

Picus Breach and Attack Simulation

Validate what your security controls actually stop



Picus Breach and Attack Simulation continuously tests what your EDR, SIEM, firewall, and WAF actually block and detect against the newest attacker techniques, then provides the fixes and re-validates that the gap closed.

Problem:
Controls you assume work, but cannot prove

Without continuous testing, security teams cannot be sure their controls still stop the attacks that matter, or prove it to the board.

- Prevention and detection controls are deployed once, then **assumed to keep working** as threats evolve.
- Configuration drift, product updates, and new attacker techniques **quietly erode coverage** between assessments.
- Manual control testing needs red team skill and **does not scale** across a changing environment.

Solution:
Picus Breach and Attack Simulation

Picus safely emulates real attacker behavior against your live controls, shows exactly what they miss, and validate what they stop.

- **Validate prevention and detection controls** at scale, with no manual scripting or red team expertise required.
- **Pinpoint where controls miss the latest TTPs** across your EDR, SIEM, firewall, and WAF.
- **Close gaps with ready-to-deploy mitigations**, then re-validate that the fix held.

Test Against the Newest Threats

Run continuous, ATT&CK-mapped attack scenarios across your full stack, with emerging threats available within 24 hours of emergence.

> **2x control effectiveness in 3 months**

Fix Gaps Fast

Step-by-step guidance plus vendor-specific signatures and detection rules let you shorten MTTR and harden defenses.

> **89% reduction in MTTR for emerging threats**

Prove Measurable Impact

Evidence-based scoring shows where your controls reduce the most risk, so every action is board-ready.

> **92% fewer high or critical SLA violations**

Core Capabilities

- ✓ **Security control validation (SCV)**
Measure and optimize prevention and detection effectiveness with continuous, ATT&CK-mapped Breach and Attack Simulation.
- ✓ **Cloud security validation (CSV)**
Validate cloud configurations and identities across AWS, Azure, and GCP to surface misconfigurations and privilege risks.
- ✓ **Ready-to-deploy mitigations**
Get vendor-specific prevention signatures and detection rules mapped to every gap, so fixes ship in hours, not weeks.

- ✓ **Detection rule validation (DRV)**
Test SIEM and EDR rules to verify alerts fire as intended, cut false positives, and streamline detection engineering.
- ✓ **AI Threat Builder**
Turn any blog URL, PDF, CVE ID, or threat-actor name into a playable, ATT&CK-mapped simulation in minutes.
- ✓ **Always-current threat coverage**
Draw on 30,000+ TTPs and threat scenarios, with a 24-hour SLA for critical emerging threats from Picus Labs.

Picus Breach and Attack Simulation

One part of the Picus validation loop

Breach and Attack Simulation is the control-effectiveness engine of the Picus Platform. It works alongside two other validation components in a continuous loop, validate, decide, fix, re-validate, so you act on what attackers can truly exploit and validate what your defenses stop.

This Product

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

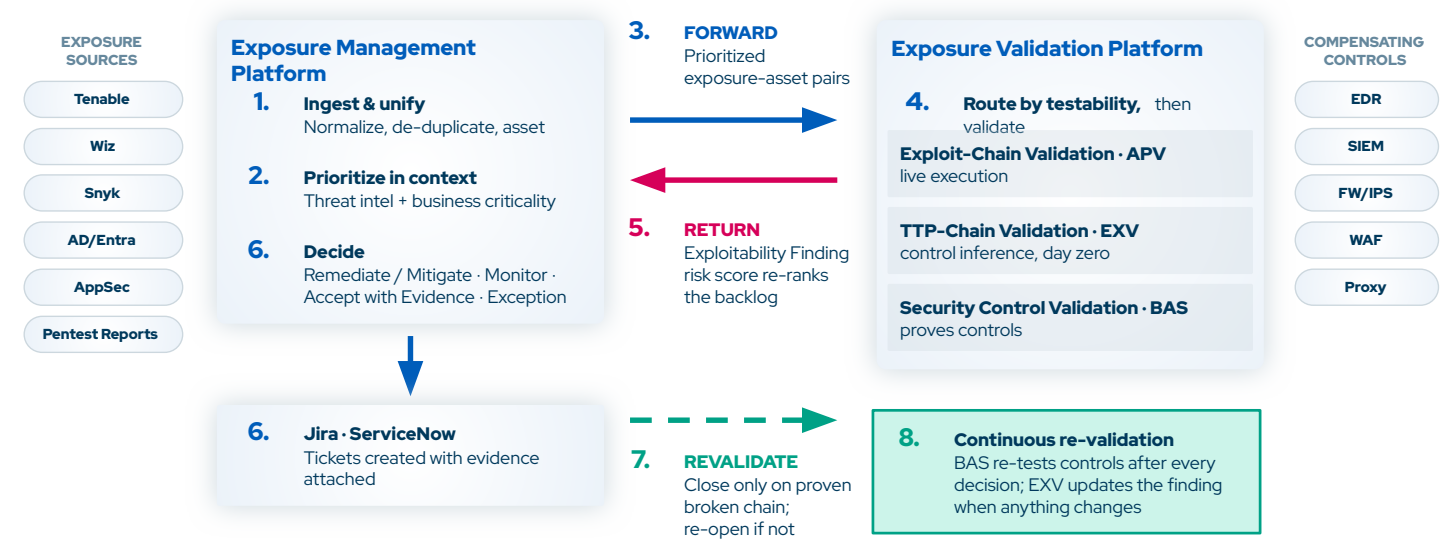
Autonomous Pentesting

Executes real exploit chains against reachable assets to show what an attacker can actually reach and do, safely, in production.

TTP-Chain Validation

Exposure Validation

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



AI Built for Security Teams

AI accelerates Breach and Attack Simulation across the Picus Platform, generating custom, ATT&CK-mapped threat scenarios from intelligence reports through AI Threat Builder, correlating attack data, and guiding remediation through Numi AI.

picussecurity.com

Experience Picus *in Action*

GET A DEMO



4.8/5.0

#1 Solution Provider*
Breach and Attack Simulation

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