Network exposure management

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

Titan is Gluware's AI and agentic architecture, delivering an agentic framework, MCP services, Titan Co-Pilot, and embedded agentic features and capabilities.

The business requirement

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.



HOW THE CAPABILITY WORKS

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.

Network exposure management

Connect the operating process to defined component responsibilities.

COMPONENTS DELIVERING THE CAPABILITY

Device Manager	Supplies inventory, software context, and associated vendor/NVD advisories.
Titan Exposure Analysis	Assesses contextual CVE relevance without making changes.
Titan Exposure Remediation	Adds supported remediation capability.
OS Manager	Performs software image deployment operations.
Config Model Editor	Performs modeled CLI/API configuration changes and defined state checks.
Network RPA	Coordinates tasks and connected operational processes.
ServiceNow Integration	Supplies configured CMDB, record, and service-process integrations.

OPERATING SCOPE

Device Manager: advisory sources

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. Cisco Support API also provides EoL/EoS and SmartNet status.

Titan Exposure Analysis: read-only assessment

Adopt visibility without enabling remediation. The business can evaluate the assessment process before deciding whether to authorize automated changes.

Titan Exposure Remediation: supported response

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

Business value and measurement

Measure relevant exposure addressed and the time to verified remediation. Teams can begin with assessment, then authorize supported remediation according to their operating rules. Device Manager advisory data and Titan's contextual assessment are distinct contributions to the same capability.

Technical documentation | Request a demo