

**FUTURE FOCUS 2026**

**Advice, insight, and  
trends for modern  
B2B IT leaders**

**ITPro.**

FUTURE  
**B2B**





# Contents

---

- 3 Welcome to Future Focus 2026
- 4 Tech priorities
- 9 The top five focus areas for ITDMs in 2026
- 16 How decisions are made and tech deployed
- 21 The secrets of our success: How vendors and ITDMs can work together in 2026
- 25 Historic hurdles and future focus
- 30 The software hype train is leaving the station, but it's running on old tracks
- 33 AI is dominating IT priorities in 2026, whether it's through the prism of security or software

# Welcome to Future Focus 2026

**Gain a better understanding of the IT landscape to drive increased business value**

Welcome to the 2026 edition of *ITPro's* annual Future Focus report.

As in previous years, we've spoken to hundreds of IT decision makers (ITDMs) to identify the key challenges, opportunities, and trends facing them in the year ahead.

We also asked them about historic problems and investment decisions to help build a full picture of what has changed, why, and when. It definitely makes for very interesting reading.

While some of the results cover familiar ground, they also offer new ways to look at old problems.

It will come as no surprise that AI continues to dominate conversations and actions, much as it did in 2025.

What's new for 2026, though, is an increased appetite for investment in this area. This indicates a big shift from just talking about AI to actually implementing it and delivering not just on expectations, but driving real business value. The latter represents a desire to ensure success and prove wrong the industry soothsayers who predict high AI project failure rates.

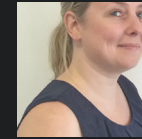
Other technologies that feature highly are automation, security (both cyber and general), and software. We delve deeper into all of these areas in the report, combining real-world insight with key takeaways for the modern ITDM.

The report also features real-world examples direct from the mouths of our research respondents, offering a peek under the hood for fellow ITDMs to help set them up for success.

We hope you find this report informative and filled with actionable insights to help you make informed decisions that drive business value both now and in the future.

— **Maggie Holland**, Global Content Director, B2B IT

## CONTENT



### EDITOR

Maggie Holland, Global  
Content Director B2B

Maggie has been a journalist for more than 20 years. She covers a range of subjects, with a particular interest in AI, cloud, management, and C-level issues, the business value of technology, green and environmental issues, and careers to name but a few. Maggie is also a keen follower of the IT channel and the role the partner ecosystem can play in setting businesses up for success.

### SUB EDITORS

Jane McCallion  
Rory Bathgate

### CONTRIBUTORS

Keumars Afifi-Sabet  
Rory Bathgate  
Bobby Hellard  
Ross Kelly  
Rene Millman

### GLOBAL VP OF CONTENT

Carmel King

### MARKETING MANAGER

Remy Le Mentec

---

## COMMERCIAL

### GLOBAL VP OF SALES, B2B

Dena Malouf

# Tech priorities



Although AI is a key focus for ITDMs in 2026, security is also front-of-mind, particularly in the wake of noteworthy cyber campaigns

Today's businesses face a dual dilemma in the IT department: finding the money for cutting-edge projects and new technology, while also investing in critical areas to keep the organization ticking over.

Every leader knows this type of balancing act is very difficult. Making the most of opportunities such as AI investments can come at the expense of much-needed cybersecurity refreshes and vice versa.

As 2026 begins, we take a look at the areas ITDMs will be most focused on for investment this year and find out what's driving this focus.

## AI CONTINUES TO DOMINATE

Predictably, AI continues to be a major focus for enterprises in the coming year. Over half of respondents (51%) stated AI will get the largest amount of investment and attention in 2026, which is in line with their 2025 priorities (52%).

**“One AI use case my organization has explored is using automation within accounting software to streamline financial processes. This reduced manual data entry errors and saved time during payroll and monthly reconciliations.”**

– FUTURE FOCUS 2026 SURVEY RESPONDENT

What has changed is the actual amount business leaders are willing to set aside for the technology, which has significantly increased.

Almost a quarter of respondents (23%) plan to invest between a third and two-fifths of their IT budget into AI projects in 2026. This is an increase of 52% year-over-year compared to the volume willing to dedicate the same amount towards AI investment in 2025 (15%).

The number of respondents saying they would invest 30% or less of their IT budget in AI, by contrast, has decreased significantly. The number of respondents indicating they will be investing 10% or less of their budget in the technology has fallen from 19% to 12% – a drop of 39% year-over-year.

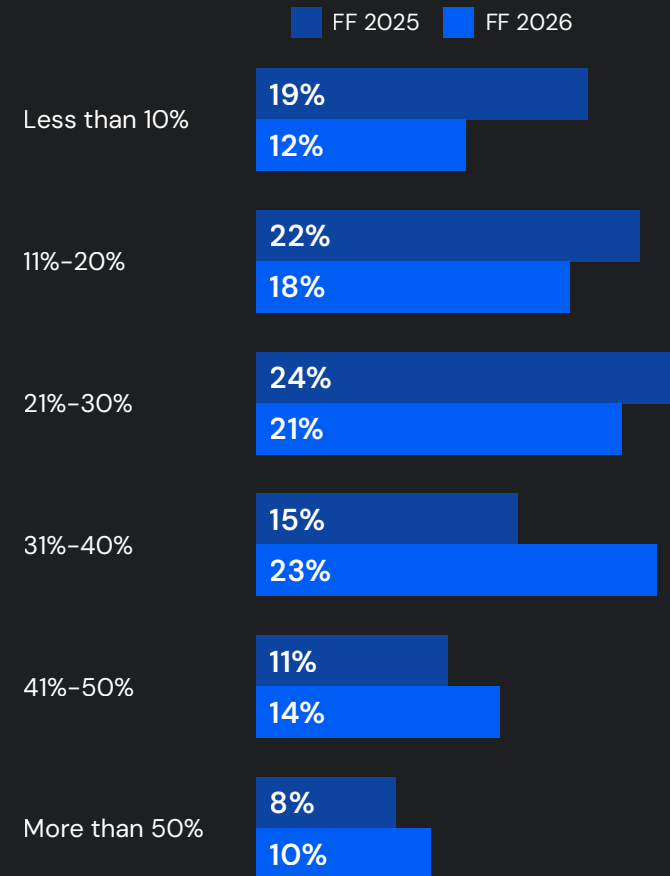
Businesses are benefiting from a wide range of AI deployments, helping them to automate tasks across numerous business functions, including customer support, filling in finance forms, and predictive analytics.

“One AI use case my organization has explored is using automation within accounting software to streamline financial processes,” said one respondent. “This reduced manual data entry errors and saved time during payroll and monthly reconciliations.”

It’s clear that concerns over AI ROI remain and there’s unease across the industry over the percentage of AI projects that will succeed or fail. [Recent MIT research](#) found 95% of enterprise AI solutions fail and [Gartner projects](#) a cancellation rate of over 40% for enterprise agentic AI projects by the end of 2027.

Haider Pasha, EMEA CISO at Palo Alto Networks, [recently told ITPro](#) that AI failure rates will likely continue to be high. He explained this was largely due to a lack of governance and security planning alongside hype around AI adoption.

## How much of your overall IT budget will be spent on AI?



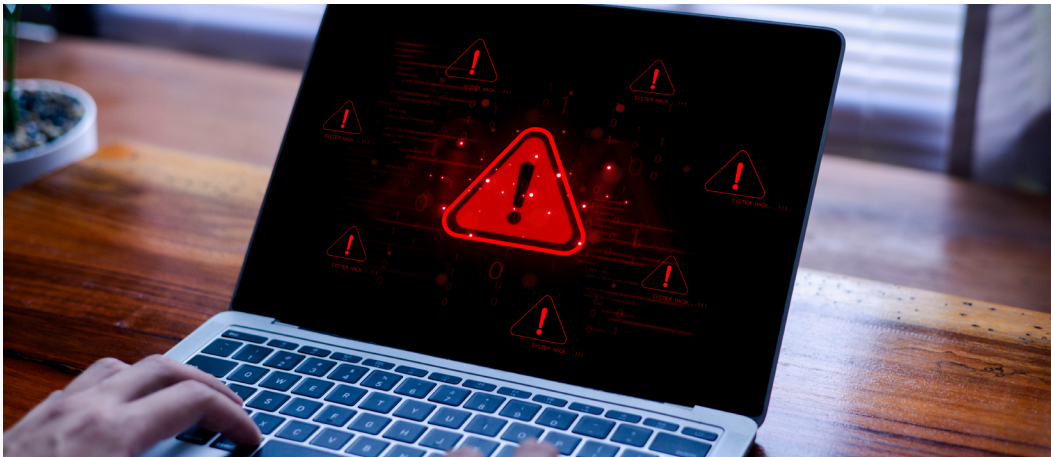
## SECURITY PREPAREDNESS IS A RISING PRIORITY

ITDMs aren't focusing on AI at the expense of all else, however. Cybersecurity is an area of particular concern in 2026, with nearly two-thirds of respondents (62%) indicating it will be more important to their business in 2026 than it was in 2025.

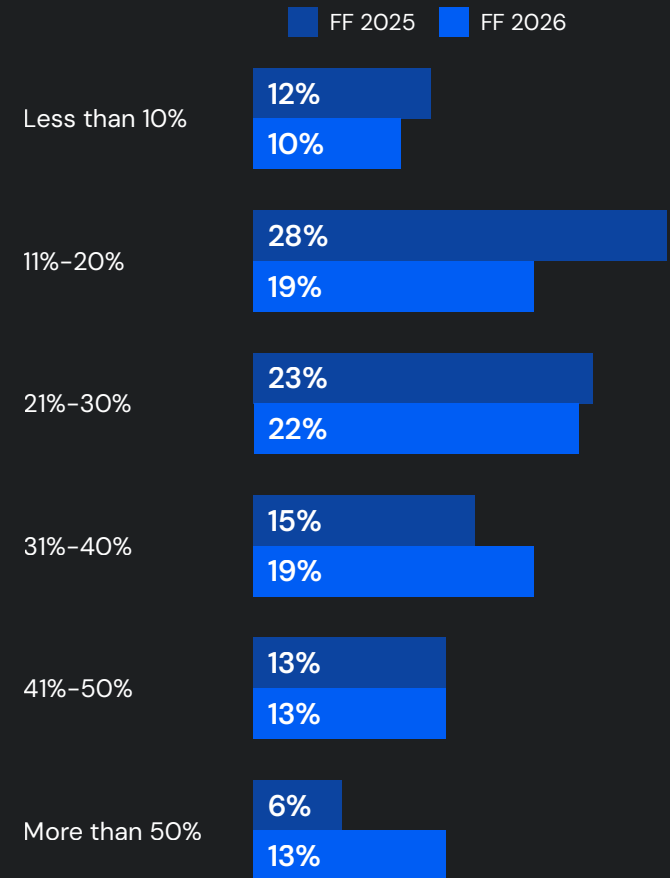
This is likely a reaction to an increase in high-profile cyber attacks and surging ransomware campaigns throughout 2025 – particularly against European enterprises. Ransomware attacks now come with an average recovery cost of \$4.5 million and cause untold damage further down the IT supply chain.

Specific incidents throughout 2025 have helped illustrate the potentially catastrophic impact of cyber attacks on a business' bottom line.

For example, the attack on Jaguar Land Rover (JLR) that began in August 2025 eventually became the most costly cyber attack in UK history, with impact estimates ranging between £1.6 and £2.1 billion (\$2.14 to \$2.81 billion).



### How much of your overall IT budget will be spent on security?



In total, more than 5,000 businesses in JLR's supply chain were affected, and the attack was even large enough to have a direct impact on the UK economy.

IT leaders aren't just fretting about the issue, however. They're also putting cold, hard cash into trying to mitigate risks.

Over a tenth of respondents (13%) said they would spend more than 50% of their IT budget on security in 2026, while the same proportion said they would be spending 41%–50%.

At the other end of the scale, 10% said they would spend less than 10% of their budget on security.

## CLOUD IS THE QUIET IMPERATIVE

Amid all the AI hype and shifting security priorities, business interest in cloud remains stable, and organizational investment is on the rise.

Some 45% of respondents said they would be spending upward of 31% of their IT budget on cloud computing, while only 13% said they would be spending less than 10%. This is a significant reversal of last year's Future Focus findings, when 71% of respondents said they planned to invest 30% or less of their budget in cloud.

In its 2025 EMEA Cloud Business Survey, PwC reported that 94% of organizations are set to expand cloud architecture in 2026. Meanwhile, 82% of organizations are shifting their approach to the cloud in response to regulatory and geopolitical changes.

Drives toward sovereign cloud form no small part of this, with region-specific data storage and processing increasingly seen as a minimum requirement for businesses. Managed environments, such as private cloud, form an integral part of sovereign cloud services alongside regional public cloud instances.

A recent Gartner study projected over 75% of enterprises outside the US will have a digital sovereignty strategy by 2030, with 61% of ITDMs in Western Europe set to increase their organization's use of local cloud providers.



# £2.1 billion

The estimated impact of the UK's most costly cyber attack, suffered by JLR in 2025

In 2025 alone, major players in the cloud, including [AWS](#), [Google Cloud](#), [Microsoft](#), and [Nutanix](#), doubled down on sovereign cloud offerings for customers in the UK and Europe. Local providers are also making hay from the trend: [BT, for example, has rolled out UK-specific cloud and AI services.](#)

Throughout 2026, businesses are targeting investments to meet regulatory and security demands. It's clear ITDMs are focused this year on segments that can offer direct productivity improvements or greater shielding from cyber and regulatory risks.



### WHAT DOES IT MEAN FOR ITDMs?

Where companies' data is held is becoming an increasingly important question, both from a regulatory perspective and a cybersecurity one. Understanding how data is processed by AI is of the utmost importance in avoiding sensitive data leaks, so any investment in cloud, AI, or cybersecurity should take this into account.

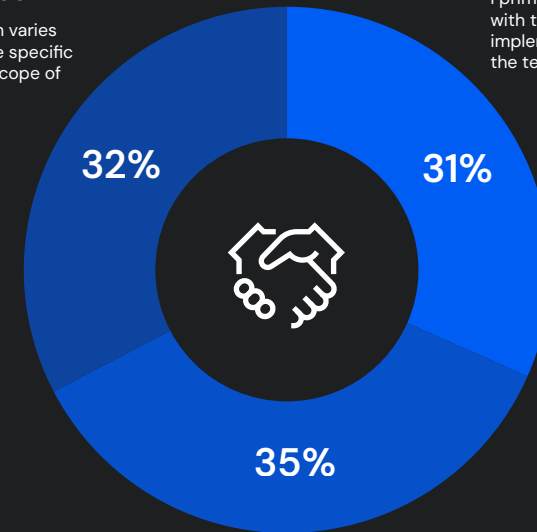
## Please describe your typical approach when initiating a technology project

### Depends on the project

My approach varies based on the specific nature and scope of the project.

### Direct vendor collaboration

I primarily work directly with the vendor to implement and manage the technology.



### Engagement through a partner

I prefer to engage with the vendor through a trusted partner or intermediary.

# The top five focus areas for ITDMs in 2026

Experts weigh in on the five most important topics businesses need to consider over the next 12 months



As part of *ITPro's* Future Focus 2026 research, we identified five key areas that ITDMs will prioritize in the next 12 months, whether through investment or operational initiatives.

Here's why they're so important and what the experts have to say about their significance in 2026.

## 1. AI

**AI remains the most prominent area in tech at present. While it made several leaps forward in 2025, attention now turns to realizing the benefits of pilots and finding ways for the technology to make a meaningful difference to operations.**

It's a pivotal moment in the wider enterprise; with data playing far more of a role across different divisions, businesses now have a chance to find new competitive advantages that haven't been seen before.

"The entire sector environment depicts a struggle to balance the increasing benefits of AI-enabled productivity with the rapidly escalating issues associated with governance, origin, and autonomy risks," Joshua Copeland, adjunct professor at Tulane University, tells *ITPro*.

## Top 5 Areas of Investment in 2026

1

AI

2

Cybersecurity

3

Software

4

Security (physical/general)

5

Automation

“The fact is now widely recognized that AI has moved beyond a competitive advantage and has evolved into an infrastructural element where each and every strategic move depends upon the effective use of AI.”

In 2026, agentic AI will also become far more integral. Many businesses will seek to operate layers of AI agents – especially in SaaS platforms and other core software – to orchestrate IT workflows and drive a major productivity revolution.



### EXAMPLES OF AI IN ACTION

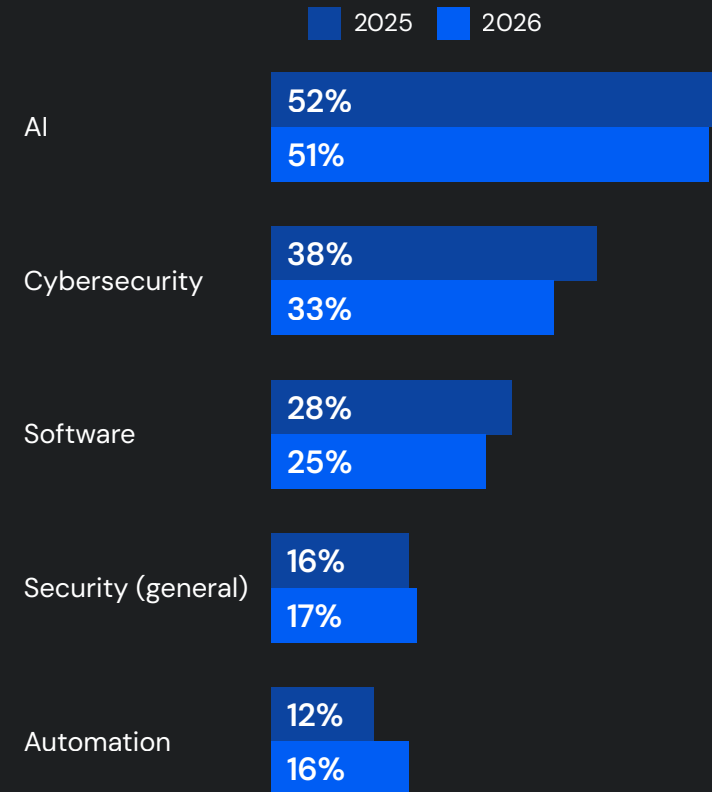
AI agents, chatbots, copilots, and vibe coding tools



### READ MORE ON AI

- [Does the US AI Action Plan add up and how will it change the global AI landscape?](#)
- [How can businesses avoid AI resentment in the workforce?](#)
- [How Dragon Copilot is helping clinicians spend more time with their patients](#)
- [The best AI tools for business to try today](#)

If you compare your 2025 focus to your 2026 plans, which technologies would you say got/will get the largest amount of investment and attention?  
(Please choose the three biggest areas)



## 2. CYBERSECURITY

**Cyber attacks are growing in sophistication and the next year will challenge organizations to continue implementing measures like AI-driven threat detection and zero trust architectures.**

It's not just businesses that are using AI and automation to increase productivity and unlock new opportunities – threat actors are, too. AI is both lowering the barrier to entry for would-be cyber criminals while making those already involved more professionalized and efficient. Businesses will need to reckon with the need to increase the ways they protect themselves, given that talented cybersecurity professionals are still hard to come by and budgets are scarce.

“The next phase of the cyber arms race is on,” says Brian Jackson, principal research director at Info-Tech Research Group. “Cyber criminals are already adopting agentic AI hacking kits that automatically scan for vulnerabilities, burrow their way into victims’ networks, and cement a foothold to extract value. Social engineering is becoming even more deceptive with video and audio deepfakes or AI-personalized emails.”

One of the biggest problems in 2025 was data security and privacy, with businesses this year also focusing more on stronger tools, employee training, and regular system updates. These are critical opportunities, with AI playing a role in new systems like recruitment, fraud detection, and real-time threat detection.



### EXAMPLES OF CYBERSECURITY IN ACTION

Firewalls and antimalware, regular credential reverification, staff training to recognize phishing and deepfakes, and zero trust



### READ MORE ON CYBERSECURITY

- [Could years of AI conversations be your biggest security blind spot?](#)
- [Simulating attacks: how to use tabletop exercises in incident response](#)
- [The most prominent infostealers and how businesses can protect against them](#)
- [Trend Micro issues warning over rise of ‘vibe crime’ as cyber criminals turn to agentic AI to automate attacks](#)
- [Warning issued as surge in OAuth device code phishing leads to M365 account takeovers](#)



### 3. SOFTWARE

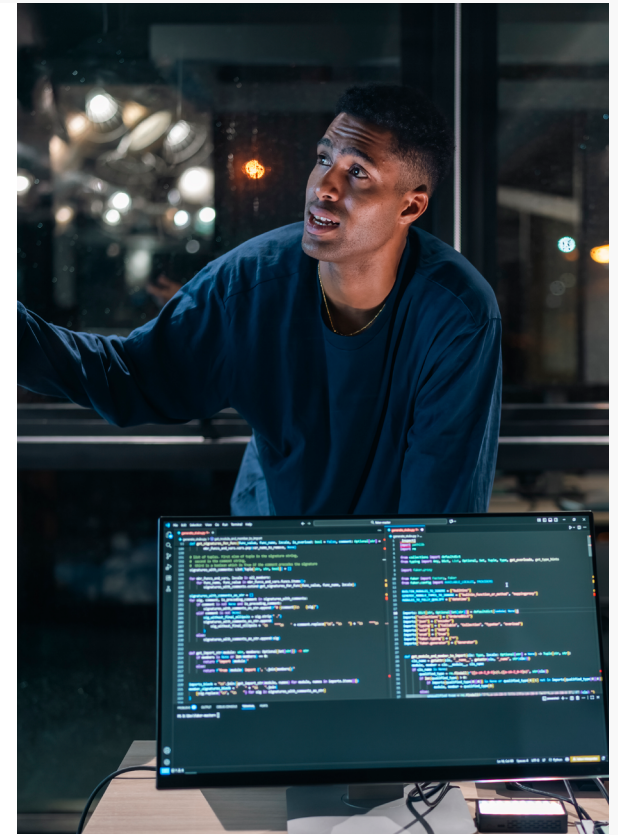
**Managing software platforms in the age of AI and advancing business technologies and frameworks is a major challenge going into 2026. Businesses are still grappling with outdated systems and integrating AI into them will be a major priority.**

Many companies are facing the reality that their existing systems and software stacks simply aren't up to the job when it comes to innovations like AI. *ITPro's Future Focus 2026* research shows that ITDMs are facing a serious challenge in integrating new technologies with the numerous systems already in place.

"Software is getting this renewed attention simply because so many companies hit the wall with older systems that cannot adapt to real-time data or AI-driven workloads," Krishna Kandi, senior software engineer at Convoke and senior IEEE member, tells *ITPro*.

"The infrastructure many businesses are burdened with was never built for flexibility," he says, adding that in the wider industry there's a shift toward smaller components, more observability, and architectures that can evolve "without breaking everything else".

While not glamorous, it will be a foundational aspect of many business strategies. Neglecting older devices and technical debt poses challenges, and mitigating this is essential to growth.



#### EXAMPLES OF SOFTWARE IN ACTION:

Chatbots, collaboration tools, CRM, ERP, local LLMs/SLMs, productivity tools, and SaaS



#### READ MORE ON SOFTWARE

- [AI doesn't mean your developers are obsolete — if anything you're probably going to need bigger teams](#)
- [Applications and the afterlife: how businesses can manage software end of life](#)
- [Clunky tech is costing developers 20 working days a year](#)
- [Software 'complexity' is burning through enterprise budgets, draining productivity, and burning out employees](#)

## 4. PHYSICAL AND GENERAL SECURITY

Although cybersecurity is top of mind, other forms of security remain important – especially as the lines between digital and physical systems blur, and criminals become more sophisticated.

In the modern threat landscape, physical security threats aren't a matter of simply guarding the perimeter but understanding the new techniques criminals can deploy and the evolving routes of entry – this includes issues like drone surveillance and the distribution of the enterprise beyond one building.

“Physical security is back in the conversation because more of the physical world is now tied directly to digital systems. Doors, sensors, robotics, warehouses, even HVAC in some cases,” says Kandi. “If something goes wrong there, it hits operations immediately. The bigger context is that companies are finally admitting that physical and digital security are not separate issues. An attacker does not care about internal categories. They just look for whatever opening is easiest.”

Ongoing risk assessments, implementing modern technologies, and integrating physical infrastructure with the broader network are key steps that businesses should take – with continuous monitoring and incremental upgrades to follow.



### EXAMPLES OF PHYSICAL AND GENERAL SECURITY IN ACTION:

Biometric entry, remote wiping of lost devices, restricted access areas, and security doors.



### READ MORE ON PHYSICAL AND GENERAL SECURITY

- 'A huge national security risk': Thousands of government laptops, tablets, and phones are missing and nowhere to be found
- Cyber resilience in the UK: learning to take the punches



## 5. AUTOMATION

Generative AI might be a top priority for businesses but so too is automation, with extraordinary value lying in reducing manual and repetitive workloads for employees. Not only that, but systems like robotics and AI agents might start to play a role.

The technology is growing more sophisticated; in 2026, we might finally begin to see these systems be good enough to handle the lofty ambitions of businesses in increasing the level of automation in the enterprise. It matters because businesses crave stability and balance – and turning to automation mitigates the swings that come in the labor market as well as talent pipelines. This transition, however, should be seen as a safety net rather than a trend.

**“Automation is accelerating at rates we’ve never seen before. Advanced robotics, autonomous systems, and intelligent agents are moving from the experimental stages and into daily operations.”**

– DANIEL BURRUS, FOUNDER OF BURRUS RESEARCH



### EXAMPLES OF AUTOMATION IN ACTION:

Automated patch management, cybersecurity automation, and workflow automation.



### READ MORE ON AUTOMATION

- [Can robots work safely alongside humans? This industry leader thinks we’re not far away](#)
- [How automation is quietly redefining what “good” looks like in endpoint management](#)
- [The future of networking: programmability and automation](#)



“Automation is accelerating at rates we’ve never seen before,” says Daniel Burrus, futurist, global technology innovation expert, and founder of Burrus Research. “Advanced robotics, autonomous systems, and intelligent agents are moving from the experimental stages and into daily operations.”

Businesses in 2026 will look to increase automation in areas like payroll, data entry, and reporting, as well as customer support. These systems can sense, detect, and adapt to changing circumstances, Burrus adds, while respondents to *ITPro’s* Future Focus research say they plan to use the technology to free up human resources to tackle more complex issues.



### WHAT DOES IT MEAN FOR ITDMs?


The more things change, the more they stay the same – at least for some elements of 2026’s research. Cybersecurity is as present as it ever has been and that’s not going to change any time soon.

Similarly, investing in software, whether it’s adding something new and exciting or keeping on top of what’s already in place, will always be important.

Whether AI will eventually just be considered another aspect of software remains to be seen but for the second year in a row it’s the most important area of investment and attention for Future Focus respondents.



# How decisions are made and tech deployed



Pricing and trust are key factors in ITDMs' vendor choices, with the need to meet regulatory requirements driving spending

As organizations embrace new technologies and look to overhaul old systems, ITDMs are under pressure to purchase new solutions from vendors.

Choosing the right projects to fund and getting sign-off from relevant stakeholders is a lengthier process than ever, with more focus on trust and cost optimization.

Research for Future Focus 2026 revealed the majority of final decisions rest with the CTO, with 46% of respondents identifying this role as the crucial decision maker. In comparison, just 26% of respondents said the final decision rests with CEOs and CFOs, with CISOs coming in a distant third at 9% and IT management trailing at 3%.

This is a significant change from [Future Focus 2025](#), in which 37% of respondents said IT management was responsible for making the final decisions.

**“Vendors should be responsive, transparent, and deliver on promises, while avoiding hidden costs or delays.”**

– US FUTURE FOCUS 2026 RESEARCH RESPONDENT

## PRICING IS A TOP FOCUS

Respondents ranked pricing as the number one criterion when it comes to selecting vendors – up from third place in 2025 – followed closely by product or service features, and vendor reputation.

This change highlights a sharper focus by organizations on spending and return on investment (ROI) from any purchase.

Anxiety among respondents over getting bang for their buck is also registered in the number of decision-makers involved in making certain purchasing decisions.

**“Don’t ghost us or change prices once we decide on one.”**

– US FUTURE FOCUS 2026 RESEARCH RESPONDENT

While in the 2025 report, almost a third (30%) of respondents said budgets of £200k or more were overseen by just one or two people, only 18% said the same in the 2026 report. This shows that decisions are becoming more complex and, regardless of who makes the final decision, more people are involved somewhere along the way.

“A good vendor/customer relationship is based on trust, clear communication, and reliability,” said one US-based respondent. “Vendors should be responsive, transparent, and deliver on promises, while avoiding hidden costs or delays.”



Another respondent, also based in the US, stressed the importance of vendor follow-up, strong communication, and transparency on pricing.

“Don’t ghost us or change prices once we decide on one,” they said.

With greater focus on pricing, ITDMs are necessarily selective about the projects that receive their organization’s funding. Just under half of respondents (49%) said they undertake between one and three IT projects per year, while almost a fifth (18%) now only undertake one project annually.

This is a significant shift compared to last year’s research results, with the number of respondents focusing on a sole project up 97% and those engaged in six or more projects down by a third (33%).

## REGULATIONS DRIVE NEW SPENDING

When it comes to purchasing new solutions, a desire to reduce risk and to meet cybersecurity insurance requirements (or reduce insurance premiums) ranked highest. More than a fifth of respondents – with 21% and 20% respectively – cited them as primary motivators for purchases.

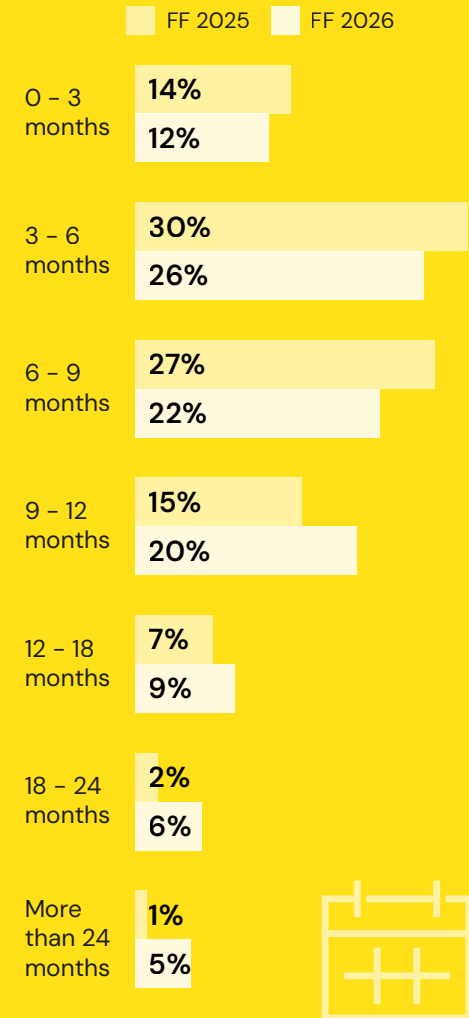
There’s a noteworthy difference between the two factors, however. While the number of respondents indicating insurance policies had affected purchasing decisions has increased 29% year-over-year, the total of those who pointed to risk reduction as a primary factor fell by 43%.

These findings match a marked reduction in the number of respondents who say incidents drove them to purchase new solutions, which fell from 19% of overall respondents in 2025 to just 7% in 2026 – a decrease of 64%.

This paints a picture of a sector increasingly moved to invest in products to reduce overheads and meet compliance, rather than one scrambling to fix operational or cybersecurity issues in their core business systems.

The data backs this up: 57% of respondents indicated regulation would be more important in 2026 than it had been in 2025, and 18% identified the need to follow government regulations as a primary motivation for IT purchases.

### What is the average time between starting a project and signing a contract to go live?



A number of noteworthy pieces of legislation affecting business data and IT systems use came into effect throughout 2025, including the [Digital Operational Resilience Act \(DORA\)](#), the [EU AI Act](#), and [Cyber Resilience Act \(CRA\)](#) in the EU.

There is a grace period for some of these pieces of legislation, however. For example, the CRA came into force in December 2024, but firms have until 11 December 2027 become compliant with the law, although mandatory reporting starts from September 2026.

The [UK's Data Use and Access Act](#), meanwhile, is undergoing implementation, and the country's [Cyber Security and Resilience Bill](#) is expected to take effect sometime in 2026.

## TRUST IS AN ABSOLUTE PREMIUM

One of the main themes of this year's Future Focus research is the emphasis ITDMs place on trust. This isn't just a matter of vendor reputation; it's an assessment of the ongoing transparency and reliability of the relationship between a customer and vendor.

When asked what makes a good vendor/customer relationship, a huge number of respondents stressed the importance of trust.

"A good vendor relationship is built on trust, transparency, and mutual value," said one US-based respondent.

Trust isn't the only factor in maintaining long-term relationships with customers, though; the [price of entry for new technology such as generative AI](#) and AI agents also has a significant influence.

A recent Capgemini report found [enterprise trust in agentic AI remains low](#), demonstrating that vendors will need to continue to demonstrate their trustworthiness to secure spending from business AI budgets.



The importance that ITDMs place on trust is also reflected in a notable lengthening in the amount of time it takes businesses to start a project and actually sign a contract to make it live.

While the majority of businesses still take 12 months or less to bring projects to fruition in this manner, the number of respondents who said it takes nine months or less declined compared to 2025.

On the other side of the equation, the proportion of respondents who took between nine and twelve months to finalize their contract after starting a project increased 36%. Those taking more than 24 months increased by a whopping 373%.

Ultimately, the picture Future Focus 2026 paints is one of cautious, prudent spending by organizations. Recognizing their legal responsibilities as well as the opportunities at their fingertips, ITDMs are choosing to spend big on limited projects with trusted partners.



## WHAT DOES IT MEAN FOR ITDMs?

Regulation is an increasingly important consideration for the IT community. The EU introduced three new pieces of legislation that businesses operating within the region must abide by, focusing on security and AI. On top of this, organizations operating in the UK will need to abide by its Data Use and Access Act, as well as its incoming cybersecurity regulations. While experts believe compliance with GDPR will already cover some of these bases, IT leaders must nevertheless check they are compliant and make adjustments if necessary before the time to become compliant runs out.



# The secrets of our success: How vendors and ITDMs can work together in 2026

How can vendors earn the trust of ITDMs?  
And how can organizations make sure they are choosing the right partners?



In 2026, ITDMs continue to face the challenge of finding the right vendor in a landscape where new and more sophisticated technologies seem to be emerging all the time. Anxieties like fear of missing out (FOMO) can encourage would-be buyers to rush into opportunities headfirst, without fully considering the consequences.

That's why it's important to pause for thought before making commitments, especially when it comes to aligning yourself with a vendor that may make or break how well you implement a technology.

For technology vendors, meanwhile, demonstrating and proving trust and consistency is vital to long-term success. Businesses live or die by how well they can forge relationships with customers. When a relationship and resultant experiences are perceived as good or more, vendors really can build the foundation of long-term success.

*ITPro's* Future Focus 2026 research has cast a spotlight on what ITDMs value most when looking to forge new partnerships, with key criteria including communication, transparency, and honesty, as well as building mutual value.

Vendors are encouraged to truly act as an equal partner and be up front at all times. Flexibility is important, as is accountability for decisions. In 2026, building these partnerships will be essential to success.

**"Both sides should see each other as partners working toward shared goals rather than just a buyer and seller."**

— US FUTURE FOCUS 2026 RESEARCH RESPONDENT

## THE BUSINESS BACKDROP FOR 2026

Conversations around AI are already inescapable in 2026, and accelerated adoption is top of the agenda for many ITDMs. Finding the right partner, in this context, is crucial to ensure a quick ROI.

“The two biggest forces that will shape business are unprecedented enterprise AI investment/digital transformation, and the drive to turn AI potential into operational outcomes,” Ramnish Singh, chief solutions officer at cloud provider Onix, tells *ITPro*.

“Global IT spending is booming. Most of it is fueled by AI infrastructure, cloud services, and digital modernization. This puts pressure on ITDMs to deliver measurable business impact, not just proofs-of-concept.”

## HOW VENDORS CAN EARN AND PROVE TRUST

*ITPro*'s research found that ITDMs prioritize several core values above and beyond all others, including reliability, clear and open communication, as well as transparency and accountability. These all fold into one key quality – trust – that will determine whether a vendor can close a deal and strike partnerships that are long-lasting and mutually beneficial with their prospective clients.

“Vendors should be responsive, transparent, and deliver on promises, while avoiding hidden costs or delays,” said one US-based respondent to a question asking for key criteria in a good vendor-customer relationship.

“Both sides should see each other as partners working toward shared goals rather than just a buyer and seller,” said another.

## What is your typical decision criteria when selecting vendors?

(Rank highest to lowest)

- 1 Pricing
- 2 Product/service features
- 3 Vendor reputation
- 4 Risk assessment
- 5 Support and licensing
- 6 Sustainability and ethics
- 7 Stakeholder recommendations
- 8 Supplier relationship
- 9 Third-Party reviews or recommendations



Kashif Rahamatullah, a multi-alliance lead at Deloitte, tells *ITPro* that trust is earned when vendors prove they not only understand the wider technology landscape but also demonstrate a nuanced grasp of a client's vertical and specific needs.

"Leading with knowledge tailored to the client's context shows that vendors are invested in meaningful outcomes, not just closing a deal," he said.

"This is reinforced by radical transparency, especially in promptly communicating product roadmap risks, pricing changes, and providing honest Root Cause Analyses (RCAs) during system failures."

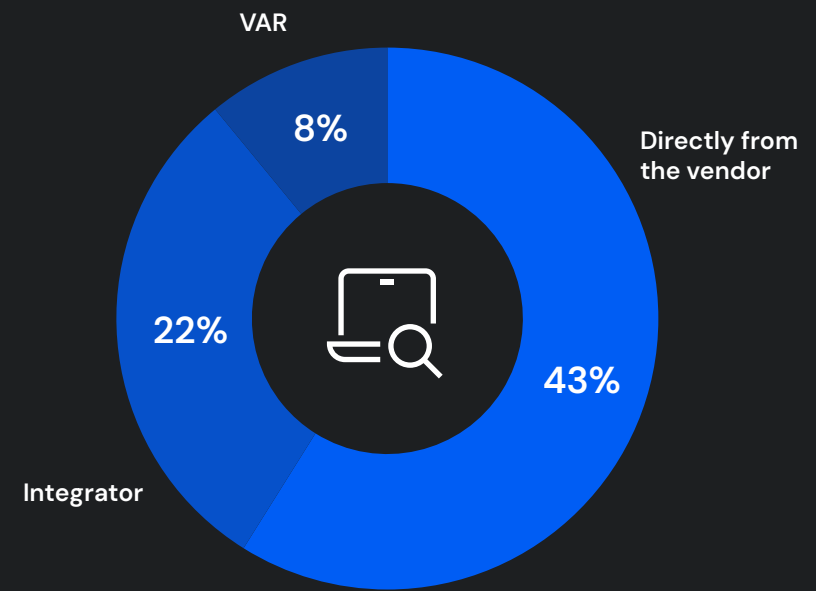
Then, he continued, it's a case of deepening trust further once the relationship has been forged. This could mean actively engaging support provision, addressing any challenges that arise promptly, or further showing that the vendor has learned the ins and outs of the core business and knows the upcoming opportunities and obstacles.

## CHOOSING THE RIGHT LONG-TERM PARTNER TO GUARANTEE SUCCESS

For ITDMs, the burden of choice may weigh heavily, given the availability of vendors to work with as well as the accelerating timescales involved.

Businesses should undertake a forward-thinking and thorough assessment rather than looking to address immediate needs, Rahamatullah added. Decision-makers can raise the chances of success by considering vendors as lasting allies and investigating not just the solutions they offer but their long-term mission, as well as their own strategic directions.

## Where do you typically prefer to procure your tech solutions?



US data only

Specifically, they should undergo “rigorous validation of technical compatibility” through PoCs and define a clear contractual exit strategy to avoid vendor lock-in. It’s also wise, Rahamatullah said, to engage with a range of the vendor’s existing clients to gauge how happy they are and determine the reliability of the vendor.

Building a successful and long-lasting partnership is a complex and multi-staged process that won’t just happen overnight. There’s plenty of work for both the vendor and ITDM to do to ensure they’re making the right decision by entering into a partnership – but the work only starts then. Care and attention are needed to improve and build on these partnerships to guarantee long-term success.

*ITPro’s* research has shown ITDMs are happy with vendors when they work well with the company’s needs, and take steps to make them feel as if they are spending their organization’s money wisely.

Those surveyed say it’s as much about the right feeling as it is about any metric or chart; honest and frequent communication is key to this, as both parties try to navigate a fast-paced and dizzying future.



### WHAT DOES IT MEAN FOR ITDMs?

The tide had already started to turn on how collaborative vendors are with each other last year and 2026 may help cement this trend to the benefit of ITDMs and businesses.

Transparency may be hard at times, but as vendors realize that loyalty is based on trust and openness, the relationship between them and their customers will improve.



# Historic hurdles and future focus

IT leaders across a range of industries are sharpening their focus on cybersecurity and compliance in 2026 amidst growing AI-related security concerns



2025 was a year of huge opportunity for ITDMs, but it was also often defined by acute challenges.

Enterprises have encountered significant technology-related hurdles against a backdrop of troubling macroeconomic conditions. IT leaders have faced a delicate balancing act, splitting their attention across an expanding array of domains.

Reflecting on the year gone by, Future Focus 2026 respondents highlighted a variety of concerns, with cybersecurity, AI integration, regulatory compliance, skills, and infrastructure modernization all top of mind.

Cybersecurity, in particular, ranked as a leading shared concern among both US and UK-based IT leaders, albeit with differing foundations.

In the UK, cybersecurity-related challenges centered largely on the potential for AI-powered threats as well as the implications of regulatory compliance.

“Cybersecurity is at an inflection point,” one UK respondent said. “Cyber attacks are being automated with AI, making them faster and harder to detect.”

Meanwhile, on the other side of the Atlantic, cyber concerns typically focused on the implications of rapid AI rollouts and cloud-related threats.

One respondent noted their main challenge lay in the “escalating sophistication of cybersecurity threats” along with the “rapid and complex integration of AI into business operations”.

“In 2025, my biggest tech problem was data security and privacy in the face of increasingly sophisticated cyber attacks,” another said.

**“Legacy security systems struggled to provide real-time visibility.”**

– FUTURE FOCUS 2026 RESEARCH RESPONDENT

## A CONFLUENCE OF CHALLENGES

Unfortunately, these issues often compound each other, leaving ITDMs facing multi-pronged considerations. On the infrastructure side, for example, UK-based respondents identified continued reliance on legacy systems as a major hurdle.

This was partly due to cyber-related risks, but it also has an impact on AI adoption, with IT leaders struggling to integrate new tools and technologies while still relying on outdated infrastructure.

“Legacy security systems struggled to provide real-time visibility, and integrating cloud applications with existing infrastructure created gaps,” one respondent said.

“Our biggest tech problem in 2025 was integrating multiple AI tools smoothly,” another noted, adding there were “not enough ways to make them work together without breaking things”.

Data privacy also posed significant challenges for IT leaders in 2025, with AI once again a key factor. The large volumes of sensitive internal data used to feed AI models mean enterprises have been forced to adopt a more robust approach to security and governance.

“AI systems rely on massive datasets, often containing sensitive personal or business information,” one respondent noted, adding that compliance had become challenging due to “evolving privacy regulations”.

This overlap between privacy and regulatory compliance was firmly in the crosshairs for both US and UK-based IT leaders. Notably, many concerns centered on balancing innovation with compliance while navigating evolving national and regional regulatory frameworks.

In the UK, for example, respondents reported continued concerns about GDPR and other EU regulations.

“Ensuring compliance with evolving privacy regulations (like GDPR or emerging local laws) became challenging,” one person said.

US-based IT leaders also reported similar challenges in adapting to changing privacy and security legislation.

## Top 10 Areas of Investment in 2026

- 1 AI
- 2 Cybersecurity
- 3 Software
- 4 Security (general)
- 5 Automation
- 6 Machine Learning
- 7 Data Center Infrastructure
- 8 Analytics
- 9 Storage
- 10 Cloud (hybrid)

“The challenge was implementing robust security measures across multiple platforms while ensuring compliance with evolving privacy laws,” one respondent said.

“This required a balance between innovation and security, and managing it effectively became crucial for protecting both user trust and company integrity.”

These worries align closely with a [report from Forrester](#), in which more than half (54%) of IT leaders identified privacy, governance, and regulatory compliance as their top priorities in 2025.

## CAPITALIZING ON OPPORTUNITIES

Despite rampant challenges, Future Focus 2026 shows IT leaders remain upbeat for next year, with investment in cloud, AI, and cybersecurity all expected to continue.

In the realm of AI, 51% of participants said this would be a priority area for investment.

The scale of investment here is also expected to increase. While 15% of Future Focus 2025 respondents planned to spend between 31% and 40% of their overall budget on the technology across 2025, 23% of this year's cohort plan to do the same in 2026, underlining an increased (52%) appetite for investment.

**“[There aren't] enough ways to make AI tools work together without breaking things.”**

– US FUTURE FOCUS 2026 RESEARCH RESPONDENT



**“The biggest technology opportunity for my business in 2026 is AI integration, especially through automation [and] personalization.”**

– US FUTURE FOCUS 2026 RESEARCH RESPONDENT

This AI-related push will also see IT leaders ramp up “AI readiness” efforts in a bid to simplify adoption projects for teams, with 58% saying this is more important than last year.

IT leaders’ end goals for AI integration vary across different industries. Generally speaking, though, typical aims are focused on driving workforce productivity and efficiency, as well as cost reduction and ensuring more personalized customer experiences.

“The biggest technology opportunity for my business in 2026 is AI integration, especially through automation, personalization, and data-driven decision-making. AI can improve efficiency, reduce costs, and enhance customer experiences, making it a key driver of growth,” one respondent said.

A continued focus on regulatory compliance is also expected in 2026, with IT leaders building on vital lessons learned this year: more than half (57%) of respondents identified this as more important this year than last.

Similarly, cybersecurity is an area of significant focus for businesses this year. Only 19% of respondents said it would be less important in 2026 than in 2025, while 62% said it would be more important this year than last.



In Future Focus 2025, just 6% of respondents said they planned to spend more than 50% of their overall IT budget on security. In this year's research, however, that figure has more than doubled, coming in at 13%.

This attention to cybersecurity investment aligns closely with analysis from Gartner, which shows global spending is set to hit \$213 billion by the end of 2025, marking a 10.4% increase on 2024 budgets.

Separate research from PwC also shows nearly one third (32%) of enterprises plan to increase cyber budgets between 6–10%.

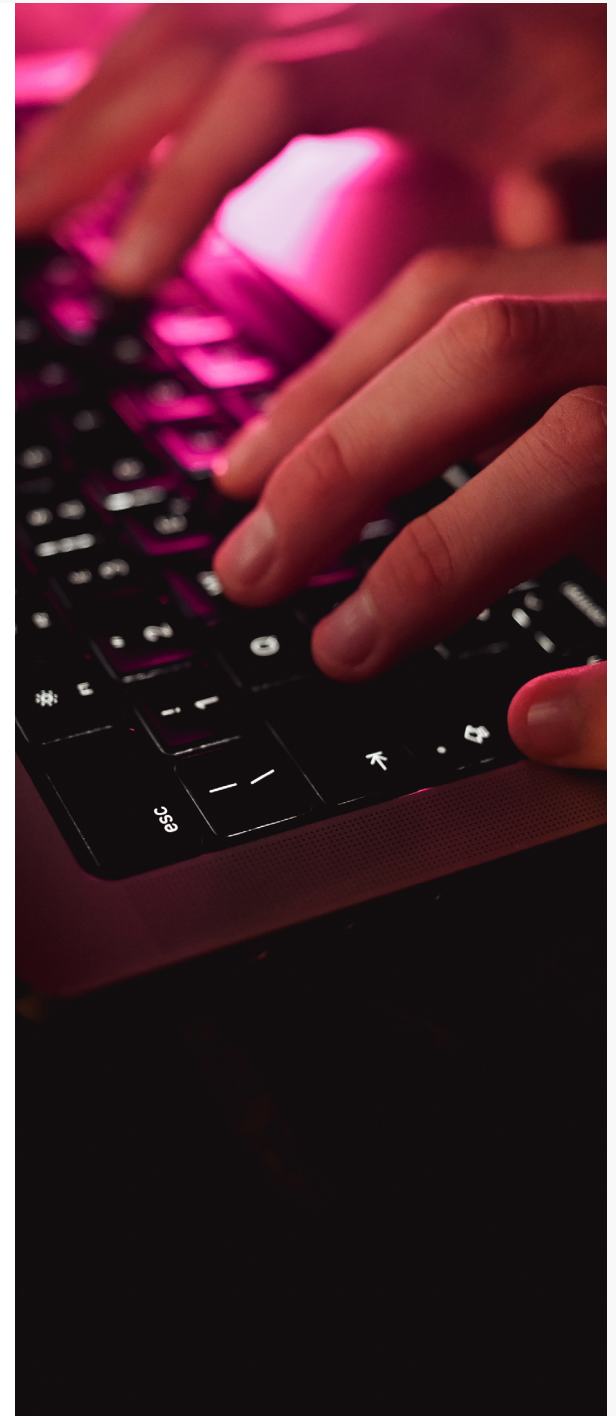
All told, Future Focus 2026 highlights a paradoxical year ahead for IT leaders. While there is a sense of optimism that enterprises can unlock tangible benefits from emerging technologies such as AI, the confluence of secondary issues means IT leaders will have to balance their attention across multiple domains.



### WHAT DOES IT MEAN FOR ITDMs?

AI is the story of 2026, and ITDMs have high hopes for the technology in the coming year. Struggles like integration are likely to remain, however, and may come to dominate the conversation as more AI applications are introduced.

Cybersecurity is an ever-present consideration but it may be regulatory changes that take precedence as ITDMs try to balance introducing new technologies with new legislation.



# The software hype train is leaving the station, but it's running on old tracks



**AUTHOR**

Rene Millman

While emergent technologies may hog the spotlight, decision makers shouldn't neglect the hardware they run on

If you have spent any time reading the technology press over the last 12 months, you would be forgiven for thinking hardware has become irrelevant. The conversation has been almost entirely monopolized by Large Language Models (LLMs), Software as a Service (SaaS) platforms, and the ephemeral "Cloud."

We have become so fixated on the magic of the software that we have seemingly forgotten about the machine.

For IT leaders, this oversight is becoming a liability. While software may be the ambition, hardware remains the capability. The uncomfortable truth for many organizations is that their digital roadmap is writing checks their infrastructure can't pay. We are standing on the precipice of the "AI PC" era, yet too many enterprises are still trying to run next-generation workloads on last-generation silicon.

**"We have become so fixated on the magic of the software that we have seemingly forgotten about the machine."**

## THE AI REALITY CHECK

The single biggest misconception about the current AI boom is that it lives entirely in the data center. While training massive models requires the brute force of hyperscale clusters, inference – the actual daily use of these tools by your workforce – is increasingly pivoting to the edge.

Latency, privacy, and cost are driving AI workloads back to the device. If your organization plans to deploy local small language models (SLMs) or leverage embedded AI assistants to boost productivity, legacy laptops with integrated graphics and aging CPUs simply won't cut it. Neural processing units (NPUs) are no longer a luxury feature for creatives; they're becoming a standard requirement for the general workforce. Without the right endpoints, expensive AI software licenses will result in nothing but frustrated employees staring at loading bars.

## THE CLOUD BOOMERANG EFFECT

This hardware renaissance isn't limited to user devices. We are also seeing a distinct shift in the narrative regarding infrastructure, often described as "cloud repatriation". The "cloud-first" mantra of the early 2020s is softening into "cloud-smart," driven largely by the stinging reality of egress fees and spiraling operational costs.

For specific, predictable, and high-intensity workloads, modern on-premises hardware is often proving to be the more cost-effective solution. Executing a repatriation strategy requires a hardware fleet that is up to the task; however, you can't bring workloads home if "home" is a crumbling server room filled with end-of-life racks. Modern servers are not just about raw speed; they are about density and energy efficiency, allowing businesses to handle denser workloads without blowing a hole in their ESG targets.



## SECURITY IS SILICON-DEEP

Finally, as we rely on software to define our security perimeter, we must remember that it's only as secure as the hardware it runs on. With the sophistication of cyber threats escalating, often aided by the very AI tools tech enthusiasts champion, firmware-level attacks are rising.

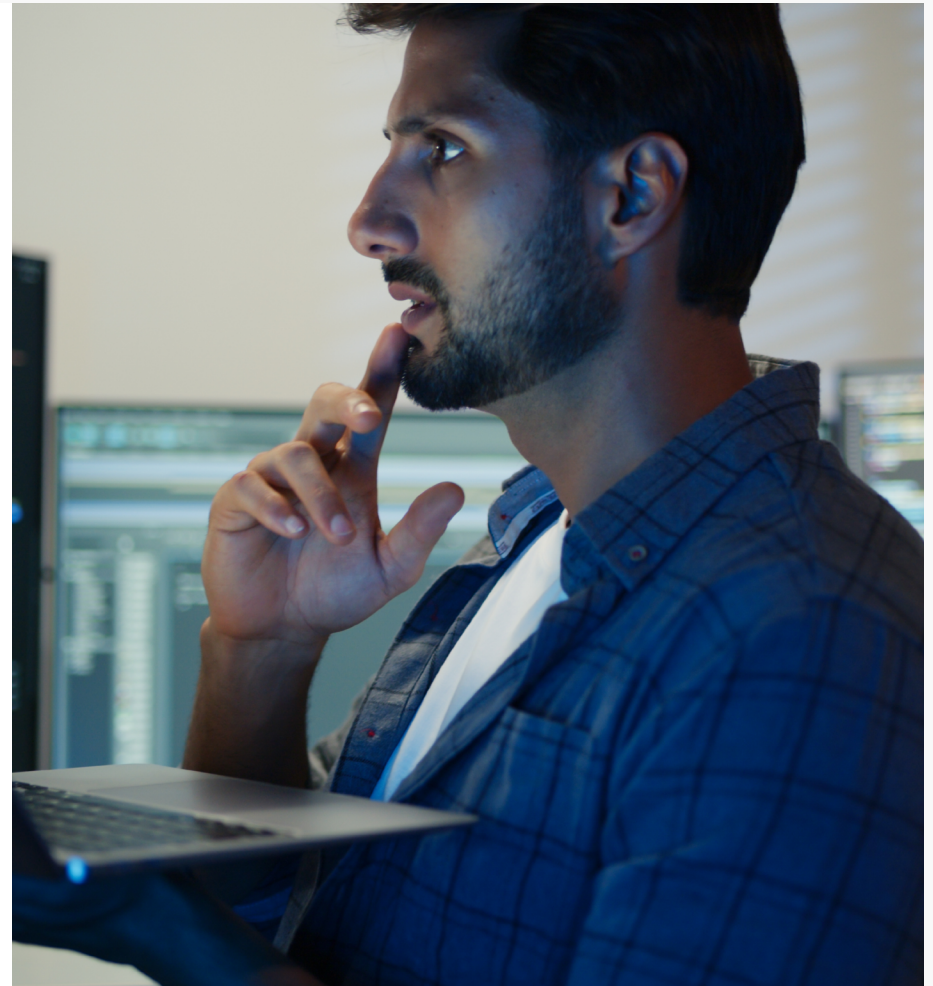
Modern ambitions around “zero trust” architectures fall flat without a hardware root of trust. Features like trusted execution environments and hardware-enacted virtualization are the bedrock upon which secure software stacks are built.

Investing in cybersecurity software without upgrading the underlying physical infrastructure is akin to installing a steel vault door on a straw house.

## APPETITES AND HALLUCINATIONS

The appetite for transformation is high, but ambition without foundation is just a hallucination. For IT leaders, the coming year can't just be the year of software adoption; it must be the year of hardware revitalization.

Whether it's the servers in your hybrid cloud or the laptop on your analyst's desk, the metal matters. If you want to win the software race, stop neglecting the engine.



### ABOUT THE AUTHOR

Rene is a freelance writer and broadcaster specializing in AI, cloud, infrastructure, and mobile technology. A former analyst for both Gartner and IDC, as well as a regular contributor to *ITPro*, he frequently appears on television to provide expert commentary on the major technology trends and companies shaping the digital landscape.

# AI is dominating IT priorities in 2026, whether it's through the prism of security or software

How can business leaders and vendors navigate the complex waters in 2026 and beyond, with AI coming to dominate thinking across all disciplines?



**AUTHOR**

Keumars Afifi-Sabet

While ITDMs have always had to keep one step ahead to move forward, the IT landscape now can feel more uncertain than ever. With so many areas in need of attention and investment across the enterprise, it's hard to know what to prioritize at any phase of your company's operations.

In 2026, ITDMs have made their priorities clear — and all roads lead to AI. Whether that's through the prism of new tools, cloud computing, security, or good old-fashioned automation, AI is the dominant theme.

*ITPro's Future Focus 2026* research highlights the five biggest tech priorities for the year ahead as AI, cybersecurity, software, physical/general security, and automation. They may seem unrelated, but all have a touchpoint with AI when you dig deeper. This is a marked shift from 2024 and 2025, when many projects were in the conceptualization or pilot phase, and priorities focused on experimentation rather than true implementation.

Trends like edge computing and hybrid cloud, which were considered important in previous years, have been eclipsed by new priorities. Cybersecurity and physical/general security are more of a priority in 2026 — but, again, through the prism of AI, given that the nature of threats has shifted. Comments from respondents demonstrate this by highlighting how much it's become embedded into the fabric of IT itself.

What does this mean in practice, though? We're not only talking about Copilot+ Windows AI PCs but unlocking productivity gains and helping ITDMs implement fundamentally new processes. Take cybersecurity, for example: the threat of AI-powered cyber attacks is forcing businesses to consider mitigation tools like automated threat detection.

**"It might seem counterintuitive, but when things are moving so fast around you, sometimes it pays off to slow down. Simply picking up the latest trends and buzzwords (or the cheapest vendor) out of fear of being left behind might lead to more problems than they solve."**

Day-to-day software, too, has become a haven for new AI functionality designed to improve workflows and increase employee productivity. There's also the struggle of figuring out how to integrate the new with the old, with many new systems not compatible with aging infrastructure.

The wider availability of AI tools and services in all areas might feel like a murky flood has submerged and clouded your decision-making. When investing in new systems, it's important to make the right decision and undergo detailed and interrogative procurement processes. This will help determine how investments into the key IT focus areas will pay off and what your organization's desired outcomes are.

It might seem counterintuitive, but when things are moving so fast around you, sometimes it pays to slow down. Simply picking up the latest trends and buzzwords (or the cheapest vendor) out of fear of being left behind might lead to more problems than they solve.

Whether it's in integrating new software, applying new automations throughout the business, or iterating on ways to keep your assets and employees safe, you should do your due diligence; make sure you are forging business relationships with your vendors that will serve you in the long term, not just for tomorrow. The sands are shifting faster than ever, so make sure you reflect on where your business – and that of your partners – is going so you can navigate the unknown together.



## ABOUT THE AUTHOR

Keumars is an experienced technology journalist and formerly the features editor at *ITPro*, where he still contributes as a writer. He has reported extensively on topics around AI, cybersecurity, and cloud computing, alongside other core topics close to the minds of ITDMs in today's business landscape.