOS 7 now behind us, enterprise users are now facing new challenges – and opportunities.

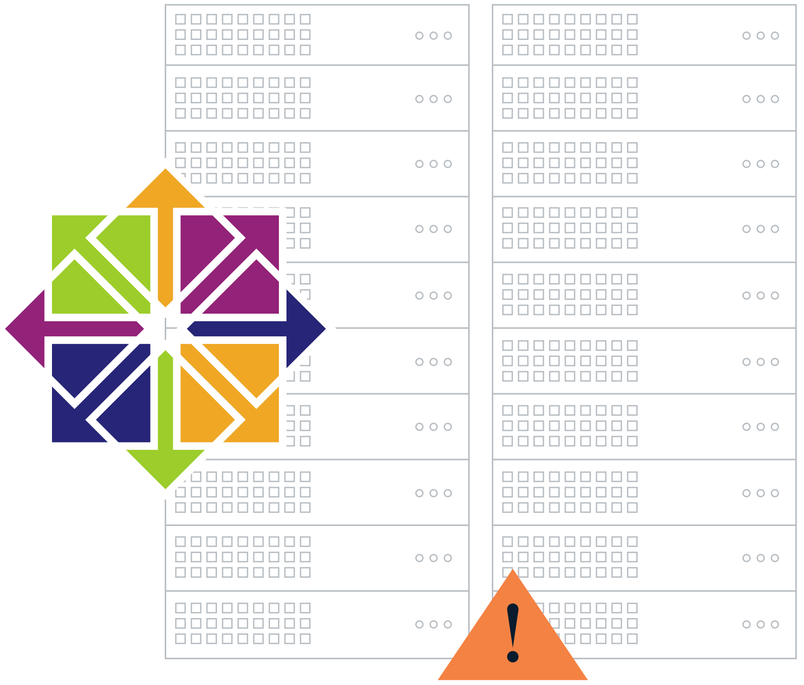
Originally launched in 2014, CentOS 7 has been a cornerstone in the architecture of numerous enterprises, boasting millions of installations worldwide. In June of 2024, security updates ceased for this distribution – which was the final stable version of CentOS.

This version's recent sunset not only highlights the need for continuous updates in technology strategies and the importance of selecting operating systems that have long-term viability, but also underscores the extensive reliance many organizations have on CentOS's stability, affordability, and compatibility.

This end-of-life shift also marks a critical pivot point for Enterprise Linux users globally. For the millions of users impacted, this cessation of security support signals a transition phase where strategic decisions must be made to maintain system security and efficiency.

In order to avoid the risk of continuing to use an unsupported OS, CentOS users have been compelled to choose among upgrading to the latest CentOS Stream (which offers rolling updates and is not appropriate for many organizations' needs), choosing another stable and supported Linux distribution, or getting extended security support from third-party vendors.

This shift is monumental in the Enterprise Linux community, affecting software deployment, security protocols, and – ultimately – business continuity planning. As organizations navigate this change, the collective movement represents one of the most significant shifts in Enterprise Linux usage in recent decades.



However, even beyond the end-of-life date of all versions of stable CentOS, there are still plenty of users currently working with it in their enterprise environments...

Most enterprise CentOS users today are working with CentOS 7

Meanwhile, about

50%

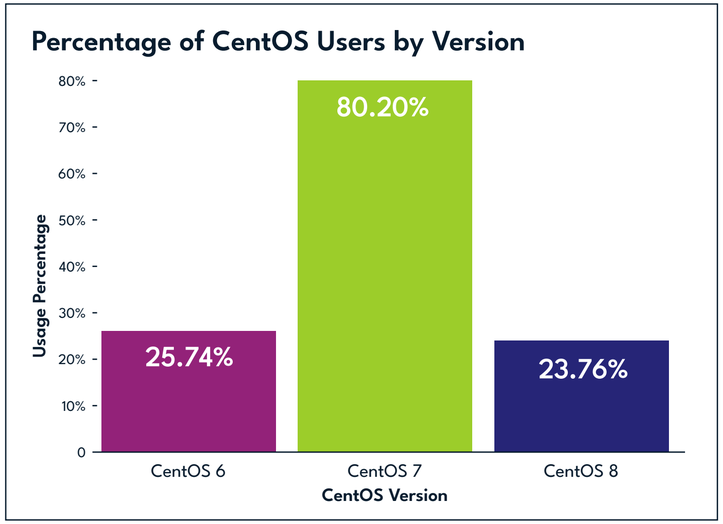
of CentOS users

are still working with versions that have been out of support for at least 3 years: **CentOS 6 and CentOS 8**

The share of CentOS users using versions 6 and 8 has remained constant year over year, only changing from 52% to 50% – indicating a likelihood that these users are in no rush to upgrade to a non-CentOS distribution that currently enjoys standard security support – either because they don't mind being at risk of vulnerability exploits or have arranged some type of long-term extended security option.

Why is CentOS 7 the most popular?

This is likely due to the fact that CentOS 7 is the stable CentOS distribution that has gone EOL most recently. Last year, CentOS 7 was also the most popular among the three, as it had not reached EOL yet at the time.



How are enterprise CentOS users staying secure when all stable versions have reached end of life?

CentOS users are either:

Carrying on without security updates, putting their systems at risk of vulnerability exploits

or

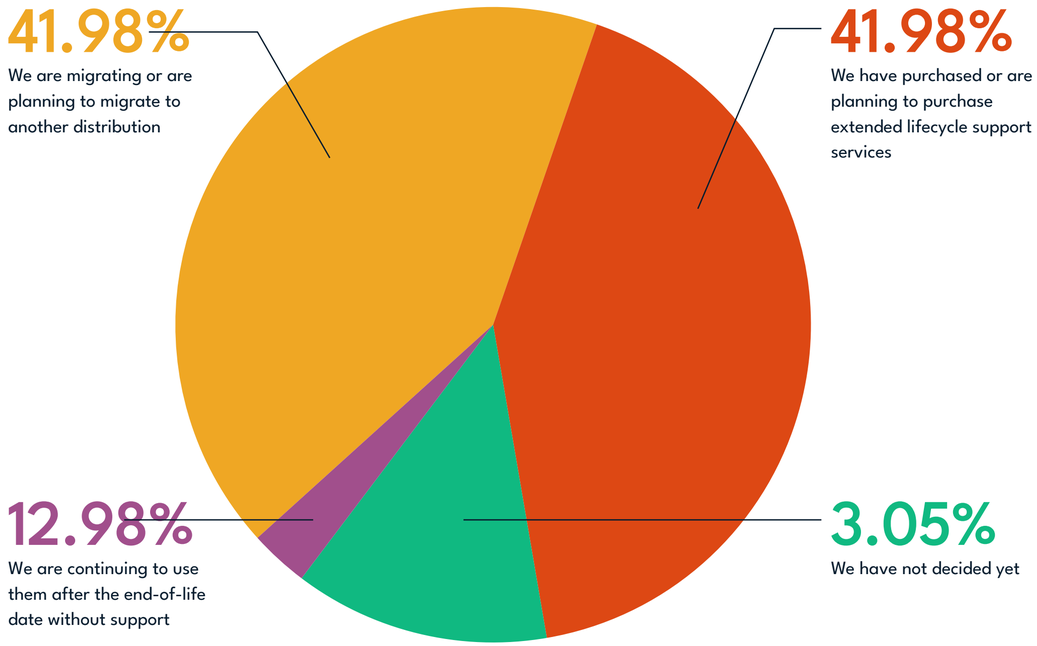
Continuing to receive security updates from a third-party extended support provider

Either way, many of these CentOS users are likely planning a migration to a currently-supported non-CentOS distribution.

This is not a rush for all users, as some extended support vendors deliver never-ending security updates, without time limits, so their customers can take as many years as they need to complete a migration without a looming end date attached to their extended support subscription.

For now, the vast majority of CentOS users' plans are evenly split between subscribing to long-term extended security support or migrating to a non-CentOS distribution

Plans for CentOS Systems



A troublingly high percentage

12.98%

of CentOS users plan on carrying on without any form of security support

– compared to 11.97% of users last year.

It's notable that organizations using CentOS without any security support are doing so despite the fact that there are **thousands of vulnerabilities that have been discovered in CentOS 6, 7, and 8 since they reached EOL.**

41.98%

are opting for extended lifecycle support services to maintain operations securely without immediate migration.

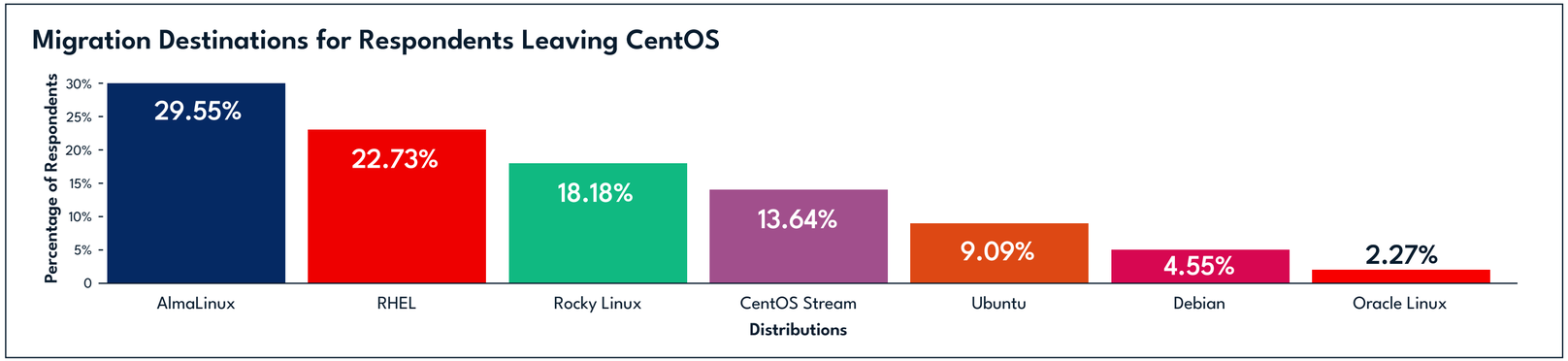
41.98%

of respondents plan to migrate from CentOS to other distributions.

There appears to have been a shift in favor towards CentOS alternatives – as only 20% of CentOS users from last year's survey indicated a plan to migrate to a non-CentOS distribution.

With nearly half of current CentOS 6, 7, and 8 users planning on migrating to a different Enterprise Linux distribution, where are they going?

The answer: overwhelmingly towards other distributions within the Red Hat Enterprise Linux (RHEL) ecosystem.



AlmaLinux emerged as the most popular choice, indicating its strong acceptance as a CentOS replacement, followed by Rocky Linux and RHEL.

RHEL Compatibility Appears to Have a Major Influence on Migration Decisions

Fewer CentOS users choosing options that aren't compatible with RHEL illuminates a distaste towards distributions outside the RHEL ecosystem. Switching to a Debian-based distribution, for example, may involve higher costs and disruptions, which is likely one of the reasons it's less popular.

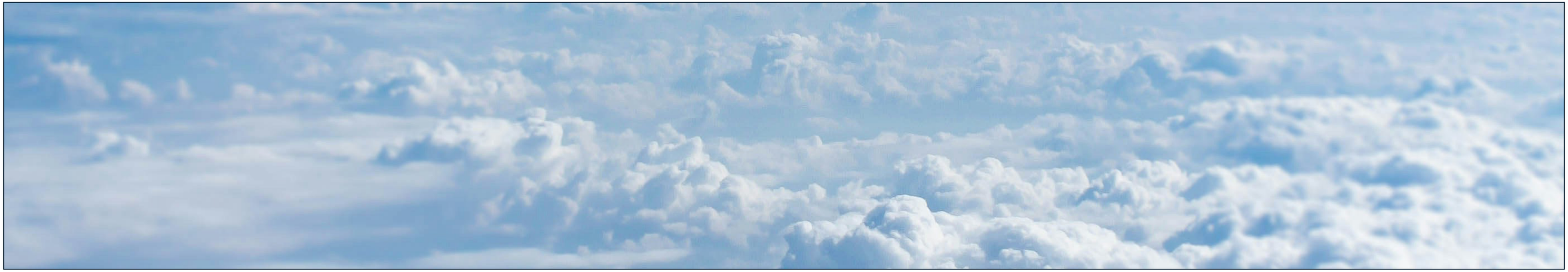
What is driving nearly a quarter of ex-CentOS users away from community-driven options?

It's clear that there's a significant preference for community-driven distributions that offer stability and familiarity, like AlmaLinux and Rocky Linux, but why are 22.73% of respondents moving to RHEL instead?

This may be explained by pre-existing agreements with RHEL, which were expanded to include previously-CentOS systems. However, there are a number of potentially false perceptions that could be leading to a preference for RHEL, like the idea that migrating from CentOS to RHEL is the "safest" route or a general lack of confidence in younger community-supported alternatives.

Additionally, former CentOS users may not be aware that community-supported options like AlmaLinux have commercial support services available from trusted third-party vendors that deliver an enterprise-grade experience similar to that of RHEL.

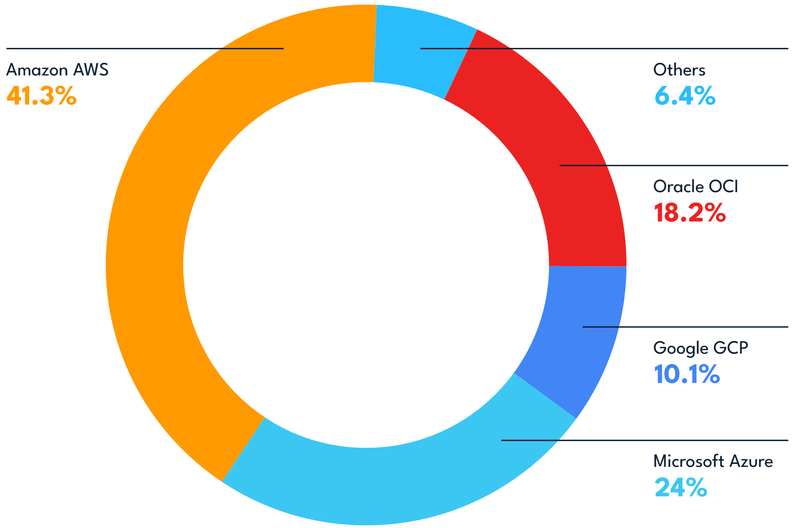
Even with these possibly incorrect perceptions, community-backed alternatives still account for the majority of the post-CentOS migrations reported.



Amazon AWS dominates among Cloud Service Providers for Linux-based systems

With Microsoft Azure taking second place with nearly a quarter of Enterprise Linux users reporting it as their preference.

Cloud Service Providers Usage for Linux-Based Systems



Some may find themselves surprised that Oracle OCI has won the favor of 12.8% - nearly a fifth - of survey respondents and the fact that **smaller providers have taken up such a significant share of Cloud Service Provider preferences among Enterprise Linux users.**

SECTION 2

Linux Patch & Vulnerability Management

- How many cybersecurity incidents are related to unpatched security vulnerabilities?
- What factors are slowing down vulnerability patches from being applied to Linux systems?
- How much time do organizations spend on coordinating and executing Linux server maintenance windows?
- How are organizations gauging the threat landscape?
- Which compliance regimes do organizations abide by?

Are enterprises improving their cybersecurity mitigation strategies?

While **fewer enterprises reported a cybersecurity incident in 2024** than in the previous year...

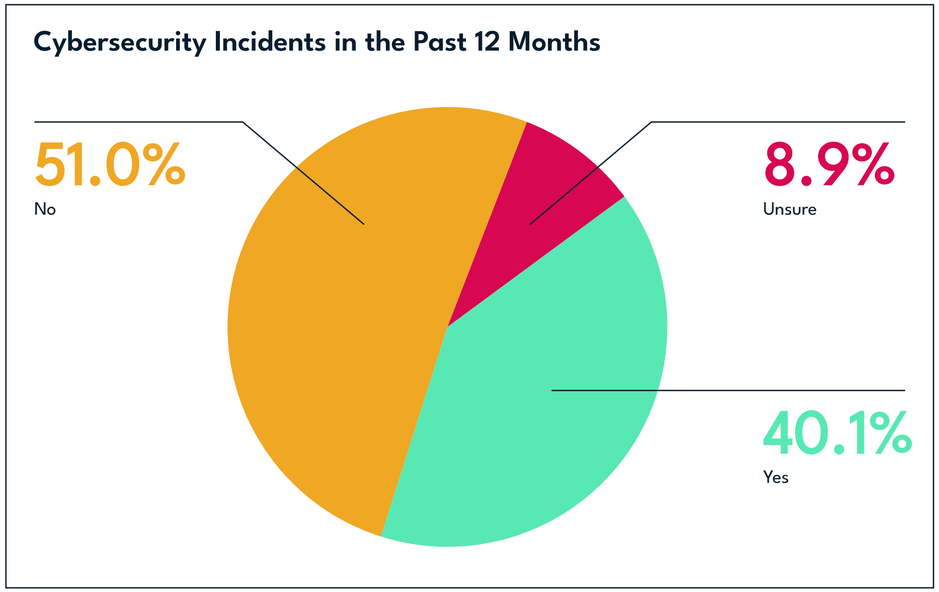
nearly half of the organizations surveyed experienced an incident.

40.1%

reported that they suffered an incident within the past 12 months, down from 50.93% in the previous year.

At the same time, more enterprises are reporting zero cybersecurity incidents

It appears that organizations have largely made positive progress in mitigating cybersecurity risk, as 51.0% of enterprises surveyed said that they did not experience an incident – up from 43.63% in the previous year.



However, uncertainty is (slightly) rising

The increase in uncertainty – from 5.43% last year to 8.9% this year – underscores the need for organizations to enhance their incident response and monitoring capabilities to ensure clarity.

Most cybersecurity incidents were linked to unapplied patches

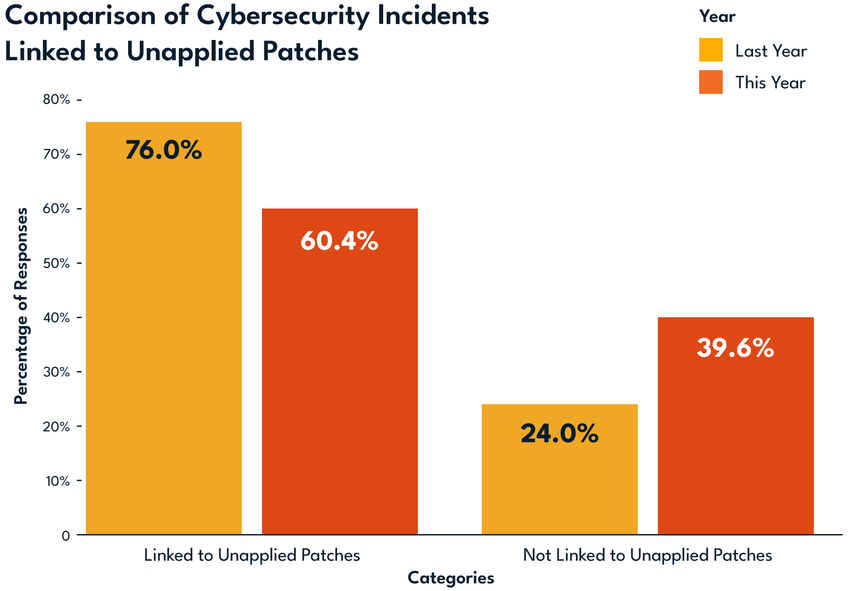
60.4% of incidents occurred while **a patch was available but was not applied.**

But cybersecurity incidents related to unapplied patches have decreased compared to last year:

in last year's report, 76% of incidents were linked to unapplied patches.

These trends indicate positive progress in patch management, but...

despite this year-over-year improvement, the fact that more than half of the reported cybersecurity incidents can be attributed to available-yet-unapplied patches shines a light on the fact that unapplied security patches remain a critical area of concern.



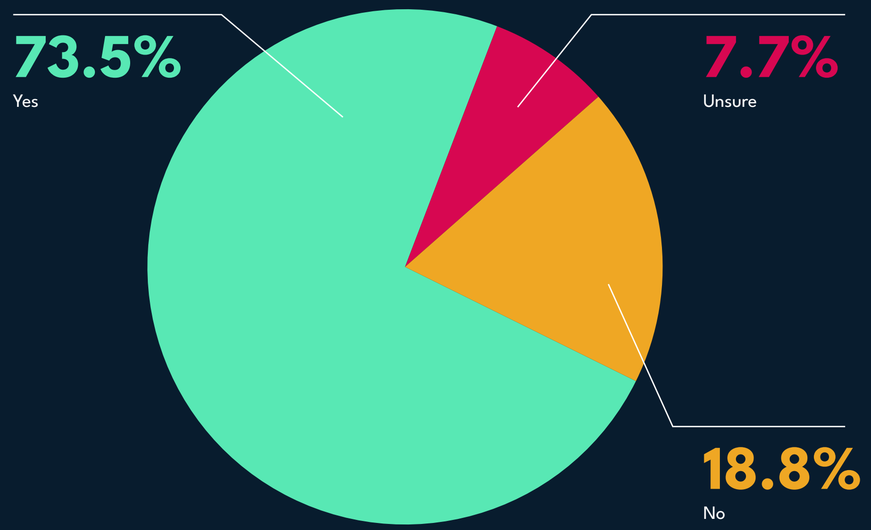
Continued efforts **in automating patch deployment, prioritizing patching processes, and enhancing patch visibility across teams** will be vital to further reducing this risk.

The vast majority of organizations that were impacted by a cybersecurity incident were already aware that they were vulnerable before the incident occurred

73.5%

of enterprises surveyed indicated that their company knew about their vulnerability exposure before the cyberattack occurred.

Awareness of Vulnerability Prior to Cybersecurity Incident



Even though they were aware of their vulnerabilities, these organizations still suffered cybersecurity incidents – highlighting a critical need for enterprises to move faster to mitigate new vulnerabilities in their systems as they appear rather than provide threat actors enough time to exploit them. There is an inertia in proactively addressing known vulnerabilities that both feeds and is fed by the "it won't happen to me" mindset.

The large share of organizations that were knowledgeable of vulnerabilities yet still suffered incidents shines a light on the challenges in cybersecurity management and the need for faster and more proactive approaches.

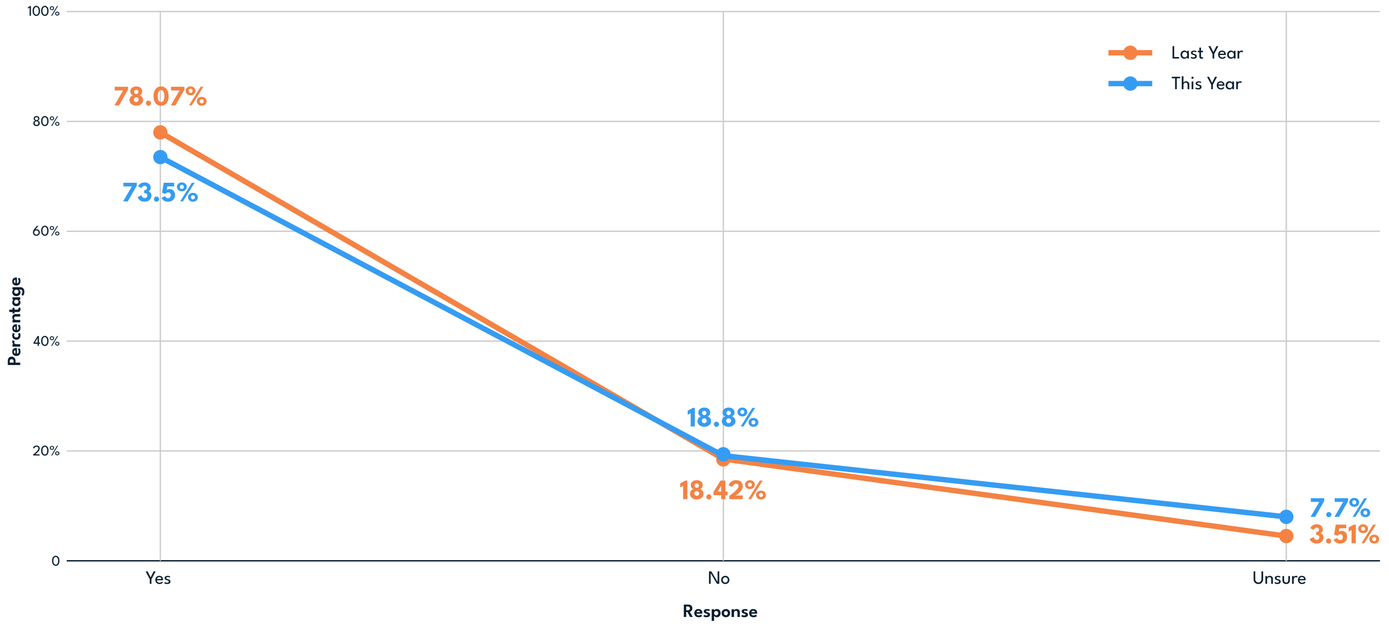
18.8%

reported that their organization was not aware of the vulnerability before the incident

....potentially as a result of a lack of effective monitoring and risk assessment practices.

Enterprises haven’t gotten much better (or worse) when it comes to awareness of their vulnerabilities before cybersecurity incidents occur

If we compare vulnerability awareness with last year's results we can see that the trend mostly remains the same.



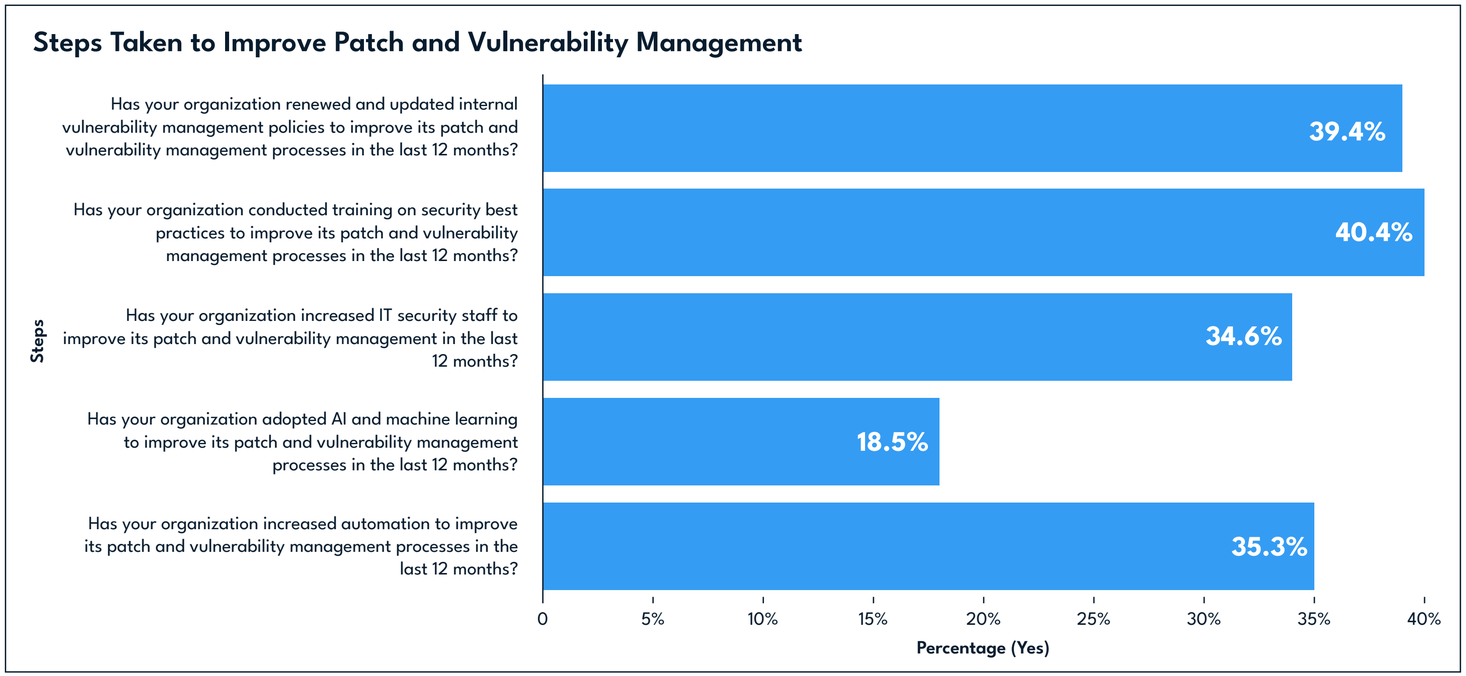
A decline in proactive monitoring or confidence in identifying vulnerabilities may explain the slight drop in awareness since last year.	**Fundamental issues in monitoring and risk assessment remain unresolved,** demonstrated by the consistent percentage of organizations unaware of their vulnerabilities year over year.	**Uncertainty about the exposure to vulnerabilities grew slightly,** reflecting a lower level of confidence on the security of their environments.	**Organizations likely need to strengthen communication and understanding of vulnerabilities** among stakeholders to halt the rise in uncertainty.

To improve patch and vulnerability management, organizations tend to focus on training and policy updates rather than AI

When asked what steps their company took to improve its patch and vulnerability management processes in the last 12 months,

the most common response was conducting training on security best practices followed by **reviewing and updating internal vulnerability management policies.**

(likely due to their lower implementation cost and higher immediate impact).



Adopting AI and machine learning is the least popular method of improving patch and vulnerability management

with only 18.5% of organizations surveyed utilizing this approach – indicating either a **lack of resources, expertise, or trust in these technologies. As you'll see in the AI section of this report, there has been a shift in expectations vs. tangible results from the use of AI over the past year.**

However, AI's lack of popularity today lays the groundwork for a potential growth area in improving automation and predictive security measures in patch management processes down the line.

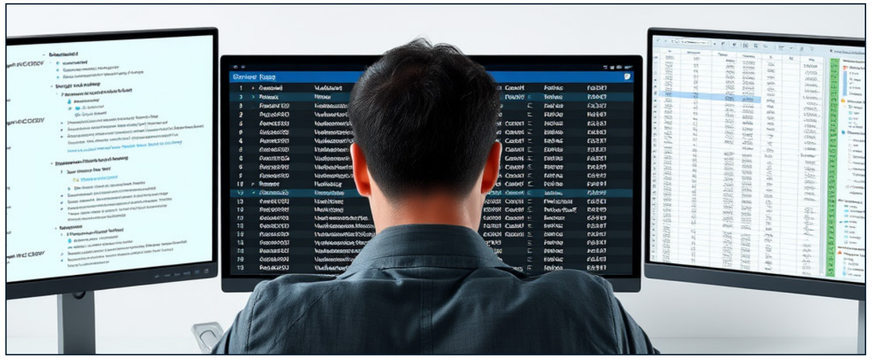
Managing the vulnerability patching process with emails and spreadsheets is slowing down remediation

Among the biggest factors causing delays in the vulnerability patching process, the top factor was communication using emails and spreadsheets – indicating a clear need for more modern and integrated tools to manage patching workflows.

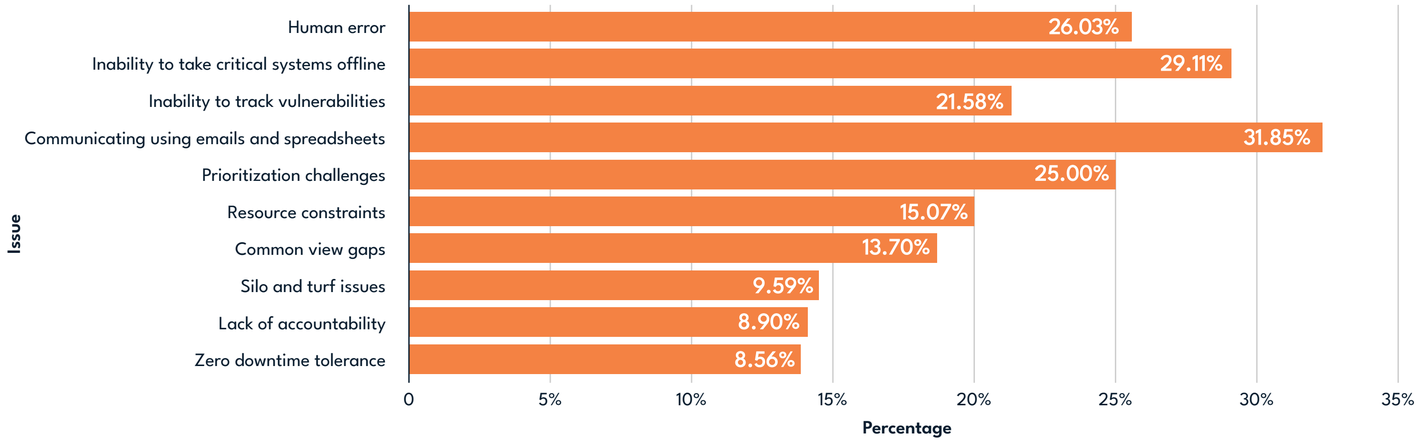
The need for constant uptime is causing patch delays as well

Nearly a third of organizations' vulnerability patches are being slowed down by an inability to take critical systems offline.

With 29.1% of organizations reporting this issue, there is clearly a commonly-shared challenge in balancing operational uptime with timely patching workflows.



Percentage of Issues Causing Delays in Vulnerability Patching



Human error (26.0%) and **prioritization challenges** (25.0%) both contribute significantly to delays as well, pointing to **potential gaps in process efficiency and training**.

Inability to track whether vulnerabilities are being patched in a timely manner affects 21.6% of users, showing a **lack of effective monitoring and reporting mechanisms.**

How Organizations Can Minimize Vulnerability Patch Delays

With the knowledge that communication using emails and spreadsheets, an inability to take critical systems offline, human error, and an inability to track vulnerabilities are the primary factors causing vulnerability patch delays, organizations can take measured steps to mitigate these challenges and accelerate their vulnerability patch workflows.

Adopt Automation

Reducing reliance on manual processes like emails and spreadsheets can streamline workflows and minimize delays.

Improve Downtime Strategies

Organizations should explore rebootless patching or other modern patch management solutions to reduce the impact of system downtime.

Enhance Training

Address human errors through continuous cybersecurity training across the organization.

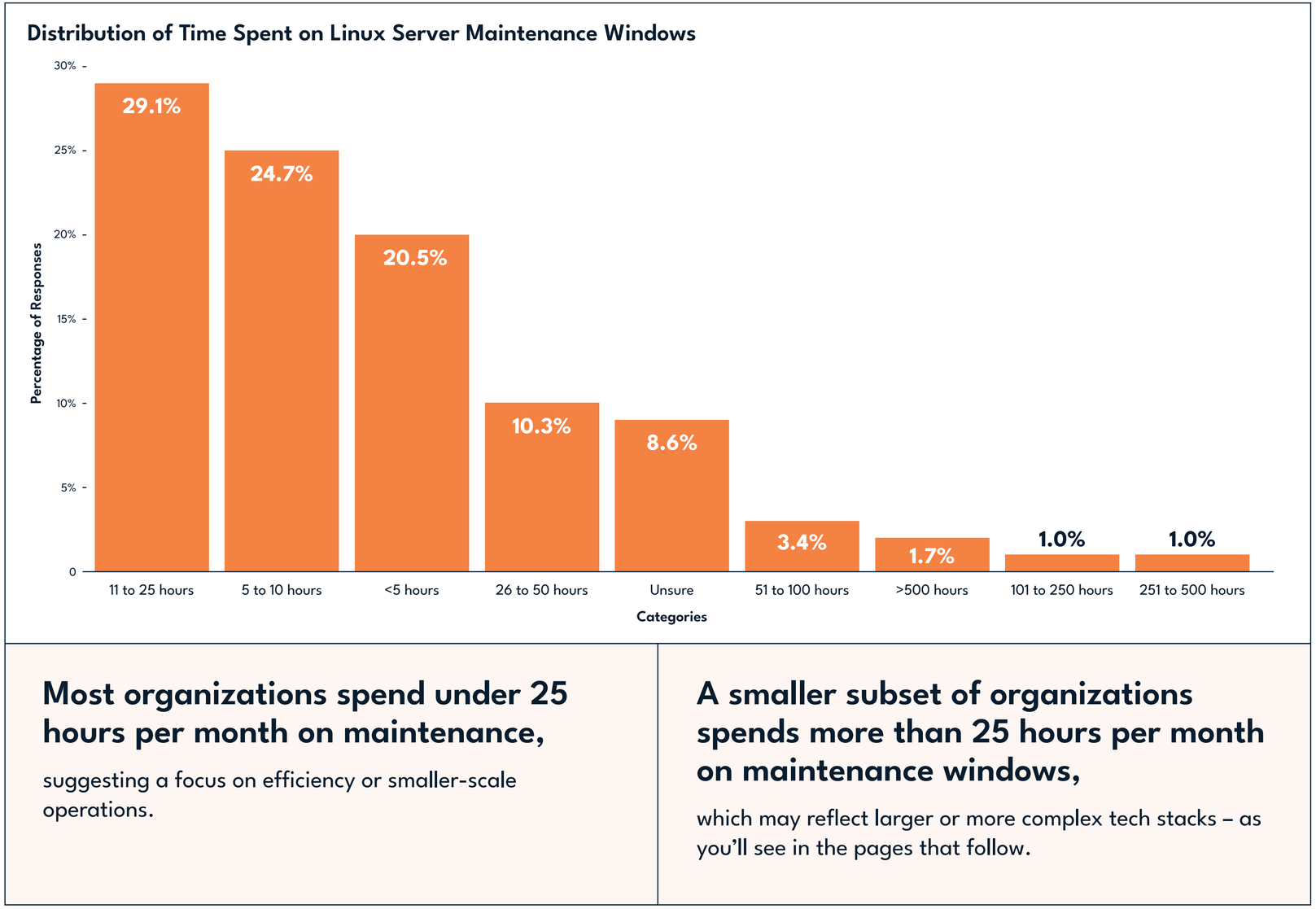
Invest in Monitoring Tools

Implement the right tools that are proven to provide real-time tracking of patch status and prioritization.

Nearly a third of organizations that rely on Enterprise Linux spend

11 to 25 hours per month

on coordinating and executing maintenance windows.



Most organizations spend under 25 hours per month on maintenance,

suggesting a focus on efficiency or smaller-scale operations.

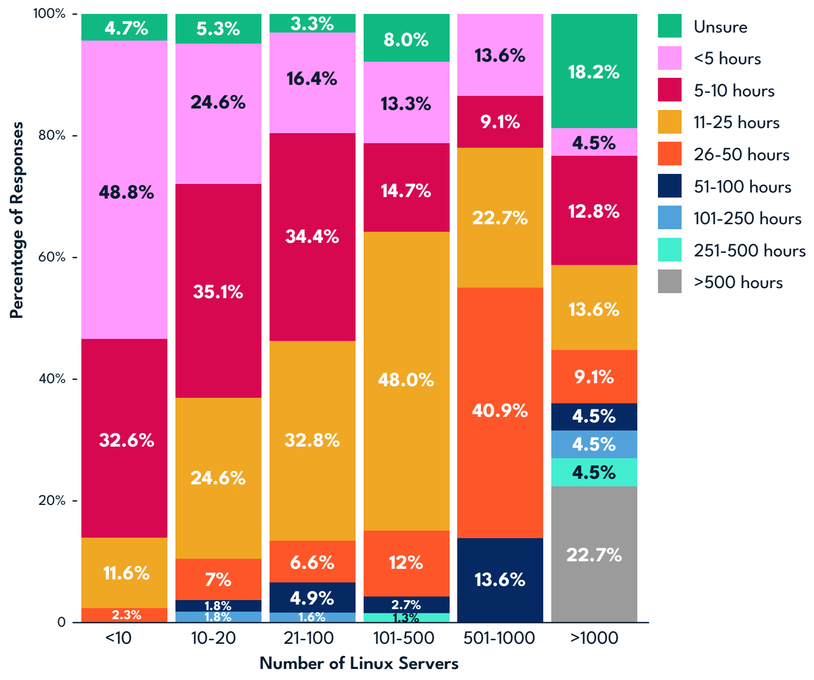
A smaller subset of organizations spends more than 25 hours per month on maintenance windows,

which may reflect larger or more complex tech stacks – as you'll see in the pages that follow.

The more Linux servers an organization is running, the more time they spend on coordinating and executing maintenance windows

Here we can see the time spent each month on maintenance windows as it varies by infrastructure size:

Distribution of Maintenance Time Across Number of Linux Servers



Time Spent on Maintenance Windows

Micro Organizations (<10 Linux servers)

- These organizations report the lowest maintenance times, with nearly **48.8% spending less than 5 hours per month on Linux server maintenance**.
- A smaller percentage (11.6%) spend **"11 to 25 hours"**, likely reflecting simpler infrastructures.

Small Organizations (10-20 servers)

- The majority spend **"5 to 10 hours" (35.1%)**, followed by **"11 to 25 hours" (24.6%)** on maintenance operations.
- These organizations demonstrate more varied maintenance time distributions due to slightly increased complexity.

Medium-Sized Organizations (21-100 servers)

- These organizations show a wider distribution of maintenance times, with **32.8% spending "11 to 25 hours"** and **34.4% spending "5 to 10 hours."**
- A smaller portion spends more time on maintenance operations, such as **26 to 50 hours (6.6%)**.

Mid-Large Organizations (100-500 servers)

- The dominant category is **"11 to 25 hours" (48%)**, reflecting significant time investment for maintenance.
- Some organizations in this group also report **"26 to 50 hours" (12%)**, highlighting increased maintenance challenges as enterprises grow out of the medium-sized category.

Large Organizations (501-1,000 servers)

- These organizations report the highest percentage of maintenance time in the **"26 to 50 hours" category (40.9%)**, reflecting the complexity of managing large-scale infrastructures.
- A small portion experiences longer maintenance times, with **13.6% in the "51 to 100 hours" category** – the largest share in this category across all infrastructure sizes.

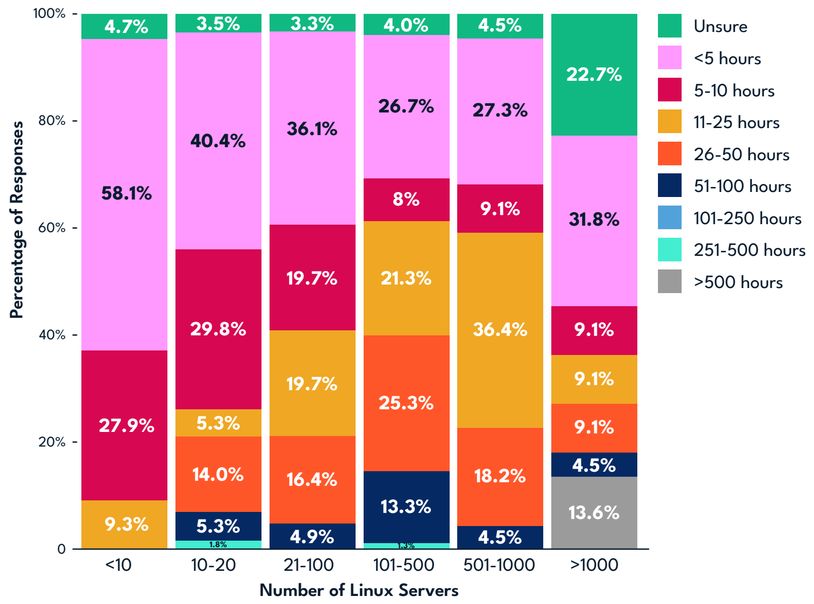
Until an organization reaches 1,000 servers, maintenance time scales in a predictable manner.

After 1,000 servers, maintenance time jumps significantly, with a large portion of organizations reporting extreme (>500-hour) maintenance efforts. This suggests that, at this scale, managing servers becomes increasingly complex despite automation.

For micro-to-small-organizations, downtime tends to last for shorter stretches of time.

However, server count does not have a strong correlation to downtime across the board – though larger organizations appear to face challenges in reducing downtime effectively despite reporting diverse ranges of downtime.

Distribution of Downtime Hours by Number of Linux Servers



Time Spent on Downtime Hours

Micro Organizations (<10 Linux servers)

- The majority **(58.1%)** experience **less than 5 hours** of downtime, with **27.9%** reporting **5 to 10 hours**, reflecting simpler infrastructure and efficient processes.
- There is minimal representation in higher downtime categories.

Small Organizations (10-20 servers)

- A significant proportion **(40.4%)** report less than **5 hours of downtime**.
- However, **29.8%** report **5 to 10 hours**, and **14.0%** experience **26 to 50 hours**, indicating increased maintenance complexity.

Medium-Sized Organizations (21-100 servers)

- About **36.1%** experience **less than 5 hours** of downtime, while **19.7%** report **5 to 10 hours**.
- Higher downtime levels, such as **11 to 25 hours (19.7%)** and **26 to 50 hours (16.4%)**, are more frequent.

Mid-Large Organizations (100-500 servers)

- Downtime is distributed evenly across categories:
  - **26.7%** report **less than 5 hours**,
  - **21.3%** report **11 to 25 hours**, and
  - **25.3%** report **26 to 50 hours**, reflecting increasing complexity.

Large Organizations (501-1,000 servers)

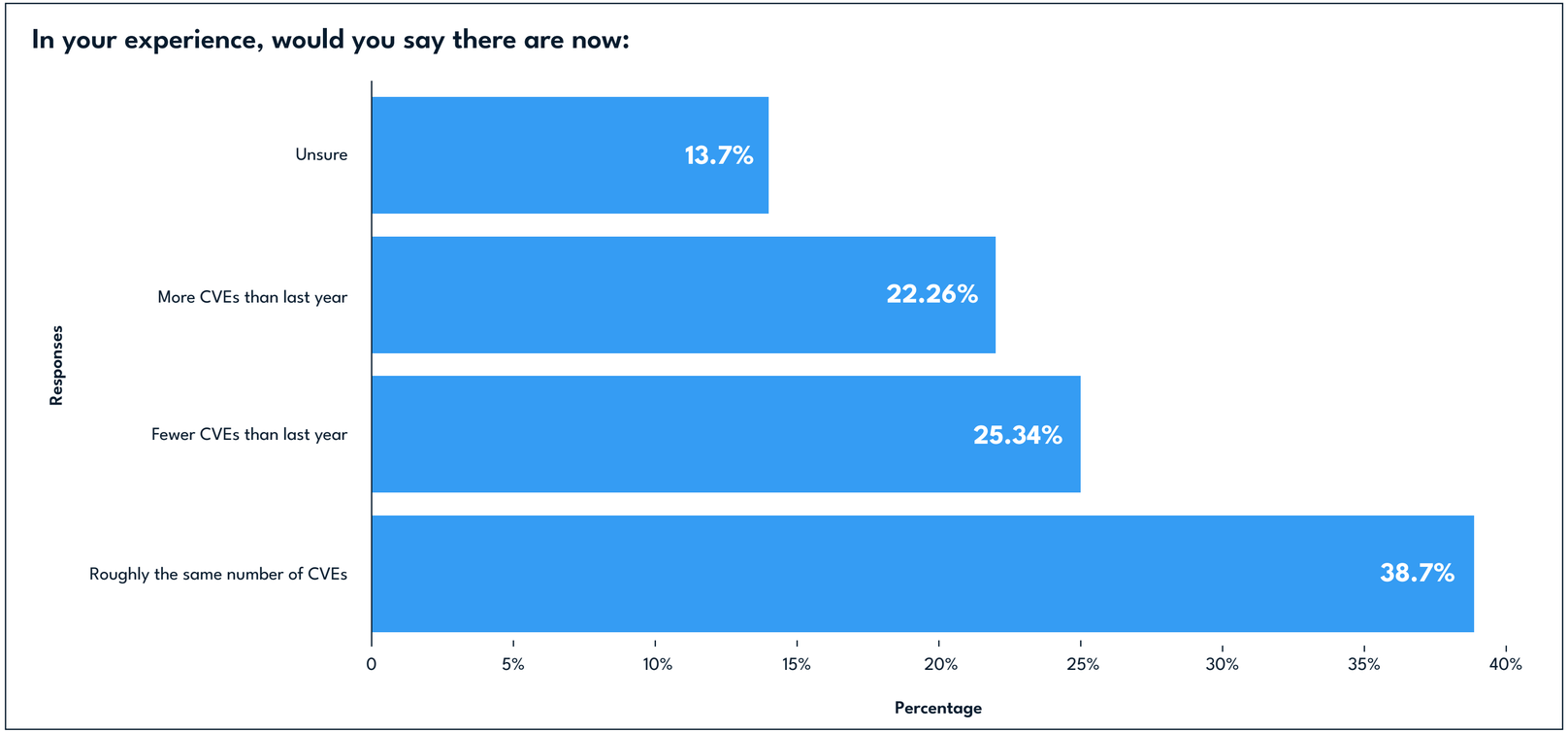
- Downtime spans multiple categories:
  - **27.3%** report **less than 5 hours**, and
  - **36.4%** experience **11 to 25 hours**.
  - **18.2%** report **26 to 50 hours**, highlighting challenges with large-scale maintenance.

Very Large Organizations (>1000 servers)

- The 13% of respondents in this category report having **>500 hours** of downtime which is a significant outlier compared to other server size categories. Very Larger Organizations likely face significant challenges in managing downtime due to the scale of their operations. Coordinating and executing maintenance at this level can be extremely time-intensive. At the same time, these organizations can still achieve a higher percentage of uptime than smaller organizations, as they are more likely to have more robust high availability options to sustain their operations.

Enterprises largely appear to believe that the inflow of CVEs is relatively stable

The vast majority of organizations believe that there were either fewer CVEs or about the same amount of CVEs impacting their Linux systems compared to last year.



Many organizations find themselves more threatened than last year

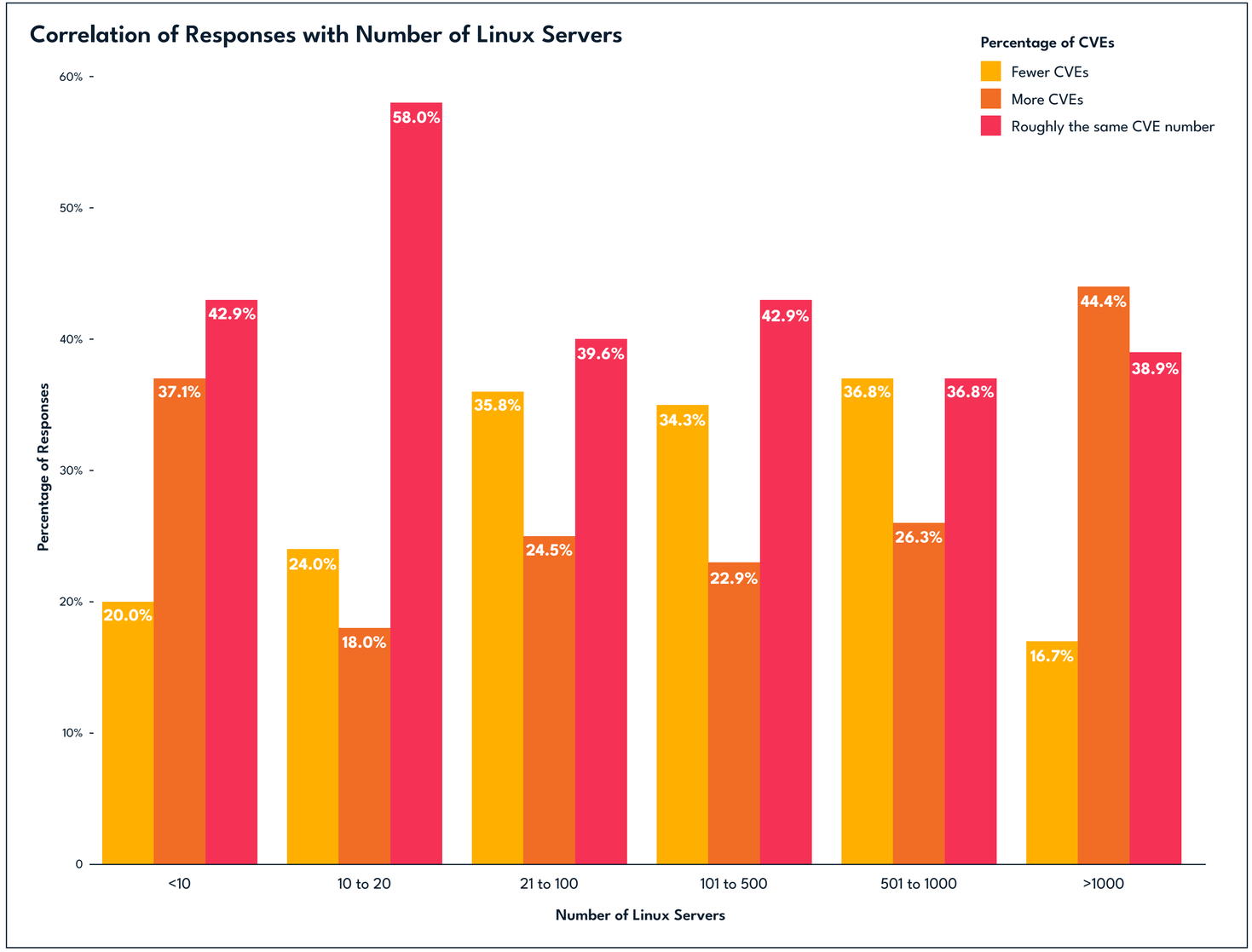
22.3% of enterprises reported more CVEs compared to last year, indicating concern from nearly a quarter of organizations regarding increasing threats or vulnerabilities in their systems.

A minority of organizations are uncertain

13.7% of respondents were unsure about the trend, possibly reflecting a lack of monitoring, awareness, or available data regarding CVEs.

Smaller organizations seem to perceive a greater increase in vulnerabilities compared to last year...

which could point to resource limitations or challenges in vulnerability management. However, this trend could also stem from the significant impact of individual vulnerabilities within smaller environments. At the same time, organizations with over 1,000 servers report the highest perception of increased vulnerabilities (44.4%). This is likely due to their expansive infrastructure, greater exposure to potential risks, and advanced monitoring systems that allow them to identify and track more vulnerabilities.



Which organizations were right?

22.26%

of organizations whose responses indicated that there are more CVEs than last year are correct.

The Reality: Vulnerabilities grew by an estimated 25% in 2024

In just the first three quarters of 2024, the number of CVEs had already grown beyond the number of CVEs for the entire previous year.

The difference is even greater depending on where you zoom in:

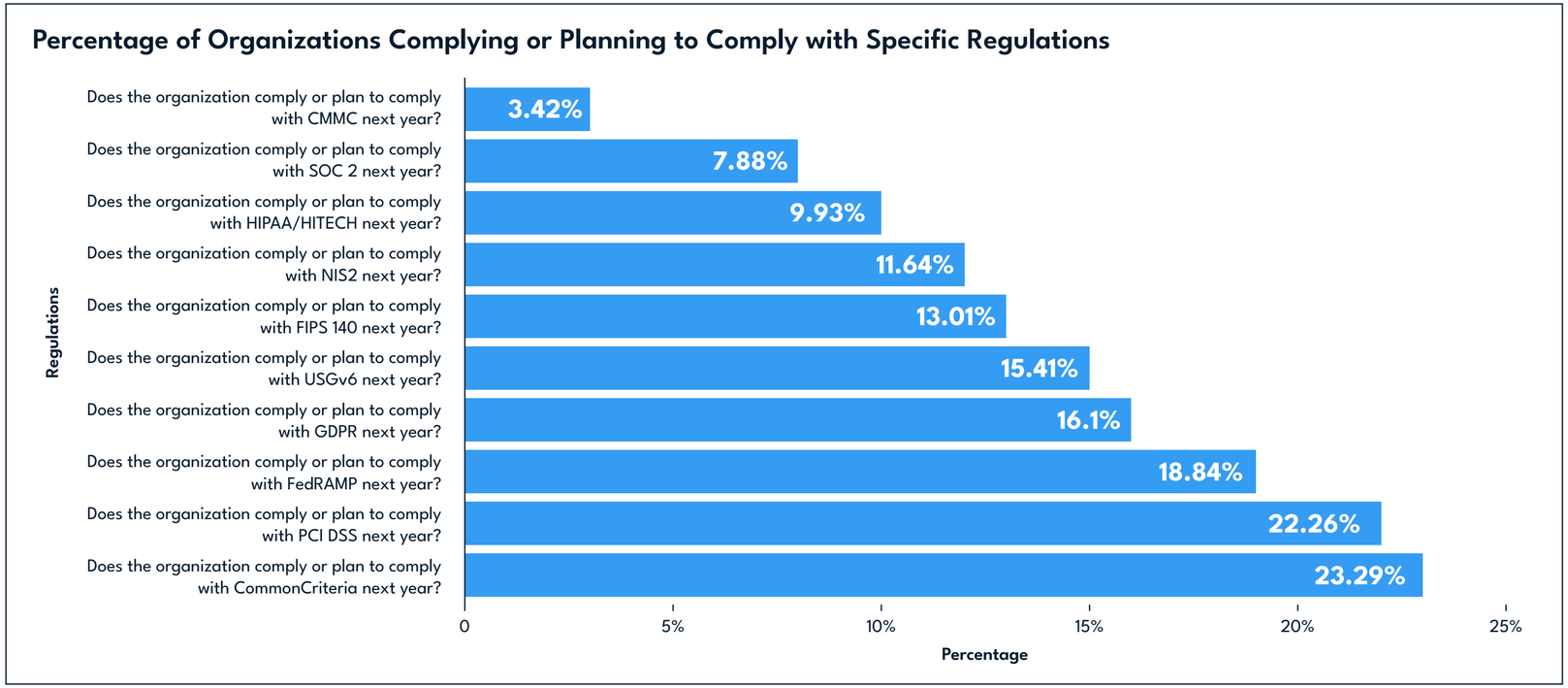
As an example, in the Linux Kernel alone, CVEs grew from 290 in 2023 to 3559 in 2024, which is about 12x more vulnerabilities.

With less than a quarter of enterprises surveyed correctly acknowledging that CVEs have grown year over year, we have a remarkable disparity between reality and awareness that may be hiding bigger issues for the IT industry.

SOURCE: https://www.cve.org/about/Metrics, https://stack.watch/product/linux/linux-kernel/

Organizations are more likely to seek compliance with CommonCriteria, PCI DSS, and FedRAMP compared to other compliance regimes.

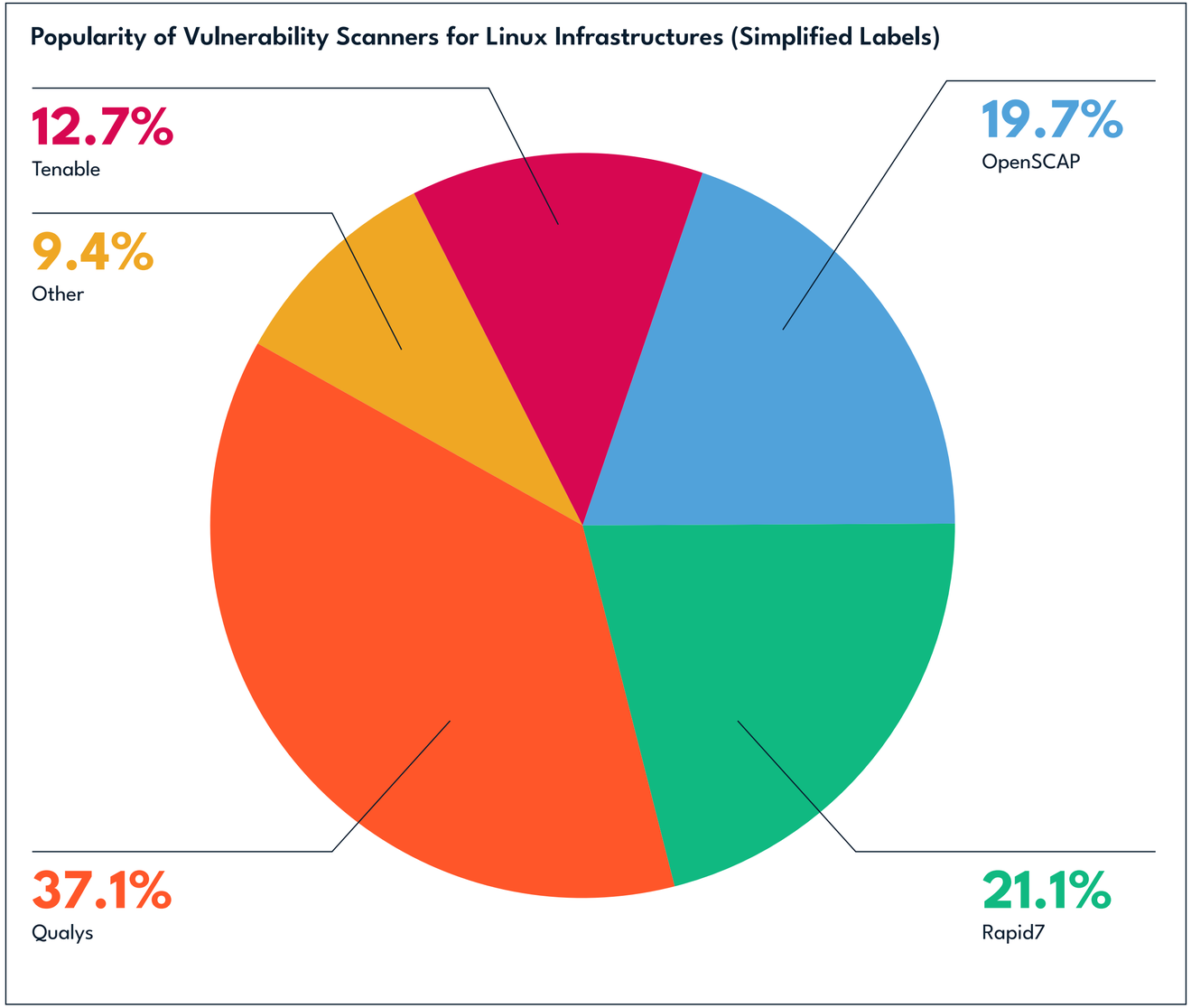
When asked which compliance regimes they plan to comply with, organizations named the following as their priorities:



Enterprises appear to be the least interested in complying with CMMC.

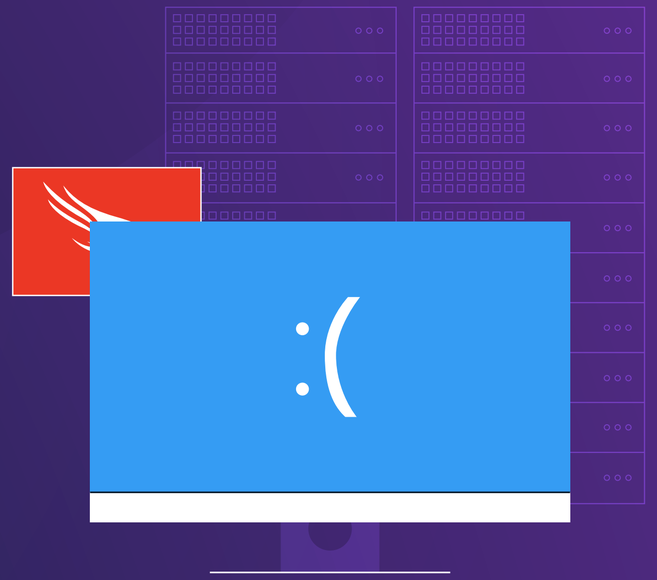
Qualys is the most popular vulnerability scanner, with Rapid7 and OpenSCAP close behind

The graph illustrates the relative popularity of vulnerability scanners used for Linux infrastructures, highlighting the percentage of organizations that utilize each tool. Qualys leads as the most widely adopted scanner, followed by Rapid7 and OpenSCAP, which show moderate usage levels. Tenable, while still in use, represents the least popular option among the analyzed tools.



SECTION 3

The CrowdStrike Incident

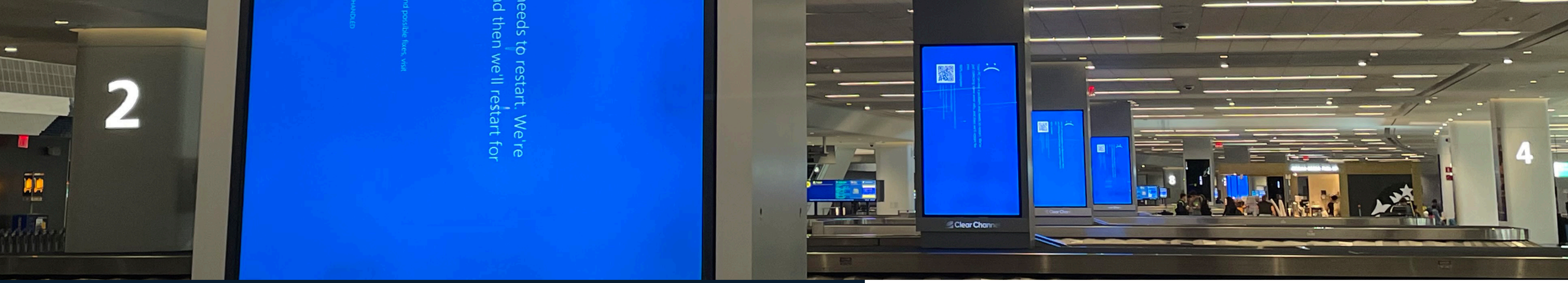


The CrowdStrike incident of July 2024 had a profound and multifaceted impact on enterprises globally.

The outage originated from a flawed software update pushed by CrowdStrike to its Falcon endpoint security software, affecting millions of devices and disrupting operations across numerous sectors, from government services to international logistics networks. Notably, the financial impact on Fortune 500 companies was substantial, with direct losses estimated at $5.4 billion, excluding broader economic effects like reputational damage or delayed operations.

While the issue affected Windows-based systems, due to the nature of modern IT infrastructure, where mixed Windows and Linux environments are commonplace, operations were disrupted across many interconnected systems outside the ones directly impacted. The nature of the disruption prevented remote recovery operations and laid bare the reliance on outdated management practices, but, at its source, there was an inability to properly test the update prior to large-scale deployment.

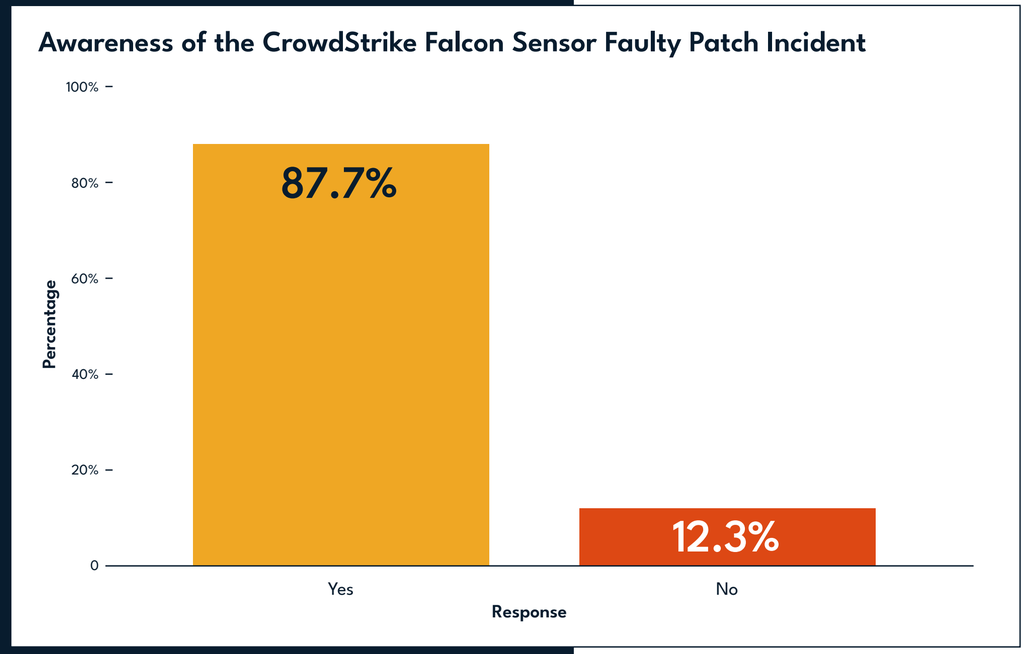
This gap in the test process for a particular update was a signal for organizations worldwide, causing process change, raising awareness to diversifying security providers, and enhancing update management processes to avoid similar large-scale disruptions. In an ironic twist of fate, an update to a well-known security software caused the most damaging and far reaching IT outage in history.



Very few Enterprise Linux users were unaware of the CrowdStrike incident

87.7%

of survey respondents knew about the incident caused by the CrowdStrike Falcon sensor faulty patch (Channel File 291).

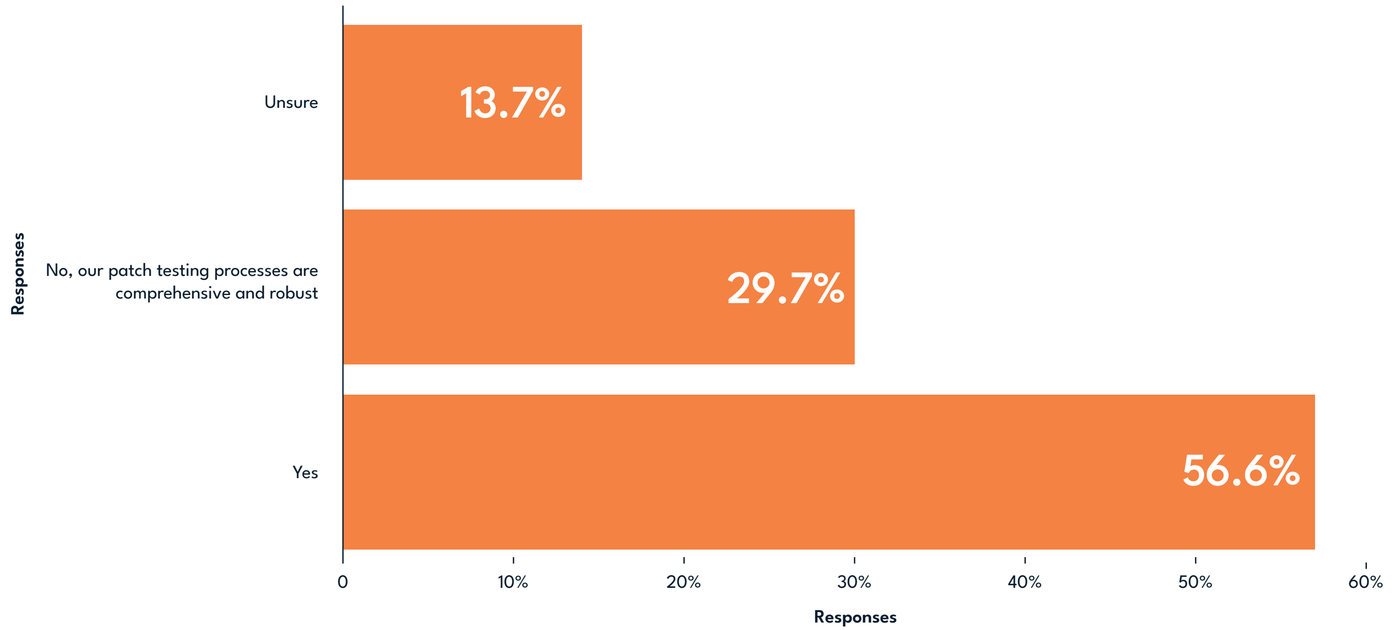


The high level of awareness suggests that the issue gained considerable visibility across organizations of all sizes in various industries, likely due to its impact and widespread reporting.

Impactful, widely-publicized incidents appear to have an influence on organizational practices

The CrowdStrike incident served as a wake-up call

Over half of organizations reviewed their patch-testing methodology as a direct result of the incident.



Almost a third of organizations are confident in their existing processes

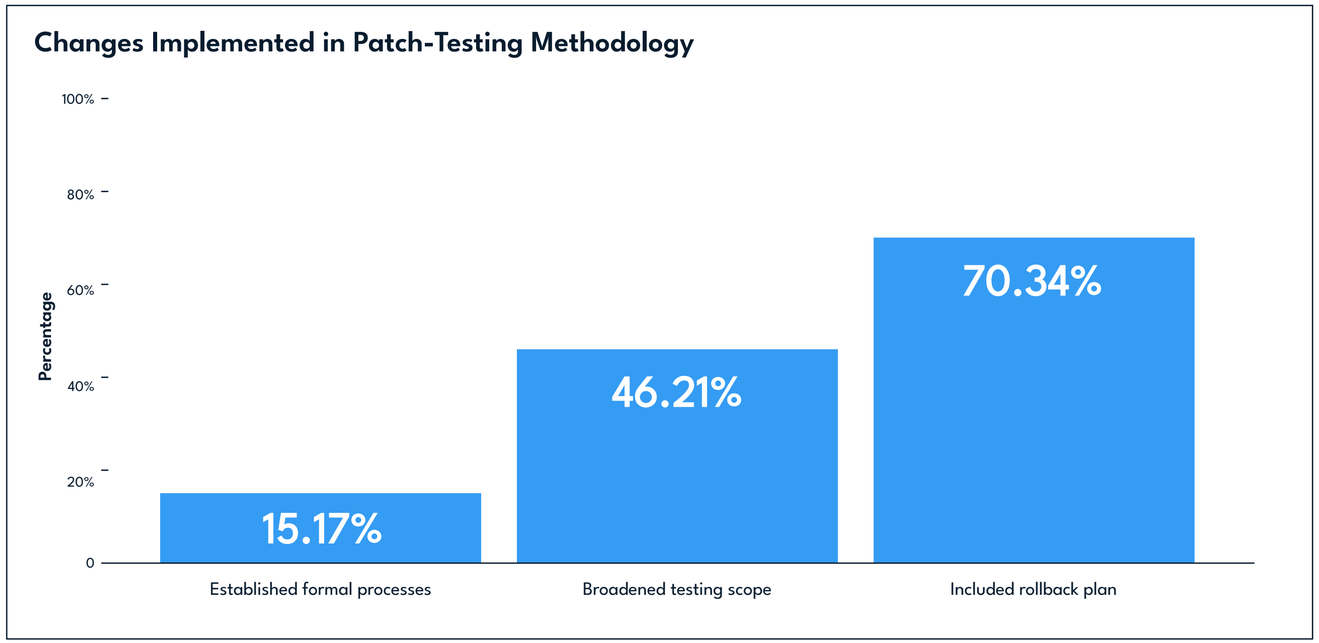
29.7% stated that their patch-testing processes were already comprehensive, suggesting that a significant number of companies had robust systems in place prior to the incident.

However, a gap in awareness remains

A small slice of the survey population – **13.7%** – were unsure if the incident caused a review, indicating potential gaps in communication or awareness within these companies regarding their patch-testing practices.

The CrowdStrike incident inspired an uptake of patch rollback plans

and, to a lesser extent, a broadening of patch testing scope



From the changes implemented as a result of the incident, we can gather that:

Contingency planning is critical in managing patch risks

For organizations who reviewed their patch-testing methodology as a direct result of the CrowdStrike incident, including a patch rollback plan was the most popular change – with **70.34%** identifying it as a change they've implemented.

There has been a shift toward more comprehensive testing of patches

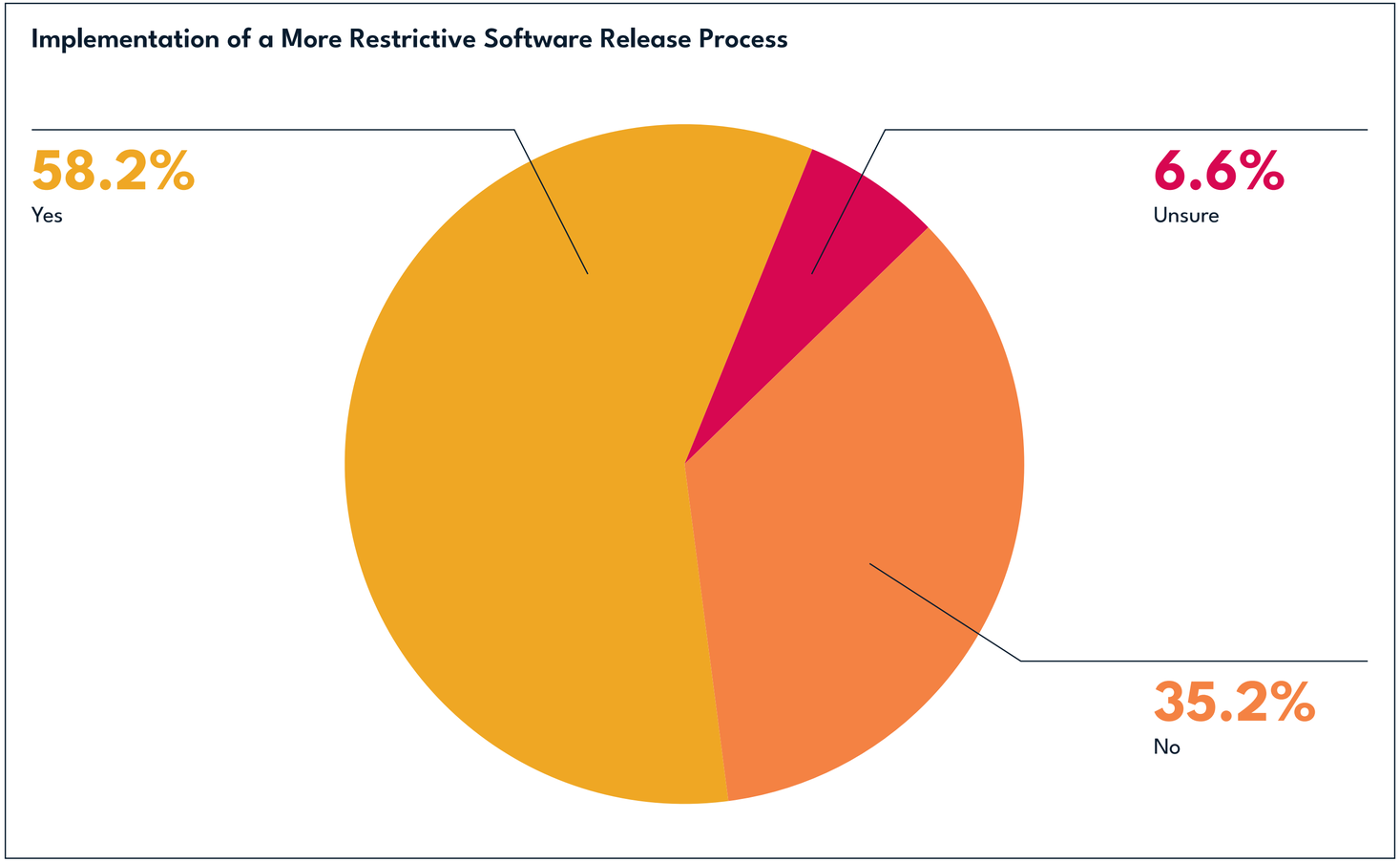
46.21% – almost half – of survey respondents indicated that they decided to broaden their patch testing scope as a result of the incident.

Formal patch testing processes were probably already widespread before the incident

Only **15.17%** of organizations chose to establish a formal patch-testing process after the incident, suggesting that many may already have a structured process in place or prioritize incremental adjustments instead.

The CrowdStrike incident led to wide-scale implementation of more restrictive software release processes

According to our survey respondents, the incident acted as a catalyst for a majority of organizations to reevaluate and tighten their release processes, illuminating a trend toward more robust security measures.



Those who did not implement a more restrictive software release process (35.2% of respondents) **may have already had a robust software release process in place.**

Many organizations rely on manual validation to ensure software security and reliability

When it comes to improving software releases post-CrowdStrike incident, the most popular pathway – reported by 59.73% of survey respondents – was expanding the scope of manual testing. This suggests that there remains a significant reliance on thorough manual checks in software release processes.

Larger testing environments are helpful in identifying potential issues

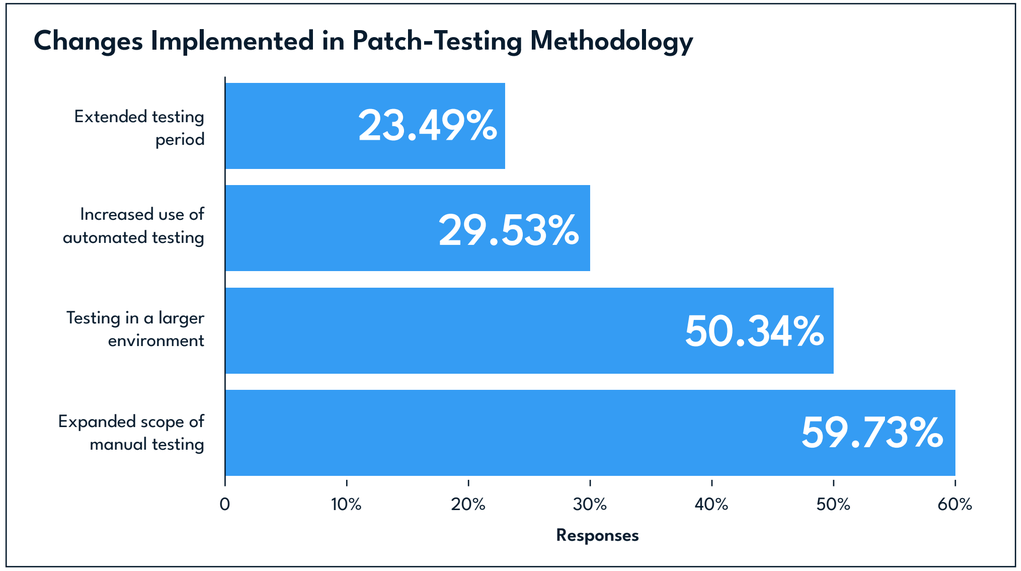
50.34% of organizations expanded their testing to a larger or more extensive environment, indicating the need for realistic testing scenarios to weed out possible problems.

Automated testing was the third most frequent change

29.53% increased their use of automated testing. However, it appears that manual testing and larger testing environments were seen as more immediate priorities. This may reflect the complementary nature of automated testing in tandem with manual testing workflows, which organizations use in combination rather than relying on just one approach.

Few organizations needed to prolong their testing period

Only 23.49% of respondents extended their testing period, possibly balancing time constraints with the need for comprehensive testing.



The changes highlight a focus on ensuring software quality through both manual and automated methods, as well as testing in realistic conditions. The relatively low adoption of extended testing periods might suggest organizational challenges like tight release schedules or resource constraints.

SECTION 4

Open-Source Supply Chain Security

The Enterprise Linux open-source supply chain comprises a diverse array of freely accessible and modifiable software tools, components, and libraries. Notable elements within this ecosystem include widely-used programming languages such as Java, Python, and PHP, alongside various libraries and packages that boost capabilities, like OpenSSL for enhanced security or Apache Struts for web application development. **However, this dependency on the open-source supply chain also presents distinct vulnerabilities.**

The public availability of the source code, while a boon to collaborative development, makes it easier for threat actors to analyze and infiltrate these open-source elements. Reliance upon compromised components could jeopardize numerous systems worldwide, positioning it as a prime target. The risks are amplified by the frequent incorporation of third-party dependencies in software development, which can trigger a domino effect of security issues affecting every application that utilizes the compromised component.

For enterprises, such vulnerabilities pose severe threats, potentially leading to data breaches, service interruptions, and diminished customer trust. Additionally, pinpointing and addressing these weaknesses becomes a formidable challenge due to the intricate network of transitive dependencies and the ongoing need for vigilance and software updates. Therefore, effectively managing risks associated with the open-source supply chain is essential for safeguarding the security and operational stability of enterprise Linux environments.

In this section:

- Are enterprises confident in the security of their open-source components?
- How do organizations handle patch management and updates for open-source components?
- What challenges do companies face in managing patches for open-source components?
- How have priorities and tactics in organizations' open-source supply chain security evolved over time?

High confidence is lacking when it comes to open-source component security

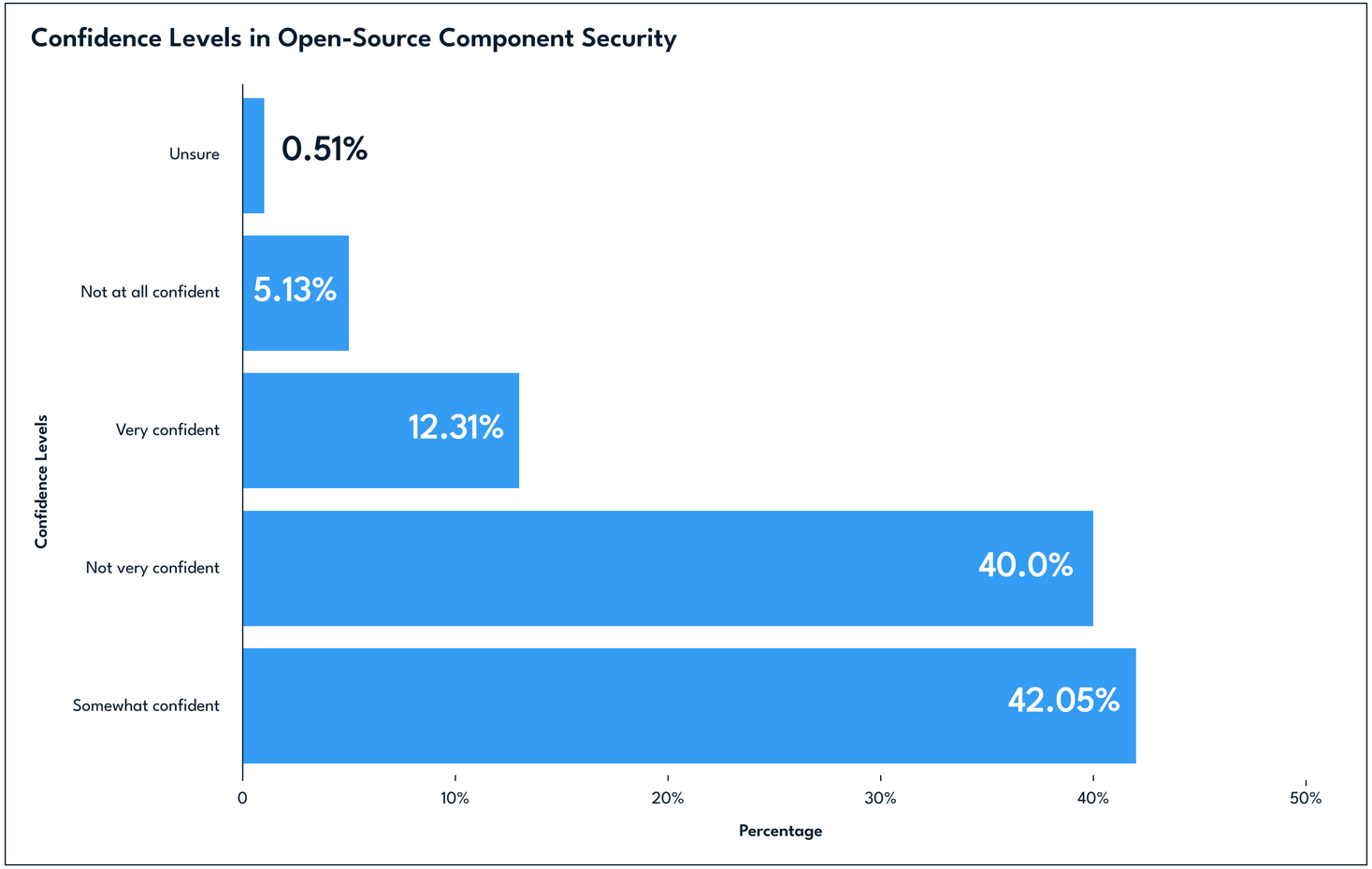
Only 12.31% of organizations are very confident that the open-source components they use, including transitive (indirect) dependencies, are up to date and secure.

However, over half of organizations

54.36%

are at least “somewhat” confident,

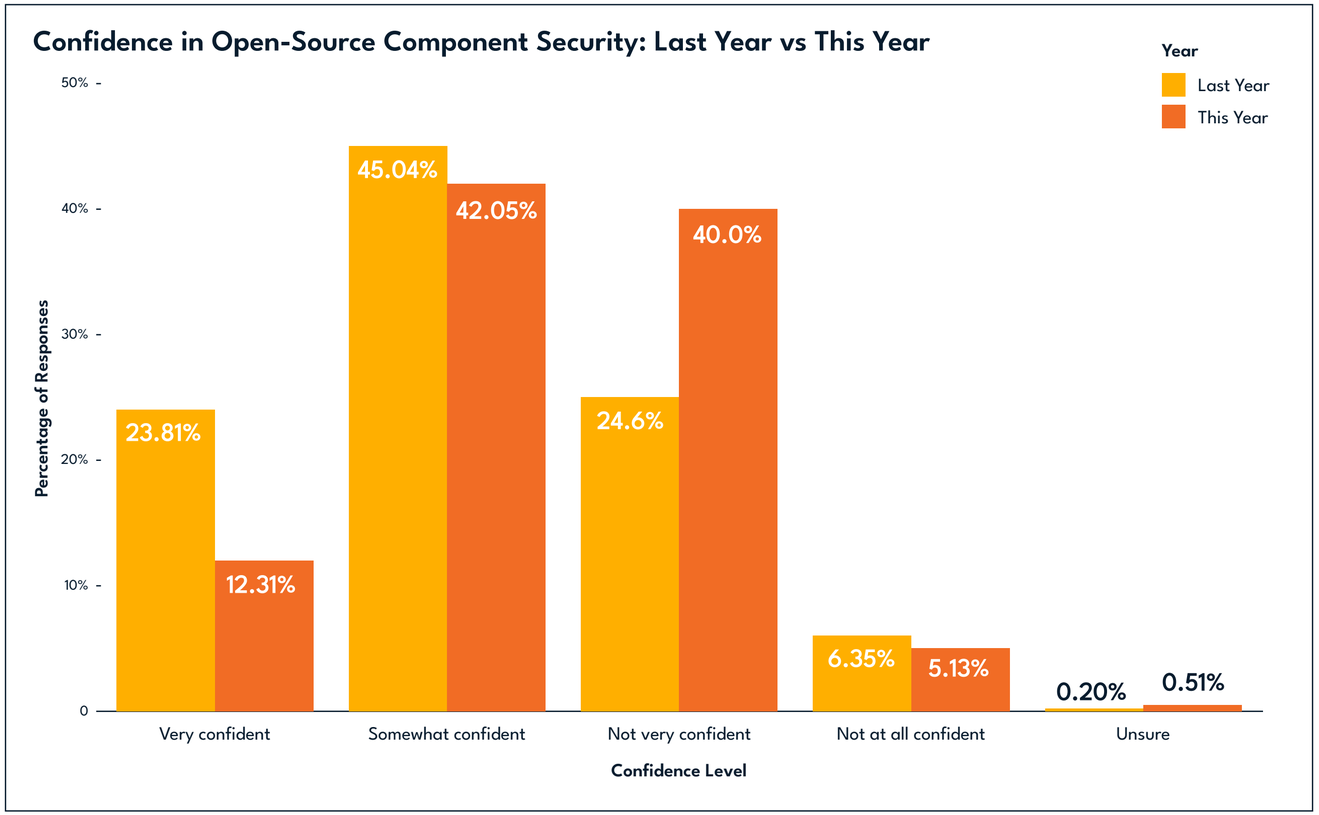
indicating a cautious yet optimistic outlook for a large swath of companies.



The rest of the organizations surveyed are mostly either “not very confident” (40%), indicating substantial concerns about the effectiveness of their open-source component management practices, or “not at all confident” (5.13%) – a smaller, but important subset that might require urgent attention and resources.

Uncertainty in open-source security is growing as time passes – while confidence is diminishing.

If we compare this data with the survey results we got last year, there are fewer organizations feeling "Very Confident" and more shifting towards "Not Very Confident."



There are fewer “very confident” organizations this year

Confidence at the highest level has dropped significantly from 23.81% to 12.31%, reflecting reduced assurance in organizations' ability to manage open-source dependencies securely.

Meanwhile, there are plenty more “not very confident” organizations compared to last year

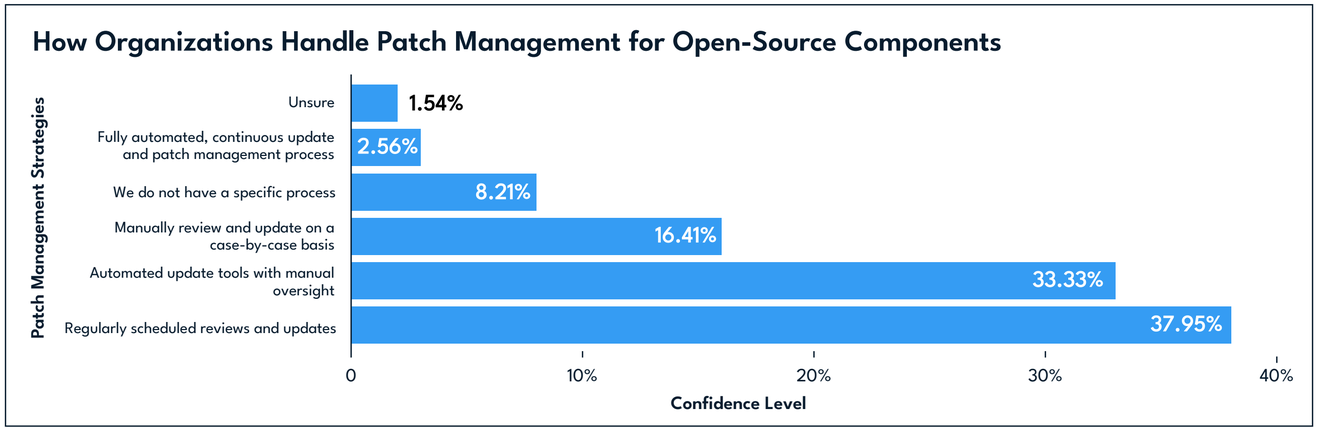
A significant rise from last year’s 24.60% to 40% this year suggests growing challenges or awareness of vulnerabilities in open-source security practices.

The zero confidence crowd hasn’t grown – or shrunken

This year’s 5.13% is only slightly lower than last year’s 6.35%, showing consistency among those with critical concerns.

When it comes to patch management for open-source components, most organizations opt for structured timeframes or partially-automated methods.

However, there has been low adoption of fully-automated solutions while a notable segment still relies on manual or ad hoc processes.



The low adoption of fully automated solutions indicates opportunities for tools and technologies that enable secure and efficient patch management.

Regularly scheduled reviews and updates reign supreme

The majority of organizations (37.95%) handle patch management through **regularly scheduled reviews and updates,** reflecting a structured approach to managing open-source components.

AI adoption isn't as strong as one may have thought

Only a small fraction (2.56%) of organizations implement **fully automated, continuous update and patch management** for patch management, suggesting that complete automation is still in its infancy or limited to specific use cases.

A third of organizations enjoy a mixed automated/manual approach

A significant portion (33.33%) use **automated update tools with manual oversight,** indicating a reliance on technology to streamline processes while retaining human control for monitoring the process.

Reactive approaches and lack of a defined process are – fortunately – in the minority

Just 16.41% of organizations **manually review and update on a case-by-case basis,** showing a more reactive approach that might be resource intensive, while 8.21% admit to **not having a specific process,** highlighting potential risks or gaps in their open-source supply chain management.

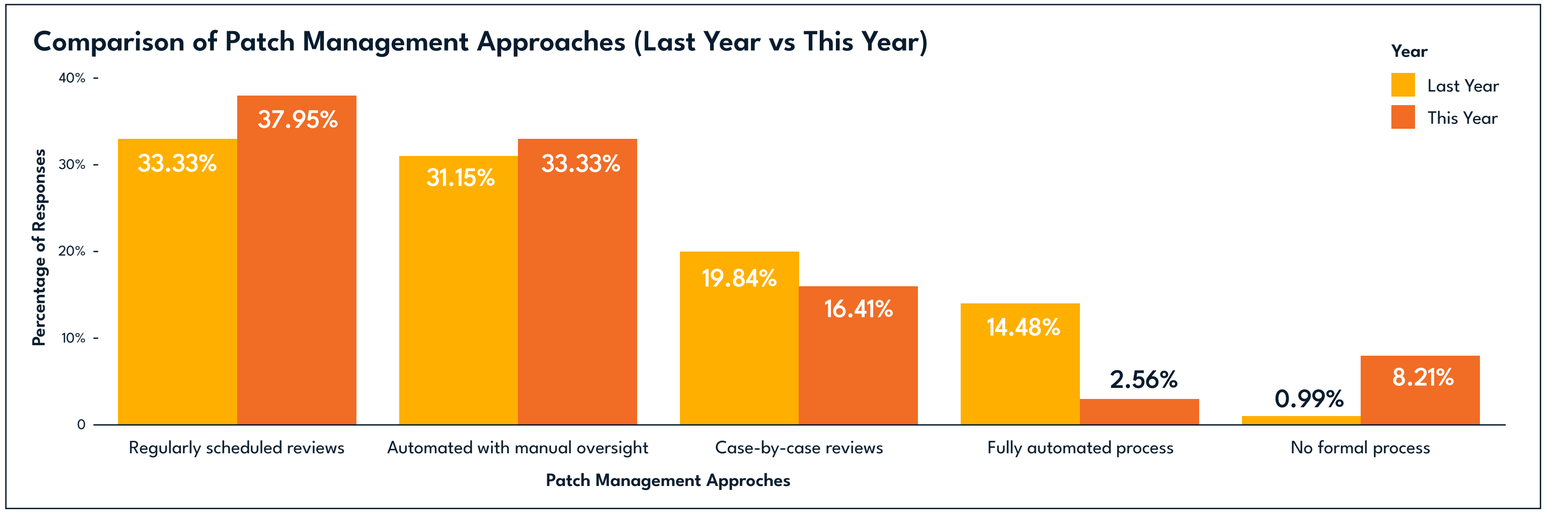
Looking at how approaches have evolved in the short term, there's a clear trend toward incorporating automation (but only when accompanied by manual oversight)

Are organizations only warming up to automation if some manual monitoring is also involved?

If we compare this data with the data we got last year, then we can see growth in incorporating automation with manual oversight – while fully automating processes declined massively year over year.

The plan: having no plan at all

Since last year, significantly more organizations (0.99% last year, 8.21% this year) reported having no formal patch management process. This raises concerns about potential vulnerabilities in open-source supply chain security, particularly for organizations lacking resources or expertise to establish structured patch management practices.



Scheduled reviews are still a leading practice

The share of organizations working with scheduled reviews for patch management has increased slightly, from 33.33% to 37.95%, making it the most common approach. This indicates that scheduled reviews continue to be a cornerstone of patch management strategies, reflecting a preference for structured and periodic updates.

More structure, less case-by-case management

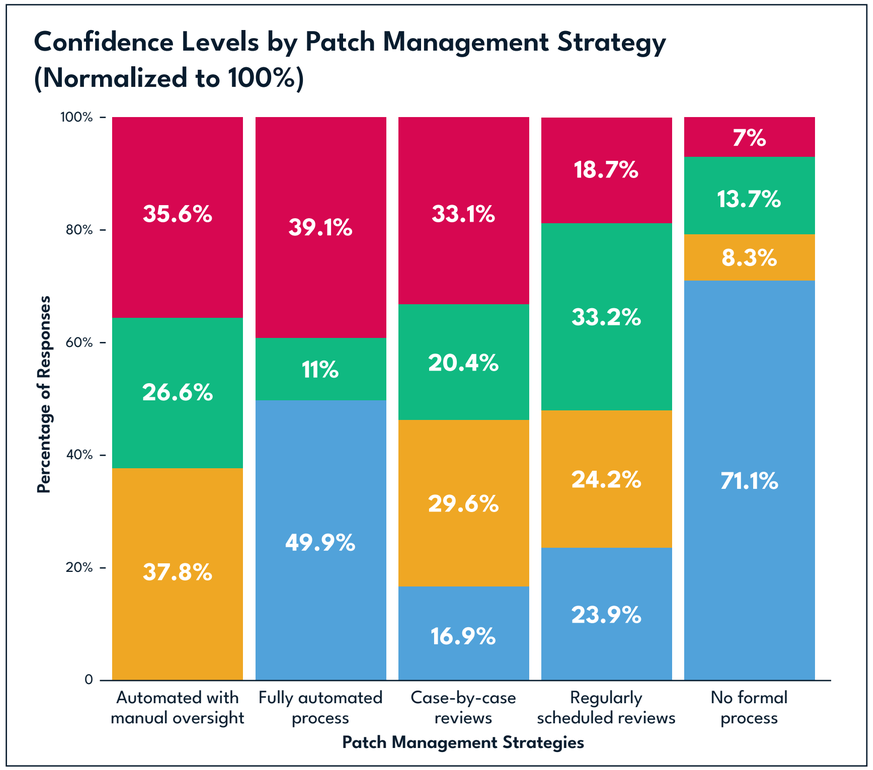
There has been a drop in the percentage of organizations relying on informal, reactive approaches, with a year-over-year decrease from 19.84% to 16.41%. This indicates a shift away from unstructured patching policies and further illuminates a general shift towards more structured or automated processes.

The biggest drop: full automation

Fully automated patch management saw a significant decline, from 14.48% last year to 2.56% this year. This sharp drop may indicate challenges in adopting fully automated systems, possibly due to technical limitations, operational complexity, or concerns about trust and control over automated processes.

Organizations that adopt structured and automated approaches tend to have higher confidence in their open-source component security

On the other hand, organizations with no formal process demonstrate the least confidence.



Full Automation: Untapped potential or well-founded apprehension?

While fully automated processes have limited adoption, their association with high confidence levels highlights their potential as an effective strategy. At the same time, their simultaneous association with a high percentage of “not at all confident” organizations may indicate that a large portion of professionals in this space don’t trust the automation that they have seen implemented.

The boldly confident 7%

It's notable that 7% of the respondents with no formal process are very confident in their patch management strategy – a remarkable group of people who, without a plan, believe sheer luck will steer them safely.

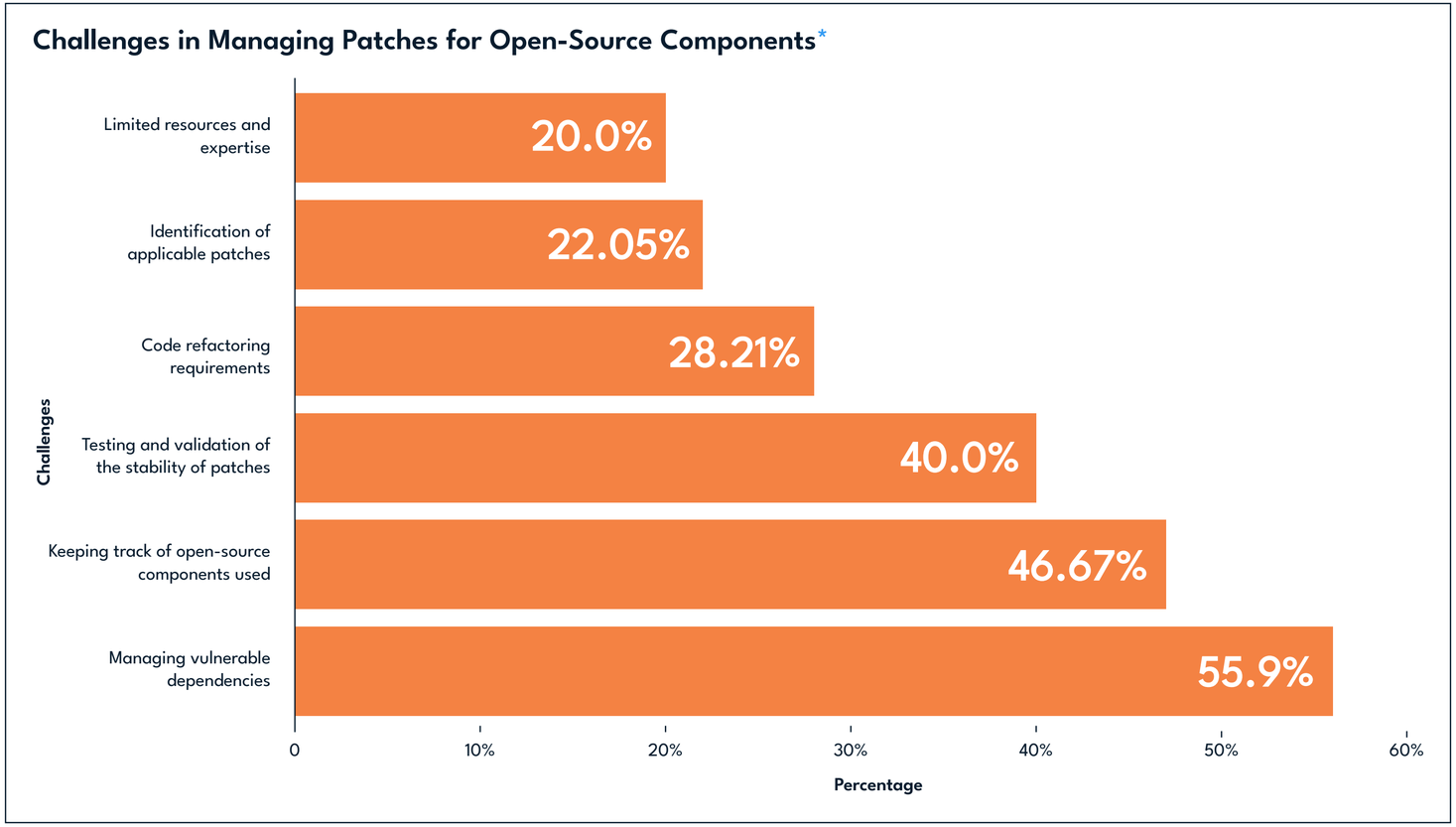
Confidence Levels

- Not at all confident
- Not very confident
- Somewhat confident
- Very confident

Organizations' environments themselves pose the largest challenges, not the ability or technical prowess at the organization.

Modern software ecosystems are highly complex and difficult to keep track of.

Managing dependencies and keeping track of open-source components are the biggest challenges according to survey respondents, reflecting the importance of inventory management, Software Bills of Material (SBOM), and the Open Vulnerability and Assessment Language (OVAL).

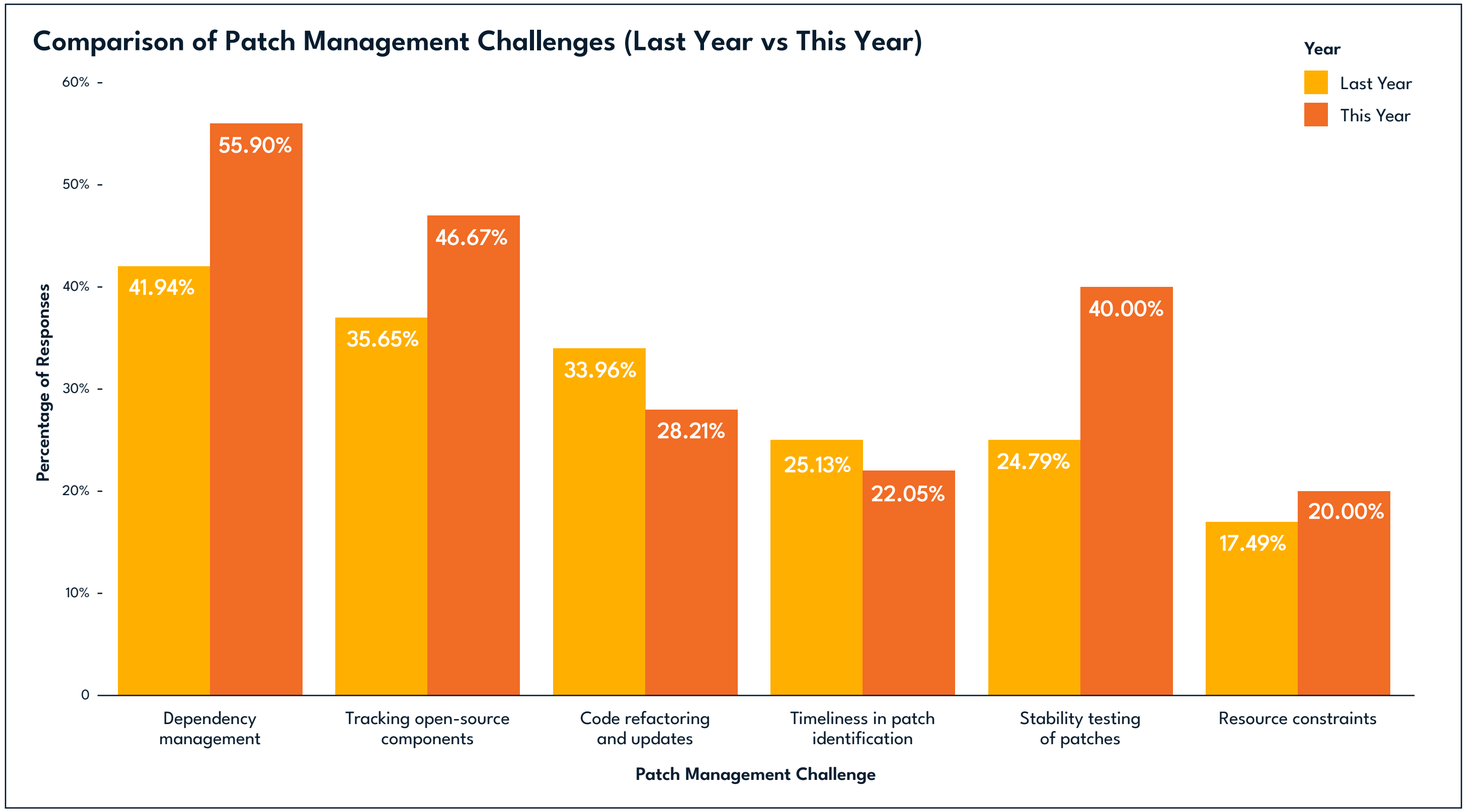


Less common challenges are likely related to resource and time constraints

Though testing and validating patches for stability before deployment (40%) and code refactoring requirements (28.21%) are not the top challenges, they are still significant. These challenges are related to workflows that require resources, time, and expertise – which come in varying supply levels depending on the organization. Identification of applicable patches (22.05%) may also point to these root causes.

*This question allowed for multiple challenges to be selected

The core difficulties in managing open-source component patches are enduring and systemic – persisting from year to year.



Compared to last year's results, the priority order of challenges has remained largely unchanged, though we can see notable changes in specific areas:

Stability testing of patches has emerged as a larger concern this year

With a significant increase from **24.79% to 40%**, organizations seem to be placing more emphasis on testing patches for stability before deployment – reflecting the growing importance of minimizing disruptions caused by patch application.

Dependency management and tracking open-source components continue to be the leading challenges

However, there is an increase in respondents reporting issues in these areas, particularly with **dependency management** now affecting a larger portion of organizations.

SECTION 5

The XZ Incident

In February 2024, a malicious backdoor was added to the Linux build of the xz utility within the liblzma library in versions 5.6.0 and 5.6.1, giving an attacker who holds a specific Ed448 private key remote code execution capabilities on the affected Linux system. XZ Utils is a widely-used open-source file compression tool integral to many Linux distributions. This event highlighted a critical vulnerability in the open-source supply chain: reliance on community-maintained repositories that might not consistently enforce stringent security measures. Had this backdoor not been caught when it was (by sheer luck, in fact), the end goal was the presence of a backdoor on every single Linux system worldwide.

The ramifications of this breach were extensive and global in scale. Organizations utilizing XZ Utils, directly or indirectly, faced potential threats that included unauthorized data access, system compromise, and the infiltration of further malicious code. The breach not only exposed immediate security lapses but also spurred a broader discussion about the security practices surrounding open-source software management. **For enterprises, this incident emphasized the need for more rigorous security protocols, including enhanced scrutiny of open-source components, regular security audits, and the adoption of a more proactive approach to cybersecurity.**

For the Enterprise Linux community, the XZ Utils backdoor incident is a critical reminder of the inherent risks in open-source software. While such software offers numerous benefits, including cost savings and customization flexibility, it also requires a high level of vigilance and robust security strategies to safeguard against similar incidents. Ensuring the security of open-source tools is vital for maintaining the integrity of an organization's operations and protecting against sophisticated cyber threats that exploit vulnerabilities within the supply chain.

In this section:

What percentage of organizations are aware of this major open-source supply chain vulnerability?

Is exposure to this vulnerability common?

What were the main causes of exposure to this vulnerability?

Did this incident spark changes in open-source patch management processes?

What measures have organizations taken to protect themselves from a similar incident in the future?

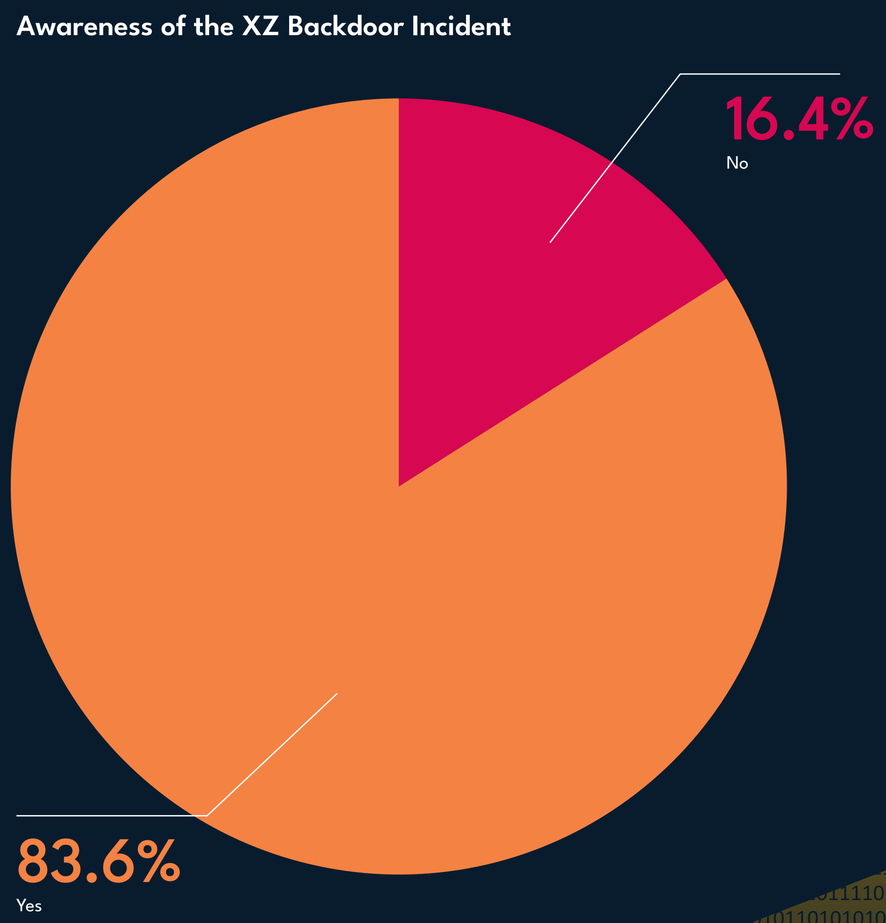
The Talk of the Town

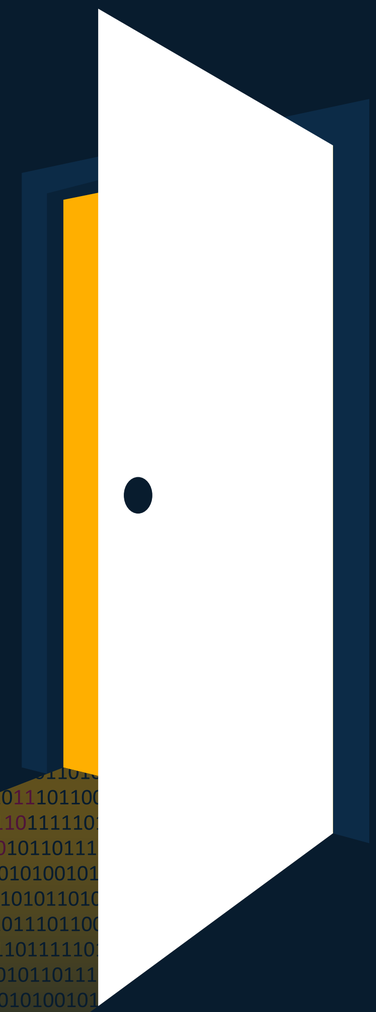
The XZ backdoor incident was widely written about – and it shows.

The vast majority of Enterprise Linux users surveyed were aware of the incident, with

83.6%

reporting that they knew about the event.





The XZ backdoor incident shines a light on how Enterprise Linux environments can be vulnerable in direct and indirect ways – whether organizations know it or not.

Indirect dependency was the primary cause

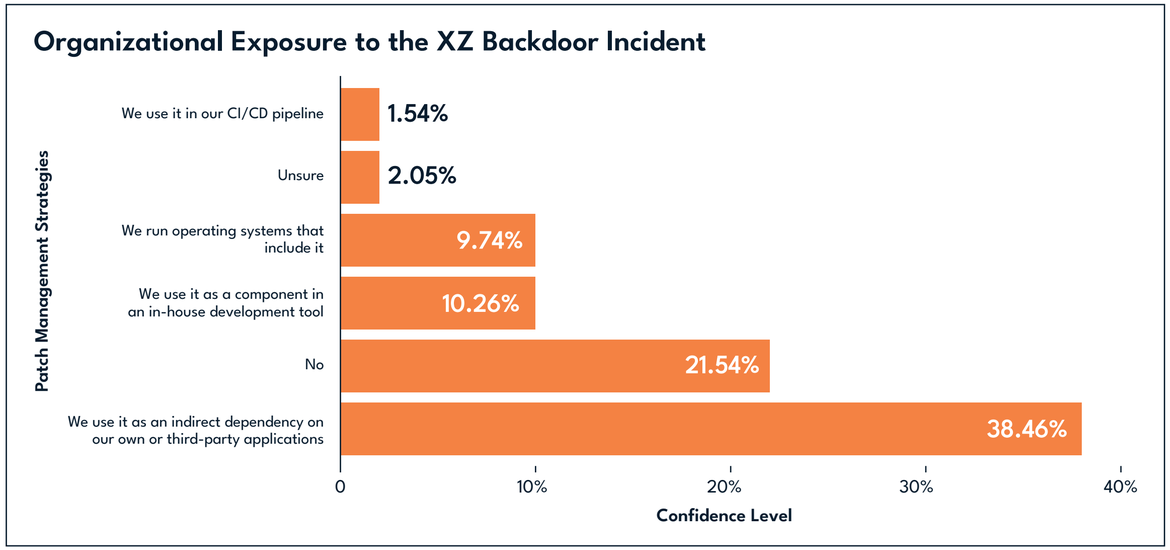
The majority of respondents (38.46%) reported exposure through indirect dependencies, indicating the pervasive nature of transitive vulnerabilities in software supply chains.

But direct integration was also a (smaller) exposure point

10.26% of respondents reported using the affected component in in-house developed software, reflecting direct integration of open-source components.

OS vendors also provided exposure through bundled components

9.74% of respondents highlighted exposure through operating systems that bundled the affected component, pointing to the challenge of managing pre-installed software.



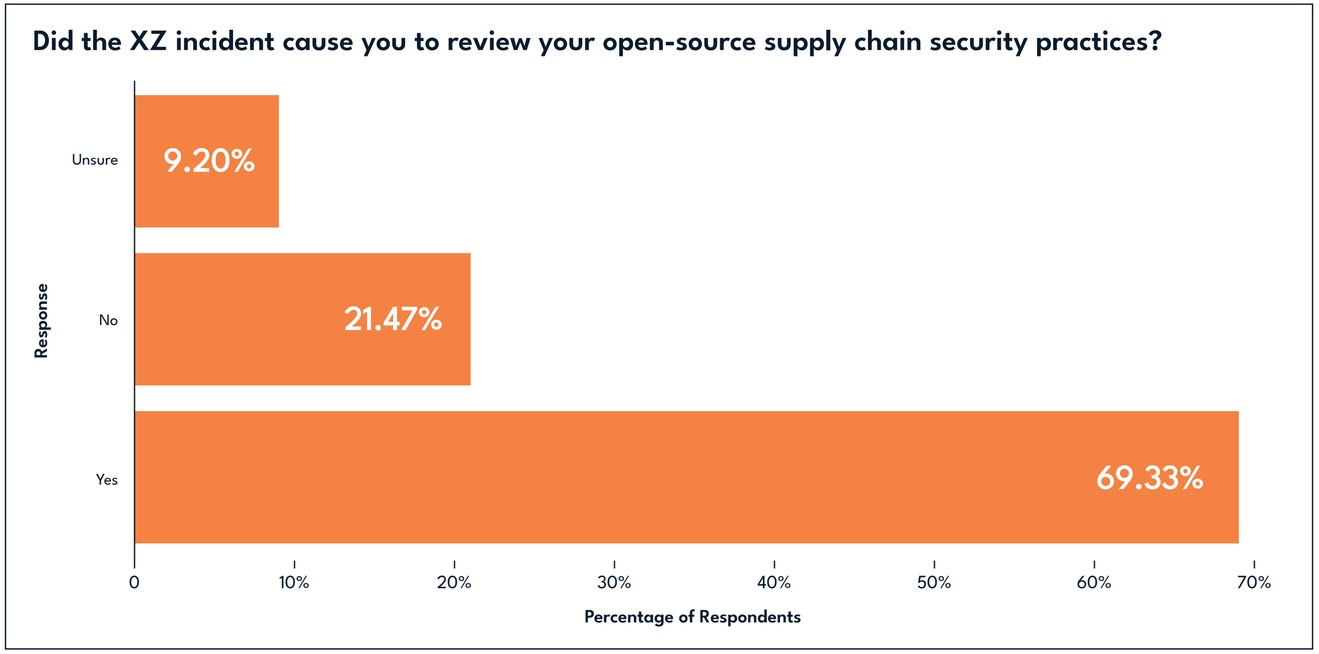
The issue was addressed quickly, so its direct exposure was low

21.54% of respondents stated that their organizations were not exposed, which may be due to robust dependency management practices or simply the fact that their distribution vendors protected them from exposure. While XZ is included in most distributions' minimal installations, most distributions didn't include vulnerable versions from this incident in their installations – enabling their users to avoid exposure from the get-go.

A catalyst for security improvements

The XZ incident had a significant impact on the Enterprise Linux space, inspiring most organizations to take another look at their security practices

More than two-thirds of enterprises reviewed their open-source supply chain security practices as a direct result of the XZ backdoor incident.



21.47%

reported no changes –

likely due to pre-existing robust measures or a surprising non-reliance on third-party code.

A minority

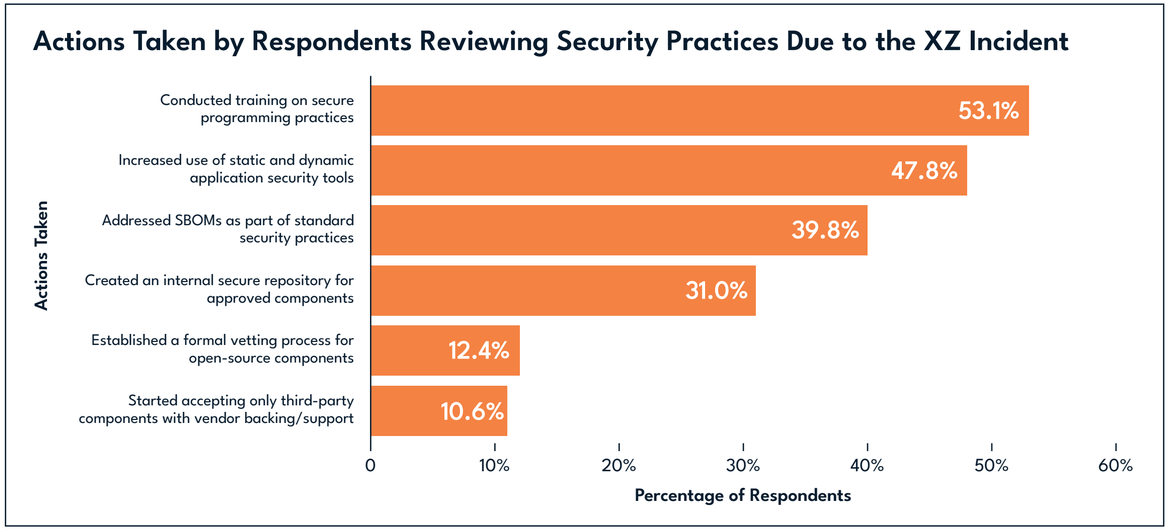
9.2%

were unsure,

suggesting potential gaps in awareness or internal communication.

The XZ backdoor incident prompted a range of proactive measures, with a clear emphasis on training, tool adoption, and dependency transparency.

These actions demonstrate an increasing maturity in how organizations manage open-source security, though the relatively lower focus on formal vetting processes suggests room for further improvement in standardizing supply chain practices.



A big push toward improving developer knowledge

Most organizations (53.10%) conducted training on secure programming practices as a result of the XZ incident, indicating a focus on enhancing developer awareness and skills.

Increased use of security tools

Many organizations (47.79%) implemented or expanded the use of static and dynamic application security tools to strengthen their software security processes.

Adoption of SBOM practices

Most organizations (53.10%) conducted training on secure programming practices as a result of the XZ incident, indicating a focus on enhancing developer awareness and skills.

More internal repositories (despite the workload)

Some organizations (30.97%) established internal secure repositories for approved open-source components, reflecting an effort to centralize and control software sourcing. These organizations appear to be explicitly accepting the extra work and responsibility involved in this endeavor as a trade-off for security.

SECTION 6

The State of Enterprise Adoption of Artificial Intelligence (AI) Technologies

Linux-based systems have increasingly become the backbone for deploying artificial intelligence (AI) technologies. This chapter explores the current state of AI on Enterprise Linux platforms, exploring how organizations perceive the impacts that they have experienced after integrating these technologies. The focus is on both the transformative potential of AI applications and the real-world outcomes observed by organizations, providing a comprehensive overview of the landscape as reported by Enterprise Linux users worldwide.

For many, AI has brought about significant improvements, leading to positive changes in business processes and outcomes. However, some enterprises also recount no noticeable changes. This chapter seeks to balance these perspectives, offering insights into what businesses expect from AI advancements and how these expectations play out after the implementation of these technologies. By examining these trends and outcomes, the chapter aims to provide a nuanced understanding of how AI is reshaping the Enterprise Linux environment, setting the stage for future developments and strategic decisions in the field.

In this section:

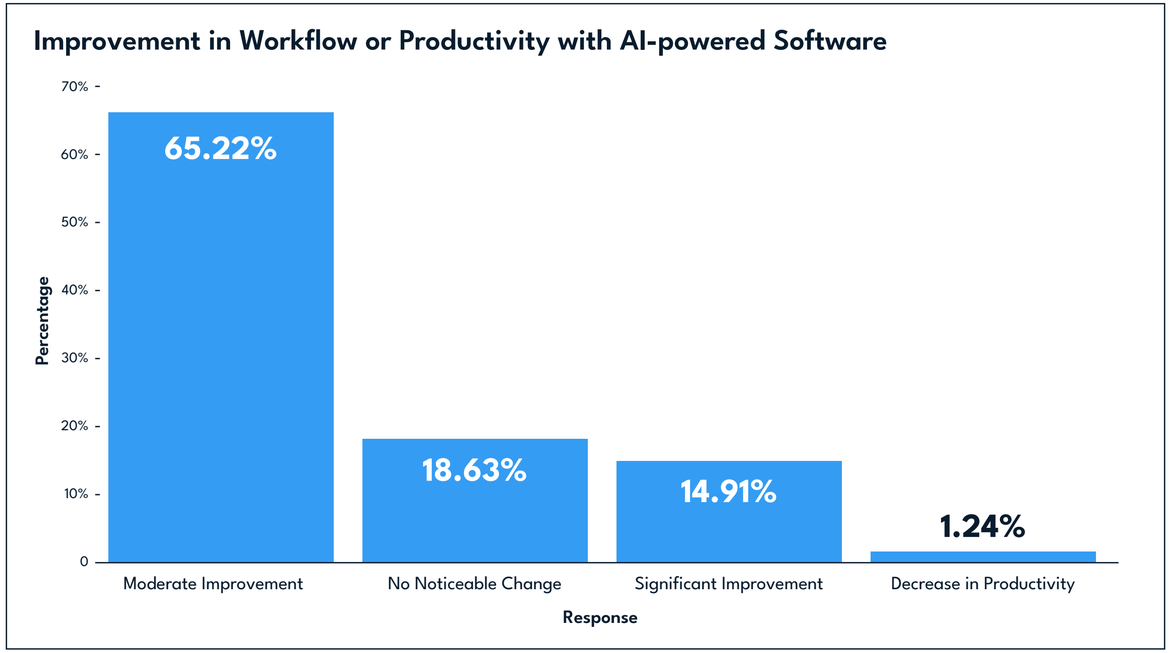
Are organizations noticing a positive impact of AI technology?

What are enterprises' primary expectations out of these technologies?

How have the perceptions of AI technology's outcomes evolved over time?

Most organizations have noticed at least a “moderate” improvement in workflow or productivity thanks to AI-powered software.

Meanwhile, negative impacts are almost nonexistent, with nearly nobody – less than 2% – reporting a decrease in productivity.



Big benefits are out there (for some)

A smaller subset of enterprises

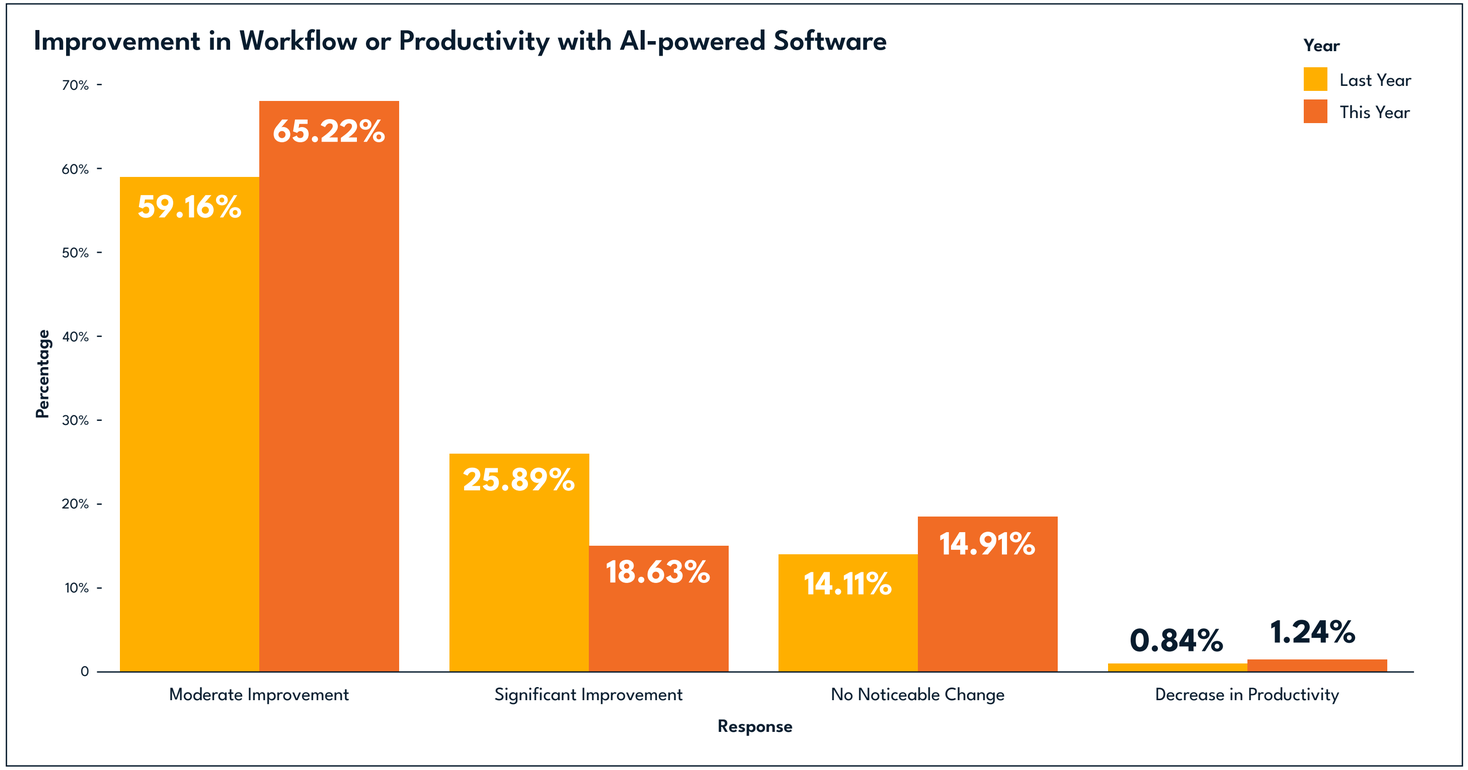
14.91%

observed a 'Significant improvement,' suggesting that AI-powered tools have substantial benefits for a minority of users.

However, nearly a fifth of enterprises reported “no noticeable change” in their workflow or productivity.

But the transformative positive benefits of AI are diminishing year over year

If we compare this data with the data from last year's survey we can see that, although AI-powered software continues to be beneficial, a significantly positive impact is perceived by fewer respondents compared to last year.



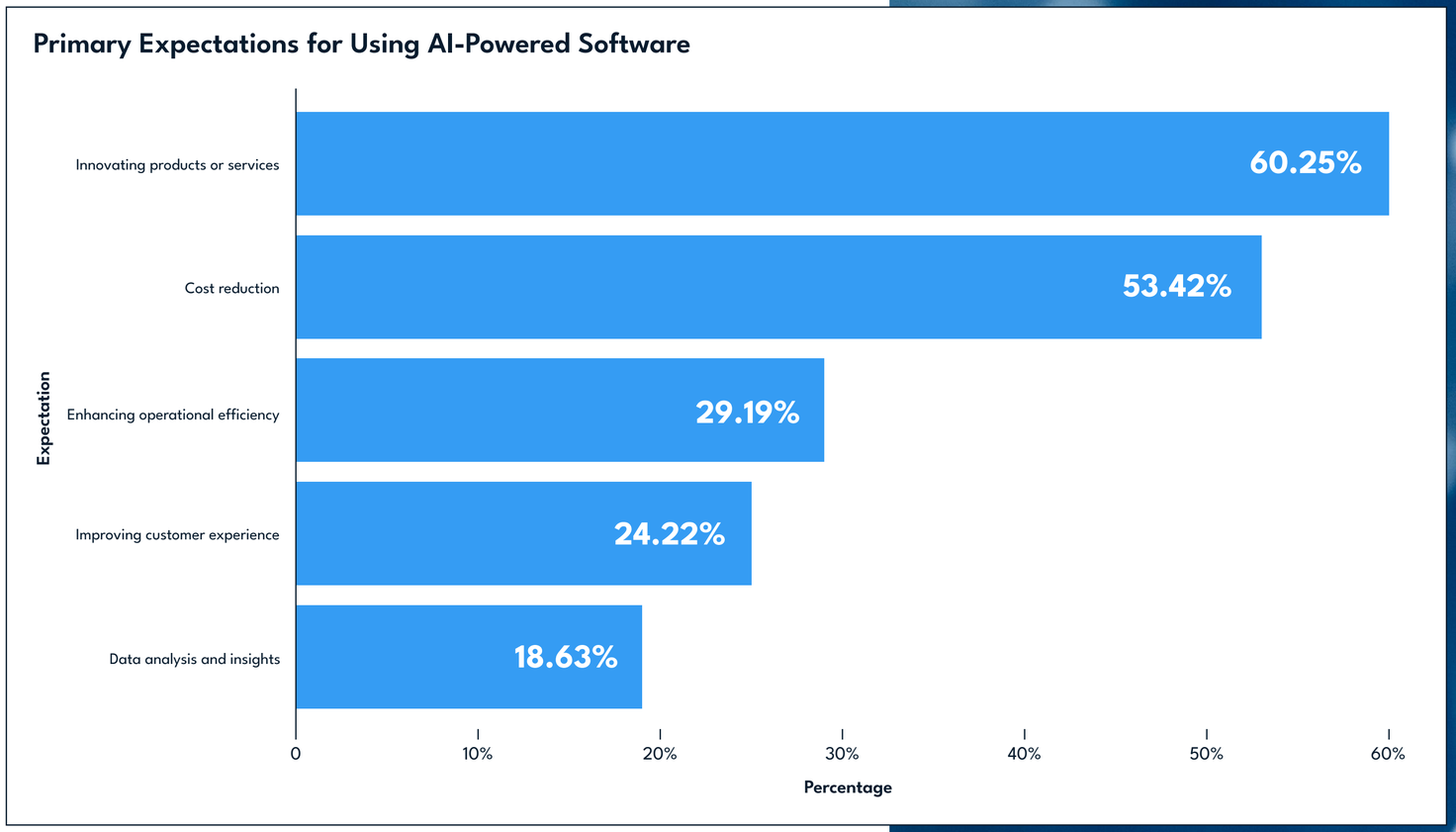
Are expectations not being met?

The percentage of respondents reporting “no noticeable change” increased by 4.52 percentage points – possibly reflecting either unmet expectations or stabilization in AI impacts.

Directly negative effects continue to be few and far between

Enterprises declaring a “decrease in productivity” grew by just 0.4%, though still remain minimal, highlighting that negative impacts remain rare.

Companies are looking to AI primarily to aid in innovation and cut costs

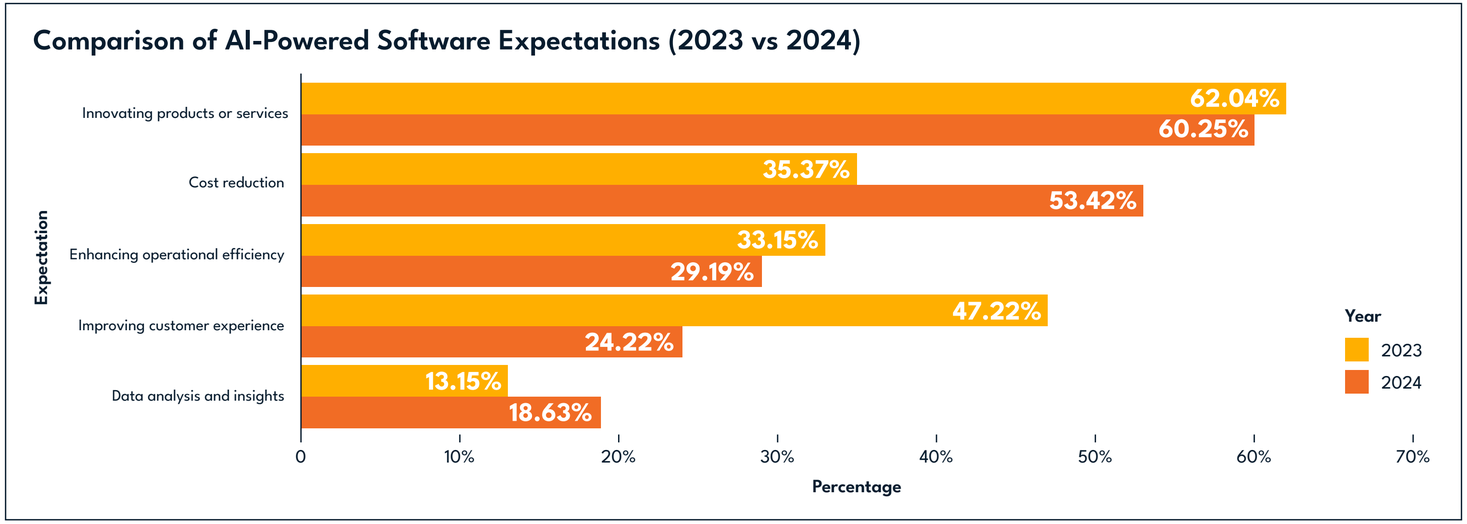


With the passage of time, organizations are increasingly viewing AI as a practical tool for cost management and process optimization rather than solely for transformative innovation.

If we compare expectations for AI to last year's survey, we see a mixed trend:

- Some categories saw a slight decrease in popularity, such as innovating products or services and enhancing operational efficiency. Improving customer experience saw the largest drop.
- Meanwhile, cost reduction experienced a significant increase and data analysis/insights grew year over year as well.

This evolution since last year suggests a shift in priorities from customer-facing AI applications toward financial and operational efficiency.



Innovation is still a key driver for AI adoption

Despite a slight dip from **62.04%** to **60.25%**, innovation in products and services still holds the largest share of respondents' expectations this year.

More organizations are hoping AI brings costs down

The most notable shift is the increase in **cost reduction** as a primary expectation, rising from **35.37%** to **53.42%**. This suggests that organizations are increasingly turning to AI not just for innovation but also as a cost-saving tool amid economic pressures.

Customer-centric expectations from AI are diminishing

Expectations around **improving customer experience** have fallen by **23%** year over year, possibly indicating that many organizations may have already achieved improvements in this area. Alternatively, it could suggest that anticipated gains from AI did not materialize as expected last year, leading organizations to shift their focus toward cost management, where they can see measurable progress.

What's Next?

The insights generated via our annual survey and analyzed within this report paint a picture of an industry where AI benefits are still being evaluated, confidence in operational practices has dropped, and challenges are plenty. With landmark cybersecurity events reshaping our understanding of the environment, organizations are experimenting with new approaches and are taking preventive steps to address potential problems.

Image by Alex Kotliarskyi from Unsplash

If your team is not working with the most advanced vulnerability management tools out there, your organization is at a higher risk of falling victim to expensive and disruptive cybersecurity incidents.

How can enterprise teams bring their vulnerability management approach into 2025?

With rampant open-source supply chain vulnerabilities, organizations continuing to coordinate maintenance operations to apply vulnerability patches, and major gaps in awareness as it relates to vulnerable systems, it is clear that many organizations using Enterprise Linux aren't taking advantage of the latest technologies when it comes to managing their vulnerabilities.

To address these challenges, it's not just about upgrading tools and solutions – it's equally crucial to rethink the processes that drive them. Where security and business needs intersect, outdated and inefficient methods should no longer be the default. Organizations must adapt to today's landscape while preparing for the accelerated changes that we're seeing, making security a top priority across the board.

When it comes to system patching and the disruptions caused by conventional methods, finding more efficient approaches is essential for handling this critical task. Whether you're managing mixed, multi-distro Linux environments or dealing with end-of-life open-source software, TuxCare provides a faster way to deploy vulnerability patches, reduce downtime, and shrink vulnerability risk exposure – including open-source supply chain vulnerabilities.

Modernizing Your Enterprise Security

Automated Rebootless Patching

TuxCare's rebootless patching solution, **KernelCare Enterprise**, enables organizations to put vulnerability patching on autopilot, deploying all the latest CVE patches automatically, in the background, without disruptions – on all popular enterprise Linux distributions.

KernelCare Enterprise ensures organizations receive security patches as soon as they become available, without needing to experience costly downtime, babysit lengthy reboots, or plan for maintenance windows – and the disruptions they trigger.

Never-Ending Security Updates for End-of-Life Systems

TuxCare's **Endless Lifecycle Support (ELS)** enables organizations to continue securely using Linux distributions, software languages, and software development frameworks that have reached end of life or no longer receive standard security support.

With ELS, TuxCare users can receive vulnerability patches for unsupported versions of CentOS, CentOS Stream, Ubuntu, Debian, Oracle Linux, PHP, Python, Spring, and .NET for as many years as they want, without time limits. This way, enterprises can seamlessly protect their systems and stay compliant for the long haul.

Enterprise-Grade Security Support

With TuxCare's **Enterprise Support for AlmaLinux**, teams that increasingly choose AlmaLinux as the standard OS for their mission-critical systems get the commercial support that organizations can't get anywhere else, provided straight from the experts that know AlmaLinux – and your environment – best.

This commercial support service transforms AlmaLinux from a community-driven distribution to an enterprise-grade powerhouse, delivering the VIP-level assistance that organizations need with the reliability of a community-powered distribution that open-source enthusiasts love.

About TuxCare's Research

Image by NASA from Unsplash

Demographics

To generate the insights found within this report, TuxCare researchers gathered data from 293 participants that use Enterprise Linux in their organizations across various industries.

Participants reported the following details of their organizations and their usage of enterprise Linux:

Organization Size

- <100: **30.82%**
- 101-500: **18.15%**
- 501-1,000: **14.73%**
- 1,001-5,000: **19.86%**
- 5,001-10,000: **9.25%**
- >10,000: **7.19%**

Organizations large and small participated in this research, but **more than two thirds of organizations surveyed have over 101 employees.**

Number of Linux servers used

- <10 systems: **14.73%**
- 10-20 systems: **19.52%**
- 21-100 systems: **20.89%**
- 100-500 systems: **25.68%**
- 501-1000 systems: **7.53%**

Most organizations surveyed operate **between 10 and 500 Linux servers**

Industries

- Automotive: **0.34%**
- Construction: **0.34%**
- Defense: **0.34%**
- Education: **9.25%**
- Entertainment and Media: **4.11%**
- Finance: **2.74%**
- Healthcare: **4.79%**
- Hospitality: **0.68%**
- IT/Technology: **40.75%**
- Industrial/Manufacturing: **18.49%**
- Insurance: **0.34%**
- Public sector: **5.14%**
- Research: **1.03%**
- Retail: **1.37%**
- Services: **4.45%**
- Telecom: **4.45%**
- Transportation: **1.37%**

While a wide array of industries were surveyed, most participants reported working in the IT/Technology, Industrial/Manufacturing, and Public Sector fields.

Job titles of survey participants

- Agile Delivery Lead: **0.34%**
- Architect Platform & Integration: **0.34%**
- Business Development: **0.34%**
- Business Owner: **0.68%**
- CEO: **2.40%**
- CIO/CTO: **3.77%**
- CISO: **1.03%**
- Compliance/Risk Specialist: **0.34%**
- DevOps: **10.62%**
- DevSecOps: **0.34%**
- IT Director: **0.68%**
- IT Manager: **0.68%**
- IT Service Manager: **0.34%**
- IT Security Analyst: **8.56%**
- Principal Engineer Cybersecurity: **0.34%**
- Product Manager: **3.42%**
- Project Manager: **0.34%**
- Researcher: **0.34%**
- Software Development Director: **0.34%**
- Software Engineer: **25.34%**
- Solution Architect: **0.34%**
- Sysadmin: **24.32%**
- System Engineer: **0.34%**
- Tech Lead: **13.01%**
- Technology Director: **0.34%**
- Vulnerability Management Specialist: **0.68%**

Participants occupied a diverse range of roles, including leadership roles. However, **most participants hold technical roles**, with Software Engineer, IT Security Analyst, and DevOps taking the top three spots.

Why TuxCare?

TuxCare is a global leader in open-source security, providing unmatched expertise in patching and security support for your enterprise systems. We deliver automated security patches to popular Linux distributions without reboots, long-term security updates for end-of-life products, next-generation vulnerability scanning, and enterprise-grade support for community-powered Linux systems – offering a comprehensive security solution for all your infrastructure needs.

With over

170,000 patches (and counting)

delivered to our users, TuxCare's solutions reduce vulnerability exposure, minimize downtime, eliminate patching-related disruptions, secure your open-source supply chain, and maintain system stability and compliance.

TuxCare protects the world's largest enterprises, government agencies, service providers, universities, and research institutions, safeguarding over 1.2 million workloads (and growing). Our mission is to drive continuous innovation through open-source technologies while minimizing the risk of cyber threats and serving as a trusted technology partner for innovative organizations across the globe.

Image by Dennis Kummer from Unsplash