State of device management

Insights, challenges, frustrations, and desires from 200+ security practitioners.

Read online:

fleetdm.com/reports/state-of-device-management

Insights from Mike McNeil

CEO & co-founder, Fleet

Businesses are taking device security more seriously than ever. Modern work environments pose many challenges for security teams, and it's becoming much more difficult for organizations to secure their devices: laptops, tablets, smartphones, and other mobile technology. Some of these devices are company-issued, but many are personal devices on which employees conduct their work — and in today's remote environment, that work could happen anywhere. So how does an organization manage its devices? Do they know if their devices are compliant and secure? Do they have ways to query them to learn more about their status in real time? Or are organizations unprepared and overwhelmed with managing thousands or hundreds of thousands of endpoints?

At Fleet, we help security teams, IT professionals, and DevOps engineers track and secure their organization's laptops and servers. But outside of our users and customers, we wanted to know more about the current state of device management, in general, to understand how security teams manage their endpoints better. We found that organizations may not be managing devices as successfully and thoroughly as they should to keep themselves safe.

We hope you consider these insights and findings as you build your device management strategy in 2022.

Key findings

- **Only a quarter say their devices are fully enrolled and upgraded**

  Only 23% of the people we asked said they have successfully enrolled all, or nearly all, of their devices in their MDM. 25% are running the latest OS version, while the remainder only have a fraction of their devices enrolled or upgraded.

- **Miscellaneous and mobile operating systems are a problem**

  When it comes to managing operating systems, 36% struggle with miscellaneous operating systems, 29% with iOS, and 26% with Android. Additionally, Windows (40%) and Linux (27%) are the platforms they use the most but don't currently manage.

- **The best practice is to have a good bring-your-own-device (BYOD) policy**

  32% say having a documented BYOD policy is a crucial best practice for their MDM strategy. They also find success measuring point-in-time compliance across all devices (31%) and tracking how quickly vulnerable software is patched (30%).

- **Compliance verification is the biggest day-to-day challenge**

  23% of our respondents say their biggest daily challenge with their MDM is being able to verify compliance across devices. 21% say getting all their devices enrolled is their top challenge, while 20.5% say maintaining accurate visibility across devices is theirs.

- **Complicated MDMs are the top deployment challenge**

  36% found it too difficult to configure and understand their MDM, while 34% also encountered confusing or limited documentation. 33% were frustrated with SSO integration, and a further 33% faced difficulty getting support.

- **Only half think their MDM is effective**

  47% find visibility into enrolled devices sufficient, 49% effectively maintain secure laptops and servers, 52% respond to incidents promptly, 55% have the visibility to investigate in real time, and 49% effectively enforce compliance and security posture — but the remainder are not finding these in their MDM.

- **Multi-factor authentication is a top priority for 2022**

  Over the next year, respondents want to focus on device security. 18% say multi-factor authentication (MFA) at login is a priority. 14% are focused on implementing zero-touch enrollment, and 13% say patching third-party applications and packages is their top priority for 2022.

Who we surveyed

Starting on February 25, 2022, we sampled 205 members of professional security teams who are directly responsible for device management. The survey was conducted online via Pollfish using organic sampling. Learn more about the Pollfish methodology.

Demographics

Gender

52% Male

48% Female

Age

26.83% 18-24

28.78% 25-34

14.15% 35-44

13.17% 45-54

17.07% 54+

Country

100% United States

Number of employees

65% 1001 - 5000

35% 5000+

Role

21.46% Other

20% Security Engineering (EngSec)

17.56% Cloud Security

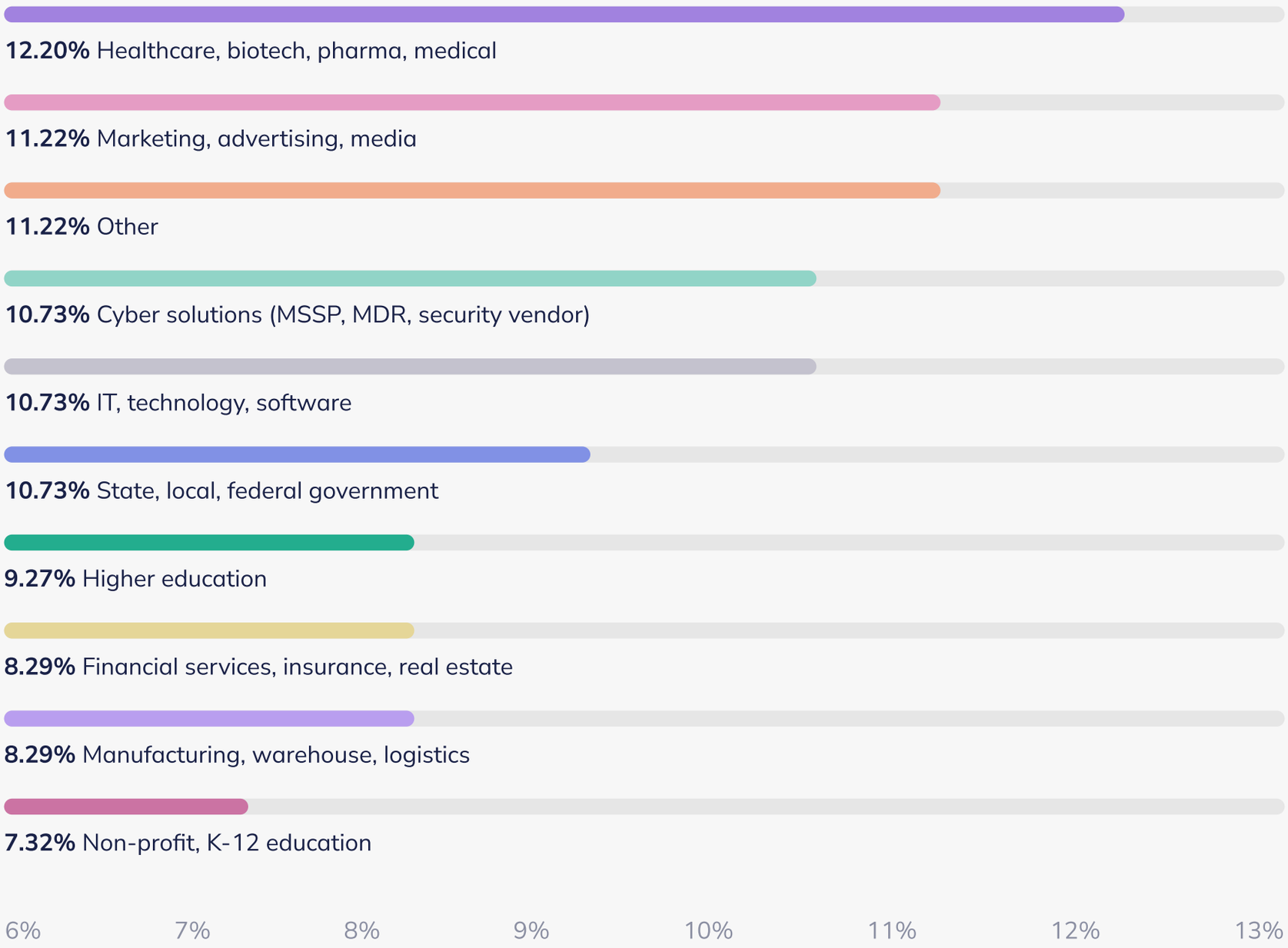
16.59% Security Operations

13.17% Vulnerability Management

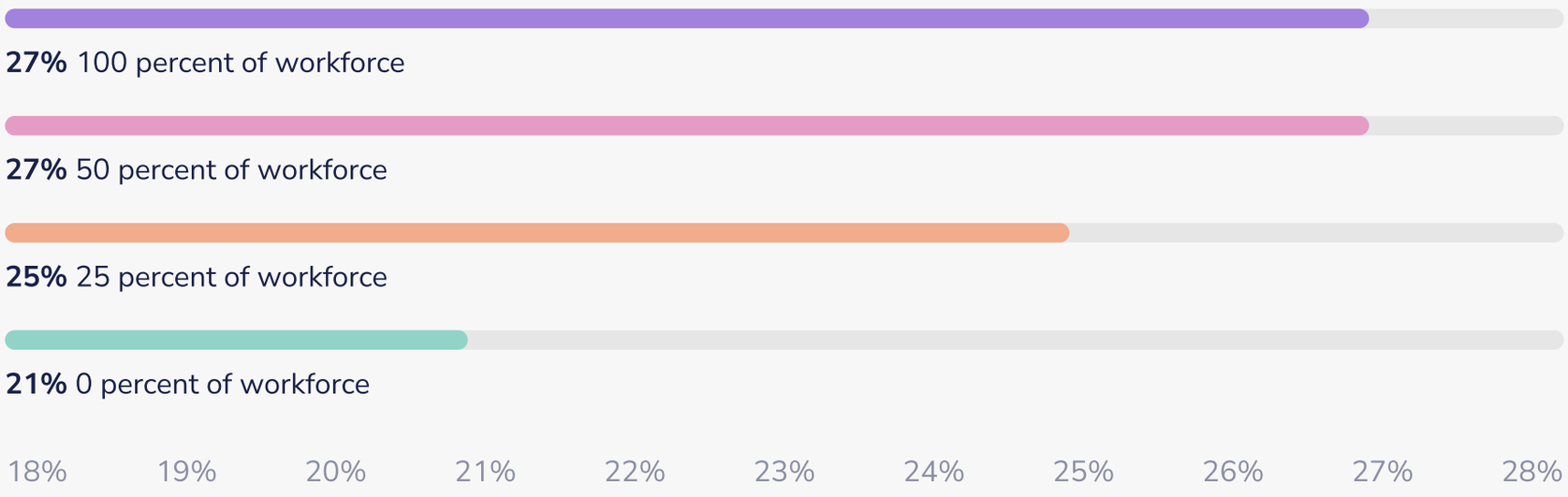
11.22% Incident Response (CSIRT, DFIR)

10% 11% 12% 13% 14% 15% 16% 17% 18% 19% 20% 21% 22%

Industry



Percentage of workforce working remotely (fully or partially)



Now, with context around our respondents — security team members responsible for device management, across a variety of industries, at various levels of remote work — let's take a closer look at what we uncovered.

PART 1

State of device management

Not only has technology enabled employees to work through laptops, smartphones, tablets, and other mobile devices, the shift to remote work has increased the need for it. More devices means a greater risk of compromise and organizational security threats, which results in an increased demand for endpoint visibility and monitoring.

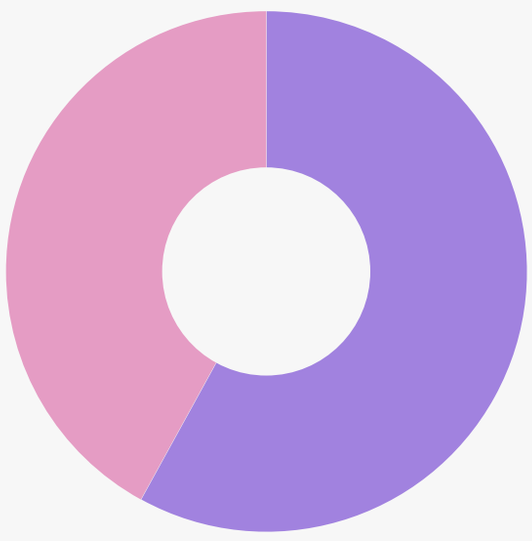
Our respondents told us about their current state of device management: what MDM they use, what devices they're managing, and what they're struggling to cover.

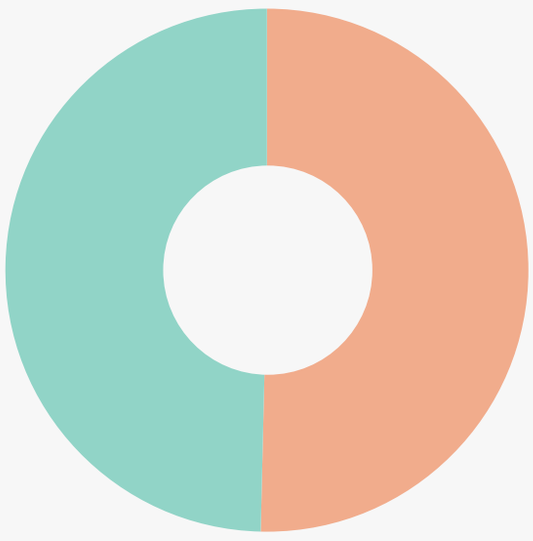
58% use a cloud MDM

Most of our respondents (57.6%) use a cloud solution hosted by a vendor for their MDM. The rest are self-managed and hosted by their organization.

Half pay per user and half pay per device

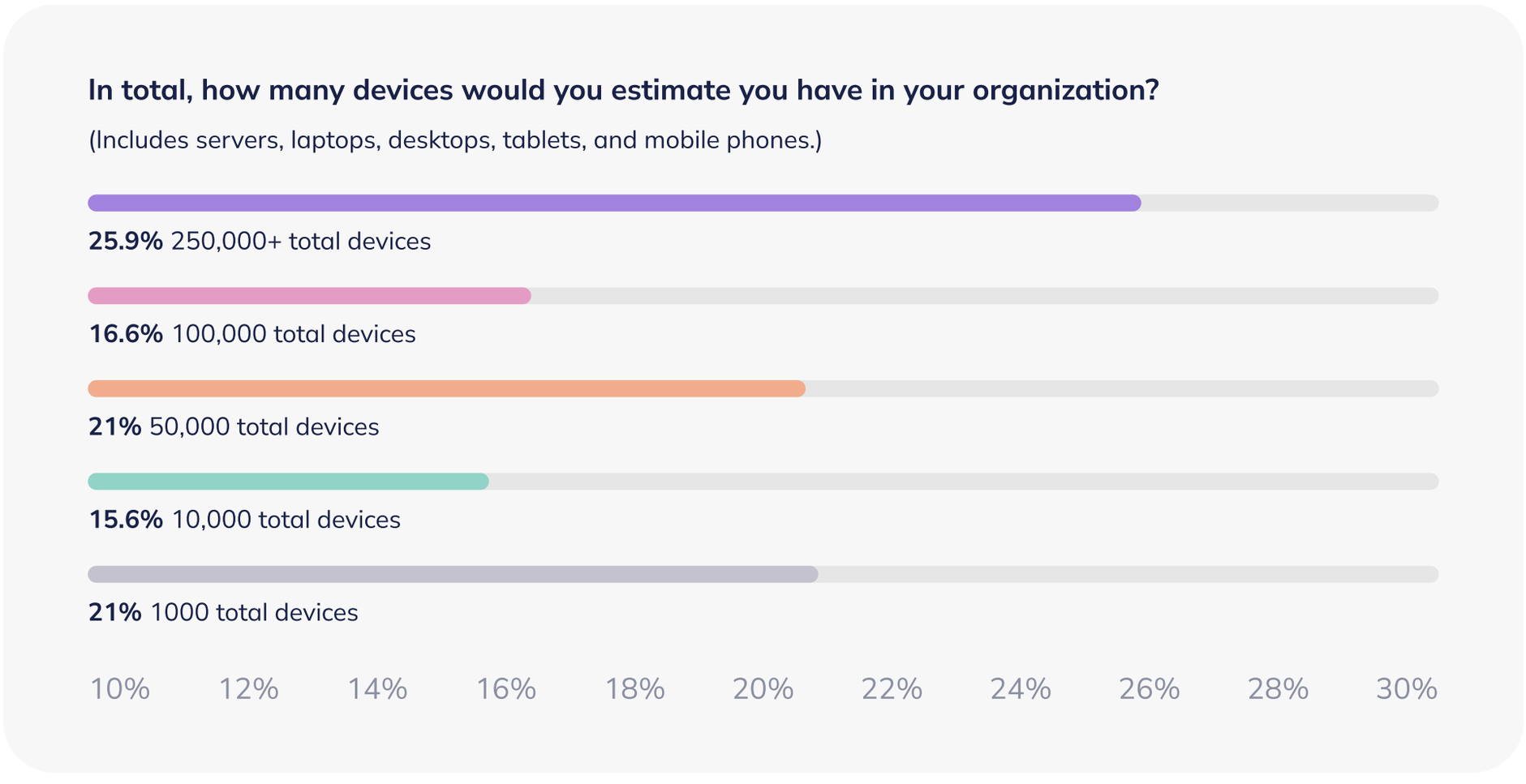
50.4% of our respondents pay per device, while the remainder pays per user.





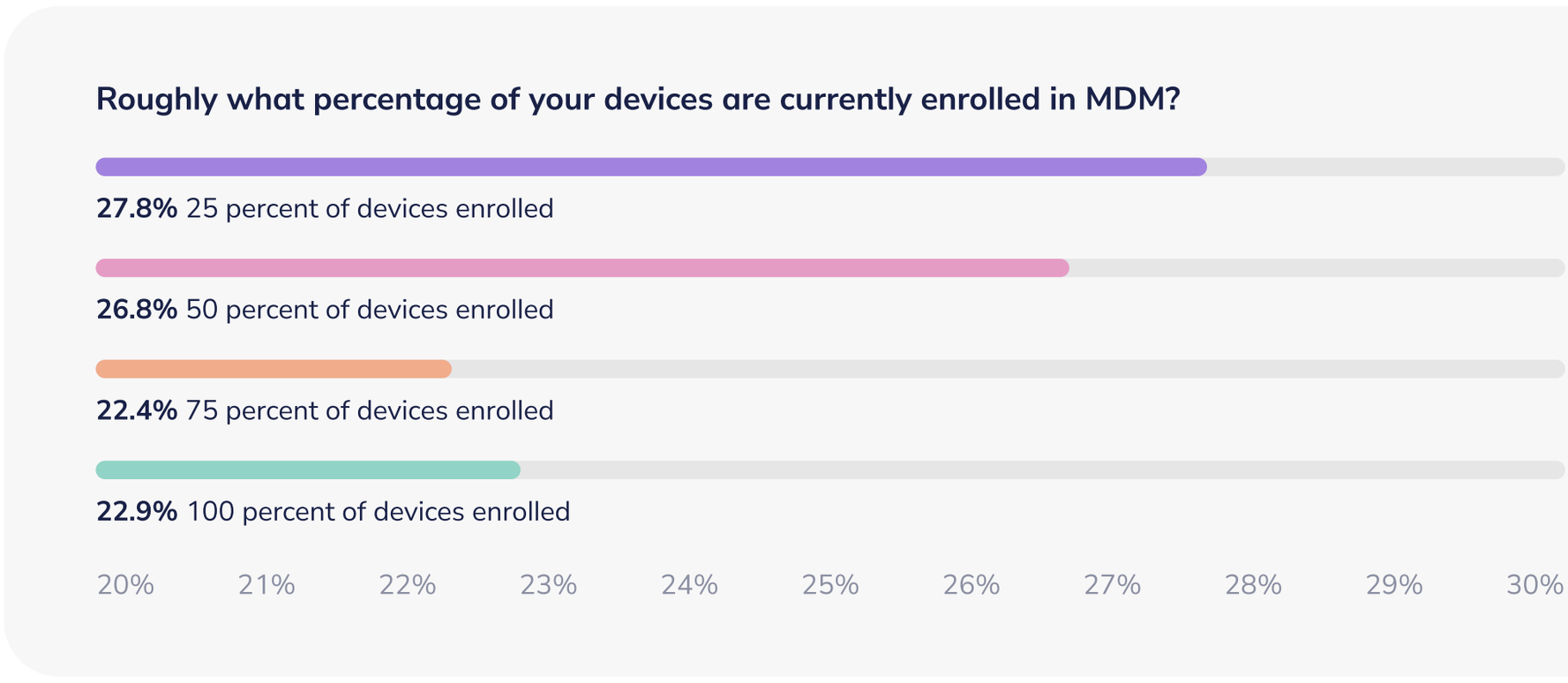
26% report their organization manages over 250,000 devices

With devices including servers, laptops, desktops, tablets, and mobile phones, the largest segment of respondents (25.9%) estimate having over 250,000 total devices in their organization's fleet.



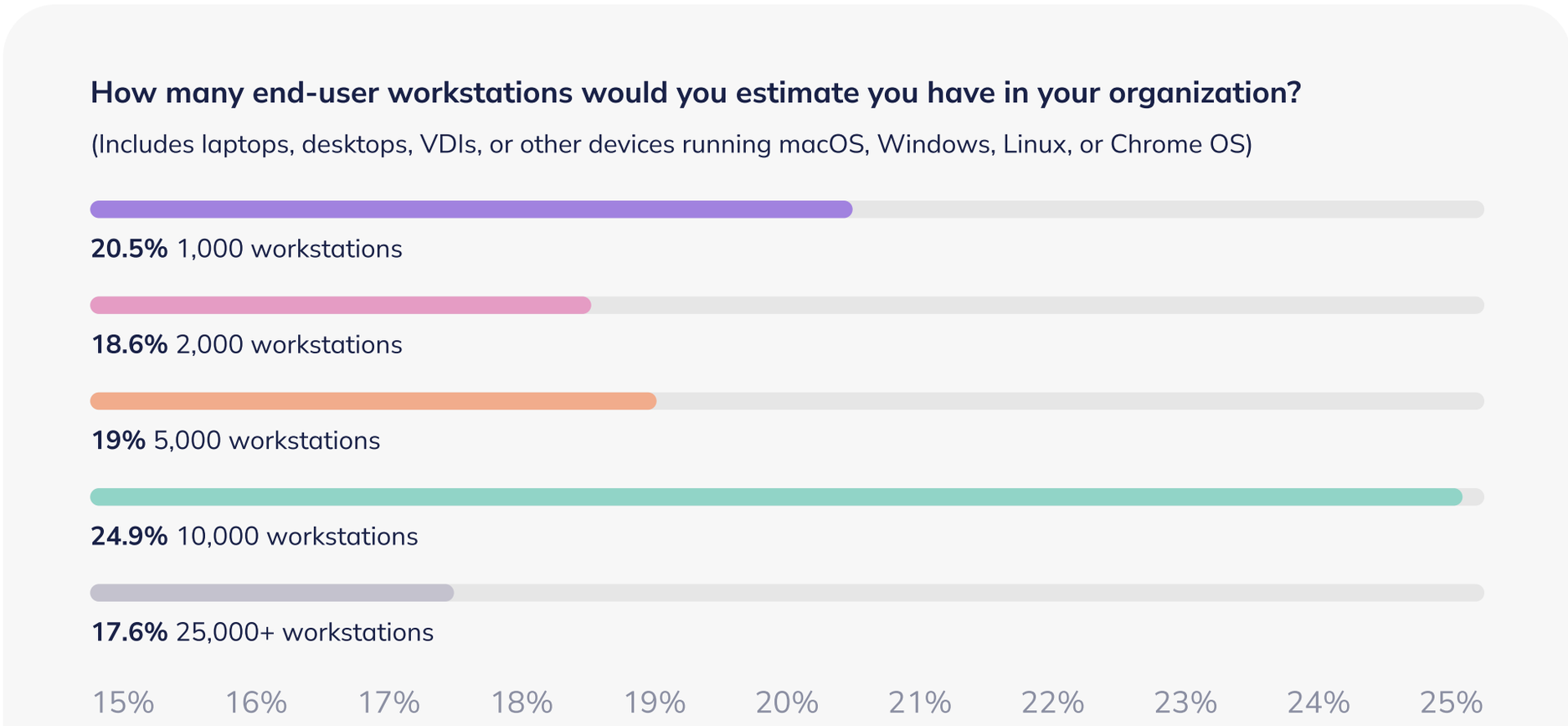
Rates of MDM enrollment vary across organizations

Respondents report varying degrees of enrollment across their organization's MDM. The majority (27.8%) have only enrolled about a quarter of their devices. 26.8% say that about half of their devices are enrolled. For 22.4%, about three-quarters of their devices are enrolled. Finally, 22.9% say they have enrolled all, or nearly all, of their devices.



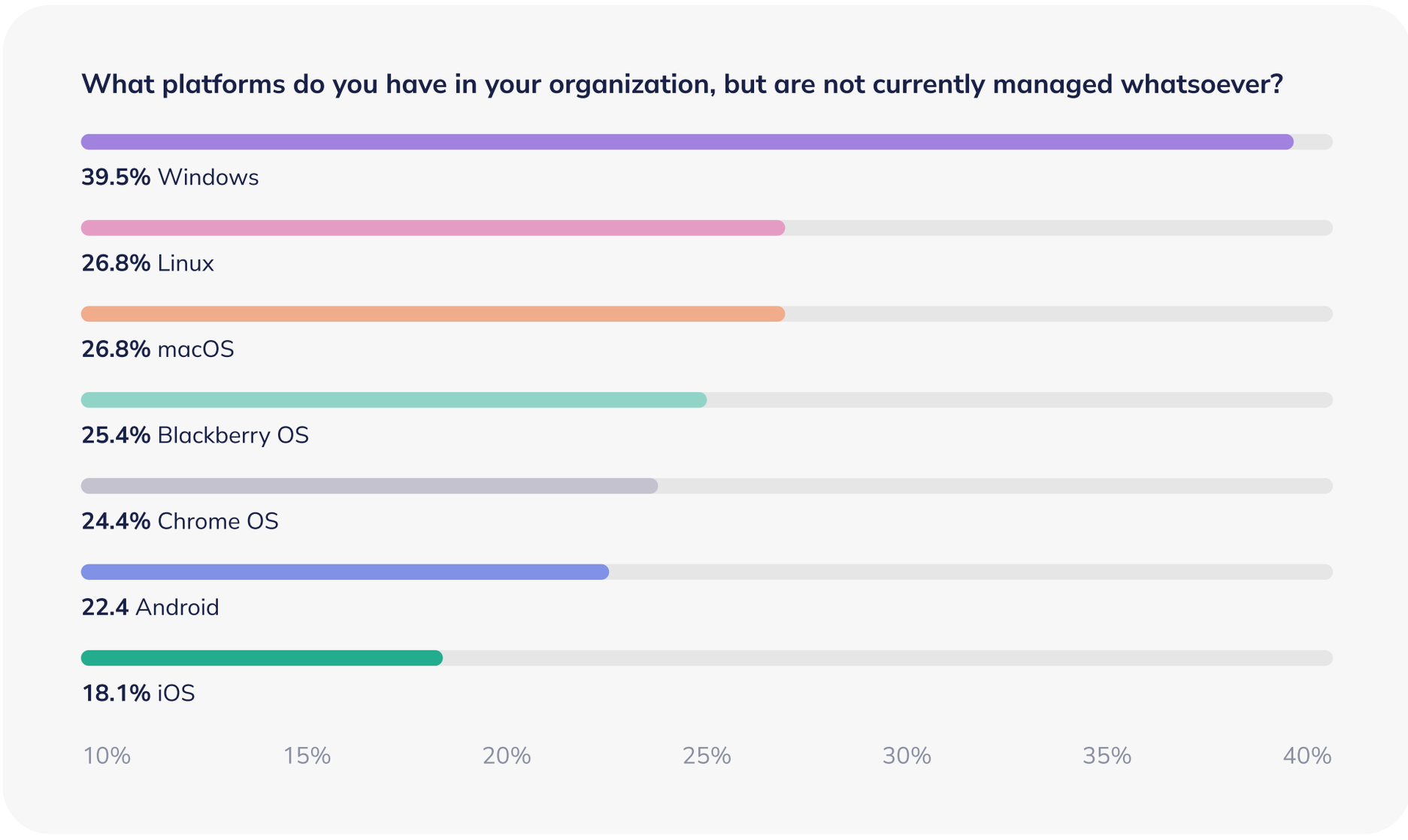
25% have 10,000 workstations in their organization

The largest segment of respondents (24.9%) report having about 10,000 workstations in their organization, including laptops, desktops, or other devices. Other respondents report having 1,000 workstations (20.5%), 2,000 workstations (18.6%), 5,000 workstations (19%), and 25,000 or more workstations (17.6%).



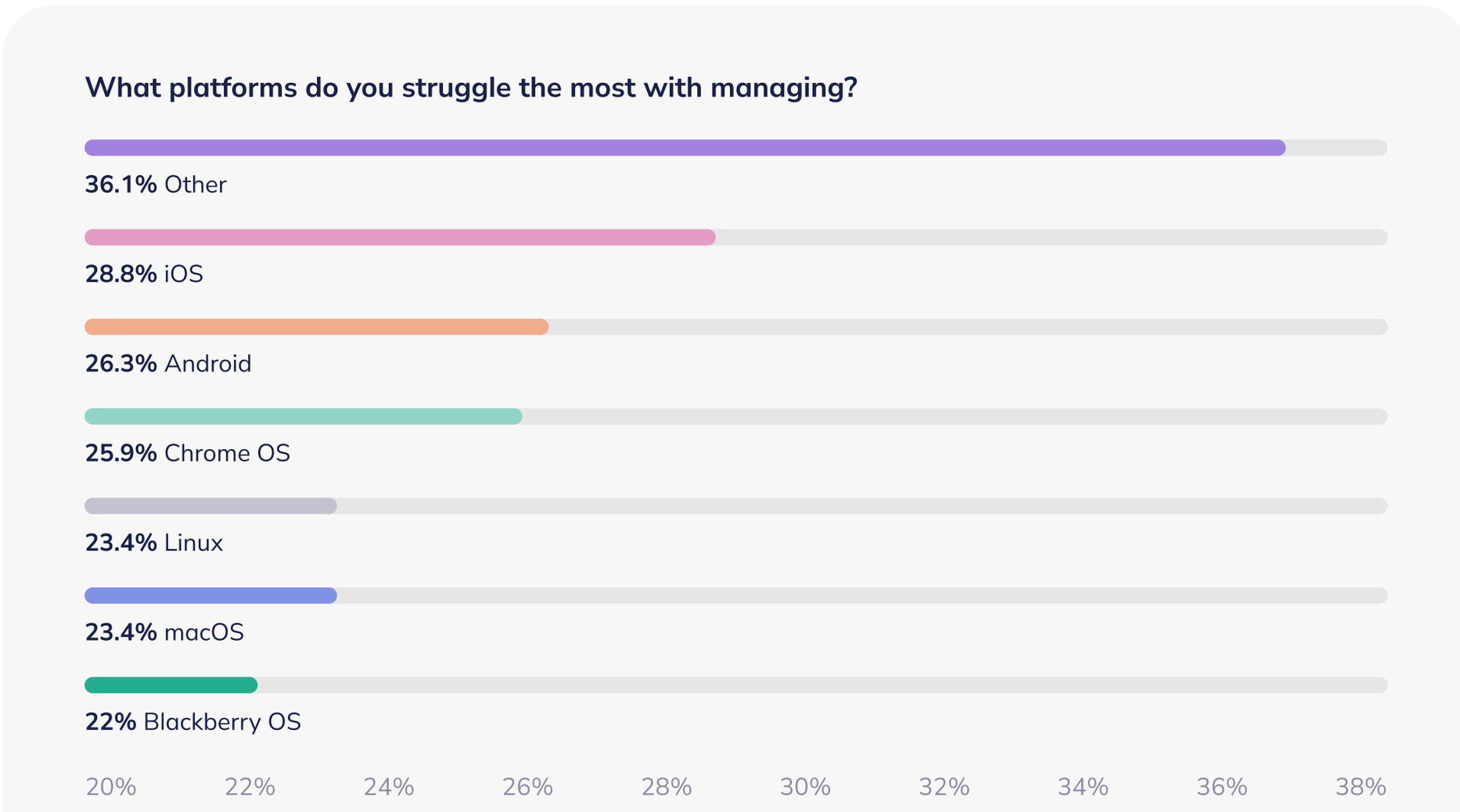
Organizations inadequately manage Windows and Linux

In a "choose all that apply" question, we asked respondents which platforms their organizations use but don't currently manage with an MDM. They replied:



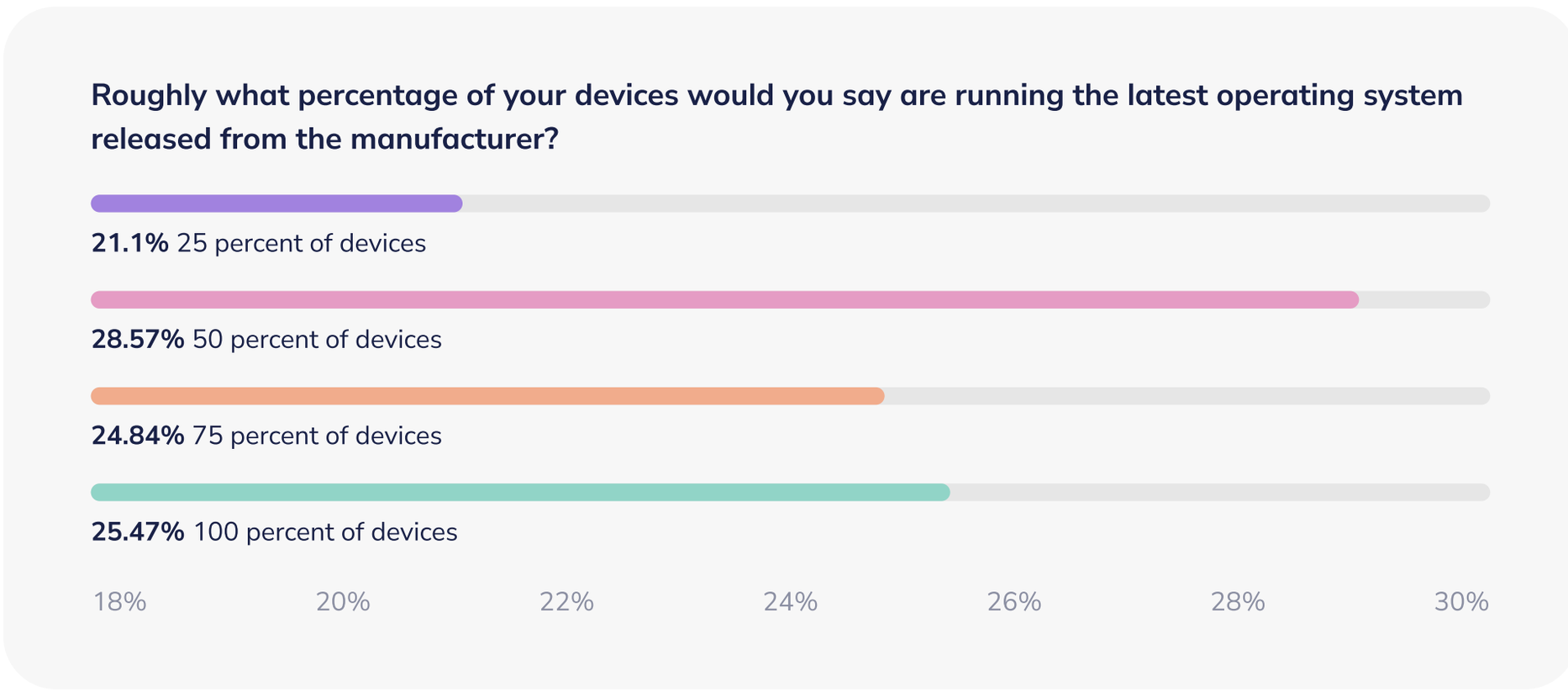
iOS and other disparate platforms are a challenge to manage

When it comes to managing various platforms, they struggle the most with managing the following (and chose all that applied):



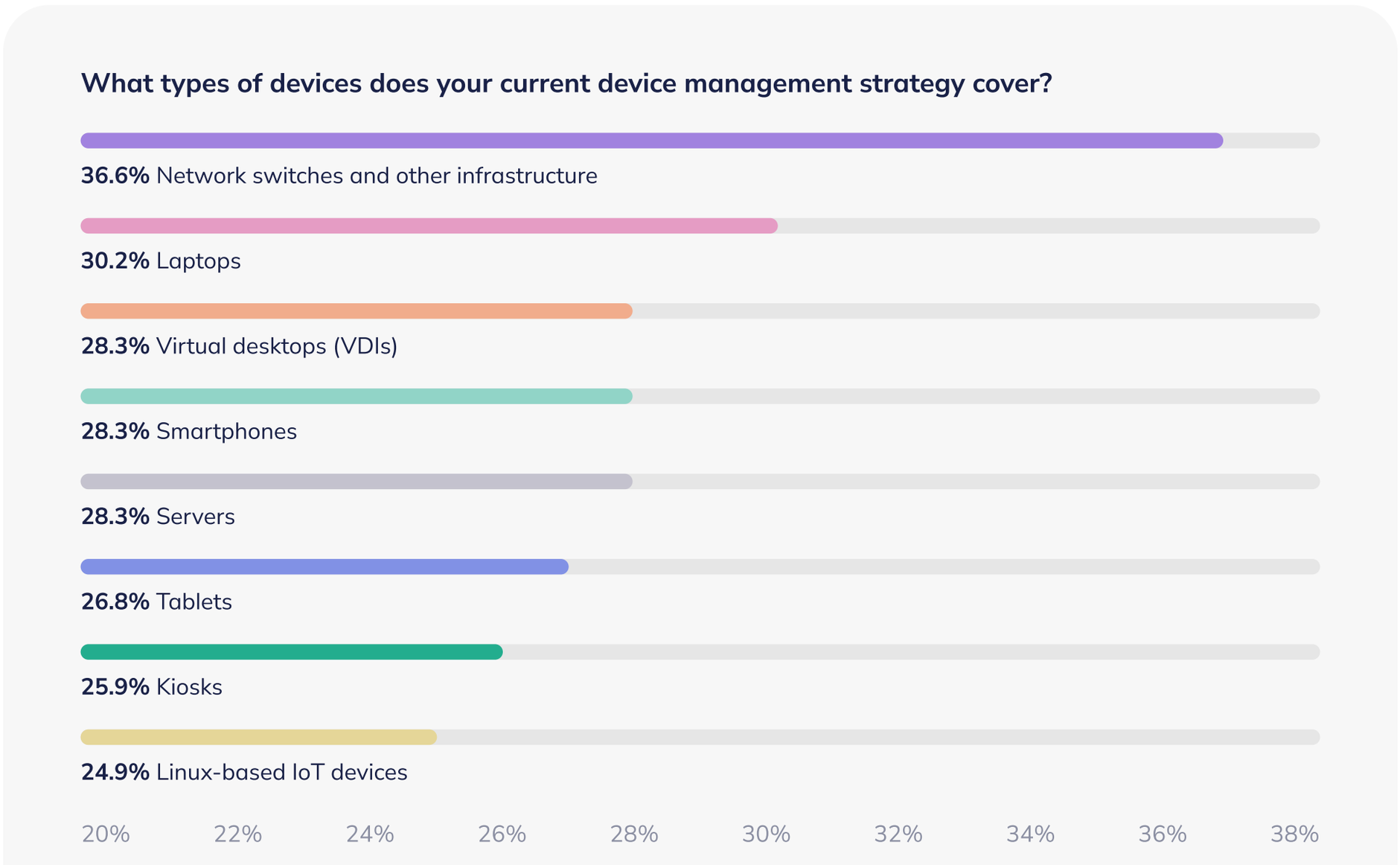
Devices are also in various states of upgrade

The majority (28.57%) reported that roughly half of their devices are running the latest operating system released by the manufacturer. 21% say about a quarter of their organization's devices are running the latest OS, while 24.84% say three-quarters have the latest OS installed. Finally, 25.47% of the surveyed people say all, or nearly all, of their devices have up-to-date operating systems installed.



Network switches and other infrastructure, laptops, and virtual desktops are a priority for device management strategies

Our respondents reported that their current device management strategy includes the following devices (we asked respondents to choose all that apply):



Summary

Our survey found that the organizations behind our respondents need ways to manage a large number of endpoints. A quarter of respondents report managing 250,000 devices or more, and a quarter are in organizations with over 10,000 workstations.

However, our respondents said that devices in their organization are at various stages of enrollment and upgrade. Some organizations report having enrolled nearly all devices in their MDM with the latest operating system. Yet, not even a quarter of devices are enrolled and upgraded for many others. This means organizations don't know which devices are at risk.

As for their MDMs, most (58%) use a vendor-issued, cloud-based solution, while the rest use a self-managed solution hosted by their organization. Devices commonly covered by their MDMs include their network switches and other infrastructure, followed by laptops, virtual desktops, smartphones, and servers. Respondents use Windows the most in their office, yet their MDM doesn't cover it, and they struggle the most to manage disparate platforms, iOS, and Android.

In our next section, we'll look deeper at what makes our respondent's MDM approach successful and what daily challenges they face.

PART 2

Best practices and challenges

Our respondents directly manage devices for their organization, as many as 250,000 or more. Are they finding success in their efforts, or are they being derailed by daily inconveniences?

Here are some of the best practices our respondents suggest for device management and some of the challenges they face each day.

Having a documented BYOD policy in place

With the rise in employees using their own devices for work, 31.7% say it's imperative to have a documented policy over usage and access.

Providing a self-service experience

Respondents also see value in letting end users troubleshoot issues themselves instead of getting IT involved.

Focusing on a seamless end-user experience

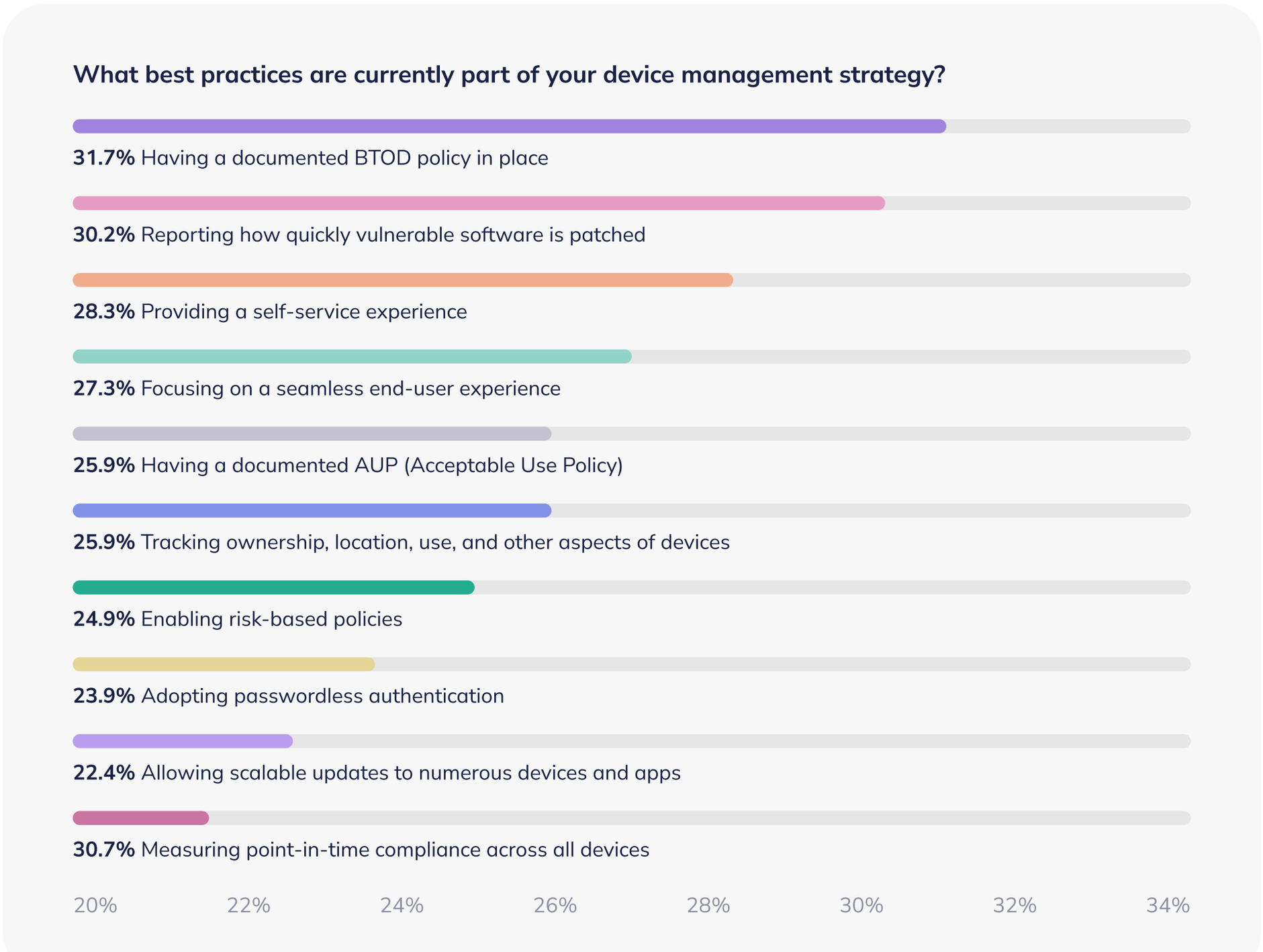
Finally, respondents stress that having a seamless solution for end-users allows easy access and continued productivity.

Measuring point-in-time compliance across all devices

Accurately monitoring devices is a struggle if you're getting stale data. Another best practice is to ensure that you're measuring real-time compliance across your devices.

Reporting time to patch vulnerable software

Another best practice is reporting — especially on time taken to patch vulnerable software — so you can gauge response time and optimize for performance.



Top challenges for MDM

The biggest challenges respondents face each day when it comes to device management are:

Verifying compliance across devices

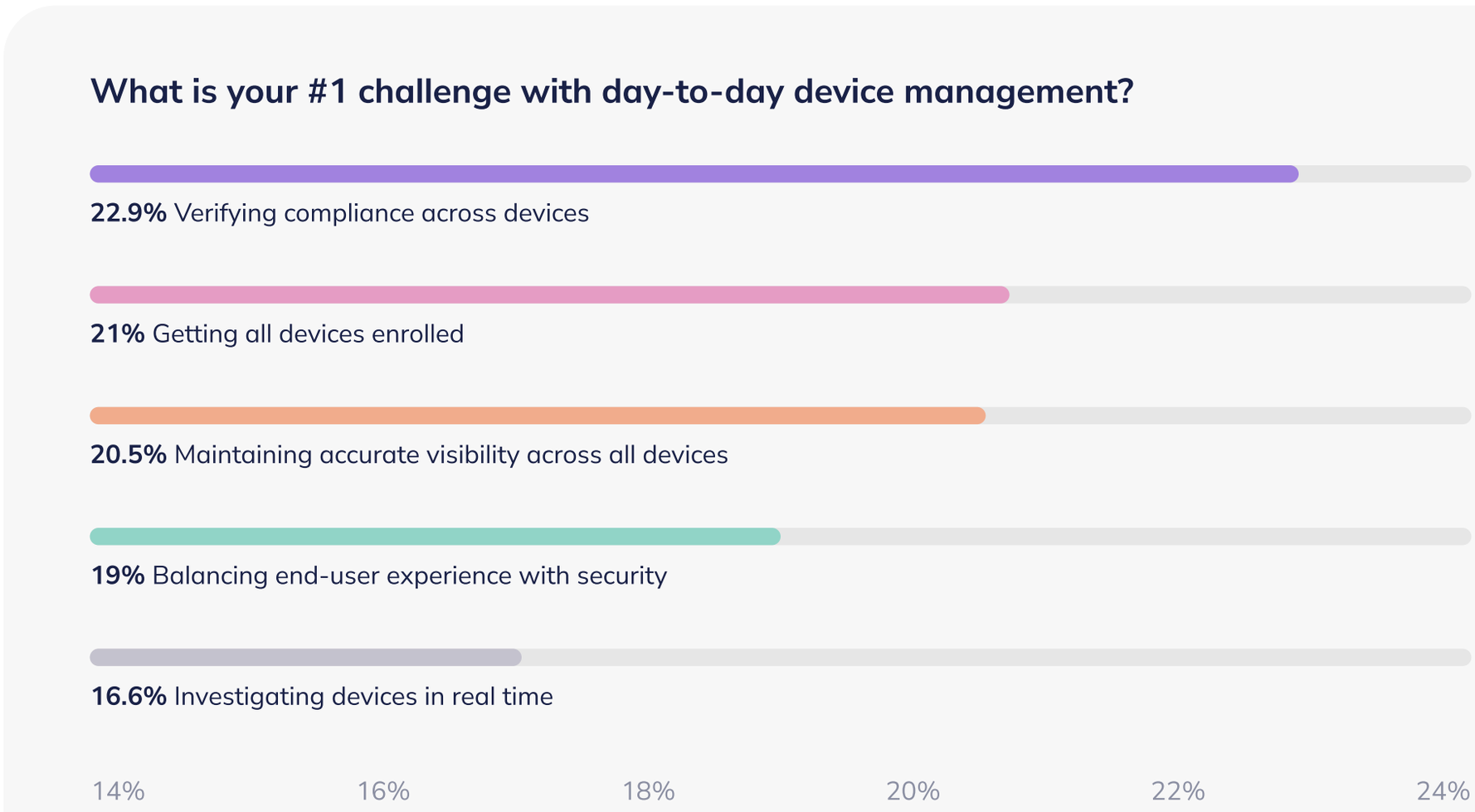
Our respondents reported that verifying compliance in real time across their devices is a successful best practice, yet 22.9% say doing so is proving difficult. Device enrollment also adds to that complexity, and where it's lacking, full compliance monitoring is impossible.

Getting all our devices enrolled

Less than a quarter said that all of their devices are enrolled — meaning enrollment has become a challenge. A further 21% report device enrollment as a daily challenge. A reason for lack of compliance could be simply getting employees to enroll their devices.

Maintaining accurate visibility across all our devices

Accurate visibility across all devices requires the right MDM solution and having all devices enrolled and monitored. 20.5% say maintaining accurate visibility across devices is their top daily challenge.



Summary

There are two key takeaways here. First, a working MDM strategy will monitor devices, verify compliance, and provide endpoint visibility in real time. Second, organizations must have devices enrolled in the first place to achieve those goals. That's why it's imperative to have a documented policy for personal device usage and why that’s at the top of the best practices list for most of our respondents. It's also why getting every device across an organization enrolled in MDM is such a challenge.

In the next section, we'll take a step back and look at why organizations choose an MDM in the first place.

PART 3

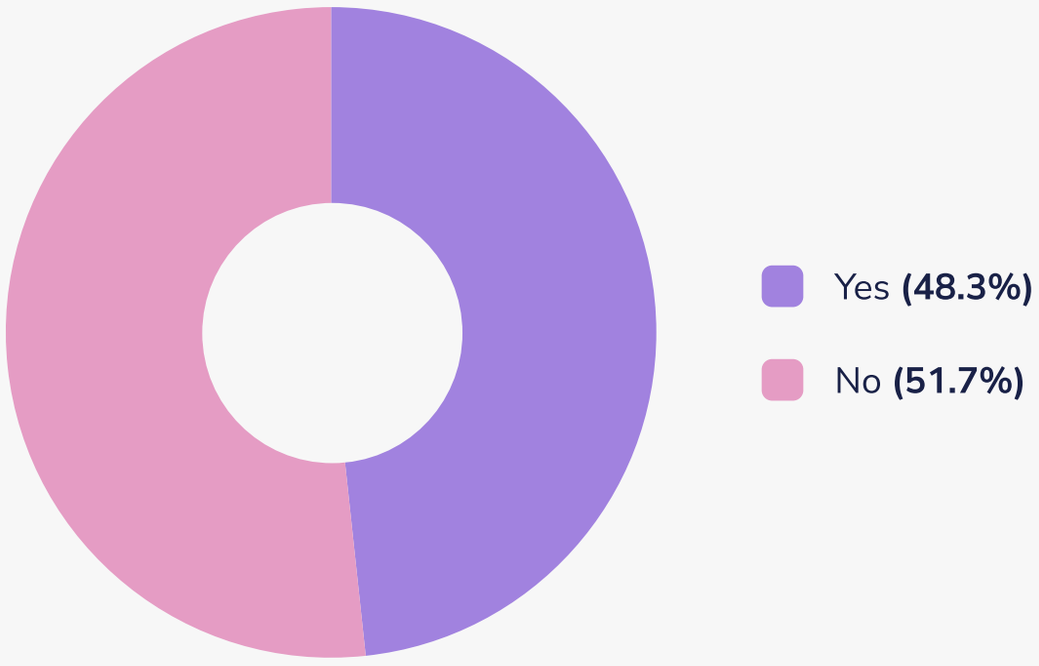
MDM deployment and implementation

Since our respondents manage devices, they can give us insight into why organizations implement an MDM, time to implementation, and implementation challenges.

48% deployed their organization's MDM

Just under half of our respondents were involved in the initial deployment of their organization's MDM.

Were you involved in the deployment of your organization’s current MDM solution?



Top reasons for MDM investment

Here are the top reasons why our respondent's organization invested in MDM:

The shift to remote work

Remote work increases endpoints outside the office, and security teams have less control over these devices' networks. In 2020 MDMs became an overnight priority for protecting organizations.

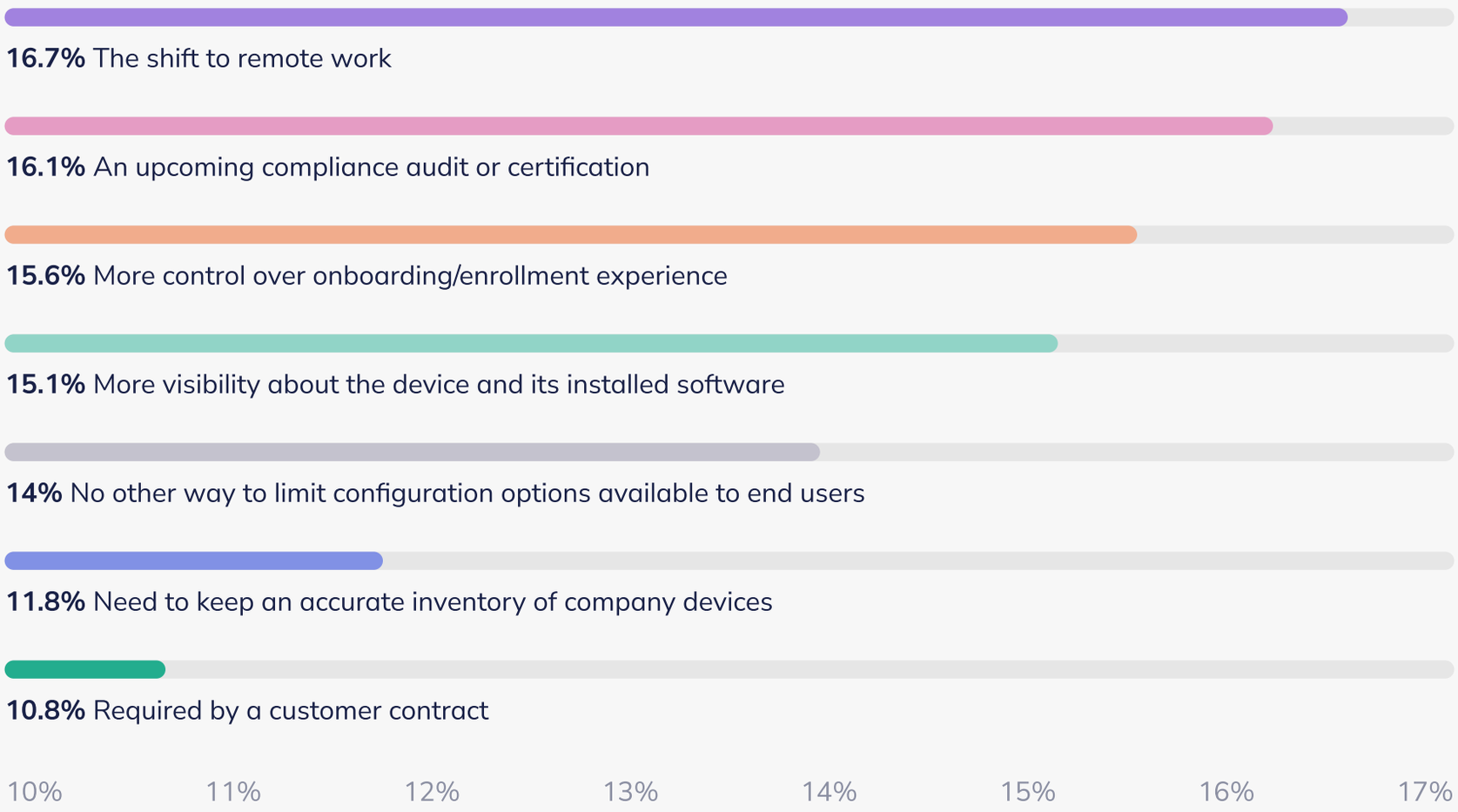
A future compliance audit or certification

16.1% say MDMs were implemented ahead of a compliance audit or certification, as teams needed better monitoring and visibility to pass them.

More control over onboarding or enrollment

15.6% say they invested in MDM to manage devices proactively.

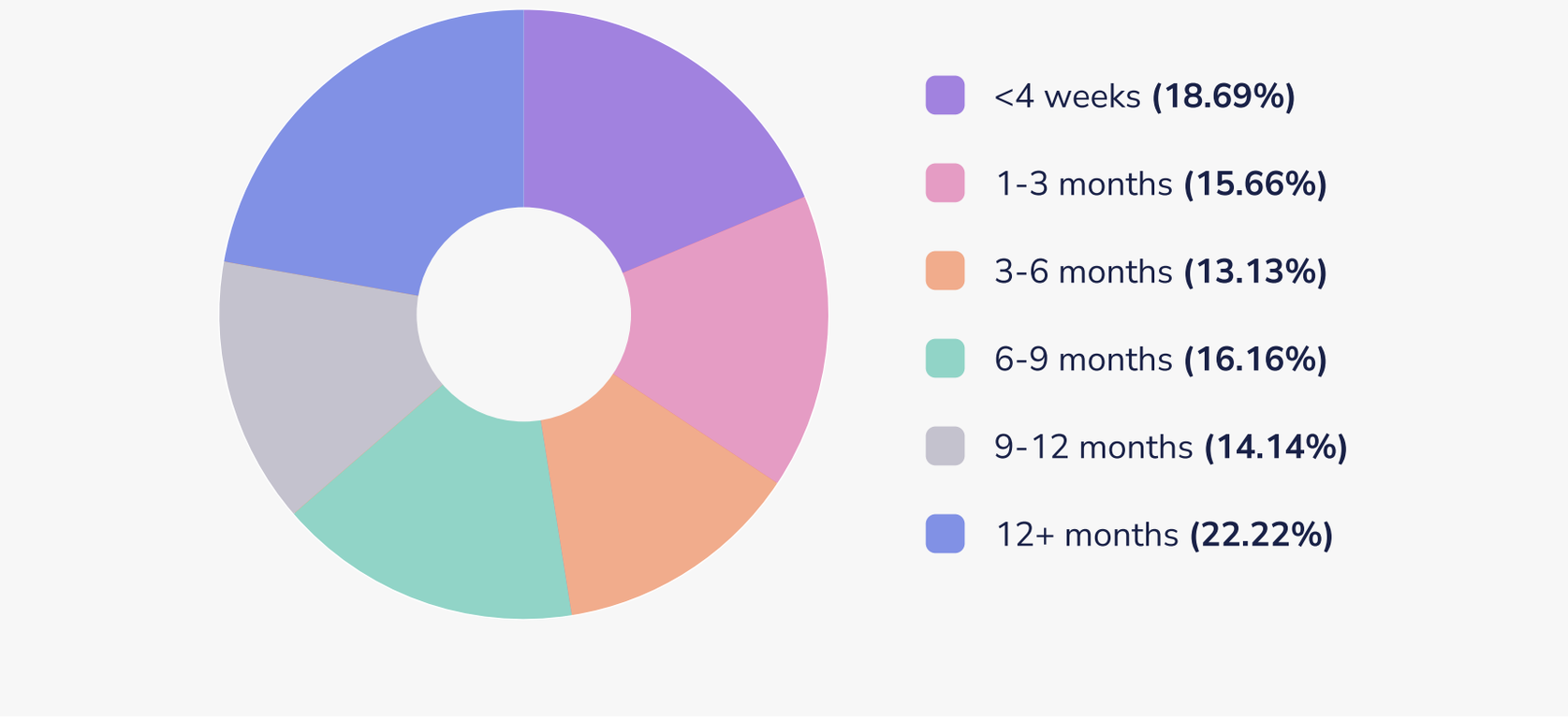
What triggered your organization to invest in an MDM solution?



22% say their MDM took over a year to implement

The largest segment (22.2%) reported that deploying and implementing their MDM took over a year. However, for 18.7%, it took four weeks or less. For 15.7%, it took one to three months, and for 13.1%, it took three to six months. For 16.2%, it took six to nine months, and for 14.1%, it took nine to twelve months.

How long do you estimate it took to completely deploy and implement your MDM?



Top deployment challenges

Respondents encountered these challenges while implementing their new MDM solution:

Comprehension and configuration difficulties

36.1% say the biggest challenge was understanding and configuring MDM features — a failure from the start.

Confusing or limited documentation

34.2% also discovered a lack of documentation to help them deploy their MDM, or found the documentation confusing.

Integrating with single sign-on

32.7% ran into problems integrating their MDM solution with SSO services like Okta and SAML.

Hard to get support

Another 32.7% said it was hard to get support from their vendor during the deployment phase.

What challenges did your team encounter while deploying your MDM solution?

Summary

Organizations with thousands of devices need a way to manage and maintain them efficiently. Our survey showed that the primary motivation to invest in an MDM came from moving to remote work during the pandemic. Other reasons for adopting MDM include ensuring compliance for an audit and wanting to manage devices more closely.

But in addition to these enrollment, real-time monitoring, and visibility challenges, our respondents also struggled to deploy their MDM. While 18.7% said that their MDM took a month or less to deploy and implement, 22.2% said it took a year or longer to roll out — which is a long time to leave devices unmonitored.

They also encountered difficulty understanding their MDM. Many found documentation insufficient, configuring MDM to their needs a challenge, and ran into problems integrating with SSO. Some found it difficult to get vendor support for these issues.

Once implemented, did our respondents find their solution effective? Many didn't, as we'll find out in the next section.

PART 4

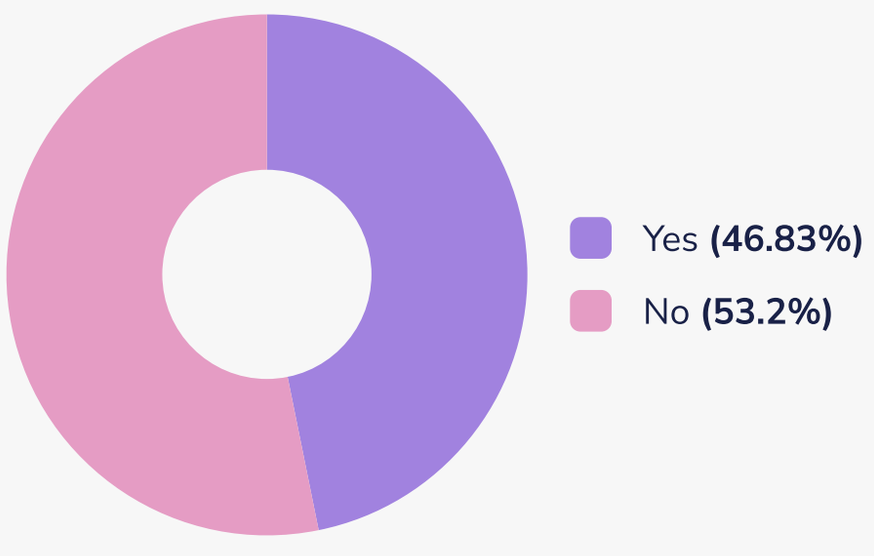
Device management effectiveness

Organizations may have a way to manage devices, but are they finding it successful? In this section, our respondents told us how effective their MDM strategy is for visibility, keeping an inventory, incident response, and other key features.

47% have sufficient visibility into enrolled devices from their MDM

Less than half say their current MDM provides sufficient visibility into enrolled devices and collects adequate security data.

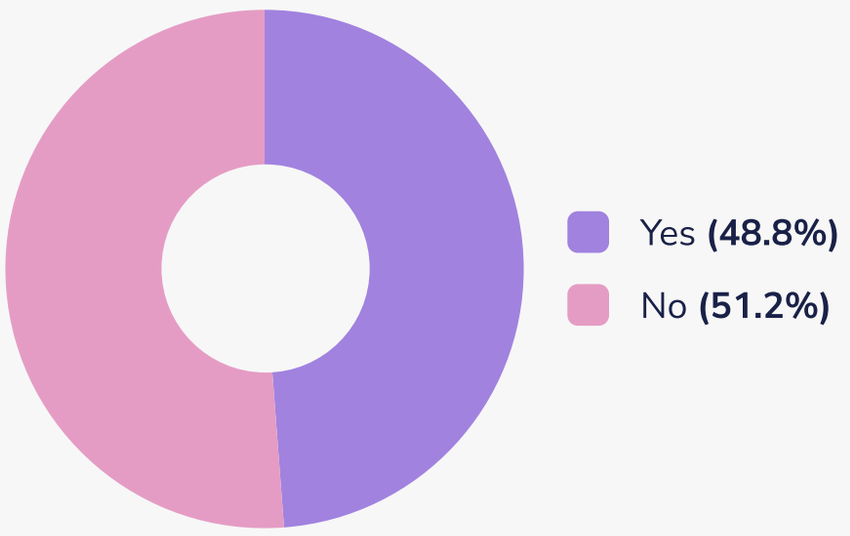
Does your current management strategy provide sufficient visibility / collect sufficient security data about enrolled devices?



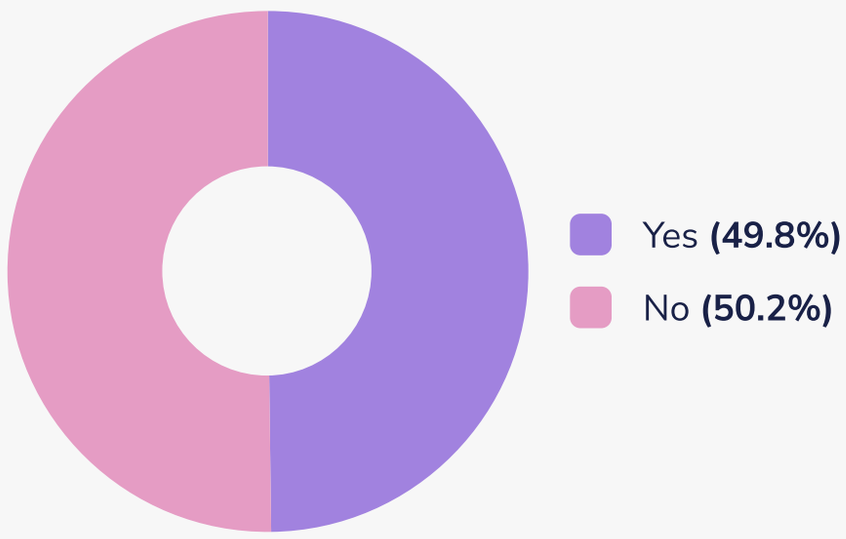
49% say their MDM effectively maintains secure laptops and servers

48.8% say their current MDM maintains secure laptops and servers, while 51.2% say it does not.

Does your current device management strategy effectively maintain secure laptops and servers?



Does your current device management strategy effectively keep an accurate inventory of all devices across all platforms?



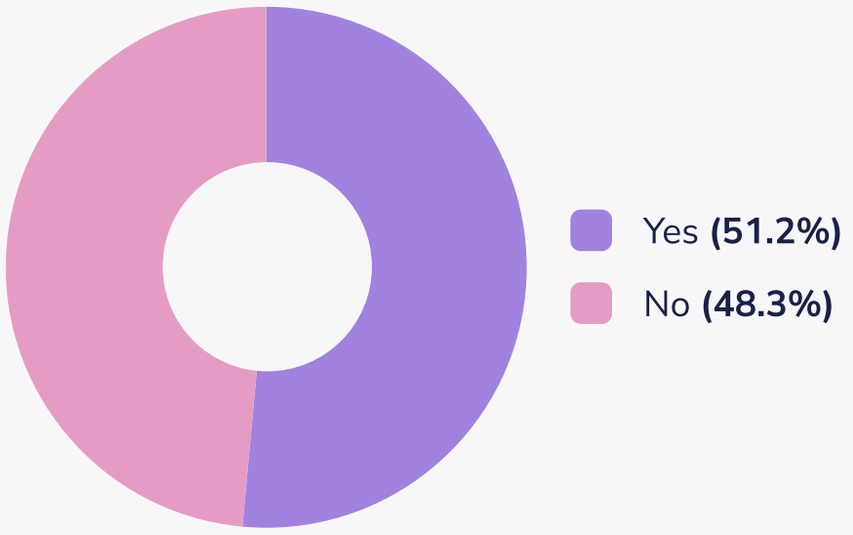
50% report their MDM keeps an accurate inventory of all devices

Our respondent's opinion on whether their MDM maintains an accurate inventory of devices across platforms was split.

52% say their MDM allows timely incident response

Just over half surveyed say their MDM allows for timely incident response. The remaining 48.3% say it does not.

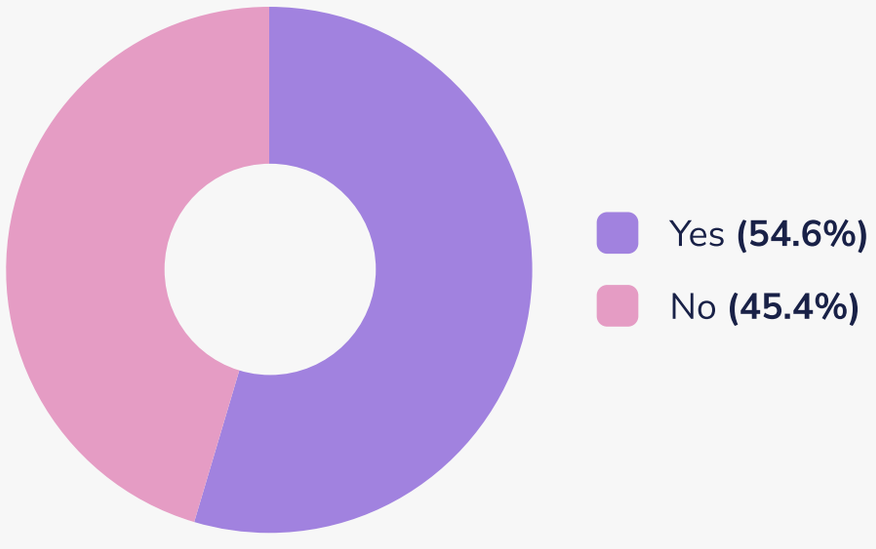
Does your current management strategy allow you to respond to incidents in a timely manner, with enough context?



55% have an MDM with the visibility to investigate in real time

54.6% say their MDM strategy offers enough visibility to investigate devices in real time.

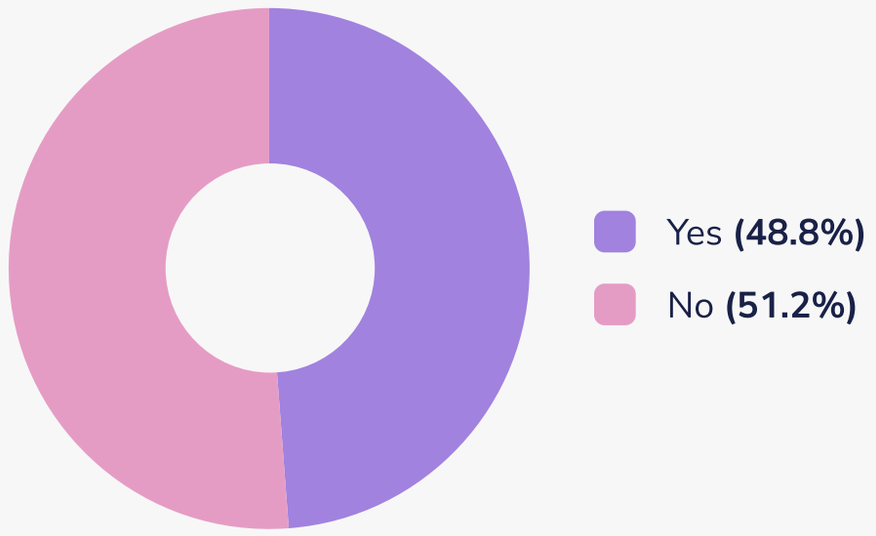
Does your current management strategy give you enough visibility to investigate what's happening on the device "right now"?



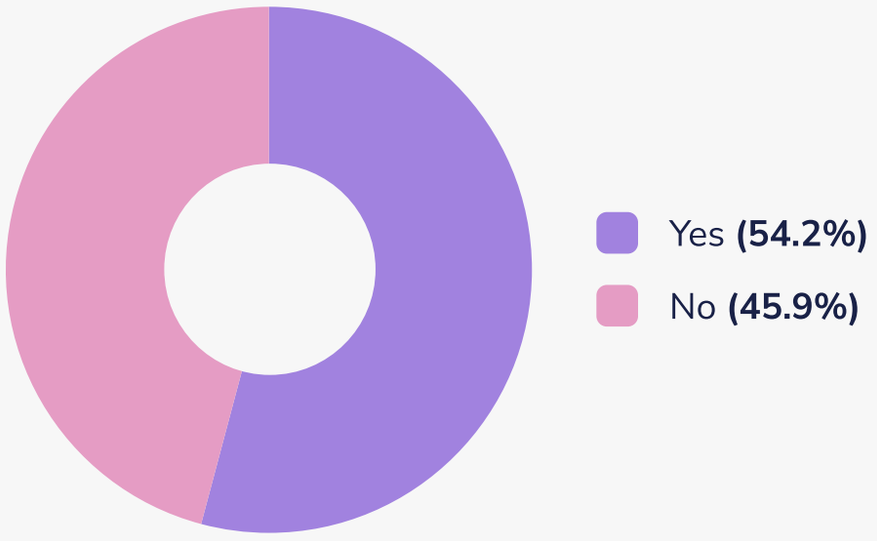
49% can effectively enforce compliance and security posture with their MDM

48.8% say their MDM effectively enforces compliance and security posture for all devices.

Does your current management strategy enforce compliance and security posture across all devices?



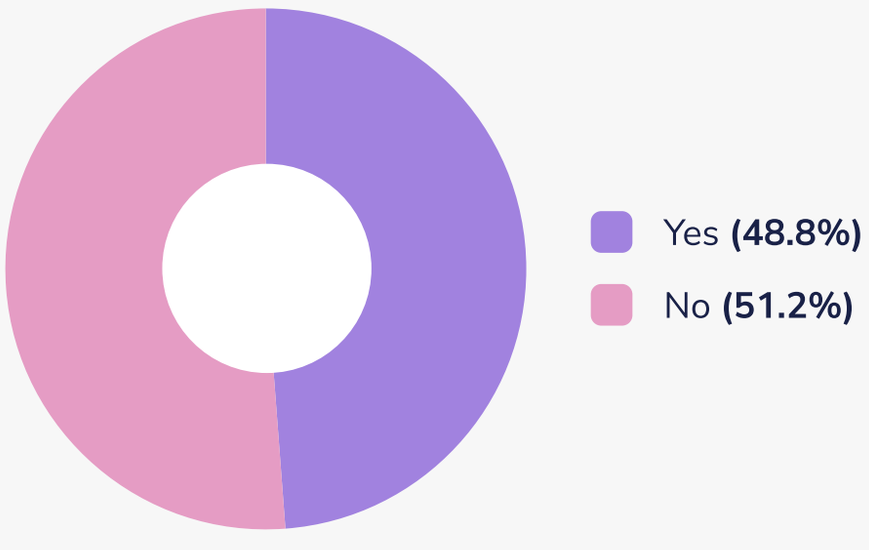
Does your current management strategy allow you to effectively automate your custom security workflows?



54% have an MDM that allows them to automate custom security workflows

54.2% say their MDM strategy allows them to automate custom security workflows, while 45.9% say it does not.

Does your current management strategy give end users a way to safely self-serve their own IT needs without involving the help desk?



49% have an MDM that allows end-users to serve their own IT needs

48.8% say their MDM gives end users a way to serve their own IT needs without calling the help desk.

Summary

A glance through the charts is enough to tell the story of MDM effectiveness: only half have adequate visibility into enrolled devices, maintain secure laptops and servers, have automated security workflows, and enforce compliance and security posture across their organization.

We'll learn more about their plans for the future in the next section.

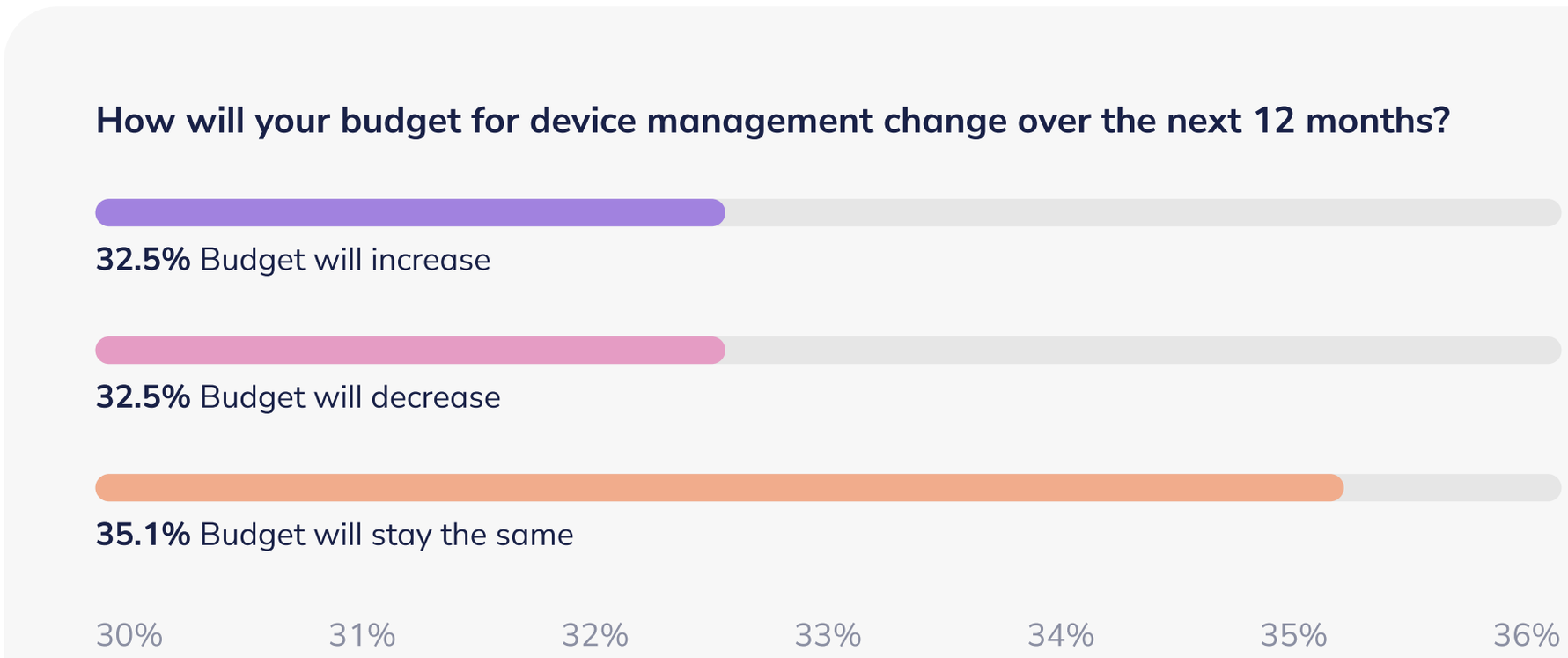
PART 5

Plans and priorities for the future

Mobile device usage is only increasing in most organizations, especially as they expand further into working remotely. But do organizations consider MDM strategy a top priority? Here's what the future looks like for device management.

Budget allocation over the next year will vary

Respondents reported varying levels of investment in MDM in the future. 35.1% say their budget will stay the same in the coming year, and 32.5% say their budget will increase. An additional 32.5% say their budget will decrease.



Most wanted MDM features

If our respondents were evaluating vendors for a new MDM solution, these are the top features they'd look for:

Cloud-hosting

As more organizations turn to the cloud and away from on-prem, 28.3% say they want a cloud-hosted MDM.

Built-in security controls with sensible defaults

The same number of respondents (28.3%) want customizable security defaults for their MDM.

Inspectable, modifiable, open-source code

Most MDMs today are black boxes without any access to code. 26.3% want open-source MDMs so that they can inspect and modify code.

Queue up software or tools at onboarding

25.9% of respondents also want more software set up out-of-the-box, including Zoom, Slack, Python, etc.

Real-time visibility of every device that's less than a minute old

Another 25.9% want to be able to check compliance and other device statuses in real time and gather data that's less than a minute old.

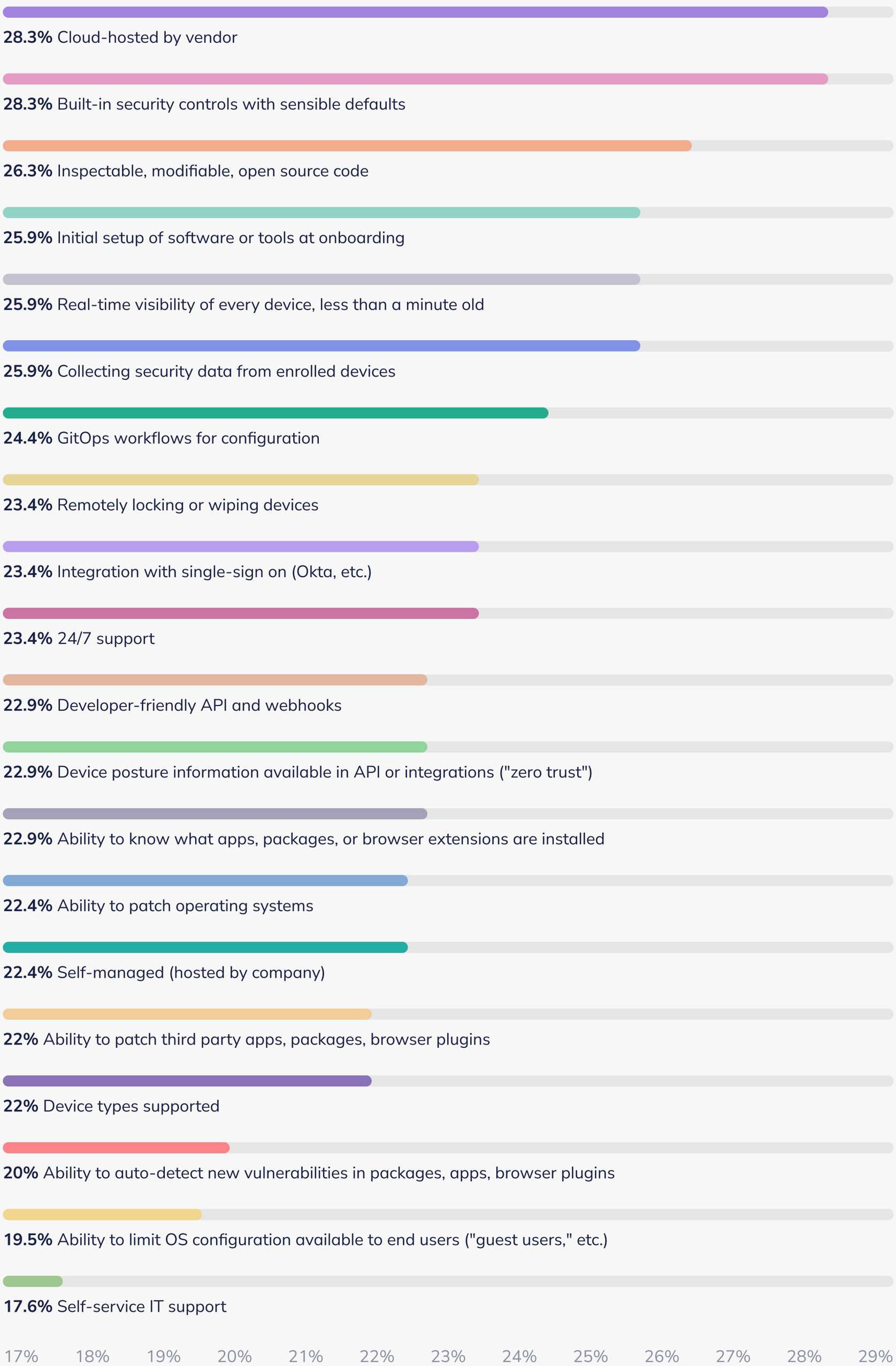
Collecting security data from enrolled devices

25.9% also want their MDM to collect security data from devices so that they can take immediate action on vulnerabilities.

GitOps workflows for configuration

Configuration was one of the main challenges our survey measured. 24.4% want to be able to configure their MDM solution more freely.

If you were evaluating a new MDM vendor, what features and capabilities would be most important to you?



Top priorities for MDM strategies in 2022

We asked respondents what their main priority is for their MDM strategy over the next year. They replied:

Device security like multi-factor authentication (MFA) at login

Using multi-factor authentication to ensure security across their organization's devices is a top priority.

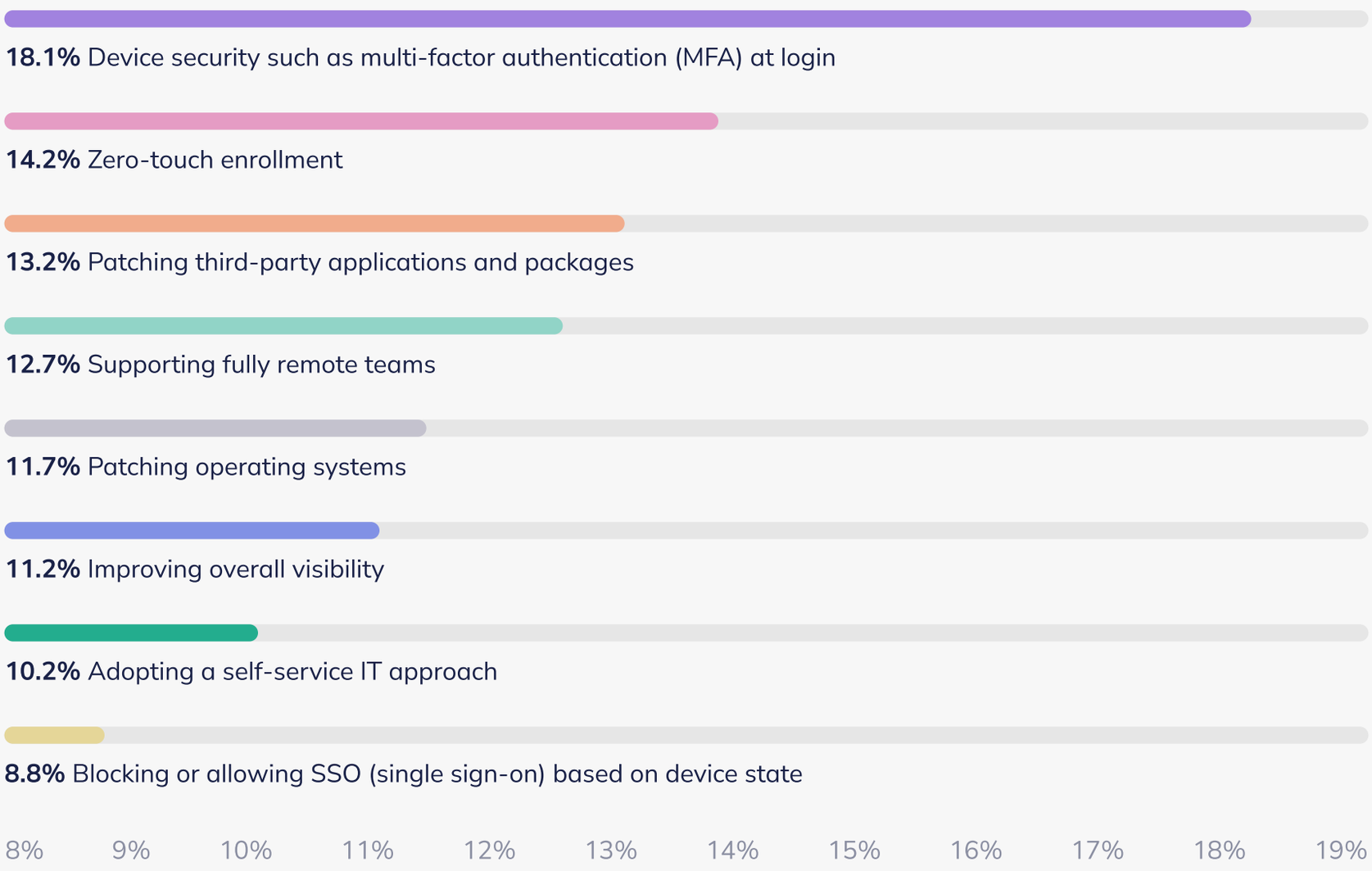
Zero-touch enrollment

Respondents also want to focus on zero-touch enrollment to increase enrollment rate and improve monitoring and compliance.

Patching third-party applications and packages

Another priority is patching and securing third-party applications on devices.

What is your #1 priority for your device management strategy over the next 12 months?



Summary

With the expected growth of remote work in the future and the number of malicious actors exploiting vulnerable endpoints on the rise, originations must have a robust MDM. Security is a top priority for our respondents. This means using multi-factor authentication across devices and protecting third-party apps and packages. Zero-touch enrollment is another priority to increase enrollment rates.

For teams that want more endpoint protection — as many as half of the security professionals we surveyed — an open-source cloud-based solution that is easy to set up, has built-in security defaults, and gives real-time visibility into their fleet will satisfy their MDM priorities.

PART 6

Preparing for the future of device management

Do organizations understand the state of their devices? Or are they underprepared to manage security and compliance in an increasingly remote world? Some organizations have near-total enrollment of their devices in an MDM solution that provides effective visibility, incident response, and security across devices. However, many others struggle with device management — often starting in the deployment phase.

If you want to strengthen your MDM strategy, or you're looking for better ways to manage devices, consider following these recommendations:

Protect remote workers with zero trust, TLS, and 2FA

With workforces split between fully remote, half remote, and no remote employees, focus on designing solutions that are as effective in an office as they are from an unknown internet connection. Considering all networks untrustworthy is the safest approach, even if your team currently works out of an office. Not assigning trust is also useful if anything prevents employees from working at the office. To keep devices safe in any location, move away from VPNs to granular proxies with TLS and two-factor authentication (2FA) that don't allow lateral movement.

Either manage Linux or don't use it

Our survey revealed that Linux is the second most common platform to exist outside the protection of an MDM. We suggest including Linux in device management or banning it. If you don't manage your fleet of Linux workstations, evaluate requirements to include them in secure configuration and monitoring. Otherwise, they pose a security risk to your organization.

Start managing containers

Also, identify your container security needs. Many respondents weren't sure if their company protects containers, and others don't currently secure them. Likely they will need to defend containers soon, and organizations who don't use these functions still have time to create their container strategy. Evaluate your existing IT and security stack to see where you can improve real-time monitoring of container workloads.

Make Windows part of your MDM

Move Windows workstations from legacy GPO management to MDM and Autopilot. It's common for Windows systems to be left unmanaged, and MDM policies for Windows are still behind. But with remote work on the rise, we can't assume laptops will be connected to the company LAN to enforce policies. Like container security above, now's the time to bring Windows — the most used OS that falls outside management — into your MDM solution.

Use open APIs for real-time compliance

Many of the challenges above focus on real-time compliance verification for all devices in an organization. To make compliance simpler, use tools with open APIs so you can query the status of devices. You also want these APIs to alert you when a policy check fails on a device. Immediate remediation can happen this way.

The future of device management

A comprehensive device management approach is a necessity for organizations, especially those with remote workers. Make sure your MDM solution offers the endpoint access and insights you need to keep your organization safe and secure.

REAL TIME | OPEN SOURCE

Safe and secure devices for security teams

Fortune 1,000 companies use Fleet to keep their MacOS, Windows, and Linux devices secure and compliant.

Try Fleet → | Schedule a demo →

fleet