TuxCare

Enterprise Linux & Open-Source Landscape Report

2024

Table of Contents

Dear Friends,

It is with great pleasure that we present the inaugural TuxCare Enterprise Linux and Open-Source Landscape Report for 2024. This report, a culmination of our first annual survey, offers a revealing glimpse into the evolving landscape of enterprise Linux and open source, marking a significant effort to identify key trends and forecast future developments in this dynamic field.

As we navigated through a year of substantial change and growth in the industry, our survey aimed to capture the pulse of the market, with our research focusing on the aftermath of pivotal events and outlining predictions for what the coming year may bring.

This report covers several critical areas:

Linux Distro Usage: In the wake of Red Hat's policy shifts, we examine the current enterprise Linux landscape, seeking to understand how these changes are influencing user preferences and industry directions.

ARM Server Adoption: As ARM continues to carve out a significant market share, we explore the confidence levels in its future role within enterprise environments, considering the complexities of its various instruction set implementations and their impact on Linux kernel performance.

Linux Patch and Vulnerability Management: This section provides insights into how organizations are navigating the challenges of security and stability within the Linux suite of products, revealing strategies and practices in patch and vulnerability management.

Open-Source Supply Chain Security: Reflecting on the surge of open-source software supply chain attacks, our report uncovers how these incidents are reshaping supply chain management strategies, detailing the primary challenges and responses to these emerging 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 findings of our survey paint a vivid picture of an industry at a crossroads, with organizations increasingly adopting sophisticated strategies to navigate the complexities of open-source software and enterprise Linux. From increased reliance on Linux in diverse environments to proactive approaches in managing security vulnerabilities and embracing AI, this report provides a deep dive into the trends that are shaping the industry.

We extend our heartfelt gratitude to all who contributed to this research. Your valuable insights not only enrich our understanding but also contribute to the collective knowledge and advancement of the enterprise Linux and open-source community.

As we look ahead, we are excited to see how the trends identified in this report will unfold and continue to influence the industry. We invite you to read, reflect, and engage with the findings of this report, as we continue our journey in shaping a more informed and innovative future.

Warm regards,
The TuxCare Team

Enterprise Linux is evolving

and organizations that rely on this technology
are evolving right alongside it

SECTION 1

Enterprise Linux Distribution Preferences & Strategies

How many distributions are enterprises using simultaneously?

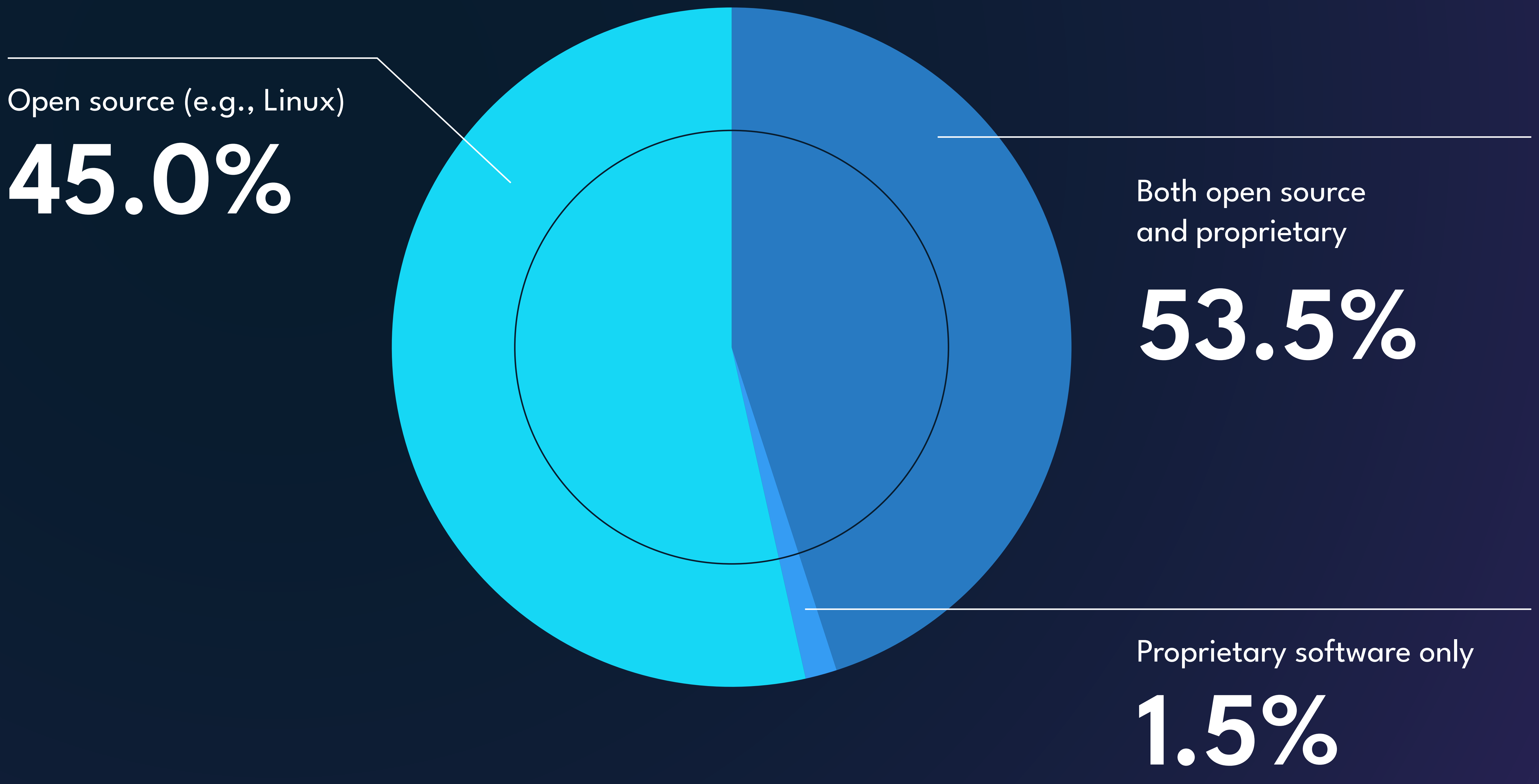
What do organizations plan to do when their current enterprise Linux distribution reaches end of life (EOL)?

How do distribution policy changes affect organizations?

98.5%

of enterprises rely on open-source software

Open-Source vs. Proprietary Usage



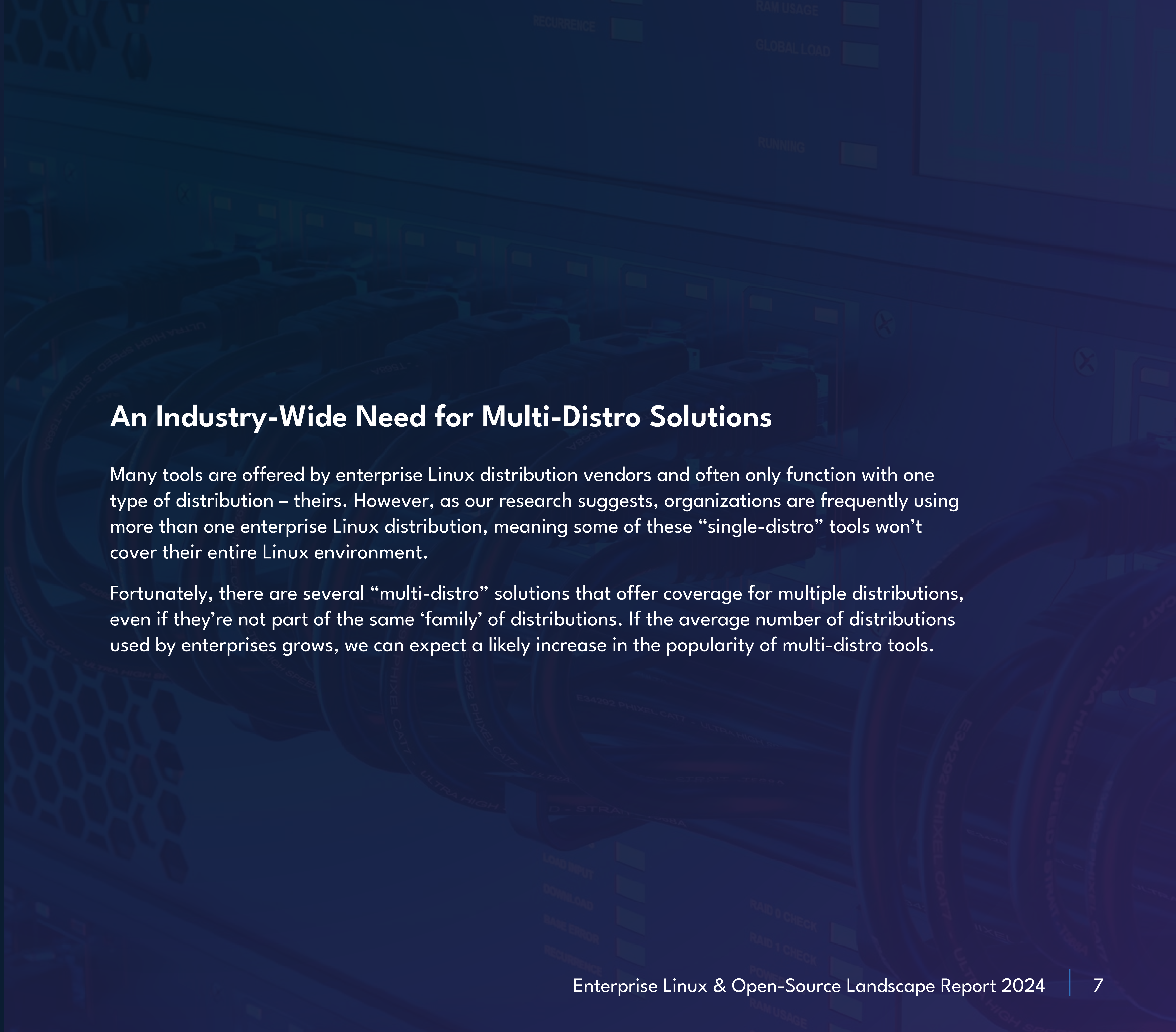
Most organizations surveyed use a combination of open-source and proprietary software in their infrastructure stack, but 98.5% rely on open-source software in some way.

Multi-distro environments are commonplace

On average, enterprises work with

1.97

Linux distributions



An Industry-Wide Need for Multi-Distro Solutions

Many tools are offered by enterprise Linux distribution vendors and often only function with one type of distribution – theirs. However, as our research suggests, organizations are frequently using more than one enterprise Linux distribution, meaning some of these “single-distro” tools won’t cover their entire Linux environment.

Fortunately, there are several “multi-distro” solutions that offer coverage for multiple distributions, even if they’re not part of the same ‘family’ of distributions. If the average number of distributions used by enterprises grows, we can expect a likely increase in the popularity of multi-distro tools.

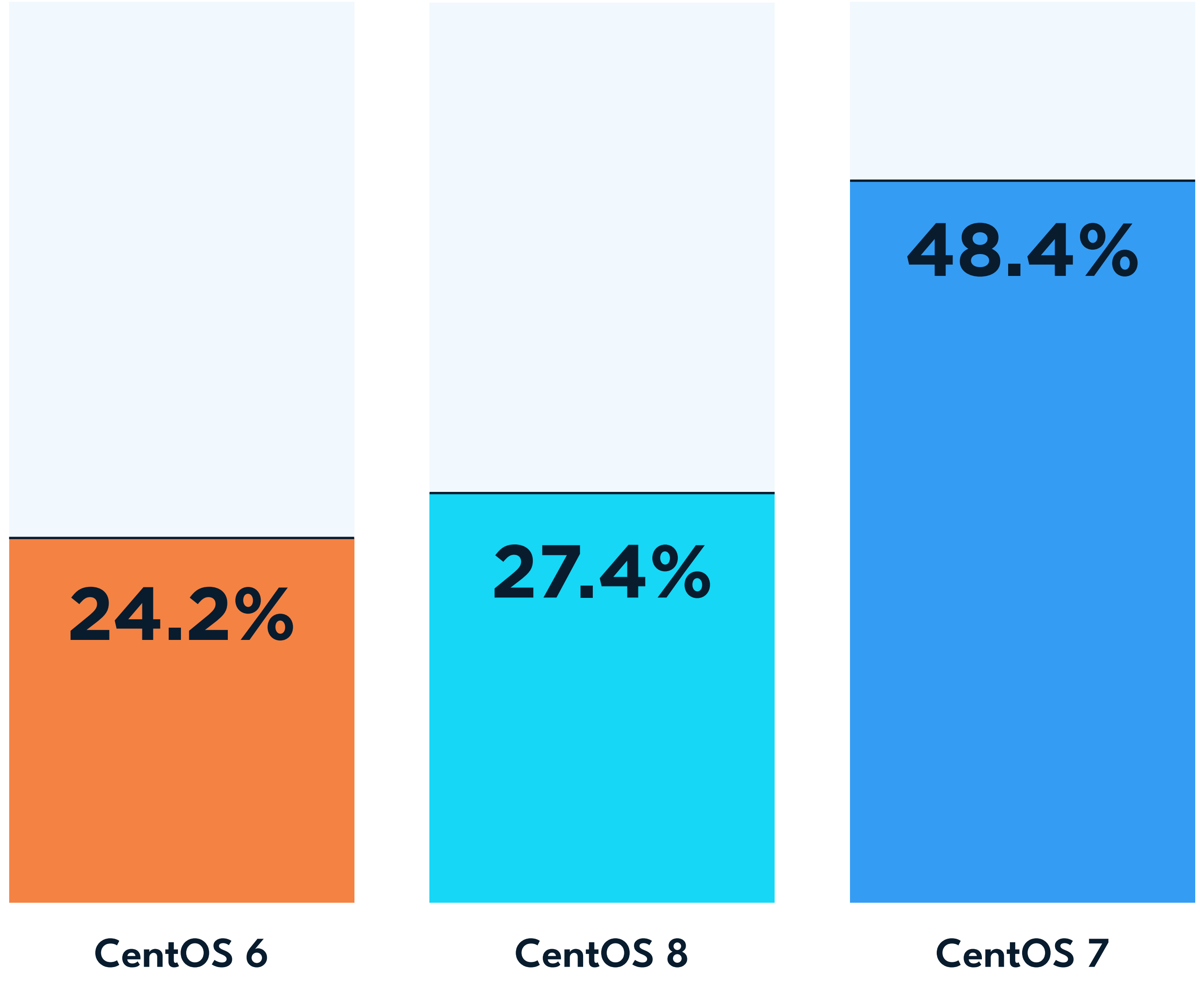
CentOS is one of the most popular distributions used by enterprises

Most enterprise CentOS users are working with CentOS 7

&

A concerning number of CentOS users are working with end-of-life versions 6 and 8

which means that their systems may be especially vulnerable if they aren't subscribed to some form of extended support service



Why does CentOS 7 take the largest share?

This is likely due to the fact that CentOS 7 is the only (and last) stable CentOS distribution that hasn't reached end of life yet, so it still receives security updates and vulnerability patches from the distribution vendor – while CentOS 6 and CentOS 8 do not.

A troubling share of enterprise CentOS users overall are still using CentOS 6 and CentOS 8, both of which are no longer supported by the CentOS project and do not receive security updates.

For CentOS 6, this figure is remarkably high, as this distribution reached its end-of-life phase a longer time ago than CentOS 8.

So how are CentOS 6 and CentOS 8 users keeping their server fleet protected, with both of these distributions already well into their end-of-life phases?

As you'll see below, many enterprise users are continuing to receive security updates for CentOS 6 and CentOS 8 with an extended support option or going without security support and putting their systems at risk of vulnerability exploits – whether or not they plan to migrate to a different distribution.

For now, organizations prefer extended support over migration when it comes to dealing with the end of life (EOL) of CentOS variations

Plans for CentOS 6

Continue using post-EOL without support: **22.22%**

Migrate to another distribution: **7.41%**

Purchase extended security support: **68.52%**

Not decided yet: **1.85%**

Plans for CentOS 7

Continue using post-EOL without support: **9.38%**

Migrate to another distribution: **22.66%**

Purchase extended security support: **61.72%**

Not decided yet: **6.25%**

Plans for CentOS 8

Continue using post-EOL without support: **7.69%**

Migrate to another distribution: **21.15%**

Purchase extended security support: **69.23%**

Not decided yet: **1.92%**

For enterprise users of all three CentOS versions

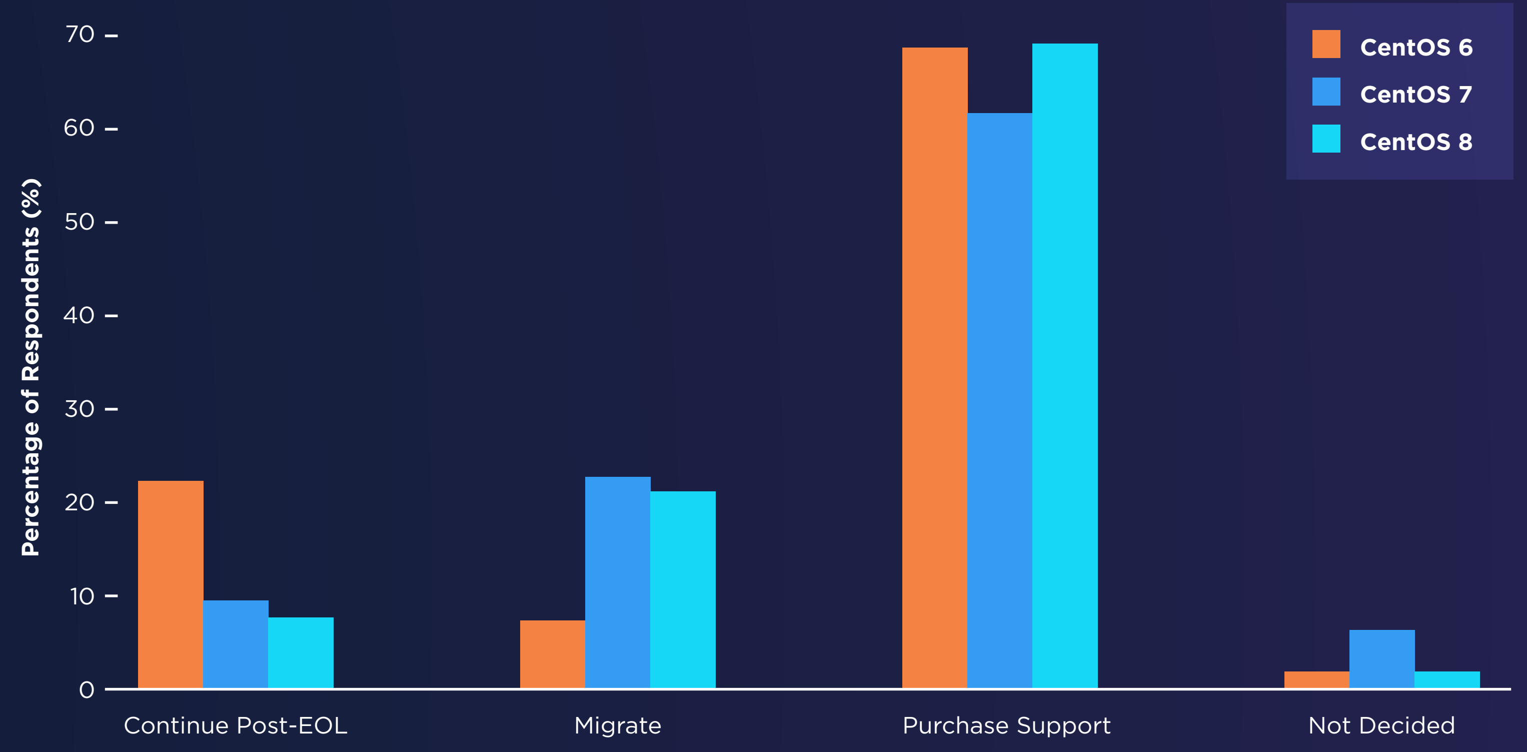
The majority of respondents (between 61% and 69%) plan on using extended support

About 20% of CentOS 7 and CentOS 8 users plan on migrating to a different enterprise Linux distribution

A troublingly high percentage (22.22%) of CentOS 6 users plan on carrying on without any form of security support – compared to 9.38% for CentOS 7 and 7.69% for CentOS 8

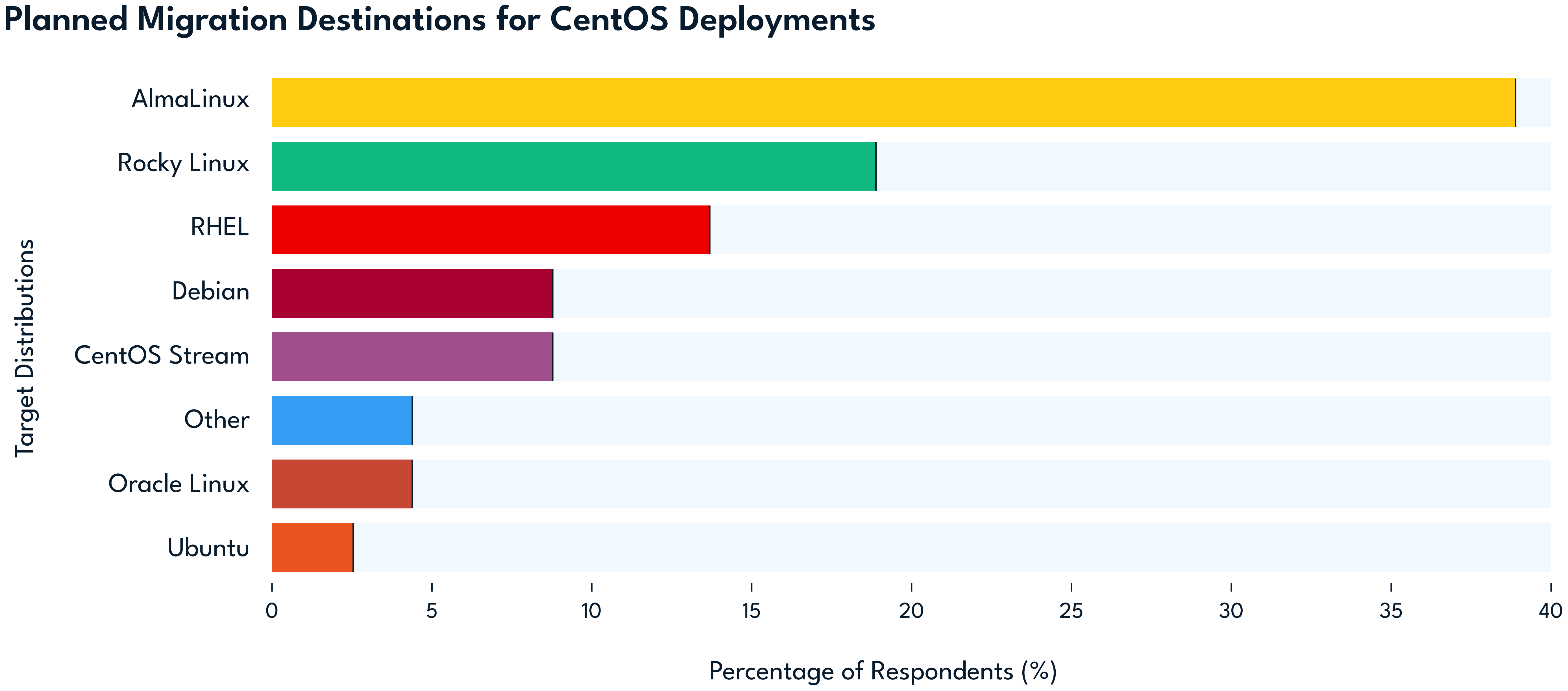
It's notable that organizations using CentOS 6 without any security support are doing so despite the fact that there are thousands of vulnerabilities that have been discovered in CentOS 6 since it reached end of life.

Plans for CentOS versions among survey respondents



Organizations using a free-of-cost enterprise Linux distribution like CentOS lean towards migrating to another free distribution rather than a paid alternative

With just 9.6% of CentOS 6, 7, and 8 users planning on migrating to a different enterprise Linux distribution, we asked which distribution they would choose as a replacement:



We are aware that this question's results diverge somewhat from other research, but it accurately depicts the response data from the survey. You can find information about how this survey was conducted on page 47 of this report.

For those opting to migrate, most enterprises are transitioning to AlmaLinux or Rocky Linux compared to Red Hat Enterprise Linux (RHEL), indicating that **organizations using a free distribution want to stay on a free distribution.**

With RHEL in third place, it appears that there is **likely a desire to move to distributions that are part of the same ecosystem as CentOS.**

Enterprise Linux distributions can make wide-ranging, impactful decisions, which organizations must grapple with....

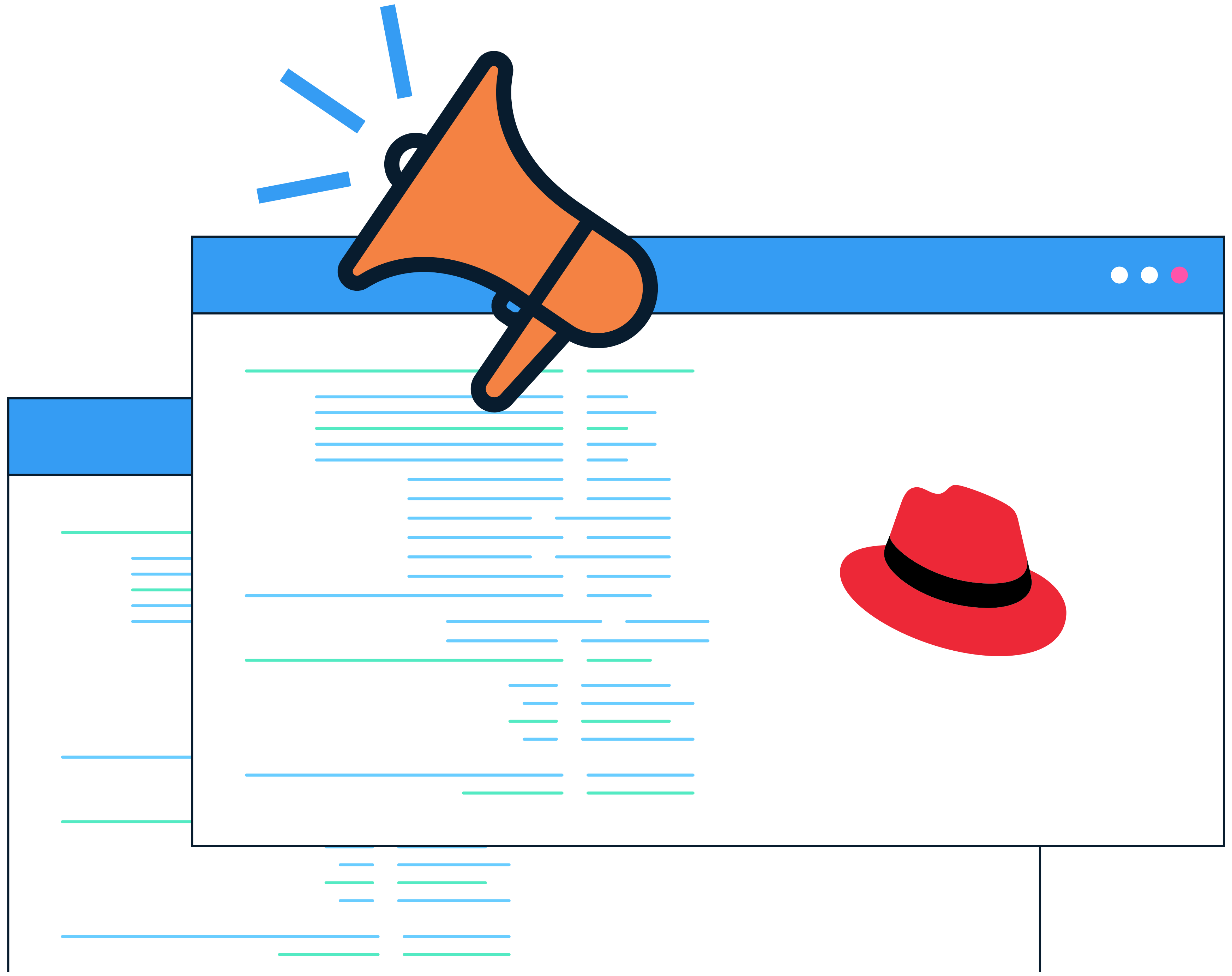
So, how do they usually fare?

Let’s take a look at a major event from 2023 as a case study:

The Red Hat Source Code Announcement of 2023

On June 21, 2023, Red Hat announced that CentOS Stream will be the exclusive repository for Red Hat Enterprise Linux (RHEL)-related source code releases, discontinuing the publication of tagged RHEL sources on git.centos.org and **limiting access to the source code for non-Red Hat customers and partners.**

While Red Hat's existing customers and partners can still access RHEL sources via the customer/partner portals based on their subscriptions, the wider open-source community, particularly RHEL-based distributions like Rocky Linux and AlmaLinux, faced significant challenges due to these restrictions.



As seen in the case of the reaction to the Red Hat shift, infrastructure size significantly influences how policy changes are viewed:

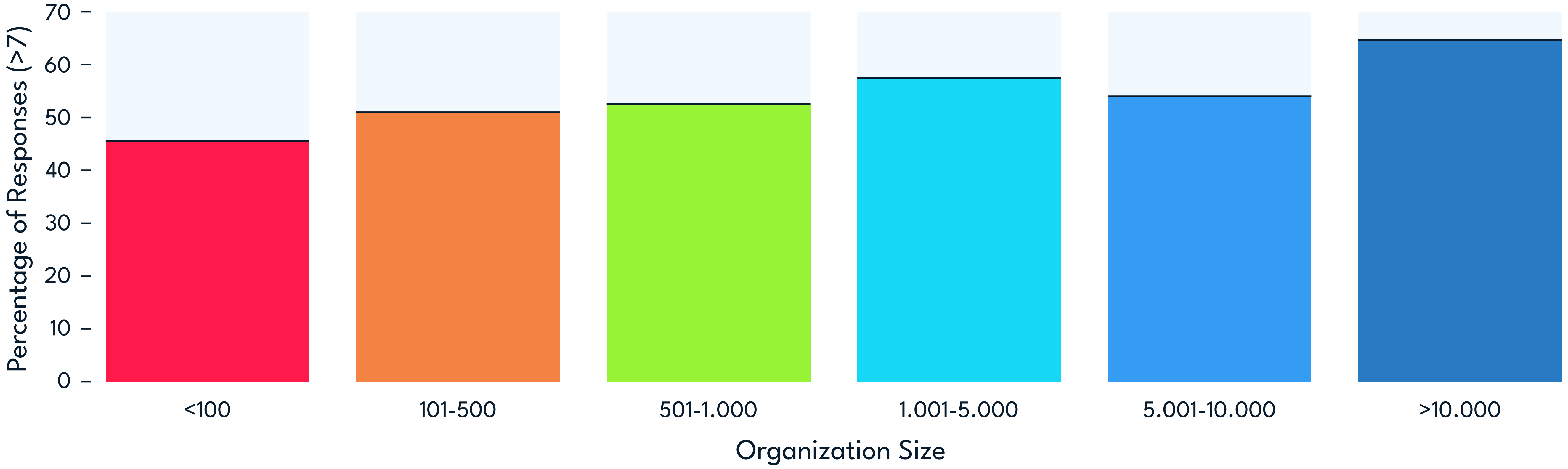
Larger organizations with extensive Linux infrastructure feel a greater impact.

64.71% of organizations with more than 10,000 employees perceive the policy change as impactful (rating above 7).

These larger organizations, 47.06% of which reported operating more than 1,000 Linux servers in their environment, are more profoundly affected by Red Hat's policy changes. Their extensive infrastructure makes policy changes more consequential, potentially requiring major adjustments in IT strategies.

We asked enterprise Linux users to rate the impact of Red Hat's new source code policy on their organization from 1 (no impact) to 10 (extremely significant impact).

Percentage of High Impact (>7) Responses by Organization Size



Meanwhile,

Smaller organizations indicated varied impacts, with just 46.49% indicating an impact above 7

possibly due to their agile nature (quicker decision-making processes, greater flexibility in operations, closer team dynamics, and less risk aversion).

Moderate-sized organizations are also affected, with 57.14% indicating high impact as well

possibly due to the potential for organizations of this size to be experiencing growth or changes in their Linux infrastructure, making them particularly sensitive to policy changes.

A larger-sized organization (indicating a higher system count) appears to make large-scale changes more cumbersome to deal with

As we saw earlier in this section, this may be the reason that many organizations are reluctant to migrate their CentOS systems to a different distribution.

SECTION 2

ARM Server Adoption in the Enterprise

What Is ARM?

ARM architecture is a family of computer processors based on a reduced instruction set computing (RISC) architecture, known for its energy efficiency and performance per watt ratio.

Compared to the more traditional x86 architecture, which is commonly used in desktops and servers, ARM processors excel in performing a substantial amount of computing work while consuming less energy. This efficiency is pivotal for enterprises aiming to reduce energy and cooling costs or seeking to achieve more computational work within the same energy budget.

As energy efficiency becomes increasingly critical in data centers and enterprise environments, particularly under the growing demand for cloud services and big data processing, ARM's low-power yet high-performance capabilities make it an attractive choice.

In enterprise Linux environments, this maximization of performance per watt can lead to significant cost savings and enhanced scalability.

Are organizations adopting ARM architecture?

What ends does ARM server adoption serve for organizations?

How suitable is the current enterprise Linux environment for ARM deployments?

What does the future of ARM architecture in enterprise Linux look like?

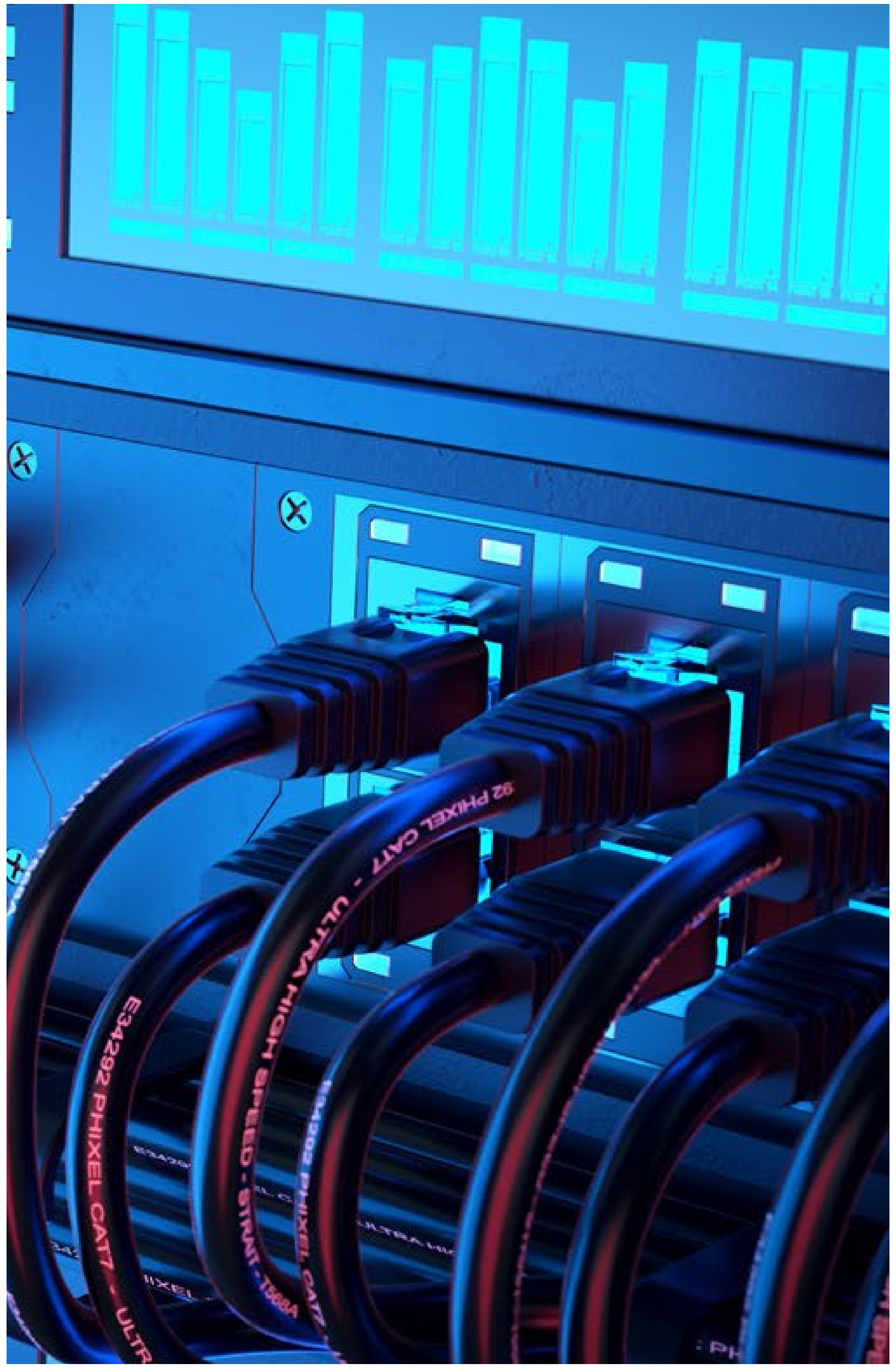
TuxCare

The popularity of ARM servers is apparent

79.76%

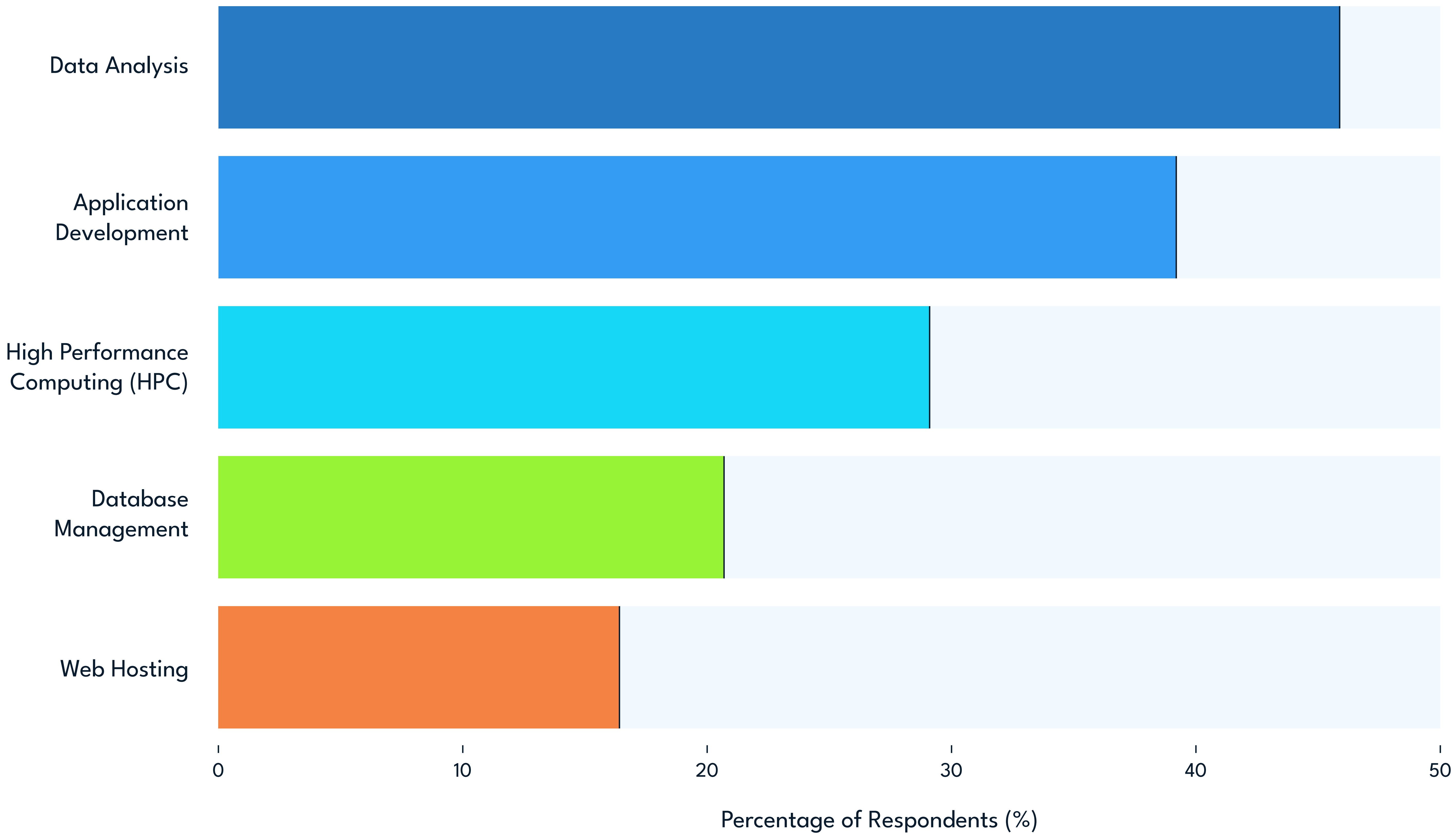
of enterprises surveyed indicated that they are currently using or planning to deploy ARM servers in their organization in the next 12 months

The positive attitude towards ARM adoption in enterprise computing signifies a broader trend in the industry towards energy-efficient and environmentally sustainable technology solutions.



The primary purpose of enterprise ARM deployments is mostly Data Analysis with Application Development & High-Performance Computing falling closely behind

Top Use Cases for ARM Servers among Respondents



But is the enterprise Linux ecosystem a welcoming and functional environment for ARM deployments?

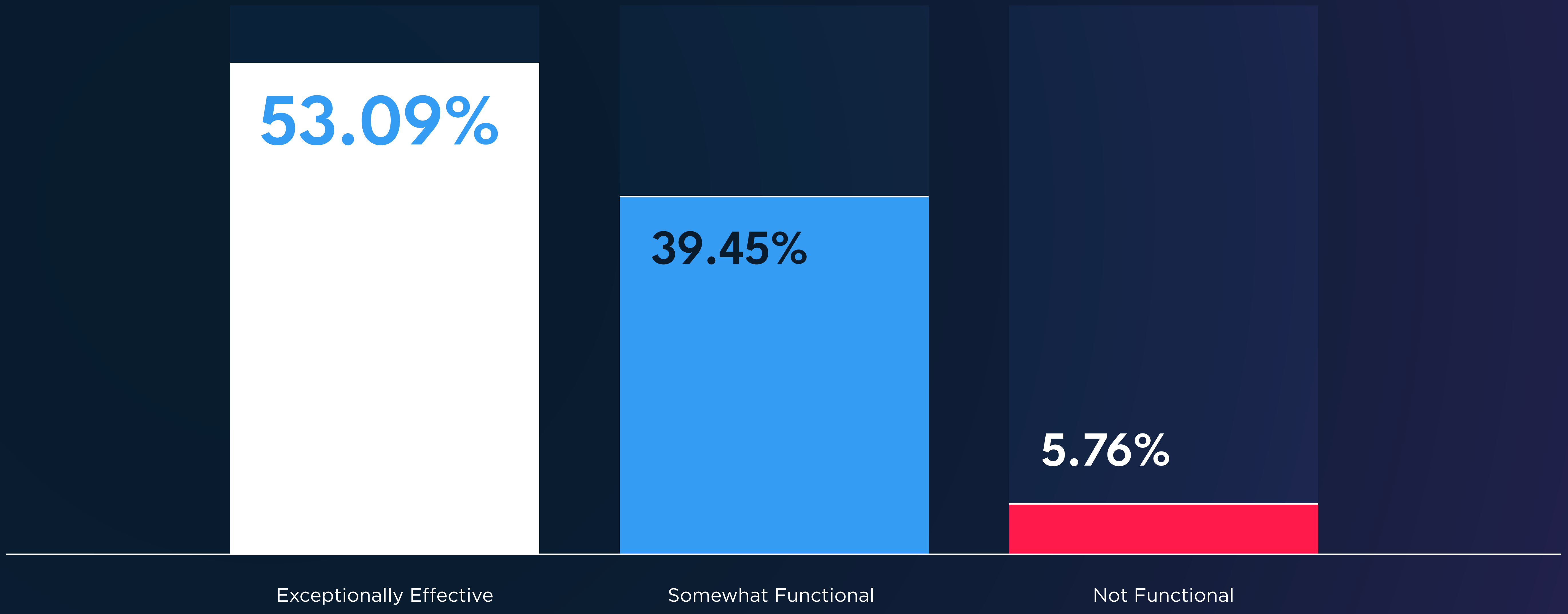
According to most enterprises,

it is

.....but there is certainly room for improvement.

53.09% of enterprises find the current level of ARM architecture support in Linux operating systems as either “exceptionally effective” (the highest rating) or “fully functional,” the second-highest rating.

However, **39.45%** of enterprises rated the current level of support for ARM architecture as just “somewhat functional” and a small minority of **5.76%** believe it to be “not functional.”



The less-than-perfect view of the current level of support may be due to:

a need for more awareness and education on ARM capabilities in enterprise Linux

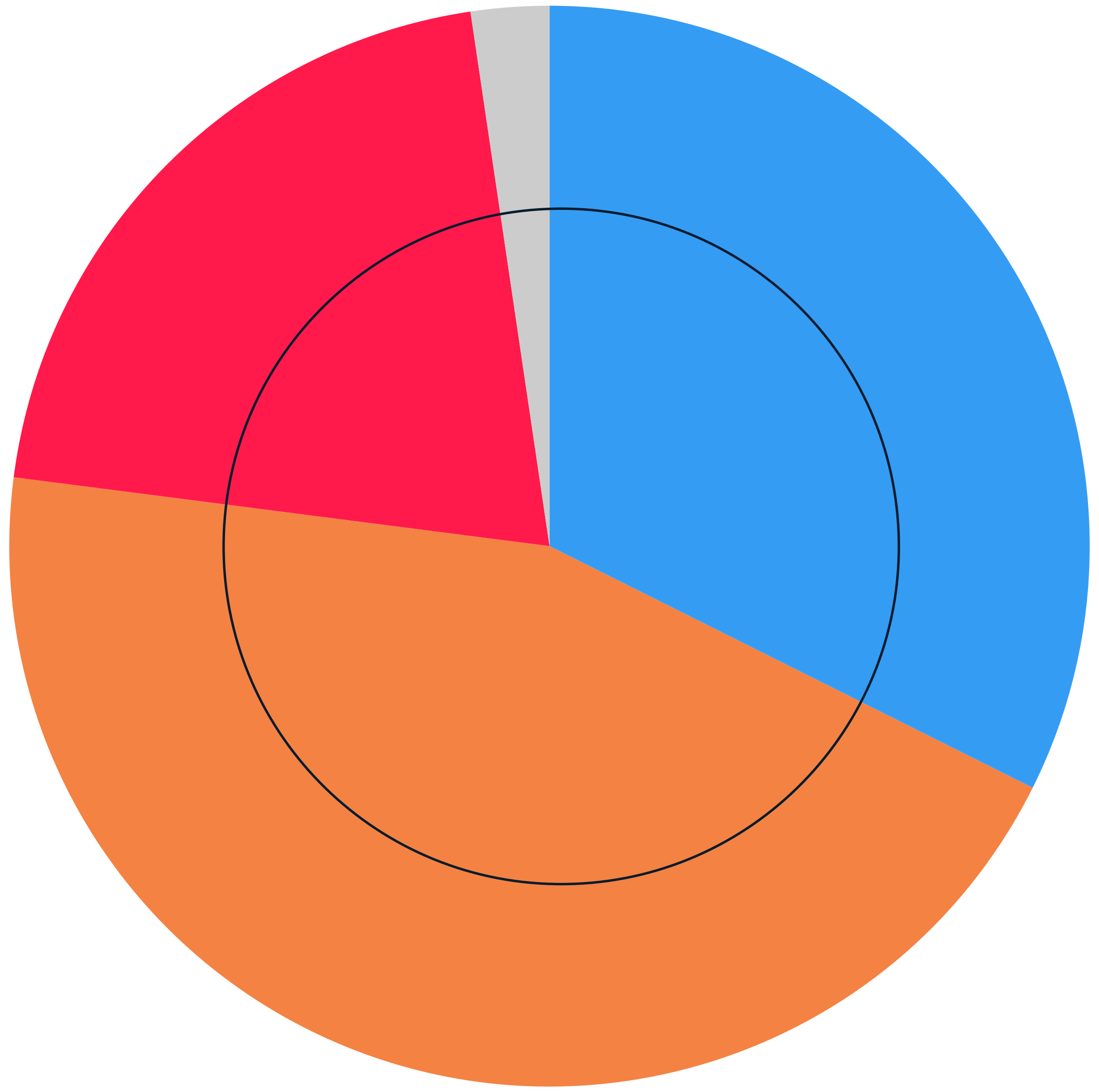
or

incomplete third-party support from applications or workloads

...both of which may be impairing the perceived functionality of the platform.

Looking forward to the next year of ARM support in enterprise Linux, the future looks bright

Expectations for ARM Architecture Support in Linux Over the Next 12 Months



32.34%

expect that ARM support will improve (most of which already had a positive view)

44.68%

believe that the level of ARM support will remain the same, with **58.10%** of them believing that it is currently either fully functional or exceptionally effective

2.34%

were unsure about their expectations for ARM support in Linux

Only 20.64%

anticipate a degradation in ARM support

Why this level of expected degradation?

Perhaps:

1. Some enterprise Linux users may become demotivated when hearing about the latest Linux improvements for ARM being rejected by upstream kernel maintainers.

or

2. A diversified environment is expected by some to lead to different platforms implementing the ARM instruction in a way that introduces new bugs or new ARM generations being introduced.

SECTION 3

Linux Patch & Vulnerability Management

How many organizations have been impacted by cyberattacks?

Are organizations who have been affected by cyberattacks knowingly vulnerable before security incidents occur?

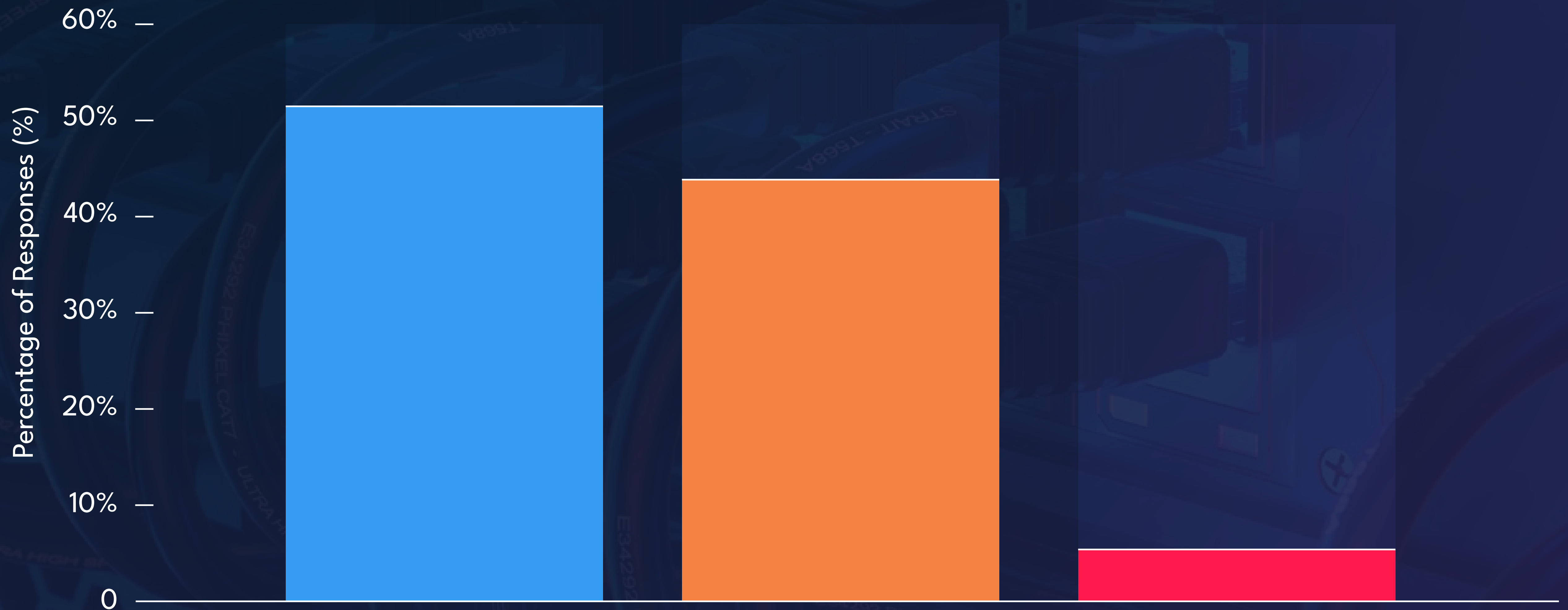
How effective are organizations at detecting vulnerabilities and how quickly do enterprises apply vulnerability patches?

Most organizations are being impacted by cyberattacks

Over Half

of enterprises experienced a cybersecurity incident in the past 12 months

When asked whether their organization has suffered a cybersecurity incident, like a malware attack, a ransomware attack, etc.,



50.93%
indicated they did

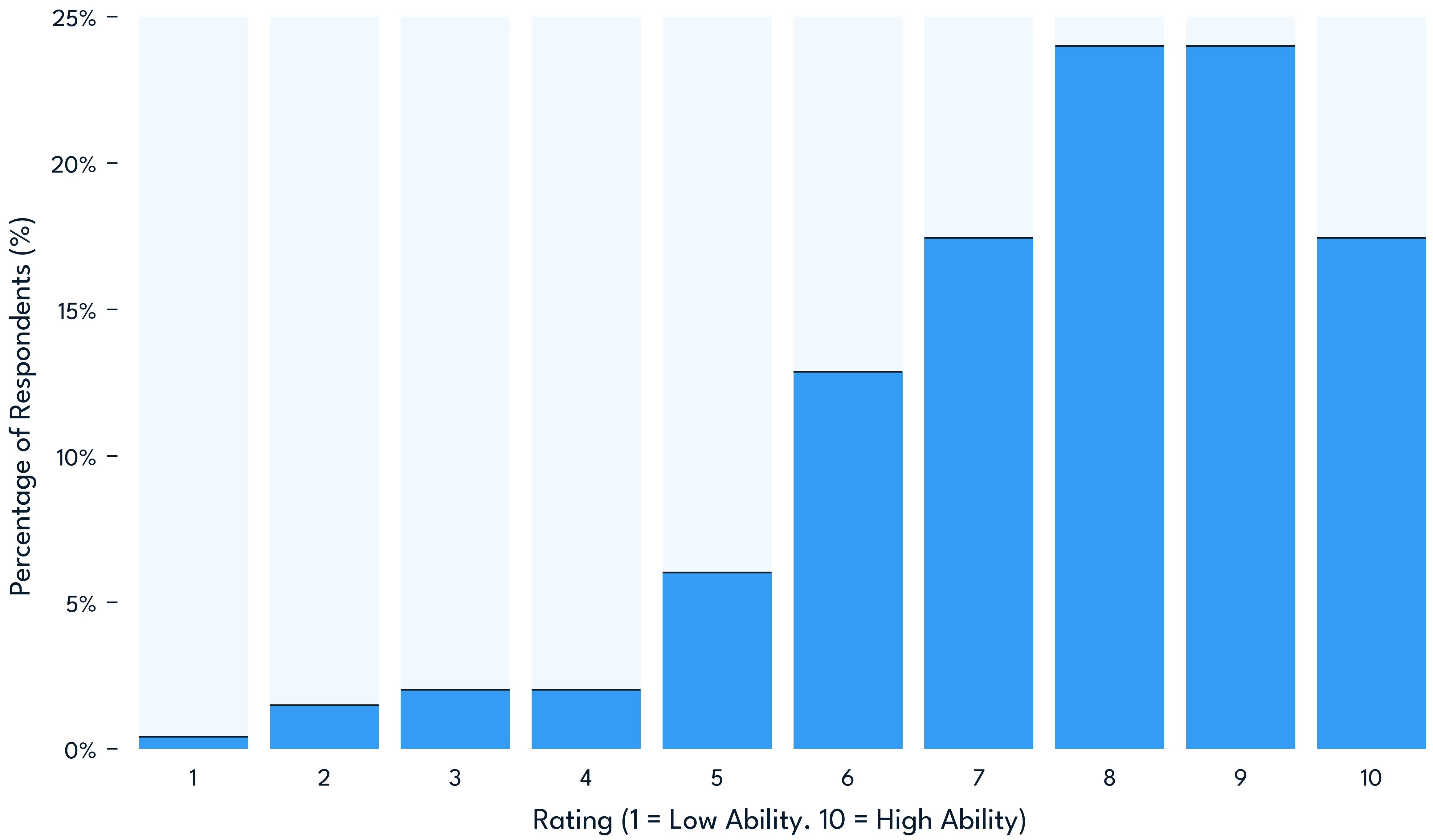
43.63%
indicated they did not

5.43%
were unsure

But, at the same time, most enterprises are confident in their ability to quickly detect vulnerabilities and prevent threats.

58.06% rated their prowess for threat detection and prevention as 8 or better

Organizations' Ability to Detect Vulnerabilities and Prevent Threats

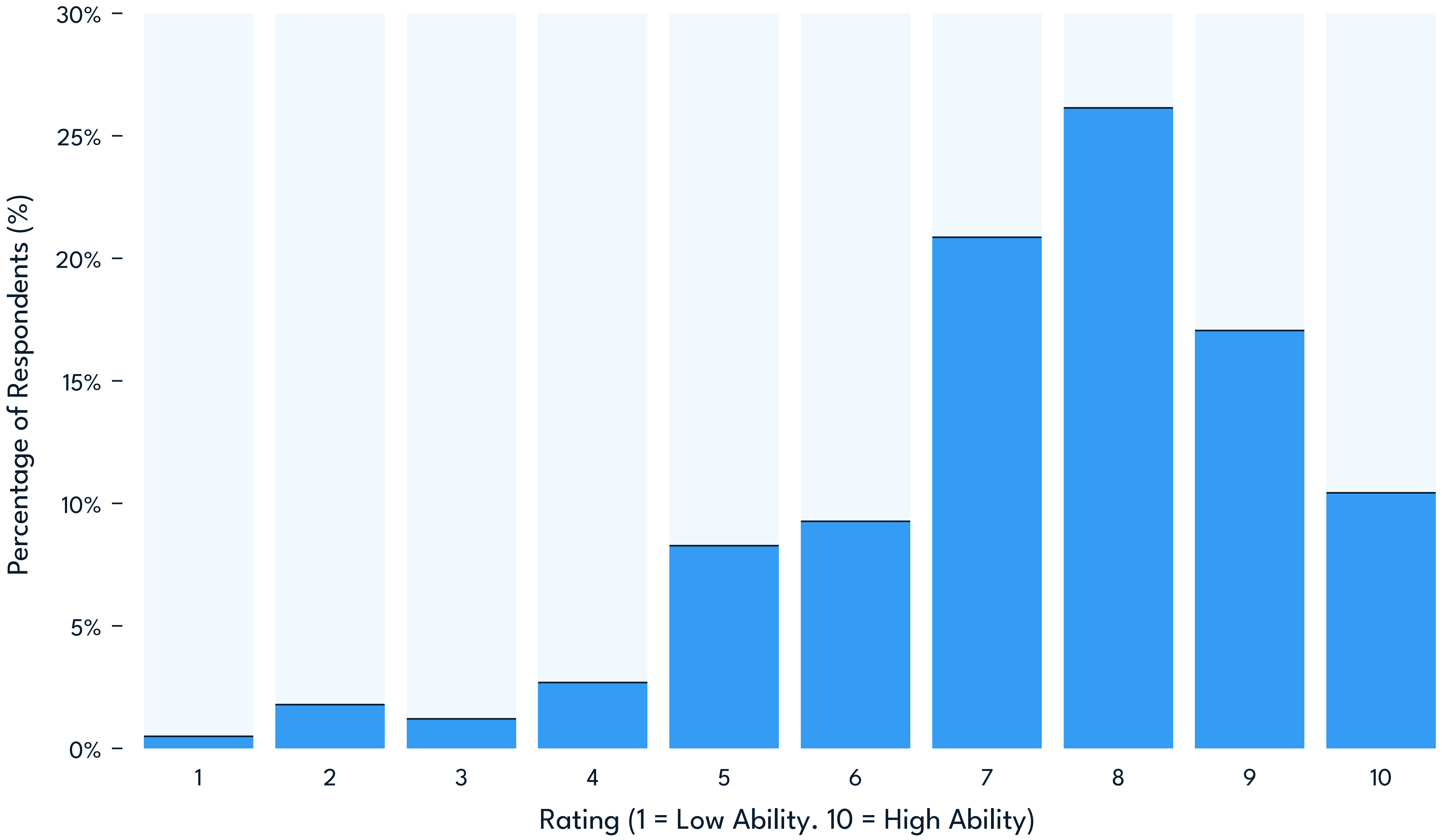


However, a sizable share of enterprises (41.94%) express low-to-medium confidence

And more than half of organizations believe they have a strong ability to patch in a timely manner

53.83% of enterprises surveyed self-assessed this ability as 8 or better

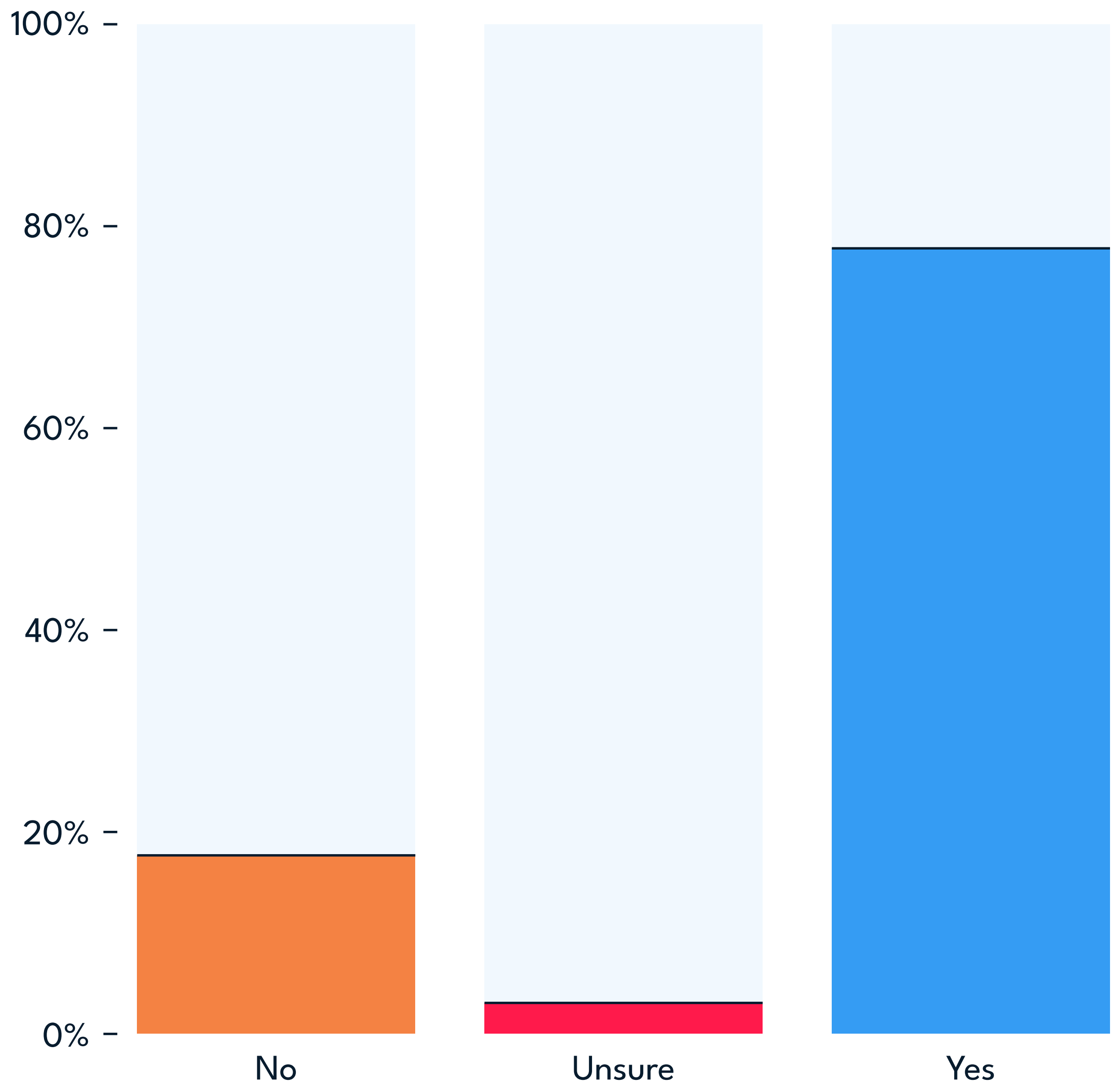
Organizations’ Ability to Detect Vulnerabilities in a Timely Manner



However, while most enterprises exhibit confidence in their vulnerability detection and patching abilities, the data shows a different reality:

The vast majority of enterprises that were impacted by a cyberattack already knew they were vulnerable prior to the incident

Organizational Awareness of Vulnerability Prior to Cybersecurity Incident



78.07%

of respondents indicated that their organization was aware of its vulnerability before the incident occurred.

Meanwhile, only

18.42%

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.**

Despite the awareness of vulnerabilities, these enterprises still experienced cybersecurity incidents, highlighting **the need for organizations to act quickly to mitigate emerging problems as they appear rather than wait for threat actors to gain an opportunity to exploit them.**

The high percentage of enterprises that were aware of vulnerabilities yet still faced incidents underscores the challenges in cybersecurity management and the need for more robust and proactive strategies.

Despite the Confidence, the Industry Has a Patching Problem

Unapplied patches (that were available at the time) caused most of the self-reported cybersecurity incidents in 2023

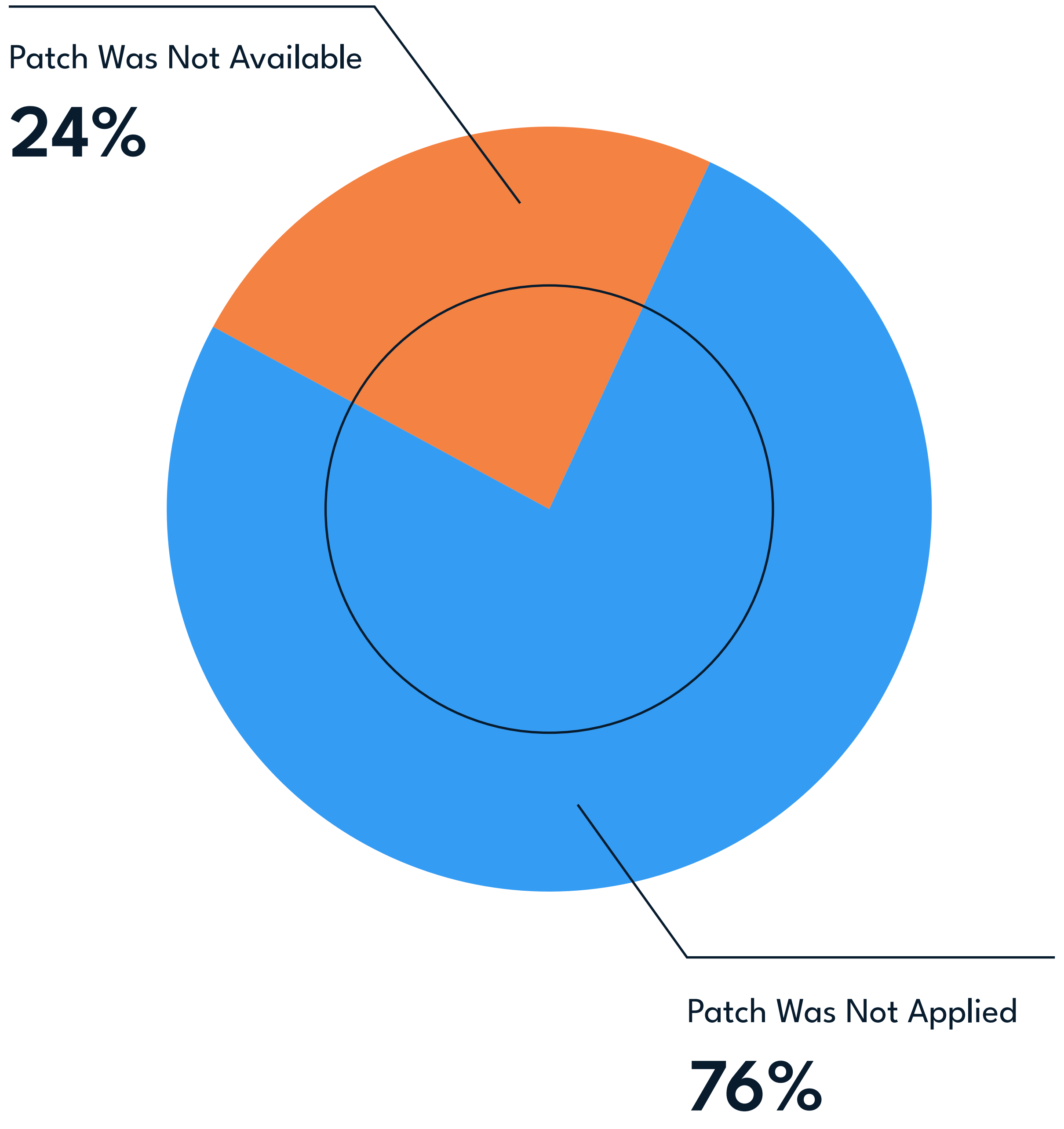
76%

of the organizations that experienced a cybersecurity incident in the last 12 months reported that the incident occurred while a patch was available but had not been applied.

This highlights a widespread challenge in patch management across various organizations. Despite the availability of patches, there is a delay or oversight in applying them.

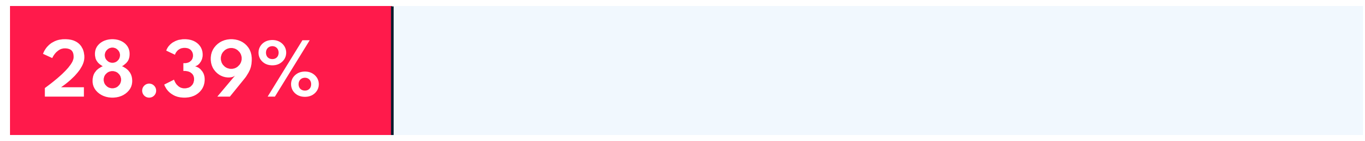
This may be due to outdated patching processes that require enterprises to interrupt services and/or cause significant downtime just to apply certain patches – a burden that can be lifted with the implementation of automation and non-disruptive patching solutions.

Percentage of Organizations with Incidents Caused by Available but Unapplied Patches



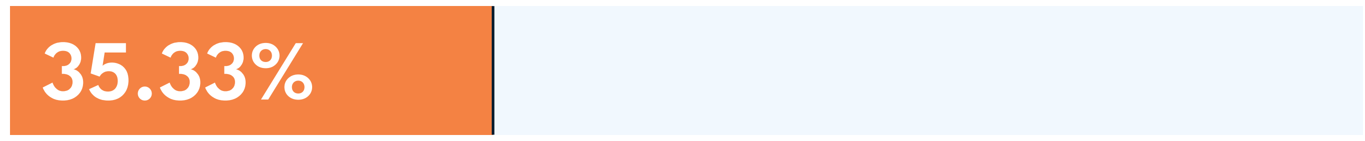
The Gap Between Perception and Action

Organizations May Be Underestimating the Impact of Vulnerabilities



28.39% of enterprises that rated their ability to patch vulnerabilities at 8 or better acknowledged awareness of their vulnerabilities prior to experiencing a cybersecurity incident.

Despite Availability of Patches, There Is Often a Delay in Applying Them



35.33% of the organizations that rated their ability to patch vulnerabilities as 8 or better experienced a cybersecurity incident when a patch was available but not applied, highlighting a widespread challenge in patch management.

The underestimated impact of vulnerabilities and delay in patching them highlight the challenges associated with vulnerability prioritization, and may be indicative of an inability to schedule a system reboot that's necessary to apply a patch, difficulty in coordinating maintenance windows, or other issues associated with a conventional patching approach.

There are more enterprises that have increased their patching times than there are those that have decreased their patching times in the last year

30.90%

of enterprises have either increased or significantly increased their patching time

While

28.86%

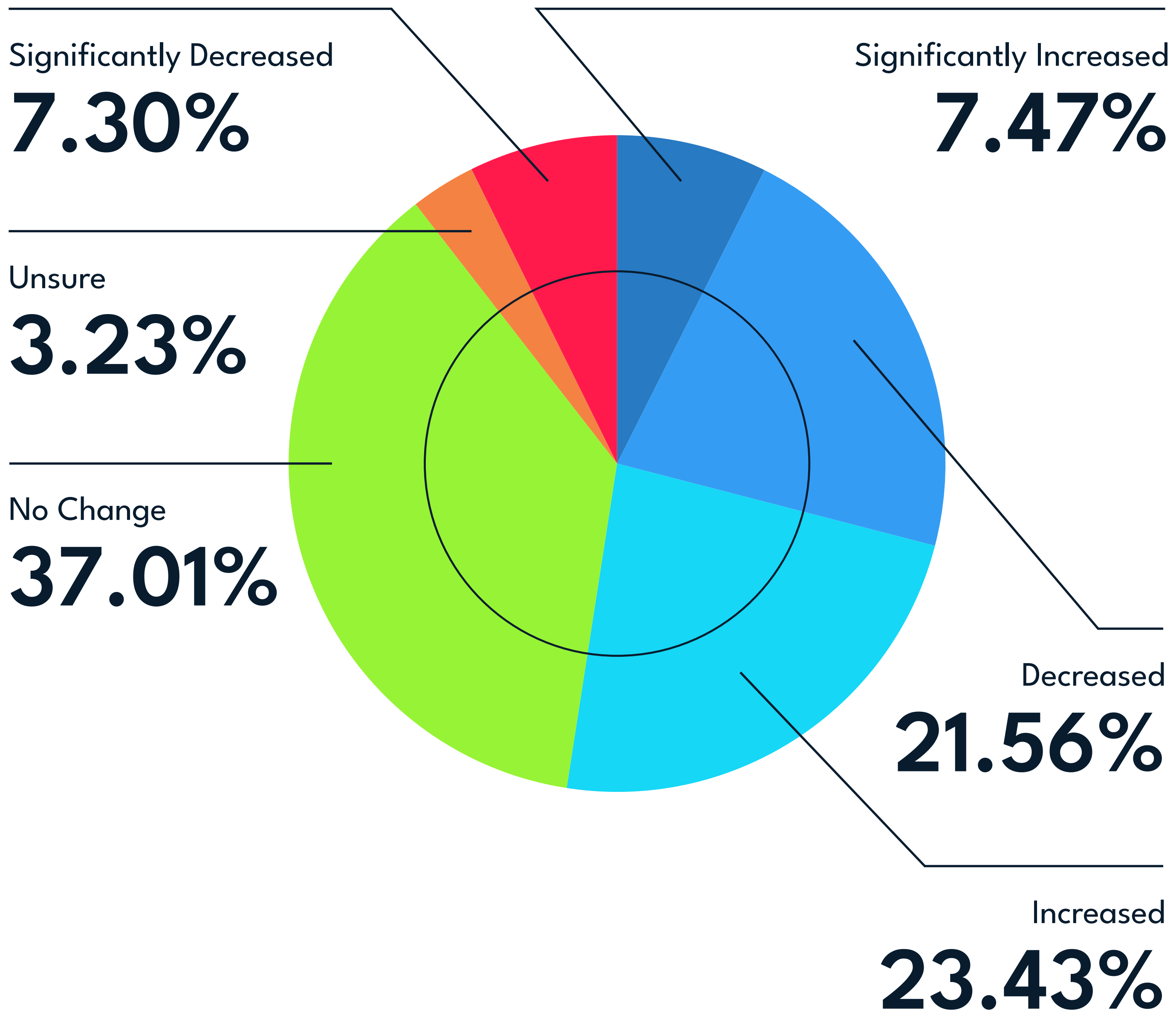
have decreased or significantly decreased that patching time

and

37.01%

of enterprises reported no change to their TTM in the past year

Changes in Patching Time



It appears that, while there is observable improvement in patch management across a portion of the industry, many enterprises still struggle with improving or maintaining their ability to patch in a timely manner. **Many organizations may benefit from enhanced processes, automation, and continuous efforts toward improvement to generate better patch management outcomes.**

Based on the data we have,

companies that self-assess their ability to patch in a timely manner as high tend to experience cybersecurity incidents at a lower rate

Of those who expressed a high level of capability (8 or better),

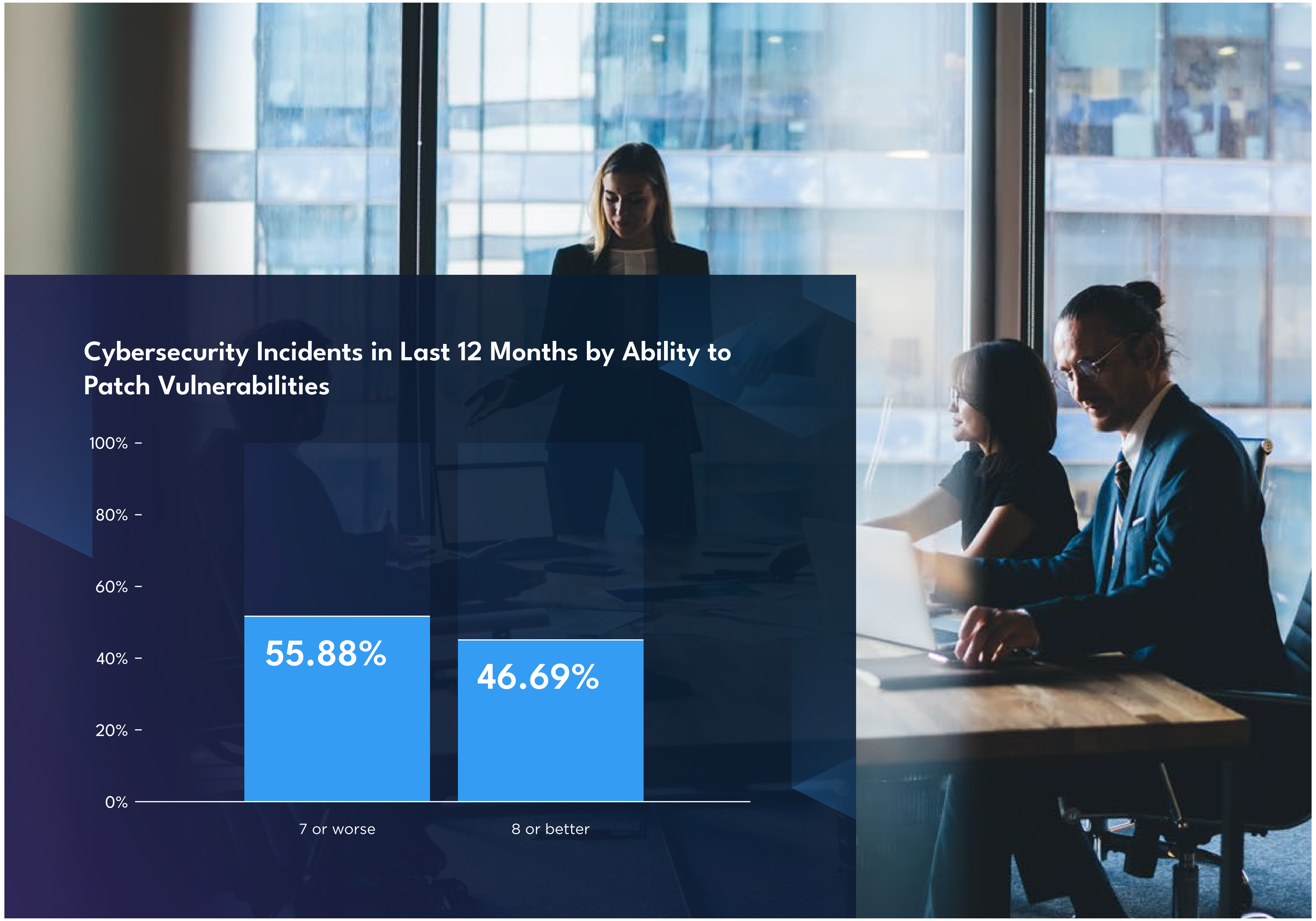
46.69%

reported experiencing a cybersecurity incident

Of those who expressed a low level of capability (7 or lower),

55.88%

reported experiencing a cybersecurity incident



Cybersecurity Incidents in Last 12 Months by Ability to Patch Vulnerabilities

Open-Source Supply Chain Security

The open-source supply chain used in enterprise Linux encompasses a range of software components, tools, and libraries that are openly available for use and modification. Popular components in this supply chain include programming languages like Java, Python, and PHP, as well as numerous libraries and packages that enhance functionality, such as OpenSSL for security or Apache Struts for web applications. However, organizations' reliance on this supply chain introduces specific vulnerabilities.

Since the source code is publicly accessible, it becomes easier for malicious actors to employ different tactics to compromise open source components. For example, a flaw in a widely used Java package endangers multiple systems globally, making it a significant target. This risk is heightened by the common practice of using third-party dependencies in software development. If one of these dependencies is compromised, it can lead to a cascade of security issues across all applications that use it.

For enterprises, this risk is particularly dangerous because it can lead to data breaches, service disruptions, and loss of customer trust. Moreover, identifying and resolving these vulnerabilities can be challenging due to the complex web of transitive dependencies and the need for constant vigilance and updates. **That's why managing open-source supply chain risk is crucial for enterprise Linux users to maintain security and operational integrity.**

Are enterprises aware of the open-source supply chain risks they face?

How do enterprises vet and approve open-source components, and how confident are they in their open-source supply chain security?

Which part of organizations are typically responsible for supply chain security processes?

What challenges do organizations typically face in securing their open-source supply chain?

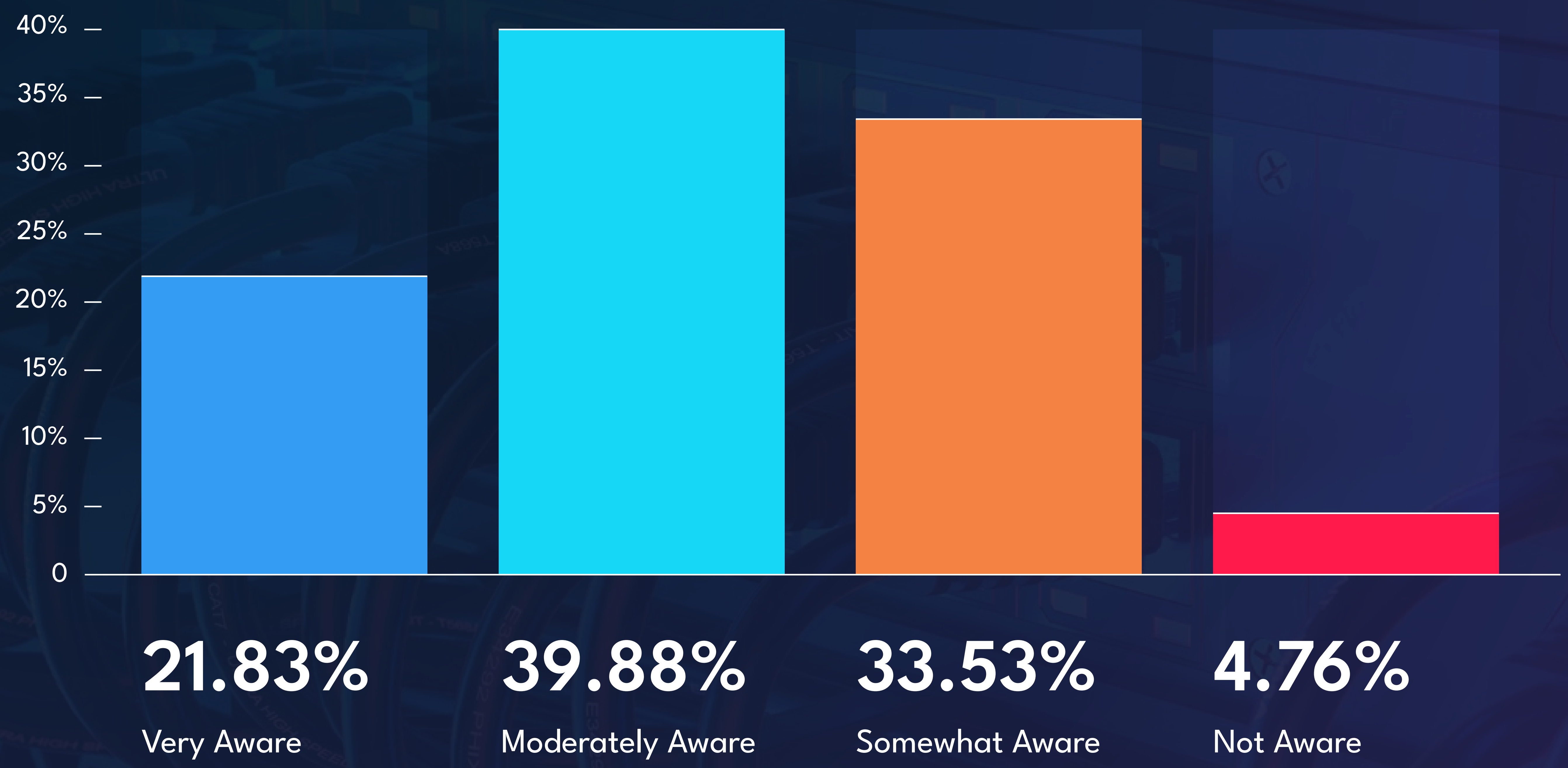
Most organizations are at least moderately aware of open-source supply chain security risks

but a deeper, more comprehensive understanding might be lacking

61.71%

believe their organization to be either moderately aware or very aware

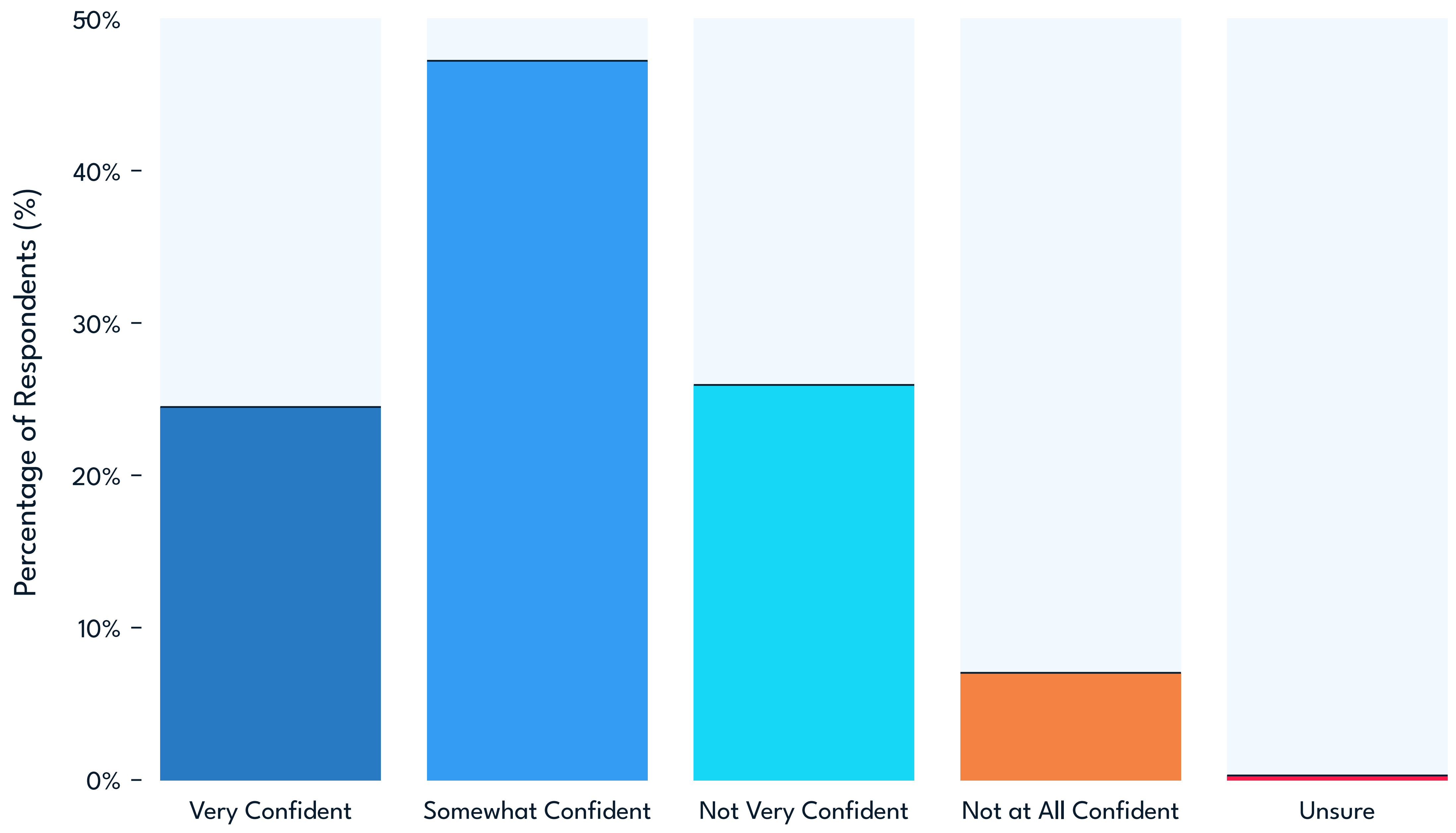
Organizations' Awareness of Open-Source Supply Chain Security Risks



While the vast majority of survey respondents said their organization had some level of awareness of these risks, the fact that only 21.83% of participants claimed their organization to be "very aware" may indicate a need for education on open-source supply chain risk among organizations that use enterprise Linux – and potentially improved security practices to mitigate this risk.

At the same time, nearly a third of the enterprises surveyed have little to no confidence in their own open-source supply chain security

Confidence in Open-Source Components' Security and Up-to-Dateness



30.95%

of enterprises are either not very confident or not at all confident that the open-source components they use are up to date and secure.

While

45.04%

of enterprises are somewhat confident, only

23.81%

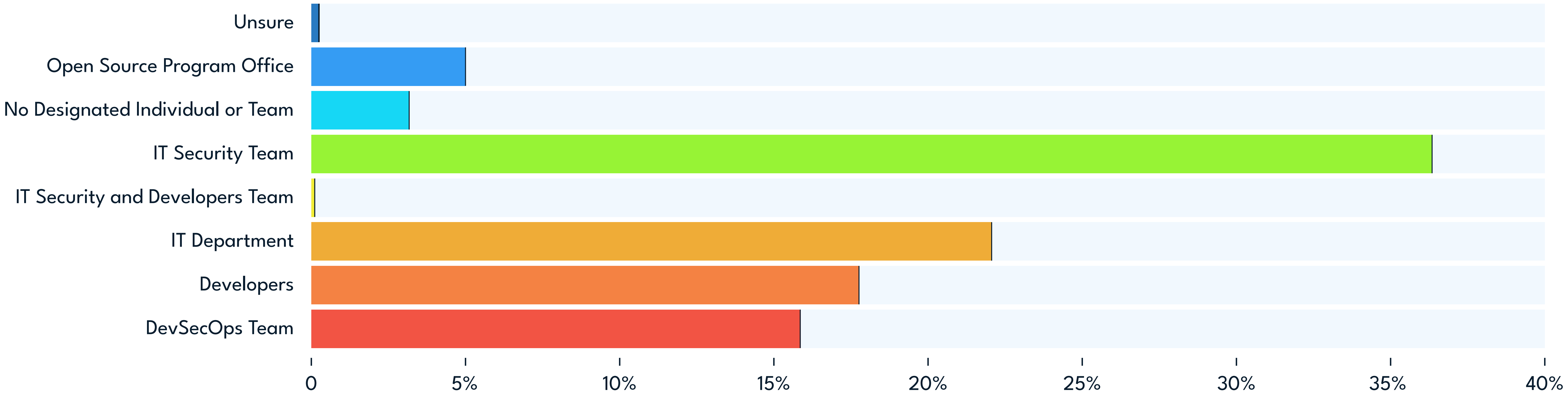
are very confident

Such a small share of enterprises expressing high confidence in this area indicates an industry-wide need for better security practices, regular training, and staying updated with the latest developments in open-source supply chain security.

IT security teams were most frequently listed (by 37.10% of respondents) as primarily responsible for overseeing the security of the open-source supply chain inside of organizations with the IT department in a general sense in second place with 21.63%.

However, a considerable number of enterprises assign this responsibility to other teams.

Primary Responsibility for Open-Source Supply Chain Security



Less than 4% have no designated individual/team or are unsure which team is responsible for supply chain security

A lack of appropriate assignment could mean that these risks end up ignored by everyone in the organization.

The small number of enterprises in this category could benefit from defining and clarifying roles in open-source security management.

A More “Modern” Approach: DevSecOps

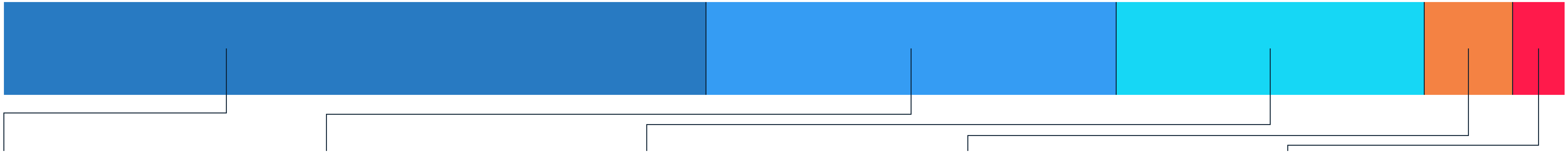
15.67% identify the DevSecOps team as the primary overseer of open-source supply chain security – an approach in which development, security, and operations are closely integrated.

Integrating Security into the Development Process

17.46% of respondents indicate that developers are primarily responsible for open-source supply chain security, demonstrating that a remarkable share of enterprises have some sort of integration of security into their development workï¬‚ows.

When it comes to vetting their open-source components, enterprises are often adopting a strategic approach and only standardizing processes for key projects or evaluating their components on a case-by-case basis

Enterprises' processes for vetting and approving open-source components before their use in projects:



45.24%

have a **standardized vetting process, but it is applied only to key projects.**

This suggests a targeted approach to risk management, focusing resources on critical areas.

26.98%

report a **comprehensive vetting process that is applied to all open-source components.**

This reflects a robust and thorough approach to open-source software management and security.

19.25%

use an **informal vetting process, evaluating open-source components on a case-by-case basis.**

This may indicate a more reactive or flexible approach, potentially with varying levels of scrutiny.

5.16%

have an **automated vetting process supplemented by manual oversight** for critical components.

This implies a blend of efficiency and focused attention where necessary.

2.78%

have **no formal process in place** for vetting open-source components.

This could signify a potential vulnerability in their software supply chain security.

In their efforts to manage patching for open-source software components, enterprises face a host of challenges

When asked about the primary challenges they face in managing patches for open-source software components, organizations voiced diverse concerns:

Dependency management is a major challenge

41.94% of enterprises indicated that managing dependencies affected by patches is a significant challenge.

The complexity of maintaining compatibility and stability across various interdependent components is a primary concern for many organizations.

Tracking open-source components is difficult

35.65% of enterprises reported difficulties in tracking numerous open-source components across different projects.

Overseeing and updating multiple software components is a common obstacle, especially in larger or more complex software ecosystems.

Code refactoring and updates require significant effort

33.96% of enterprises face challenges with code refactoring due to major updates or changes.

Keeping up with evolving software and the need for constant adaptation is a considerable task for many organizations.

Timeliness in patch identification is crucial

25.13% of enterprises find it challenging to identify applicable patches in a timely manner.

Efficient processes and tools for monitoring and applying software updates is vital.

Stability testing of patches is a concern

24.79% of enterprises claim that the need for testing and validating the stability of patches before deployment is a significant challenge.

There seem to be common concerns about the potential impact of patches on system stability and the need for rigorous testing protocols.

Resource constraints impact patch management

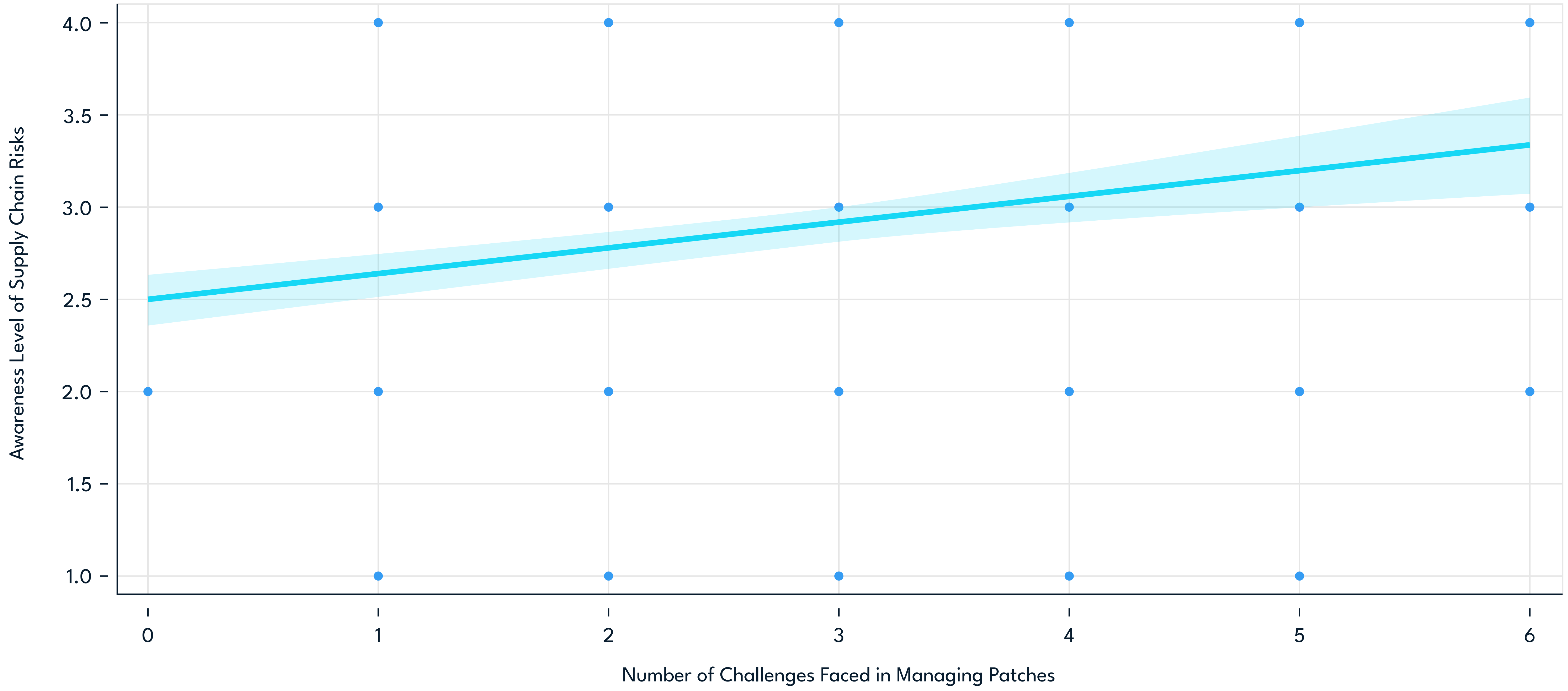
17.49% of enterprises say limited resources or expertise is a primary challenge they face.

There may be a need for more skilled personnel, better training, or more efficient management practices in the realm of open-source software.

The more aware of supply chain risk an organization is, the more challenges they tend to experience

As enterprises surveyed were able to select multiple challenges associated with managing patches for open-source software components, we found a positive correlation between the number of challenges organizations face and their awareness of open-source supply chain risks.

Correlation between Number of Challenges Faced and Awareness of Supply Chain Risks

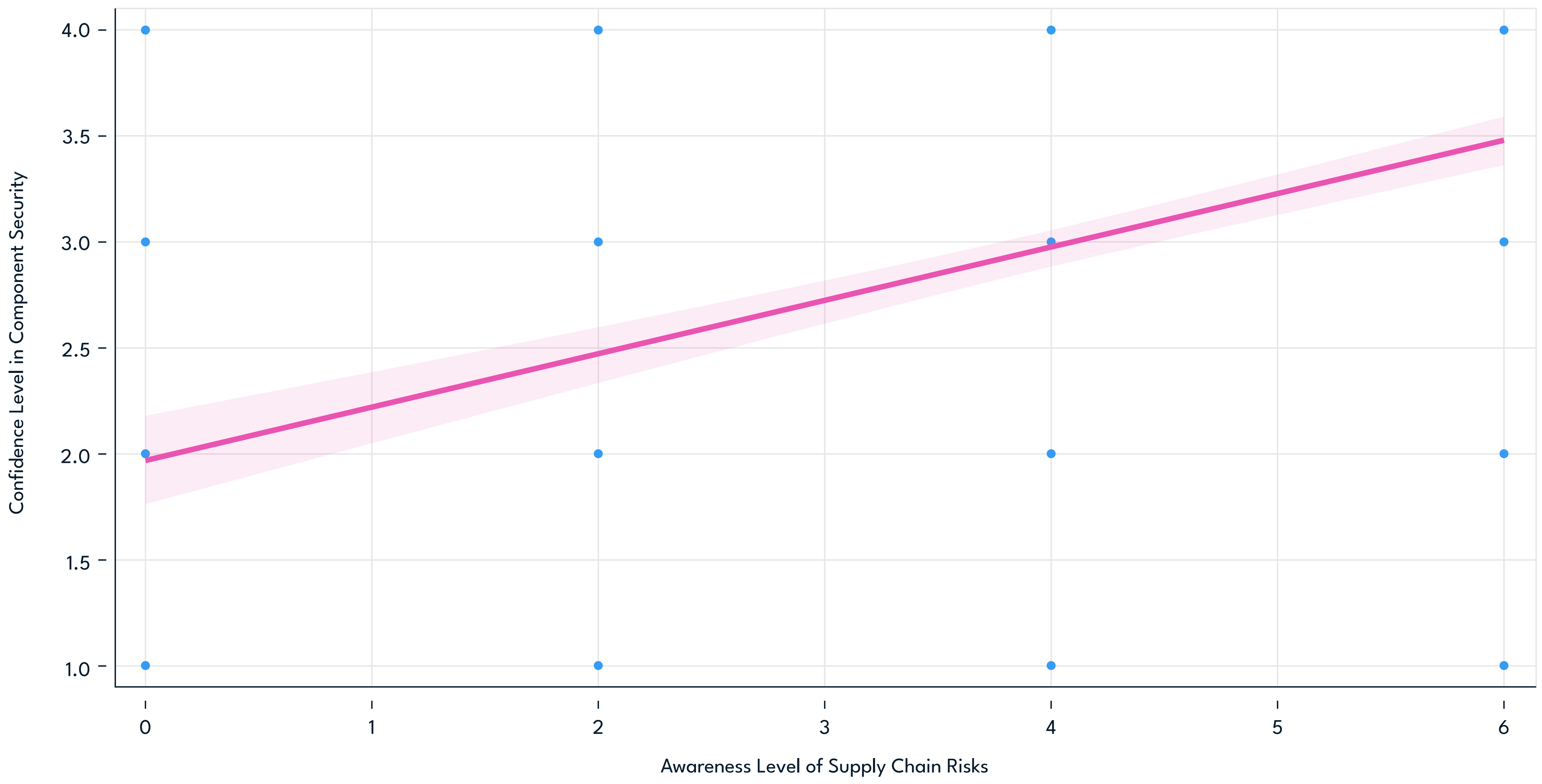


Organizations with a greater awareness of supply chain risks might be more attuned to the complexities of managing open-source components. This heightened awareness could lead to better recognition and reporting of challenges, as they are more likely to identify and acknowledge issues that less aware organizations might overlook.

Awareness also correlates to confidence in open-source security

The more aware an organization is, the more confident they tend to be about managing open-source supply chain risk

Correlation between Awareness and Confidence Levels



Awareness not only correlates with the recognition of more challenges but also correlates with confidence in open-source security. This may imply that organizations that are more aware take more comprehensive actions, which in turn increases their confidence in the security of their open-source components.

SECTION 5

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

The adoption of Artificial Intelligence (AI) in enterprise environments is gaining remarkable momentum, revolutionizing how businesses operate and innovate. A significant number of organizations are rapidly integrating AI into their systems.

This adoption is not just a trend but a strategic necessity, driven by the need for more efficient data processing, enhanced security features, and the automation of routine tasks. AI tools and frameworks are being leveraged for a myriad of purposes, including predictive analytics, machine learning, real-time decision making, and process automation.

How many enterprises are using or planning to use AI-powered software?

How many organizations are rejecting AI technology?

What share of enterprises are noticing positive results from AI adoption?

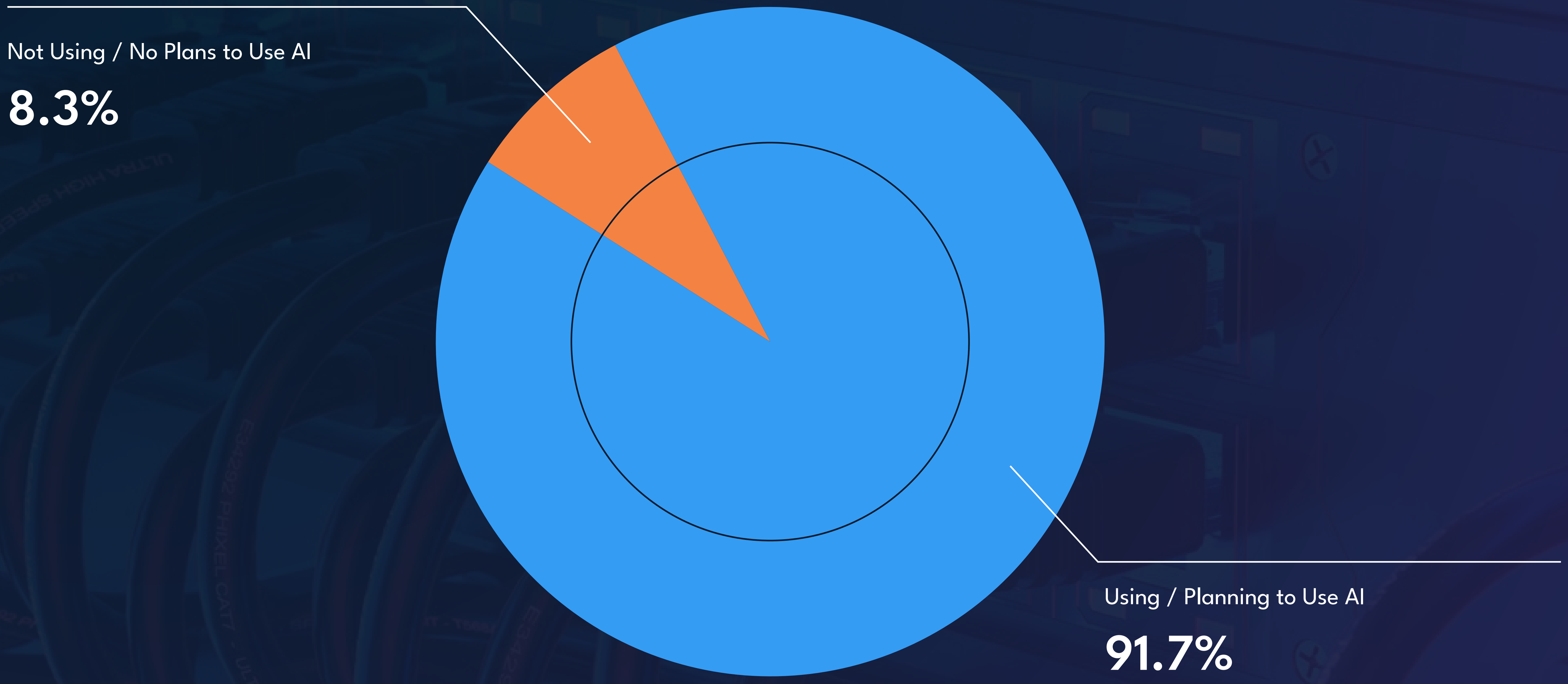
Are enterprises planning on developing their own in-house AI technologies?

The vast majority of enterprises are already riding the AI wave

91%

of organizations surveyed indicated that they are either currently using AI-powered software in their daily operations or will do so in the next 12 months

AI Software Adoption



AI has become a significant part of strategic planning and digital transformation initiatives as many organizations are planning to deploy it within the next 12 months.

The high percentage of enterprises investing in AI suggests that **many see AI as a key factor for gaining a competitive edge, improving efficiency, or innovating in their products and services.**

When we look at the three sectors from which most of our survey participants come from, we see a remarkable disparity:

Sector	Using/Planning to Use AI	Not Using/No Plans to Use AI
Industrial/Manufacturing	96.32%	3.68%
Telecom	94.38%	5.62%
IT/Technology	86.19%	13.81%

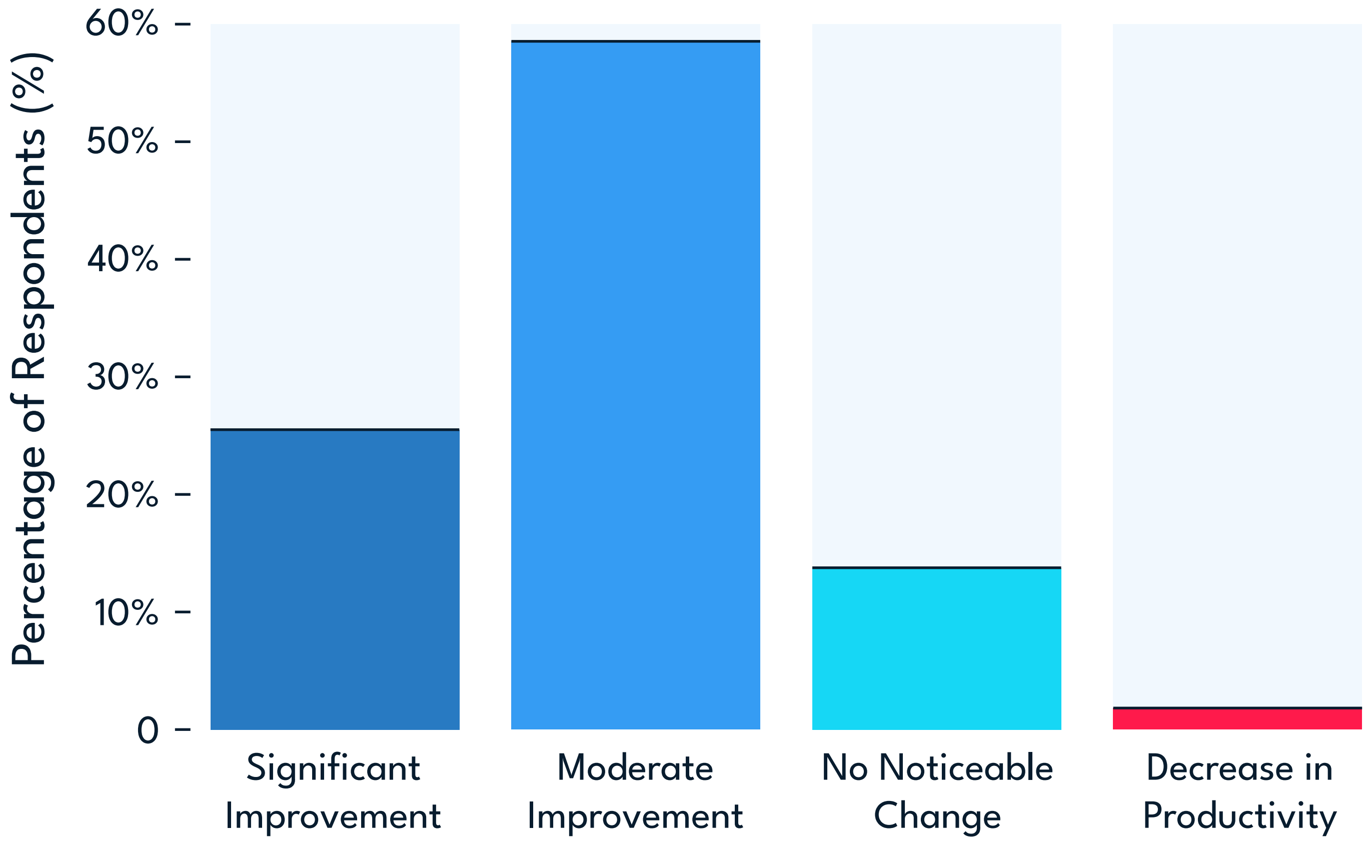
It appears that IT/Technology lags behind in adoption and plans to adopt when it comes to AI, which can be considered an unexpected outcome compared to Industrial/Manufacturing – which is traditionally considered a more conservative sector that might be less quick to adopt new innovations.

IT teams are typically known for being good at adopting new technologies but can often fall somewhat short when they need to change their processes. AI is a new technology that requires organizations and the teams within them to adopt processes to take advantage of it properly, and IT's lower rates of adoption of AI may extend to other innovations – like live patching for vulnerability management or new types of automation. Historically, IT has been known to slowly adopt landmark evolutions in technology, such as with containerization, virtualization, or even the cloud itself.

AI-powered outcomes are looking up

Of the enterprises using AI-powered software, most have noticed an improvement in their workflow or productivity as a result – and less than 1% have noticed a decrease in productivity

Impact of AI-Powered Software on Workflow and Productivity



25.89%

of enterprises reported a significant improvement

59.16%

of enterprises reported a moderate improvement

14.11%

of enterprises reported no noticeable change

0.84%

of enterprises reported a decrease in productivity

What could be causing 14.11% to not notice a change either way after adopting AI-powered software?

Perhaps organizations haven't found the right match for AI or AI doesn't directly translate into their current projects or goals – a solution-looking-for-a-problem scenario. Professionals across various industries may also fear there's a risk of AI "taking their jobs," so this phenomenon may be due to a subconscious effort to not effectively deploy AI within their organizations. Companies may also struggle to effectively implement and utilize AI software because they lack the necessary expertise.

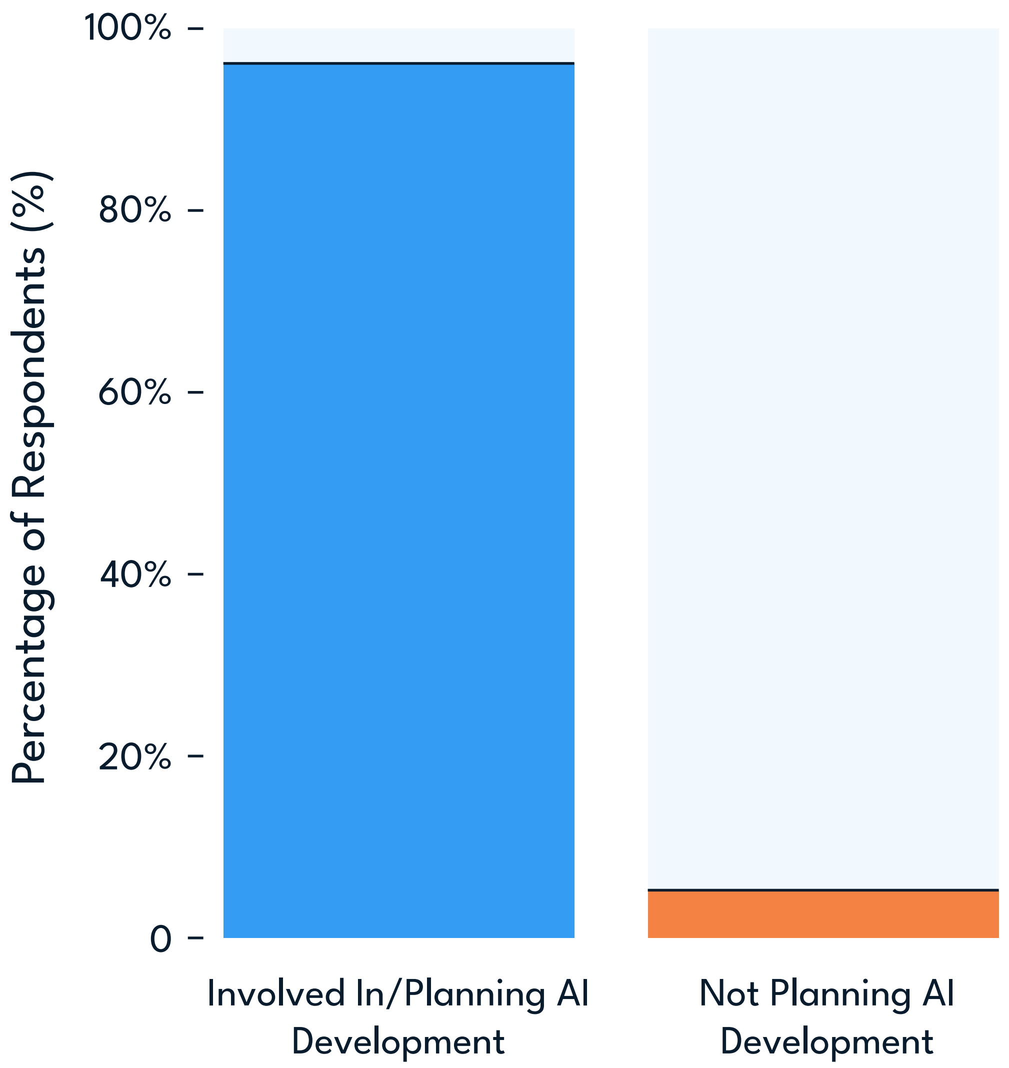
A preference for customized in-house AI solutions?

The overwhelming majority of enterprises using or planning to use AI are jumping into AI development themselves

95.37%

of respondents in this category are currently involved in or planning to start AI software development in the near future

Involvement in AI Software Development



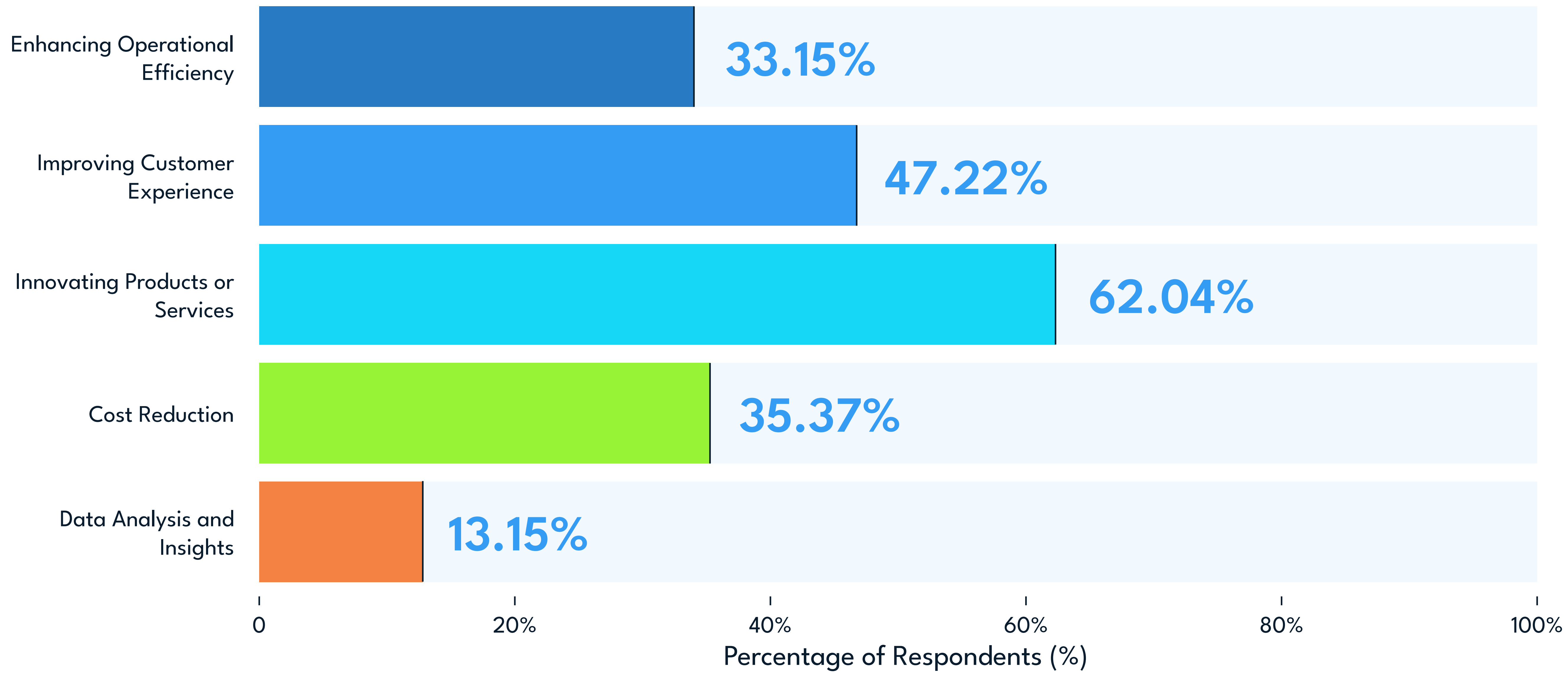
The majority share of AI-utilizing enterprises that plan on developing AI solutions themselves might suggest a preference towards in-house AI development.

This could be due to a desire for:

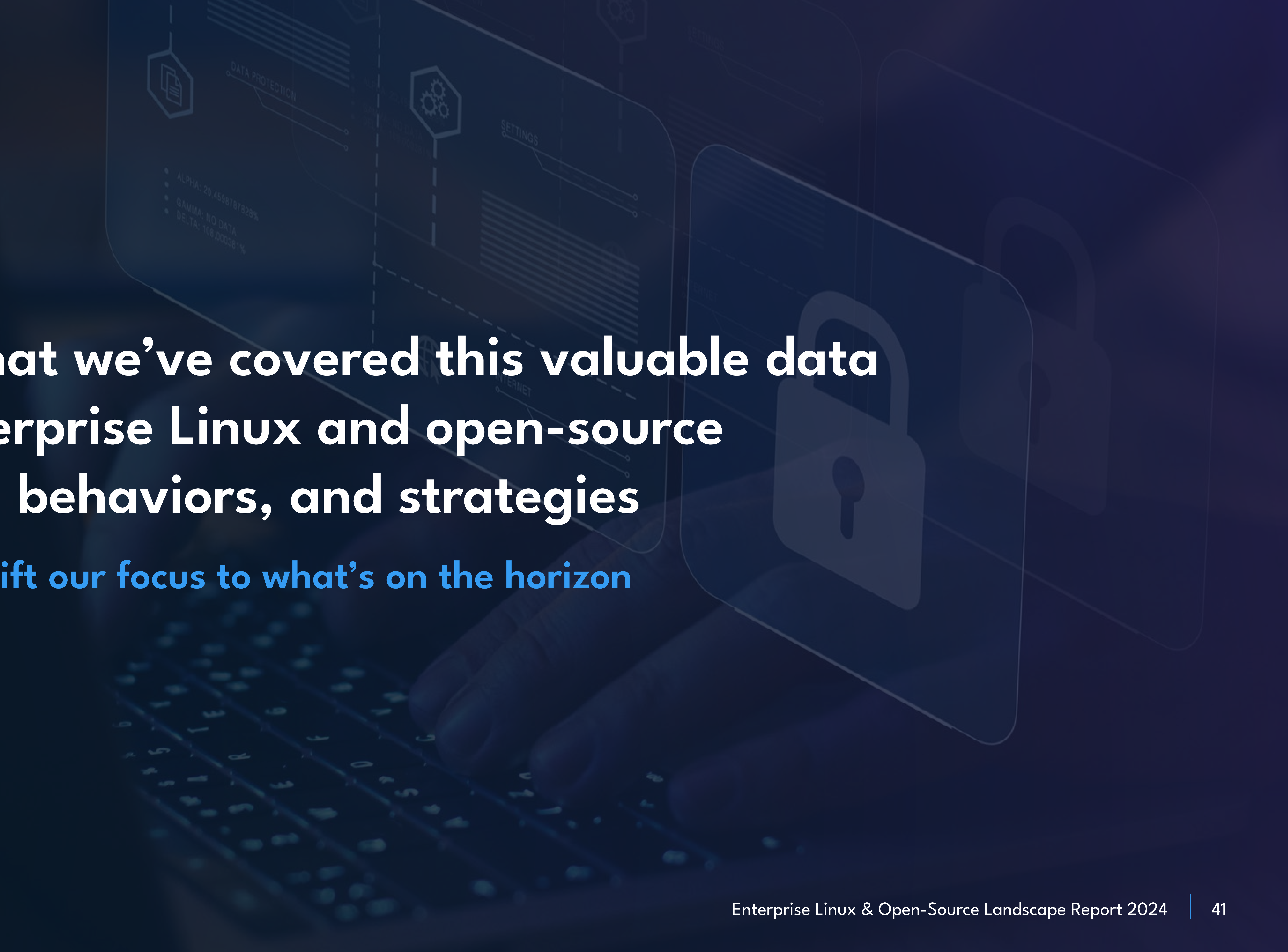
- Customized solutions
- More control over the technology
- A strategic decision to build AI capabilities internally
- Meeting compliance requirements around data privacy

Most organizations aim to innovate products or services with AI while improving customer experience is the second most popular goal

Primary Expectations from AI-Powered Software



About a third of respondents seek to use AI for reducing costs and enhancing operational efficiency and the lowest-scoring goal is data analysis and insights.



Now that we've covered this valuable data on enterprise Linux and open-source trends, behaviors, and strategies

we can shift our focus to what's on the horizon

Looking Ahead

Our 2024 survey on the enterprise Linux and open-source industry unveils pivotal trends shaping the technological landscape that organizations are navigating today. The growing preference for open-source solutions over proprietary software is driven by the obvious benefits that open-source software provides. This trend indicates a shift towards viewing open source as essential for security, quality, and strategic innovation in enterprise infrastructures.

But, of course, organizations adopting open source also seek to strike a balance between cost efficiency and robustness of their IT infrastructures. This is exemplified by the migration from CentOS to free alternatives like AlmaLinux and Rocky Linux, demonstrating organizations' pursuit of affordable, yet dependable, software solutions.

With a clear trend towards the adoption of AI-powered software, 2024 will likely see an increase in AI integration across different sectors. Organizations will continue to seek AI solutions to enhance operational efficiency, customer experience, and innovation. The in-house development of AI technologies will become more widespread, emphasizing the importance of AI in maintaining competitive advantage and adapting to changing market demands.

We are observing a similar trend in the adoption and consolidation of ARM technology within the server space, possibly linked to the increasing use of AI. ARM-based systems present a cost-effective option for data analysis and high-performance computing, both of which are highlighted as the primary use cases for deploying ARM servers in the report and are also common in AI applications. There may also be a natural alignment between AI and ARM technologies, given that the cost of current dedicated AI accelerator hardware is comparable to that of state-of-the-art complete ARM systems, making the latter a more comprehensive solution. Therefore, based on these observations, we can assume that the specific requirements of AI-driven applications are likely to boost ARM's support and adoption within the Linux ecosystem in the future.

As organizations navigate these changes, the challenges of cybersecurity, especially in vulnerability and patch management, alongside the strategic management of open-source supply chain risks, emerge as critical focal points. If your organization is not adopting the most advanced Linux and open-source cybersecurity practices, it's putting itself at risk of a costly cybersecurity incident – like the ones we've analyzed in this report.

What Now?

The data surrounding the state of enterprise Linux and open source has illuminated an industry where many organizations can greatly benefit from improved security practices, better vulnerability management solutions, and a more innovative vulnerability patching approach.

How can enterprises modernize their vulnerability patching approach?

The cybersecurity practices that were used in the early 2000s, before virtualization, containerization, and the cloud emerged, are still being relied upon – maintenance windows are still a staple of IT activities. To improve the situation, in addition to overhauling the tools and solutions used, it is also imperative to change the processes driving those activities. Where business needs and security overlap, it is no longer necessary to rely on inefficient practices that have already run their course. Adapting to the current reality, and anticipating the faster pace of change that AI reveals, becomes the priority in order to improve the security posture of the entire organization.

In what concerns systems patching, and the clashes caused by the traditional approaches, it is necessary to look for better ways to perform an increasingly fundamental task. Even if you're working with mixed, multi-distro Linux environments or end-of-life distributions, TuxCare can help your organization deploy vulnerability patches faster, minimize downtime, and get the support you need from the experts who know enterprise Linux best.

TuxCare Linux Security Solutions

KernelCare Enterprise

TuxCare's live patching solution 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, monitor lengthy reboots, or deal with end-user disruptions.

Endless Lifecycle Support (ELS)

TuxCare's 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, and Spring – protecting their systems for as many years as they need after vendor-provided security support has ended.

Enterprise Support for AlmaLinux

For AlmaLinux users, TuxCare offers the commercial support that organizations can't get anywhere else, providing break/fix support, automated live patching, extended security updates, continuous compliance, pay-as-you-go hourly support bundles, and much more.

With Enterprise Support for AlmaLinux, organizations gain access to skilled AlmaLinux security experts whenever they need them, benefiting from enterprise-grade support for this popular community-driven and free Linux distribution.

TuxCare

About TuxCare's Research

Demographics

To generate the insights found within this report, TuxCare researchers distributed a wide-ranging survey to professionals working at organizations that use enterprise Linux, including TuxCare customers. In total, 589 individuals across various industries participated in the survey.

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

Organization Size

<100 Employees: **19.35%**
101-500 Employees: **33.79%**
501-1,000 Employees: **25.81%**
1,001-5,000 Employees: **15.45%**
5,001-10,000 Employees: **2.72%**
>10,000 Employees: **2.89%**

Organizations large and small participated in this research, but **over half of organizations surveyed have between 101 and 1,000 employees.**

Industries

IT/Technology: **30.73%**
Industrial/Manufacturing: **23.09%**
Telecom: **15.11%**
Entertainment and Media: **7.98%**
Public Sector: **6.79%**
Finance: **5.26%**
Retail: **4.92%**
Services: **2.04%**
Healthcare: **1.87%**
Transportation: **0.85%**
Education: **0.51%**
Hospitality: **0.17%**

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

Job titles of Survey Participants

Software Engineer: **24.62%**
IT Security Analyst: **19.35%**
DevOps: **15.45%**
Tech Lead: **13.92%**
Sysadmin: **11.88%**
Product Manager: **7.64%**
CEO: **2.21%**
CIO/CTO: **1.53%**
Vulnerability Management Specialist: **1.36%**
Compliance/Risk Specialist: **1.02%**
CISO: **0.34%**
Head of Tech Operations: **0.17%**
Project Manager: **0.17%**
Solutions Architect: **0.17%**
Network Administrator: **0.17%**

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.

Open-Source vs. Proprietary Usage

Open source (e.g., Linux): **45.0%**
Proprietary software only: **1.5%**
Both open-source and proprietary: **53.5%**

Most organizations surveyed use a combination of open-source and proprietary software in their infrastructure stack, but 98.5% rely on open-source software in some way.

Number of Linux Servers Used

<10 Servers: **11.54%**
10-20 Servers: **29.20%**
20-100 Servers: **26.83%**
100-500 Servers: **24.45%**
500-1000 Servers: **3.90%**
>1000 Servers: **3.57%**
Unsure: **0.51%**

Most organizations surveyed operate between 10 and 500 Linux servers

Why TuxCare?

TuxCare is a global leader in open-source security, providing unmatched expertise in patching for your entire Linux estate. We deliver security patches to popular Linux distributions, end-of-life systems, programming languages, and more – offering a comprehensive security solution for all your infrastructure needs.

With over 100,000 patches – and counting – delivered to our users without reboots, 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 a million work-loads (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.

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