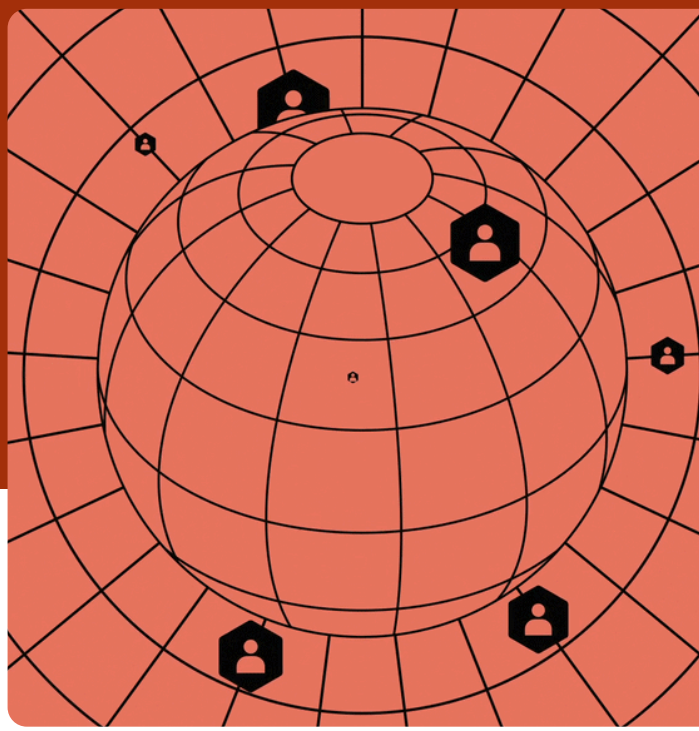
SecurityScorecard

DATA SHEET

TITAN Secure

Threat-Informed Third-Party Risk Management



PRODUCT OVERVIEW

TITAN Secure provides a revolutionary threat-informed solution that transforms how organizations identify, prioritize, and act on cyber risks across their supply chain. With unified continuous monitoring, real-time breach intelligence, and automated discovery into a single workflow, TPRM and Security teams can proactively make data-driven decisions to address common challenges:

- **Siloed Risk Data:** Assessment results, security ratings, and breach feeds often live in disconnected tools, creating an incomplete and fragmented picture of risk.
- **The "Shadow" Vendor Gap:** Organizations lack visibility into unknown 3rd and hidden 4th-party partners, creating a massive, unmanaged attack surface.
- **Noise Without Context:** Security teams struggle to separate critical threats from thousands of alerts, with no clear way to prioritize risks based on actual business impact.
- **Friction-Heavy Outreach:** Manual, email-based communication with vendors delays remediation during critical security incidents or zero-day events.

TITAN Secure addresses these challenges through a fundamentally more resilient Threat-Informed Methodology. The platform non-intrusively scans the global IPv4 web space every day to identify misconfigurations and compromises. It then automatically enriches these technical signals with granular internal vendor data, such as data access levels and service criticality to prioritize the risks that pose the most significant threat to your bottom line.

Use Cases

Breach Insights and Triage

Assessing the impact of a vulnerability across the supply chain.

Shadow Vendor Discovery

Revealing unknown 4th-party concentration risks that could lead to systemic failures.

Continuous Compliance

Mapping real-time vulnerabilities to regulatory controls to maintain an auditable, evergreen trail of oversight.

Key Features

Automatic Vendor Discovery: Surfaces 4th-party relationships hiding on the extended attack surface that legacy GRC tools miss.

Exchange Hub & File Vault: Replaces messy email threads with a centralized “many-to-many” engagement tool and secure evidence repository to accelerate the onboarding and remediation lifecycle.

Real-Time Security Event Insights: Instantly translates technical security events into an executive-ready “Blast Radius” report to quantify potential business impact and triage efforts.

Vendor Contact Management: Reach vendor-provided contacts and add additional contacts to facilitate seamless vendor collaboration.

Advanced Filters for Prioritization: Empowers teams to instantly isolate high-criticality vendors (e.g., those with PII access) to focus resources where they matter most.

Unified Observation Workflows: Provides a single, consistent way to track the state of security findings from creation through resolution across the entire ecosystem. Observation types include:

- Vulnerabilities
- Application misconfigurations
- DNS misconfigurations
- Information leak
- Insecure endpoints
- Out of date products
- Potential compromise
- Typosquatting

What’s possible with TITAN Secure

Benefit	Outcome
Operational Efficiency	Streamlines security findings into a single, predictable workflow, eliminating the need to pivot between disconnected tools.
Risk Reduction	Converts security incidents into actionable "blast radius" assessments to measure business impact.
Proactive Outreach	Proactively reach out to your vendors about high risk security findings in their ecosystem to reduce the risk of an event later on.
Accelerate Response	Empower your team to instantly respond when an event occurs without trying to derive impact across multiple tools triage the event in one place.
Internal Reporting	Generate reports to share internally to demonstrate what happened and what you're doing about it.
Frictionless Vendor Engagement	No need to hunt down contacts for every vendor when an incident occurs. TITAN Secure provides contacts for 100K+ organizations in our ecosystem, taking the guessing out of your remediation processes. Your vendors benefit from a unified platform to respond and manage requests.

Technical Details

Data Capacity

Collects over 27 billion data points every single week to fuel threat-informed insights.

Scanning Performance

Non-intrusive scans of global IPv4 space across 1,500+ ports everyday.

Integrations

Designed to ingest data from existing security findings and seamlessly integrate with legacy TPRM platforms like ServiceNow, OneTrust, and ProcessUnity.

Management

Centralized VRM Dashboard and Download Center for real-time visualization and auditable data repository.