



Toolkit:

A phased approach to improving DEX

Practical steps for improving your IT and security operations while addressing digital employee experience goals





78% of employees say that they would be more productive if they had different technology at their disposal.

Introduction

Although the average knowledge worker might once have just grumbled about tech issues and managed as best they could, that's no longer the case. Employees expect a high-quality digital employee experience — and they're not shy about demanding it. According to survey results presented in the [2023 Digital Employee Experience report](#), 78% of employees say that they would be more productive if they had different technology at their disposal. Paying close attention to these shifting winds, organizations that want to attract and retain top talent are placing a higher priority on improving the technology experience they provide to their employees — also known as the digital employee experience (DEX).

IT would like nothing more than to rise to this challenge. If anything, today's IT pros relate to their colleagues' frustrations. According to the [2023 Everywhere Work Report](#), 22% of IT and security professionals surveyed say they are considering quitting their jobs in part due to the apps and tech tools they're required to use at work. Their jobs have become harder as the IT estate has rapidly grown and become more complex, with the volume of applications, services and user devices continuing to increase.

Pursuing a DEX initiative can seem overwhelming, especially given the many priorities your IT team is now juggling, but it doesn't have to be. You can move the needle on your digital employee experience by taking an incremental approach that supports your daily IT and security operations while also benefiting your long-term DEX goals.

Inside:

This toolkit provides you a step-by-step plan for launching a DEX initiative. It shows you how to take a staggered approach that instantly helps your IT and security operations, while steadily improving DEX over the long term.

Along the way, you'll learn how to create a DEX score that helps you measure your progress toward achieving your DEX goals. You'll also discover how to prove return on investment (ROI) at each step for your daily IT and security operations, so you can make an effective case for an investment in a high-quality DEX that benefits the entire organization.

This document is provided strictly as a guide. No guarantees can be provided or expected. This document contains the confidential information and/or proprietary property of Ivanti, Inc. and its affiliates (referred to collectively as "Ivanti") and may not be disclosed or copied without prior written consent of Ivanti.

Ivanti retains the right to make changes to this document or related product specifications and descriptions, at any time, without notice. Ivanti makes no warranty for the use of this document and assumes no responsibility for any errors that can appear in the document, nor does it make a commitment to update the information contained herein. For the most current product information, please visit [ivanti.com](https://www.ivanti.com)



01 **Step 1:** Understand what you have

02 **Step 2:** Connect patching data

03 **Step 3:** Automate IT workflows

04 **Step 4:** Track and continuously improve DEX

01

Step 1:

Understand what you have

To begin making gradual DEX improvements, you must first understand what you have in your environment. This includes discovering assets, as well as consolidating asset information in one place so it can be easily maintained. But because your IT estate is so complex, encompassing a huge constellation of endpoints, users, network infrastructure and edge devices, it's harder than ever to get a unified view of what you have.



Did you know?

48% of security professionals say they have low or moderate visibility into all assets on their network.

Discover Assets

The only way to actually get the complete and real-time visibility you need is to layer active and passive discovery together. This lets you see not just network switches, printers and other devices that are typically always connected, but also user devices that may be only intermittently connecting to your network.

With both active and passive discovery capabilities, you can easily see not just network switches, printers and other devices that are typically always connected, but also user devices that may be only intermittently connecting to your network. Enhancing your ITSM with information about all assets on your network means that your service desk teams can easily identify which device is the actual source of the issue and resolve the problem quicker.



360° Visibility

You can access useful information about the assets in your environment by enabling integration with other sources that may already have it, such as your endpoint management, IT asset management solution, or your purchase records system. At this stage, it's crucial to normalize and reconcile data between these data sets so that you can create a single source of

truth for all of your IT assets — for example, in a configuration management database (CMDB) or an asset management database (AMDB).

Using connectors to add crucial contextual information will help you understand why those devices are present on your network and even map out relationships and dependencies between them. Then, you can begin identifying your critical services and how they impact the digital employee experience.

The 360-degree view of all your assets enables you to proactively manage them. From this point on, when you discover new devices, you can more easily bring them under direct management, too. As we'll explore in more depth later in this guide, these process improvements will allow you to give your users a smoother support experience. You will also have the visibility needed to properly secure your assets, reducing the likelihood that threat actors will be able to compromise them without your knowledge.

“Customer hired eight engineers to build a solution to reconcile data sources (SCCM, ServiceNow, purchasing records, internal database). Discovered that they had 70K devices that were not properly accounted for across their data sources.”

- Fortune 20 Organization



“To be able to pull this detail from one system moving forward will help our department be much more transparent to our customers AND make it easier for them to request assets. Overall, our goal is to minimize both losses and inefficient processes.”

City of Seattle

Measure investments

Understanding what you have unlocks ROI in other ways, as well. For example, with instant access to information on the warranty status of your assets, you can avoid spending money on battery replacements that are already covered by a warranty or optimize spend for hardware refresh by analyzing device performance. These insights can help you make smarter decisions on whether to re-image or replace workstations, while analytics on application use shed light on what applications employees are actually using, so you can save money and devote IT support resources to where they are needed most. Ultimately, your service desk will be empowered with insights that enable quicker and better issue resolution, leaving users with a better digital employee experience.

“We have seen and will continue to see significant savings in asset and warranty management, by proactively monitoring device health, such as battery performance, Ivanti gives us real-time actionable intelligence, so we can automate or make more informed decisions and keep our users productive.”



[Kingston University](#)





How to prove ROI for immediate and long-term goals

Getting a complete understanding of your entire IT estate is the first step to improving both your day-to-day IT and security operations, as well as your long-term digital employee experience. There are a number of benefits from taking this step and a variety of KPIs you could set to prove the ROI. Here are the main ones:

	Benefits	Potential KPI's
 Daily IT & security operations perspective	Transparency of complete IT estate and risk surface in a single place	Asset usage, health and performance
	Optimized cost of IT device management and maintenance	Spend on applications and cloud subscriptions
	Improved compliance and asset lifecycle management	Changes in the IT environment
 Long-term DEX perspective	Clear baseline for device performance	Inventory and usage
	Defined indicators to track asset health & usage	Device status and performance
	Easy monitoring of degradation over time	System failures

Step 2:

Connect patching data

As the IT estate has rapidly expanded, IT has found it even harder to carry out proper change management. This expansion has also created a tempting attack surface for malicious actors to target. Meanwhile, cyber threats have become more sophisticated and severe, putting the organization at increased risk.

Obviously, IT and security teams can't afford to take their eye off the ball when it comes to security. But the age-old trade-off between security and flexibility persists to this day — while IT seeks enhancing user productivity and operational efficiency, security teams put compliance and protection against breaches above all. Rather than keeping these two organizational priorities in tension with one another, it's time to balance DEX and security. The secret to doing so lies in getting the necessary visibility and understanding of your environment, so you can improve security and DEX in tandem with one another.

Every organization needs to continuously identify risks, prioritize what needs to be updated and then push the necessary changes out to the environment. This is especially true when it comes to keeping employee devices up to date with patches. Patch management isn't just about security; it has a direct impact on the digital employee experience, as well.

When IT pushes out patches, they often become the target of blame for the next couple of weeks, as users assume all of their DEX issues were caused by the latest patch. If the IT team doesn't have visibility into what's going on in this area, as well, the organization as a whole — employees and IT alike — will suffer a productivity hit whenever it's time to issue a patch.



Did you know?

85% of C-level executives agree that poor digital experiences lead employees to use unsafe workarounds.



Link patching data

You can resolve this chronic pain point by incorporating patching data to your DEX view. First, connect your [patch management](#) to your ITSM platform and then augment the relevant asset information so you have all the insights you need in one place. Now, your team can not only access asset information but also gain further context as to whether an issue is with the device or caused by the change in the environment and is likely to affect other users, too.

Evaluate patch cycles

Once that is done, you can actually [evaluate](#) how well patch cycles are going within your organization, beginning with a small pilot group. When your DEX information is readily available to your service desk, you can actually see whether users in that pilot group are opening tickets and, if so, whether those tickets are related to any of the updates that just took place.

With stability and performance data that you have already collected, your IT and security teams can easily and proactively determine whether your users are encountering crashes or other performance issues — all without having to manually gather this information. Given that [29%](#) of IT professionals cite collaboration as a priority, it's worth noting that this step can help bring your IT and security teams' goals closer together.

Integrate DEX with GRC

Now that you have visibility into how your patches are affecting your users, you can handle the change management aspect of the patching process much more efficiently. You can even leverage DEX to [advance your strategic security initiatives](#). For example, you can integrate your DEX data with your governance, risk and compliance (GRC) within the IT service management (ITSM) system. These integrations make it much easier to implement best practices like a change advisory board (CAB), which approves patches before they are rolled out organization-wide.



“The visibility and automation provided by Ivanti Neurons for Patch Intelligence saved SouthStar Bank several days a month researching and resolving vulnerabilities.”

[SouthStar Bank](#)



Did you know?

A proactive risk-based vulnerability program can reduce an organization's data breach incidents by 80%.



Gartner

[“Implement a Risk-Based Approach to Vulnerability Management”](#)



How to prove ROI for immediate and long-term goals

Having your patch data connected to your service management processes and tools is hugely supportive of improving your daily IT and security operations, all while helping you enhance the long-term digital employee experience. Here are the main benefits and potential KPIs to prove the ROI to your organization:

	Benefits	Potential KPI's
 Daily IT & security operations perspective	Reduced productivity loss from security vulnerabilities	Cost of lost productivity per out of date device impacted by security risk/malware
	Reduced risk of shadow IT	Number of out of date devices potentially impacted by security risk/malware
	Improved risk compliance and change management	Volume of approved patch cycles
 Long-term DEX perspective	Users don't have to think about security in the EW because everything is underpinned by sec.	Number of devices out of compliance
	Reduced interruptions caused by security incidents	Business user productivity opportunity cost per security incident
	Reduced change impact on users and IT employees	Number of IT support calls related to security

Step 3:

Automate IT workflows

When your employees have trouble using the technology they rely on to get their work done, organizational productivity takes a hit. Each user runs into 3.67 digital experience issues per day on average. Each time they do, it takes them up to 20 minutes to regain their focus. If they submit a ticket, then your limited IT resources must be mobilized to help them get back on track as soon as possible. By automating IT workflows that touch on the digital employee experience, you can get out in front of this recurring problem and save everyone time.



Did you know?

48% of office workers prefer to fix their own tech problems when possible.



Streamline service desk processes

IT service desk automation delivers especially high business value when it comes to the digital employee experience, helping your IT support organization shift left and begin leveraging self-healing capabilities to solve problems before users even notice them.

Meanwhile, convenient self-service tools allow users to address straightforward problems on their own, lowering ticket volume even further while improving their DEX. For tickets that require expert attention, automatic ticket classification will make sure that it is assigned to the right member of the IT team, removing yet another task from the IT “to-do” list.

Shift Left

Automation gives your team great opportunities to not only keep up with increasing ticket volume but also to shift left, reducing costs and risks. With the combined capabilities of artificial intelligence (AI), machine learning (ML), sensors and automation, you can consolidate all of the tools and processes your IT team uses for remediation on a daily basis.

This allows first-line analysts to resolve issues that would otherwise have been escalated to specialists. As a result, your employees will get their problems solved more quickly and your organization will enjoy increased productivity. And to help evaluate the actual impact on DEX, AI-driven automation bots can automatically survey your employees, so you’ll never be in the dark when there are lingering areas that still need improvement.



\$716.6K Savings
from self-service onboarding/
automated provisioning.

“Ivanti Neurons enables what I call ‘contactless intervention’ and you can create ‘custom actions.’ As part of this, we needed to determine if we wanted to solve small problems continuously or let small problems solve themselves, which would let us get to the big stuff.”

SouthStar Bank

Prevent issues

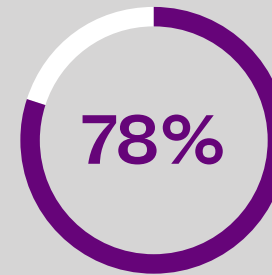
You can use automation to perform preventative maintenance and proactive monitoring. Look out for issues that could affect the user if they were allowed to get worse, such as hard disks that are running out of space or CPUs that are overheating because their fans are blocked. If the problem has already begun to affect the user, your IT staff can still use self-healing bots to automatically collect as many insights as possible about the issue, run the appropriate tests, and give the analyst a head start on remediating the glitch as soon as they pick up the ticket.



\$560.5K end user productivity savings
from self-healing environments.

Enhance the employee DEX

By automating these IT workflows, you can embrace a shift-left approach to IT service delivery that reduces the degree of IT intervention required on a regular basis and gives your users a better digital employee experience. Not only will employees encounter fewer issues to begin with, but the problems they do run into will be fixed much faster. When their workplace technology is running smoothly and they're able to focus on the task at hand, they'll be more satisfied with the technology at their jobs and more likely to stay at the organization.



78% of knowledge workers say they could be more productive with different tools.

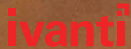


Enhance DEX for IT

IT also benefits from these automations in the form of reduced ticket volume, an accelerated mean time to resolution, increased first call resolution and a better ROI on the staff time that is devoted to resolving the tickets that do come in. As these key performance indicators (KPIs) steadily improve, your senior analysts and IT administrators can dedicate their expertise toward strategic IT advancements, ultimately transitioning your IT organization from a reactive posture to a proactive one — all while enhancing the digital experience for your IT team.

“Ivanti Neurons is a game changer for us. We will have the ability to proactively create an incident then auto-remediate the issue before our employees even know there is a problem. This is how IT earns respect and how we become a proactive IT organization!”



Technical Services Team Lead
Global Manufacturing & Distribution Facility





How to prove ROI for immediate and long-term goals

Automating your workflows brings great efficiencies to your daily IT and security operations and helps improve digital employee experience for both your users and IT teams. Here are the main benefits and KPIs that can help you prove the ROI for your organization:

	Benefits	Potential KPI's
 <p>Daily IT & security operations perspective</p>	Accelerated issue resolution	First-call resolution & Mean-Time to Repair
	Reduced cost service desk	Ticket & escalations volume
	Reduced resources spent on routine incidents resolution	Ticket avoidance / deflection & volume of self-healed incidents
 <p>Long-term DEX perspective</p>	Improved productivity	Time saved on issue resolution
	Improved service desk experience	Urgency and priority of issue
	Reduced digital friction	User sentiment & satisfaction (NPS)

Step 4:

Track and continuously improve DEX

In addition to making incremental improvements to your DEX that improve daily and IT security operations, it's also important to set your organization up for long-term success. Accordingly, consider leveraging DEX-specific solutions that can help you advance DEX in the long-term and inform your broader, strategic decisions.

Our research shows that 17% of knowledge workers either have quit or would consider quitting due to poor tech — and the figure is nearly 2x as high for Gen Z. When technology becomes vital in retaining and attracting talent, continuous improvement of DEX needs to get on the priority list of not only IT but the organization overall.

What's an XLA (experience-level agreement)?

XLAs set the standards for DEX and help organizations better measure satisfaction. They evaluate how technology improves (or hinders) employee experiences.

What is a digital employee experience (DEX) score?

A DEX score is a quantification of the overall level of satisfaction that employees have when engaging with each application, system, service or device.



Did you know?

56% of IT professionals say they don't have a high level of buy-in from the C-suite for DEX initiatives.

Introduce XLAs

Start understanding the success of your DEX program by implementing an experience-level agreement (XLA) within your IT team. An XLA will help you measure user satisfaction on a continuous basis, not just a transactional one. Although your team may already be working with SLAs, XLAs will enable you to focus on employee happiness and productivity, rather than only availability and responsiveness. Plus, you will be able to benchmark the real-world experience of actual end users instead of just tracking the performance and availability of assets.

Create a baseline

Keep adding to your DEX score over time. That will give you a baseline understanding of where you're at, so you can keep track of how you're doing and make timely course corrections if needed. This approach provides you a more comprehensive view of your organization's DEX, including device health, application health network performance, and security health. It also monitors key aspects of the service experience that affect your DEX, such as the number of open tickets, their severity levels, their age, and even the user sentiment (i.e., the language used and frustration level it expresses) associated with them.



"Upon implementing an ITSM that enabled a better DEX, the IT department at Victoria University saw their NPS jump from around 54% to 60% to 90%."

Victoria University

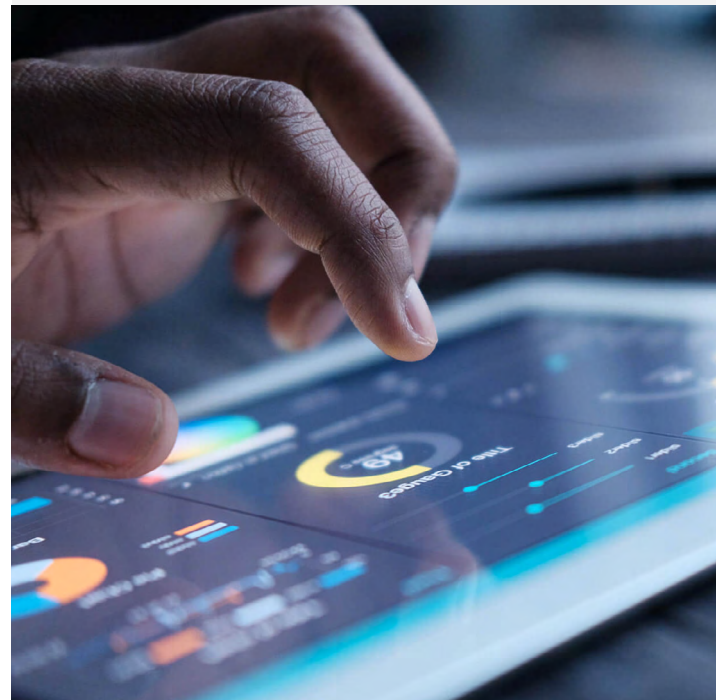
Monitor DEX over time

Once your baseline DEX score is in place, you'll have a much better understanding of what's normal and what's anomalous. With that insight, you will be able to monitor employee sentiment — and you'll be able to take action when it begins to dip. You'll also have better visibility into your overall tech stack performance and typical usage of your assets (for example, normal CPU usage and disk consumption). This way, you can more readily spot something irregular that warrants further investigation.

Ultimately, with the awareness gained from monitoring your DEX, you'll also have the understanding needed to make smarter investment decisions. For example, if the same disk consumption problem starts appearing among all laptops from the same vendor, you may decide to re-evaluate your contract or consider other providers.

Leverage real-time operational intelligence

From there, you can take a further step toward becoming even more proactive by leveraging the real-time operational intelligence that's reflected in your DEX score. This way, you can surface insights from the platform that will enable you to adopt a more sophisticated approach to DEX management. With all of these improvements in place, your IT team will eventually be able to spend the balance of its time focusing on strategic IT and security priorities.



Continuous improvements



Now you are on the path of continuous improvements. Define, commit to, continuously measure and improve both quantitative metrics associated with the performance of digital technology and qualitative measures that capture overall employee satisfaction, digital adoption, and help desk experience to measure satisfaction on a continuous basis.

Start using DEX data to support broader organizational strategic decision-making. Partner with procurement to help inform technology investments across the business or with HR to support their employee retention initiatives. Leverage DEX to elevate IT's role to a strategic business partner level in your organization.



How to prove ROI for immediate and long-term goals

The final step in optimizing your digital employee experience allows you to continuously improve by using the vital DEX insights for evaluating and making strategic decisions about both your daily IT and security operations and DEX program. Proving ROI to the organization is critical at this stage, so here are the main benefits and KPIs to help you with this:

	Benefits	Potential KPI's
 Daily IT & security operations perspective	Proactive IT	DEX score
	Improved IT & security maturity	Optimized technology spend & Improved security posture
	Sustainability / Green IT	IT carbon footprint & energy consumption
 Long-term DEX perspective	Transparency of DEX program adoption	XLAs
	Employee engagement	CSAT scores
	Talent retention	Attrition rate

Conclusion

If you find the prospect of a DEX initiative overwhelming, that's understandable. DEX can seem daunting at first, especially when you're already balancing the security and operational requirements of a rapidly growing IT estate with the mandate to provide a digital employee experience that drives productivity and job satisfaction.

However, rather than handling DEX like a massive, all-encompassing undertaking, think about what you're already doing now, where you could be doing better and how you can apply a staggered approach to your DEX improvements. This process begins with **understanding what you have** in your IT environment, then **connecting patch data** to enable better change

and security management, then **automating your IT workflows** so you can embrace a shift-left perspective and finally **continuous improvement** that allows you to steadily inform strategic decision-making across the organization.

The journey will take time and careful planning, but the effort will be well worth it. With proper visibility into the digital employee experience, you won't have to guess at the root causes of issues impacting your users anymore. Efficient patch management will alleviate a major recurring pain point for users and IT alike, strengthening security in the process.

As you gradually continue implementing your DEX improvements, the benefits will begin to compound, giving you substantial forward momentum. Automating IT workflows will allow you to resolve issues before users even notice them, all while giving your first-level analysts the context they need to quickly address the tickets that do come in without having to escalate them.

At this stage, your KPIs will improve, IT will earn more trust from its colleagues throughout the organization and your IT leadership will have increased flexibility to pursue higher level strategic priorities. Finally, by establishing a comprehensive baseline for where you're at and where you want to go, you will have a full set of powerful tools and continuous improvement processes in place for proactively managing the digital employee experience, no matter what technological transformations and evolving trends await your organization in the future.



Toolkit:

A phased approach to improving DEX

Practical steps for improving your IT & security operations
while addressing digital employee experience goals



[ivanti.com](https://www.ivanti.com)

1 800 982 2130

sales@ivanti.com