

Stratix Research Shows Most Companies Have Worrying Endpoint Management Vulnerabilities

Companies are using more and more connected devices, but they're behind in managing them

A circular inset on the right side of the slide shows a person's hands interacting with a tablet. The tablet screen displays a colorful bar chart and a pie chart. The person is wearing a black watch on their left wrist. The background of the inset is a blurred office setting.

in partnership with
SOTI



Executive Summary



Survey of IT Leaders Examines the Current State of Endpoint Management

The number of devices now used by companies, healthcare organizations, and educational institutions is staggering. The average enterprise manages tens of thousands, and with IoT and mobile device use cases growing, IT teams will be tasked with managing more and more with every passing year. It can be complex and time-consuming—especially when organizations have multiple endpoint management platforms.

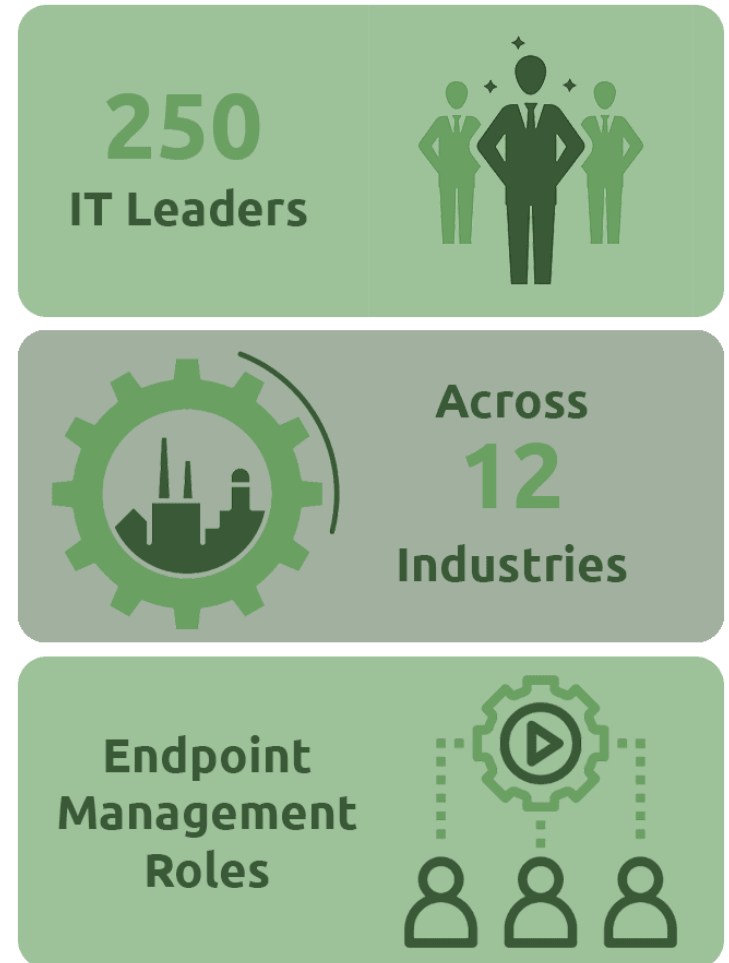
The solution is holistic unified endpoint management (UEM) that enables the control of every kind of endpoint—including PCs, mobile devices, printers, and IoT—from a single platform, which simplifies management, reduces the workload, and significantly improves security. UEM can even be used to tailor user experiences to specific workflows for enhanced productivity.



With this research in partnership with SOTI, we wanted to learn how far organizations truly are down the path of UEM.

- How embedded is it in their strategy, decision-making, and self-accessed vulnerabilities?
- How covered are they across their entire technology environments?
- How many endpoint management platforms do they have?
- Do they outsource or have the resources to handle it internally?
- Why do/would they outsource?

To get our information, Stratix surveyed 250 IT leaders across more than a dozen industries who have endpoint management as part of their job responsibilities. With our questions, we have a good picture of the current state of endpoint management, including vulnerabilities, pain points, and solutions.



The margin of error is +/- 5.89%.

Key Findings

One of the most striking results in our survey is respondents told us they think 30 percent of their endpoints lack adequate management. In a world where just one unmanaged device can be the access point for a major data breach, that's a troubling statistic.

We also found while more respondents chose mobile devices as their biggest vulnerability, when we dug deeper, it became clear there are greater concerns.

Going beyond the security aspects, we saw that despite high awareness of the value of UEM, most organizations are juggling multiple endpoint management platforms. That means they're missing significant opportunities.

Read on as we dive deeper into the research and examine why organizations aren't doing better in this area.

What percentage of your endpoints do you think your organization adequately manages?



● % of devices not adequately managed

Why Endpoint Management Matters

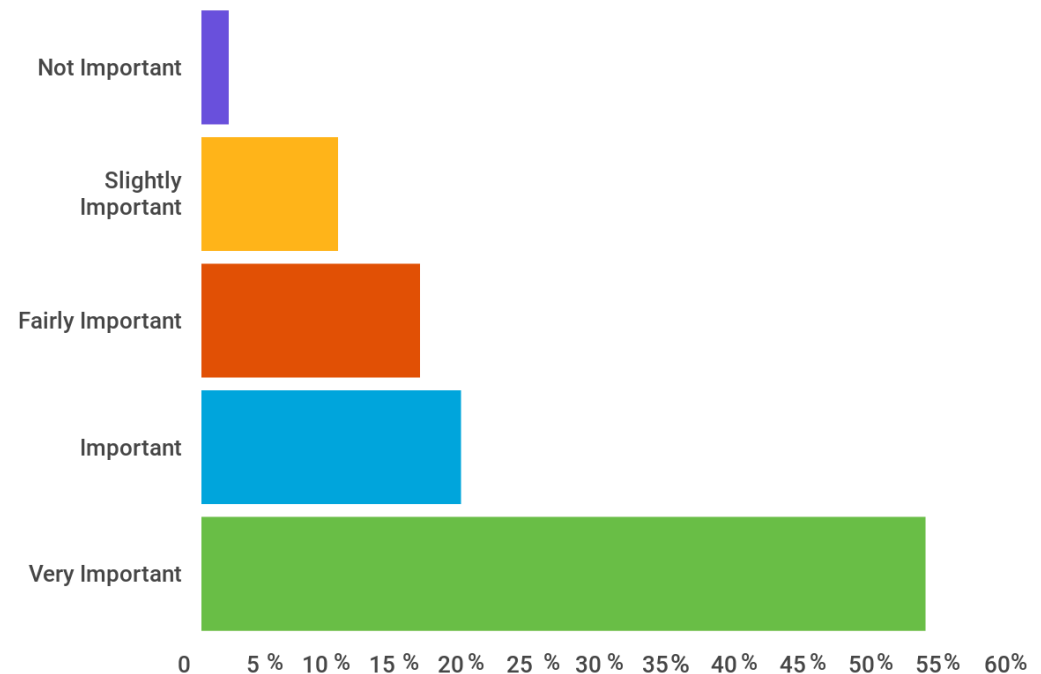


What's the Perception Out There?

In our survey, respondents acknowledged that endpoint management is crucial for maintaining a secure, compliant, and efficient IT environment. It ensures an organization's technology operates smoothly while minimizing risks and maximizing productivity.

When asked how important endpoint management is to their organization's IT strategy and decision-making, more than 70 percent ranked it as either important or very important.

How Important is Endpoint Management to Your Organizations IT Strategy?



Importance of endpoints in the organization	Percentage of Endpoints Covered	
	Not at all important	33%
	Slightly important	52%
	Important	63%
	Fairly important	67%
	Very important	76%

Digging into the data further, we found a direct relationship between the perception of importance and the percentage of endpoints managed within organizations. The higher the perception of importance, the greater the percentage covered, and vice versa.

Ninety percent of the group that ranked endpoint management as very important also said they use it to automate tasks. That means they're significantly reducing the complexity of routine IT workflows and the time spent on them. Automation plus better security equals cost savings—both in terms of operations spending and reduced security liabilities.

The survey found a distinct correlation between how endpoint management is strategically viewed and the organization's acuity with UEM.

Our Research Shows Where Companies Fall Short



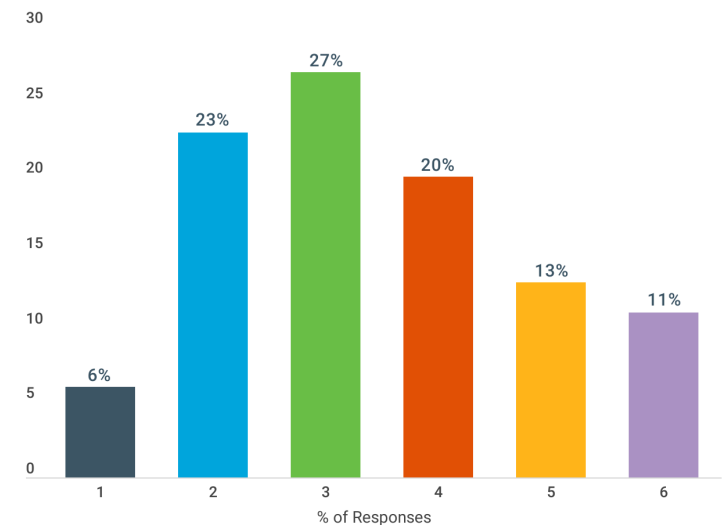
They Know There's a Better Way, But...

Ninety percent of our respondents told us they're aware that a UEM solution can manage all endpoints from a single platform, including PCs, mobile devices, IoT, printers, and BYOD. Despite that, 94 percent are using more than one endpoint management platform.

Six percent had one platform, while the majority averaged between two and four. We know at Stratix from our relationships with customers and providers stretching over decades that many mobile solutions were adopted piecemeal within companies, and each often had its own mobile device management (MDM) platform. That's now snowballed into a high level of complexity, but many organizations are limited by small IT teams and a lack of expertise, so there's an inability to improve despite the understanding that they could if they consolidated everything into a holistic UEM platform.

With a comprehensive solution, you manage all devices and operating systems from a single pane of glass. A single platform also gives IT teams flexibility and choice, knowing that no matter what device type is selected for future projects, the UEM can handle them.

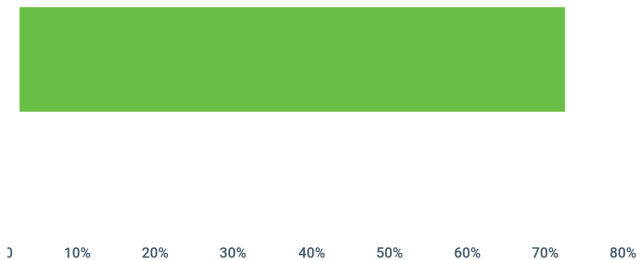
How many endpoint management platforms does your organization use?



Disturbing Gaps in Coverage

As mentioned in the Executive Summary, we were shocked to find our respondents think only 70 percent of their endpoints are adequately managed—meaning they're very vulnerable to security issues, increased downtime, and higher support costs.

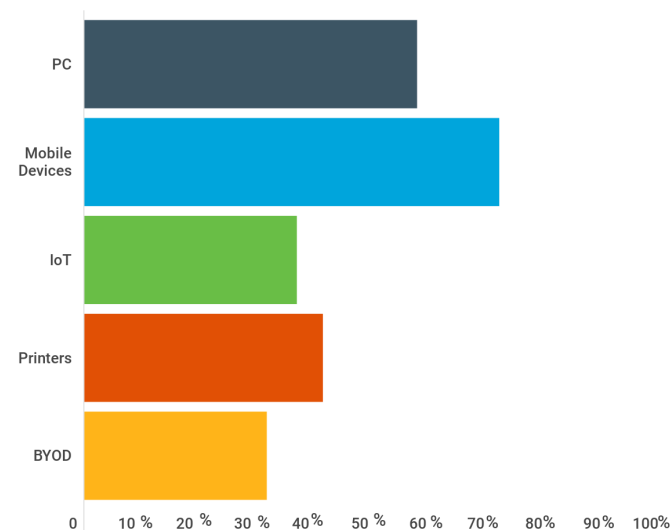
What percentage of your endpoints do you think your organization adequately manages?



Which Devices Are Vulnerable?

Our research found a perception that mobile devices rank highest as potential vulnerabilities, followed by PCs, printers, IoT, and then Bring Your Own Device (BYOD) equipment.

What do you think your organizations vulnerabilities are?



Note: Multiple choice answer so percentages do not equal 100.

The research indicates, not surprisingly, that there is a bias in selecting mobile devices among respondents because mobile was the starting point of UEM, having emerged from effective Mobile Device Management (MDM) solutions. It was, therefore, necessary to go a layer deeper into the data and assess respondents on their self-reported percentage of endpoints adequately managed compared with where they think their vulnerabilities are. That's where the data gets interesting.

In the table on this page, you can see how when an organization adequately manages its devices as a whole, it's more likely that it understands where its actual vulnerabilities lie.

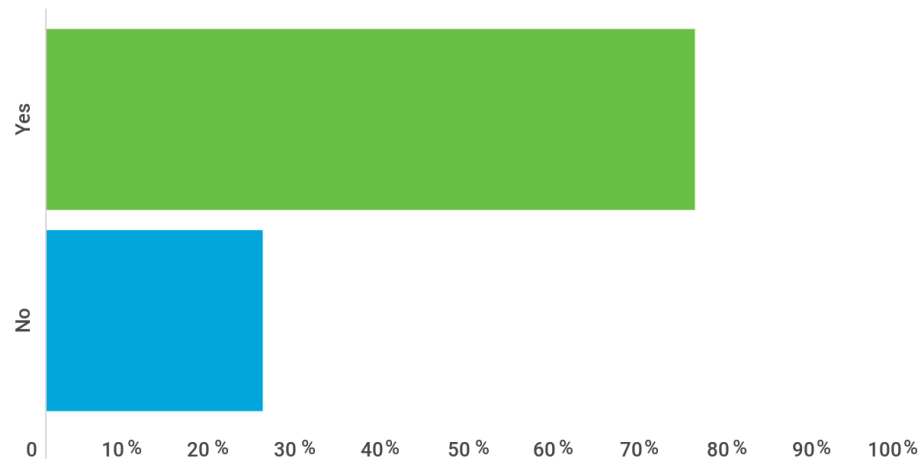
- For organizations scoring their percentage of endpoints adequately managed between 51-75 percent, mobile devices were of the lowest concern, and printers were their highest.
- For organizations scoring their percentage of endpoints adequately managed between 76-100 percent, BYOD and laptops were the highest vulnerabilities. These organizations likely are looking toward a more holistic UEM strategy that incorporates laptops and BYOD.

% of Endpoints Adequately Managed	PCs	Mobile Devices	IoT	Printers	BYOD
<25%	2%	3%	1%	4%	4%
26% - 50%	18%	20%	18%	17%	7%
51% - 75%	32%	31%	36%	38%	33%
76% - 100%	48%	46%	45%	42%	56%

Our findings consistently confirm our hypothesis that respondents realize that having multiple endpoint management platforms is a problem, with 76 percent calling the lack of a comprehensive UEM solution a vulnerability. So again, we see how a lack of resources and expertise is holding organizations back.

So again, we see how a lack of resources and expertise is holding organizations back.

Do you feel like your organization is vulnerable because it doesn't have a comprehensive unified endpoint management solution vs. multiple MDM or EMM platforms?



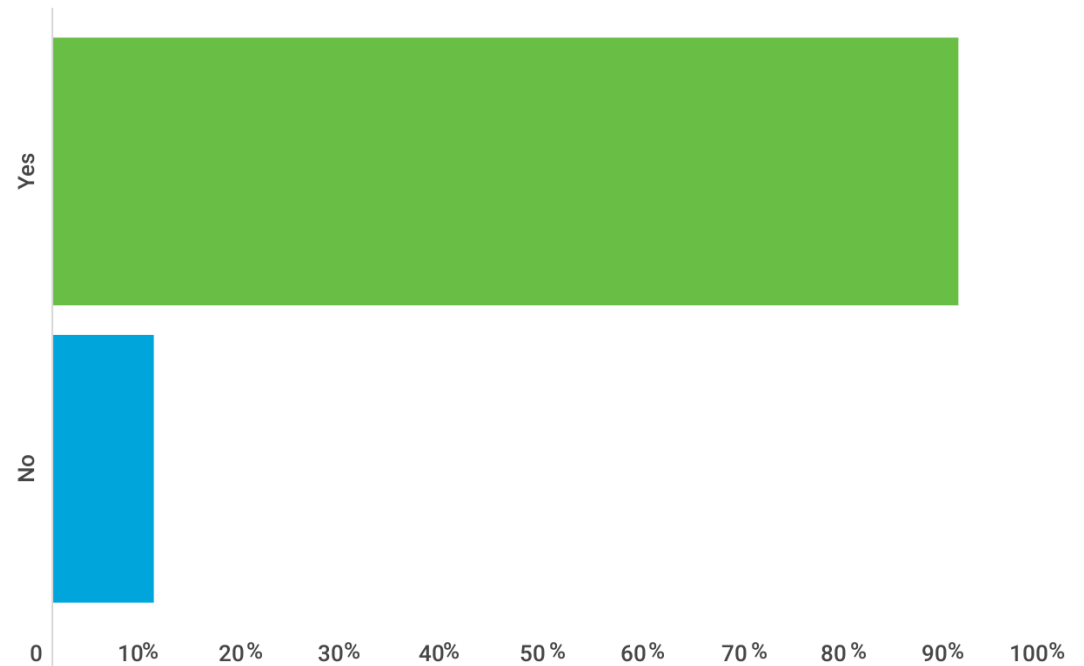
Automation is a Priority



There's More to Endpoint Management Than Just Security

The automation of routine IT tasks is a significant benefit of endpoint management platforms, and our research found more than 90 percent of respondents are looking for ways to do more of it. That shows they need to free up resources that are currently bogged down with maintenance tasks that—while important—could be handled faster with a UEM solution.

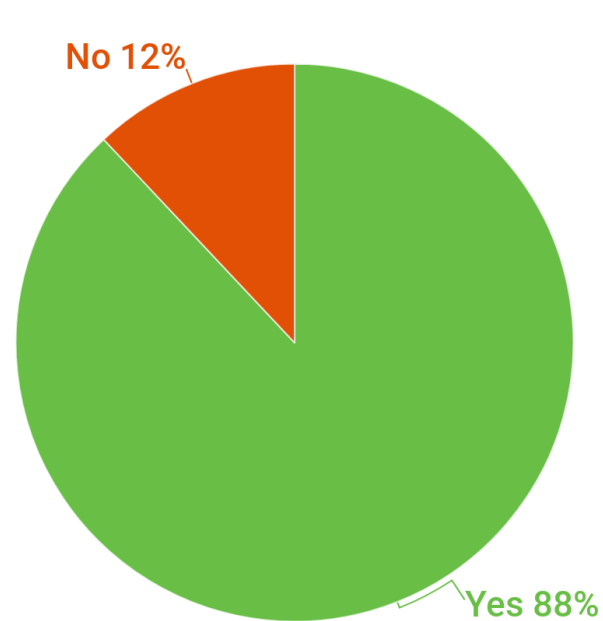
Is finding ways to automate IT tasks a priority for your organization?



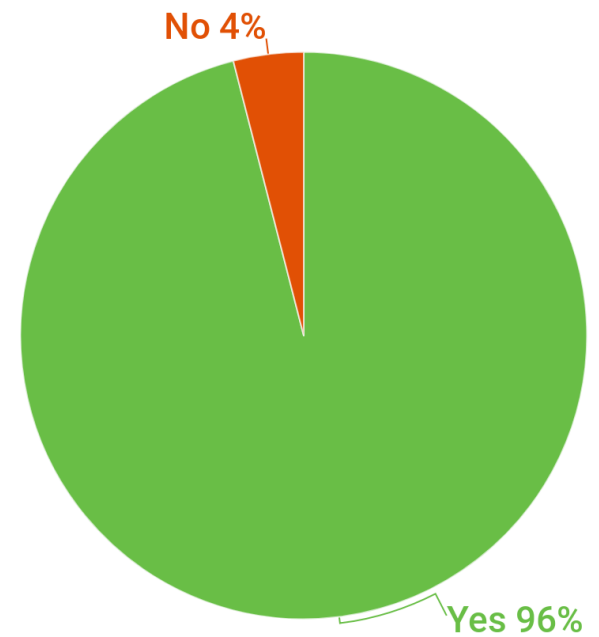
Digging deeper into the data, the desire for more automation is greater in organizations that outsource their endpoint management vs. those that do it in-house.

That suggests they've found more efficiency in outsourcing.

Is finding ways to automate important?



In-house

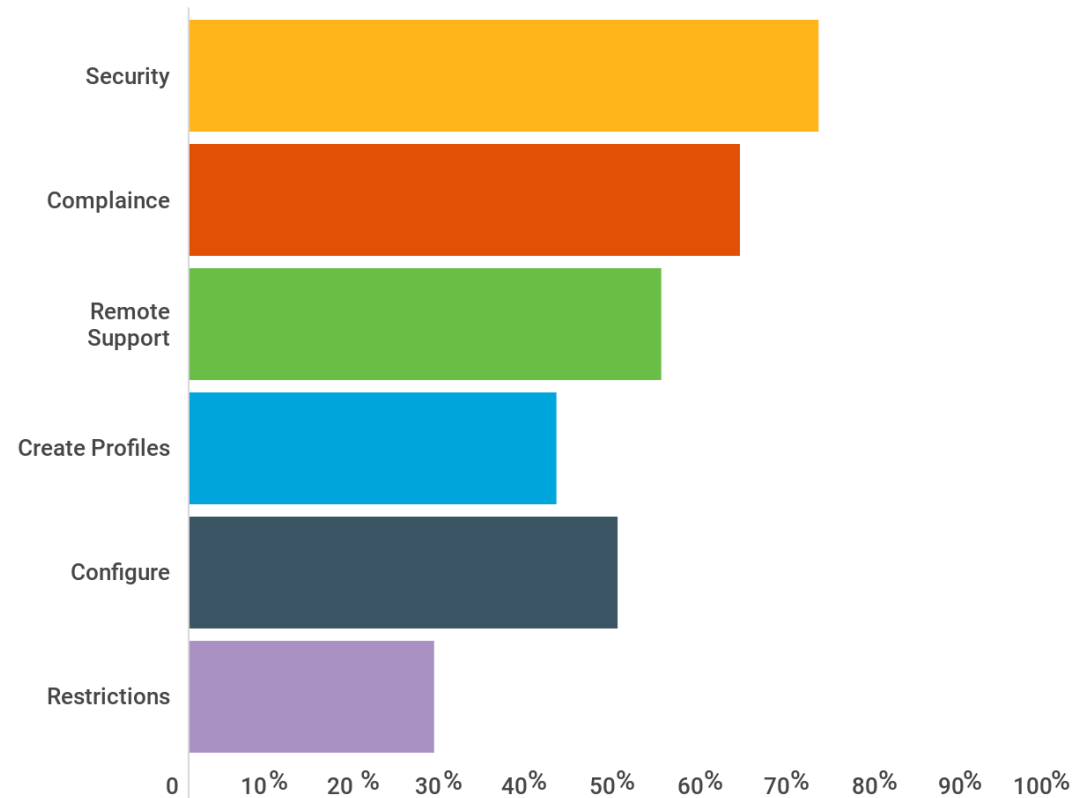


Outsource

We asked our respondents how they use UEM and got a ranking for use cases. The numbers are highest for security and compliance. We found those that outsource focus more on security while it's nearly evenly split for DIY organizations. Across the entire group, there's significant use of UEM for remote support and configuration. Fewer use it for creating profiles, and less than 30 percent for restrictions.

For those who are not leveraging UEM for custom profiles, it could be a lack of knowledge of what's possible, or they don't have workflows where it's an advantage. Custom profiles tied to a user's login are especially useful in organizations that leverage shared devices. In retail, for example, an associate who focuses primarily on customer service would benefit from a different home screen configuration and apps than one who mainly does inventory management.

What do you use UEM for?



The Majority of Companies Don't Outsource Endpoint Management



Those That Don't Outsource Are More Likely to Have Fractured Environments

Our survey also looked at whether organizations handle their own endpoint management or if they outsource and why. Nearly 60 percent do it themselves.

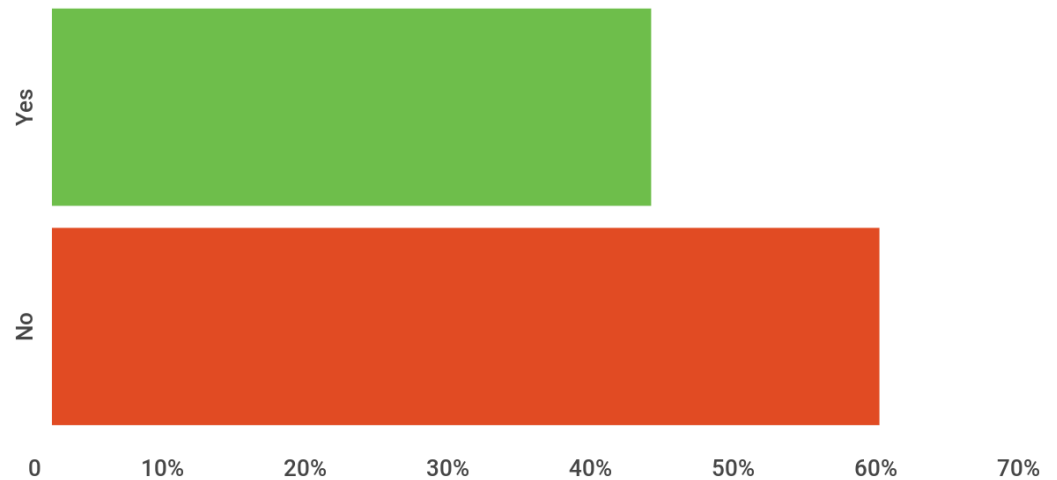
The top five reasons given for not outsourcing:

1. Have adequate in-house resources
2. Quality concerns
3. Less control
4. Communication barriers
5. Cost

The top five reasons for outsourcing:

1. Too difficult to staff/support
2. Difficult to support complex environments
3. Difficult to train and retain
4. Want to focus on the AI of the platform and not on maintenance
5. Maintain service levels with small in-house staff

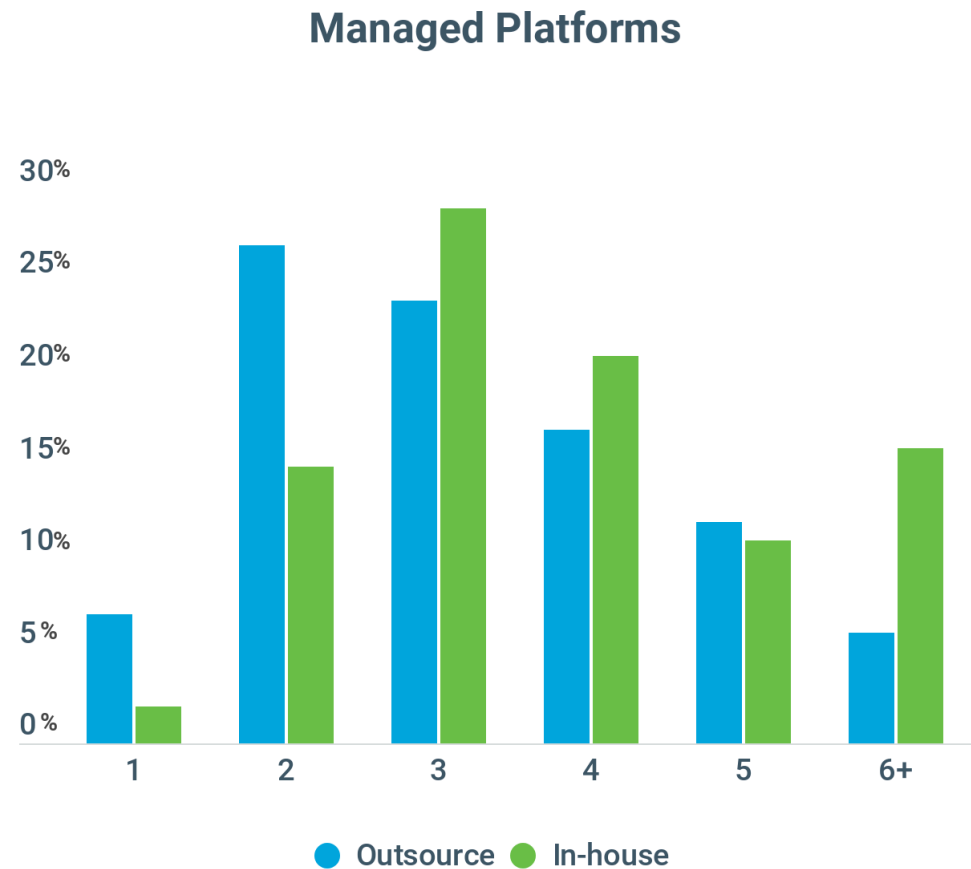
Do you outsource your endpoint management?



We found that those who do it themselves are more likely to have more platforms to manage and a less homogeneous environment—meaning they have more vulnerabilities and pay more in operational costs. UEM solutions offer device analytics that drive data-driven strategic decisions.

For example, analytics on battery conditions and predicted remaining lifespan gives allows IT leaders to precisely time device refreshes.

The data further showed that organizations that outsource are less likely to report that they adequately manage their endpoints. Ninety-four percent of those who outsource said they're happy with their provider, and only six percent are not.



We asked for reasons. Those who are dissatisfied with their outsourcer said:

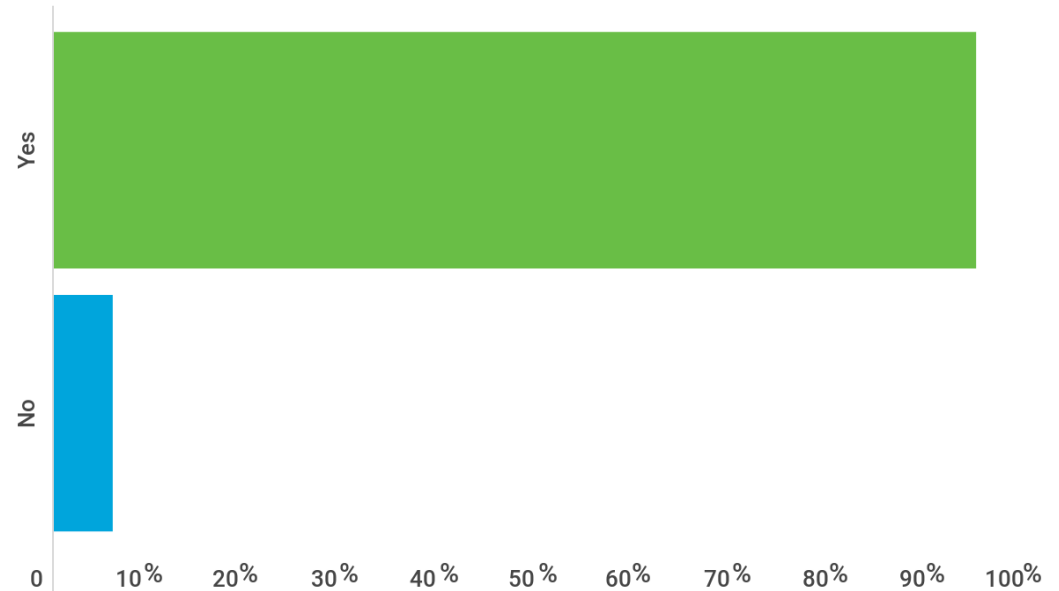
- They do not seem very responsive to our needs
- Seem to be just skimming by the skin of their teeth
- Because we are having some difficult issues within our organization
- They do not have very good control over my costs
- Not always available. Slow response

Whereas those who are satisfied said:

- Cost-effective
- Provide certified experts
- Improve our policies
- Great response times
- Streamline, good quality, reliable
- Frees me up

It's clear from the data that it's important for organizations to ask around before choosing a managed services provider, but when they have a relationship with a good one, they are able to reduce costs, cover more endpoints, and leverage more features of the platform strategically.

Are you happy with your current outsourcing provider?



Conclusions



Organizations Can Do Better

The main takeaway from this research is that while organizations know the value of holistic endpoint management, most have yet to move to a single UEM platform and are juggling multiple solutions—meaning they're missing out on potential savings, better security, and increased efficiency.

This study aligns with [past surveys by Stratix](#) that show organizations often do not have holistic technology strategies across the board. Individual departments are often responsible for designing, procuring, deploying, and supporting their technology. That kind of siloed thinking negates opportunities for scale and can detract from greater strategic goals and nimbleness.

Because they're stuck in multi-platform endpoint management environments, organizations are not secure enough, are wasting resources, and are missing opportunities for cost savings along with cutting-edge solutions such as BYOD containerization and more.

It's well known that many IT teams are reluctant to outsource because of the perception of losing control or poor quality, but this research shows there's actually more of both when you have the expertise and accountability of a high-quality managed services provider. While it offers tremendous value, configuring a holistic UEM platform across such diverse endpoints as PCs, mobile devices, printers, and IoT requires specialized knowledge that many organizations lack. That's expertise that leading MSPs bring to the table.



Interested in talking more about your endpoint management strategy? Reach out to Stratix today.

[Contact Us](#)

About Stratix

Wherever your organization is in its mobile-first journey, you don't have to go it alone. Stratix has led from the front on mobility for four decades. We can help you design and deliver end-to-end mobile technology solutions that make your organization's mobility convenient, easy, and cost-effective. We execute deployments at scale and with precision so they work in the hands of your end users out of the box. Once devices are in service, we provide ongoing world-class managed services and visibility tools that ensure nonstop mobility throughout their lifecycle. For additional information, visit www.stratixcorp.com



About SOTI

SOTI

SOTI is a proven innovator and industry leader for simplifying business mobility solutions by making them smarter, faster and more reliable. With SOTI's innovative portfolio of solutions, organizations can trust SOTI to elevate and streamline their mobile operations, maximize their ROI and reduce device downtime. Globally, with over 17,000 customers, SOTI has proven itself to be the go-to mobile platform provider to manage, secure and support business-critical devices. With SOTI's world-class support, enterprises can take mobility to endless possibilities. For more information, visit soti.net.

Thank You for Reading Our Research Report!

Is your organization struggling with unmanaged endpoints?

Speak with one of our UEM experts to get an assessment of your endpoint environments and work towards a plan to create a holistic unified endpoint management and improve security.