EMA

IT & DATA MANAGEMENT RESEARCH,
INDUSTRY ANALYSIS & CONSULTING

Evolving Requirements for Digital Experience Management (DEX)

July 2022 EMA eBook
By Steve Brasen

Prepared for

ivanti

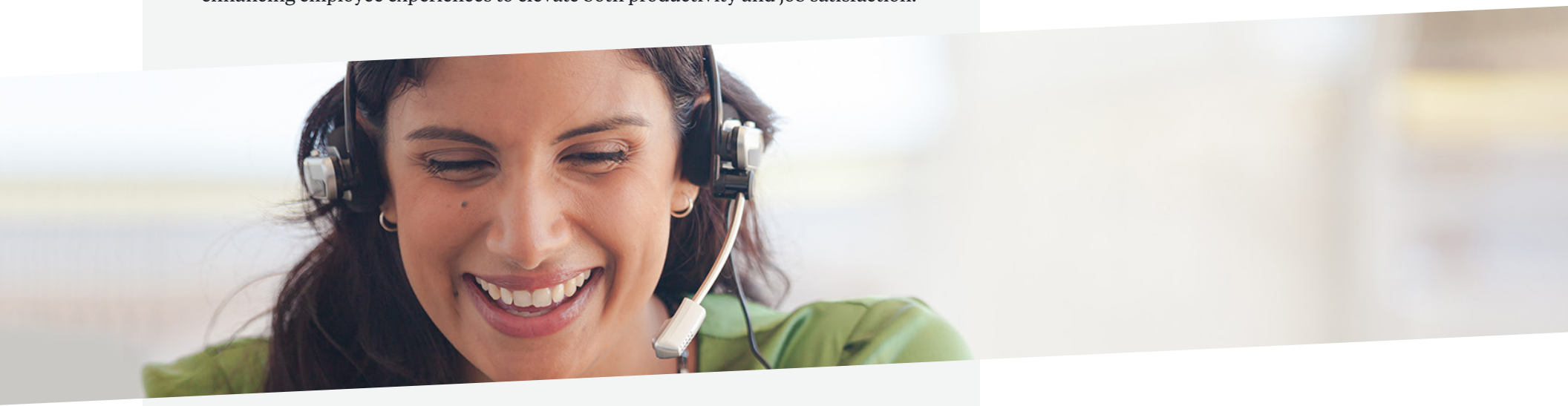
Table of Contents

Embracing Modern Management Theory

Over the past few years, businesses have reassessed embracing user-centric approaches to IT. In particular, the "modern management theory" postulates that job satisfaction predicates workforce productivity, rather than financial compensation. Applying this principle to the present day, use of IT requires digital technology to serve the workers, rather than the other way around.

Today, the type and usability of the technology businesses offer to employees are chief factors for attracting and retaining a talented workforce. According to research conducted by IT management solution provider Ivanti, 41% of businesses they surveyed reported they had lost IT workers because they were unhappy with having to perform excessive workloads. Rather than focusing on delivering "user-centric" technology that solely targets the goal of making workers productive,[1] modern management approaches address the broader goal of enhancing employee experiences to elevate both productivity and job satisfaction.

Increasingly, businesses are defining specific requirements for improving employee experiences through digital transformation and modern management toolsets. These objectives are either added to existing service-level agreements (SLAs) or independently documented in experience-level agreements (XLAs). Emerging trends in IT management clearly indicate that enterprises are focusing on enhancing employee digital experiences to address today's most compelling technology challenges.



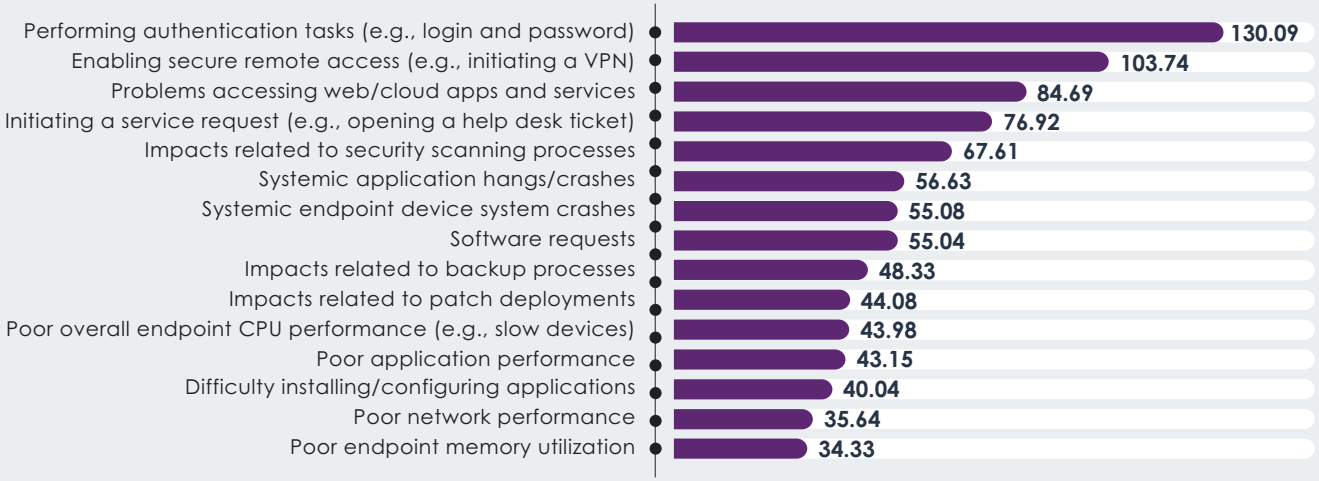
[1] Top IT Trends for the Everywhere Workplace, 2021

Digital Experience Inhibitors

The importance of managing employee digital experiences is easily quantified by evaluating the sheer number of events that impact workforce productivity. On average, workers who regularly employ digital technology to perform job tasks are affected by an endpoint management challenge 919 times per year, which translates to about 3.67 issues per business day.[2] Each of these disruptions can have a cascading effect on employee performance. Any time a user is distracted from performing a job task, it can take as much as 20 minutes for them to refocus back on their job function after the issue has been resolved.

The high frequency of employee experience impacts also reduces the effectiveness of IT administrators. On average, 40% of business workers contact enterprise help desk support each week regarding a digital experience issue, unnecessarily overburdening support personnel and increasing the overall cost of IT operations. Even worse, many workers will forgo contacting help desk support and instead ask an unqualified peer for a workaround that may actually further reduce their productivity. In that case, the root cause of the disruption is never discovered, and incidents are doomed to repeat until someone informs an actual IT administrator of the problem.

Business employees suffer a wide variety of productivity-impacting issues. However, the most frequently experienced are related to meeting security requirements, such as access authentication, initiating VPN connections, malware scans, and patch deployments. Also frequently encountered are difficulties accessing cloud-hosted SaaS and web services.



Average number of times per year each user suffers digital experience issues, according to surveyed businesses

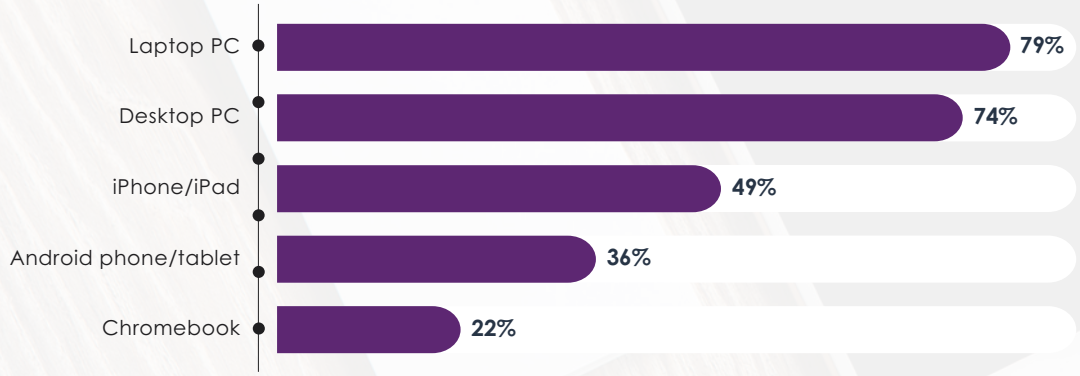
[2] Identifying Effective Digital Employee Experience (DEX) Management Solutions: A Quantitative Analysis, 2021

Employee Experiences in a Multi-Device World

Business employees who are required to utilize digital technology as part of their job function today employ, on average, 2.6 different devices, including desktop PCs, laptops, smartphones, and tablets.[3] To be productive, they need to be able to access and use business IT resources in a consistent manner across all of the devices they utilize—regardless of whether they use them frequently or periodically. However, ensuring this seamless experience may prove challenging given that unique form factors for each device (such as screen sizes, input devices, and operating systems) require different user interactions.

The methods used to acquire and access different applications and IT service also vary greatly, depending on the type of device. Some users may download resources via apps stores or business app portals, while others can utilize SaaS, web, or virtual apps. Ultimately, the device types and configurations must accommodate individual user preferences.

Percentage of survey respondents indicating the types of devices they use to perform job tasks



The broad variety of endpoint device configurations makes consistent and centralized management of user experiences across all employee devices difficult. Typically, this is because administrators lack holistic visibility across all devices, inhibiting their ability to correlate device states and user activities. To accurately assess user experiences, organizations should identify and remediate any problems, performance degradations, and seek opportunities for improvement consistently on all devices in real time. Features supporting unified endpoint management (UEM) that include strong cross-platform support that is centrally managed greatly enhance DEX solutions.

[3] EMA Contextual Awareness Research Report, 2020

Supporting the Everywhere Workplace

Responding to workforce pressures and business continuance requirements during the COVID-19 pandemic, organizations have substantially increased support for the performance of work tasks outside of the physical office. Today, 91% of business workers who utilize IT services perform at least some of their job tasks at home or at other remote locations.[4] Only 9% of business employees have returned to the office full time, while another 9% are now working from home full time. The majority of workers (82%) are employing a hybrid approach, performing tasks both in and out of the office. On average, 47% of business tasks are now performed outside of the physical office.

Having been introduced to the "Everywhere Workplace" benefits during the pandemic, most workers are reluctant to ever return full time to a physical office. According to Ivanti's research,[5] more than 87% of business employees prefer the flexibility of being able to perform job tasks outside of the physical office, while 71% noted they would prefer the ability to work from anywhere over receiving a promotion. Additionally, many respondents indicated they have achieved significant personal benefits as a result of being able to work remotely, including:

43% reported improvements to their work/life balance

40% reported saving money as a benefit

48% reported that the reduced commuting time gave them more time to perform work and personal tasks

Today's workers require—and often demand—the same digital experiences operating remotely as they encounter when they are physically in the office, such as easily accessing systems and IT services. This requires the ability to operate fluidly over non-business networks (including private and public Wi-Fi and internet services) without having to deal with delayed or dropped connections. Network connections are particularly essential for enabling remote communications, such as to support video conferencing.

When workers operate remotely, it can also be challenging for administrators to troubleshoot, remediate, and perform maintenance on their devices. Employees should be able to expect the same level of support services regardless of their physical location. Similarly, businesses must meet continuous requirements for security and compliance on company devices and any time they are communicating with business-hosted services.

[4] Identifying Effective Digital Employee Experience (DEX) Management Solutions: A Quantitative Analysis, 2021
[5] Everywhere Workplace Report, 2022

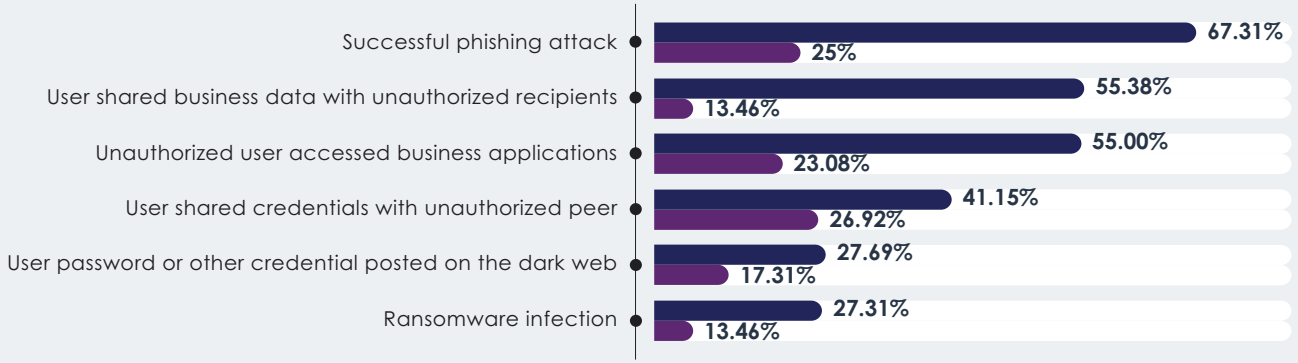
Impacts of Security on Employee Experiences

Ironically, one of the most overlooked impacts to employee digital experiences is also the most disruptive. Organizational requirements for security are constant distractions for users and performance drains on endpoint devices. Typically, organizations view security and employee experiences as diametrically opposed forces—as you increase one, you decrease the other. Based on this perspective, most businesses choose to enforce security over enabling a productive workforce. However, EMA research indicates that a reduction in security friction results in significantly fewer breach events.[6]

Security concerns are certainly warranted, and breach events can significantly inhibit workforce performance. For instance, malware infections and ransomware attacks can damage devices and prevent access to critical resources. Browser cookies and malicious software can also coopt endpoint devices to perform unauthorized tasks (such as cryptojacking), reducing their performance. Once a device or employee account is compromised, it can be very disruptive and time-consuming to remediate, particularly if it requires a full system recovery—not to mention damaging to business reputations and finances. Security breach events can also take an emotional toll on workers by adding stresses that impact their productivity. It is therefore important to recognize that preventing security breaches is itself a method of improving employee experiences.

Unfortunately, many common security management processes are also very impactful to the performance of day-to-day work tasks. High-friction authentication processes (e.g., passwords, 2FA OTPs, etc.) inhibit access to key business resources. Network tunneling tools (such as VPNs) are often cumbersome to use but are required to gain secure access to business systems. Additionally, security patch deployment processes and malware scans degrade endpoint performance and may force system reboots.

To ensure security with minimal disruption to employee experiences, policies and automated processes must be adaptable to work around legitimate end-user business requirements.



Comparing the percentage of surveyed organizations experiencing security breaches in the preceding 12 months between those with high-friction and low-friction access security processes

[6] EMA Contextual Awareness Research Report, 2020

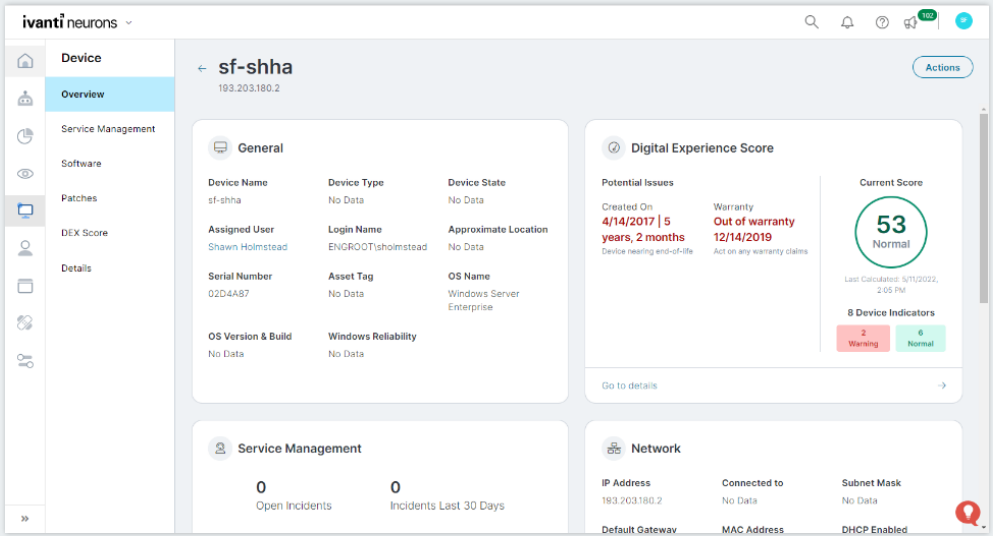
Identifying Solutions for Success

The greatest challenge with introducing an optimal DEX solution is addressing the breadth of requirements across the four key areas of support. Most DEX platforms on the market today focus their management strengths on just one or a few areas of key functionality, such as monitoring, analysis, or automation. Gaps in offered DEX solutions are typically addressed by relying on points of integration with third-party products or the development of custom automation scripts. However, the DEX platforms that will most effectively meet a business's unique requirements are those that will equally and natively support key functionality across all four pillars of support. A unified approach to DEX is easier to deploy and maintain, while also more rapidly achieving returns on investment.

The evolving business requirements for managing employee digital experiences can only be achieved with a unified DEX platform that provides core functionality for monitoring devices, determining employee sentiment, analyzing conditions, and automating effective responses. As an example, the Ivanti Neurons suite of management solutions offers a comprehensive and unified portfolio of DEX functionality. Real-time visibility into devices, users, applications, and IT services, coupled with flexible employee sentiment surveys, means Ivanti Neurons provides unified visibility of both objective and subjective employee experience states. Collected information is analyzed and calculated into a standardized user experience score, and the included "Smart Advisors" provide prebuilt charts on device and environment conditions while offering actionable guidance on improvements and remediation actions.

Ivanti Neurons provides fully automated remediation functionality. Self-healing scripts, called "bots," run on demand or continuously in the background to perform tasks for correcting performance issues, making configuration changes, and implementing environment improvements. While the platform includes an extensive library of prebuilt bots, it also provides an easy-to-use, low code/no code tool for creating custom bot workflows.

Ivanti's DEX functionality is also fully extensible, enabling integrated support with other Ivanti management technologies supporting unified endpoint management (UEM), patch management, service management, and spend intelligence. A library of connectors is also provided for integrating directly with third-party management solutions, such as ServiceNow, and custom integrations may be created with the use of the provided REST API.



About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help EMA's clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals, and IT vendors at **www.enterprisemanagement.com**. You can also follow EMA on **Twitter** or **LinkedIn**.

1995 North 57th Court, Suite 120, Boulder, CO 80301 +1 303.543.9500 **www.enterprisemanagement.com**

4190.080122