

# Full-stack network automation.

Built to accelerate business value.

Gluware automates multi-vendor, multi-platform networks through CLI and API interfaces. Offload maintained foundations and connect lifecycle capabilities to NetBox, Ansible playbooks, ServiceNow, Python, and enterprise systems to deliver visible business value.

## Offload the foundation. Accelerate business impact.

Network automation has proven its value. Yet teams can remain consumed by device interactions, parsers, normalization, release qualification, and platform maintenance. Every new vendor or OS change adds work before the next business priority can advance.

Gluware makes those shared foundations maintained platform capabilities for the supported network. Teams can invest above the value line in company policy, operational processes, exceptions, and verified results.

### BUSINESS OUTCOMES

#### Security

Connect device advisories and contextual exposure assessment to supported, verified remediation.

#### Compliance

Check required controls, coordinate correction, and present evidence of the status covered.

#### Continuity

Apply software and configuration changes through repeatable plans, previews, and defined assessments.

#### Growth

Bring new infrastructure under management and apply capacity released from recurring foundation maintenance.

### Build above the value line.

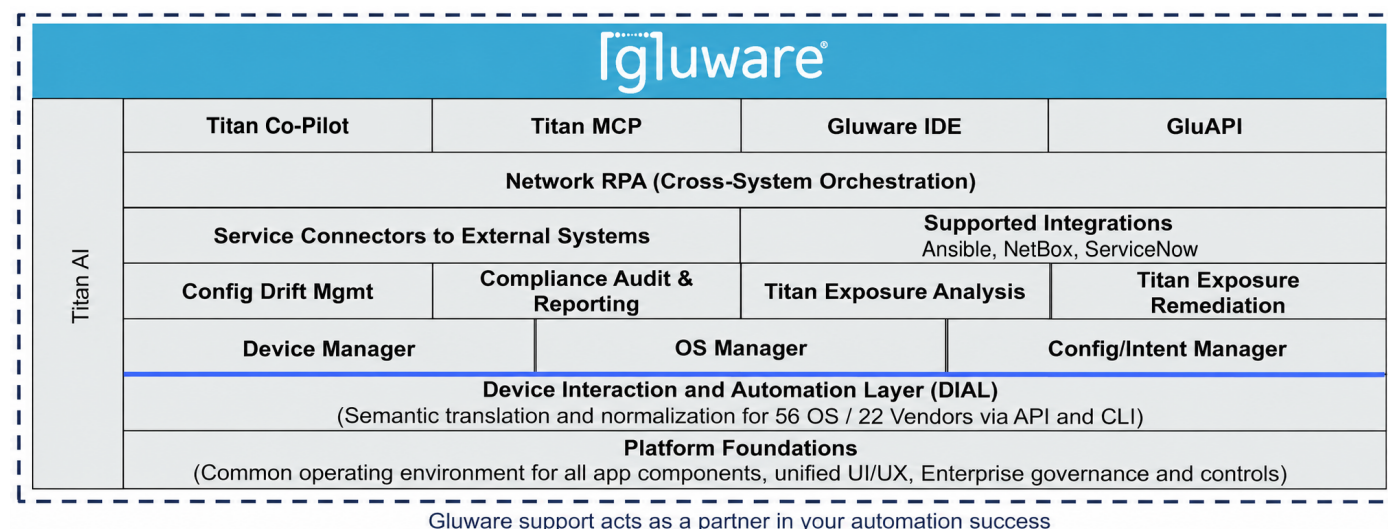
The full stack provides lifecycle constructs and solutions alongside orchestration, integrations, and builder interfaces. The team starts with usable capabilities and extends what is specific to the business.

# Offload the maintained foundations.

Platform services. Device interaction.

Control supplies the operating environment and governance. DIAL handles supported device interaction, semantic translation, normalization, and validation. Supporting package and file services make the applications usable.

## THE FUNCTIONAL PLATFORM STACK



## A maintained device-interaction foundation

DIAL offloads work that every automation initiative needs but that is not custom to the business. Teams can invest in the policies and processes that reduce exposure, maintain controls, protect services, and support expansion. The maintained foundation reflects more than twelve years and over a million engineering hours of investment, with dozens of DIAL package releases each year.



## Deploy where the enterprise needs it.

Run Gluware on supported on-premises hypervisors, including VMware ESXi and Microsoft Hyper-V, or in the customer's cloud-provider environment. The Gluware Primary Orchestration Engine and Gluware Zone Engine(s) support central orchestration and distributed processing. Distributed Gluware File Server instances bring image delivery closer to target devices.

12+ years of foundation investment | 1M+ hours of engineering effort | 56 OS / 22 vendors supported by DIAL

# Business outcomes and lifecycles.

Each capability connects several functions into an operating process.

The components delivering each capability are shown below. Component roles are summarized on pages 5 and 6.



## Network discovery & onboarding

Discover the fleet, establish device context, and turn existing configurations into models your team can manage.

**Components:** Device Manager; Config Model Editor; DIAL; Network RPA; NetBox Integration; ServiceNow Integration.



## Network exposure management

Bring device advisories, contextual CVE assessment, and supported remediation into a governed network process.

**Components:** Device Manager; Titan Exposure Analysis; Titan Exposure Remediation; OS Manager; Config Model Editor; Network RPA; ServiceNow Integration.



## Device & OS lifecycle management

Connect discovered inventory, device advisories, image selection, deployment plans, and operational checks.

**Components:** Device Manager; OS Manager; File Server; Config Model Editor; Network RPA; Data Explorer.



## Cross-system orchestration

Connect network tasks, source-of-truth data, service-management steps, external executors, and records in a repeatable process.

**Components:** Network RPA; Service Connectors; NetBox Integration; ServiceNow Integration; Ansible Integration; GluAPI; Config Model Editor; Gluware IDE.



## Configuration intent & drift management

Define reusable configuration intent, detect departures, apply modeled changes, and reassess the result.

**Components:** Config Model Editor; Config Drift & Audit; Network RPA; Version Control; Device Manager; DIAL.



## AI-assisted automation building

Combine conversational assistance, development tools, and supported agent services with the applications that operate the network.

**Components:** Titan Co-Pilot; Titan Intelligent MCP Server / Services Framework; Gluware IDE; Solutions Manager; Config Model Editor.



## Continuous compliance & reporting

Connect repeatable policy checks, corrective processes, and evidence that operations, security, and compliance teams can review.

**Components:** Config Drift & Audit; Data Explorer; Config Model Editor; Network RPA; Dashboard; Version Control.

# Automation capabilities.

Choose the capability your next outcome needs.

The components delivering each capability are shown below. The individual capability briefs provide the operating process and scope.



## Network discovery

Build repeatable discovery plans for multi-vendor networks using seeded neighbor discovery or subnet scanning.

**Components:** Device Manager; DIAL; Gluware Control; Network RPA; GluAPI.



## Process automation

Connect application tasks, decisions, approvals, and records through visual orchestration.

**Components:** Network RPA; Service Connectors; Ansible Integration; GluAPI; Gluware IDE.



## Network state assessments

Define CLI/API state checks for on-demand assessment, provisioning pre/post checks, and Network RPA tasks.

**Components:** Config Model Editor; Network RPA; Device Manager; DIAL.



## Device inventory

Maintain discovered hardware, software, configuration, site, and advisory information in a shared device inventory.

**Components:** Device Manager; NetBox Integration; ServiceNow Integration; Data Explorer; Dashboard.



## NIST & Cisco CVE/PSIRT integrations

Associate Cisco PSIRT advisories and NIST/NVD CVE information with discovered devices and software.

**Components:** Device Manager; Gluware Control; Titan Exposure Analysis; OS Manager; Config Model Editor.



## Configuration audit

Evaluate required and forbidden configuration conditions with repeatable audit policies and evidence.

**Components:** Config Drift & Audit; Config Model Editor; Network RPA; Data Explorer; Version Control.



## Network state audit

Evaluate captured operational command results against defined rules and retain findings for review.

**Components:** Config Drift & Audit; Device Manager; Network RPA; Data Explorer; Version Control.



## Git integration

Synchronize supported constructs, audit policies, and Network RPA artifacts with Git-based repositories.

**Components:** Version Control; Config Model Editor; Config Drift & Audit; Network RPA; Gluware Control.



## OS management & patching

Plan, validate, schedule, and review supported network software upgrades, downgrades, and patching operations.

**Components:** OS Manager; File Server; Device Manager; Config Model Editor; Network RPA.



## Backup & restore

Back up supported device configurations and preserve the model, policy, and process artifacts needed to operate them.

**Components:** Device Manager; Network RPA; Version Control; Config Model Editor; Config Drift & Audit.

# Foundations, lifecycles and outcome solutions.

Know what delivers each capability.

## FOUNDATIONS



### Gluware Control

Gluware Control provides the common operating environment, unified interface, governance, and scheduling services for the Gluware application suite.



### DIAL

The Device Interaction and Automation Layer handles multi-vendor device interaction, semantic translation, normalization, and deterministic validation through CLI and API interfaces.

## FUNCTIONAL LIFECYCLE COMPONENTS



### Device Manager

Discover and inventory devices, inspect configuration and software state, and maintain the fleet information that network automation depends on.



### OS Manager

Use OS catalogs and deployment plans to select approved images, validate readiness, schedule upgrades or downgrades, and review execution results on supported devices.



### Config Model Editor

Model multi-vendor CLI and API intended configuration state with declarative enforcement.

## BUSINESS OUTCOME SOLUTIONS



### Config Drift & Audit

Capture actual configuration and operational state, compare it with baselines, and audit the controls required by your enterprise.



### Titan Exposure Analysis

The read-only assessment component of Titan Exposure Management evaluates CVEs using OS, configuration, and operational state.



### Titan Exposure Remediation

The remediation component of Titan Exposure Management can orchestrate supported patches or compensating controls with approvals, validation, and outcome verification.

## MODELING AND PLATFORM SERVICES



### File Server

Store and manage the OS image and related files used by Gluware OS Manager.



### Version Control

Use Git integration for supported audit policies, configuration-model constructs, and Network RPA processes.



### Solutions Manager

Find and install Gluware packages in the appropriate organization, including the functionality and modeling support used by the application suite.

# Orchestration, integrations and interfaces.

The component reference explains ownership, dependencies, and functionality.

## ORCHESTRATION AND INTEGRATIONS



### Network RPA

Build and run visual processes that connect Gluware applications, external systems, operational logic, scheduling, and traceable tasks.



### Service Connectors

Bring ITSM, CMDB, DDI, and other external systems into Gluware automation processes through service connectors.



### NetBox Integration

Synchronize mapped device and site properties between Gluware and NetBox, with configurable property ownership, linking rules, exclusions, and schedules.



### ServiceNow Integration

Synchronize mapped inventory with ServiceNow CMDB and use Service Connector tasks in Network RPA to connect ticket and change processes to automation.



### Ansible Integration

Use Network RPA to incorporate Ansible playbooks into processes that span Gluware applications and external systems.

## VISIBILITY AND REPORTING



### Dashboard

Customize dashboards and widgets for application, administrative, scheduling, and operational information.



### Data Explorer

Build reusable reports from data stored by Gluware, with field selection, filtering, grouping, formatting, scheduling, and exports.

## AI AND BUILDER INTERFACES



### GluAPI

Give external systems a programmatic interface to invoke and coordinate Gluware automation processes.



### Gluware IDE

Define custom network features, data models, business logic, Network RPA tasks, and integration logic through the Gluware development environment.



### Titan Co-Pilot

Use a conversational and agentic interface to develop and extend automation on Gluware's maintained, validated platform.



### Titan Intelligent MCP Server / Services Framework

Provide a standardized MCP interface and a services framework for coordinating agents, Gluware capabilities, and external services.

# Connect exposure assessment to verified action.

Bring device advisories, contextual CVE assessment, and supported remediation into a governed network process.

A growing volume of advisories and AI-driven vulnerability discovery increases the pressure to assess and act faster. Device and software information identify the starting point; configuration and operational context help determine which findings matter in the live network. The business needs that assessment connected to a safe response.

## NETWORK EXPOSURE MANAGEMENT



### Discover devices and retrieve advisories

Gluware uses API integration with NIST/NVD for multi-vendor CVE information and Cisco Support API integration for Cisco PSIRT advisories, including their CVEs. Cisco CVE information comes from Cisco, not NIST/NVD.



### Determine relevant exposure

Titan Exposure Analysis evaluates vulnerability relevance using OS, configuration, and operational context. This read-only assessment extends the advisory information already available through Device Manager.



### Select and execute a supported response

Titan Exposure Remediation connects relevant findings to supported patches or compensating controls. OS Manager handles software deployment plans; Config Model Editor handles modeled CLI/API configuration changes. Each operation follows its supported execution path.



### Coordinate, verify, and record

Network RPA and supported integrations can connect assessments, change tasks, approval steps, and records. Verification is designed around the relevant finding and the supported process; displaying an advisory alone does not establish that exposure has been removed.

## Security and trust in the automation foundation

Role-based access control (RBAC), detailed audit logging, LDAP and RADIUS authentication, SAML single sign-on (SSO), OAuth with Proof Key for Code Exchange (PKCE), and two-factor authentication support enterprise access policies. Authentication modes are configured alternatives. Centralized credential management uses AES-256-CBC encryption and integrates with CyberArk through Gluware Vault. TLS protects configured connections; organization-level data retention controls manage stored artifacts and logs.

[Technical documentation](#) | [Request a demo](#)

**Request a demo.**