COMPONENT OVERVIEW

Titan Exposure Analysis

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

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



A matching software version is only the start of the investigation.

Security teams need to understand which advisories apply to the operating network and why. Manually matching CVEs to software, checking configuration, and inspecting device state can delay decisions while new advisories continue to arrive. Exposure Analysis applies agentic assessment to that context without changing the network.

CORE FUNCTIONALITY

Evaluate operating context

Assess vulnerabilities against discovered OS information, configuration, and operational state rather than relying on the version alone.

Support actionable decisions

Use the assessment to identify relevant findings and consider the response appropriate to the supported environment.

Start with read-only assessment

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

Business contribution

Relevant assessment helps teams direct remediation effort toward the exposure that matters in their environment. It provides a practical first step toward agentic network operations while leaving authorization for infrastructure changes with the customer.

Titan Exposure Analysis

Functions, dependencies, and operating boundaries.

RELATED FUNCTIONS AND 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 Remediation: supported response

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

DIAL: device-aware validation

Apply deterministic, model-aware validation and translation for the infrastructure being managed. The same foundation supports intent-based operations and validation of proposed AI actions.

> **Working with the wider platform**
>
> Exposure Analysis is the assessment component of Titan Exposure Management. Exposure Remediation adds governed write operations when customers are ready to take that next step. Both use the Gluware platform foundation.

Supports: Network exposure management; NIST & Cisco CVE/PSIRT integrations.