Auvik

IT trends 2024: industry report

The automation imperative

Table of Contents

Auvik

Executive Summary

With many IT teams reporting difficulty sourcing talent, it comes as no surprise that the theme for this year's IT Trends Report is automation.

Whether the topic is managed service providers (MSPs) and how they can ensure quality of service to their clients, or an internal IT department and their challenge to do more with the limited tools and team members available, automation can contribute to a better end-user experience.

Another highlight from the data inside this report comes from the topic of internal visibility for manager roles and above. It becomes apparent in the results that there is a gap between the experiences of IT operations personnel on the front lines and what their management perceives. What can be done to bring teams and their leadership into alignment? We'll draw further conclusions on this topic and make recommendations throughout the report.

For now, consider the impact of the tools your organization uses for front-line IT employees. Do those tools help or hinder how employees deliver the expected end-user experience? In a time when budgets can be tight, when talent is hard to find, and tool sprawl can stretch as far as 20+ network related applications and 500+ SaaS programs in inventory, automating even a portion of the manual labor currently on technicians' plates can create change. In fact, we might go so far as to say you can't afford *not* to be thinking about automation.
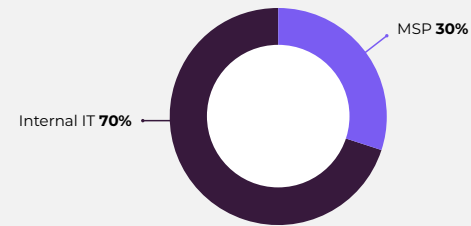
Methodology & Firmographics

This report presents the results from an online survey that was conducted on behalf of Auvik Networks and was completed by 2,100 IT professionals. The survey was fielded in Q4 of 2023. The objective of this survey was to examine the evolving roles of IT professionals and departments, including their reporting structure, top strategies, time management practices, and ongoing challenges.
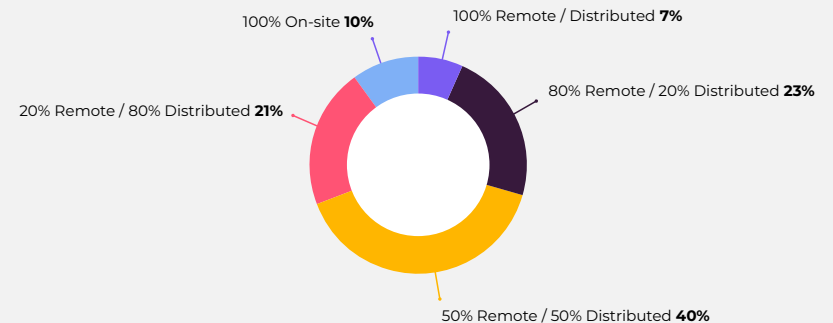
The survey also looked at what technology IT professionals are using to both manage day-to-day operations and prepare for future needs. We compared data against trends seen in 2023, to highlight what's changed, what's stayed the same and what could be on the horizon. The survey includes respondents from Managed Service Providers (MSPs) and internal IT teams. There is a +/- 2% Margin of Error at 95% confidence.

Canada **3%**

UK **2.5%**

Spain **1.5%**

US **84%**

Mexico **7%**

ROW **2%**
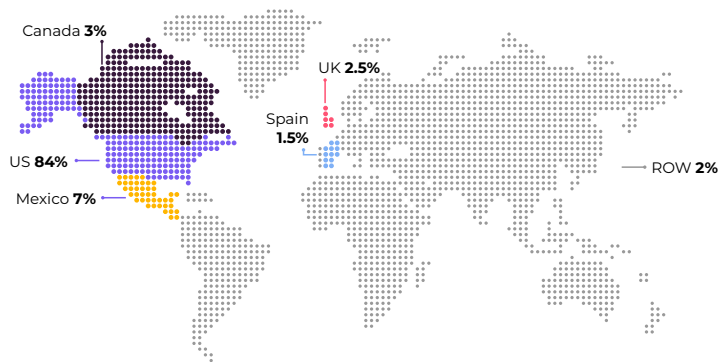
Mix of internal IT vs. managed service provider (MSP)

MSP **30%**

Internal IT **70%**

Remote, hybrid, and on-site working models

100% On-site **10%**

100% Remote / Distributed **7%**

80% Remote / 20% Distributed **23%**

20% Remote / 80% Distributed **21%**

50% Remote / 50% Distributed **40%**

MSP response breakdown

Number of employees

- 1–50 **4%**
- 51–100 **9%**
- 101–200 **15%**
- 201–500 **33%**
- 500+ **39%**

Role distribution

- Systems Administrator **2%**
- Helpdesk/Service Desk Manager or Technician **2%**
- Network Practitioner (administrator or engineer) **3%**
- Operations Manager **25%**
- VP or Director **25%**
- CEO/CIO/CTO/COO **36%**
- Owner/Operator **6%**

Internal IT team response breakdown

Number of employees

- 5000+ **9%**
- 1–250 **8%**
- 251–500 **16%**
- 501–1000 **31%**
- 1001–5000 **36%**

Role in IT

- CEO/CIO/CTO/COO **36%**
- User **15%**
- VP or Director **22%**
- IT or Operations Manager **43%**

Internal IT team response breakdown [cont.]

Number of IT employees

| 1–5 **5%** | 6–10 **12%** | 11–20 **32%** | 21–50 **38%** | 50+ **13%** |

Industry

Industry	Percentage
IT managed service provider (MSP)	30%
Financial services	12%
Manufacturing	12%
Education	10%
Healthcare	8%
Professional / business services	5%
Retail	5%
Information technology (non-MSP)	4%
Utilities \ energy	4%
Other	4%
State / local government	4%
Transportation	3%
Leisure / hospitality	2%
Federal government	<1%

01

Auvik

Section 1

The Modern Network

Network homogenization

The majority of respondents in this year's report (69%) describe their client's networks as either fully or mostly homogenized, meaning most devices are made by the same vendor.

69%

of respondents describe their client's networks fully or mostly homogenized

17%

of MSPs say their client's networks are composed of several different vendors

Worth considering also is the significant number of MSPs (17%) who say their clients' networks are composed of several different vendors. In industries like government and utilities/energy, internal IT teams also report that their organization's network composition is mixed (51% and 52% respectively).

Tool sprawl

Most (44%) of IT professionals are working with at least 10 or more network-related tools in their organization. Of government respondents, 44% reported using more than 20 network-related tools. This is an alarming amount of tool-sprawl, especially considering there are tools that exist specifically to mitigate the number of tools an IT professional needs to manage networks.

Number of network-related tools organizations are using

- 20+ **15%**
- 1–3 **7%**
- 4–10 **37%**
- 10–20 **41%**
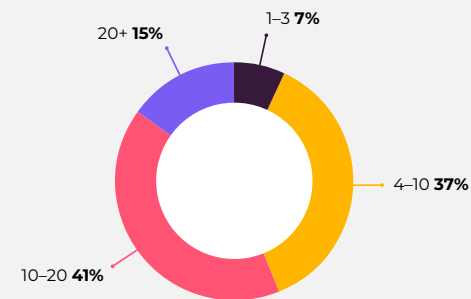
Remote readiness

Remote readiness has been an important topic in the research for this report in past years. Post 2020, less than 10% of internal IT teams support a workforce that is 100% on-site, which means IT is supporting some level of remote working about 90% of the time.

90%

support at least some level of remote work

40%

half remote, half on-site

The most common team structure is half remote, half on-site (40%). Smaller organizations (250 employees or less) are more inclined to have either fully-remote or fully on-site workforces, rather than a blend of both. As expected, tech and IT industries are more likely to be fully remote, while healthcare was more likely to be 100% on-site.

2023 vs 2024 data:

There's been a 5% increase in workplaces with a 50/50 split between remote and on-site. Of those respondents who support at least some remote workers some of the time, most (96%) agree or strongly agree that their network toolset is prepared to meet these needs.

C-suite respondents are more likely to report a higher level of confidence in the toolset, with 58% who strongly agree. IT technicians are the least likely to report a high level of confidence in the toolset, with 35% who strongly agree.

58%

C-suite with a high level of confidence in the toolset

35%

IT technicians with a high level of confidence in the toolset

→ IT technicians are the least likely to report a high level of confidence in the toolset

This is the first in a series of data points that suggest a gap between what management perceives and the actual difficulties faced in the field.

Note: IT technicians who use Auvik were the most likely to express confidence at this employee level, with over 57% saying they strongly agree that their network toolset is prepared to support remote work.

![Auvik]

Network activities

39%
Make config
changes weekly

48%
Fully remote orgs
report daily
back-ups

Most (39%) configuration changes are being made to networks on a weekly basis. Government IT is three times more likely (12%) to make configuration changes only on an annual basis. Utilities/energy IT are almost twice as likely (40%) to make daily configuration changes. IT pros from 100% remote orgs are much more likely to report daily back ups of configs (48%) than the average IT employee (27%)

⚠️ **CAUTION**

C-suite respondents are much more likely to report daily configuration changes (30%) than technicians (8%). C-suite is also more likely to report daily configuration backups (36%) than technicians (20%). Either upper management is not aware of the real amount of work going into configuration, or technicians are simply so time-strapped that they struggle to meet company policy in this area.

23%
gap in response

Technicians

C-suite

Less likely to report
daily config backups

Most likely to report
daily config backups

Documentation
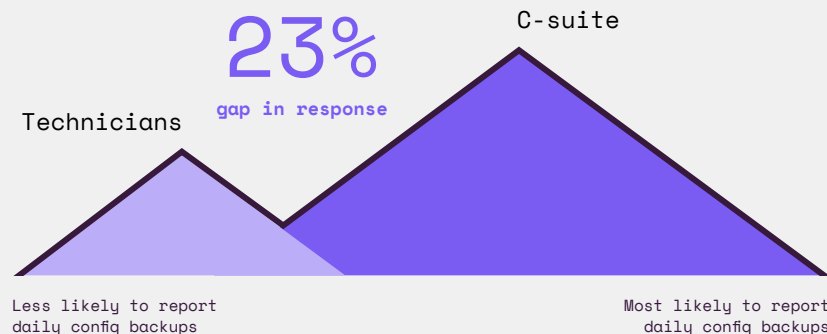
36%
Update network
documentation
weekly

29%
MSPs update
network
documentation
daily

The most common cadence for updating network documentation is weekly (36%). MSPs are most likely to do these network documentation updates more frequently; 29% report daily updates. As expected from industries that require strict compliance and timeliness, transportation, leisure and hospitality, and healthcare show the highest instances of automated network documentation (14% and 13% respectively).

Could these practices be beneficial for other organizations to adopt, considering increasing concern for security and compliance?

We'll address this in section 4 of this report. →

Monitoring and other activity on the network

The top five network management activities in 2024 include:

61%
Monitoring

55%
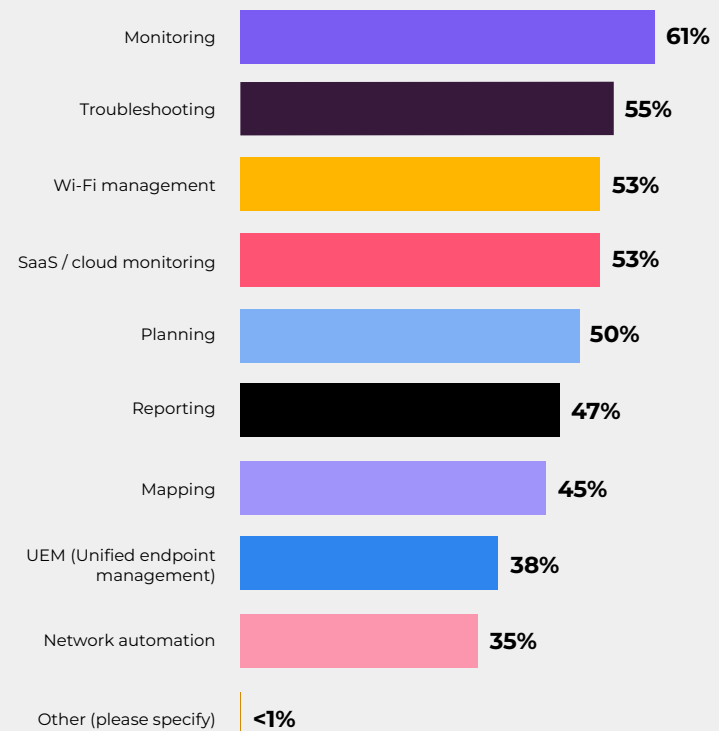Troubleshooting

53%
Wi-Fi management

53%
SaaS/ cloud monitoring

47%
Reporting

Only half of respondents said network planning was something their company engaged in. While this may seem like a less significant task if your network has been consistent for a while, remember that network planning can involve important security tasks like making time for hardware patches and replacements, or updating the network to prepare for technology advances in an industry, such as the move toward Chromebooks for schools.

Network management activities

Activity	Percentage
Monitoring	61%
Troubleshooting	55%
Wi-Fi management	53%
SaaS / cloud monitoring	53%
Planning	50%
Reporting	47%
Mapping	45%
UEM (Unified endpoint management)	38%
Network automation	35%
Other (please specify)	<1%

2023 vs 2024 data:

+4%

SaaS management
activity

+13%

Mapping network
activity

SaaS management as activity has increased by 4% since 2023 (49% to 53% in 2024). The biggest change in network activity focus is around mapping, which climbed 13%, from 32% in 2023 to 45% in 2024. This is also implied by the increasing security focus, as network mapping is a component in IT compliance.

The utilities/energy industry as a whole engages in the most network management activities. Larger companies were more likely to engage in network automation activities.

Company size is quite a big factor in automation: the larger the company, the more likely they are to engage in network automation activities—except at the 5000+ level, where we see this number drop off again, suggesting difficulty in implementation at the enterprise level.
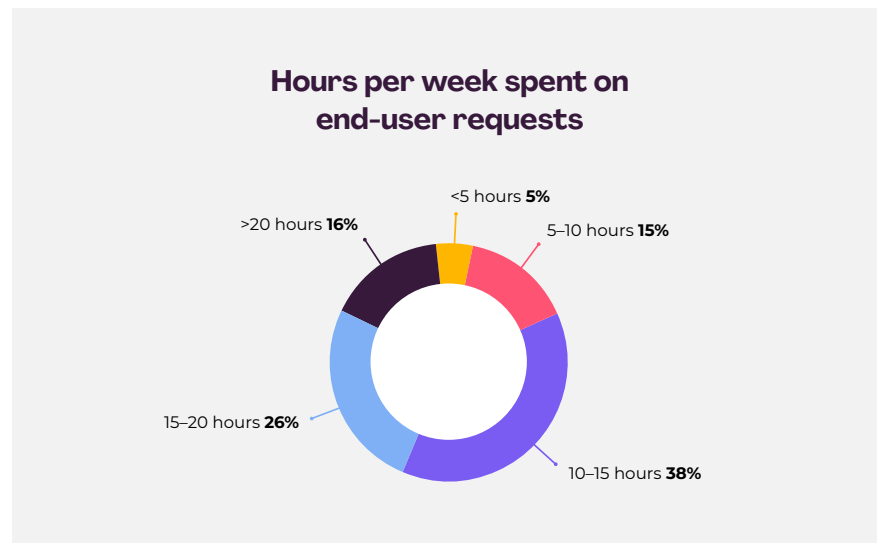
Network automation based on company size

02

Auvik
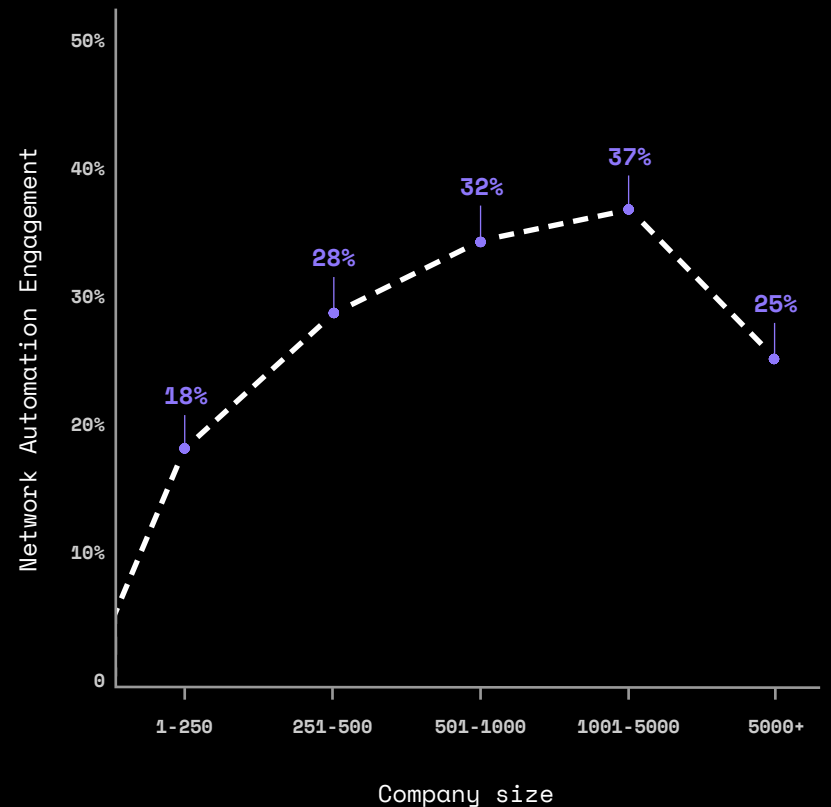
The Modern IT Professional

Most (47%) IT professionals report working between 31 and 40 hours, which would be considered an average or balanced work week, with MSPs leading this number and averaging 50% of their employees working the 31 to 40 hour range.

Hours per week spent on end-user requests

<5 hours **5%**

>20 hours **16%**

5–10 hours **15%**

15–20 hours **26%**

10–15 hours **38%**

The majority (64%) of internal IT departments spend between 10 to 20 hours a week resolving end-user requests. However, a whopping 16% spend over 20 hours a week on these reactive tasks. Almost half (47%) of government IT pros report spending above 20 hours a week on end-user requests.

What can be done about the enormity of this burden on front-line technicians?

Understanding the importance of end-user satisfaction is one factor. It may also be significant to consider whether the tools at IT professionals' disposal are helping or hindering their work.

So, let's first take a look at the metrics.

⟶
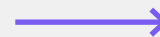
How IT professionals are evaluated on their work

Metric	Not important	A little important	Somewhat important	Very important	The most important
Percentage of uptime / downtime	1%	7%	18%	52%	23%
Cost of downtime	1%	6%	21%	47%	25%
Cost of IT overall	1%	5%	22%	46%	27%
Number of incidents	1%	6%	20%	48%	24%
Severity of incidents	1%	4%	20%	47%	28%
Number of tickets closed in a time period (day, week, etc.)	1%	5%	22%	49%	22%
Mean time to recolution (MTTR)	1%	4%	21%	49%	24%
Customer / user satisfaction	1%	3%	16%	43%	38%

The most important success metrics for report respondents this year include customer or end-user satisfaction (38%), severity of incidents resolved (28%), and cost of IT overall (27%).

38%
Customer or
end-user
satisfaction

28%
Severity of
incidents
resolved

27%
Cost of IT
overall

In industries where customer satisfaction was not the most pressing metric, cost and severity of incidents resolved were still considered the most important.

39%
of transportation,
leisure &
hospitality said
cost was the most
important

28%
of retail
said severity
of incidents
resolved was most
important

One answer for how to improve the balance between resolving high-priority items and giving end-users a great customer experience may lie in outsourcing some IT tasks to an MSP.

Interestingly, C-suite roles are more likely to list customer satisfaction as the most important metric (46%), compared to technicians (26%), IT operations managers (33%) and VP/directors (38%), suggesting that the higher you go in the organization, the more the customers' experiences are emphasized.

Emphasis on customer satisfaction

Technicians
26%

IT operations
managers
33%

VP/directors
38%

C-suite
46%
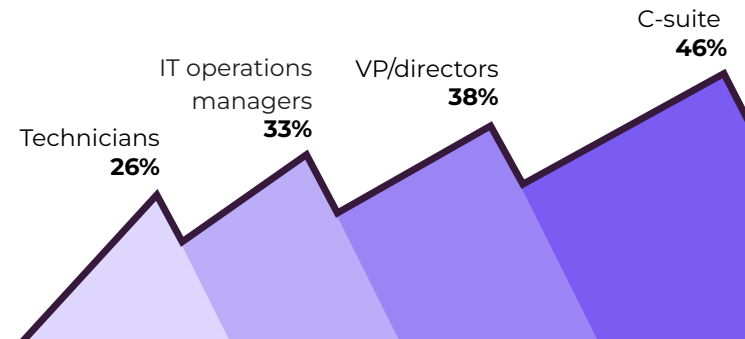
We know that keeping workers productive regardless of where they are working from is a high priority for IT departments. So why does management seem to emphasize this more than the technicians who serve the customers directly?

It could be due to a number of factors:

→ Burden of work outweighing ability to be proactive

→ Difficult or severe incidents to resolve outweighing smaller requests

→ Lack of visibility in real-time to network connectivity or other issues

→ Morale due to talent shortages or high expectations

Outsourcing

Nearly three of four respondents said they outsource some network related tasks or functions, the same number as outsourced in 2023.

While there's been no change in the number of IT professionals reporting some outsourcing, there have been changes to how many activities are outsourced:

2023		**2024**
25%	△ 10% →	35%

Mapping

32%	△ 10% →	42%

Troubleshooting

35%	△ 9% →	44%

Configuration
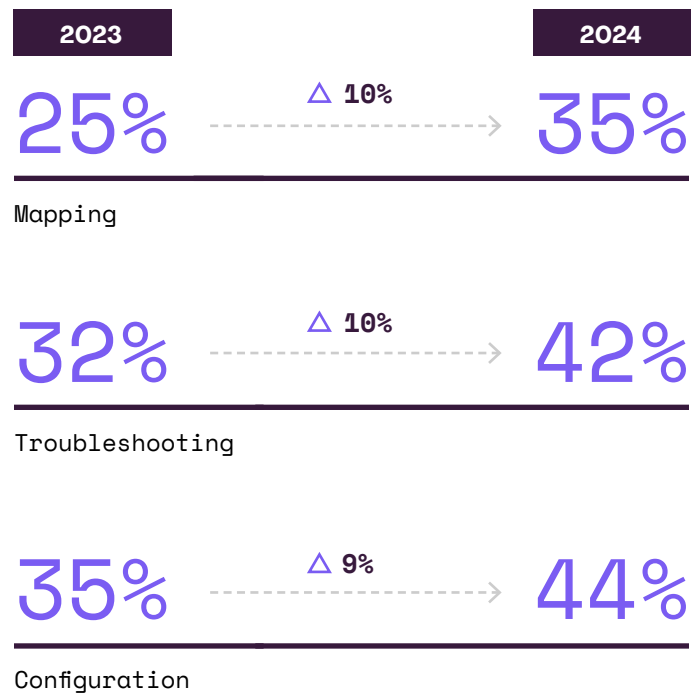
Utilities (87%), financial services (80%), and healthcare (80%) were most likely to outsource tasks.

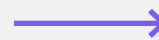| 87%	80%	80%
Utilities ITs that outsource network tasks	Financial services ITs that outsource network tasks	Healthcare ITs that outsource network tasks

But has the amount of work or the daily requirements of the job changed in the last year?

Signs point to "yes" but we'll discuss in part III of the report.

⟶

44%
Configuration

+42%
Configuration backup

+41%
Troubleshooting & Wi-Fi management

Configuration is the top (44%) outsourced activity, followed by configuration backup (42%), troubleshooting (41%) and Wi-Fi management (41%). Only 1% of IT professionals outsource all IT functions.

IT professionals in government are the least likely to outsource (only 50% of these IT professionals do outsource)—with the tasks they outsource most often being:

62%
Documentation

56%
Configuration

49%
Wi-Fi management & SaaS/cloud monitoring

2023 vs 2024 data:
There's been no change in the amount of outsourcing for SaaS/cloud monitoring tasks either (40% in 2023 and 2024), even though SaaS management as an activity has increased by 4%. As we hinted at earlier in this section, workloads and expectations are rising despite the struggle to search for talent to fill the gaps.

Outsourced network tasks or functions

Task	%
Configuration	44%
Configuration backup	42%
Monitoring	41%
Troubleshooting	41%
Wi-Fi management	41%
SaaS / cloud monitoring	40%
Mapping	35%
Documentation	35%
Planning	35%
Reporting	34%
Network automation	32%
UEM (Unified endpoint management)	30%
Other (please specify)	<1%

Auvik

03

Auvik
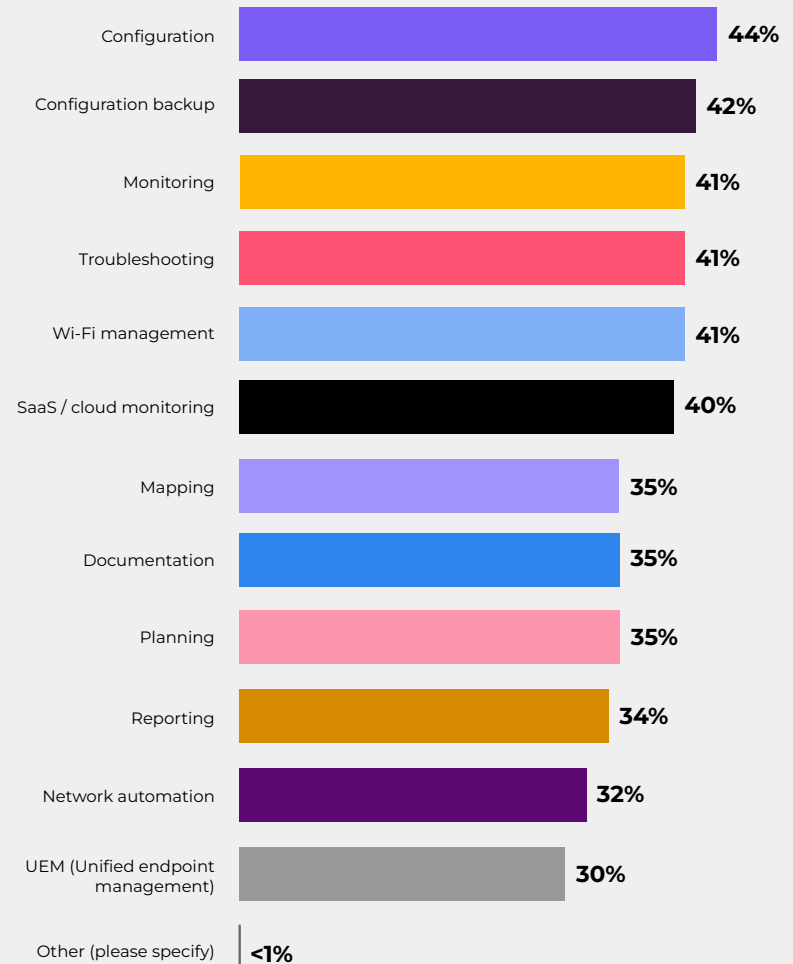
Today's Challenges

IT professionals' top three priorities for their 2024 roadmap include cloud security, network security and cloud management. One in four respondents listed shadow IT visibility as a high priority for 2024, while 28% listed SaaS management as a high priority for 2024. Network management is a top priority for

15% of those surveyed. C-suite respondents were most likely to list hiring as a top three priority for 2024, perhaps suggesting this need for additional talent has not yet been communicated throughout their organizations.
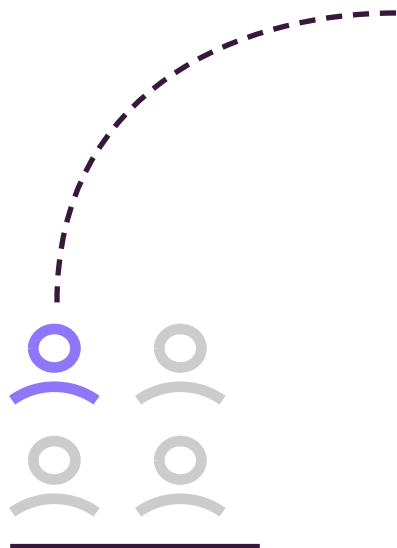
1 in 4 listed shadow IT visibility as a high priority for 2024.

Priority	Already have a solution	Not on 2024 roadmap	May make the 2024 roadmap	High priority on 2024 roadmap	Top 3 priorities on 2024 roadmap
Shadow IT visibility	22%	14%	29%	26%	9%
SaaS management	19%	13%	24%	28%	15%
Cloud management	20%	12%	22%	30%	16%
Cloud security	21%	11%	20%	28%	20%
Endpoint remote management	19%	12%	23%	30%	16%
Endpoint security patching	20%	12%	23%	30%	14%
Network security	24%	12%	19%	26%	19%
Network management	24%	11%	19%	30%	15%
Hiring / acquiring specialists	21%	15%	23%	28%	14%

Wishlist items

Researching new technology was at the top of the list (43%) of network-related activities IT professionals would like to be doing but aren't. Other items on their wish lists include security/cybersecurity (41%), programming and automation (39%), and training/continuous learning (37%).

43%
Network-related actvitites

41%
Security/ cybersecurity

39%
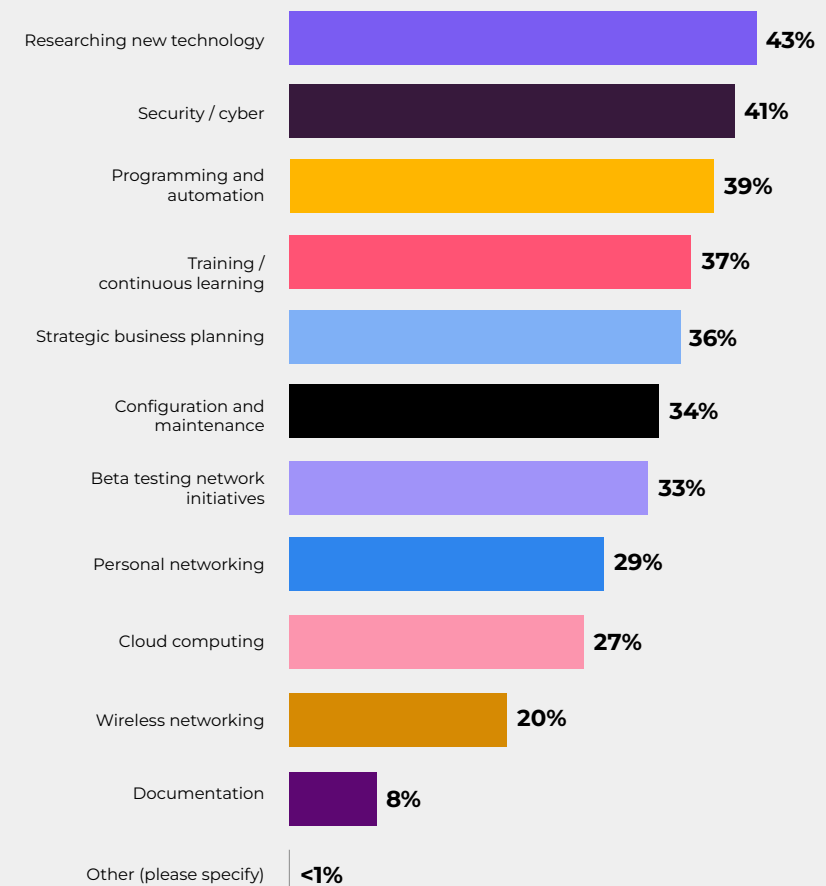Programming & automation

37%
Training/ continuous learning

If there is a takeaway from these wish list items, it's that skilled professionals continue to be hard to find, and those already hired don't have time to be researching new technology or upskilling themselves because their plates are full! What might bring a balance—and also improve the chances these employees would have more time in their days—is automation.

2023 vs 2024 data:
Researching new technology remains in high interest year over year (42%). But it's significant to note that there's been an 11% increase in interest for programming and automation, from 29% in 2023 to 40% today.

Network-related activities IT pros would like to be doing but aren't

Activity	Percentage
Researching new technology	43%
Security / cyber	41%
Programming and automation	39%
Training / continuous learning	37%
Strategic business planning	36%
Configuration and maintenance	34%
Beta testing network initiatives	33%
Personal networking	29%
Cloud computing	27%
Wireless networking	20%
Documentation	8%
Other (please specify)	<1%

What's keeping IT pros from fulfilling their wishlist?

Lack of time, as predicted, is the most cited reason IT professionals can't get to their wish lists (43%).
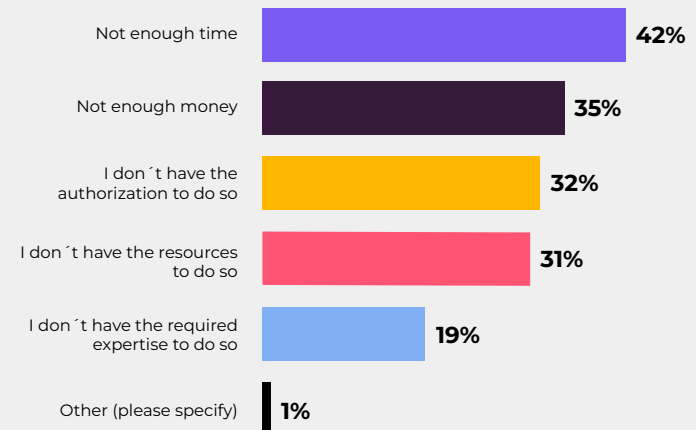
43%

Lack of time

However, about one in three respondents also cited cost, authorization and lack of resources as reasons. Some industries are experiencing a swap between lack of time and cost (lack of money) as the biggest blockers, noted here:

→ Transportation, leisure and hospitality

→ Financial services

→ Healthcare

→ Utilities/energy

2023 vs 2024 data:
For most respondents, time continues to be the biggest obstacle when it comes to aspirational activities (42%). But cost is an increasing barrier, with 35% citing not enough money as something that prevents implementing these activities, a 10% increase since 2023. More IT professionals also see authorization as a growing barrier, with 32% citing they don't have the proper authorization (versus 25% in 2023).

Top barriers to wishlist

Barrier	%
Not enough time	42%
Not enough money	35%
I don´t have the authorization to do so	32%
I don´t have the resources to do so	31%
I don´t have the required expertise to do so	19%
Other (please specify)	1%

Top challenges for the IT industry in 2024

The obstacle voted to be a top challenge of 2024 is the shortage of skilled professionals (49%).

49%
face a shortage of skilled professionals

56%
of mid-sized companies face staffing challenges

Governments are feeling budget and **staffing challenges** more strongly than other industries, with 71% of employees in those departments listing both as challenges they're facing in 2024.
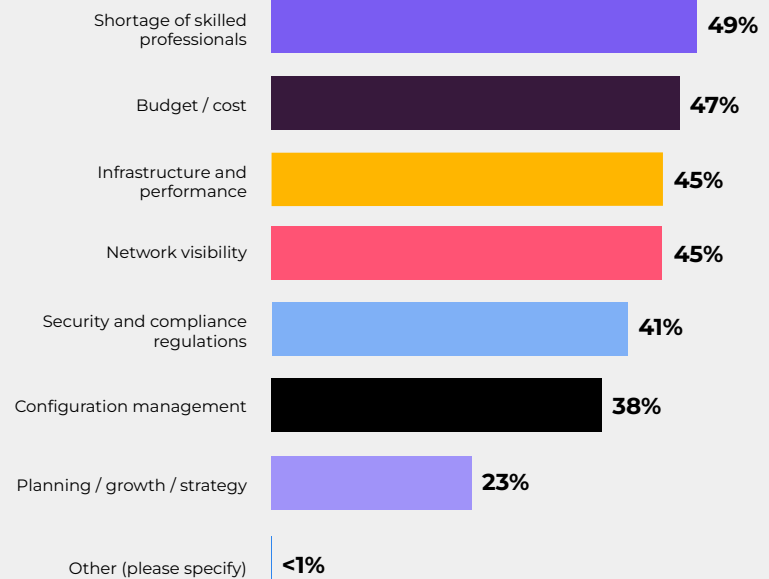
Security and compliance is the biggest challenge faced by IT professionals in financial services, with 53% listing it as a challenge.

Companies with 251 to 500 employees are those most likely to face staffing challenges (56%).

2023 vs 2024 data:
Budget was the top challenge in 2023, but staffing has surpassed it in 2024. We see an 11% increase in ITs experiencing configuration management challenges, rising to 38% in 2024. There's also been a 10% increase in ITs experiencing Infrastructure and performance challenges this year (27% to 38%).

Top challenges for IT departments

Challenge	Percentage
Shortage of skilled professionals	49%
Budget / cost	47%
Infrastructure and performance	45%
Network visibility	45%
Security and compliance regulations	41%
Configuration management	38%
Planning / growth / strategy	23%
Other (please specify)	<1%

⚠ **CAUTION**
There was a correlation between seniority of role and concern over security and compliance, including configuration management. This suggests that employees with boots on the ground may be struggling to prioritize security practices and compliance tasks when faced with understaffed departments and tight budgets.

Could automation, especially the automating of configuration backups (both a compliance concern and a configuration management item) be part of a solution?
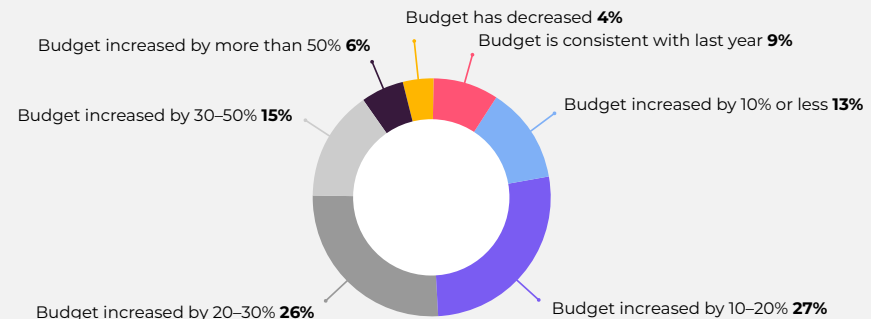
Time is money, and budget is key

The majority (86%) of respondents reported increased budgets in 2024. Nearly 50% said they'll see an increase of at least 20% from 2023, and almost 75% said they'll receive 10% or more beyond last year. Larger firms (1000+ employees) are driving this increase, with smaller firms more likely to have stable or shrinking budgets.

Only 4% of respondents are seeing budget decreases, which are happening more at smaller organizations, with 13% of one to 50 employee MSPs reporting decreases and 14% of one to 250 employee internal IT teams reporting decreases.

Utilities and the energy industry are seeing some of the biggest budget increases, with 44% reporting their budget will improve 30 to 50% in 2024.

YoY budget changes

Budget has decreased **4%**
Budget is consistent with last year **9%**
Budget increased by more than 50% **6%**
Budget increased by 10% or less **13%**
Budget increased by 30–50% **15%**
Budget increased by 20–30% **26%**
Budget increased by 10–20% **27%**

An incredible 98% of respondents are making more investments in 2024. When it comes to what they're planning to do, IT professionals are relatively split on priorities. The top planned investments for 2024 are SaaS monitoring and management (48%), Wi-Fi management (46%), and cloud monitoring and management (46%).

48%
plan to invest in SaaS monitoring

46%
plan to invest in Wi-Fi management

46%
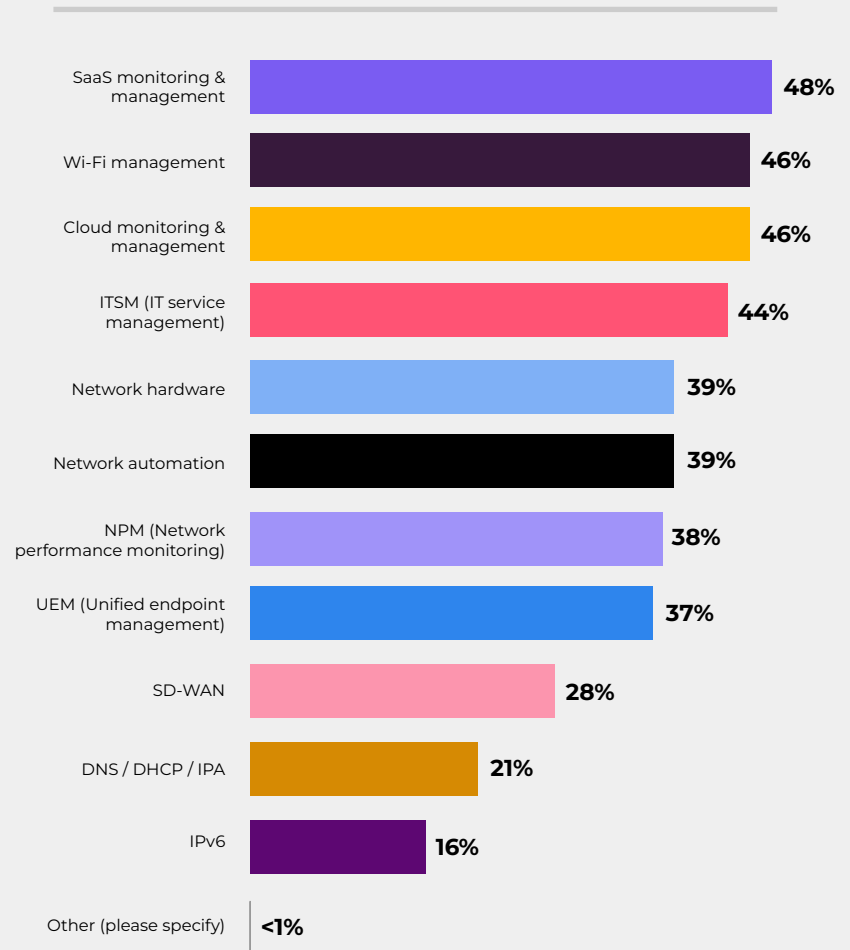plan to invest in cloud monitoring and management

Financial services show the most interest in SaaS monitoring and management, with 56% of their IT professionals saying they have plans to invest in that area in 2024. More than half (53%) of government respondents report planned investments for NPM (network performance monitoring) in 2024. ITs at small companies (one to 250 employees) are five times more likely to not have any planned investments than the average IT.

2023 vs 2024 data:

The number of respondents with planned investments has grown in every area surveyed since 2023. Network automation has seen the biggest growth, which is aligned with the needs we're discussing in this report. Compared to 2023, 24% more IT professionals are reporting planned investments in this area.

The slowest growth is in the unified endpoint management area (only a 4% increase between 2023 and 2024). Later in the report we'll look at how the respondents indicated they were planning to implement these trends.

Planned investments over the next 12 months

Category	Percentage
SaaS monitoring & management	48%
Wi-Fi management	46%
Cloud monitoring & management	46%
ITSM (IT service management)	44%
Network hardware	39%
Network automation	39%
NPM (Network performance monitoring)	38%
UEM (Unified endpoint management)	37%
SD-WAN	28%
DNS / DHCP / IPA	21%
IPv6	16%
Other (please specify)	<1%

04

Section 4

Trends for Technology

Automation

When looking at what IT professionals are currently automating, 71% of respondents described network and SaaS tasks as "mostly" or "completely automated." These same tasks in the energy, government, and education industries are even more likely to be automated (89%, 86%, and 79%).

On average, these network and SaaS tasks are completely or mostly manual 29% of the time. Network documentation is the most likely to be completely manual (11%), which is a department with room for more automation to assist with compliance. We see an increase in "completely automated" responses in every category as company size grows. But this peaks at the 1001 to 5000 company size, with 5000+ company size reporting fewer completely automated tasks.

Task	Completely manual	Mostly manual	Mostly automated	Completely automated
Network documentation	11%	21%	42%	26%
Network infrastructure mapping	7%	22%	42%	29%
Network device configuration backup	8%	18%	40%	34%
Configuration pre-change validation	8%	21%	40%	31%
Configuration post-change remediation	7%	21%	40%	32%
Workstation remediation	7%	22%	42%	29%
SaaS application inventory management	6%	20%	43%	32%
SaaS account inventory management (User account access inventory)	8%	22%	41%	30%
Employee onboard lifecycle of SaaS tools	9%	23%	38%	30%
Employee off-boarding lifecycle of SaaS tools	8%	24%	40%	28%
SaaS license expense management (removal of unused licenses, etc.)	8%	20%	41%	31%

AI and machine learning models

Almost all (96%) of IT professionals are using some kind of AI/machine learning tool.

Top tools include:

47%
Whale Cloud

44%
NetBrain

44%
AISWare
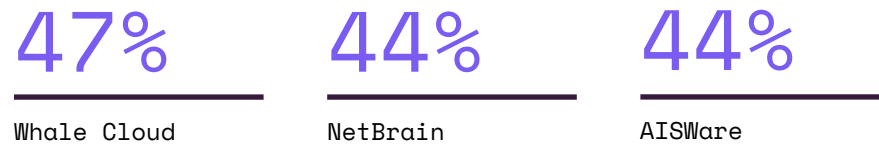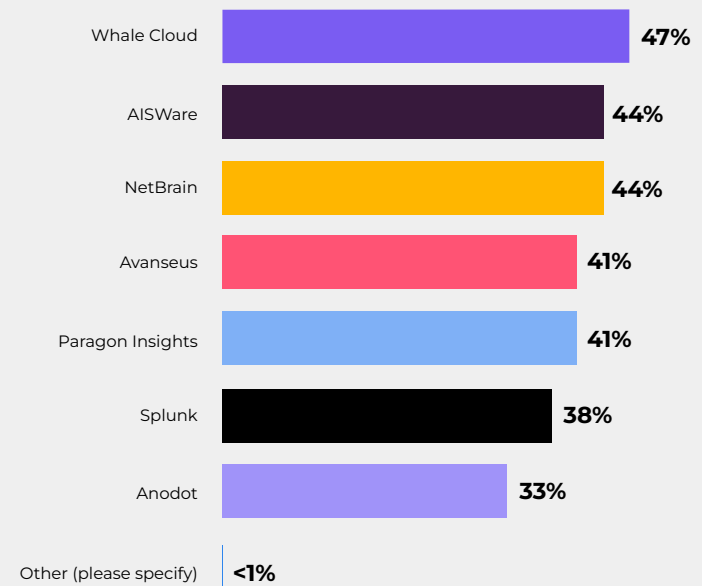
In comparison, only 74% of small MSPs (one to 50 employees) and 85% of small internal IT teams (at one to 250 employee companies) are using AI/machine learning tools.

While adoption of AI/machine learning tools increases with seniority, smaller companies are less likely than their larger peers to have fully implemented an AI tool.

Top AI or machine learning applications

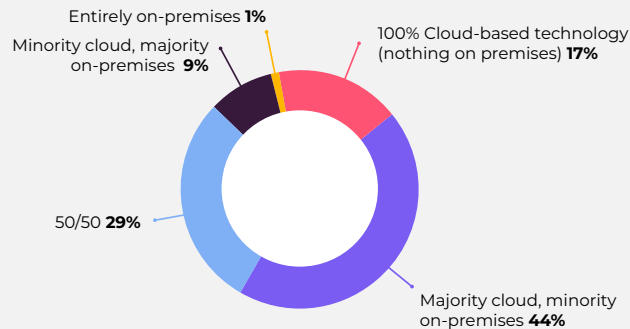| Application	Percentage
Whale Cloud	47%
AISWare	44%
NetBrain	44%
Avanseus	41%
Paragon Insights	41%
Splunk	38%
Anodot	33%
Other (please specify)	<1%

On-premises or cloud-based

Many IT professionals estimate at least a 50/50 split of cloud-based and on-prem infrastructure, and 17% work with entirely cloud-based infrastructure.

Healthcare IT professionals are more likely to have most or all on-premises infrastructure (15%). Business services are the most likely to be entirely on-premise, but this is still only 4%.

Companies with 501 to 1000 employees were the most likely to have 100% cloud based infrastructure (21%). Organizations of one to 250 employees are most likely to have 100% on-prem infrastructure (14%).

Amount of cloud infrastructure organizations currently have in place

Entirely on-premises **1%**

Minority cloud, majority on-premises **9%**

100% Cloud-based technology (nothing on premises) **17%**

50/50 **29%**

Majority cloud, minority on-premises **44%**
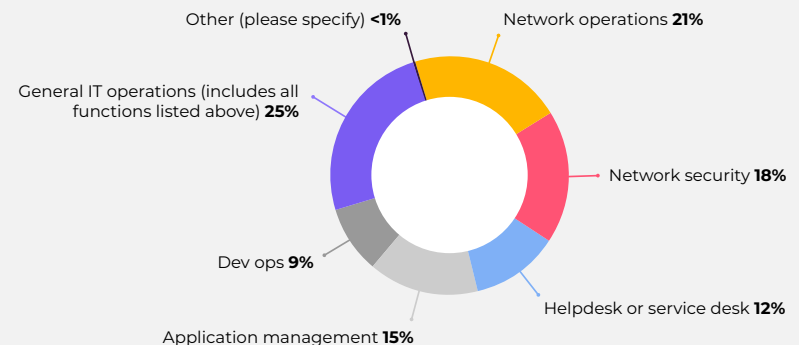
SaaS is up for grabs

Who is responsible for monitoring and managing the IT of end-users?

One in four respondents say general IT operations, while about one in five say network operations, 18% say network security.

The majority of IT professionals are reporting either limited or zero visibility on all SaaS and web applications we asked about. This may be a smaller issue for government organizations, where the majority report automated logging for all of the above.
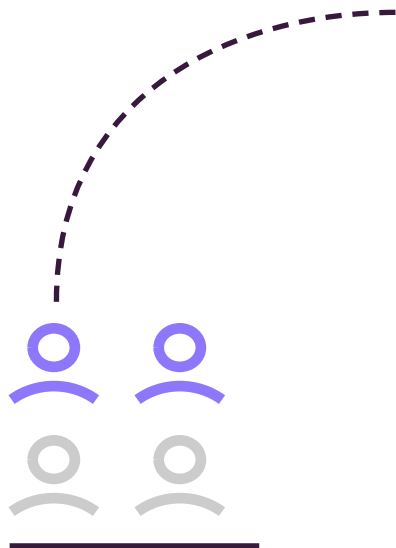
Healthcare appears to have the least amount of visibility into employee sharing accounts, with 27% of IT professionals in this industry reporting zero visibility into how or when employees share accounts—that could be risky!

Roles responsible for supporting end-users, their workstations, and SaaS applications

Other (please specify) **<1%**

General IT operations (includes all functions listed above) **25%**

Network operations **21%**

Network security **18%**

Dev ops **9%**

Helpdesk or service desk **12%**
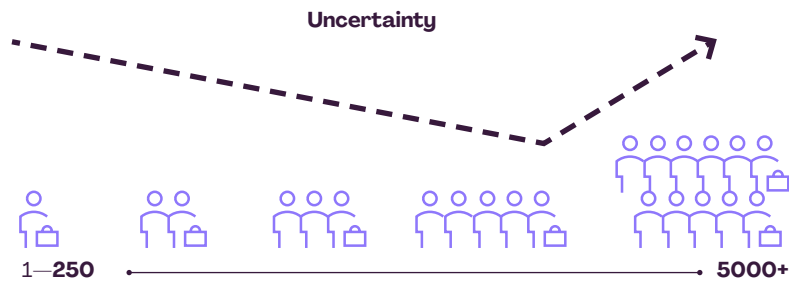
Application management **15%**

Organizations use a high number of SaaS applications, with nearly three in five using over 50 applications. It's also worth noting that the number of SaaS apps only increases with the size of the organization.
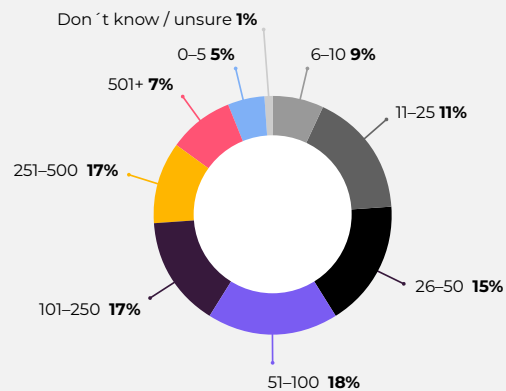
	Zero visibility	Limited visibility	Automated logging
Shadow IT application adoption	13%	52%	35%
Account access logs to all SaaS applications	14%	39%	47%
Employees sharing accounts on SaaS applications	15%	41%	45%
Employees leveraging service accounts (support@, hr@, marketing@, etc.) on SaaS applications	13%	44%	43%
SSO usage in SaaS applications	13%	45%	43%
MFA usage in SaaS applications	10%	43%	46%

52% have limited visibility into shadow IT adoption

Smaller organizations (one to 250 employees) are five times more likely to say they're unsure or don't know how many SaaS applications their teams use. While this uncertainty declines as organization size grows, it spikes again for 5000+ employees, with 3% unsure about the number of SaaS apps.

Uncertainty

1—**250**   **5000+**

Number of SaaS applications used

Don´t know / unsure **1%**
0–5 **5%**
6–10 **9%**
11–25 **11%**
26–50 **15%**
51–100 **18%**
101–250 **17%**
251–500 **17%**
501+ **7%**

⚠ **CAUTION**

While government appears to have some of the highest numbers for SaaS apps used (49% say there are 251 to 500 apps in use by their teams), we also noticed that:

48%

of government respondents have as low as zero visibility on MFA usage

46%

report near zero visibility on employees sharing accounts within apps

46%

said they have limited or zero visibility on SSO for those apps

Security and compliance and the network

We have already seen how security and compliance are potentially taking hits due to understaffing, but what kind of activities does this impact? Top tasks for regulatory compliance include:
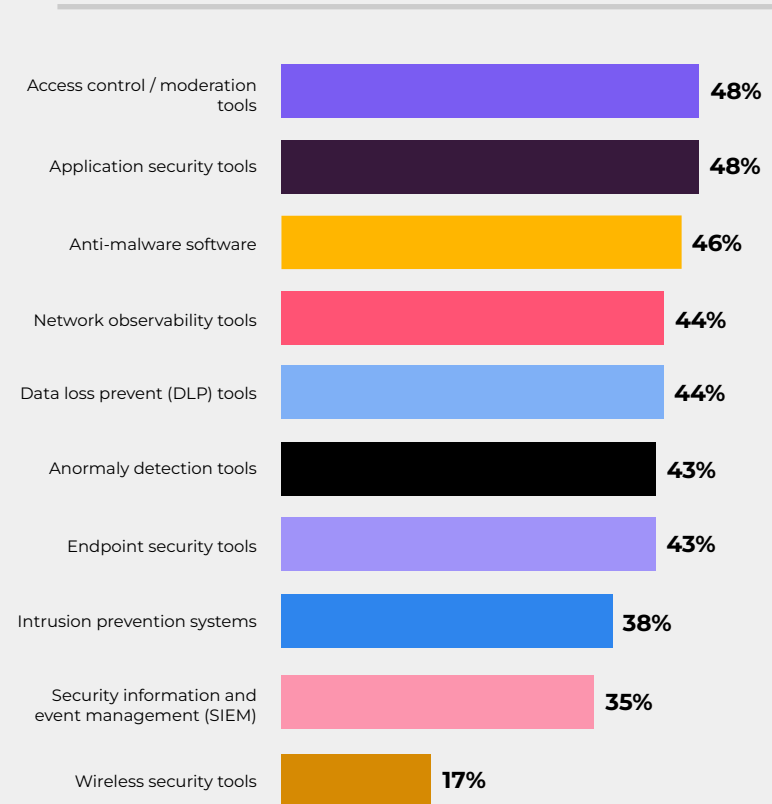
Hardware documentation

60%

Network infrastructure mapping

69%

Software inventory

76%
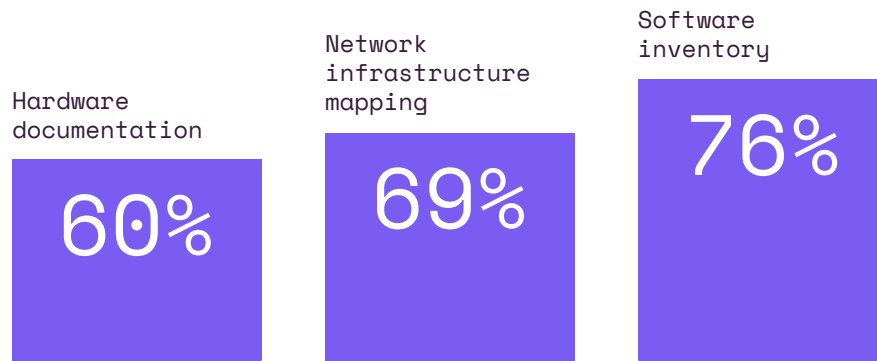
The most common task performed for regulatory compliance is "software inventory" (76%) with government, energy, and media industries also more likely to perform "backups" for compliance. In terms of tools, almost half of all respondents are using or considering using access control or moderation tools. Application security tools were the second item that most respondents showed interest in, with 48% saying they use one or will implement one soon. Network observability tools also ranked high in this category with 44% already looking into them for assistance with security.

Interestingly enough, many of the tasks on this list of top security practices can be very easily automated.

With a solution in place like a network management tool, or even outsourcing some of the systems maintenance to an MSP, organizations can take some of their IT teams' valuable time back for them!

Network Ops Security currently in use or in consideration for use in next 12 months

Tool	Percentage
Access control / moderation tools	48%
Application security tools	48%
Anti-malware software	46%
Network observability tools	44%
Data loss prevent (DLP) tools	44%
Anormaly detection tools	43%
Endpoint security tools	43%
Intrusion prevention systems	38%
Security information and event management (SIEM)	35%
Wireless security tools	17%

05

Section 5

Conclusion

Now that you've read the data, what is there to do about it?

First, we recommend looking into an automation plan for some of the manual backup tasks and documentation, especially if your organization is feeling the pain of difficulty hiring skilled talent.

Automating maintenance and compliance tasks are usually the easiest to start with.

There are quite a few high-quality solutions that can help with this—and we're one of them!

If you can't hire a specialist for your network roles, or you need an extra technician or help desk body right away—i.e. you can't wait for planning technology and painful implementation—why not consider using a managed service provider to bridge the gap?

Many MSPs are even starting to specialize in security-as-a-service—very helpful if this is a key area for your organization. Auvik supports a large number of MSPs, who are often early adopters of the kind of automation practices and other new technologies sought after by growing companies.

Don't make your own internal IT or managed services team continue to feel the burden of reactive ticket resolution.

It can quickly gobble up time they want to spend advancing company initiatives in technology. Hire where you can and outsource or automate where you can't. Consider checking in with the service desk to get the boots-on-the-ground perspective, which can help you figure out what solutions will increase a technician's productivity and job satisfaction. After all, they're the ones making sure you're able to keep your organization running strong.

16%

of internal IT departments spend 20+ hours a week resolving end-user requests.

☾+

Staffing surpassed budget as the top challenge in 2024.

2X

C-suite executives are nearly 2x as confident as IT technicians in the effectiveness of their network tools for supporting a remote or hybrid workforce.

About Auvik

A cloud-based IT management platform, Auvik helps IT departments proactively manage their networks, endpoints, and SaaS applications.

Auvik manages one million network devices and three million SaaS applications across 100,000 networks, and provides monitoring services for more than 10 million devices.
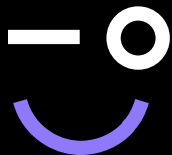
Network Management

SaaS Management

Wi-Fi Management

Across all our products, the key is absolute simplicity.

· Seamless deployment

· Intuitive interface

· Effortless automation

The result is less friction for IT departments, so that everyone can work **however** and **wherever** they want.

Visit auvik.com to start your free 14-day trial today.

97%

of survey respondents who use Auvik are happy with their choice.

67%

say they are very satisfied.