

SOLUTION BRIEF

PICUS PLATFORM AND THREATCONNECT INTEGRATION

Integration Benefits

✓ **Validation-Based Risk Modeling**

Through its integration with ThreatConnect, Picus transforms validated exploitability and control efficacy data into accurate, business-aligned risk metrics.

✓ **Evidence-Backed Financial Risk**

Replace assumptions with validated control performance. Quantify financial exposure based on real adversary techniques mapped to MITRE ATT&CK.

✓ **Business-Aligned Prioritization**

Connect exposures to business units, services, and critical assets, enabling security teams to focus remediation where it matters most.

✓ **Continuous CTEM Alignment**

Support the Continuous Threat Exposure Management (CTEM) cycle with validated, dynamic risk scoring instead of static maturity assessments.

✓ **Credible Communication for Executives**

Turn technical findings into decision-ready metrics, backed by data you can defend to auditors, insurers, and leadership.

Evidence-Based Cyber Risk Quantification with Validation:

The Picus x ThreatConnect Integration

Cyber risk is no longer a theoretical exercise. Boards, insurers, and business leaders want clear, defensible, and financially grounded answers to a simple question: What is our real cyber risk, and what should we fix first?

Traditional risk quantification tools rely on questionnaires, assumptions, or maturity guesses. This leads to polished but unreliable scores that don't reflect how controls actually perform. Picus and ThreatConnect solve this problem by combining continuous adversary simulation with rigorous financial risk modeling, giving organizations a transparent and evidence-based view of cyber risk.



How Picus x ThreatConnect RQ Integration Works

1. Picus simulates attacks using real adversary techniques mapped to the MITRE ATT&CK framework.
2. The Picus Platform evaluates control performance and identifies exposures within the organization's environment.
3. Validated exposure data feeds directly into ThreatConnect Risk Quantifier (RQ).
4. ThreatConnect RQ calculates financial risk uniquely for each organization, considering factors such as exploitability, asset value, threat actor activity, and real-world control effectiveness.
5. Results appear in the Picus Business Risk Dashboard, providing clear financial impact metrics, top threat actors, and prioritized risk across the organization.

ABOUT PICUS

At Picus Security, our priority is making it easy for security teams to continuously validate and enhance organizations' cyber resilience.

Our Security Validation Platform simulates real-world threats to measure control effectiveness, confirm exploitable exposures, and identify high-risk attack paths to critical assets.

As the pioneer of Breach and Attack Simulation, we help organizations operationalize Continuous Threat Exposure Management (CTEM) with validated evidence, clear prioritization, and faster remediation.

Experience Picus in Action

[GET A DEMO](#)



4.9/5.0
#1
Solution Provider

4.8/5.0
Highest-rated
Vendor



Gartner, Voice of the Customer for Adversarial Exposure Validation, Peer Contributors, 30 October 2025

GARTNER is a registered trademark and service mark, and the GARTNER PEER INSIGHTS CUSTOMERS' CHOICE badge and PEER INSIGHTS are trademarks and service marks, of Gartner, Inc. and/or its affiliates in the U.S. and internationally and are used herein with permission. All rights reserved.

Gartner Peer Insights content consists of the opinions of individual end users based on their own experiences with the vendors listed on the platform, should not be construed as statements of fact, nor do they represent the views of Gartner or its affiliates. Gartner does not endorse any vendor, product or service depicted in this content nor makes any warranties, expressed or implied, with respect to this content, about its accuracy or completeness, including any warranties of merchantability or fitness for a particular purpose.

© Picus Security. All Rights Reserved.

All other product names, logos, and brands are property of their respective owners in the United States and/or other countries.

Enhancing Cyber Risk Decisions with Validation With Picus x ThreatConnect Risk Quantification Integration

Together, Picus and ThreatConnect give organizations something they've never had before: a transparent, defensible, and continuously updated view of cyber risk grounded in measurable evidence.

This integration enables teams to replace theory with validation, prioritize action based on true financial impact, and communicate risk in clear business terms. It strengthens CTEM programs with validated exploitability data and helps organizations make faster, more confident decisions at every stage of the risk lifecycle. By uniting Picus' adversary simulations with ThreatConnect's industry-leading financial modeling, organizations can finally connect cyber risk to business reality.



Picus Security Validation Platform

Picus Security Validation Platform simulates cyber threats to consistently validate, measure and enhance organizations' cyber resilience. It facilitates a more proactive and threat-centric approach to security by automatically evaluating the effectiveness of security controls, identifying high-risk attack paths, and helping to optimize threat prevention and detection capabilities.

Why is security validation important?

- Controls don't perform out-of-the-box and must be customized.
- New threats mean that security tools can lose their effectiveness.
- Infrastructure drift creates weaknesses that can go unaddressed.
- Pentesting is vulnerability-focused and quickly out of date.
- Boards, auditors & insurers want evidence of security effectiveness.