TeamViewer

TeamViewer AI
Security, control, and data handling

for TeamViewer DEX and TeamViewer ONE Enterprise

Trust Centre: compliance.teamviewer.com

Note: This document applies specifically to TeamViewer Remote, Tensor, and ONE platform capabilities and does not cover other TeamViewer products unless explicitly stated.

Executive summary

This document provides an overview of how TeamViewer AI features handle data and keep customers in control within the TeamViewer DEX platform. It summarises the shared security foundations and explains how TeamViewer AI capabilities — across insights, automation and reporting — support efficiency while meeting enterprise security and privacy standards.

AI designed for efficient support with built-in control

TeamViewer AI is designed to improve the efficiency of IT operations and support across product environments while ensuring that customers remain in control. It follows a security-by-design approach to data handling, incorporating policy- and role-based controls, data minimisation, privacy protections and strong encryption throughout the AI lifecycle — from ingestion and processing to storage and delivery.

TeamViewer AI enables:

- **Insights:** AI-driven trend detection, root-cause analysis, and actionable recommendations based on real-time DEX analytics (DEX Insights)
- **Scripting and automation library:** A SCALE-powered hub of proven automations scripts and custom AI-generated scripts—ready to run via DEX, APIs, and self-service. (DEX Hub)
- **Reporting & analytics:** AI-powered reporting that turns natural language questions into real-time visual reports and dashboards based on DEX data and tailored to the needs of the business (Tia Reporting)

Key commitments at a glance:

- **Admin-controlled rollout and access** through Admin Settings, permissions, policies, and/or RBAC/ABAC controls.
- **Personal data is minimized** and protected through privacy controls, including anonymization where applicable.
- **Data is protected with encryption in transit and at rest**, supported by controlled key management.
- Customer data is **not used** to train TeamViewer DEX AI models.
- **Third-party AI services (LLM-powered)** are used in a controlled manner under defined conditions and documented via the Third Party TermsTeamViewer.

Shared AI services for TeamViewer DEX platform

TeamViewer DEX applies TeamViewer AI's security and data-handling principles to digital employee experience use cases. DEX capabilities help IT teams detect experience degradations early, understand impact, and prioritize remediation, while maintaining enterprise-grade controls for access, data protection, and secure processing.

AI capabilities are delivered through the TeamViewer DEX platform and follow the security and data-handling controls described in this chapter, including DEX-specific platform services, data locations, and AI services.

Admin & user controls C

This layer provides a governance foundation for the TeamViewer DEX AI platform. It empowers administrators and users to manage how AI is used via defined policies and permissions, ensuring responsible and compliant AI operations.

AI admin policies & permissions

Company administrators have several levers to control how TeamViewer DEX AI is configured, used, and rolled out:

- **Admin Settings** → **AI Admin Settings**
  Configure TeamViewer DEX AI functionalities, controlled based on license type.
- **Admin Settings** → **User Permissions**
  Control user access to AI-generated content via permissions, for example, which users can view DEX Intelligence Insights.

Deterministic human-in-the-loop design

A design principle ensuring humans remain involved at critical decision points. This approach combines automated efficiency with human judgment, keeping AI processes consistent and controlled outcomes aligned with operational intent.

Audit trace access

Comprehensive access to action traces across the platform, supporting transparency for audits, troubleshooting, and continuous improvement.

Encryption and storage S

This layer is the secure data backbone for TeamViewer DEX AI, storing relevant data and platform logs in an encrypted and resilient way.

Data storage locations (as stated)

- Microsoft Azure (including Azure-hosted Databricks): EU-27, UK, US or CA, depending on deployment region.

Encryption standards (as stated)

Data is encrypted in transit and at rest using industry-standard encryption mechanisms (e.g., TLS for data in transit and AES-256 for data at rest). More details: https://www.teamviewer.com/de/resources/trust-center/industry-leading-security/

AI services (LLM-powered) P

This layer comprises the core intelligent services and safeguards that power the TeamViewer DEX AI stack's capabilities. It brings advanced AI functionality, such as security controls, safety guardrails, external AI integrations, and coding automation together in a secure, controlled way. Customer data is **not used** to train TeamViewer DEX AI models.

AI security

Built-in defences to protect AI-driven processes and data from threats or misuse, maintaining a secure operational environment for AI features.

AI guardrails

Predefined safety controls that guide and limit the AI's behaviour and outputs to acceptable, ethical, and policy-aligned boundaries.

Third-party LLM services

TeamViewer DEX AI uses LLM services hosted by **Azure OpenAI**, subject to Microsoft's published terms and documentation:

- **Provider terms:** Microsoft Azure Legal Information
- **Data processing reference:** Data, privacy, and security for Azure OpenAI Service
- **Hosting locations (as stated):** EU-27, UK,US and CA

Code generation

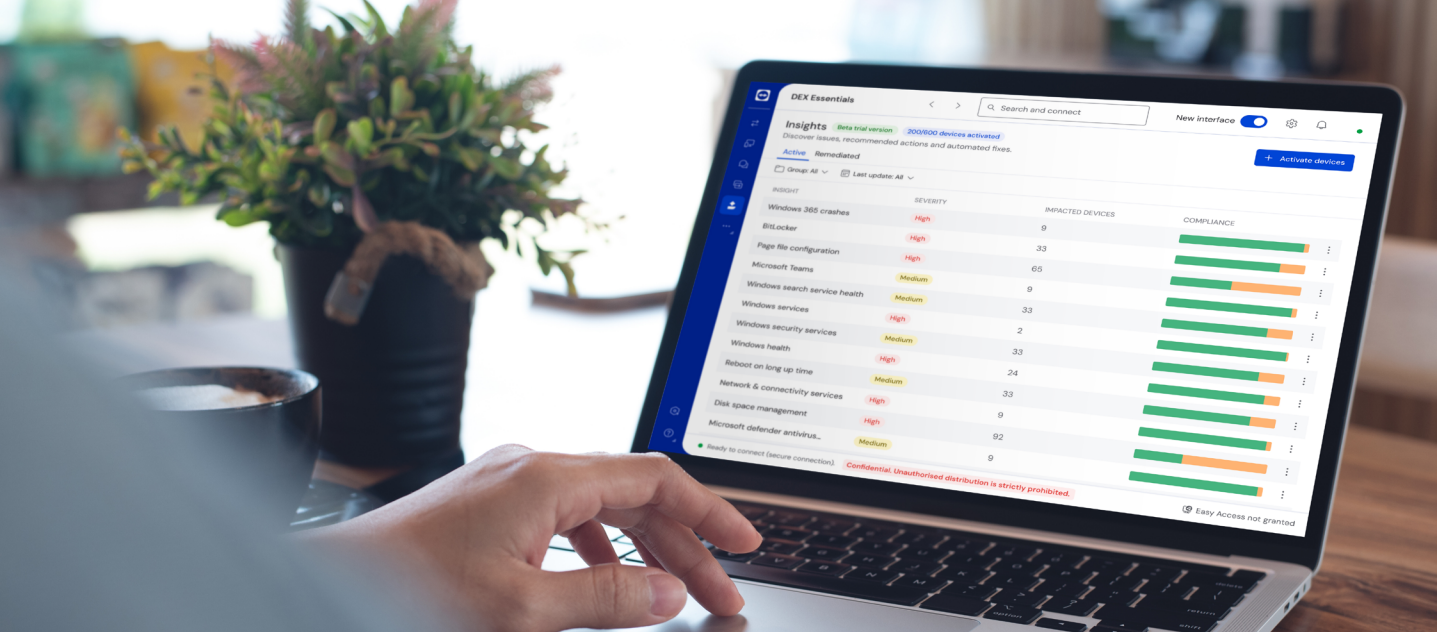
Automated creation of scripts and code to accelerate remediation and automation development (where applicable to the feature).

Client runtime & scripting technology R

This layer is the on-device execution environment for AI-driven actions and automation scripts. It ensures intelligent workflows run reliably on user endpoints with minimal latency and deterministic outcomes, combining automated speed with robust design for supporting consistent and controlled outcomes and human oversight when needed.

- **Script & approval signing**
  A secure validation and approval process for automation scripts. Each AI-generated or automated script requires digital sign-off by authorized personnel, ensuring that only vetted actions are executed.

- **Client technology**
  The local software component or agent that runs AI and automation on user devices, providing a stable runtime for endpoint execution and integration into device workflows.



- **Scripting technology**
  The automation engine that translates insights into repeatable actions through scripts, enabling consistent remediation and operational tasks across the IT environment.

End-to-end traceability

An overarching layer that tracks every step and decision across AI-enabled processes. It provides visibility from initial AI outputs to final action, establishing accountability and a reliable audit trail.

AI & human decision tracking

Detailed logging of decisions made by both AI and human users, capturing AI recommendations and human approvals.

Signing & execution tracking

Continuous tracking of script approvals and execution events, including who authorized and initiated actions.

Immutable audit log

An append-only audit log designed to preserve integrity and detect unauthorised modification of system events and decisions. It provides a verifiable record of AI actions and human interventions, supporting compliance reviews, security audits, and end-to-end traceability.

permissions, ensuring scripts can only be generated and used by authorized team members.

Script generation, storage, and execution

- Support teams trigger AI-powered script generation; scripts can be generated from prompts and/or prior Session Insights.
- Generated scripts are saved in the tenant cloud Script Database for review and reuse.
- Script execution remains permission-controlled and is performed through Remote Scripting workflows.

Architecture overview across TeamViewer DEX AI features

The following architecture diagrams show how TeamViewer DEX delivers AI-enabled capabilities across insights, automation, and reporting. Each feature builds on shared enterprise foundations: role-based access controls, tenant isolation, secure processing pipelines, and governed AI services, to ensure data is handled predictably and securely from ingestion to end-user delivery.

DEX Intelligence Insights

This layer is the on-device execution environment for AI-driven actions and automation scripts. It ensures intelligent workflows run reliably on user endpoints with minimal latency and deterministic outcomes, combining automated speed with robust design for supporting consistent and controlled outcomes and human oversight when needed.

Admin controls

Access to DEX Intelligence Insights is governed through DEX platform permissions, enabling role-based visibility to insights and dashboards. Users require the All-Instructions Actioner, Intelligence Administrator and Inventory User roles to access this capability.

Data signal collection (telemetry layer)

DEX Intelligence Insights starts with broad, continuous collection of experience signals from endpoints and systems. Lightweight agents and integrations capture what users and devices are experiencing—performance, reliability, responsiveness, and failures—across devices, operating systems, applications, and networks. The goal at this stage is not interpretation, but designed to provide comprehensive visibility with minimal disruption.

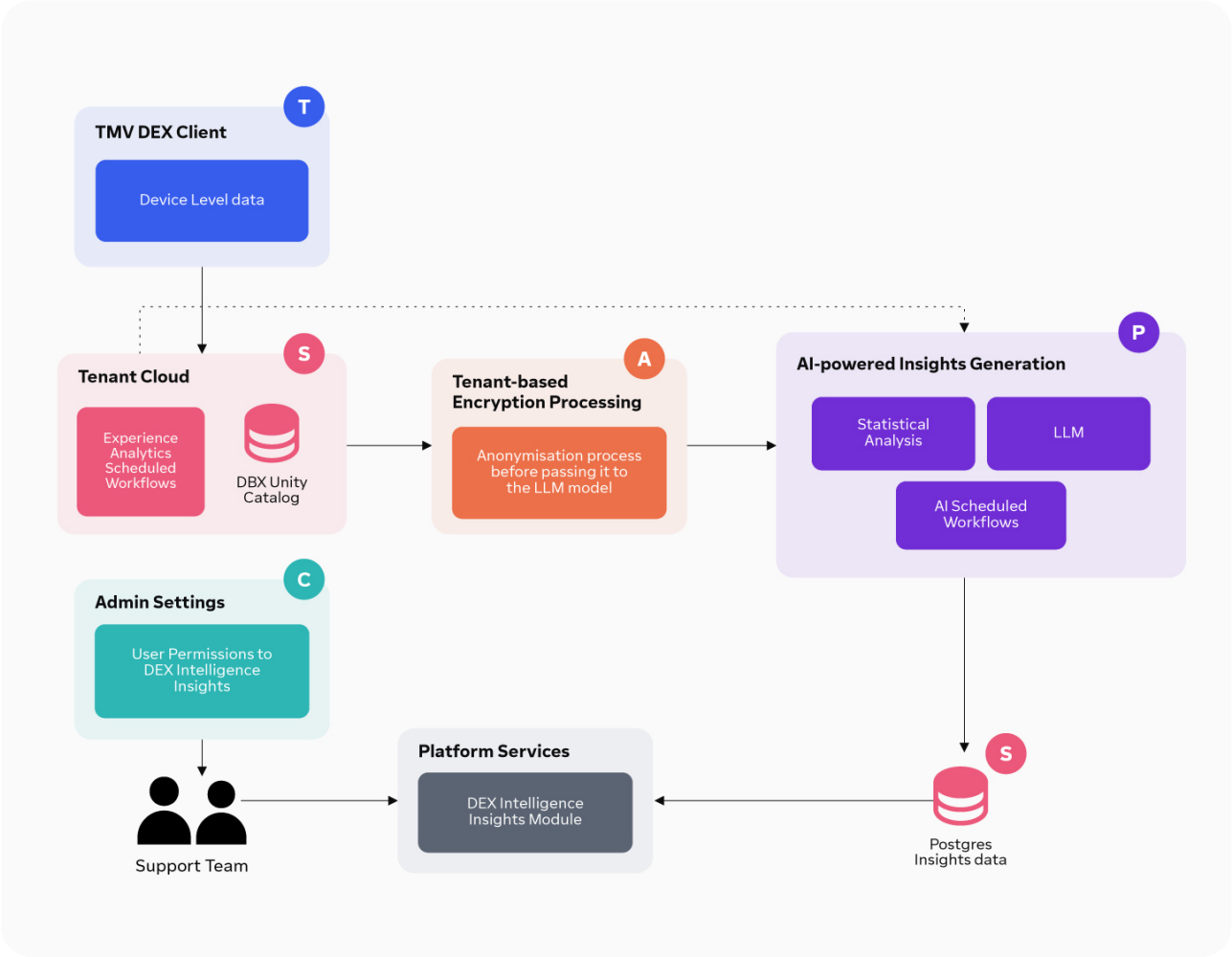
Secure ingestion, processing, and insight generation

Collected signals are securely ingested into the platform through authenticated and encrypted pipelines, standardized, and streamed at scale. Signals are then normalized and enriched with context (device/application/environment and organizational attributes) so raw metrics become structured experience events. Analytics engines detect anomalies, regressions, recurring issues, and emerging risks using deterministic rules and machine-learning models. Detected patterns are translated into human-readable insights explaining what is happening, who is impacted, severity, and whether an issue is new or recurring—packaged with evidence and recommendations.

Delivery (consumption layer)

Insights are surfaced through role-based dashboards and integrations/APIs to support IT operations, service desks, and leadership reporting.

DEX Intelligence Insights architecture



The diagram illustrates how administrators configure access boundaries and role-based visibility (C), how experience signals are anonymized at the tenant level before being passed to AI services (A), and how AI services analyze signals to generate human-readable insights (P). Insights are stored and delivered through tenant-protected processing and dashboards under secure data handling controls (S). End-to-end traceability supports oversight through audit traces and decision tracking (T).

Legend (letters map to TeamViewer DEX AI platform services)

- **C** — Control · Admin & user controls
- **A** — Process · AI services (LLM-powered)
- **P** — Process · AI services (LLM-powered)
- **S** — Secure · Data services & storage (Encryption & storage)
- **T** — Trace · End-to-end traceability

Feature availability

- TeamViewer ONE Enterprise

DEX Hub

The DEX Hub is a central location for building, managing and reusing automation content, combining permission-controlled access with AI-powered script generation and a shared automation library. AI can generate scripts but does not execute them automatically; access and execution are governed through role-based controls and automation workflows.

Admin controls

Access to DEX Hub and the Tia Script Builder is governed through role-based permissions. Users require the Solutions Core role to access these capabilities.

AI code builder engine

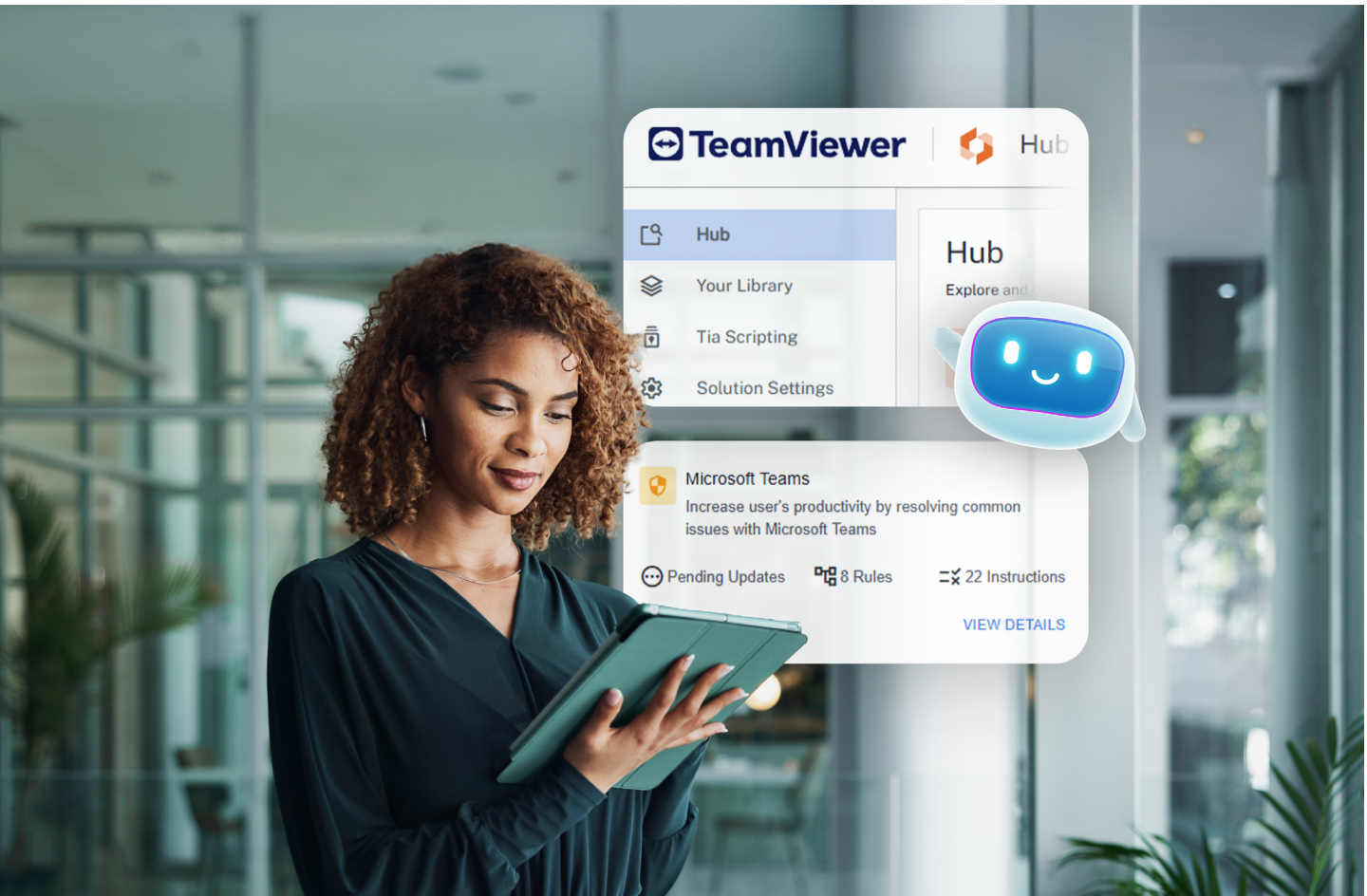
DEX Hub includes an AI-powered code generation component leveraging the SCALE Code Builder framework to translate plain-language requests into ready-to-run automation script drafts.

Central automation library

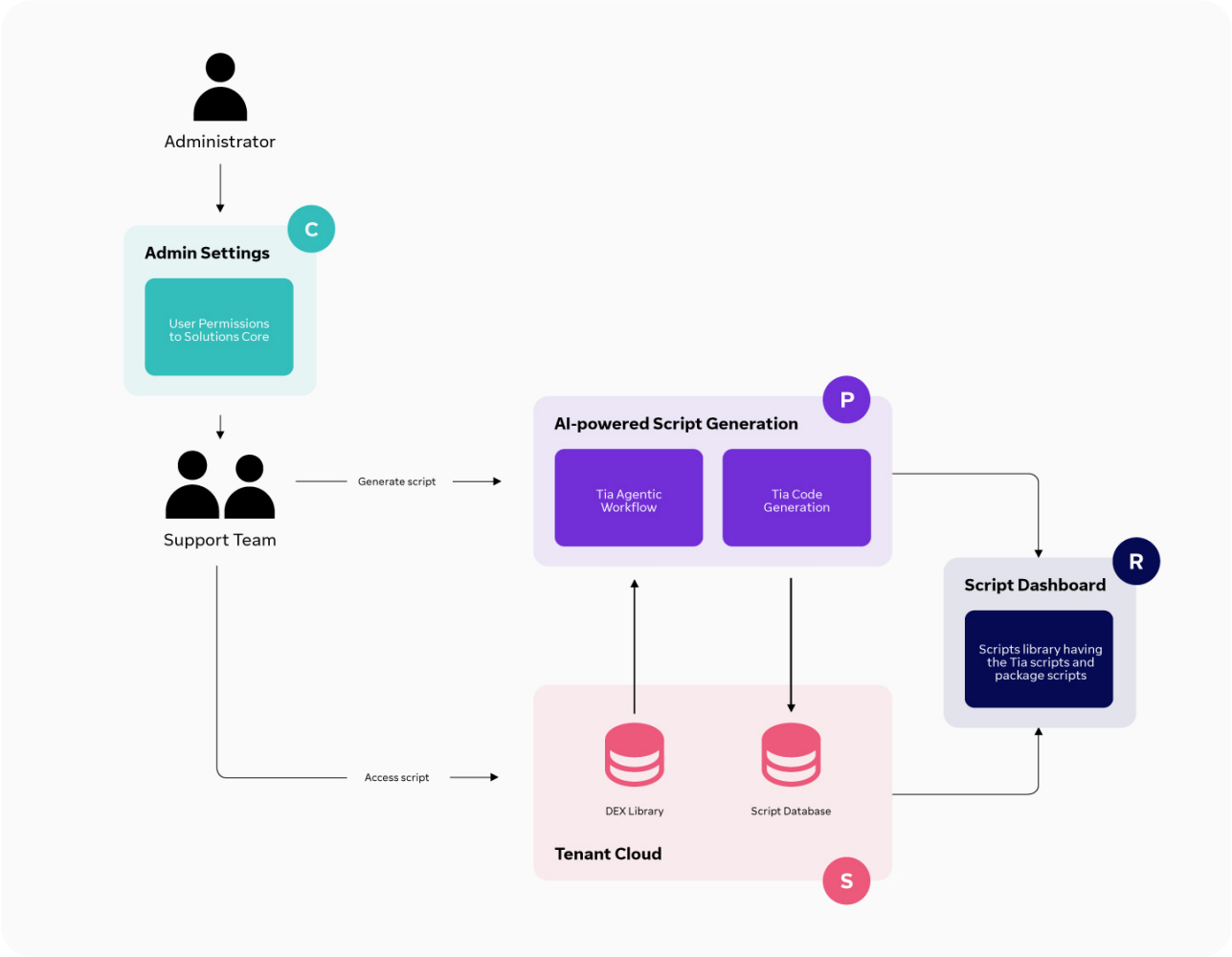
Built on the DEX Library, DEX Hub provides a central repository of automations (instructions, scripts, packs), including default content and customer-created scripts generated via the code builder. This supports reuse and controlled adoption across teams.

Governance and execution

Automation content is stored centrally for review and reuse. Script signing/approval and execution tracking support governance and oversight.



DEX Hub architecture



The diagram illustrates how administrators control access to DEX Hub and the script builder via role-based permissions (C), how AI services generate automation script drafts from plain-language requests (P), and how scripts are stored in tenant libraries (DEX Library and Script Database) and managed via the Script Dashboard (S). On-device runtime and signing controls ensure scripts are executed deterministically under governance (R), with traceability through signing and execution tracking and an immutable audit log (T).

Legend (letters map to TeamViewer DEX AI platform services)

- **C** Control · Admin & user controls
- **P** Process · AI services (LLM-powered)
- **S** Secure · Data services & storage (Encryption & storage)
- **R** Run · Client runtime & scripting technology
- **T** Trace · End-to-end traceability

Feature availability

- TeamViewer DEX
- TeamViewer ONE Enterprise

Tia Reporting

Tia Reporting brings self-service analytics into the DEX platform—combining tenant-isolated data models with AI-assisted querying and embedded dashboards. Users can ask questions in natural language and explore insights, while access remains governed through RBAC/ABAC and tenant-scoped data boundaries.

Admin controls and access boundaries

Tia Reporting reuses platform authentication and enforces RBAC for feature access and ABAC for data-level filtering. Session tokens are dynamically generated to ensure secure, scoped access to reporting data. Users require the Experience Admin role to access these capabilities.

Data ingestion & processing

Platform data is streamed via Kafka and processed through ELT pipelines (Bronze Silver →Gold). Final aggregated datasets are prepared for reporting and exposed through Databricks.

Multi-tenant data isolation

A shared data platform is logically segmented using tenant-specific schemas and filtered views. Access is controlled via dedicated service principals, ensuring strict tenant isolation for multi-tenant reporting.

Reporting & query execution

ThoughtSpot connects to tenant-specific schemas and automatically generates data models from metadata. User queries are translated by the Spotter LLM into SQL, executed on Databricks, and returned as visual insights.

Embedded user experience

Users interact with dashboards via the embedded ThoughtSpot SDK. Requests are routed through the Consumer API, enabling seamless access to insights directly within the DEX platform without additional authentication steps.

Tenant provisioning & setup

When a new tenant is created, the admin layer provisions Databricks schemas, ThoughtSpot Orgs, and access controls. Data models and permissions are automatically applied to enable reporting readiness.

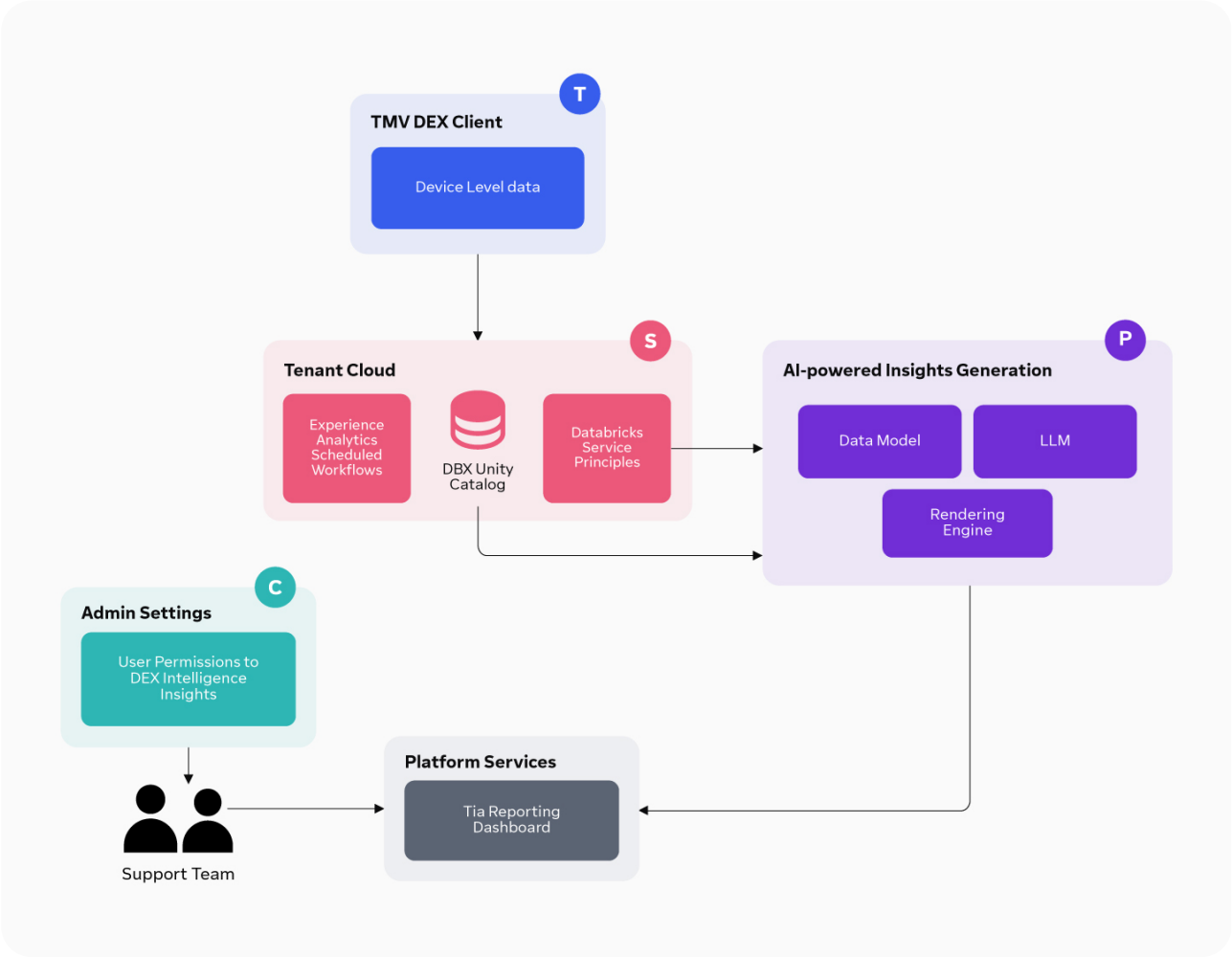
Reporting deployment & scale

Reporting models are centrally managed in a Template Org and distributed using TML files, ensuring consistent, version-controlled deployment of dashboards and insights across tenants.

End-to-end insight delivery

The overall flow connects ingestion to insights: Kafka →ELT →Databricks →Tia →Dashboards, providing an integrated analytics experience within the DEX platform.

Tia Reporting architecture



The diagram illustrates how the platform enforces tenant isolation and access controls through RBAC for feature access and ABAC for data-level filtering (C), how reporting services process data from Kafka through ELT pipelines into Databricks and translate user questions into SQL via LLM-assisted query execution (P). Data is handled within tenant-scoped schemas and protected through encrypted storage controls (S). End-to-end traceability preserves accountability across reporting access, model deployment, and query execution (T).

Legend (letters map to TeamViewer DEX AI platform services)

- **C** — Control · Admin & user controls
- **P** — Process · AI services (LLM-powered)
- **S** — Secure · Data services & storage (Encryption & storage)
- **T** — Trace · End-to-end traceability

Feature availability

- TeamViewer DEX
- TeamViewer ONE Enterprise

FAQ

What data does DEX Intelligence Insights process?

DEX Intelligence Insights processes device-level experience signals collected from endpoints and integrated systems. This includes telemetry related to performance, reliability, responsiveness, and failures across devices, operating systems, applications, and networks. These signals are normalized and enriched with contextual metadata before being analyzed to generate insights.

How are DEX Intelligence Insights protected during processing?

DEX Intelligence Insights uses authenticated and encrypted pipelines for data ingestion and processing. Prior to interact with LLM-powered components, data is subject to tenant-level minimisation and anonymization measures. Insights are stored in the platform and accessed through role-based controls and integrations.

Is DEX AI data used to train AI models or build a knowledge layer?

No. Customer data processed by TeamViewer DEX AI features is not used to train TeamViewer AI models.

Data processed solely for the purpose of delivering the requested functionality, such as generating insights, script drafts, or reporting outputs, and is handled within the controls described in this document.

TeamViewer does not use customer data to build or contribute to shared or cross-customer AI models.

Does DEX Intelligence Insights send raw endpoint data directly to the LLM?

No. Data is not sent to LLM services in raw form. Prior to any AI processing, data undergoes tenant-level minimization and anonymisation measures to reduce exposure of sensitive or identifiable information.

Who can access DEX Intelligence Insights?

Access to DEX Intelligence Insights is governed through role-based access controls (RBAC). Permissions define which user can view dashboards, analytics outputs, and insights based on their roles and responsibilities.

How is access to DEX Hub and the Tia Script Builder controlled?

Access to DEX Hub and the Tia Script Builder is governed through admin settings and role-based permissions. Users require the Solutions Core role to access these capabilities.

What does DEX Hub do?

DEX Hub provides a central place to create, store, and reuse automations. It includes an AI-powered code builder that translates plain-language requests into script drafts, and a shared library where automations, scripts, and packs can be stored and managed.

What is stored in DEX Hub?

DEX Hub stores automation content in the tenant-scoped cloud storage, including:

- default scripts provided by TeamViewer
- customer-created scripts generated through the code builder
- reusable packs and automation components

This content is managed through the DEX Library, Script Database, and Script Dashboard.

Are scripts automatically executed by DEX Hub?

No. DEX Hub can generate script drafts but does not execute them automatically. Access and execution are governed through role-based controls and automation workflows.

Where is TeamViewer DEX AI data stored?

TeamViewer DEX AI data is stored in Microsoft Azure regions (EU-27, UK, US and CA). Processing and analytics are performed using Azure-hosted services, including Databricks, withing TeamViewer-managed environments.

Is TeamViewer DEX AI data encrypted?

Data is encrypted in transit and at rest using industry-standard mechanisms (e.g., TLS for data in transit and AES-256 for data at rest). In addition, DEX Intelligence Insights uses authenticated and encrypted pipelines for ingestion and processing.

Which AI services (LLM-powered) are used?

TeamViewer DEX AI uses LLM services hosted by Azure OpenAI under Microsoft's published terms and documentation. These services operate in declared regions (EU-27, UK,US and CA) and are integrated in accordance with TeamViewer's data protection and security standards.

How is tenant isolation enforced for reporting and analytics?

A shared data platform is logically segmented using tenant-specific schemas and filtered views. Access is controlled via dedicated service principals. For reporting, access is enforced through RBAC for feature access and ABAC for data-level filtering, with scoped session tokens for secure, tenant-specific access. m

What auditability and traceability exist for AI-driven workflows?

TeamViewer DEX AI includes end-to-end traceability capabilities, including AI & human decision tracking, signing & execution tracking, and an immutable audit log to support compliance reviews, security audits, and oversight.

What terms govern the use of TeamViewer DEX AI Services?

TeamViewer DEX AI Services are regulated by the AI specific terms set out in Section B.7 of the End User License Agreement (EULA) (here). AI features may include third party AI models or technologies and its usage is subject to their terms in the then-current version available at https://www.teamviewer.com/en/legal/ai-terms/.

Furthermore, the use of the TeamViewer DEX AI Services must comply with the Acceptable Use Policy provided at the same link.

TeamViewer

About TeamViewer

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 640,000 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 more than 1,800 people globally. In 2024, TeamViewer achieved a revenue of around EUR 671 million. TeamViewer SE (TMV) is listed at Frankfurt Stock Exchange and belongs to the MDAX. Further information can be found at www.teamviewer.com.

www.teamviewer.com/support

TeamViewer Germany GmbH
Bahnhofsplatz 2 73033 Göppingen Germany
+49 (0) 7161 60692 50

TeamViewer US Inc.
5741 Rio Vista Dr Clearwater, FL 33760 USA
+1 800 638 0253 (Toll-Free)

Stay connected

www.teamviewer.com