eG Innovations

Transforming Digital Employee Experience for Modern Enterprises

A Unified, Top-Down Approach to Monitoring, Optimizing, and Elevating Employee Productivity with eG Enterprise

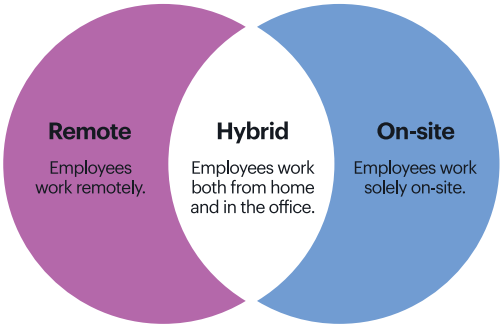
WHITEPAPER

Enhancing Employee Experience is Now a Business Imperative

For decades, enterprise IT strategies were primarily oriented toward serving external users — customers, partners, and revenue-generating digital touchpoints. Internal users were not a priority. As long as systems were "up" and support teams could respond to tickets, employee experience was considered secondary.

This assumption no longer holds. The rapid adoption of remote work and hybrid work models permanently changed how organizations operate. When employees work across diverse networks, devices, and locations, the quality of their digital experience becomes directly tied to organizational productivity, collaboration, and customer outcomes. Today, poor digital experience does not just inconvenience employees — it slows business execution.

The Hybrid Workspace



As a result, enterprises are now making Digital Employee Experience (DEX) as a priority. CIOs increasingly view DEX as a central metric for IT performance, employee satisfaction, and even talent retention.

> **"Through 2027, 75% of organizations without a DEX strategy and tool will fail to successfully reduce digital friction."**
>
> *Source: Gartner Magic Quadrant for Digital Employee Experience Management Tools, 2025*

This whitepaper discusses a top-down approach to Digital Employee Experience (DEX), where business outcomes — not just tool capabilities — determine what needs to be monitored, how insights should be prioritized, and how IT teams should act. It explains:

- Why DEX has become a strategic necessity
- How it differs from traditional monitoring and observability
- What capabilities define a modern DEX monitoring
- How eG Enterprise offers deeper visibility and diagnostics than leading DEX vendors
- How organizations can operationalize DEX to improve productivity and reduce IT costs

What is Digital Employee Experience (DEX)?

Digital Employee Experience encompasses the holistic quality of an employee's digital interactions with the digital tools, technologies, and systems they depend on every day. This includes:

- Laptops, desktops, thin clients, and mobile devices
- Virtual desktops and applications (e.g., Citrix, Omnissa Horizon, AVD)
- Cloud and SaaS platforms (e.g., Teams, Zoom, Salesforce, Microsoft 365)
- Enterprise applications and business systems
- Corporate networks, VPNs, and edge infrastructure

DEX is not about infrastructure metrics, neither is it measured solely by technical performance metrics. Instead, DEX reflects what the user actually experiences — logon times, responsiveness, application availability, network stability, device health, collaboration quality, and more.

Why DEX has Become Critical for Organizations?

There are three reasons why DEX is a fundamental necessity:

- **Support for hybrid work styles:** Employees now work from home, offices, and shared workplaces. IT no longer controls the entire digital chain (home Wi-Fi, consumer routers, ISPs, VPNs, SaaS applications, etc.), yet is still responsible for the outcome – i.e., employee productivity. Lack of visibility across uncontrollable segments like home Wi-Fi, ISPs, personal devices, and cloud services makes troubleshooting employee complaints difficult.
- **Increasing use of SaaS and cloud-based tools:** Organizations irrespective of size are using hundreds of SaaS applications. These include collaboration tools (Teams, Zoom), communication and productivity tools (M365), file sharing platforms (OneDrive, GoogleDrive), CRM and ERP systems (Salesforce, Workday, SAP), HR and finance systems, ticketing systems (ServiceNow, PagerDuty, Freshdesk), and many more. Performance issues with these services may originate anywhere — endpoints, cloud providers, virtual desktops, identity platforms, or the applications themselves. IT teams do not have end-to-end visibility and this makes troubleshooting slow and challenging.
- **Employee productivity is directly tied to IT experience:** Slow devices, application crashes, Teams/Zoom call quality issues, and virtual desktop lag have a measurable impact on output. Research consistently shows that poor digital experience is one of the top drivers of employee frustration and lost productivity.

> **"The ability to measure and continually improve the digital employee experience using technology, employee sentiment and organizational data is critical for a thriving digital workplace."**
>
> *Source: Gartner Magic Quadrant for Digital Employee Experience Management Tools, 2025*

What DEX Monitoring Tools Aim to Achieve?

DEX monitoring tools are used by IT teams to monitor the experience of their employees. The primary goals of these tools include:

- **Ensuring high-quality user experience:** DEX tools continuously collect telemetry from endpoints, applications, networks, and user journeys to ensure employees have a smooth, responsive digital workspace.
- **Enhancing employee productivity:** By identifying bottlenecks — CPU spikes, memory constraints, poor Wi-Fi strength, slow VDI profiles, SaaS latency — DEX monitoring tools help eliminate disruptions before they affect employees' ability to work.
- **Reducing support ticket volume:** Since most employee issues originate on endpoints or networks, proactive DEX monitoring helps detect and fix these problems before users raise tickets.
- **Providing IT with actionable insights:** DEX tools correlate experience issues across different IT tiers so IT teams can quickly determine whether a problem lies in the endpoint, SaaS service, VDI session or backend system. This cuts down mean time to resolution (MTTR) and enables targeted improvements.

What organizations gain from DEX Monitoring?

- ✓ Higher employee productivity and fewer IT disruptions
- ✓ Reduced operational costs from lower helpdesk call volumes
- ✓ Improved IT efficiency through automated diagnostics and root cause analytics
- ✓ Better talent retention, as employees expect seamless technology experiences
- ✓ Stronger business continuity through proactive detection and remediation of user experience

Key Capabilities of a DEX Monitoring Solution

A complete DEX platform typically covers the following dimensions:

- **Endpoint performance and health:** A poorly functioning endpoint can affect user experience. Hence, in-depth insights of the endpoint are required.

These include utilization levels on the endpoint and user-focused metrics like not-responding applications, blue screen of death crashes, etc.

- **Connectivity from the endpoint:** Since poor connectivity from the endpoint results in productivity loss, monitoring this is important. When users work from remote locations, monitoring connectivity becomes even more important. It is essential to pinpoint where the problem lies – in the corporate infrastructure or in the applications, or in a user's location.
- **VDI performance:** Corporate access is usually provisioned for remote workers through a virtual desktop infrastructure. Key metrics to monitor for VDI include availability of the infrastructure, logon times, application access and screen refresh times.
- **SaaS application performance:** Since a number of productivity and collaboration applications are SaaS based, performance of these applications from the user endpoints must be monitored.
- **Dashboards, Reports and AI Analytics:** While collecting the right metrics is key, it is equally important to present these metrics to IT teams in simplified dashboards. Customizable reports are essential for IT teams to present DEX metrics to management. At the same time, the breadth of metrics collected means that it is not possible for IT teams to manually analyze all these metrics to detect performance anomalies. DEX monitoring tools must use machine learning and other AI technologies to analyze large data sets, glean and present interesting insights that can proactively help IT teams focus on enhancing the DEX score for employees.

Monitoring vs. Observability vs. DEX

- Monitoring = Are systems up?
- Observability = Why is the system behaving this way?
- DEX = Are employees able to work productively and without friction?

DEX Monitoring with eG Enterprise

eG Enterprise is a unified observability solution that provides complete insights into all aspects of DEX. With built-in sovereignty by design, eG Enterprise is available as an on-premises solution, deployable on the cloud or as fully turnkey SaaS solution delivered from a region suited to the each customer's compliance needs. eG Enterprise's key capabilities for DEX monitoring are described below:

- **Universal synthetic monitoring for end-to-end digital experience monitoring:** The idea of synthetic monitoring is to use automated software robots that continuously simulate user interactions and measure the end-to-end digital experience. In a VDI environment, for example, a synthetic workflow may include opening a browser, navigating to the remote access portal, logging in, selecting a virtual desktop or application, launching it through a thin-client application (such as Citrix Workspace App), and performing predefined tasks inside the session.

  While there are many synthetic monitoring tools for web applications, there are very few that work for thin client or other thick client applications that employees might use. eG Enterprise's Universal Simulation technology is unique in its support for any type of application. Synthetic monitoring is a two-step process, requiring recording of a typical user session and its subsequent continuous playback.

  During the recording process, an administrator guides the system by indicating where to click, where to enter credentials, and what the expected screen should look like at each step. Because thin-client applications are not browser-based, the simulation engine uses optical character recognition (OCR) to capture screen states and validate that each interaction has completed successfully.

  At the end of the recording, the system generates a script that becomes the input to the playback engine. By scheduling playback sessions at regular intervals — across one or multiple locations — IT teams can proactively validate availability, responsiveness, and workflow continuity across their digital workspace.

  Step-level latency measurements (see Figure 1) help pinpoint exactly where delays occur, enabling faster diagnosis of login issues, portal slowness, application launch problems, or thin-client behavior changes.

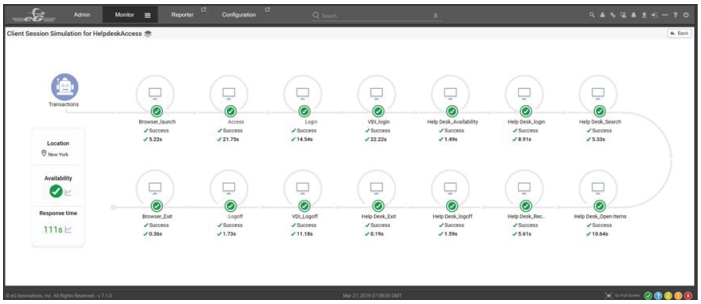


Figure 1: eG Enterprise's synthetic monitoring tests all components of the service delivery chain. This dashboard shows every step of the workflow simulated and the response time for each step, making it possible to identify the problematic step.

The universal nature of this simulation framework empowers organizations to monitor not only virtual desktop environments but also thick-client applications, web-based platforms, and SaaS services such as Salesforce, Workday, and Microsoft 365. This unified approach ensures IT teams gain proactive visibility across the entire digital workspace — receiving early-warning alerts whenever a critical business application begins to slow down or becomes unavailable. By detecting and escalating these issues before they impact employees, IT can coordinate with helpdesk teams and resolve performance degradations swiftly, preserving workforce productivity and user satisfaction.

- **Comprehensive monitoring of endpoints:** Since employees access their digital workspaces from a wide variety of endpoints, it is critical for IT teams to understand how these endpoints themselves are performing. Issues such as a runaway process on the device, a browser memory leak, or a handle leak in a client application can all manifest as slowness — even when backend systems are healthy. For remote workers connecting from home, shared networks, or public kiosks, poor Wi-Fi strength or unstable internet connectivity can further degrade the user experience.

  eG Enterprise provides unified, deep monitoring for this diverse endpoint landscape. Lightweight agents are available for Microsoft Windows, macOS, and Linux devices. For thin-client environments, the IGEL agent is distributed via the IGEL application portal, while the Dell ThinOS agent is built directly into the operating system. ChromeOS monitoring is supported in an agentless manner through API integration with Google Central. Figure 2 below illustrates the monitoring insights available for Windows endpoints. Similar capabilities are available for other operating systems as well.

Operating System

- CPU and GPU utilization
- Memory utilization
- Page file utilization
- Disk busy
- Disk space usage
- OS handles in use
- Blue screen of death
- Boot time
- DNS status

Networking

- Bandwidth usage by interface
- Packet discards by interface
- Queue length by interface
- TCP connections established
- TCP segment traffic (in/out)
- TCP retransmission

Events/Security

- System events by criticality
- Security events by criticality
- Application events by criticality
- Powershell executions
- Windows update status
- Vulnerable system drivers

Sessions

- Established sessions
- Disconnected sessions
- Active and Idle time
- Logon time and breakdown
- GPO processing

Applications

- Concurrent instances running
- Resource usage by application
- Application launch time
- Browser URLs accessed
- Browser resource usage

Digital Experience

- User Input delay
- Wi-Fi Signal Strength
- Local network latency
- ISP and Internet latency
- Latency by application and internal vs. external
- Digital experience rating

Figure 2: A summary of eG Enterprise's capabilities for monitoring endpoints.

The endpoint monitoring capabilities of eG Enterprise allow IT teams to answer a broad range of diagnostic and experience-related questions, including:

- Is the endpoint under resource stress? Are CPU or memory levels abnormally high, and which applications or processes are responsible for it?
- Is excessive disk activity impacting performance? Which processes are generating high IOPS and causing slow responsiveness?
- Are any applications leaking OS handles? Continuous handle growth can degrade system stability and slow down employee workflows.
- Why is the system booting slowly? How long does the endpoint take to boot, and which services or drivers are contributing to slow startup?
- Are there occurrences of Blue Screen of Death (BSOD)? What triggered these OS failures and what corrective actions are needed?
- Are there any issues that will affect the device lifespan of physical endpoints? Are there issues with disk or battery health?
- Are DNS queries failing from the endpoint? DNS resolution failures often translate into slow or failed application access.
- Are software updates pending? Outdated systems may face performance issues, security vulnerabilities, or compliance gaps.
- Is user interaction latency high? What is the maximum gap between employee input and system response? This is an important digital experience and employee satisfaction metric.
- Is Wi-Fi connectivity impacting the employee experience? What is the signal strength of the connected wireless network?

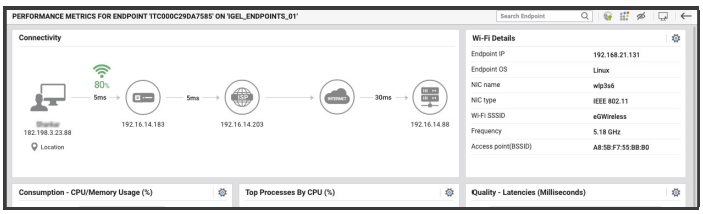


Figure 3: Measure endpoint connectivity including WiFi strength, local, ISP and Internet connectivity to identify bottlenecks at the employee end.

- Is network latency to the Internet high? And if so, is the root cause the local network (e.g., home Wi-Fi) or the employee's ISP?
- What is the detailed system configuration of the endpoint?
- Are there any security concerns on the endpoint including critical security-event log messages, execution of non-compliant PowerShell scripts, vulnerable drivers, or other indicators of risk?

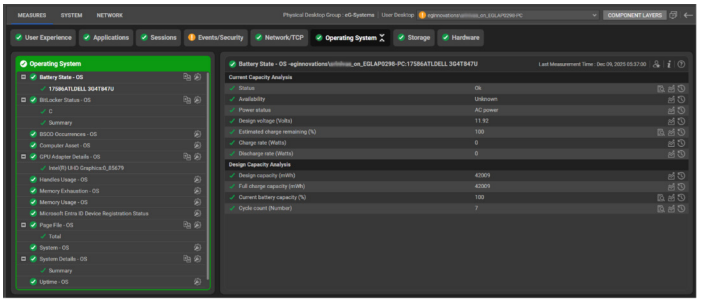


Figure 4: Real-time monitoring of endpoint performance in eG Enterprise.

- **Insights into all aspects of virtual desktop / application performance:** Technologies like Citrix, Omnissa Horizon, and many others are used to provide employees with secure, remote access to virtual desktops and applications. It is essential for virtual desktop / application access to be fast. A DEX tool must be able to provide insights into all the different aspects of employee experience in a virtual infrastructure:
  - Logon is a key step of the process that involves authenticating the employee, loading their profiles, and executing logon scripts to set up permissions. It is important to monitor logon times for employees and ensure that they stay within acceptable limits (30-60 seconds is a rule of thumb). At the same time, a DEX tool should also be able to pinpoint why logon is slow – is it due to authentication, due to logon script execution, group policy processing, or profile loading?
  - When an employee clicks on an application, various dependencies including DLLs and other add-ons are loaded. DEX tools must monitor application launch times as slowness can affect employee experience.
  - Another key measure of employee experience is screen refresh latency. High latency can be discomforting for employees – keystrokes may

not show up on time, screen changes may be slow and overall productivity is affected. A DEX tool must monitor employee-perceived latency and alert if these values are above a set threshold limit.

- DEX tool should have a capability to report events like application crashes, not-responding events, session disconnects, etc., as these have an adverse effect on employee experience.
- Since VDI is a shared infrastructure, a few employees taking up excessive resources (CPU, memory, disk, etc.), can affect the experience for others. It is important to monitor resource usage by session and report offending processes and applications.

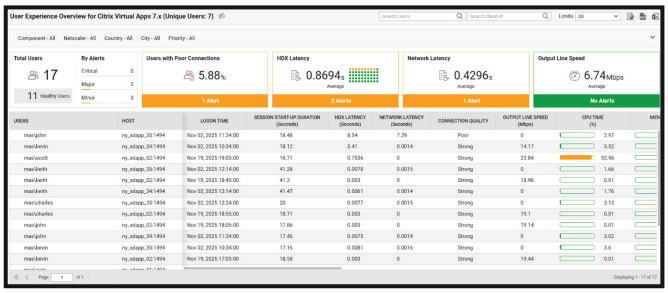


Figure 5: Dashboard showing employees accessing the VDI environment and their respective session metrics.

A virtual desktop infrastructure is distributed and involves several different tiers – the session hosts where users log in to, a connection broker that authenticates users and allocates them to a session host, the profile server where user profiles are stored, the datastore where user to application permissions are stored, etc. – a DEX tool must provide end-to-end visibility into all of the VDI tiers.

Built over years of experience with some of the most challenging VDI deployments in the world, eG Enterprise offers comprehensive and specialized monitoring for VDI technologies, covering all of the monitoring needs outlined above. Furthermore, since users experience virtual desktop/app latency end-to-end, eG Enterprise also integrates VDI and endpoint monitoring. As you can see from Figure 6, eG Enterprise shows a pictorial session topology view highlighting the different components of the virtual desktop infrastructure that a specific employee session is being supported by. If the employee's endpoint is also monitored in eG Enterprise, the IT admin can also see the employee's endpoint and its health state in the same topology view, so they can easily determine if a slow access complaint is due to the endpoint or due to the virtual desktop tiers.

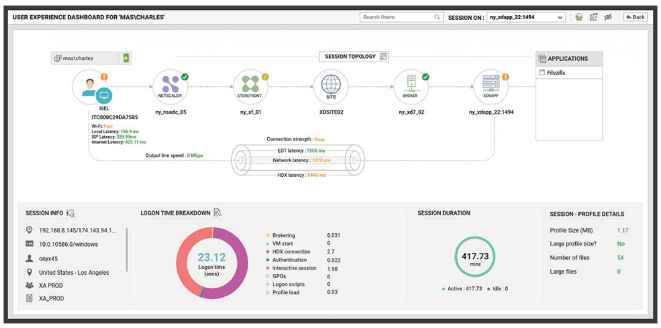


Figure 6: See the session topology of an employee's session – from endpoint to virtual application/desktop. Easily differentiate home Wi-Fi issues and ISP issues from those involving other VDI/DaaS tiers.

Similar capabilities are available for self-hosted and vendor-hosted DaaS as well. Full support is available for Microsoft Azure Virtual Desktop (AVD) technology and AWS WorkSpaces (cloud-based VDI offerings).

- **Security and Compliance Monitoring:** Security and compliance are important for ensuring employee productivity. Many organizations have standardized on CIS benchmarks as the standard based on which endpoints and virtual desktops are configured. DEX tools must allow comparison of current configuration of each endpoint/desktop to CIS standards and assess the configuration drift (see Figure 7).

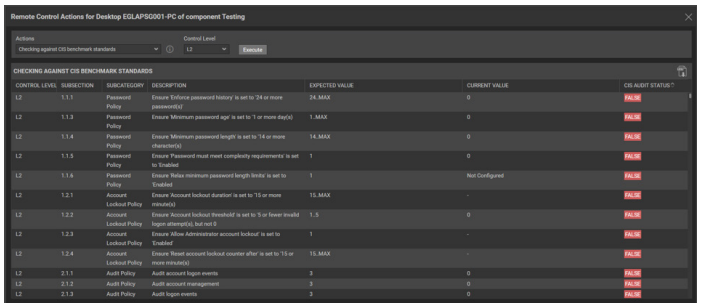


Figure 7: Comparing a desktop's configuration to CIS standards

Agents on the desktops/endpoints can be configured to look for security warnings, including vulnerable system drivers, pending Windows and Microsoft Office updates, BitLocker status, new files in system folders, execution of insecure Powershell scripts, etc.

Microsoft Intune is a cloud-native unified endpoint management (UEM) platform that enables organizations to manage, secure, and govern their entire device ecosystem – physical, virtual and in the cloud. It centralizes key capabilities including:

- Device management (configuration, compliance policies, OS updates)
- Application management (deployment, patching, access control)

- Security posture enforcement (Conditional Access, encryption, vulnerability exposure)
- Mobile application and data protection (MAM, app sandboxing, DLP controls)

UEM plays a foundational role in DEX because it provides the control layer that ensures devices are healthy, updated, compliant, and consistently configured across the organization. When OS updates, security policies and coniguration changes stall or fail, devices can become out-of-date, applications could stop working, and employees see degraded performance (slow login, CPU spikes, repeated update loops). If policies are not enforced correctly, employees could be blocked from email and Teams. Hence, Intune monitoring is a key component of any DEX strategy. eG Enterprise has API integration with Microsoft Intune, and reports on devices not in compliance, devices with critical failures, devices that have not checked in for many days, etc.

Another key component of many modern IT environments is Microsoft Entra ID. It is the central identity layer that authenticates every employee, device, and application across Microsoft 365, SaaS services, hybrid workloads, and enterprise apps. In short, Entra ID is the "front door" to the digital workplace. If Entra ID doesn't work, employees cannot log in, cannot access applications, and cannot be productive. If Entra ID is slow or experiencing failures, this can lead to access issues with Microsoft Teams and Outlook. Hence, monitoring Entra ID is extremely important. Use continuous monitoring to find out which rules are causing conditional access failures. eG Enterprise's continuous monitoring helps get a consolidated view of Microsoft Entra ID health and performance. From its monitoring console, find out which rules are causing conditional access failures, analyze interactive and non-interactive sign-in logs to detect logon failures and reasons for them. Proactively identify and attend to client secrets nearing expiry, which if left unattended will result in application outages.

Figure 8: Unified dashboard highlighting Intune health, Entra ID health, desktop and endpoints status, internet access speeds, SaaS service health and more.

- **Monitoring of digital experience for web applications:** Although synthetic monitoring monitors the health of web applications, its checks are limited to a few workflows only. What about the rest? This is where passive monitoring comes in.

Many web application monitoring tools use JavaScript injection to monitor web application performance. A small JavaScript snippet is added to the web application's pages (this is possible for most SaaS applications too) and when employees access these pages, the JavaScript snippet is downloaded to the client browser, executes on the browser and reports information about page load time, any errors during page loading, as well as details of the client location, IP address, browser version, etc. This information is collected by an analytics engine, processed and presented to IT teams via dashboards and reports. (see Figure 9).

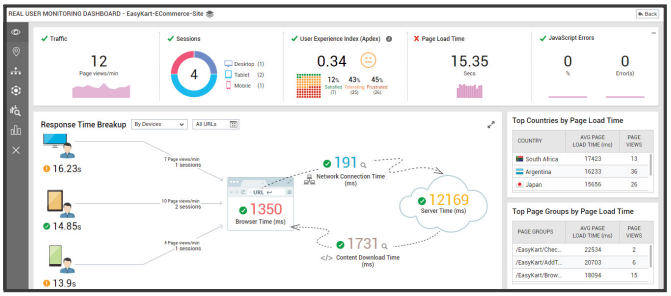


Figure 9: Performance insights about employee accesses to web applications

Modern browsers collect a wealth of insights about web performance. The JavaScript snippet taps into browser APIs to export some key insights to the analytics engine. For instance, in the figure above, you can see a breakdown of the overall page load time into network connection time, server time, content download time and browser rendering time. This breakdown can help determine where a performance bottleneck lies and to initiate corrective action to remediate the problem (i.e., is it a network problem, SaaS provider problem, endpoint problem or an application content issue?).

At the same time, as with web applications, monitoring of real user interactions is also required. Microsoft 365 and Zoom support APIs through which DEX tools can get insights into user interactions with these services. For instance, the Teams API provides call records about all the Teams calls made by employees of an organization including when the call originated, did it involve audio, video and screen sharing, how long did it last, who joined the call, what

was the latency, jitter and call quality experienced during the call. Analyzing such metrics helps IT teams proactively initiate actions to enhance employee experience.

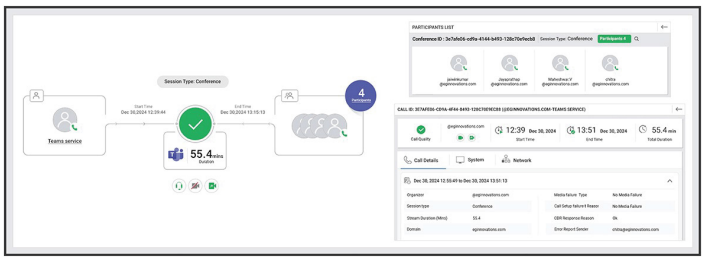


Figure 10: DEX monitoring captures real-time metrics of Microsoft Teams calls.

- **Going beyond employee experience to troubleshooting insights:** While monitoring and benchmarking employee experience is important to take action when the experience is unsatisfactory, IT teams also need additional insights into where the problems or bottlenecks lie. Because of the heterogeneous nature of today's IT environments, identifying the root-cause of employee experience issues is extremely challenging. It is critical and helpful when insights into every layer and tier of the service delivery chain are available at the click of a button.

  IT teams often must rely on different tools to track the health of different tiers of the infrastructure. Analyzing different tools and correlating between their insights is a manual and time-consuming process. Unified observability offered by eG Enterprise through its monitoring of over 650 different technologies from a single pane of glass avoids the constant shuttling that IT admins have to do when using multiple different tools. With eG Enterprise, IT admins can correlate employee experience with usage patterns, abnormal variations and insights from other tiers of the infrastructure and thereby quickly identify where the root-cause of a problem lies.

eG Enterprise observability supports 650+ different infrastructure and application technologies.

AIOps for DEX

For an enterprise with even just a few hundred users, considering all the tiers of the digital landscape, a DEX tool can collect hundreds of thousands of metrics. Analyzing these metrics manually is impossible. Hence, DEX tools must have the capabilities to automatically analyze metrics and pinpoint the potential bottlenecks that can affect employee experience. AI/ML-based correlation and causation in DEX monitoring helps with issue prioritization.

eG Enterprise includes a number of AIOps capabilities that make it easy for organizations to act on DEX metrics:

- **Using machine learning to auto-baseline metrics:** While static thresholds work for metrics such as availability and response times, they do not work for time-varying metrics such as workloads, utilization levels and alike. For time-varying metrics, eG Enterprise includes auto-baselining capabilities that analyze time of day, day of week behaviour, to define a dynamic baseline of performance. Real-time performance is then compared against these baselines and performance anomalies are flagged to administrators. This automatic analysis capability is a key to proactively alerting IT admins to issues that may occur in a distributed, heterogeneous infrastructure.

- **DEX scoring:** IT executives are not concerned about individual metrics on every endpoint. They need to see a composite score that represents the experience levels of employees – easy to understand and track-able. Typically, this is referred to as a DEX score – value between 0 and 100, with 100 representing a great experience and 0 representing a very poor experience. With eG Enterprise, one can configure a DEX score to be computed by considering a combination of different latency, utilization and availability metrics (see Figure 11). Using this score, executives can then see what percent of employees have experience below a specific score.

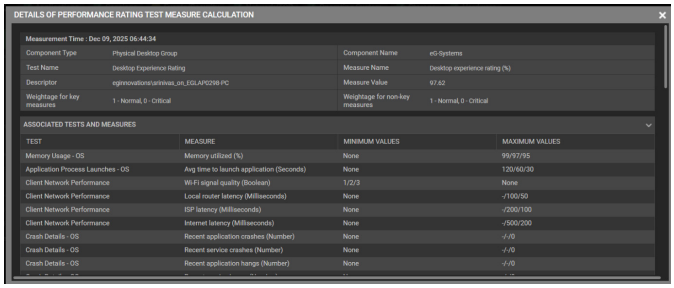


Figure 11: How a DEX score is computed

- **Specialized dashboards and reports for different stakeholders:** There are different stakeholders in an organization, each with different areas of focus and needs. The dashboards and reports a VDI admin may want to see are different from what an end user architect may want to see. eG Enterprise includes a variety of out-of-the-box dashboards and reports for these different needs (see Figure 12, for example). The top 25 reports that any VDI admin would want to see are included out of the box. At the same time, to cater to specialized needs, eG Enterprise also offers custom dashboards. A report builder offers similar functionality for historical reporting. Role-Based Access Control (RBAC) optimizes access and security for the various groups of stakeholders accessing eG Enterprise and its reports.

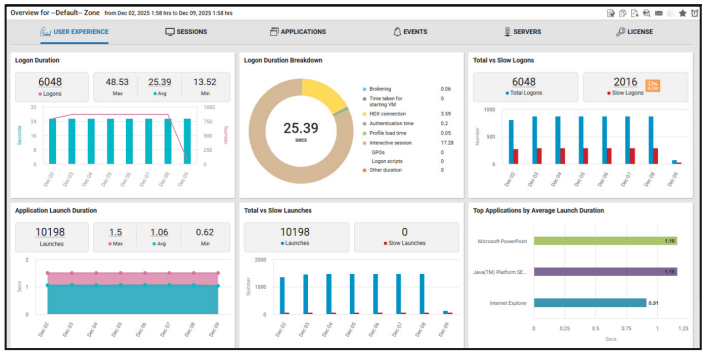


Figure 12: Pre-defined report highlighting employee experience when accessing VDI.

- **Integration with ITSM systems:** IT teams rely on ITSM systems where tickets are created for each incident reported by an employee. To simplify adoption, it is essential that the DEX tool be integrated seamlessly with the existing ITSM system. eG Enterprise integrates out of the box with over 25 different ITSM tools including popular ones such as ServiceNow, PagerDuty, BMC Remedy, ConnectWise and more. This integration is automatic – when an alarm is triggered in eG Enterprise, an incident in the ITSM tool is automatically created. The incident is pre-populated with details of the problem that triggered the incident. The incident to alarm mapping is used to then auto-update the incident as the alarm state changes in eG Enterprise (e.g., if a problem worsens or is resolved).

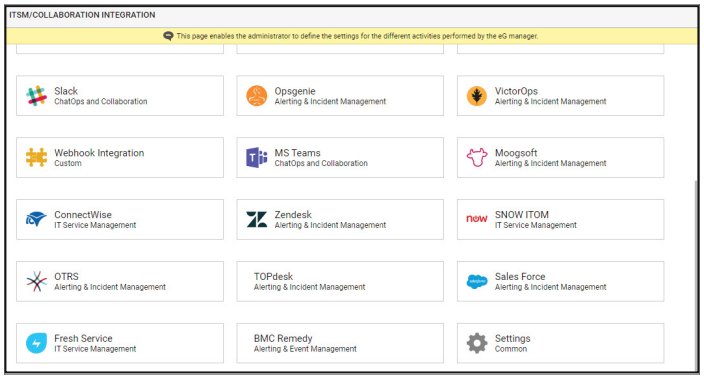


Figure 13: You will find the full list of trouble-ticketing and ITSM systems integrated with eG Enterprise in the administration tab of the main eG Enterprise unified console.

- **Remote control of the monitored systems:** When an alert is detected in eG Enterprise, IT admins may need to immediately take action to remediate the issue. eG Enterprise's remote control capability helps administrators use remote control actions on servers, endpoints and other systems. Common actions include:
  - Rebooting servers and endpoints
  - Shadowing user sessions and taking screenshots of their sessions for support reasons
  - Disconnecting idle sessions to avoid resource wastage
  - Collecting data from the session remotely for diagnostic purposes
  - Executing scripts or commands remotely for diagnostic or remediation, e.g., "Kill user GPO (Group Policy Objects) policies"

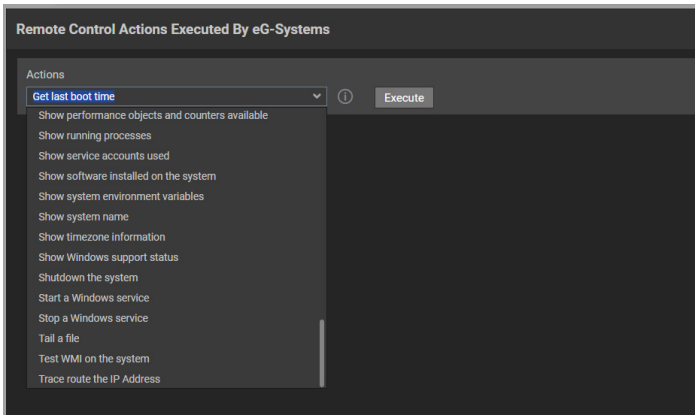


Figure 14: Some of the remote actions that can be executed against endpoints, VDI components and any monitored component.

- **Automatic remediation:** The ability to act upon actionable insights is a key feature of DEX monitoring. eG Enterprise provides automated remediation capabilities that fix common issues without human intervention by running scripts, restarting services, clearing caches, and applying updates. Domain-aware solutions provide turnkey self-healing remediation for common problems.

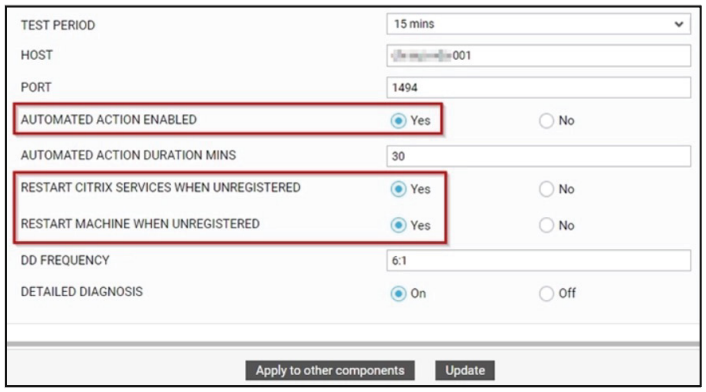


Figure 15: eG Enterprise includes turnkey configurable remediation actions for common issues such as unregistered Citrix VDAs

- **Proactive employee notifications:** Future versions of eG Enterprise will provide notifications directly to employees about actions they can take to enhance their productivity. These include notifications about poor Wi-Fi strength, ISP connectivity issues, high resource usage on virtual desktops, etc. Doing so allows employees to take an active role in the IT operations process and can significantly reduce the number of calls that IT helpdesks have to handle.
- **Integration with Gen AI services for effective use:** The adoption of DEX tools is heavily dependent on their ease of use. Often, the metrics collected are technical in nature and users of the tool may not be aware of the significance of a metric or its interpretation and what action needs to be taken when an alert is detected. eG Enterprise addresses this problem by integrating with Gen AI services to simplify employee experience management. The GenAI service can analyze metrics collected by the DEX tool, interpret them and inform an IT admin in an easily understandable manner as to why a metric was collected, what it's current value means, where the cause of an anomaly may lie and how to resolve an issue. Gen AI integration of DEX tools is a key to increased adoption and usage. eG Enterprise offers out of the box integration with Chat GPT and Gemini. Support for other LLMs is in the roadmap.

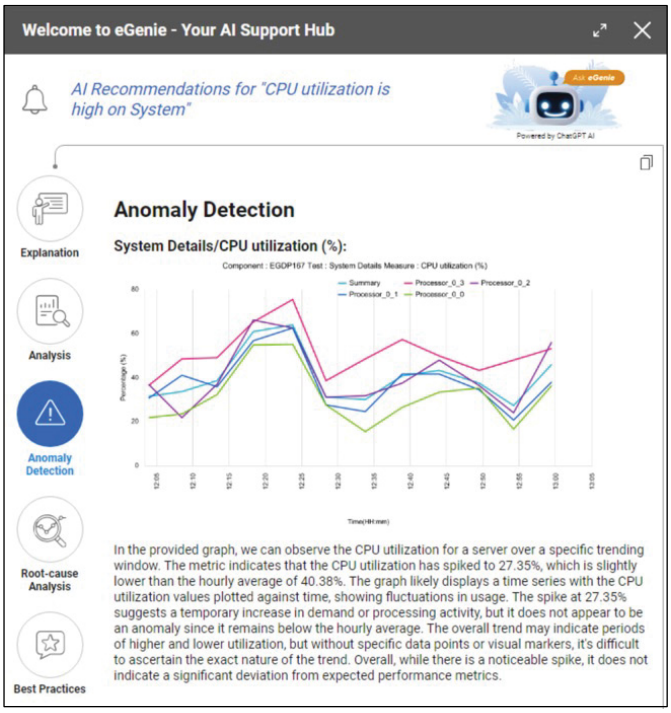


Figure 16: Integration of GenAI services with eG Enterprise allows IT teams to get better insights and precise recommendations.

Why eG Enterprise for DEX Monitoring?

- Unique universal synthetic monitoring for any desktop/application without needing any coding or developer assistance.
- Deployable 100% on-premises or on the cloud.
- Multi-tenant with role-based access, integrated with SAML/Active Directory.
- Unique ability to cover employee-facing technologies and underlying infrastructure and application stacks that often require separate tooling.
- Deployable as a white-labelled, pay-per-use service by DEX service providers.

Aligning DEX with Business Needs

Across industries, most organizations approach digital employee experience (DEX) initiatives from a bottom up perspective. The starting point is typically a technology decision: selecting tools, choosing telemetry formats, enabling instrumentation, or adopting a new vendor platform. While well-intentioned, this approach often results in tool sprawl, inconsistent data models, fragmented visibility, and escalating operational costs. The business impact — productivity, revenue leakage, operational risk, employee frustration — remains unclear or unaddressed.

A more effective approach is a top-down observability and DEX strategy, where visibility requirements are derived from the outcomes the business needs to achieve. Instead of asking "what tools should we use?", the discussion focuses on "what questions must we answer to ensure consistent and high-quality digital experience?" This shift ensures that every metric captured, every dashboard deployed, and every diagnostic insight delivered aligns directly with business value.

Start by identifying the business processes, roles, and KPIs that are most sensitive to digital friction. Before designing the DEX architecture, ask:

- **What business processes are most sensitive to digital disruptions?**

  Financial transactions, manufacturing operations, clinical workflows, and customer service operations often have zero tolerance for latency, login failures, or application crashes. Prioritizing these workflows ensures that monitoring efforts protect what matters most.

- **Which employee segments need the highest experience quality?**

  Not all roles are equally impacted by digital degradation.

  - Contact center agents require low latency and consistent voice/video quality.
  - Traders and financial analysts need very high application responsiveness.
  - Engineers and developers depend on high-performance VDI, CI/CD pipelines, and collaboration systems.

  Understanding these segments enables targeted visibility rather than blanket monitoring.

- **What metrics matter most to business productivity?**

  Metrics such as task completion time, logon duration, application responsiveness, virtual desktop latency, collaboration tool quality, incident MTTR, and self-service success rates often correlate directly with productivity. These metrics become the foundation of a DEX scorecard.

- **What early-warning signals correlate with degraded employee productivity?**

  High CPU load on virtual desktops, increasing network retransmits, authentication bottlenecks, slow API calls, application memory pressure, or rising helpdesk tickets may be leading indicators of future disruption. Identifying these signals allows IT to shift from reactive troubleshooting to proactive prevention.

Once these questions are answered, align your DEX adoption accordingly. The table below highlights how DEX capabilities align to business needs.

Business Goals	How DEX Helps
Fast employee access	Great logon experience
Reduced downtime	Proactive detection of problems, accurate identification of the root-cause of problems
Reduce support tickets	Automatic actions to resolve issues, employee notifications and self-service capabilities
Enhance hybrid work efficiency	Endpoint monitoring (WiFi strength, network connectivity monitoring), DEX for SaaS services
Better collaboration outcomes	Teams/Zoom metrics including call quality, jitter, packet loss
Reduce IT Operations costs	Automatic integration with ITSM workflows, unified platform for end-to-end visibility

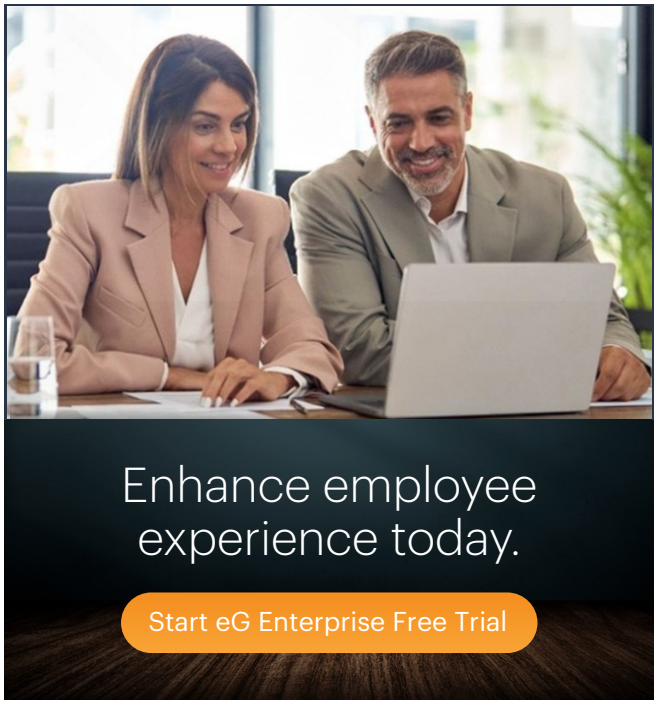
Conclusion

Digital Employee Experience is no longer an optional initiative—it is a strategic enabler of productivity, satisfaction, and operational excellence. As hybrid work becomes the norm and digital ecosystems grow more complex, traditional monitoring tools cannot keep pace with the visibility and intelligence IT teams require.

A top-down DEX strategy helps organizations:

- ✓ Focus on employee outcomes, not tool outputs
- ✓ Reduce operational cost
- ✓ Improve workplace productivity
- ✓ Enhance collaboration quality
- ✓ Strengthen business continuity

eG Enterprise is uniquely positioned to deliver this vision by combining DEX, observability, deep diagnostics, and AI-driven intelligence in one unified platform.



www.eginnovations.com | info@eginnovations.com

USA: +1 866 526 6700 I UK: +44 (0)207 993 8325 I The Netherlands: +31 (0)70 205 5210 I Germany: +49 (0)151 222 852 96 I LATAM: +5511 98123 6966
Singapore: +65 6423 0928 I Hong Kong: +852 3511 6785 / 86 I India: +91 44 4263 9553 / 9566 I Korea: +82 02 318 0392 I ANZ: +61 8 7079 0524