PICUS x NATICA

SECURITY CONTROL VALIDATION

High Performance Breach & Attack Simulation

Reduce risk by validating detection and prevention effectiveness

Organizations struggle to understand which cybersecurity threats will have the most impact on their business operations. Security teams need the ability to fine-tune both detection and prevention by validating the effectiveness of their controls. By validating, teams can easily identify and shut down the most business-critical cyber threats, improving their overall security posture.

What Security Control Validation Does

Picus Security Control Validation (SCV) is a breach and attack simulation (BAS) product that:

- **Identifies gaps in your security posture** through on-demand testing of your existing security infrastructure and controls
- **Validates the efficacy of your controls** against thousands of real-world threats, including malware, ransomware, vulnerability exploits, APTs, and more with the Picus Threat Library
- **Provides vendor-specific mitigations and actionable remediation recommendations** to save time
- **Gives industry and geographical context**, improving alert relevance and decreasing alert noise
- **Tracks security posture changes over time with continuous or on- demand testing** of infrastructure changes, network issues, and configuration drift, enabling a consistent security posture
- **Integrates with top SIEMs and EDRs,** targeting whether alerts and vulnerabilities are detected and logged
- **Maps simulation results against The MITRE ATT&CK Framework**, to quickly identify gaps and prioritize threat mitigations that pose the greatest risk to your organization

Product Highlights:

✓ **Save time and focus on what matters**
Prioritize high-risk vulnerabilities and misconfigurations while demoting low-risk gaps

✓ **Identify context-based gaps and get actionable mitigation recommendations**
Simulate real-world cyber threats

✓ **Optimize SecOps**
Let your SecOps teams work on what matters

✓ **Maximize your security stack's effectiveness**
Measure the efficacy and scalability of your existing cybersecurity investments

✓ **See if your security profile is improving over time**
Continuous, repeatable, and on-demand testing and validation for your security controls and ops

Comprehensive Integrations:

Network Security	SIEM	EDR	XDR
Cisco	Splunk>	Microsoft Defender for Endpoint	Trend Micro
Citrix	Microsoft Sentinel	CrowdStrike	SentinelOne
Paloalto Networks	IBM Security QRadar	VMware Carbon Black	Cortex XSOAR

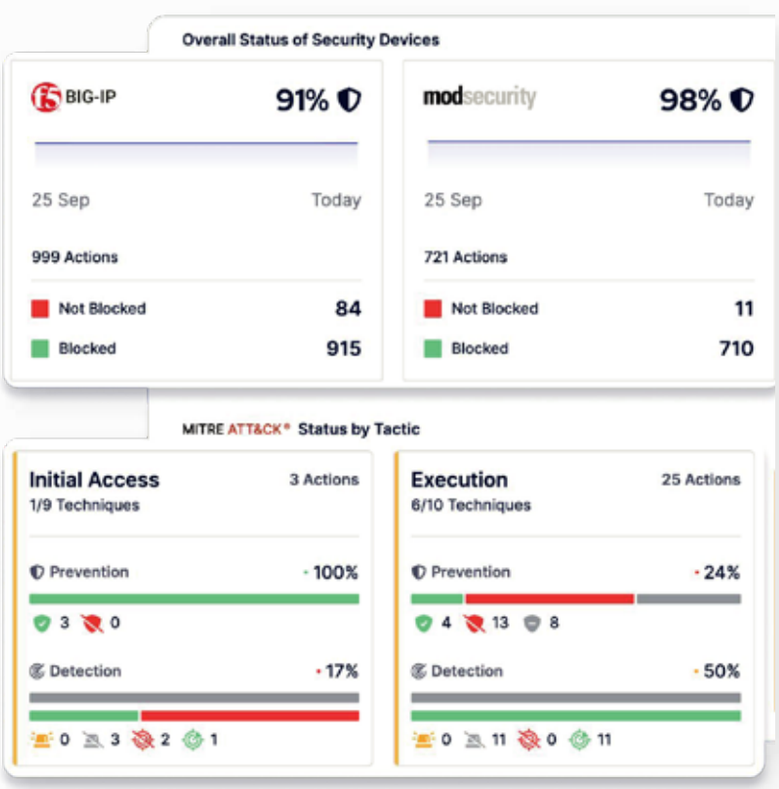
More partnerships are added regularly. To see our latest integrations visit: picussecurity.com/integrations

How We Solve the Problem

Unmatched Breach and Attack Simulation

Picus BAS has the added benefit of our proven threat simulations and premium threat library, powered by award-winning breach and attack simulation (BAS) technology, the cornerstone of Picus's Security Validation Platform. SCV measures and strengthens your cyber resilience by continuously testing the effectiveness of your security controls. SCV simulates the full attack cycle including insider threats, lateral movement, and data exfiltration with:

- **Superior Content -** Picus provides the building blocks to create and execute simulations tailored to your business using our extensive, daily-updated threat library, threat templates, threat intelligence, and threat builder feature.
- **Actionable Learnings / Insights to Mitigations -** Easily take the next steps through vendor-specific mitigations, MITRE ATT&CK mappings, and customizable reports
- **Breach and Attack Simulations -** This is where we pull it all together so you can validate controls, discover gaps, and take proactive measures



MITRE ATT@CK Mapping

Visualize the threat coverage provided by your security controls against the MITRE ATT&CK framework to build a more resilient security posture.

Picus maps to the framework providing up to date data on Privileged Access, Persistence, Execution, Initial Access and more.

SCV Features:

✔ Operationalize the MITRE ATT&CK® framework providing threat coverage visualization to quickly identify gaps and prioritize high-risk threat mitigations

✔ Validate technologies focusing on Continuous Threat Exposure Management (CTEM)

✔ Customize threats and attack scenarios

✔ Compare security scores across geographies, industries, and against other members of our extensive global user community

✔ Supports cross-platform operating systems - Windows, MacOS, and Linux

Gartner Peer Insights Customers' Choice 2024

Highest Rated Vendor

4.8/5

Gartner, Voice of the Customer for Breach and Attack Simulation Tools, Peer Contributors, 30 January 2024

Pasific Plaza A Blok Sevinçli Sok. N:3 K:8 Küçükbakkalköy Ataşehir 34750 İstanbul
Tel: +90 (212) 296 61 90 E-mail: infoNatica@natica.com.tr
www.natica.com.tr