



Shift Left: The IT leader's digital workplace maturity playbook

A practical guide to moving from reactive to predictive IT





Table of contents

(Clickable links)

00 · Introduction	
From digital workplace ambition to operational maturity	03
01 · The evolution of the digital workplace	06
02 · Why digital maturity stalls	10
03 · The maturity gap: Where digital friction persists	13
04 · Bridging the digital workplace maturity gap	17
05 · The shift left playbook	21
06 · Building experience-led IT organizations	26
07 · Conclusion	
The maturity journey	29



Introduction

From digital workplace ambition to operational maturity

Think your digital workplace transformation is complete?

You've invested in state-of-the-art collaboration solutions, endpoint management tools, and security infrastructure. You've embraced hybrid work and digitized essential workflows. On paper, your transformation looks complete.

But are your digital workplace improvements delivering measurable value? And when issues arise, what happens next?

The pattern is familiar: an employee experiences digital friction and opens a ticket; IT **reacts** with an investigation and eventual resolution. Even the most advanced tools will underperform within a strictly reactive operating model because this model exists to solve problems, not prevent them.

Friction inevitably returns, which impacts employee productivity, increases operational costs, and erodes confidence in IT.

This is the gap between digital workplace ambition and digital workplace maturity.

1.3

The average number of workdays per month employees lose to digital friction.



[The Impact of Digital Friction, 2025 Report](#)

We recently surveyed 750 IT professionals about their organizations' digital employee experience (DEX). Across six core DEX capabilities, the average maturity score is **17 out of 30 (57%)**. The typical organization creates repeatable processes, metrics, and training to promote digital workplace maturity, but many don't apply them consistently. Only a small minority reaches predictive capabilities.

This is the plateau many face: equipped with modern tools, making progress towards prediction and prevention, but still operating reactively by default. The next phase of digital workplace transformation requires IT teams to detect issues before they cause disruption, automate remediation, and continuously improve the digital employee experience.

In other words, **shifting left**.

This playbook shows what shifting left looks like in practice. Drawing on research and real-world insights, it outlines how you can move from reactive support to proactive and predictive IT.



57%

average maturity score across six core DEX capabilities

Shift left

DEFINITION

Shift left is a service strategy that moves issue detection, diagnosis, and resolution closer to the end-user—reducing reliance on higher-tier support and accelerating time to fix. In the digital workplace and EUC environment, shift left is enabled by better endpoint visibility, proactive monitoring, self-service tools, and automation, allowing Level 0/1 teams or even employees themselves to resolve issues that previously required specialist intervention.

This reduces ticket volume, lowers support costs, and improves the overall digital employee experience.



The evolution of the digital workplace

The evolution of the digital workplace

The digital workplace has evolved in distinct phases, each reshaping **how IT supports business**. And understanding this context is key in the journey to digital workplace maturity.

Infrastructure focused

The digital workplace was once defined by infrastructure. IT's role was to maintain devices, networks, and on-premises systems. Uptime, availability, and control were the measures of success. Employees worked within fixed environments, and behind the scenes IT kept systems running. When something broke, **IT stepped in reactively** to fix it.

Rising IT complexity

Cloud computing and SaaS applications marked the next major shift. No longer tied to a single location or device, employees could access tools from anywhere. Organizations rapidly adopted collaboration platforms, cloud services, and mobile device management.

This enabled hybrid work at scale and introduced **new layers of complexity**. IT environments were more distributed and became harder to manage through traditional, reactive approaches.

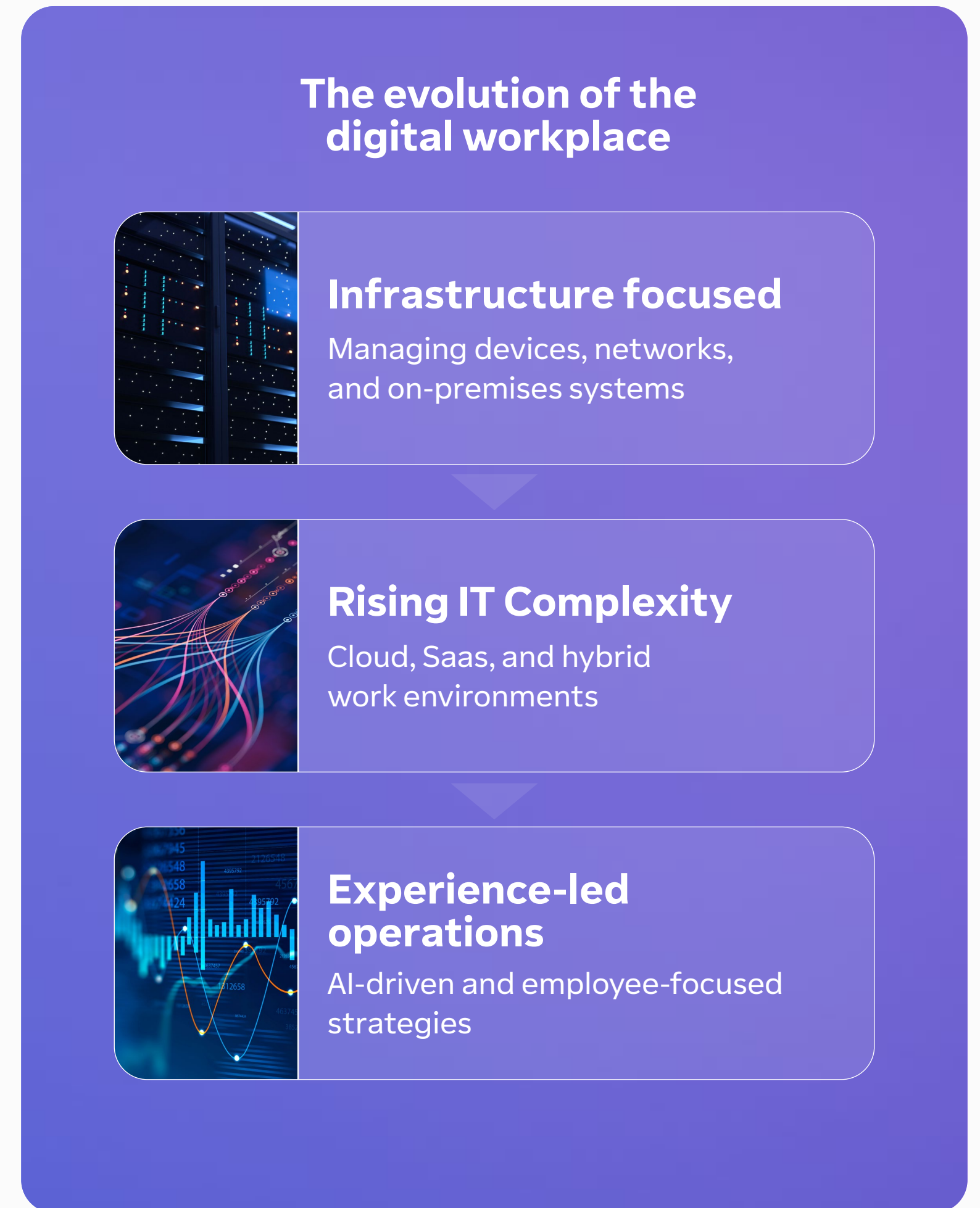
Experience-led operations

Today, the best digital workplaces are **experience-led operations powered by AI**.

Foward-thinking organizations are focusing on digital workplace performance: how effectively it operates, impacts employee productivity, and delivers measurable business value.

This reorientation allows IT teams to move beyond basic device management and fix-it tickets. They now have the power to shape experiences and drive their businesses to new heights of productivity, transformation, and growth.

DEX connects what IT delivers—devices, applications, connectivity, support—with how your employees experience technology in their day-to-day work.





When friction goes unmanaged

Digital friction doesn't stay contained; it compounds. As our 2025 [Impact of Digital Friction](#) report highlights, what begins as isolated technical issues can quickly escalate to other areas of your business:

“Approximately half (48%) of respondents report that digital friction caused delays in critical operations or projects within the last year, while 42% cite direct revenue loss and 37% say their organization has lost customers due to IT dysfunction.”

Left unaddressed, digital friction infects productivity, performance, and trust. Maintaining systems and reacting to problems isn't sufficient.

You need to actively monitor, maintain, and improve experience, and this is where digital workplace maturity comes in.

Impact of digital friction on business outcomes

● Agree ● Neutral ● Disagree

Digital friction has caused delays in critical business operations or projects



Digital friction has led to lost revenue at my company



Digital friction has caused a loss of customers or clients



[The Impact of Digital Friction, 2025 Report](#)

Why digital workplace maturity matters

In mature environments, technology, experience, and operations align to business outcomes. Employees can focus on meaningful work without disruption, IT operates proactively, and teams continuously measure digital experience, enabling AI adoption and innovation. The digital workplace becomes more than infrastructure. It becomes a performance engine for business.

This translates into tangible impact:



Maturity shifts the focus from managing tools to delivering outcomes, connecting technology performance directly to business value. And this evolution is fundamentally changing what organizations expect of IT teams.



Why digital maturity stalls



Why digital maturity stalls

After years of investing in modernizing the digital workplace, it's easy to believe that maturity naturally follows. Although some of the foundations may be in place, operating models must evolve to match. That's why maturity isn't defined by the tools organizations deploy. **We define it by how effectively the digital workplace operates.**



Andrew Hewitt, VP of Strategic Technology, TeamViewer

"The modern role of IT is to support digital workplace maturity by delivering exceptional digital employee experience, streamlining operations, and driving adoption of AI across the organization."

The 57% plateau

When we talk about digital workplace maturity, we see a clear plateau. Our recent survey of 750 IT professionals reveals that the average DEX maturity score is **17 out of 30, just 57% of maximum maturity.**

At this level, organizations standardize processes, deploy tools, and create repeatable workflows. But they aren't yet **proactive and AI-driven.**

Across every capability, the same pattern appears:

- 81% monitor DEX, but only **7% leverage predictive, AI-driven experience insights.**
- 91% provide support systems beyond phone and email, but only **8% use AI-driven, proactive support.**

- 82% offer workspace personalization options, but only **8% deliver AI-driven, adaptive personalization.**
- 81% go beyond ad-hoc DEX feedback collection, but only **15% use either predictive, AI-driven sentiment insights or embedded sentiment analysis.**

Efficiency:



The result is a ceiling effect, with IT teams suffering under:



Operational inertia

Processes designed for reactive support



Tool fragmentation

Multiple systems without unified insight or action



Siloed teams

Endpoint, service desk, and application teams operating independently



Reactive workflows

Resolving issues after disruption, not before

IT professionals describe environments shaped by repetition, fragmentation, and inefficiency.

“People and departments are too focused on their own goals instead of the common good.”

IT Manager, IT Services and Consulting industry

“It seems like fixing one thing breaks another, and it can be a constant dance to try and get things working together.”

Director IT Operations, Manufacturing industry

“I find the number of dependencies involved is frustrating. Progress often relies on multiple systems, teams, or approvals, which can slow delivery even when the solution itself is clear.”

Technical Support Engineer, Computer and Network Security industry

“One of the most frustrating things about working in IT is dealing with issues that are preventable but still keep happening—often because of limited time, budget constraints, or resistance to change.”

Sr. IT Support Analyst, Financial Services industry



The maturity gap: where digital friction persists

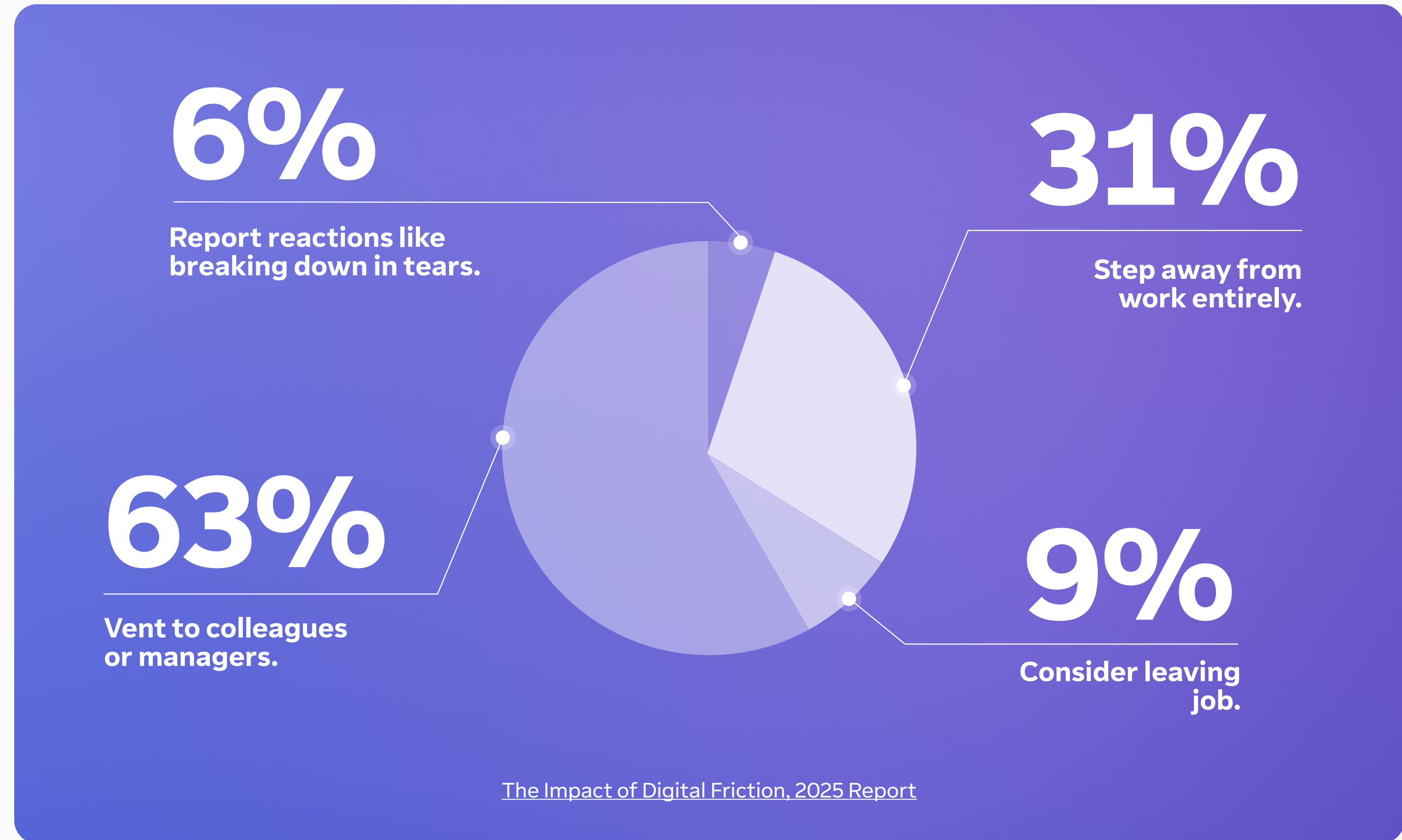
The maturity gap: where digital friction persists

Imagine starting your day with a simple task, joining a meeting or accessing a file, only for a slow device or failed login to obstruct you. Minutes pass, work stalls, and frustration builds.

When technology fails, employees feel it. Many vent to colleagues or managers (63%), some step away from work entirely (31%), and a small but notable percentage report reactions like breaking down in tears (6%). Nine percent even considering leaving their job.

These insights reveal that, despite progress in some areas, digital friction persists.

This is the maturity gap.




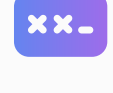




Understanding digital friction

Digital friction is any challenge with workplace technology that prevents your employees from doing their job efficiently, or in some cases, at all.

It occurs when systems, applications, or devices fail to perform as intended, disrupting workflows and limiting productivity. This can happen across any environment from office desktops and hybrid setups to field operations and industrial settings.

Our [Impact of Digital Friction report](#) highlights the most common types of digital friction:

-  Connectivity issues (88%)
-  Hardware failures (80%)
-  Software failures or crashes (82%)
-  Authentication problems (80%)
-  Unexpected software updates (85%)
-  Cybersecurity issues (66%)

Although individual issues may seem like minor or short-term inconveniences, their impact spreads, and the consequences are significant:

- Delays to critical projects and operations
- Lost revenue and missed business opportunities
- Increasing security and compliance risk
- Reduced employee productivity and engagement
- Erosion of trust in IT and digital systems

Where maturity breaks down

You can see the gap between digital investment and digital maturity clearly in day-to-day operations. Even in the most modern environments, disruption still triggers IT workflows.

This reactive pattern persists because **visibility, automation, and coordination** are still limited. IT is unable to identify issues early, and remediation often requires manual intervention. What this reveals is a lack of operational integration. Modern tools aren't yet working together to **anticipate and prevent issues**.

Digital friction creates business risk.
And in environments where IT
operates reactively, that risk
becomes systemic.

The operational and human cost

Reactive IT comes at a cost, both operationally and for the people behind the systems:

- **Increasing resolution times**, due to diagnosing issues after failure
- **Mounting support volumes**, with repeated and preventable incidents
- **Overwhelming IT resources**, limiting time for strategic work
- **Creating inconsistent user experiences**, reducing productivity and confidence

The human impact of reactive IT practices is just as clear too. As one IT professional explains, “one of the most frustrating aspects is being stuck in a reactive cycle. We often spend more time fixing repetitive issues manually rather than having the resources to implement long-term, proactive solutions that would prevent these problems from affecting employees in the first place”. Another states they’d feel more satisfied if they had “more time for strategic projects and improvements”.

This feedback reflects environments where IT is trapped in **cycles of firefighting**, rather than free to innovate and improve.

“We often spend more time fixing repetitive issues rather than having the resources to implement long-term proactive solutions...”

Director of IT Operations, Healthcare industry



Bridging the digital workplace maturity gap

Shift left: Bridging the digital workplace maturity gap

Bridging the maturity gap demands a fundamental change in how IT operates. And this is where the concept of **shift left** comes in.

Shift left is about IT identifying and addressing issues earlier, before employees feel friction, before they raise tickets, and—crucially—before they lose productivity.

Overall, this reflects a broader evolution in IT’s role. No longer confined to resolving incidents, today’s IT should anticipate needs, optimize experience, and support seamless work at scale.

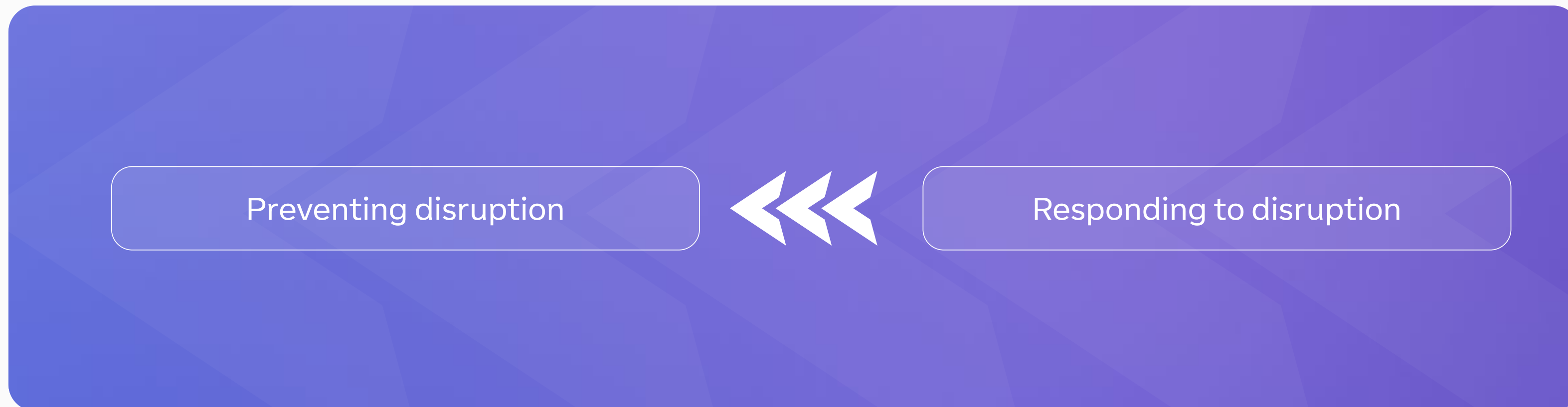
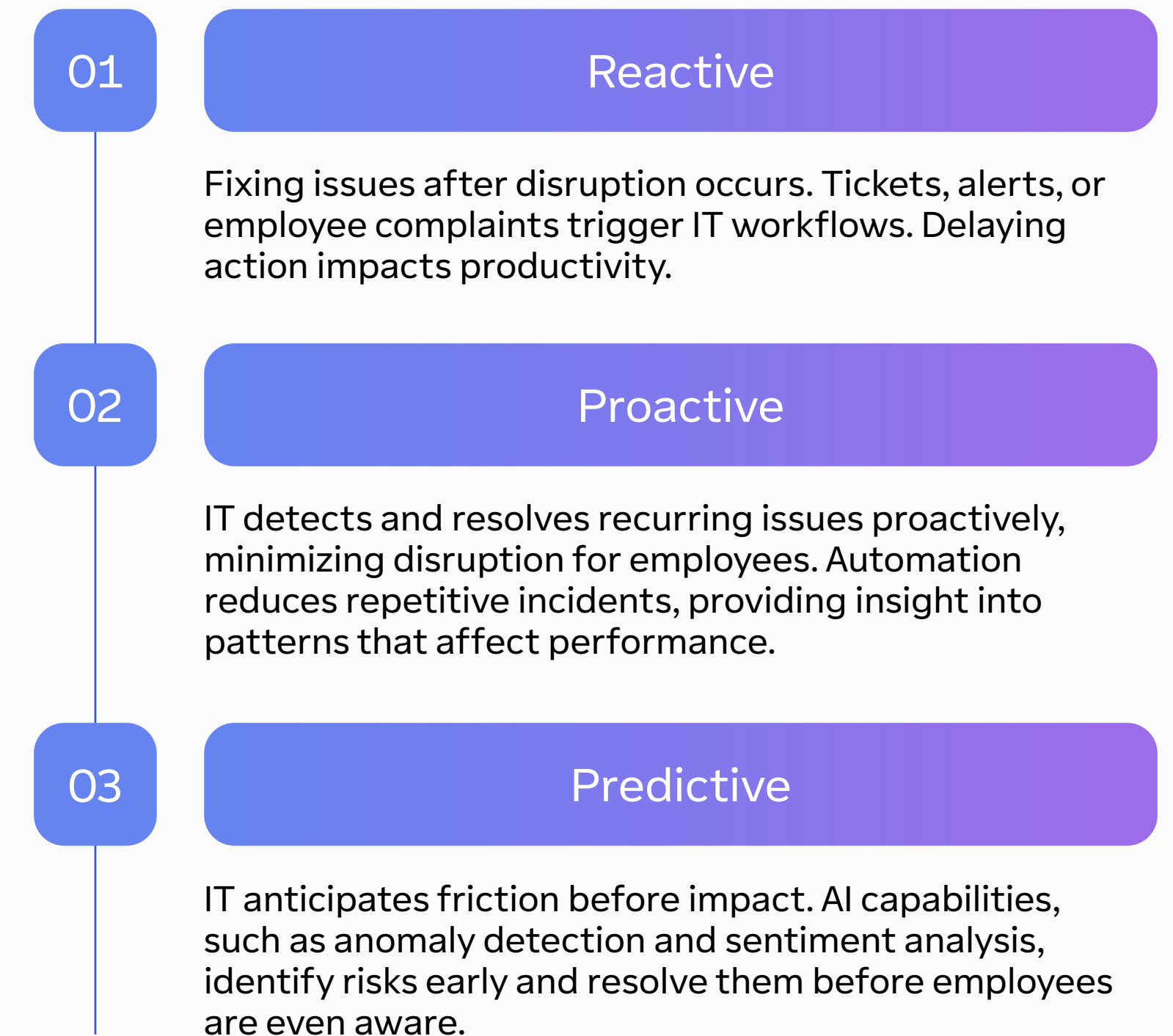
In practice, this means:

- Detecting issues before they escalate
- Automating remediation to reduce manual intervention
- Using experience and performance data to guide decisions
- Continuously improving the digital workplace environment
- Conducting in-depth interviews with employees to design the right experience from the beginning

In other words, shifting left is the strategic path to becoming **faster than friction**.

From reactive to predictive IT

Shifting left is a progression, where you move through three stages of maturity:



IT teams want to shift left

No longer satisfied with keeping systems running, teams want to eliminate recurring issues, reduce manual effort, and focus on higher-value work:

“I wish my IT team could automate more of our routine maintenance tasks.”

IT Director, SaaS and Software industry



“I wish our team had more time and resources to be proactive. It would help prevent problems before they affect users and make things run more smoothly.”

Sr. Manager IT Engineering, Government Administration



“I wish we could predict problems before they arise and know how to address them before they get out of hand.”

Head of IT Information Security Officer, Investment Banking industry



The push toward shift left is driven by real operational need, and our research shows that this movement is already underway. For example, we can see the adoption of proactive practices in the **22%+ using automated monitoring with alerts** and the **21%+ using automated remote support workflows**.

While predictive practices remain rare, typically in the 5-10% range across all capabilities, these figures indicate both the progress made and opportunity ahead.

The business case for predictive operations

The move toward predictive IT is a business advantage. As you shift left, you'll see the impact across multiple dimensions:

- **Employee productivity improves**, friction declines, and workflows remain uninterrupted.
- **IT efficiency increases** with fewer repetitive tickets and less manual troubleshooting.
- **Operational resilience strengthens** as you identify and address risks earlier.
- **Innovation capacity grows** as IT teams spend less time firefighting.

This shift also aligns directly with what IT professionals want: less repetitive work, more automation, and greater strategic impact.

Higher maturity creates the right conditions for IT to evolve from a reactive support function into a proactive, and even predictive, driver of business performance.

“Automation and efficiency improvements make the biggest difference.”

VP Information Technology, IT Services and Consulting industry



The shift left playbook

The shift left playbook

By this point, the case for shifting left is clear. IT leaders are under pressure to improve security and compliance, reduce operational costs, and deliver better digital experience—all while accelerating automation and AI adoption. At the same time, many teams remain stuck resolving preventable issues.

Shift left offers a practical path forward by addressing issues earlier in the lifecycle, reducing disruption, eliminating repetitive work, and creating space for IT teams to focus on strategic initiatives. The result is a more efficient, resilient, and experience-led operating model.

By following this path, you can systematically reduce repetitive manual tasks, eliminate common sources of digital friction, and improve employee experience at scale.

But shifting left isn't a single initiative. It begins with operational discipline, advances through intelligent automation, and evolves into predictive digital operations powered by experience intelligence. Each phase builds confidence, capability, and momentum, helping you operate proactively in a digital workplace that can't afford to be reactive.

This playbook outlines that journey across three phases: **stabilize and standardize, automate and optimize, and predict and prevent.**



**Stabilizing and standardizing operations
establishes trust and control**



**Automating and optimizing reduces workload
and accelerates resolution**



**Predicting and preventing issues eliminates
downtime and enables smarter, data-driven decisions**

Phase 1 Stabilize and standardize



Goal: Operational control

Phase 1 focuses on regaining control of the digital workplace foundation. Before IT can improve efficiency or employee experience, the environment must be secure, visible, and consistent. Without this baseline, automation and AI can introduce risk rather than reduce it.

The first priority is **endpoint visibility**. A real-time, data-driven view of your environment is vital to understand what devices exist, whether they're compliant, and how they're performing. This includes validating whether critical policies—such as encryption and compliance controls—are enforced, and functioning as expected. Visibility replaces assumptions with facts and helps IT to prioritize action based on impact.

Software integrity is equally important. Core management and security agents, such as Intune or SCCM, should be operational, and reporting reliably. When these agents fail silently, blind spots emerge. This undermines security, compliance, and confidence in data. Phase 1 ensures that these foundational components operate correctly.

Patching is another essential pillar of operational control. Many operate at partial compliance without full visibility. Phase 1 emphasizes benchmarking your patching posture with real-time data, and using that insight to prioritize remediation. Without secure and up-to-date endpoints, experience-led initiatives can't succeed.

Remote support standardization plays a key role in stabilizing operations. IT teams work to standardize remote support and access workflows, so employees can be supported consistently, regardless of location. This includes consolidating overlapping tools, reducing operational complexity, and ensuring remote access meets security and compliance requirements. The goal is to support hybrid work securely while eliminating gaps that increase risk. Even at this early stage, **AI adds value**. Instead of manually reviewing dashboards, you can use correlation analysis of telemetry data to surface compliance issues, identify emerging risks, and highlight top ticket drivers. AI-supported troubleshooting, including early use of agents like Tia (TeamViewer intelligent agent) helps resolve issues faster and focus human effort where it has the greatest impact.

Outcome

The outcome of Phase 1 is a stable, secure, and compliant **operational baseline**. You gain confidence by making endpoints visible, enforcing policies, and understanding risk. This foundation enables consistent support for your employees and prepares you for experience-led and AI-driven improvements in the next phase.

PHASE 1 CHECKLIST



Establish real-time endpoint visibility

- Monitor encryption, compliance, and policy enforcement
- Ensure coverage across all endpoints



Verify software integrity

- Confirm key agents such as Intune or SCCM are running and reporting
- Identify and remediate blind spots



Benchmark patching status

- Measure compliance using real-time data
- Prioritize patching based on risk



Strengthen security and compliance with AI insights

- Use telemetry data to identify gaps
- Surface top ticket drivers early

Phase 2

Automate and optimize



Goal: Reduce manual work

With operational control in place, Phase 2 moves focus from infrastructure to automation and digital experience improvement. The objective is to help IT become more efficient—with reduced manual effort, eliminated repetitive tasks, etc.—and improve your DEX through proactivity. At this stage, IT teams analyze where digital friction has the greatest impact. Instead of responding to incidents after disruption occurs, experience insights and ticket data pinpoint the most common and costly issues. This marks a clear shift away from maintaining systems to improving how they're experienced.

The first step is **identifying top ticket drivers**. Consider AI-powered tools, like TeamViewer Session Insights, to document all known issues. You can then look to telemetry to uncover issues yet to happen.

Automation is then applied deliberately. Rather than attempting broad automation, you should prioritize the three most common ticket drivers. These high-volume, repeatable issues are ideal candidates for automation. Teams can leverage existing automations and instructions or create custom workflows to resolve issues before they escalate or spread.

As automation maturity grows, attention shifts to **mission-critical systems**, for example homegrown apps, point of sale, and kiosks. These environments may require more upfront effort and customization, but the long-term value is undeniable. Automating key workflows improves reliability, reduces operational risk, and delivers lasting efficiency gains.

Establishing **digital experience benchmarks** is essential at this stage. By tracking experience metrics over time, you can measure improvement, monitor friction hotspots, and demonstrate the value of automation and AI investments. These benchmarks provide a clear, data-backed view of progress, and a foundation for continuous optimization.

Outcome

The outcome of Phase 2 is **proactive IT operations**. You can reduce repetitive work, improve response times, and give your teams more freedom to focus on higher-value initiatives. By embedding intelligence into workflows and prioritizing based on experience data, your IT aligns with employee needs and business priorities.

PHASE 2 CHECKLIST



Identify top ticket drivers

- Focus on issues with the highest employee impact



Optimize mission-critical software

- Identify systems with high automation potential
- Invest upfront for long-term gains



Deploy targeted automations

- Start with the top three ticket drivers
- Resolve issues before escalation



Establish digital experience benchmarks

- Track improvements over time
- Monitor friction hotspots

Phase 3

Predict and prevent



Goal: Anticipate friction before impact

Phase 3 marks the transition **from proactive to predictive** IT operations. While still emerging for many organizations, it represents the next stage of digital workplace maturity. This is where teams anticipate and prevent issues altogether.

The focus shifts to **continuous experience intelligence and AI-driven insight**. Instead of relying only on known issues, you can begin identifying unusual patterns and emerging risks before they affect employees. This supports a move from early resolution to prevention.

Predictive use cases include forecasting device failures, detecting gradual performance degradation, and assessing how planned changes, such as software updates, will impact different employee groups. These insights allow you to assess risk before acting—reducing disruption and improving confidence in decision-making.

As capability matures, **AI accelerates remediation**. IT teams can automate responses to emerging issues and, in well-defined and trusted scenarios, enable systems to act independently. This reduces manual intervention while maintaining control and oversight.

As autonomy increases, so does the need for **testing and validation**. IT can simulate changes, measure impact, and refine AI models based on real-world outcomes. This ensures predictive actions remain aligned with business expectations and don't introduce unintended risk. This phase is a gradual process. It means progressing deliberately, identifying where predictive insight can add value, and expanding from there.

Outcome

The outcome of Phase 3 is **predictive digital operations** that minimize disruption and build long-term organizational resilience. At this stage, you'll be able to anticipate friction, prevent downtime, and make confident, data-driven decisions. Employees benefit from more reliable, consistent digital experiences, while IT teams shift their focus from incident response to continuous optimization.

PHASE 3 CHECKLIST



Leverage AI insights for anomaly detection

- Identify unusual patterns and emerging risks
- Predict failures and performance degradation



Test and measure impact

- Simulate changes before deployment
- Refine models based on outcomes



Deploy AI-driven remediation

- Train AI agents for defined scenarios
- Reduce human intervention in routine issues

Together, these 3 phases form a practical shift left journey. By stabilizing first, automating next, and predicting over time, IT leaders can move intentionally toward an autonomous digital workplace that's efficient, resilient, and experience-led.



Building an experience-led IT organization

Building an experience-led IT organization

We've covered the technical path to shift left. But making it work at scale requires an organizational shift to an experience-first mentality.

In this mentality, experience is a core operating principle, shaping decisions, guiding investment, and influencing how work gets done across your business.

This experience-led approach can be seen through key distinct but complementary components: people, process, and technology.

People

Machines don't experience—only people do. Achieving shift left at scale requires rethinking how teams are set up, how leadership operates, and how you capture employee feedback and act on it.

01 | How you organize

Fragmented ownership often leads to fragmented experiences. For this reason, it's vital to move away from siloed ways of working. Teams like end-user computing (EUC), service desk, and applications need to coordinate. For example, through cross-functional ownership, dedicated DEX teams, or XMO (Experience Management Office) models. The aim is a cohesive all-in-one experience prioritizing shared employee journeys, not isolated systems.

02 | How you lead

Better leadership helps to enable shift left.

Taking responsibility for how technology shapes employee experience and, by extension, business outcomes. This involves elevating digital experience to a leadership issue: bringing experience metrics to leadership dashboards and focusing on driving adoption, rather than just deploying tools. This means putting employee experience at the very core of your business.

03 | How you listen

To improve an experience, you have to first understand how it feels.

[A recent study by Gallup](#) found that 20% of the world's employees experience daily loneliness. When it comes to employee experience, this clearly has a significant impact—and yet it won't appear in any dashboard.

While telemetry and analytics provide important signals, they don't capture the full picture. You must actively listen to and act on human experience. This should involve some formal listening capacity that allows employees to share feedback, alongside sentiment data and behavioral analytics. This is also where XMO models can help.

The most important thing is to make employee perception measurable and actionable. If you collect feedback but don't communicate follow-up actions, it can break employee trust quickly and permanently.

Process

At the process level, shifting left means moving from reactive support to proactive—and ultimately predictive—operations. This starts with designing better experiences upfront.

Early on, focus on reducing instability, shortening incident duration, capturing knowledge, and standardizing remediation. From there, automate workflows, use experience data to spot friction earlier, and apply **experience level agreements (XLAs)** to prioritize what matters most to employees.

At higher levels of maturity, processes evolve to anticipate issues before they happen and prevent disruption before employees feel it. In practice, that means **shift left workflows, automation pipelines, and experience-led prioritization.**

Technology

To support shift left at scale, you need a technology environment that is connected, scalable, and manageable, not a growing collection of disconnected tools.

Consolidate where it makes sense, integrating existing systems, and choosing **unified platforms** that create shared visibility across endpoint management, remote support, ITSM, security, and DEX.

Experience-led teams use technology with deliberate intention. They use telemetry and experience data to identify friction, guide investment, and support the transition from reactive support to proactive operations.

AI plays an important role here when applied to practical use cases like faster troubleshooting, anomaly detection, and automated remediation. Used in this way, technology maturity brings **more coherence, less complexity, and a stronger foundation** for predictive digital operations.

The future: Predictive digital operations

With this experience-led foundation in place, organizations can move toward predictive digital operations and identifying patterns even earlier.

The value is clear: **less reactive IT, increased capacity, and a more consistent digital experience.** This translates into higher productivity, stronger retention, and improved business resilience.

Closely tracking and responding to experience supports predictive IT. And by reducing repetitive work, predictive IT further improves employee experience. From there, we can also expect **more autonomous IT operations**, in which agents can act on their own. But we're not quite there yet.

For now, predictive IT is the most realistic target. And with predictive DEX technologies still sitting at just 5–10% adoption, the opportunity window remains wide open. The takeaway? The future of IT is predictive, and it starts with shifting left.



Conclusion



The foundations of the digital workplace are already in place. But as this playbook has shown, maturity isn't defined by what's been deployed. It's defined by **how effectively it operates.**

The gap between ambition and maturity is where **digital friction persists.** Closing that gap requires a shift in mindset as much as a shift in technology. One where IT moves from reacting to disruption to preventing it, from managing systems to enabling experience, and from supporting the business to shaping it.

Shift left provides a practical path forward, building control, unlocking efficiency, and enabling predictive, experience-led operations over time.

The opportunity is significant. Those who make this shift will reduce friction, improve performance, and elevate the role of IT as a driver of productivity, resilience, and growth.



TeamViewer provides a Digital Workplace platform that connects people with technology – enabling, improving and automating digital processes to make work work better.

In 2005, TeamViewer started with software to connect to computers from anywhere to eliminate travel and enhance productivity. It rapidly became the de facto standard for remote access and support and the preferred solution for hundreds of millions of users across the world to help others with IT issues. Today, more than 635,000 customers across industries rely on TeamViewer to optimize their digital workplaces – from small to medium sized businesses to the world’s largest enterprises – empowering both desk-based employees and frontline workers.

Organizations use TeamViewer’s solutions to prevent and resolve disruptions with digital endpoints of any kind, securely manage complex IT and industrial device landscapes, and enhance processes with augmented reality powered workflows and assistance – leveraging AI and integrating seamlessly with leading tech partners. Against the backdrop of global digital transformation and challenges like shortage of skilled labor, hybrid working, accelerated data analysis and the rise of new technologies, TeamViewer’s solutions offer a clear value add by increasing productivity, reducing machine downtime, speeding up talent onboarding, and improving customer and employee satisfaction.

The company is headquartered in Göppingen, Germany, and employs around 1,900 people globally. In 2025, TeamViewer achieved a revenue of around EUR 768 million. TeamViewer SE (TMV) is listed at Frankfurt Stock Exchange and belongs to the SDAX. Further information can be found at www.teamviewer.com.

www.teamviewer.com

TeamViewer Germany GmbH

Bahnhofsplatz 2
73033 Göppingen
Germany

TeamViewer US Inc.

5741 Rio Vista Dr
Clearwater
FL 33760
USA

Stay Connected

www.teamviewer.com