



2023 Survey

# Employee Productivity Surveillance Technology



# Contents

- 3** Executive Summary
- 5** Key Findings
- 8** The prevalence of EPST
- 10** Honor code: IT staff are uncomfortable deploying surveillance tech
- 12** Transparency essential, but lacking
- 14** Taking a stand
- 16** What's at stake: consequences hit recruitment and retention
- 20** IT workers would risk their job to do what's right
- 22** Data access concerns outweigh possible productivity gains
- 24** Conclusion
- 25** Methodological Notes

# Executive Summary

**As leaders turn to technology to monitor workforce productivity, they fail to consider the harm they will do to the team responsible for implementation — their IT department.**

To understand what happens to IT teams when given such an assignment, 1E surveyed 500 IT workers and 500 IT managers, in partnership with Wakefield Research. The results demonstrate the need for companies to reevaluate using employee productivity surveillance technology (EPST).

Though most IT staff currently work for companies that use EPST, they harbor discomfort about deploying it to watch their

colleagues, especially if the company isn't fully transparent about the practice. Many IT workers report they would raise their concerns with leadership before following orders to deploy this tech, and some would even flat-out refuse. Most IT managers admit they wouldn't force a staff member to deploy and monitor the tech if they refused. And once EPST is deployed, many in IT say they would defy company policy and inform colleagues about it, even helping them use anti-surveillance workarounds.



## Definition

Employee productivity surveillance technology (EPST) refers to a range of tools that companies use to monitor employees' productivity.

## Common EPST



Monitoring web activity



Logging time spent using various programs



Keylogging, click-logging



Video recording



Audio recording

“

*“Most research and reporting on this issue to date has focused on the employees that companies spy on. They’re more anxious and resentful, more likely to fake work, quit, and even steal workplace property. Yet, until now, the research has overlooked the perspective of those tasked with spying: IT workers and managers.”*

**Ian Greenleigh**

*Vice President of Brand and Communications, 1E*



2023 EPST SURVEY

# Key Findings

## Discomfort abounds



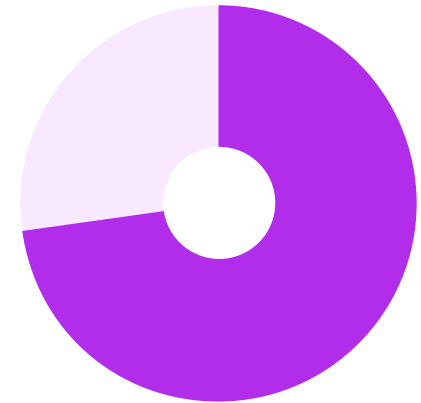
80%

of IT managers think staff  
would be comfortable  
deploying EPST



46%

of IT workers are  
comfortable deploying  
EPST



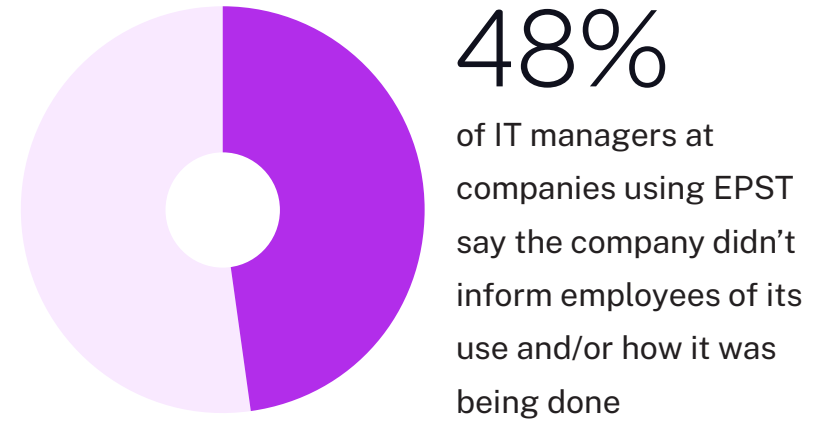
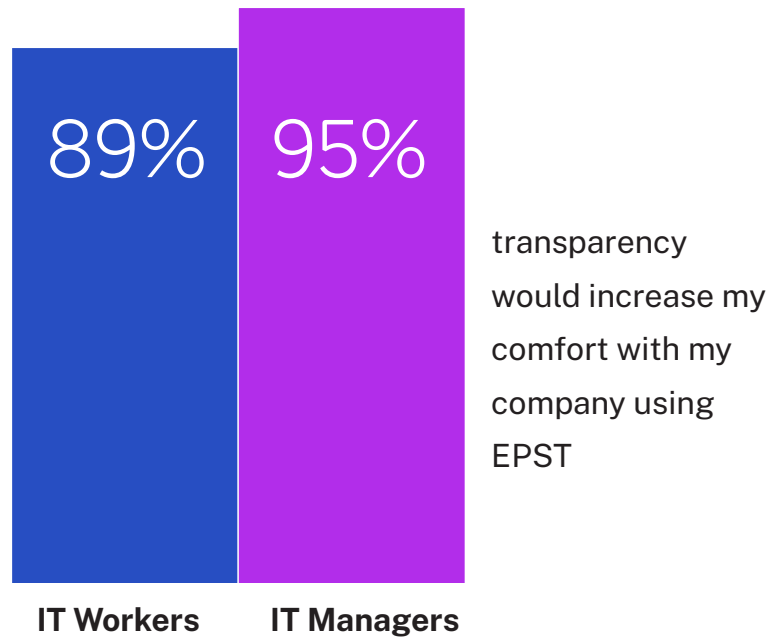
73%

of IT managers are  
uncomfortable telling  
their staff to deploy EPST

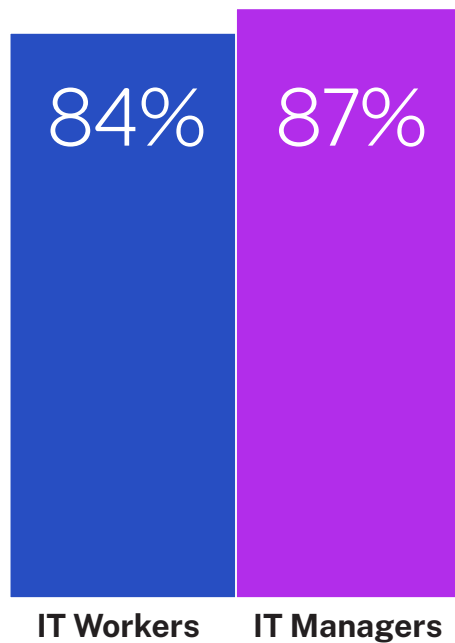
**70% of IT Managers**

wouldn't force staff to deploy and monitor  
EPST if they refused

## Transparency essential, but lacking



## Leaders, beware



have seen negative impacts since their company started using EPST



48% of IT workers would turn down an otherwise desirable IT position if they knew the company used EPST

# The prevalence of EPST

Leaders are concerned about their ability to supervise, especially in remote and hybrid environments — and companies have turned to tech for help. In fact, nearly 9 in 10 IT managers (89%) have first-hand experience with EPST, with 83% saying their current employer uses it and 19% reporting experience with it at a previous company. Similarly, more than 4 in 5 IT workers (84%) describe themselves as very or extremely familiar with EPST, with the same percentage (84%) having first-hand experience with it at a current (77%) or former (21%) employer.

If IT team members don't already have experience with EPST, they likely will soon. Among IT managers at companies that don't use EPST today, 4 in 5 (79%\*) believe their company is at least somewhat likely to start in the next three years.





83%

of IT managers say their  
current employer uses  
EPST



79%

of IT managers believe their  
company is likely to start using  
EPST in the next 3 years

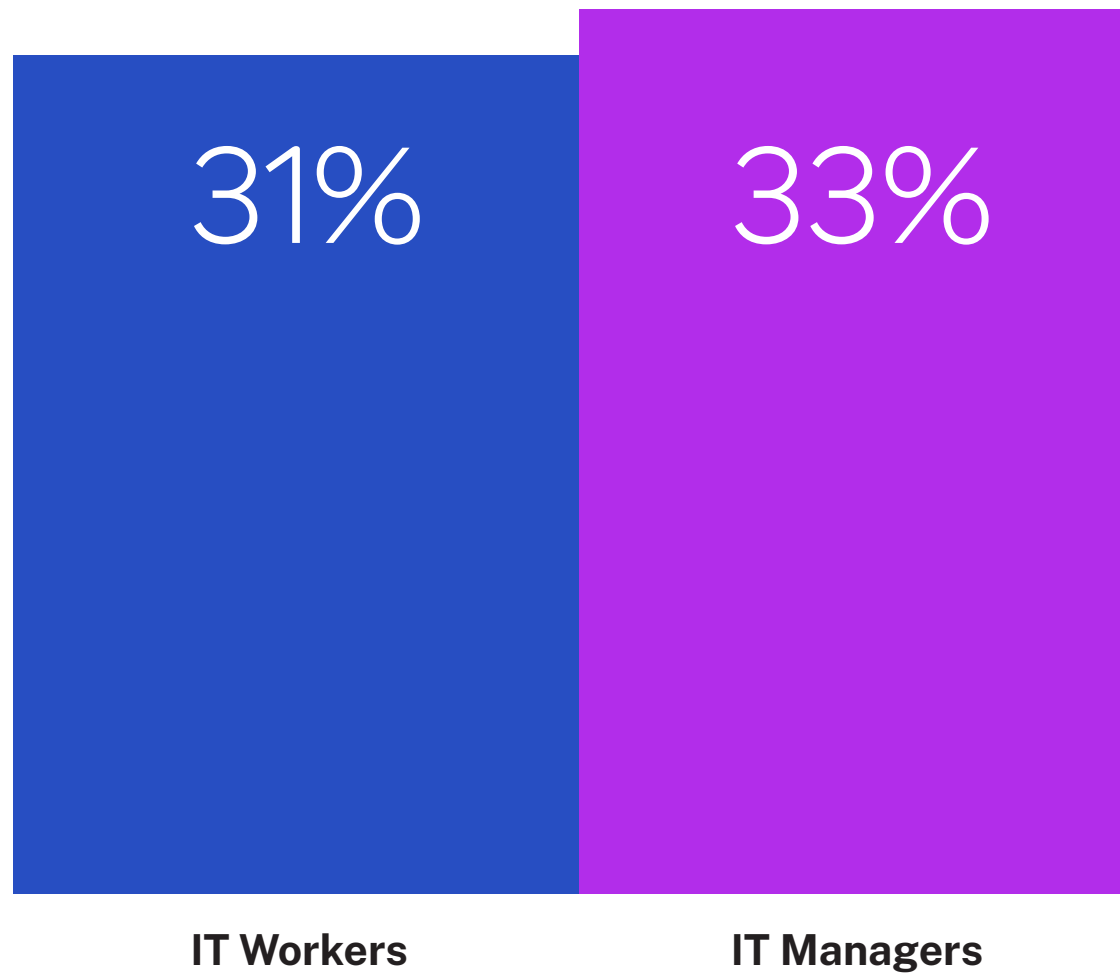
# Honor code: IT staff are uncomfortable deploying EPST

More than two-thirds of IT workers (69%) and IT managers (67%) believe it's appropriate for companies to monitor what employees are really doing on company time. But 31% of IT workers and 33% of IT managers say EPST is an invasion of privacy and shouldn't be used under any circumstances.

Despite a majority believing it's an acceptable practice, nearly 3 in 4 IT managers (73%) wouldn't be comfortable instructing their own staff to deploy EPST. This discomfort serves IT leaders well. Not only do IT workers find the

prospect of spying on co-workers unsettling, IT managers also severely underestimate the turmoil this would cause their team. While 4 in 5 IT managers (80%) say their staff would be comfortable with being told to deploy EPST, only 46% of IT workers say they'd be comfortable doing so.

Further, nearly half of IT workers (46%) say requiring them to deploy EPST to monitor their colleagues would cause them even greater anxiety than having their own productivity monitored.



think EPST is an invasion of privacy and should not be used under any circumstances



2023 EPST SURVEY

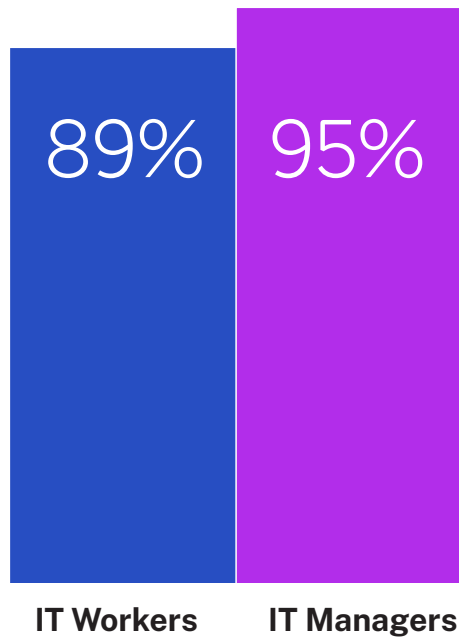
# Transparency is essential, but lacking



Disclosure has a massive impact on the comfort level of IT teams. Nearly all IT managers (95%) and 89% of IT workers say transparency would increase their comfort with their company using EPST.

Yet surprisingly, many aren't seeing that level of transparency in action. Of the IT managers whose current company uses EPST, nearly half

(48%) say employees either weren't informed that the technology is being used at all or were told it is being used but not how the surveillance is being conducted.



say transparency would increase their comfort with their company using EPST



48% of IT managers say employees either weren't informed that the tech is being used and/or of how the surveillance is being conducted



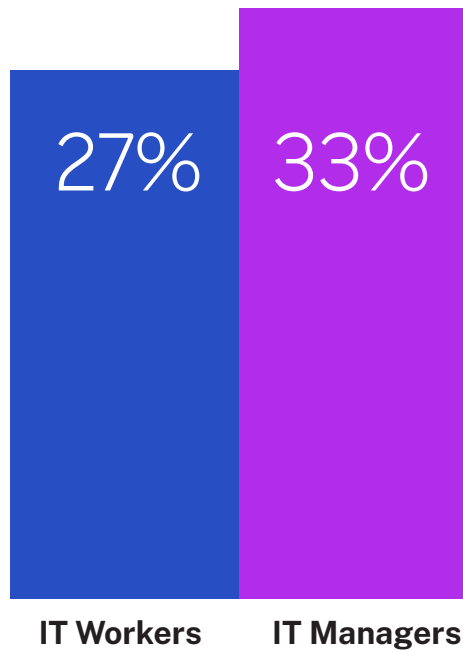
2023 EPST SURVEY

# Taking a stand

Before rolling out EPST, company leaders can expect to encounter IT's unease and should be prepared for a rocky implementation. More than a quarter of IT workers (27%) and a third of IT managers (33%) would raise their concerns with leadership before following an order to deploy EPST and monitor their colleagues.

Some aren't even willing to raise the issue of a potential compromise. Nearly 1 in 10 IT managers (8%) and 5% of IT workers would outright refuse to deploy the tech.

Fortunately for non-management level staff, those who refuse would have their supervisors' support: 70% of IT managers wouldn't force their staff to follow through. Included in that total is a quarter (25%) who would respect staffers' values and assign the task to others, without even issuing so much as a written warning.



would raise concerns about EPST with leadership



70% of IT managers wouldn't force their staff to follow through

# What's at stake: consequences hit recruitment and retention

Using EPST will hamper talent management, affecting both recruitment and retention efforts. If surveilling employees' productivity becomes part of a company's brand, it sets them back in the competition for talent. More than half of IT workers (52%) would turn down an otherwise desirable IT position if they knew the company used EPST.

Bringing surveillance tech on board can also spur current employees to seek other opportunities. Three-quarters of IT workers

whose company isn't currently using EPST (75%) say requiring them to deploy the tech to track other employees would negatively impact their willingness to remain in their current position. This includes 30% who would begin actively applying for other positions and 3% who would quit immediately. More than 2 in 5 say it would leave them more open to other offers (41%), making them an easy target for recruiters seeking to fill their IT positions.





84%

**IT Workers**




87%

**IT Managers**

have seen negative  
impacts since  
company started  
using EPST



**Negative impacts** seen at companies using EPST



**This avoidable talent drain is equally as likely to extend to management. 76%\* of IT managers whose company isn't currently using EPST say having to ask their team to deploy it would negatively impact their willingness to remain in their current position, including more than a third (35%\*) who would begin actively applying for other jobs.**

The danger radiates to other teams, too. 87% of IT managers and 84% of IT workers at companies using EPST have seen negative impacts since their company started using it. Specifically, respondents say it has led to declining employee loyalty (33% of IT managers and 29% of IT workers) and employees losing trust in company leaders (26% of IT managers and 29% of IT workers).

These IT teams also report impacts to workers' wellbeing, including increases in worker anxiety (29% of IT managers and 30% of IT workers), quicker employee burnout (29% of IT managers

and 28% of IT workers), and declining morale (27% of IT managers and 26% of IT workers).

When a company experiences an increase in distrust and anxiety among workers, elevated employee turnover follows. More than a quarter of IT managers (28%) and IT workers (27%) at companies using EPST have seen employees quit as a result. Exacerbating the situation, nearly as many IT managers (27%) and even more IT workers (30%) say it has become increasingly difficult to hire new staff since the company deployed the tech.

Companies not already using EPST risk a fortune if they choose to spy. As it stands, the potential negative impact is staggering. Nearly half of IT workers (48%) would expect employees to lose trust in company leaders if the company deployed the tech, 42% would expect a decline in employee loyalty, 40% predict employees would quit, and 31% believe it would become difficult to hire new staff.

2023 EPST SURVEY

# IT workers would risk their job to do what's right

Transparency is so important for IT workers that many are willing to sidestep company policy to make sure their colleagues are informed.

Nearly 3 in 4 IT workers (73%) would tell other employees the company was using EPST, even if doing so was against policy. Additionally, nearly as many IT workers (72%) would tell colleagues of any known workarounds.

Comfort varies greatly according to the specific surveillance technology used, making it vital that companies are open with employees about their practices. IT professionals are largely aligned in accepting the business case for keeping tabs on productivity, but their sentiment also clearly highlights boundaries. They're most comfortable with their company monitoring basic online

behavior such as web activity (58% of IT workers and 58% of IT managers) and logging time spent using various programs (57% of IT workers and 49% of IT managers).

However, they are more likely to see some proxy measures for productivity as overreach — an invasion of privacy that also has little business value. Less than half are comfortable with their company using keylogging and click-logging (49% of IT workers and 42% of IT managers) or video recording (43% of IT workers and 39% of IT managers). And even fewer are comfortable with screenshot captures (39% of both groups) or audio recordings (36% of IT workers and 39% of IT managers).

of IT workers would  
tell employees  
company was using  
EPST

73%

of IT workers  
would tell of any  
workarounds

72%

# Data access concerns outweigh possible productivity gains

Though they've seen — or would expect — downsides to using EPST, most IT workers (69%) and IT managers (71%) believe worker productivity increases when they know they are being watched.

A quarter of IT workers (25%) and nearly a quarter of IT managers (24%) say the technology's ability to measure productivity is inaccurate because it doesn't provide a full view of an employee's work and contributions.

Less than a third of IT workers (32%) and IT managers (32%) feel an employee's direct line supervisor should have access to personally identifiable information (PII) collected using the

tech. Less than half of IT workers (44%) and IT managers (48%) think senior-level leaders like C-suite or division heads should have access to such PII, either.

Instead, nearly 9 in 10 IT workers (88%) agree employees should have access to their own data, reiterating the importance of transparency.

As IT professionals are responsible for safeguarding data, it stands to reason they believe they're trained and qualified in its handling: More than 2 in 3 IT workers (69%) and more than 3 in 4 IT managers (76%) feel IT staff should have access to PII collected using EPST.



“

*“It’s very likely that the perceived increase in productivity is actually an increase in ‘presenteeism.’ Other studies have shown that surveilled employees are more than two times more likely to pretend to be working, and spend an average of 67 minutes per day beyond their normal work hours so others see they are online. Acting productive and being productive are very different.”*

**Ian Greenleigh**

*Vice President of Brand and Communications, 1E*

## 2023 EPST SURVEY

# Conclusion

EPST is becoming extremely common, and the vast majority of those that don't currently use it are likely to do soon. But IT managers and their staff are uncomfortable spying on colleagues, and many would only do so after speaking up. Among the concerns are the negative impacts on their own well-being and that of employees, doubts regarding the accuracy of the data produced, the creation of talent management problems, and an erosion of trust in leadership and loyalty to the company.

Internal backlash could doom implementation from the start, as the vast majority of IT personnel would disclose its use to colleagues

and offer workarounds even if it violated company policy. With nearly half of IT managers who have been at their companies for 5 years or less viewing the technology as an invasion of privacy, the pushback appears likely to continue.

IT departments are now in a precarious position, and companies must decide whether the known risks of using productivity surveillance technology are worth the potential rewards.

***\*Small base size; findings are directional.***



## 2023 EPST SURVEY

# Methodological Notes

The 1E IT Workers and 1E IT Managers Surveys were conducted by Wakefield Research among 500 US IT workers, employed full-time in non-management roles, at companies of 500 or more employees, and among 500 US IT Managers, with a minimum seniority of manager, at companies of 500 or more employees, between February 16th and February 27th, 2023, using an email invitation and online surveys.

Results of any sample are subject to sampling variation. The magnitude of the variation is measurable and is affected by the number of

interviews and the level of the percentages expressing the results. For the interviews conducted in this particular study, the chances are 95 in 100 that a survey result does not vary, plus or minus, by more than 4.4 percentage points from the result that would be obtained if interviews had been conducted with all persons in the universe represented by the sample.

## About 1E

What if each digital employee experience (DEX) was better than the last? The 1E platform helps IT teams improve end user experience, tighten security, reduce costs, and evolve operations from cost center to strategic enabler. Over one-third of the Fortune 100 rely on 1E's single-agent solution with real-time automation and remediation for more visibility, control, compliance, and observability. Now, all operations teams can provide exceptional employee experiences, increase IT efficiency, and reduce service delivery time.

[1E.com](https://www.1e.com)

## About Wakefield Research

Wakefield Research is a leading, independent provider of quantitative, qualitative, and hybrid market research and market intelligence. Wakefield Research supports the world's most prominent brands and agencies, including 50 of the Fortune 100, in 90 countries. Our work is regularly featured in media.

[WakefieldResearch.com](https://www.wakefieldresearch.com)