

Picus Exposure Validation

Defensible Decisions for Every Exposure, No Exploit Required



Picus Exposure Validation proves which exposures are exploitable in your environment without firing a live exploit, including the restricted assets and day-one CVEs a live test can't safely reach, so every call rests on evidence.

Problem:
Expanding Attack Surface & Unproven Risk

Metric	Pain Point
~135 new CVEs / day ¹ , and <0.5% ever patched ²	Backlog grows faster than any team can safely clear
Only ~32% of the attack surface tested each year ³	Critical, restricted, and air-gapped assets go unproven
~1% of CVEs ever exploited in the wild ⁴	Every call rests on assumptions, not evidence

Solution:
Picus Exposure Validation

Map any CVE to the TTP chain its exploitation requires, then validate that chain against your real, deployed controls, no live exploit fired.

- **Reach what live exploits can't.** Restricted, air-gapped assets, and day-one CVEs, validated.
- **Act on real risk.** What your controls miss and attackers can reach, not what scores high, a 9.8 in the world can be a 2 in your environment.
- **Decide on evidence.** Patch, Mitigate, Monitor, or Accept with evidence.

Cover what live tests can't
No Exploit Needed

Prove exploitability where no live exploit can safely run, on restricted, air-gapped, and day-one exposures a live test can't safely reach.

Cut the backlog
98%

Smaller critical backlog⁵

Deprioritize what your controls already block, proven by evidence, then clear the queue.

Respond faster
89%

Lower MTTR⁵

Evidence-backed response to the exposures that are truly exploitable, not just the ones that score high.

Core Capabilities

- ✓ **TTP-chain validation**
Decompose any CVE into the techniques an attacker must chain to exploit it, then validate each step against your real, deployed controls.
- ✓ **Day-one exploitability**
Get an exploitability verdict the day a CVE drops, before your scanner has even run, so you act while the window's still open.
- ✓ **Closed-loop remediation**
Ready-to-deploy signatures and detection rules, then re-validate to prove the gap is closed. One fix blocks a technique CVEs share, present and future.

- ✓ **Evidence-based prioritization**
Picus Exposure Score and Picus Asset Score blend control performance, asset criticality, business context, and exploit signals (CVSS, EPSS, KEV).
- ✓ **Control-aware decisions**
Base every result on your real, deployed defenses (EDR, GPO, LSASS protection, allow-listing, firewall), not a static CVSS or EPSS label.
- ✓ **One evidence pipeline, one answer**
Unify automated pentest, manual pentest, bug bounty, and breach and attack simulation results into a single pipeline, findings plus proof.

¹ 2025 Vulnerability Forecast: Year-End Review by FIRST, ² Project Glasswing: An initial update by Anthropic, ³ 2026 OMDIA RESEARCH · AI PENTESTING EDITION, ⁴ The 2026 VulnCheckExploit Intelligence Report, ⁵ Single Picus customer data; results may vary based on the environment, ⁶ Picus Customer Results

Picus Exposure Validation

One part of the Picus validation loop

Picus Exposure Validation is the TTP-chain validation engine of the Picus Platform. Alongside Autonomous Pentesting and Breach and Attack Simulation, it runs one continuous loop: validate, decide, fix, re-validate, so every decision rests on evidence.

Security Control Validation
Breach and Attack Simulation
Picus Breach and Attack Simulation continuously tests the live stack to validate which prevention and detection controls actually work.

Exploit-Chain Validation
Autonomous Pentesting
Executes real exploit chains against reachable assets to show what an attacker can actually reach and do, safely, in production.

This Product
Exposure Validation
Proves exploitability without firing an exploit, covering the restricted assets and CVEs no live test can safely touch.

How It Works | From a CVE to a defensible decision, no live exploit fired.

1. INGEST
Take any CVE or finding
Pull in any CVE, scanner finding, or asset, reachable or not, from the tools you already run.

2. MAP
Break down the TTP chain
Break the exploit into the techniques an attacker must chain. One technique recurs across a whole family of CVEs.

3. VALIDATE
Test against your controls
Run each technique against your real, deployed defenses, no live exploit fired.

4. DECIDE
Resolve with evidence
Patch, Mitigate, Monitor, or Accept with evidence, each backed by the chain, controls, and result.

Then it re-validates as your controls and assets change, so the decision stays current.

Connect to the Tools You Already Trust

Picus Platform offers out-of-the-box API integrations across every layer of your security stack, with 75+ integrations spanning on-prem, cloud, and hybrid, so you maximize the value of your existing security investments.



picussecurity.com

Experience Picus *in Action*

GET A DEMO

FALL 2026

Leader

4.8/5.0

#1 Solution Provider*

Breach and Attack Simulation

*G2, Breach and Attack Simulation (BAS) Solutions, Fall Grid Report, 1 September 2026

Gartner

Peer Insights

Customers' Choice 2026

4.8/5.0

Highest-rated vendor*

Adversarial Exposure Validation

*Gartner, Voice of the Customer for Adversarial Exposure Validation, Peer Contributors, 27 August 2026